

Тема 1. Вступ

- 1.1. Чому вивчається передача даних?
- 1.2. Передача даних
- 1.3. Комп'ютерні мережі
 - 1.3.1. Поняття та архітектура комп'ютерної мережі
 - 1.3.2. Розподілена обробка
 - 1.3.3. Мережні критерії
 - 1.3.4. Застосування
- 1.4. Протоколи і стандарти

Л []

1.1. Чому вивчається передача даних?

Всесвітня мережа Інтернет та WWW технологія, де широко використовується передача даних, є прикладом справжньої можливості глобальної співпраці (прикладі глобального зв'язку в одній країні, між країнами тощо).

Слід відмітити, що комп'ютерні мережі змінюють діяльність людини та спосіб її життя. Ділові рішення приймаються набагато швидше, а особи, що приймають рішення повинні мати швидкий доступ до достовірної інформації. Але, щоб знати наскільки швидко ми можемо зв'язатися за допомогою мережі, ми повинні знати як працюють мережі, які типи технологій доступні. Коли в організації або навчальному закладі з'являється новий підрозділ, технологія повинна бути гнучкою, щоб відобразити зміну конфігурації. Розуміння цих процесів та знання, коли використовувати кожен тип технології є суттєвим для забезпечення підтримки динамічної зміни інформаційного середовища.

Поява персонального комп'ютера привела до значних змін у бізнесі, промисловості, науці, і освіті. Технологія обробки інформації, не кажучи про підготованих спеціалістів, стала дружньою для нетехнічних робітників, щоб використовувати. Продавці, бухгалтери, професори, дослідники, секретарі, адміністратори почали проектування їхнього власного розкладів spreadsheets, подань, і баз даних. Корпорації і університети почали купляти мікрокомп'ютери, щоб полегшити управління інформацією. Оскільки ці мікрокомп'ютери були встановлені, то традиційні термінали, які забезпечили пасивні зв'язки з центральними процесорами, були усунуті. Термінальна емуляція через РС в даний момент забезпечила новий гострий біль у з'єднанні з центральним сервером.

Навіть зі всіма цими новими показниками степеня виконання, люди не мали ефективного шляху, щоб спільно використовувати дані. За винятком тих комп'ютерів, що приєднані безпосередньо до центрального процесора, будь-кому, хто хотів отримати або послати інформацію, було необхідно зробити це вручну. У новіших комп'ютерах, дані могли б або бути скопійовані на дискету і фізично перевантажені на інший РС, або надрукований та надіслані поштою, факсом, або кур'єром до адресата; потім повторно завантажені на віддалений комп'ютер. Це не тільки було тратою часу, але також створило інші незручності.

І стандарти продуктивності також змінювалися. Чому чекати тиждень на дані з іншої країни поштою, коли, якщо комп'ютери могли б передавати дані один одному, це могло б пройти майже миттєво?

Подібна революція відбувається в мережах передачі даних. Технологічна прередача просування робить це можливим для зв'язків комунікацій, щоб перенести більші і швидші сигнали. У результаті, служби розвиваються, щоб дозволити використання розширеної розрядності, включаючи розширення до встановлених телефонних служб, як наприклад

селекторна нарада, голосова пошта; нові цифрові служби включають відео конференції і пошук інформації.

Розробка відповідних апаратних засобів була одним із викликів проектувальників мережі. Проектування зв'язків між персональними комп'ютерами, робочими станціями, та іншими цифровими пристроями вимагає розуміння потреб користувачів. Як інформація передається? Хто використовує спільно дані і, який вид використовується спільно? Скільки фізично потрібно передавати інформацію? Розділення даних обмежується до окремого комп'ютера всередині одного офісу, або дані також потрібно використати спільно з локальними пересувними офісами, або з непередбаченою кількістю абонентів у всьому світі? Фактично, щоб управляти роботою ефективно, багато установ сьогодні повинні мати більш ніж один тип мережі.

1.2. Передача даних

Коли ми спілкуємося, ми спільно використовуємо інформацію. Цей розподіл може бути локальним або віддаленим. Між індивідами, локальний зв'язок звичайно відбувається персонально, в той час, як віддалений зв'язок розподілений у просторі. Термін телекомунікації, який включає телефон, телеграф, і телебачення, означає зв'язок на віддалі (“теле” грецькою означає далеко).

Слова “Дані” відноситься до фактів, принципів, і команд, представлених в будь-якій формі та погоджується сторонами, що створюють і використовують дані. У контексті комп'ютерних інформаційних систем, дані представляються за допомогою елементів (або біті) двійкової інформації, вироблених і використаних у вигляді нулів та одиниць.

Передача Даних є обмін даними (у вигляді 0 і 1) між двома пристроями через певну форму передачі (як наприклад провід чи кабель).

Передача даних вважається локальною, якщо комунікаційні пристрої є в тій же будівлі або обмеженій географічній зоні, і вважається віддаленою, якщо пристрої на великій віддалі.

В комп'ютерних системах дані представляються двійковими одиницями (або бітами), що передаються і приймаються у вигляді нулів і одиниць.

Щоб відбулася передача даних, комунікаційні пристрої повинні бути частиною системи комунікації складеної з комбінації апаратних засобів і програмного забезпечення. Ефективність системи передачі даних залежить від трьох основних характеристик:

1. Доставка. Система повинна доставити дані до потрібного адресата. Дані повинні бути отримані за допомогою призначеного пристрою або користувача і тільки за допомогою того пристрою або користувача.
2. Точність. Система повинна доставити дані точно. Дані, які були змінені в передачі і залишені невірними, є непридатними.
3. Своєчасність. Система повинна доставити дані до вчасно. Дані, доставлені пізно, є непотрібними. У випадку даних відео, звуку, і голосу, своєчасна доставка означає доставку даних тоді, коли вони створюються, у тому ж порядку, що вони створюються, і без суттєвої затримки. Цей вид доставки називається передача в реальному масштабі часу.

Система передачі даних складається з п'яти компонентів (рис. 1.1).

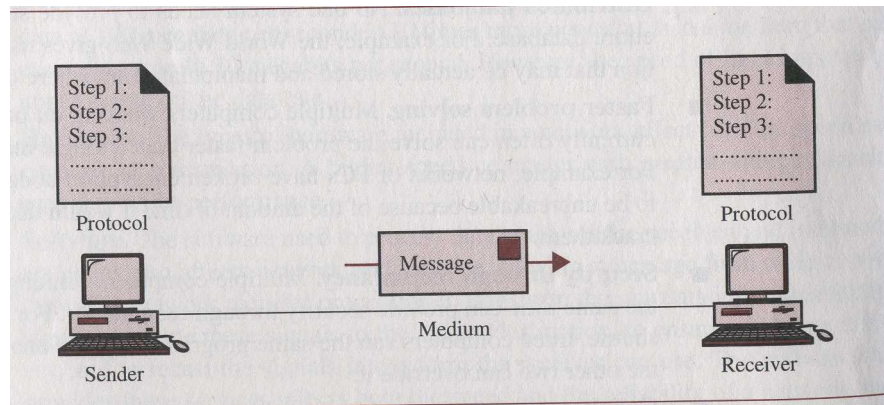


Рис. 1.1. Компоненти системи передачі даних.

1. Повідомлення. Повідомлення є інформацією (даними) для передачі. Воно може складатися з тексту, чисел, зображень, звуку, відео або будь-якої їх комбінації.
2. Відправник. Відправником є пристрій, який посилає повідомлення. Він може бути комп'ютером, робочою станцією, телефонним апаратом, відеокамерою, тощо.
3. Приймач. Приймачем є пристрій, який отримує повідомлення. Це може бути комп'ютер, робоча станція, телефонним апарат, телевізор, тощо.
4. Носій. Носієм передачі є фізичний маршрут, яким повідомлення посилається від відправника до приймача. Це може бути вита пара, коаксіальний кабель, оптоволоконний кабель, лазер, або радіохвилі (наземні або супутникові мікрохвилі).
5. Протокол. Протоколом є набір правил, які керують передачею даних. Це угоду між комунікаційними пристроями. Без протоколу, два пристрої можуть бути з'єднані, але не можуть передавати дані.

1.3. Комп'ютерні мережі

1.3.1. Поняття та архітектура комп'ютерної мережі

Комп'ютерна мережа – це система розподіленої обробки інформації, що складається як мінімум із двох комп'ютерів, які взаємодіють між собою за допомогою засобів зв'язку.

Засоби зв'язку мають забезпечувати надійну передачу інформації між комп'ютерами мережі. Комп'ютери, що входять до складу мережі. Комп'ютери, що входять до складу мережі, виконують досить широке коло функцій, основними з яких є:

- організація доступу до мережі;
- керування передачею інформації;
- надання обчислювальних ресурсів і послуг абонентам мережі.

При розгляді комп'ютерних мереж широко використовуються поняття: клієнт і сервер. На структурному рівні під сервером розуміється комп'ютер, що надає свої ресурси іншим комп'ютерам, названим клієнтами.

На програмному рівні під сервером і клієнтом маються на увазі процеси (програми), що виконують відповідно, функції надання і використання мережевих ресурсів. Крім того, комп'ютери, через які користувачі одержують доступ до ресурсів комп'ютерної мережі, прийнято називати робочими станціями.

За функціональним призначенням комп'ютерів, мережі прийнято поділяти на однорангові і мережі на основі серверів. В одноранговій мережі всі комп'ютери рівноправні, кожний з них може бути як клієнтом, так і сервером. При цьому ресурси кожного комп'ютера умовно поділяються на локальні і мережеві. Локальними називаються власні ресурси кожного з комп'ютерів, незалежно від того підключений він до мережі чи ні. Мережевими називається частина локальних ресурсів, які надає кожний комп'ютер в загальне користування іншим комп'ютерам. Якщо один з комп'ютерів мережі використовує ресурси іншого комп'ютера, то він виступає у ролі клієнта. Відповідно, процесор, що надає ресурси, вважається

на цей момент сервером. Однорангова організація зазвичай використовується в невеликих мережах, що включають не більше 10 комп'ютерів.

У мережах на основі серверів виділяються окремі комп'ютери для серверів і клієнтів. Для кожного виду мережевих ресурсів створюється свій сервер, наприклад, файловий сервер, сервер преси, сервер бази даних тощо.

Комп'ютерні мережі у свою чергу поділяються на глобальні і локальні. Глобальні мережі охоплюють значні території, це може бути окрема держава, один або декілька континентів. Наприклад, мережа Інтернет охоплює всю земну кулю. Локальна мережа розміщується в рамках окремої організації або корпорації.

Будь-яка комп'ютерна мережа характеризується своєю архітектурою, яка визначається (рис. В.1) її топологією, протоколами, інтерфейсами, мережевими технічними і програмними засобами. Топологія комп'ютерної мережі відображає структуру зв'язків між її основними елементами. Через низку причин існує відмінність між топологіями глобальних і локальних мереж. Топологія глобальних мереж характеризується достатньо складною, неоднорідною структурою. У свою чергу, топологія локальної мережі, зазвичай, має визначену структуру: лінійну, кільцеву або деревоподібну.



Протоколами називають правила взаємодії функціональних елементів мережі.

Інтерфейси – це засоби сполучення функціональних елементів мережі. Варто звернути увагу, що у ролі функціональних елементів можуть виступати як окремі пристрої, так і програмні модулі. Відповідно до цього, існують апаратні і програмні інтерфейси.

Під мережевими технічними засобами мають на увазі різноманітні пристрої, що забезпечують об'єднання комп'ютерів в єдину комп'ютерну мережу. До цих пристроїв відносяться мережеві контролери, вузли комутації та ін.

Мережеві програмні засоби керують роботою комп'ютерної мережі і забезпечують відповідний інтерфейс з користувачами. До мережевих програмних засобів належать мережеві операційні системи і допоміжні (сервісні) програми.

Кожна із складових архітектури комп'ютерної мережі характеризує її окремі властивості, і тільки їх сукупність характеризує всю мережу загалом. Таким чином, вибір комп'ютерної мережі може бути зведений до вибору її топології, протоколів, апаратних засобів і мережного програмного забезпечення. Кожна з цих компонент є відносно незалежною. Наприклад, мережі з однаковою топологією можуть використовувати різні методи доступу, протоколи і мережеве програмне забезпечення. У різних мережах можуть застосовуватись однакові протоколи і (або) мережеве програмне забезпечення. Це розширює можливість вибору най-і більш оптимальної архітектури комп'ютерної мережі.

1.3.2. Розподілена обробка

Мережі використовують розподілену обробку, в якій завдання розділяється між багатьма комп'ютерами. Замість поодинокі великої машини, відповідальної за всі аспекти процесу, окремий комп'ютер (звичайно персональний комп'ютер або робоча станція) є піднабором.

Переваги розподіленої обробки включають наступне:

- **Захист/герметизація.** Розробник системи може обмежити вид взаємодії, які даний користувач може мати з повною системою. Наприклад, банк може дозволити доступ користувачів до їхніх власних об'ємів ресурсів системи через автоматизовану машину (АТМ) без дозволу їх доступу до повної бази даних банку.
- **Розподілені бази даних.** Жодній системі не потрібно надавати ємність запам'ятовувального пристрою для повної бази даних. Наприклад, World Wide Web надає доступ користувачів інформації, яка може дійсно зберігатися і оброблятися де-небудь в Internet.
- **Швидше розв'язування проблеми.** Багато комп'ютери, які працюють над частинами проблеми одночасно, часто можуть розв'язати проблему, швидше, ніж одинока машина. Наприклад, мережі комп'ютерів розшифрували коди, які були недоступні для одного комп'ютера.
- **Захист через надлишковість.** При виконання багатьма комп'ютерами та ж програма може забезпечити захист через надлишковість. Наприклад, в Шатлі, три комп'ютери виконують ту ж програму, так щ при апаратній похибці, інші два можуть замінити.
- **Партнерське виконання.** Як багато комп'ютерів, так і багато користувачів можуть взаємодіяти над завданням. Наприклад, в мережєвих іграх з багатьма користувачами дії кожного гравця є видимими для всі і впливають на інших.

1.3.3. Мережні критерії

Щоб бути розглянутим ефективним і ефективним, мережа повинна відповідати критеріям. Найбільш важливими з них є продуктивність, надійність, і захист (рис. 1.2).

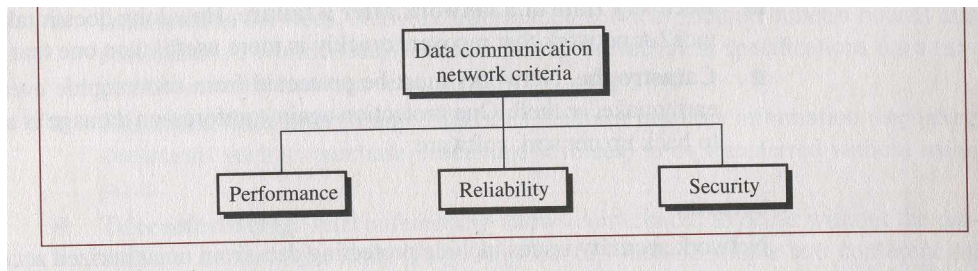


Рис. 1.2. Мережеві критерії

Продуктивність може бути виміряна багатьма способами, включаючи транзитний час і тривалість відповіді. Транзитний час є кількість часу, який вимагається для повідомлення, щоб передаватися від одного пристрою до іншого. Тривалість відповіді є тривалість розробки між запитом і відповіддю.

- Продуктивність мережі залежить від кількості коефіцієнтів, включаючи кількість користувачів, тип передавального носія, можливості зв'язаних апаратних засобів, і ефективність програмного забезпечення.
- Кількість користувачів. Коли є велика кількість одночасних користувачів можна сповільнити тривалість відповіді в мережі, не розроблений, щоб координувати важкі завантаження потоку обміну. Проект даної мережі базується на вимозі про виплату внеску за акції середньої кількості користувачів, які спілкуватимуться в будь-який момент. У періодах пікового завантаження, однак, фактична кількість користувачів може перевищити середню величину і таким чином зменшити продуктивність. Як мережа відповідає на завантаження є мірою продуктивності.
- Тип передавального носія. Носій визначає швидкість, з якою дані можуть передаватися (швидкість передач даних). Сьогодні мережі переміщуються до швидшого і швидшого передавального носія, як наприклад оптоволокно. Носій, який може перенести

дані в 100 megabits за секунду, є в 10 разів потужнішим, ніж носій, який може перенести дані тільки в 10 megabits за секунду. Однак, швидкість легко нав'язує верхню границю швидкості передач даних.

- Апаратні засоби. Типи апаратних засобів, які включаються в мережу впливають як на швидкість так і розрядність передачі. Комп'ютер вищої швидкості з більшою ємністю запам'ятовувального пристрою забезпечує кращу продуктивність.
- Програмне забезпечення. Програмне забезпечення, яке використовується, щоб виконувати дані у відправникові, приймачі, і проміжних вузлах, також впливає на продуктивність мережі. Переміщення повідомлення від вузла до вузла через мережу вимагає, щоб виконання перетворило неопрацьовані дані в готові до передачі сигнали, щоб послати ці сигнали до відповідного адресата, щоб гарантувати безпомилкову доставку, і, щоб привести сигнали у вираз, який приймач може використовувати. Програмне забезпечення, яке забезпечує таке обслуговування, впливає як на швидкість, так і надійність мережевого зв'язку. Добре розроблене програмне може пришвидшити процес і зробити передачу більш ефективною.

На додаток до точності доставки, мережева надійність вимірюється за допомогою частоти відмови, часу, який потрібний зв'язок, щоб опрацювати відмову, і стійкість мережі при аварії.

- Частота відмови. Всі мережі інколи аварійно завершуються. Мережа, що часто несправна є непотрібною користувачу.
- Час відновлення мережі після відмови. Скільки треба часу, щоб відновити службу? Мережа, яка відновлюється швидко є більш корисною.

- Відмова. Мережі повинні бути захищені від катастрофічних подій, як наприклад вогонь, землетрус, або крадіжка. Один захист проти непередбаченого пошкодження є надійна система копіювання мережевого програмного забезпечення.

Мережеві проблеми безпеки (захисту) включають захисти даних від несанкціонованого доступу і вірусів.

- Несанкціонований доступ. Для того, щоб мережа була корисна, чутливі дані повинні бути захищені від несанкціонованого доступу. Захист може бути завершений в кількості рівнів. На нижньому рівні є коди ідентифікації користувача і паролі. На вищому рівні є методи кодування. У цих пристроях, дані систематично змінюються таким шляхом, що, якщо вони перехоплені за допомогою несанкціонованого користувача, вони будуть нерозбірливі.
- Віруси. Через те, що мережа є доступною від багатьох, вона може бути вразливою до комп'ютерних вірусів. Вірус є незаконно представлений код, який пошкоджує систему. Хороша мережа захищається від вірусів за допомогою апаратних засобів і програмного забезпечення, розробленого специфічно для цього.

1.3.4. Застосування

За короткий час мережі передачі даних стали обов'язковою частиною промисловості, науки, освіти, індустрії розваг. Деякі мережеві **застосування** в різних галузях є наступним:

- Торгівля. Обчислювальні мережі широко використовуються як в торгівлі, так і організаціях збуту. Професіонали торгівлі використовують їх, щоб зібратися, обмінятися даними, і аналізувати дані, які мають відношення до потреб вимоги і циклів розробки виробів. Програми збуту включають

teleshopping, який використовує комп'ютери або телефони, приєднані до мережі виконання команди, і on-line служби замовлення для готелів, авіаліній, і так далі.

- Фінансові служби. Сьогодні фінансові служби повністю залежать від обчислювальних мереж. Додатки включають пошуки кредитної історії, іноземну валюту і служби інвестиції, і електронну передачу фондів, яка дозволяє користувачу перенести гроші без відвідування банку.
- Виробництво. Обчислювальні мережі використовуються сьогодні в багатьох аспектах виробництва, включаючи промисловий процес безпосередньо.
- Електронний обмін повідомленнями. Можливо найбільш широко уживаний мережевим додатком є електронна пошта.
- Служби Каталога. Служби Каталога дозволяють спискам файлів зберігатися в центральному сховищі.
- Інформаційні служби. Мережеві інформаційні служби включають дошки оголошень і банки даних. World Wide Web розташовують пропозицію технічних специфікацій на новий продукт в інформаційній службі.
- Електронний обмін даними. Він дозволяє діловій інформації (включно з документами, як наприклад замовлення на поставку і накладні) бути перенесеним без паперу.
- Teleconferencing. Телеконференція дозволяє конференціям відбутися без учасників, які є в тому ж приміщенні. Додатки включають conferencing з простим текстом (де учасники спілкуються через їхні клавіатури і комп'ютерні монітори), голосові conferencing (де учасники в кількості розміщень спілкуються одночасно по телефону), і відео conferencing (де учасники можуть як дивитися, так і говорити один з одним).

- Мобільний телефон. У минулому, двох сторонах бажання використовувати служби телефонної компанії було необхідно з'єднати за допомогою фіксованого фізичного зв'язку. Сьогодні мобільні мережі роблять це можливим, щоб підтримати безкабельні телефонні зв'язки.
- Кабельне телебачення. Майбутні служби, забезпечені за допомогою мереж кабельного телебачення, можуть включати відео на запит, також як і та ж інформація, фінансовий, і служби комунікацій, на даний момент забезпечені за допомогою телефонних компаній і обчислювальних мереж.

1.4. Протоколи і стандарти

Протоколи:

У обчислювальних мережах зв'язок відбувається між суб'єктами в різних системах. Об'єкт є будь-що, здатне до передачі або отримання інформації. Приклади включають прикладні програми, пакети передачі файлів, вікна перегляду, керування бази даних, і програмне забезпечення електронної пошти. Система є фізичним об'єктом, який містить один або суб'єктів. Приклади включають комп'ютери і термінали.

Але два суб'єкти можуть не тільки послати бітові потоки один одному і сподіватися, щоб їх зрозуміли. Для з'єднання, суб'єкти повинні домовитися про протокол. Протоколом є множина правил, які керують передачею даних. Протокол визначає те, що спілкується, як спілкується, і, коли повідомлено. Ключовими елементами протоколу є синтаксис, семантика, і узгодження в часі.

- Синтакс звертається до структури або формату даних, означаючи команду, в якій вони представлені. Наприклад, простий протокол міг би сподіватися, що перші вісім бітів є адресою відправника,

других вісім бітів, які є адресою приймача, і потік, який є повідомленням безпосередньо.

- Семантика означає кожну секцію бітів. Як є специфічне зображення обробляється, і, яка дія приймається на основі інтерпретації? Наприклад, в адресі ідентифікують маршрут, який приймається або кінцевого адресата повідомлення?
- Час означає дві характеристики: коли дані повинні бути послані, і як швидко вони повинні дійти.

Стандарти передачі даних попадають в дві категорії: де-факто і де-юре (рис. 1.3).

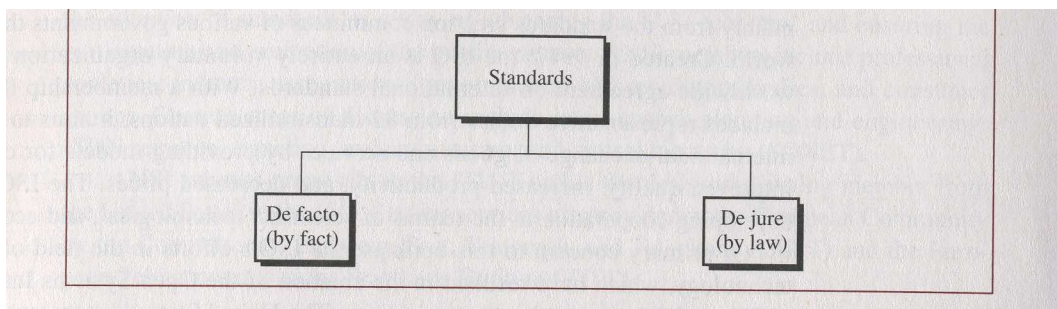


Рис. 1.3. Категорії стандартів

Стандарти De-jure є тими що були видані законно за допомогою офіційно визнаного органу. Стандарти, які не були схвалені за допомогою організованого органу, але, були прийняті, оскільки стандарти через дуже поширене використання є стандарти de-facto. Стандарти De-facto часто встановлюються оригінально за допомогою пошуку фірм-виробників, щоб визначити функціональні можливості нового продукту або технології.

Стандарти De-facto можуть надалі бути поділені на два класи: приватний і не приватний. Приватні стандарти є оригінально розробленими за допомогою комерційної організації, як основа для операції продуктів. Вони зветься приватними, через те, права на них має компанія, яка розробила їх. Ці стандарти також зветься закритими стандартами, через те, що вони

закривають від комунікації між системами, виробленими за допомогою різних продавців. Не приватні стандарти є тими, що оригінально розробляються за допомогою груп або комітетів, які перетворили їх у державну власність; вони також зветься відкритими стандарти, через те, що вони відкривають комунікації між різними системами.

Стандарти розробляються за допомогою співробітництва між комітетами розробки стандартів, форумами, і контрольними органами уряду.

Комітети Розробки Стандартів

У той час, як багато організації присвячуються заснуванню стандартів, дані і дистанційні зв'язки в Північній Америці залежать перш за все від тих, опублікованих за допомогою наступного:

- Організація Міжнародних Стандартів (ISO).
- Міжнародний Сектор Стандартів Дистанційного Зв'язку Союзу Дистанційних Зв'язків (ITU-T, раніше МККТТ).
- Американський Національний Інститут Стандартів (ANSI).
- Інститут Електричних і Електроніки Інженерів (IEEE).
- Електронна Асоціація Індустрій (EIA).
- Telcordia.

ISO

Є багатонаціональним органом, чие членство витягається створюється з комітетів утворення стандартів різних урядів. Створений в 1947, ISO є цілком добровільною організація, присвячена всесвітньо відомій угоді на міжнародних стандартах. З членством, що на даний момент характерні органи з 82 країн. ISO є активним в співробітництві наукової, технологічної, і економічної діяльності.

ITU-T

З початку 1970, кількість країн визначала національні стандарти для дистанційних зв'язків, але був досі небагато міжнародної сумісності.

Організація об'єднаних Націй відповідальна за формування частини Міжнародного Союзу (МСЕ) Дистанційних зв'язків, комітету, Консультативної Комісії для Міжнародної Телеграфії і Телефонування (МККТТ). Цей комітет захопився дослідженням і заснуванням стандартів або дистанційних зв'язків взагалі і телефонної системи даних зокрема. На Березні, 1993, ім'я цього комітету було змінено на Міжнародний Сектор Стандартів Дистанційного зв'язку Союзу телекомунікації (ITU-T).

ITU-T розділяється на групи дослідження з різних аспектів промисловості. Національні комітети (як наприклад ANSI в Сполучених Штатах і СЕРТ в Європі) представляють пропозиції до цих груп дослідження. Якщо група дослідження погоджується, пропозиція ратифікується і стає частиною стандарту ITU-T, що видається кожні чотири роки.

Відомі стандарти ITU-T вищого ступеня є серія (V V.32, V.33, V.42), які визначають передачу телефонними лініями; серія (X X.25, X.400, X.500), які визначають передачу над експортованими цифровими мережами; електронна пошта і служби каталога; і Інтегрована Цифрова Мережа Служб (ISDN), яка включає частини іншої серії і визначає міжнародну цифрову мережу, що з'являється.

ANSI

Незважаючи на ім'я, Американський Національний Інститут (ANSI) Стандартів є цілком таємна неприбутковою корпорацією, не встановлює зв'язків з федеральним урядом США. Однак, всі види діяльності ANSI є зв'язані з добробутом Сполучених Штатів. Виражена мета ANSI's включає служіння національною установою координування для добровільної стандартизації в Сполучених Штатах, прийняття стандартів, як шлях просування економіки США. Елементи ANSI включають професійні товариства, асоціації промисловості, урядові і регулярні органи, і споживчі групи.

ANSI представляє пропозиції до ITU-T і є визначеним елементом голосування від Сполучених Штатів до ISO. Подібні служби забезпечуються в Європейському Товаристві за допомогою Комітету Європейської Пошти, Телеграфу, і Телефону (CEPT) і Європейського Інституту Стандартів Дистанційних зв'язків (ETSI).

IEEE

Інститут Електричних і Електронних Інженерів (IEEE) є найбільше професійне технічне товариство в світі. Інтернаціональне за метою, воно прагне просунути метод, творчість, і якість продукту в галузі електротехніки, електроніки, і радіо також як і у всіх зв'язаних переходах розробки. Як одна з мети, IEEE розглядає розробку і прийняття міжнародних стандартів для обчислення і комунікації. IEEE має спеціальний комітет для локальних обчислювальних мереж (LANs), від яких прийшов Проект 802 (наприклад, 802.3, 802.4, і 802.5 стандартів).

EIA

Вирівняна з ANSI, Електронна Асоціація (EIA) Індустрій є неприбутковою організацією, яка займається сприянням виробництва електроніки. Види діяльності включають експортовану освіту правосвідомості і зусилля лоббі на додаток до розробки стандартів. У полі інформаційної технології, EIA зробила суттєві вклади за допомогою визначення фізичних інтерфейсів зв'язку і електронних сигналізаційних технічних умов для передачі даних. Зокрема, EIA-232-D, EIA-449, і EIA-530 визначають послідовну передачу між двома цифровими пристроями (наприклад, комп'ютер до модему).

Telcordia, яка раніше називалася Bellcore, є відростком Bell Labs. Telcordia проводить дослідження і ресурси розробки для просування дистанційних зв'язків і технології.

Контрольні Органи

Вся технологія комунікацій є схильною до регулювання за допомогою урядових агентств, як наприклад Федеральна Комісія з комунікації (FCC) в Сполучених Штатах. Намір цих агентств - захистити експортований інтерес за допомогою регулювання радіо, телебачення, і провідних/кабельних комунікацій.

FCC

FCC має повноваження над зв'язуючою окремі штати і міжнародною торгівлею, оскільки це має відношення до комунікацій. Кожна частина технології комунікацій повинна мати схвалення FCC перед тим, як це може бути куплене на ринку (перевірте ваш телефон чи комп'ютер на наявність коду FCC). Специфічна відповідальність FCC включає наступне:

- Щоб проглянути коефіцієнт і додатки плати за послуги, створені за допомогою телеграфу і телефонних постачальників.
- Щоб проглянути технічні специфікації апаратних засобів комунікацій.
- Щоб встановити розсудливі коефіцієнти громадського перевізника окупності.
- Щоб відділити і розподілити радіо частоти.
- Щоб присвоїти частоти носія для радіо і телевізійних передач.

Тема 2. Базова концепція

2.1. Конфігурація зв'язку

2.2. Топологія

2.3. Вид передачі

2.4. Різновиди мереж

Л []

Основні Поняття

Перед дослідженням специфічних засобів того, як дані передаються від одного пристрою до іншого важливо зрозуміти зв'язок між суміжними пристроями. П'ять загальних принципів надають основу для цього зв'язку:

- Лінійна конфігурація.
- Топологія.
- Передавальний режим.
- Категорії мереж.
- Internetworks.

2.1. Конфігурація зв'язку

Лінійною конфігурацією називають шляху, яким два або більше пристрої зв'язку під'єднують до лінії. Зв'язок є фізичне з'єднання, яке переміщує дані з одного пристрою до іншого. З метою мисленого уявлення, найпростіше уявити собі зв'язок, як відрізок, між двома точками. Для того, щоб відбувся зв'язок, два пристрої повинні бути з'єднані деяким шляхом до тої ж лінії в той же час. Є дві можливі лінійні конфігурації: двоточкова і багатоточкова (рис. 2.1).

Точка-точка

Конфігурація точка-точка забезпечує визначений зв'язок між двома пристроями. Повна розрядність каналу резервується для передачі між тими двома пристроями. Найбільш конфігурацію точка-точка використовують фактичну довжину шини або кабеля, щоб з'єднати два кінці, але інші опції, як наприклад мікрохвилі або зв'язки сателіта, є також можлива (рис. 2.2). Коли ви змінюєте телевізійні канали за допомогою інфрачервоного дистанційного управління, ви встановлюєте двоточкову лінійну конфігурацію між дистанційним управлінням і системою елемента управління телебачення.

Багатоточковий

Багатоточкова конфігурація (також її називають multidrops) є однією в якій більш ніж два специфічні пристрої використовують спільно поодиноким зв'язок (рис. 2.3).

У багатоточковому середовищі, розрядність каналу використовується спільно, або в просторі або в часі. Якщо окремі пристрої можуть використовувати зв'язок одночасно, це є просторово загальнодоступна лінійна конфігурація. Якщо користувачі повинні робити по черзі, це є загальнодоступна лінійна конфігурація в часі.

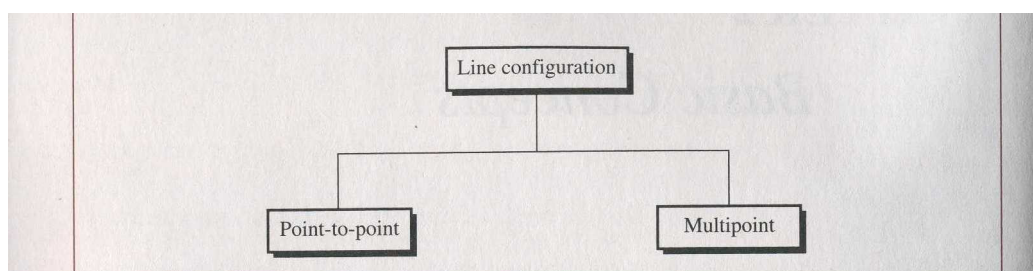


Рис. 2.1. Два категорії передачі даних

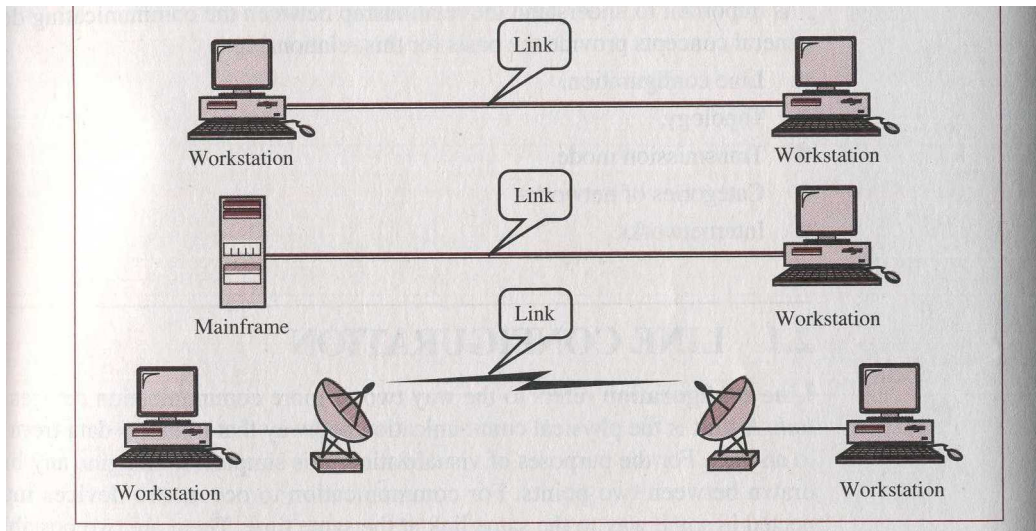


Рис. 2.2. Конфігурація точка-точка

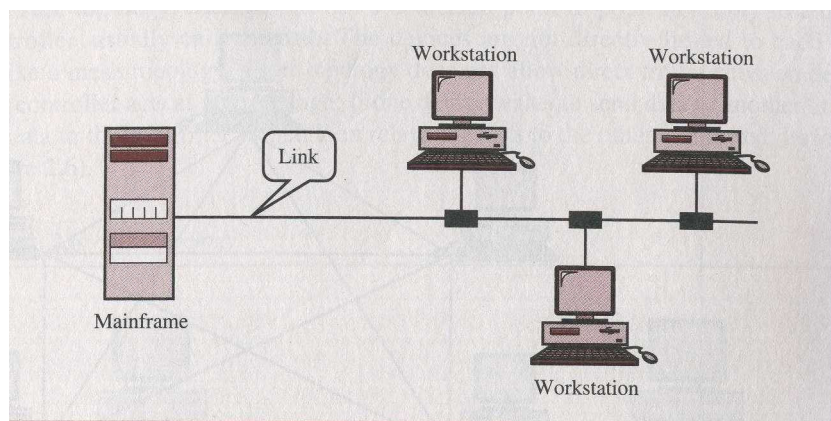


Рис. 2.3. Багатоточкова конфігурація

2.2. Топологія

Під терміном топологія розуміється конфігурація мережу на площині, фізично або логічно. Два або більше пристрої приєднуються до зв'язку; два або більше зв'язки формують топологію. Топологія мережі є геометричним зображенням всіх зв'язків і пристроїв (вузлів)у. Є п'ять основного можливий топологій: mesh, зірка, дерево, шина, і кільце (рис. 2.4).

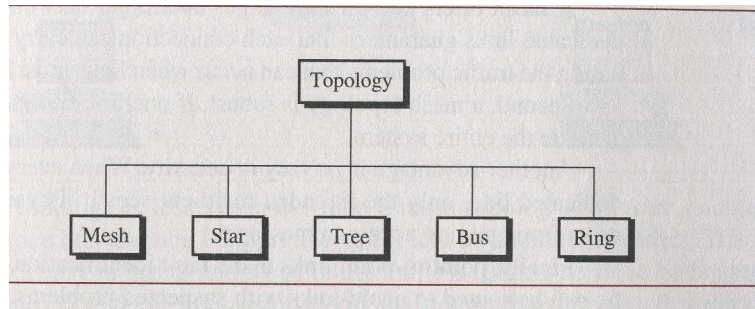


Рис. 2.4. Категорії топологій

Ці п'ять мітки описують те, як пристрої в мережі зв'язуються, швидше ніж їх фізичне розміщення. Наприклад, зіркова топологію не означає, що всі комп'ютери в мережі повинні бути розміщені фізично навколо концентратора. Два зв'язки є можливими: рівний-рівний, де пристрої використовують спільно зв'язок однаково, і первинний-вторинний, де один пристрій контролює трафік.

Сітка

У сітковій топології, кожний пристрій має визначений двоточковий зв'язок з кожним пристроєм (рис. 2.5).

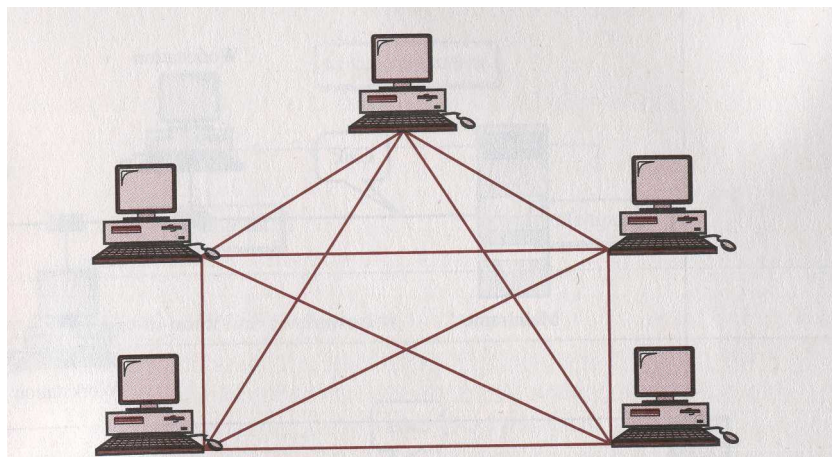


Рис. 2.5. Сіткова топологія

Сітка пропонує окремі переваги над іншою топологією мережі. Спершу, використання визначених гарантованих зв'язків, що кожний зв'язок

може перенести власне завантаження даних, таким чином ліквідуючи проблеми потоку обміну, які можуть відбутися тоді, коли зв'язки повинні бути використані спільно за допомогою багатократних пристроїв.

Другий, сіткова топологія є надійною. Якщо один зв'язок стає непридатним, це не виводить з ладу повну систему.

Інша перевага є таємність або захист. Коли кожне повідомлення передано по певній лінії, тільки назначений приймач бачить це. Фізичні границі запобігають іншим користувачам від доступу до повідомлень.

Нарешті, двоточкові зв'язки роблять ідентифікацію помилки і легку ізоляцію дефекту. Потік обміну може бути розбитий, щоб уникнути зв'язків з підозрюваними проблемами. Ці засоби надають мережевому адміністратору можливість виявити розміщення несправності і допомагають у виявленні причини і розв'язку.

Головні невігоди сіткової топології зв'язані з кількістю кабеля і кількістю портів, яких вимагається. Спершу, через те, що кожний пристрій повинен бути приєднаний до кожного іншого пристрою, установка і переконфігурація є важкою. Другий, справжній об'єм проводки може бути більший, ніж доступний пропускна здатність. І, остаточно, апаратні засоби, яких вимагається, щоб з'єднати кожний зв'язок, можуть бути дорогі. З цих причин сіткова топологія звичайно здійснюється до певної міри.

Зірка

У зіркоподібній топології, кожний пристрій має відданий двоточковий зв'язок тільки до центрального контроллера, звичайно викликав концентратор. Пристрої безпосередньо не з'єднуються один з одним. На відміну від сіткової топології, зіркоподібна топологія не дозволяє прямий потік обміну між пристроями. Контроллер служить для обміну: Якщо один пристрій хоче послати дані до іншого, він посилає дані до контроллера, який потім передає дані до іншого пристрою (рис. 2.6).

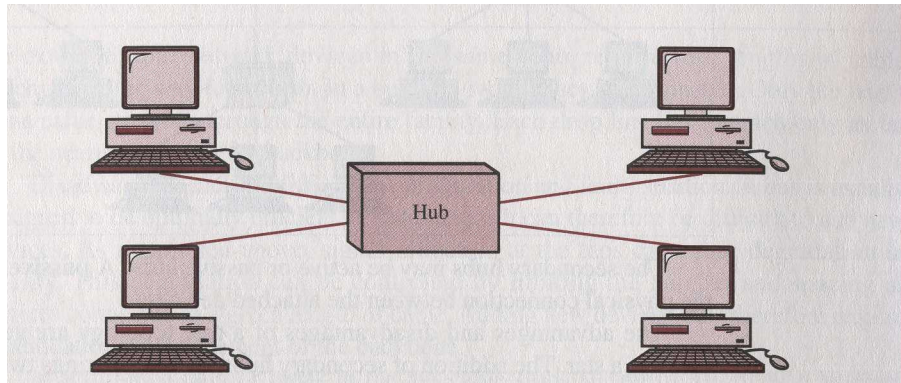


Рис. 2.6. Зіркова топологія

Зіркоподібна топологія є дешевшою, ніж сіткова топологія. У зірці, кожний пристрій потребує тільки одного зв'язку і одного порту, щоб приєднати його до будь-якої кількості інших. Цей також полегшує встановлення і переконфігурування. Менше потрібно кабелів.

Інші переваги включають стійкість. Якщо один зв'язок аварійно завершується, інші зв'язки залишаються активними. Цей коефіцієнт також надає себе до легкої ідентифікації помилки і дефектної ізоляції. Поки концентратор працює, це може використовуватися, щоб спостерігати проблеми зв'язку і обхідні недосконалі зв'язки.

Однак, хоч зірка вимагає далеко меншого кабелю, ніж сітка, кожен вузол повинен бути з'єднаним з центральним концентратором. З цієї причини більшого укладання кабелю вимагається в зірці, ніж в деякій іншій топології (як наприклад дерево, кільце, або шина).

Дерево

Деревоподібна топологія є відхиленням зірки. Як в зірці, вузли в дереві з'єднуються з центральним концентратором, який контролює потік обміну до мережі. Однак, не кожний пристрій підключає безпосередньо в центральний концентратор. Більшість пристроїв приєднуються до вторинного концентратора, що по черзі приєднується до центрального концентратора (рис. 2.7).

Центральний концентратор в дереві є активний концентратор. Активний концентратор містить повторювач, який є пристроєм апаратних засобів, який відновлює отримані двійкові коди перед посиленням їх зовні. Повторення підсилює передачі і збільшує відхилення, яке сигнал може мандрувати.

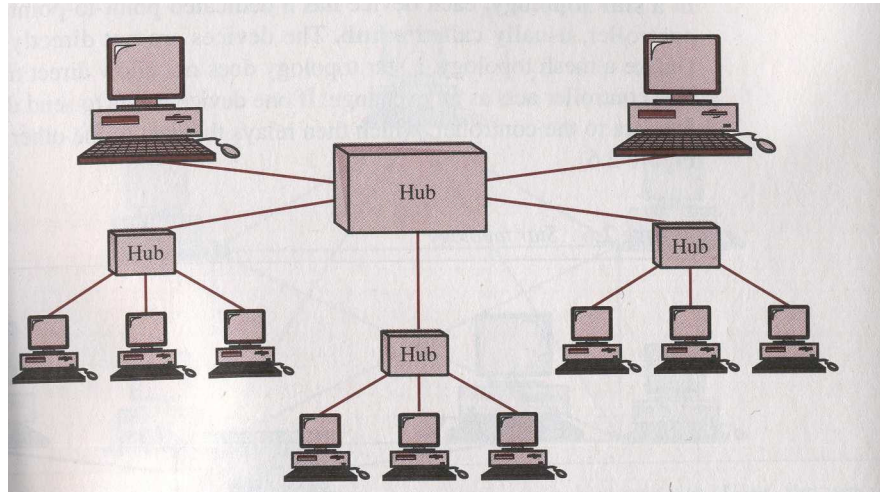


Рис. 2.7. Зіркова топологія

Вторинні концентратори можуть бути активні або пасивні концентратори. Пасивний концентратор забезпечує фізичний зв'язок між під'єднаними пристроями.

Переваги і недоліки деревоподібної топології взагалі так само, як у зірки. Доповнення вторинних концентраторів, однак, приносить дві подальші переваги, це дозволяє більшим пристроям бути під'єднаним до поодинокого центрального концентратора і може таким чином полегшити відхилення, яке сигнал проходить між пристроями. Другий, це дозволяє ізолювати мережу і мають пріоритет над комунікаціями від різних комп'ютерів. Наприклад, комп'ютери, під'єднані до одного вторинного концентратора, може бути наданий пріоритет над комп'ютерами під'єднаними до вторинного концентратора. Цим шляхом, мережеві проектувальники і операція можуть гарантувати чутливі дані часу – немає необхідності чекати доступ до мережі. Хороший приклад деревоподібної топології може бути в кабельній TV, де

кабель від вузлового поштового підприємства розділяється на головні переходи і кожний перехід на менші переходи і так далі. Концентратори використовуються тоді, коли кабель відділений.

Шина

Шинний топологія, з другої сторони, є багатоточковою. Одні довгі кабельні backbone, як основа, щоб з'єднати всі пристрої мережі (рис. 2.8).

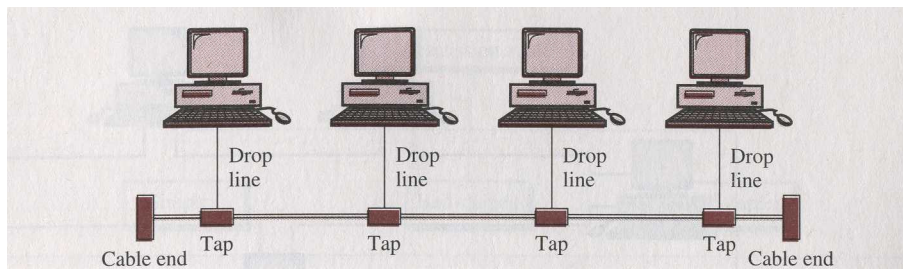


Рис. 2.8. Шинна топологія

Вузли приєднуються до кабеля шини за допомогою строчок відпущення і відводів. Строчка відпущення є виконання заучуваного напам'ять *tap* між пристроєм і головним кабелем. Відвід є з'єднувач, що або *ses* в головний кабель або пробиває вкладення в футляр кабеля, щоб створити контакт з металічним ядром. Як сигнальні мандрівки вздовж основи, деяка енергія є *trans-ned* в тепло. Таким чином, це стає слабшим і слабшим далі, який цьому необхідно мандрувати.

Ця причина є границя на кількості відводів, які шина може підтримувати і на відстань між тими відводами.

Переваги шинного топологія включають легкість установки. Кабель основи може бути вздовж найбільш ефективного маршруту, потім приєднаний до вершин за допомогою строчок відпущення. Цим шляхом, шина використовує менше кабеля, ніж отвір, зірка, або дерев. У зірці, наприклад, чотири мережеві пристрої в тій же кімнаті вимагають чотирьох частин кабеля, який досягає до всього шляху до концентратора. У шині, ця

надлишковість ліквідується. Тільки кабель основи розтягується через повні засоби. Кожній строчці відпущення необхідно досягнути тільки наскільки найближча точка на основі.

Недоліки включають важку переконфігурацію і дефектну ізоляцію. Шина звичайно розробляється, щоб оптимально бути ефективною в установці. Це може таким чином бути важке, щоб додати нові пристрої. Як згаданий вище, сигнальне відображення у відводах може викликати погіршення в якості. Це погіршення може контролюватися за допомогою обмеження номера і проміжку пристроїв, приєднаних до даної довжини кабеля. Додавання нових пристроїв може таким чином вимагати модифікації або заміни основи.

Крім того, несправність або розрив в кабелі шини зупиняє всю передачу, навіть між пристроями на тій же стороні проблеми. Пошкоджена область відображає сигнали назад в напрямі до початку, завади створення в обох напрямках.

Кільце

У кільцевій топології, кожний пристрій має віддану двоточкову лінійну конфігурацію тільки з двома пристроями з обох сторін цього. Сигнал передається вздовж кільця в один напрямку, від пристрою до пристрою, поки це досягає до адресата. Кожний пристрій в кільці об'єднує повторювач. Коли пристрій отримує сигнал intended для іншого пристрою, повторювач відновлює біти і передає їх (рис. 2.9).

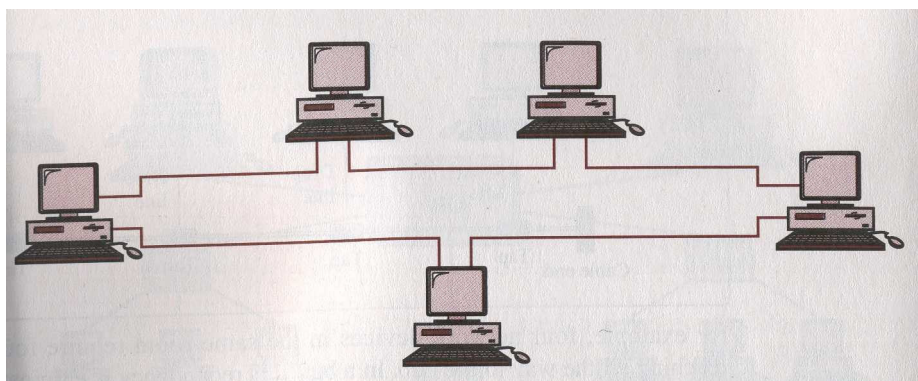


Рис. 2.9. Кільцева топологія

Кільце є відносно легким, щоб встановитися і переконфігурувати. Кожний пристрій з'єднується тільки з невідкладними сусідами (або фізично або логічно). Щоб додати або вилучити пристрій вимагає переміщення тільки двох зв'язків. Єдині обмеження є носій і розгляди потоку обміну (максимальна кільцева довжина і кількість пристроїв). Крім того, дефектна ізоляція спрощується. Взагалі в кільці, сигнал обертається часом весь. Якщо один пристрій не отримує сигнал протягом конкретизованого періоду, це може видати тривогу. Тривога попереджує про небезпеку мережеву операцію до проблеми і розміщення.

Однак, неспрямований потік обміну може бути невигодою. У простому кільці, розрив в кільці (як наприклад відключена станція) може відключити повну мережу. Це безсилля може бути розв'язане за допомогою використання подвійного кільця або перемикача, здатного до закриття від переривання.

Гібридні Topologies

Часто мережа об'єднує окремі topologies, як subnetworks, зв'язаний в більшій топології. Наприклад, один відділ справи, можливо, вирішив використовувати шинний топологія, в той час, як інший відділ має кільце. Два може бути з'єднані один одному через центральний контроллер в зіркоподібній топології (рис. 2.10).

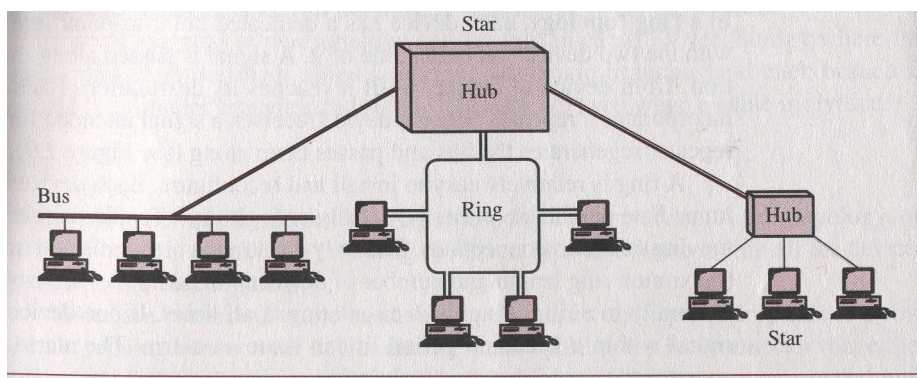


Рис. 2.10. Гібридна топологія

2.3. Вид передачі

Термін передавальний режим використовується, щоб визначити напрям сигнального потоку між двома з'єднаними пристроями. Є три типи режимів передачі: simplex, напівдуплексний, і дуплексний (рис. 2.11).

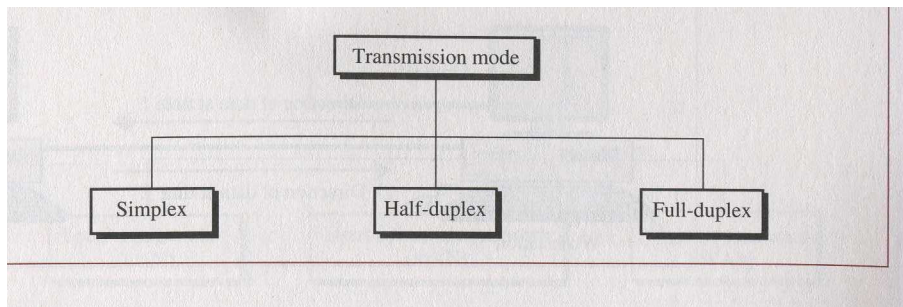


Рис. 2.11. Види передачі

Simplex

У simplex режимі, сполучення непрямоване, як на вулиці з одностороннім рухом. Тільки одна з двох станцій на зв'язку може передати; інша може тільки отримати (рис. 2.12).

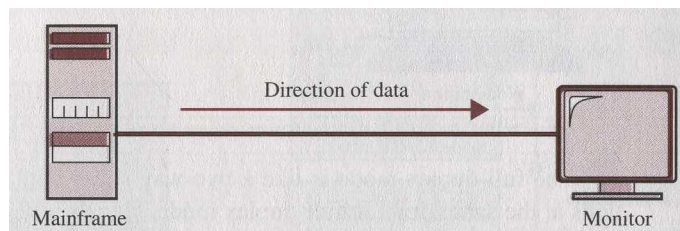


Рис. 2.12 Simplex

Клавіатури і традиційні монітори є прикладом simplex пристроїв. Клавіатура може тільки представити ввід; монітор може тільки прийняти вивід даних.

Напівдуплексний

У напівдуплексному режимі, кожна станція може як передати так і отримати, але не в той же час. Коли один пристрій посилає, інший може тільки отримати, і навпаки (рис. 2.13). Напівдуплексний режим є подібним до однієї вузької дороги з двостороннім рухом. У той час, як автомобілі рухаються в одному напрямку, автомобілів, яким потрібно в іншу сторону повинні. У напівдуплексній передачі, повна розрядність каналу приймається вище ніж потрібно для двох пристроїв під час передачі. Walkie-talkie та СВ радіо є обидві напівдуплексні системи.

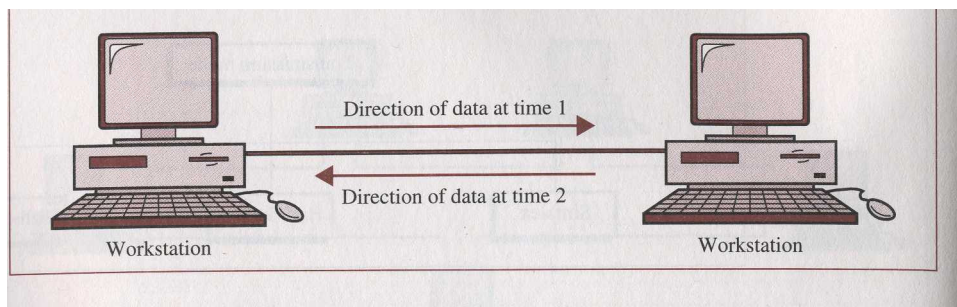


Рис. 2.13. Напів-дуплекс

Дуплексні

У дуплексному режимі, станції можуть, як передати, так і отримати одночасно (рис. 2.14).

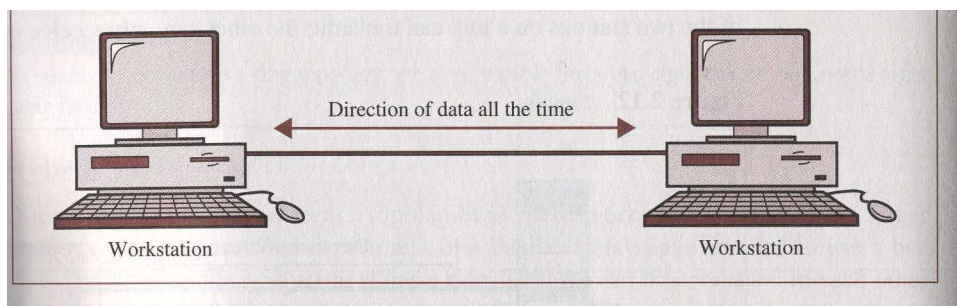


Рис. 2.14. Дуплекс

Повністю-дуплексний режим є подібно двобічній вулиці з витіканням потоку обміну в обох напрямках в той же час. У повністю-дуплексному режимі, сигнали, які ідуть в будь-який напрямку, використовують спільно розрядність зв'язку. Це розділення може відбутися двома шляхами: або зв'язок повинний містити два фізично окремі передавальні маршрути, один

для посилення і інший для отримання, або розрядність каналу відділяється між мандруванням сигналів в розташованих на протилежному боці напрямках.

Один загальний приклад повністю-дуплексного зв'язку є телефонна мережа. Коли двоє людей спілкуються за допомогою телефону, можна як говорити, так і чекати на відповідь в той же час.

2.4. Різновиди мереж

Сьогодні, коли ми згадуємо про мережі, ми взагалі маємо на увазі три початкових категорій: локальні обчислювальні мережі, metropolitan area network, і wide area network. У яку категорію попадає мережа, визначається за розміром, монопольний використанням, відхиленням, і фізичною архітектурою (рис. 2.15).

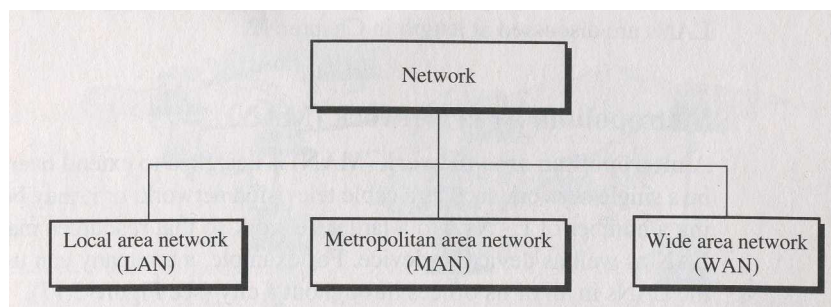


Рис. 2.15. Категорії мереж

Локальна обчислювальна мережа (LAN)

Локальна обчислювальна мережа (LAN) це звичайно використовується приватно і зв'язує пристрої в окремому офісі, будівлі чи кампусі (рис. 2.16). Залежно від потреб організації і типу технології, яка використовується, LAN може бути такою ж простою як два комп'ютери і принтер в чийсь власному офісі, або це може продовжитися через компанію і включати голос, звук, і зовнішні відео пристрої. На даний момент, розмір LAN обмежується до декількох кілометрів.

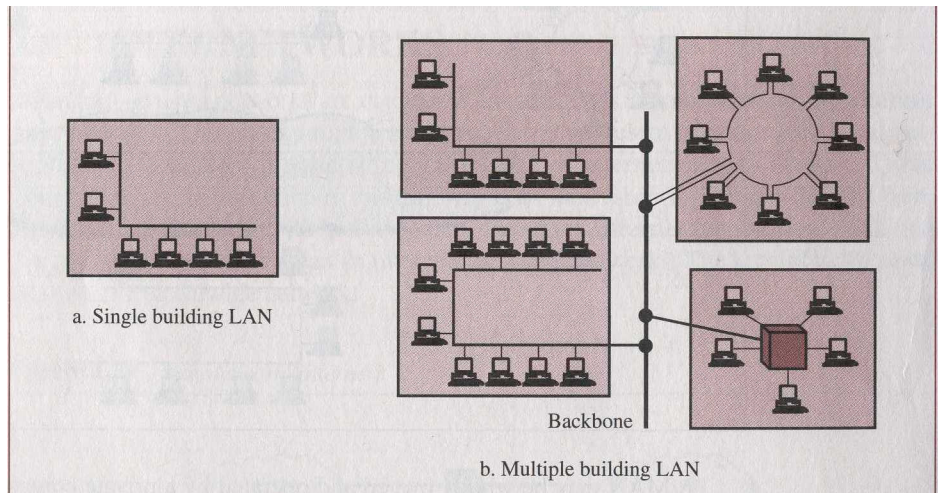


Рис. 2.16 LAN

LANs розробляються, щоб дозволити ресурсам бути використаним спільно між персональними комп'ютерами або робочими станціями. Ресурси, які використовуються спільно можуть включати апаратні засоби (наприклад, принтер), програмне забезпечення (наприклад, прикладна програма), або дані. Загальний приклад LAN, знаходиться в багато ділових додатках, з'єднує робочу групу зв'язаних комп'ютерів завдання, наприклад, працюючи інженером робочі станції або визнаючи за комп'ютери. Одному з комп'ютерів може бути наданий диск великої розрядності і він може стати сервером для інших клієнтів. Програмне забезпечення може зберігатися на цьому центральному сервері і використовуватися, якщо потрібно всією групою. У цьому прикладі, розмір LAN може бути визначений за допомогою ліцензування обмежень на кількості користувачів на копію програмного забезпечення, або за допомогою обмежень на кількості користувачів, які отримали дозвіл, щоб мати доступ до операційної системи.

На додаток до розміру, LANs відрізняються від інших типів мереж за допомогою їхнього передавального носія і топології. Взагалі, даний LAN використовуватиме тільки один тип передавального носія. Найбільш загальний LAN topologies є шина, кільце, і зірка.

За традицією, LANs мають швидкості передач даних в 4 до 16 Mbps області. Сьогодні, однак, швидкості зростають до 100 Mbps з гігабітними системами на перспективу.

Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) розробляється, для продовження над цілим містом. Це може бути поодиноким мережа, як наприклад мережа кабельного телебачення, або це може бути засобами об'єднання кількості LANs в більшу мережу так, щоб ресурси могли бути використані спільно, також як і пристрій до пристрою. Наприклад, компанія може використовувати MAN, щоб з'єднати всі LANs у всіх офісах через місто (рис. 2.17).

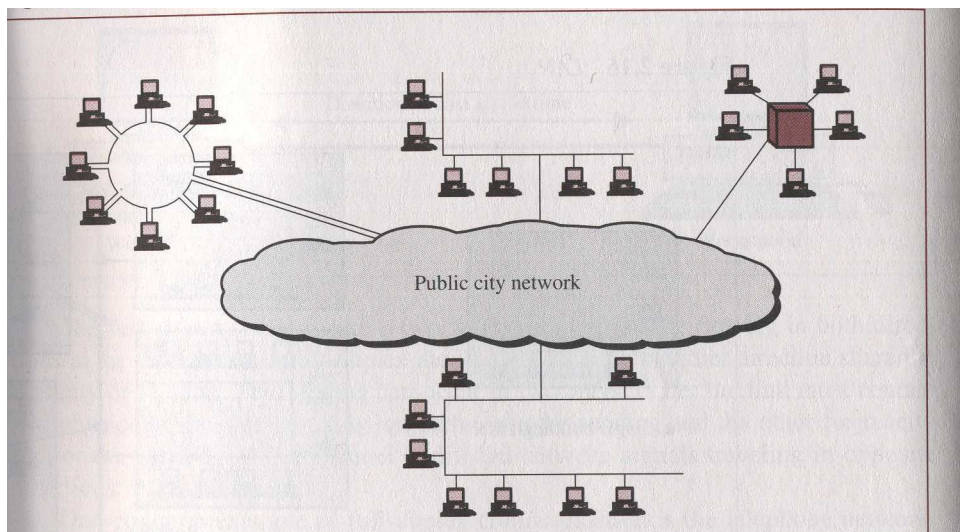


Рис. 2.17. MAN

MAN, часто перебувають у власності окремої компанії, наприклад як телефонна компанія.

Wide Area Network (WAN)

Wide Area Network (WAN) забезпечує віддалену передачу даних, голосу, зображення, і відео інформації у великих географічних областях, які можуть охопити країну, континент, або навіть весь світ (рис. 2.18).

У контрасті до LANs (які залежать від їхніх власних апаратних засобів для передачі), WANs може використати експортовані, здані в оренду, або таємні пристрої сполучення, звичайно в комбінаціях, і може таким чином виміряти безмежну кількість миль.

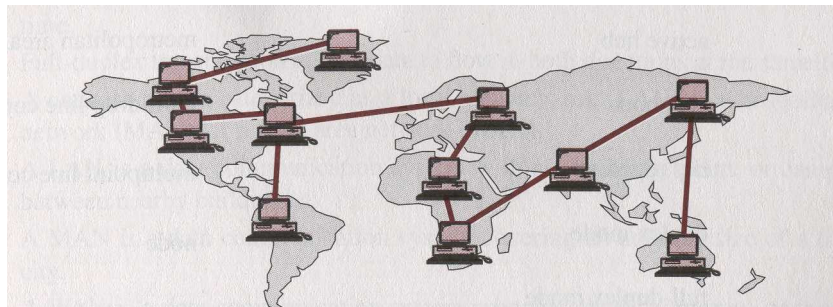


Рис. 2.18. WAN

INTERNETWORKS

Коли дві або більше мереж з'єднані, вони стають *internetwork*, або *internet* (рис. Цифру 2.19; на рисунку, блоки помічені R представляють маршрутизатори). Індивідуальні мережі з'єднуються в *internetworks* за допомогою використання пристроїв міжмережевої взаємодії. Ці пристрої, які включають маршрутизатори і шлюзи, обговорюються в Розділі 21. Термін *internet* (lowercase) не повинен сплутуватися з *Internet* (uppercase). Перше твірний елемент, який використовується, щоб означати взаємозалежність мереж. Друге ім'я специфічної всесвітньо відомої мережі.

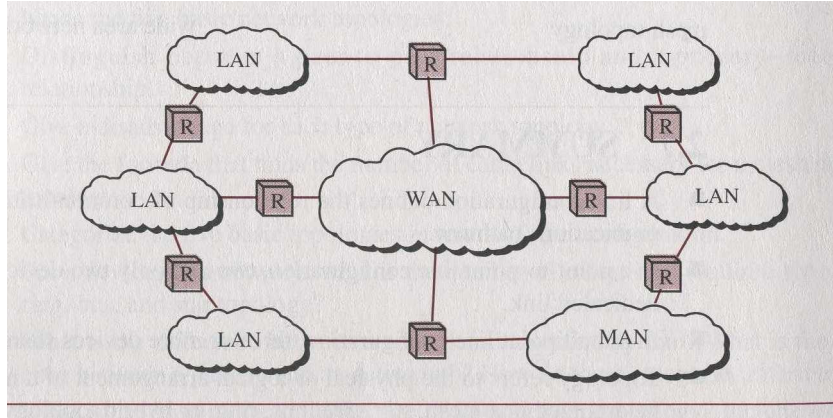


Рис. 2.19 Internetwork (internet)

Тема 3. Еталонна модель взаємодії відкритих систем OSI

3.1. Модель

3.1.1. Рівнева архітектура

3.1.2. Рівноправні процеси

3.1.3. Організація рівнів

3.2. Функції рівнів

3.2.1. Фізичний рівень

3.2.2. Канальний рівень

3.2.3. Мережний рівень

3.2.4. Транспортний рівень

3.2.5. Сеансовий рівень

3.2.6. Рівень подання

3.2.7. Прикладний рівень

3.3. Набір протоколів TCP/IP

Л []

Встановлена в 1947, Організація Міжнародних Стандартів (ISO) є багатонаціональним органом, присвяченим всесвітньовідомій угоді з міжнародних стандартів. Стандартом ISO, який охоплює всі аспекти мережевих комунікацій, є модель Взаємодії Відкритих Систем (OSI). Відкрита система є моделлю, яка дозволяє зв'язуватись будь-яким двом різним системам незважаючи на їхню основну архітектуру. Протоколи роблять тіснішою взаємодію між різнорідними системами. Метою моделі OSI є налагодження комунікації між різними системами без вимоги зміни логіки базового обладнання і програмного забезпечення. Модель OSI не є протоколом; це є модель для розуміння і проектування архітектури комп'ютерної мережі, яка є гнучкою, стійкою і сумісною.

3.1. Модель

Модель взаємодії відкритих систем є рівневим каркасом для проектування мережевих робочих систем, який дозволяє комунікацію через всі типи обчислювальних систем. Вона складається із семи окремих, але зв'язаних між собою рівнів, кожний з яких визначає сегмент процесу передачі інформації через мережу (рис. 3.1). Розуміння основ моделі OSI надає тверду основу для дослідження передачі даних.

3.1.1. Рівнева архітектура

Модель OSI складається із семи перелічених рівнів: фізичний рівень (Physical Level), канальний рівень (Data Link Layer), мережний рівень (Network Layer), транспортний рівень (Transport Layer), сеансовий рівень (Session Layer), рівень подання (Presentation Layer), і прикладний рівень (Application Layer). На рис. 3.2 показано рівні, включені тоді, коли повідомлення послане від пристрою до пристрою В. Коли повідомлення передається до В, воно може пройти багато проміжних вузлів. Ці проміжні вузли звичайно включають тільки перші три рівні моделі OSI. У розробці моделі, проектувальники скоротили процес передачі даних на нижніх рівнях до основних елементів. Вони ідентифікують, які мережних функції використовуються і об'єднують ті функції в дискретні групи, що стали рівнями. Кожний рівень визначає сімейство функцій, чітко розподілених між рівнями. За допомогою визначення і локалізації функціональних можливостей таким чином, проектувальники створили архітектуру, яка є як охоплюючою, так і гнучкою. Найбільш важливо, що модель OSI дає повну прозорість між різними несумісними системами.

Figure 3.1 The OSI model

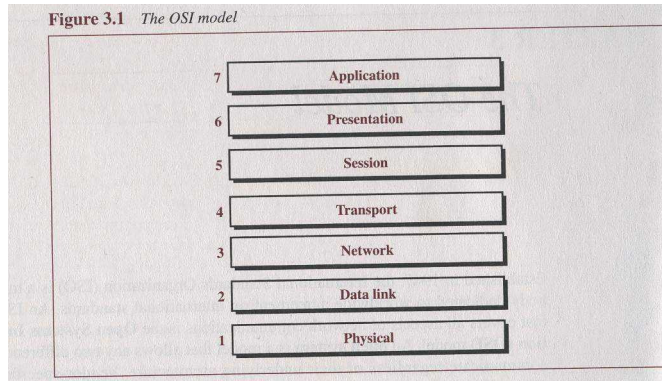
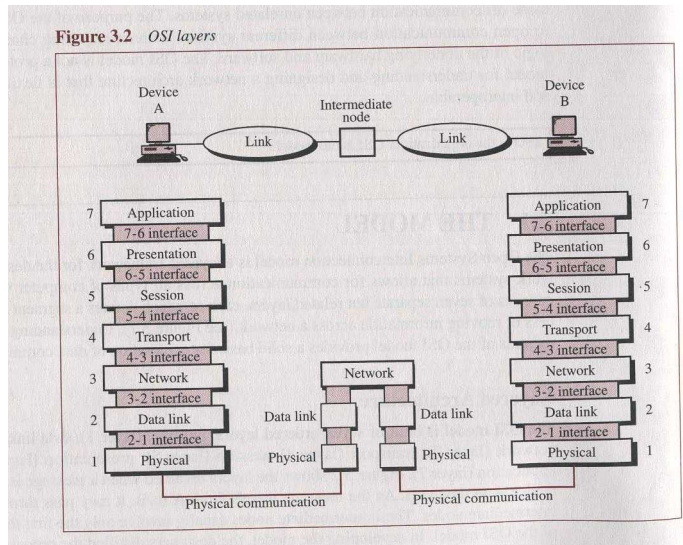


Figure 3.2 OSI layers



3.1.2. Рівноправні процеси

Всередині поодинокі машини кожен рівень викликає служби тільки нижчого рівня. Рівень 3, наприклад, використовує служби рівня 2 і обслуговує рівень 4. Між машинами, рівень x на одній машині спілкується з рівнем x на іншій машині. Цей зв'язок управляється за допомогою погодженої серії правил і протоколів договорів. Процеси на кожній машині, які спілкуються на даному рівні, називаються рівноправними процесами (peer-to-peer). Зв'язок між машинами є таким чином рівноправним процесом з використанням протоколів, відповідних даному рівню.

На фізичному рівні, зв'язок є прямим: машина А посилає потік бітів до машини В. На вищих рівнях, однак, передача даних повинна йти вниз через рівні машини А, потім наверх до машини В, і потім повертатися через рівні.

Кожний рівень в посилаючій машині додає власну інформацію до повідомлення, яке це отримує від верхнього рівня і передає весь пакет до нижнього рівня. Ця інформація додається у виразі заголовків (headers) або кінцевиків (дані елемента управління, додані до початку або кінця пакету даних).

Заголовки додаються до повідомлення на рівнях 6, 5, 4, 3, і 2. Кінцевик додається на рівні 2.

На рівні 1 повний пакет перетворюється у вираз, який може бути переміщений в отримуючу машину. У отримуючій машині, повідомлення розгортається рівень за рівнем, за кожним разом виконується отримання і видалення визначених даних. Наприклад, рівень 2 видаляє дані, які призначаються для нього, потім решта даних передається до рівня 3. Рівень 3 видаляє дані, які призначаються для нього і передає решту до рівня 4, і так далі.

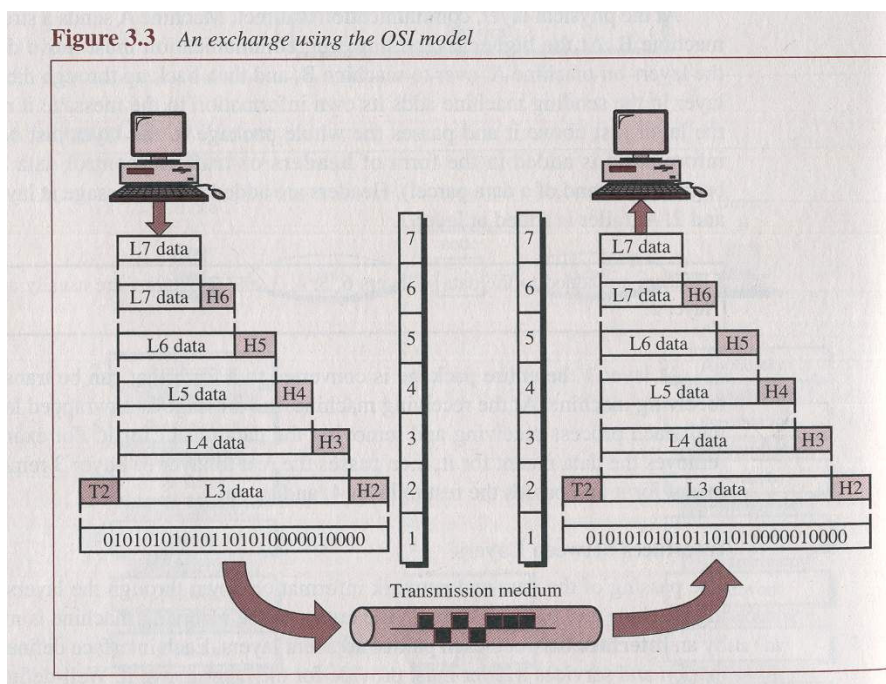
Передача даних і мережевої інформації знизу через рівні посилаючої машини і посилення через рівні отримуючої машини створюється можливою за допомогою інтерфейса між кожною парою суміжних рівнів. Кожний інтерфейс визначає, яку інформацію і послуги рівень повинний надати для вищого рівня. Чіткі інтерфейси і функції рівня забезпечують модульність мережі. Поки рівень забезпечує очікуване обслуговування вищого рівня, специфічна реалізація функцій може бути змінена або замінена без змін вимоги на навколишні рівні.

3.1.3. Організація рівнів

Сім рівнів можуть розглядатися, з точки зору приналежності до трьох підгруп. Рівні 1, 2, і 3 – фізичний, каналний і мережевий – рівні мережевої підтримки; вони мають справу з фізичними аспектами передачі даних від одного пристрою до іншого (як наприклад електричні специфікації, фізичні

зв'язки, фізична адреса, узгодження передачі в часі і надійність). Рівні 5, 6, і 7 – сеансовий, подання і прикладний – можуть розглядатися як рівні підтримки користувача; вони дозволяють сумісність між різнорідними системами програмного забезпечення. Рівень 4, транспортний рівень, гарантує надійну передачу даних, в той час, як рівень 2 гарантує надійну передачу на одиночному зв'язку. Верхні рівні OSI майже завжди здійснюються в програмному забезпеченні; нижчі рівні є комбінацією апаратних засобів і програмного забезпечення, за винятком фізичного рівня, який є здебільшого апаратним засобом.

На рис. 3.3, який показує повне зображення рівнів OSI, даних L7 означає, що елемент даних на рівні 7, даних L6 означає елемент даних на рівні 6, і так далі. Процес починається на рівні 7 (прикладний рівень), потім послідовно переміщується від рівня до рівня в порядку спадання. На кожному рівні (крім рівнів 7 і 1), до елемента даних додається заголовок. На рівні 2, також додається кінцевик. Коли проходи елементу форматуваних даних проходять фізичний рівень (рівень 1), змінюється електромагнітний сигнал і передається каналами фізичного зв'язку.



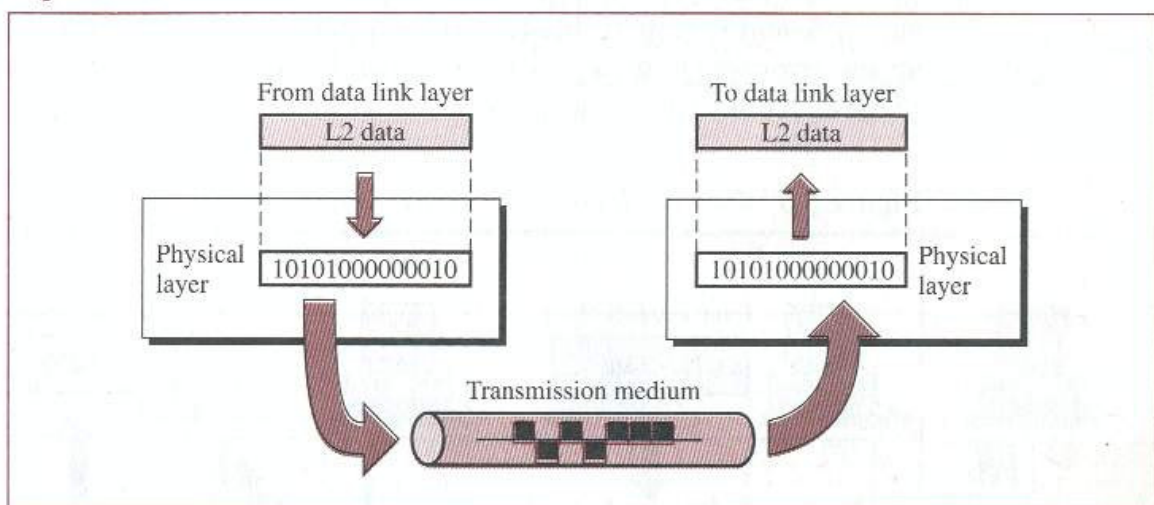
При досягненні адресата, сигнал попадає на рівень 1 і знову перетворюється в біти. Елементи даних потім пересилаються через рівні OSI. Оскільки кожний блок даних досягає до наступного вищого рівня, заголовки і кінцевики, під'єднані до цього у відповідності посилення рівня видаляються, і виконуються дії відповідно рівню. На той час, коли воно досягає рівня 7, повідомлення приймає відповідний вид і стає доступним для отримувача.

3.2. Функції рівнів

3.2.1. Фізичний рівень

Фізичний рівень координує функції, необхідні для передачі бітового потоку через фізичний носій. Він працює з автоматичними і електричними специфікаціями через інтерфейс і носій даних. Він також визначає процедури і функції, що необхідно виконати фізичним пристроям та інтерфейсам для передачі даних. На рис. 3.4 показано становище фізичного рівня щодо передавального носія і каналного рівня.

Figure 3.4 Physical layer



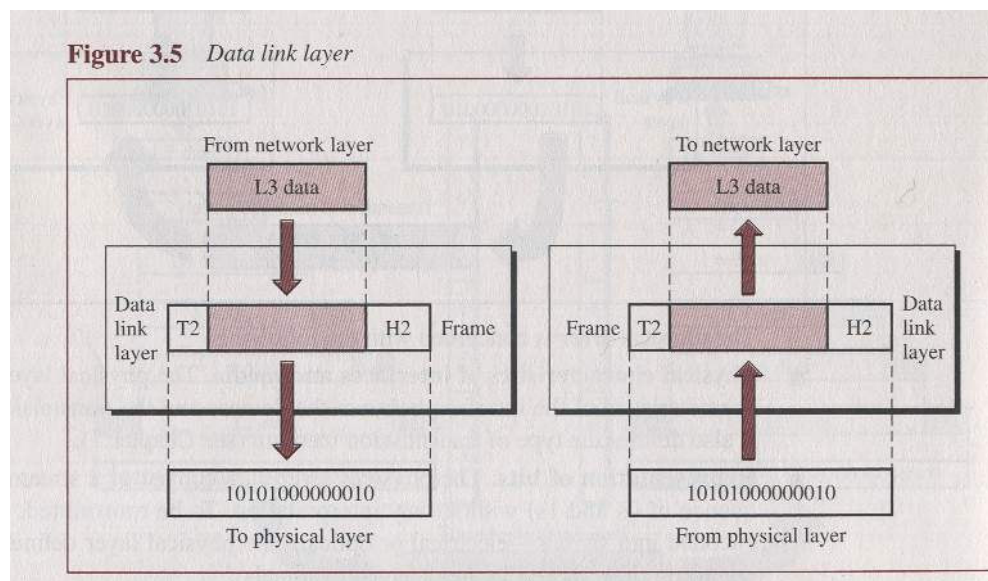
Основні функції і характеристики фізичного рівня:

- Фізичні характеристики інтерфейсів і носія. Фізичний рівень визначає характеристики інтерфейса між пристроями і передачею даних. Він також визначає тип передавального носія.
- Відображення бітів. Фізичні дані рівня складаються з потоку бітів (послідовність нулів і одиниць) без будь-якої інтерпретації. Щоб бути переданими, біти повинні бути перекодовані в сигнали – електричні або оптичні. Фізичний рівень визначає тип кодування (як нулі і одиниці перетворюються на сигнали).
- Швидкість передачі даних. Передачу оцінюють за кількістю бітів посланих за секунду – це також визначається за допомогою фізичного рівня. Іншими словами, фізичний рівень визначає тривалість передачі біта.
- Синхронізація бітів. Відправник і приймач повинні бути синхронізовані на рівні бітів. Іншими словами, годинники відправника і приймача повинні бути синхронізовані.
- Лінійна конфігурація. Фізичний рівень зв'язується із пристроєм зв'язку. У двоточковій конфігурації, два пристрої зв'язуються через виділений зв'язок. У багатоточковій конфігурації, зв'язок є розподіленим між окремими пристроями.
- Фізична топологія. Фізична топологія визначає те, як пристрої з'єднуються для організації мережі. Пристрої можуть бути з'єднані, з використанням сіткової топології (кожний пристрій, приєднаний до кожного пристрою), зіркової топології (пристрої з'єднуються через центральний пристрій), кільцевої топології (кожний пристрій приєднується до наступного, формуючи кільце), або шинною топологією (кожний пристрій на загальному зв'язку).
- Передавальний режим. Фізичний рівень також визначає напрям передачі між двома пристроями: simplex, напівдуплексний, або дуплексний. У simplex режимі, тільки один пристрій може послати;

інший може тільки отримати. Simplex режим є зв'язком oneway. У напівдуплексному режимі, два пристрої можуть послати і отримати, але не в той же час. У дуплексному режимі, два пристрої можуть послати і отримати одночасно.

3.2.2. Канальний рівень

Канальний рівень перетворює фізичний рівень, необроблені передавальні засоби, до надійного зв'язку і відповідає за доставку від вузла до вузла. Це примушує фізичний рівень бути позбавленим помилок для верхнього рівня (мережвий рівень). На рис. 3.5 показано зв'язок каналного рівня до мережі і фізичних рівнів.



Основні функції і характеристики каналного рівня:

- Формування кадру. Канальний рівень відділяє потік бітів, отриманих від мережного рівня в керовані пакети даних, які називаються фреймами.
- Фізична адреса. Якщо фрейми мають бути розподілені між різними системами в мережі, канальний рівень додає заголовок до фрейма, щоб визначити фізичну адресу відправника (адресу джерела даних) і/або

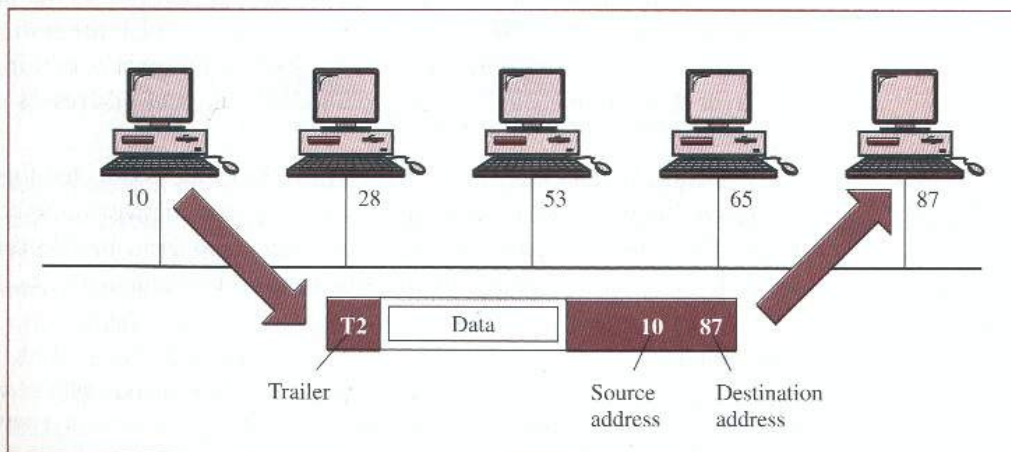
приймача (адреса) фрейма. Якщо фрейм призначений для системи назовнішні, адресою приймача є адреса пристрою, який з'єднує одну мережу до іншої.

- Керування потоком даних. Якщо коефіцієнт отримування даних приймача є меншим, ніж коефіцієнт, вироблений у відправникові, каналний рівень накладає механізм керування потоком даних, щоб запобігти заповненню приймача.
- Обробка помилок. Канальний рівень додає надійність до фізичного рівня за допомогою додавання пристроїв, щоб виявити і повторно передати пошкоджені або втрачені фрейми. Він також використовує пристрій, щоб запобігти дублюванню фреймів. Обробка помилок нормально досягається через кінцевик, доданий до кінця фрейма.
- Контроль доступу. Коли два або більше пристрої приєднані до того ж зв'язку, протоколи каналного рівня є необхідними, щоб визначити, який пристрій має контроль за зв'язком в будь-який даний момент.

Приклад.

На рис. 3.6 вузол з адресою 10 посилає кадр на вузол з фізичною адресою 87, причому два вузли відповідно зв'язані. На каналному рівні цей кадр містить фізичну адресу в заголовку. Це єдина адреса яку потрібно. Решта заголовку містить іншу інформацію потрібно на цьому рівні. Кінцевик звичайно містить додаткові біти необхідні для виявлення помилки.

Figure 3.6 Data link layer (Example 3.1)

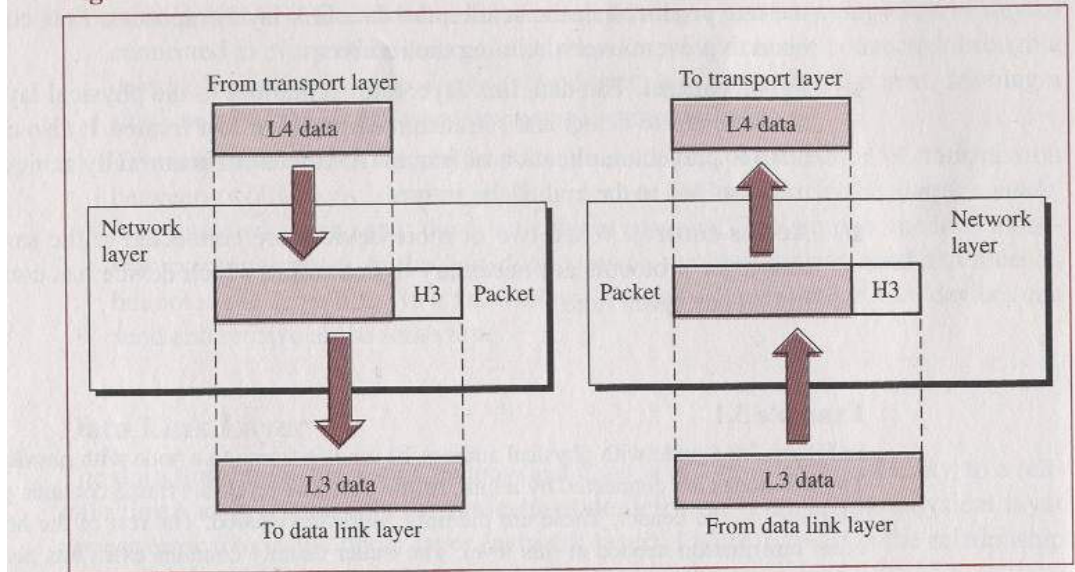


3.2.3. Мережний рівень

Мережевий рівень є відповідальним за джерело до доставки пакету до адресата через мережеві зв'язки. Тоді як канальний рівень обробляє пакети між двома системами у тій же мережі (зв'язки), мережевий рівень гарантує, що кожний пакет доставляється від початкової точки до кінцевого адресата.

Якщо дві системи приєднані до тієї ж лінії зв'язку, вони звичайно не вимагають мережевого рівня. Однак, якщо дві системи під'єднані до різних мереж із з'єднувальними пристроями між мережами, часто мережевий рівень має потребу передати джерело до адресата. На рис. 3.7 показано зв'язок мережевого рівня з каналу зв'язку і транспортних рівнів.

Figure 3.7 Network layer



Основні функції і характеристики мережевого рівня:

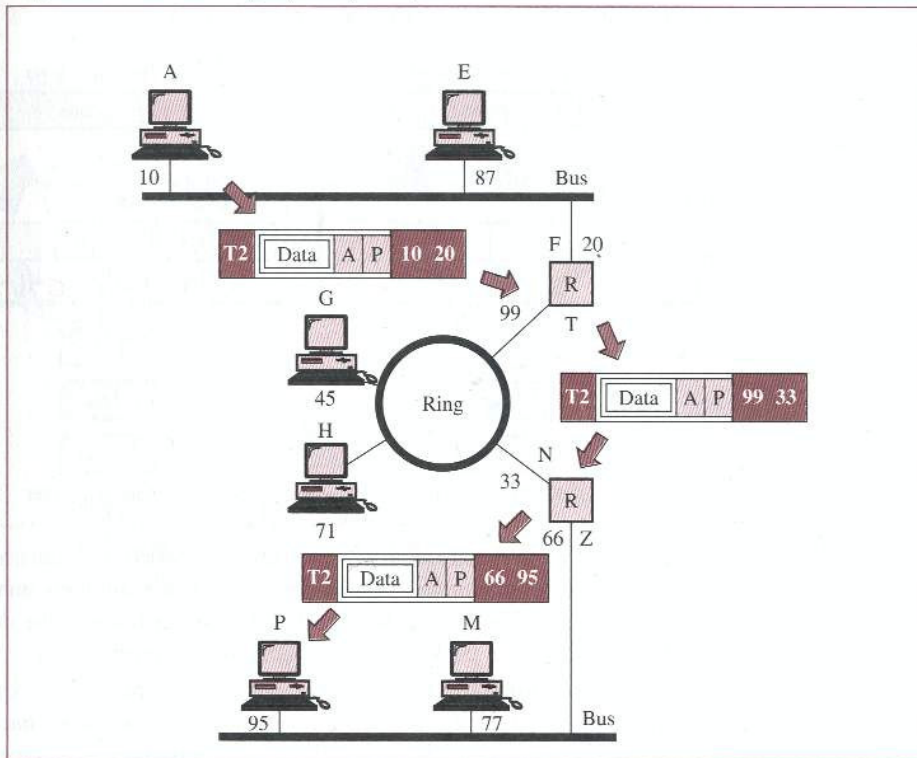
- Логічне адресування. Фізичне адресування, здійснене за допомогою канального рівня, поводить ся з проблемою адресування у певному місці. Якщо пакет передається за межі мережі, ми потребуємо іншої системи адресування, щоб допомогти відрізнити джерело і системи адресата. Мережевий рівень додає заголовок до пакету, який приходить від верхнього рівня, що, між іншим, включає логічні адреси відправника і приймача.
- Маршрутизація. Коли незалежні мережі або зв'язки з'єднані разом, щоб створити internetwork (мережу мереж) або велику мережу, з'єднувальні пристрої (маршрутизатори або шлюзи) посилають пакети до їхнього кінцевого адресата. Одна з функцій мережевого рівня - забезпечити цей пристрій.

Приклад.

Уявимо, що у вузлі 3.8 ми хочемо послати дані з вузла з мережевою адресою А і фізичною адресою 10, розміщеному в одній локальній

обчислювальній мережі, іншому вузлу з мережевою адресою 95, розміщеному в іншій локальній обчислювальній мережі. між цими пристроями розміщені різні мережі, ми не можемо використовувати тільки фізичні адреси; фізичні адреси мають локальну дію. Ми потребуємо тут універсальну адресу, яку можна передавати через різні мережі.

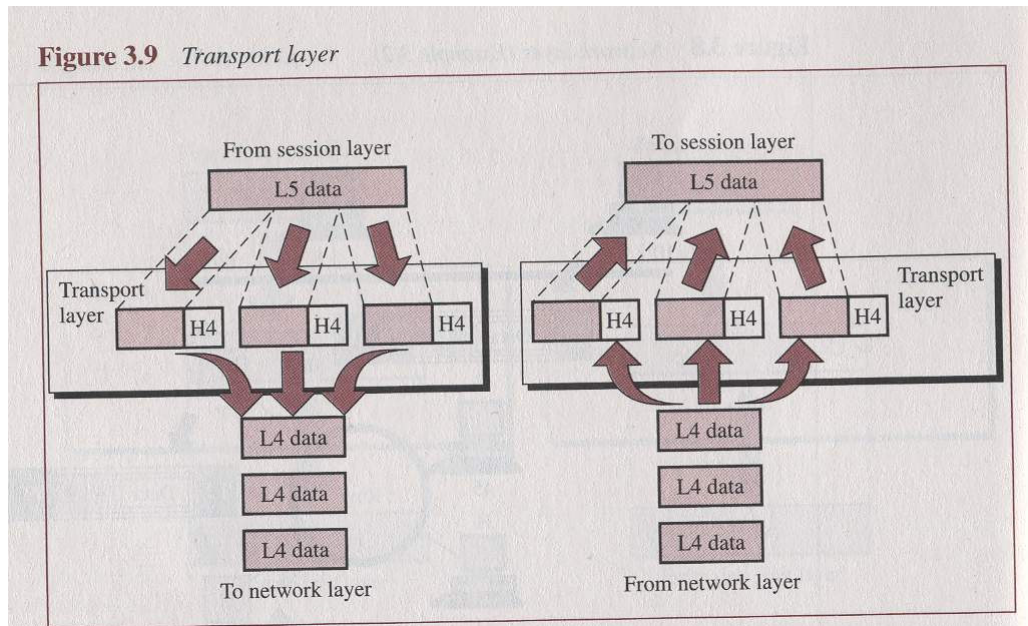
Figure 3.8 Network layer (Example 3.2)



3.2.4. Транспортний рівень

Транспортний рівень є відповідальним за доставку до адресата (end-to-end) повного повідомлення. Тоді як мережевий рівень розглядає end-to-end, як доставку індивідуальних пакетів, він не визнає ніякого зв'язку між тими пакетами. Це поводить незалежно, немовби кожний пакет належить окремому повідомленню. Транспортний рівень, з другого боку, гарантує, що все повідомлення прибуває непошкодженим і в порядку, передбаченому як модулем обробки помилок, так і керуванням потоком даних в джерелі. На

рис. 3.9 показано зв'язок транспортного рівня з мережевим рівнем і сеансовим рівнем.



Для додаткового захисту, транспортний рівень може створити зв'язок між кінцевими портами. Зв'язок є поодиноким логічним маршрутом між джерелом і адресатом і асоціюється зі всіма пакетами в повідомленні. Створення зв'язку включає три зв'язаних кроки, встановлення зв'язку, передачу даних, і проведення зв'язку. За допомогою обмеження передача всіх пакетів до окремої приватної шини, транспортний рівень має більший елемент управління і впорядкування потроком, виявлення помилок і їх виправлення.

Основні функції і характеристики транспортного рівня:

- Адресація службових точок. Комп'ютери часто виконують програми одночасно. З цієї причини, джерело доставки від адресата означає доставку не тільки з одного комп'ютер до іншого, але також від специфічного процесу (виконання програми) на комп'ютері до специфічного процесу (виконання програми) на іншому. Заголовок транспортного рівня таким чином повинен включати тип адреси який викликав адресацію службової точки (адреса порту). Мережевий рівень

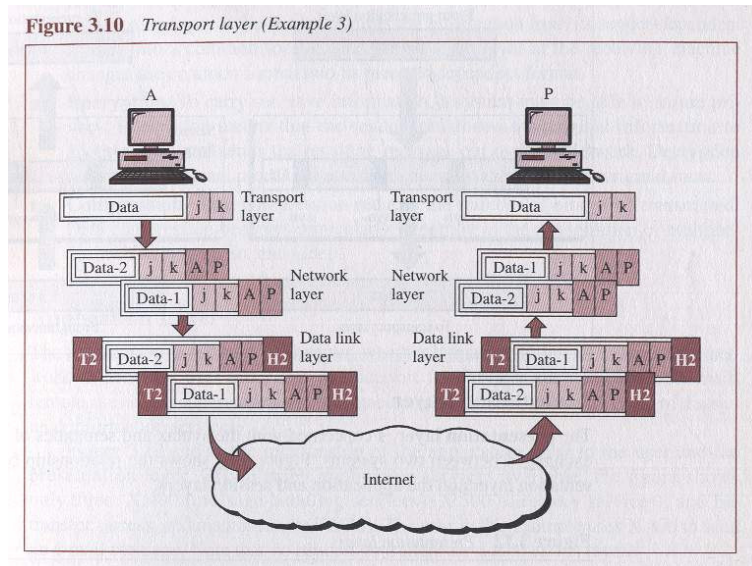
отримує кожний пакет до певного комп'ютера; транспортний рівень отримує повне повідомлення до певного процесу на тому комп'ютері.

- Сегментація і повторні збори. Повідомлення розділяється на визначені сегменти. Кожний сегмент містить порядковий номер. Ці номери надають транспортному рівню можливість повторно правильно зібрати повідомлення в адресата і, щоб ідентифікувати і замінити пакети, які були втрачені в передачі.
- Елемент управління зв'язку. Транспортний рівень може бути або без встановлення зв'язку або орієнтованим на зв'язок. Транспортний рівень без встановлення зв'язку поводиться з кожним сегментом, як незалежний пакет і доставляє його до транспортного рівня адресата. Після того, як всі дані перенесені, зв'язок завершується.
- Керування потоком даних. Подібно каналного рівня, транспортний рівень є відповідальним за керування потоком даних. Однак, керування потоком даних в цьому рівні виконується end-to end, частіше ніж через поодинокий зв'язок.
- Обробка помилок. Подібно каналному рівню, транспортний рівень є відповідальним за обробку помилок. Однак, обробка помилок в цьому рівні виконується end-to end, частіше ніж через поодинокий зв'язок. Посилаючий транспортний рівень переконується, що повне повідомлення досягає отримуючого транспортного рівня без помилки (пошкодження, пошкодження, або дублювання). Виправлення помилок звичайно досягається через повторну передачу.

Приклад.

На рис. 3.10 показано приклад транспортного рівня. Дані, що приходять з верхнього рівня мають адресу порту j і k (j є адресою відправника і k є адресою приймача). Оскільки розмір даних більший, ніж може утримувати мережевий рівень, дані розділяються на два пакети, кожен

пакет доставляється до адреси точки обслуговування (j і k). Потім на мережевому рівні мережеві адреси (A і P) додаються до кожного пакета. Пакети можуть пересилатися різними шляхами і прибувати в довільному порядку. Два пакети доставляються на мережевий рівень, який відповідає за усунення мережевої адреси із заголовка.



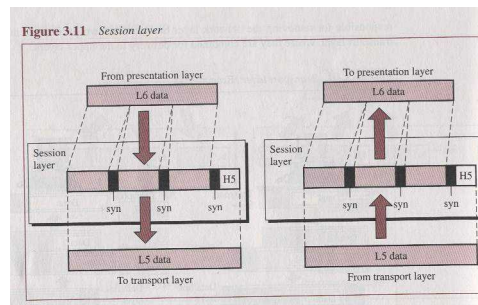
3.2.5. Сеансовий рівень

Служби, забезпечені за допомогою перших трьох рівнів (фізичний, каналний і мережевий), не є достатніми для деяких процесів. Сеансовий рівень є мережевим діалоговим контролером. Він встановлює, підтримує, і синхронізує взаємодію між суміжними системами.

Основні функції і характеристики сеансового рівня:

- Діалоговий елемент управління. Сеансовий рівень дозволяє двом системам вступити в діалог. Він дозволяє комунікацію між двома процесами, щоб мати позицію або в напівдуплексному (в одну сторону) або дуплексному (в дві сторони). Наприклад, діалог між терміналом, приєднаним до центрального процесора може бути напівдуплексним.
- Синхронізація. Сеансовий рівень дозволяє процесу додати контрольні точки (точки синхронізації) в потік даних. Наприклад, якщо система

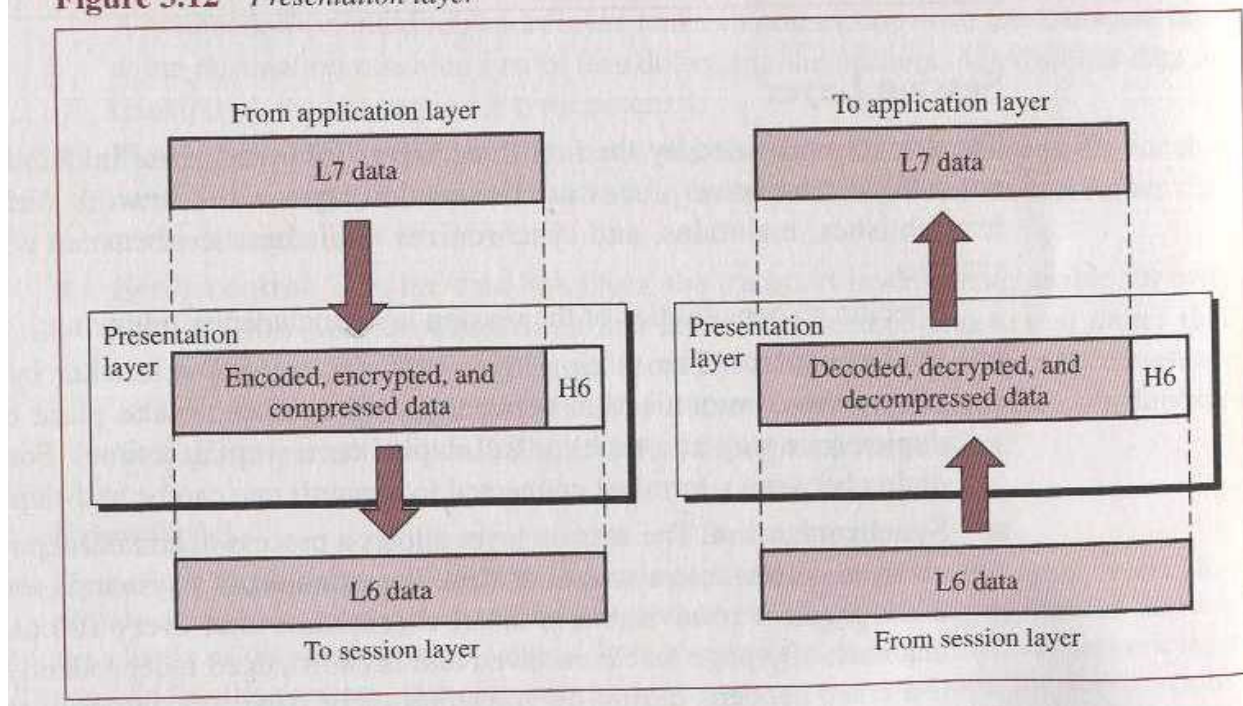
посилає файл на 2000 сторінок, доцільно вставити контрольні точки після кожних 100 сторінок, щоб гарантувати, що кожний елемент зі 100-сторінок отримується і розпізнається незалежно. У цьому випадку, якщо збій стається протягом передачі сторінки 523, повторна передача починається зі сторінки 501: сторінки від 1 до 500 не потрібно повторно передавати. Рис. 3.11 ілюструє зв'язок сеансового рівня до переміщення і рівнів подання.



3.2.6. Представницький рівень

Рівень подання стосується синтаксису і семантики обміну інформації між двома системами. Рис. 3.12 показує зв'язок між рівнем подання і прикладним рівнем і сеансовим рівнем.

Figure 3.12 Presentation layer



Основні функції і характеристики представницького рівня:

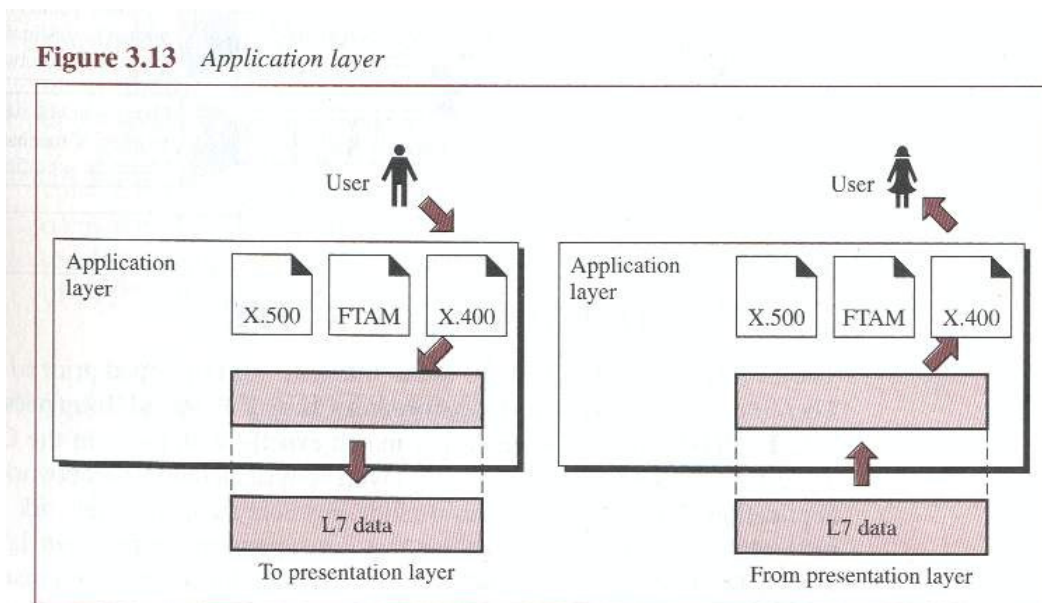
- Трансляція. Процеси (виконання програм) в двох системах звичайно обмінюють інформацію у вигляді рядків символів, номерів, і так далі. Інформація повинна бути змінена на бітові потоки до передачі. Тому, що різні комп'ютери використовують різні системи кодування, рівень подання є відповідальним за сумісність між різними методами кодування. Рівень подання у відправнику змінює інформацію залежно від формату відправника в загальний формат. Рівень подання в отримуючій машині змінює загальний формат в формат приймача.
- Кодування. Щоб перенести чутливу інформацію, система може заповнити таємність. Кодування означає, що відправник перетворює первинну інформацію до іншого виразу і посилає повідомлення за межі мережі. Розшифровування змінює первинний процес, щоб перетворити повідомлення до первинного виразу.

- Компресія. Ущільнення Даних зменшує кількість бітів, яка передається. Ущільнення даних стає особливо важливим в передачі мультимедіа, як наприклад текст, звук, і відео.

3.2.7. Прикладний рівень

Прикладний Рівень дозволяє користувачу – людині або програмному забезпеченню мати доступ до мережі. Це забезпечує інтерфейси користувача і підтримку для служб, як наприклад електронна пошта, дистанційний доступ до файлів і передачу, загальнодоступне керування базою даних, і інші типи розподілених інформаційних служб.

На рис. 2.13 показано зв'язок прикладного рівня до користувача і рівня подання. Багато доступних прикладних служб додатку, на рисунку показано тільки три: X.400 (служба електронних повідомлень); X.500 (служби каталога); передача файлів, доступ, і управління (FTAM). Користувач в цьому прикладі використовує X.400, щоб послати повідомлення електронною поштою. Слід звернути увагу, що заголовки або кінцевики не додаються на цьому рівні.

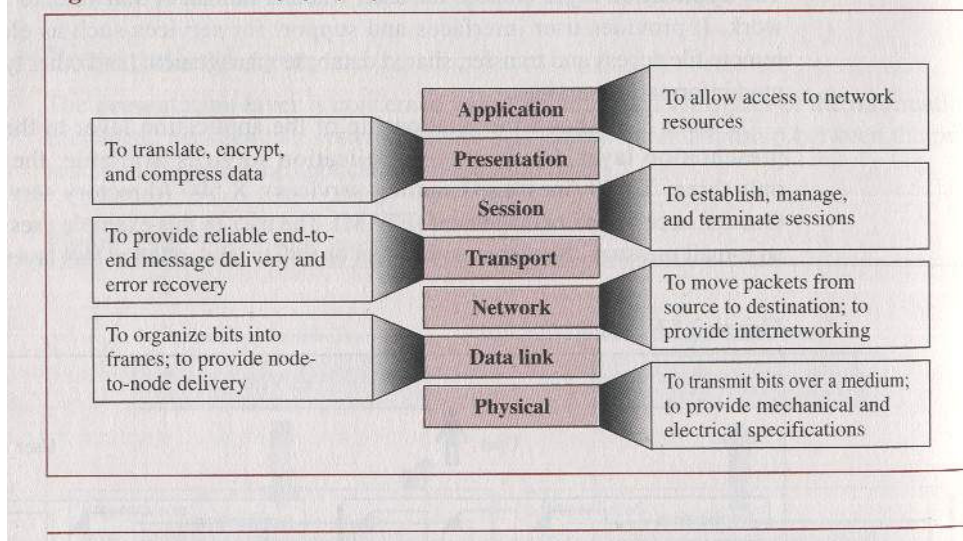


Прикладний рівень забезпечує наступні служби і сервіси:

- Мережевий віртуальний термінал – є версією термінального фізичного програмного забезпечення і дозволяє користувачу вийти до віддаленого головного комп'ютера. Щоб зробити так, додаток створює емуляцію терміналу програмного забезпечення у віддаленому головному комп'ютері. Комп'ютер користувача комунікує з термінальним програмним забезпеченням, яке, по черзі, зв'язується з головним комп'ютером, і навпаки. Віддалений головний комп'ютер вважає, що він спілкується з одним з власних терміналів і дозволяє вхід.
- Передача файлів, доступ, і управління (FTAM). Цей додаток дозволяє користувачу мати доступ до файлів на віддаленому комп'ютері (щоб зробити зміни або прочитати дані), щоб забрати файли з віддаленого комп'ютера; і, щоб управляти або контролювати файли на віддаленому комп'ютері.
- Поштові служби. Цей додаток надає основу для передання електронної пошти і пам'яті.
- Служби Каталога. Цей додаток надає доступ до джерел розподіленої бази даних для всесвітньої інформації про різні об'єкти і служби.

На рис. 3.14 показано підсумок всіх семи рівнів.

Figure 3.14 Summary of layer functions



3.3. Набір протоколів TCP/IP

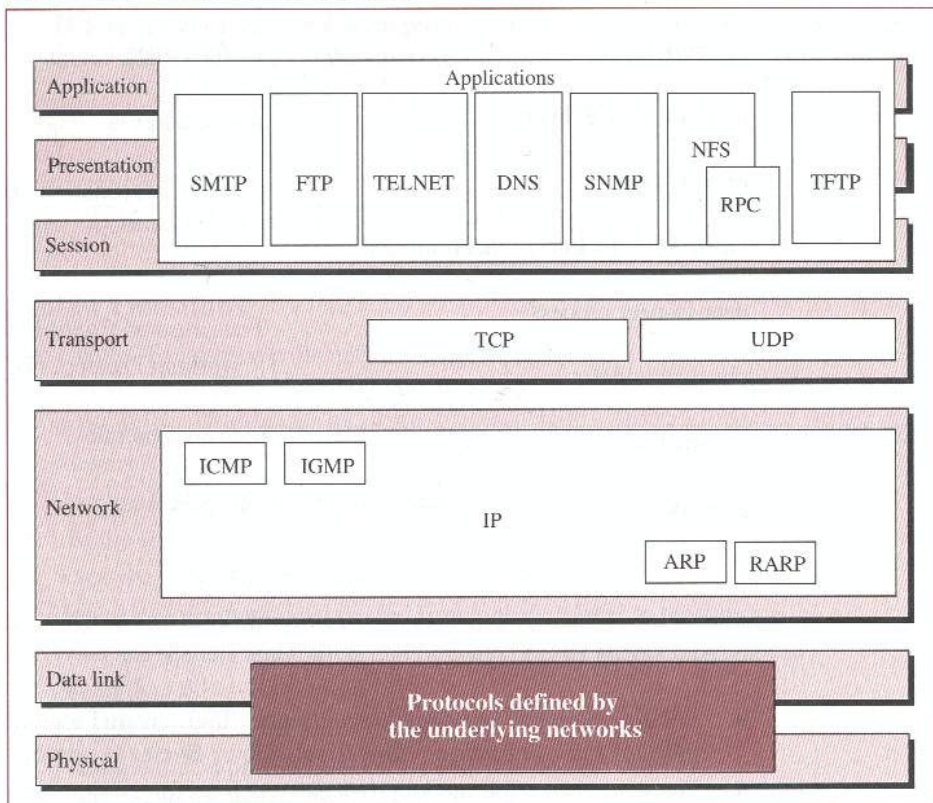
Набір протоколів TCP/IP, що використовується в Internet, розроблявся до моделі OSI. Таким чином, рівні в наборі протоколу Протоколу (TCP/IP) Протоколу контролю передачі/Міжмережевої взаємодії не підходять цілком точно до моделі OSI. Набір протоколу TCP/IP складається з п'яти рівнів: фізичний, каналний, мережевий, транспортний і прикладний. Перші чотири рівні забезпечують фізичні стандарти, мережевий інтерфейс, міжмережеву взаємодію, і транспортні функції, які відповідають першим чотирьом рівням моделі OSI. Три найвищі рівні в моделі OSI, однак, представляються в TCP/IP за допомогою одного прикладного рівня (рис. 3.15).

TCP/IP є ієрархічним протоколом, складеним з інтерактивних модулів, кожний з яких забезпечує специфічні функціональні можливості, але вони є не обов'язково взаємозалежними. В той час модель OSI конкретизує, які функції належать кожному з рівнів. Набір протоколу TCP/IP містять відносно незалежні протоколи, які можуть бути змішані залежно від потреб системи. Термін ієрархічні засоби означає, що протокол верхнього рівня

підтримується за допомогою одного з протоколів більшого або нижчого рівня.

На транспортному рівні, TCP/IP визначає два протоколи: управління передачею (TCP) і Протокол Датаграми Користувача (UDP). На мережевому рівні, головний протокол визначається за допомогою TCP/IP Міжмережева взаємодія Протоколу (IP), хоч є деякі інші протоколи, що підтримують рух даних на цьому рівні.

Figure 3.15 TCP/IP and the OSI model



Тема 4. Сигнали

- 4.1. Аналогові/цифрові
- 4.2. Періодичні/неперіодичні перетворення Фур'є
- 4.3. Аналогові сигнали та часово-частотні області
- 4.4. Складні сигнали та їх характеристики
- 4.5. Цифрові сигнали

Література []

Головним завданням фізичного рівня є переміщення інформації у формі електромагнітних сигналів через засіб зв'язку. При прийомі цифрової статистики від іншого комп'ютера, передачі зображень з робочої станції розробника, або зв'язується із віддаленим центром управління, усе це пов'язано з передачею інформації через мережеві зв'язки. Інформація може бути голосом, зображенням, числовими даними, символами, або закодованим повідомленням, яке може бути прочитаним користувачем і має цінність для отримувача: людини або машини.

Інформація може бути у формі даних, голос, картина, і так далі.

Загалом, інформація, придатна до споживання людиною або додатком, не знаходиться у формі, придатній для передачі по мережі. Наприклад, неможливо передати фотографію через мережу через все місто. Можна передати, проте, закодований образ фотографії. За винятком посилання справжньої фотографії, можна використати шифратор, щоб створити потік нулів та одиниць, яке говорить отримувачу як реконструювати зображення фотографії.

Але навіть нулі та одиниці не може бути посланий як є через лінії зв'язку. Вони повинні бути перетвореними у форму, яку можуть сприйняти засоби передачі. Засоби передачі працюють за допомогою передачі енергії

уздовж фізичного шляху. Отже потік даних нулів і одиниць повинен бути перетворений на енергію у формі електромагнітних сигналів.

Щоб бути переданий, інформація повинна бути перетвореними у електромагнітні сигнали.

4.1. Аналогові та цифрові сигнали

Як дані так і сигнали, що представляють їх, можуть бути у аналоговій або цифровій формі. Аналогові є набором специфічних точок даних і всіх можливих точок між ними. Цифрові є дискретними – набір специфічних точок, без інших точок між ними.

Аналогові і цифрові дані

Дані можуть бути аналоговими або цифровими. Приклад аналогових даних – людський голос. Коли хтось розмовляє, в повітрі створюється безперервна хвиля. Це може бути сприйнята мікрофоном і перетворена на аналоговий сигнал.

Приклад цифрових даних – дані, що запам'ятовуються в пам'яті комп'ютера у формі нулів і одиниць. Вони звичайно перетворюється на цифровий сигнал, коли їх потрібно перемістити з однієї точки до іншої всередині або за межами комп'ютера.

Аналогові та цифрові сигнали

Подібно інформації, яку вони представляють, сигнали можуть бути або аналогові або цифрові. Аналоговий сигнал – безперервна форма хвилі, яка плавно змінюється в часі. Оскільки хвиля переміщається від значення А до значення В, вона включає нескінченне число значень уздовж всього шляху. Цифровий сигнал даних, з іншої сторони, є дискретним. Це може мати тільки обмежене число певних значень, нулів і одиниць. Переміщення цифрового

сигналу від значення до значення є миттєвим, подібно включеному та вимкнутому світлу.

Ми звичайно ілюструємо сигнали відкладаючи їх перпендикулярних осях. Вертикальна вісь представляє значення або силу сигналу. Горизонтальна вісь представляє тривалість у часі. Малюнок 4.1 ілюструє аналог і цифровий сигнал даних. Крива, що представляє аналоговий сигнал є гладкою і безперервним, проходячи через нескінченне число точок. Вертикальні лінії цифрового сигналу даних, проте, демонструють раптовий стрибок, що його сигнал робить від значення до значення; плоскі вершини і нижні рівні вказують, що ті значення фіксовані. Іншим способом, щоб виразити відмінність є, те що аналоговий канал змінюється безперервно залежно від часу, в той час, як цифровий сигнал змінюється миттєво.

Сигнали можуть бути аналоговими або цифровими. Аналогові сигнали можуть мати будь-яке значення з ряду; цифрові сигнали даних можуть мати тільки обмежене число значень.

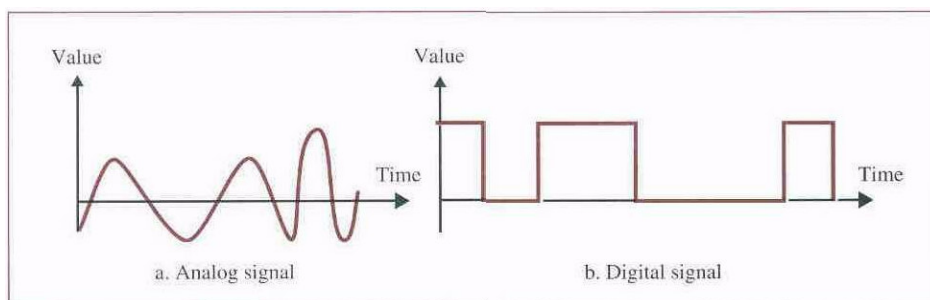


Рис. 4.1. Порівняння аналогових та цифрових сигналів

4.2. Періодичні та неперіодичні перетворення Фур'є

Як аналогові, так і цифрові сигнали може мати дві форми: періодичний та аперіодичні (неперіодичні).

Періодичні Сигнали

Сигнал є періодичним сигналом, якщо він співпадає із зразком в межах вимірюного інтервалу часу, який називається періодом, і повторює зразок з певними ідентичними подальшими періодами. Завершення одного повного зразка називається циклом. Період визначається як кількість часу (вираженому в секундах) необхідного, що завершити один повний цикл. Тривалість періоду, представленого T , може бути різним для кожного сигналу, але вона є постійною для будь-якого даного періодичного сигналу. На рис. 4.2 показано гіпотетичні періодичні сигнали.

Періодичний сигнал складається з безперервно повторюваного зразка. Період цього сигналу (T) виражається в секундах.

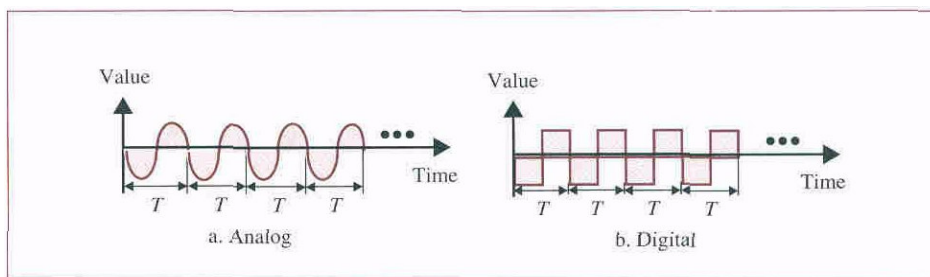


Рис. 4.2. Приклади періодичних сигналів

Неперіодичні сигнали

Неперіодичні сигнали змінюються постійно без співпадання із зразком або циклом, який повторюється з часом. Приклади неперіодичних сигналів показано на рис. 4.3.

Неперіодичні сигнали не мають зразка, по якому вони повторюються.

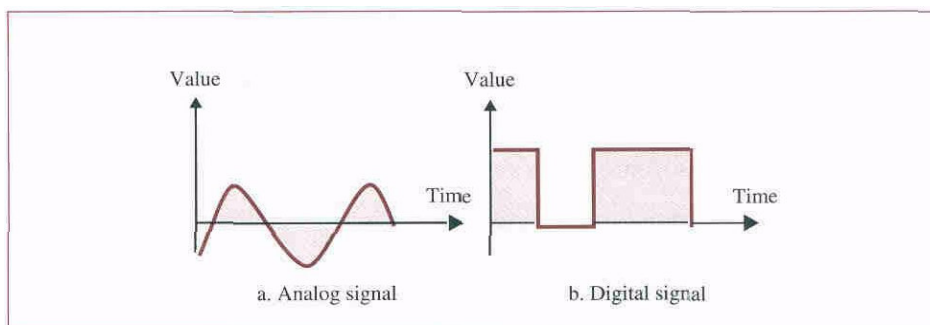


Рис. 4.3. Приклади неперіодичних сигналів

За допомогою методу перетворення Фур'є, що будь-який неперіодичний сигнал може бути перетворений у нескінченну кількість періодичних сигналів. Розуміння особливостей періодичних сигналів, таким чином, надає розуміння неперіодичних сигналів.

Неперіодичний сигнал може бути перетворений на нескінченну кількість періодичних сигналів.

Теоретичні основи передачі даних

Інформація може передаватися по мережі за рахунок зміни якої-небудь фізичної величини, наприклад напруги або сили струму. Уявивши значення напруги або сили струму у вигляді однозначної функції часу t (J), ми зможемо змодельовати поведінку сигналу і піддати його математичному аналізу. Цьому аналізу і присвячені наступні розділи.

Ряди Фур'є

На початку XIX сторіччя французький математик Жан-Батист Фур'є довів, що будь-яка періодична функція $g(t)$ з періодом T може бути розкладена в ряд (можливо, нескінченний), що складається з сум синусів і косинусів:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft); \quad (2.1),$$

де $f = 1/T$ – основна частота (гармоніка), a_n і b_n – амплітуди синусів і косинусів n -ї гармоніки, а c – константа. Подібне розкладання називається рядом Фур'є. Розкладена в ряд Фур'є функція може бути відновлена по елементах цього ряду, тобто якщо період T і амплітуди гармонік відомі, то початкова функція може бути відновлена за допомогою суми ряду (2.1).

Інформаційний сигнал, що має кінцеву тривалість (всі інформаційні сигнали мають кінцеву тривалість), може бути розкладений в ряд Фур'є, якщо уявити, що весь сигнал нескінченно повторюється знову і знову (тобто інтервал від T до $2T$ повністю повторює інтервал від 0 до T , і т. д.).

Амплітуди a_n можуть бути обчислені для будь-якої заданої функції $g(t)$. Для цього потрібно помножити ліву і праву сторони рівняння (2.1) на $\sin(2\pi kft)$, а потім проінтегрувати від 0 до T . Оскільки:

$$\int_0^T \sin(2\pi kft) \sin(2\pi nft) dt = \begin{cases} 0 & \text{при } k \neq n, \\ T/2 & \text{при } k = n, \end{cases}$$

залишається тільки один член ряду: a_n . Ряд b_a зникає повністю. Аналогічно, множачи рівняння (2.1) на $\cos(2\pi kft)$ і інтегруючи за часом від 0 до T , ми можемо обчислити значення b_a . Якщо проінтегрувати обидві частини рівняння, не змінюючи його, то можна отримати значення константи c . Результати цих дій будуть наступними:

$$a_n = \frac{2}{T} \int_0^T g(t) \sin(2\pi nft) dt, \quad b_n = \frac{2}{T} \int_0^T g(t) \cos(2\pi nft) dt, \quad c = \frac{2}{T} \int_0^T g(t) dt.$$

4.3. Аналогові сигнали та часово-частотні області

Аналогові сигнали можуть бути класифіковані як прості або складові. Простий аналоговий канал, або хвиля синуса, не може бути перетворений на простіші сигнали. Складовий аналоговий канал складається з багатьох синусових хвиль.

Прості аналогові сигнали

Хвиля синуса – фундаментальна форма періодичного аналогового каналу. Зображається як проста крива вібрації, зміна над курсом циклу є гладкою і послідовною, безперервною в часі течії. На рис. 4.4 показано

хвилю синуса. Кожний цикл складається з єдиної дуги над віссю часу, завершеною єдиною дугою нижче. Хвилі синуса можуть повністю описуватися трьома характеристиками: амплітуда, період або частота і фаза.

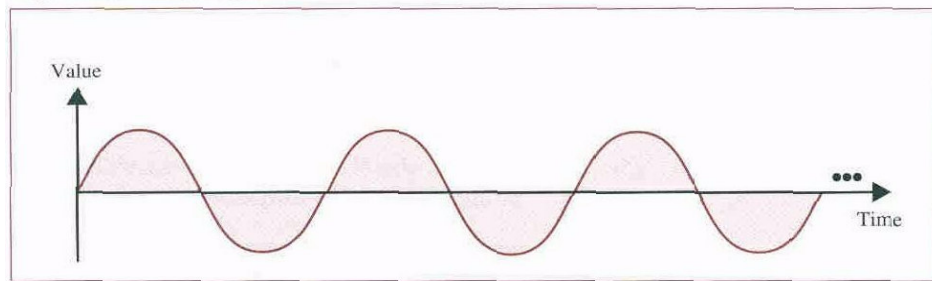


Рис. 4.4. Синусові хвилі

Амплітуда

На графі, амплітуда сигналу – значення сигналу у будь-який момент на хвилі. Вона є рівною вертикальній відстані від даної точки хвилі до горизонтальної осі. Максимальна амплітуда хвилі синуса є рівною верхньому значенню на вертикальній осі (рис. 4.5).

Амплітуда вимірюється у вольтах, амперах, або ватах, залежно від виду сигналу. Вольти відносяться до напруги; ампери відносяться до струму, і вати відносяться до потужності.

Амплітуда відноситься до висоти сигналу. Одиниця амплітуди залежить від типу сигналу. Для електричних сигналів, одиницями є вольти, ампери, або вати.

Період і Частота

Період відноситься до тривалості часу, в секундах, які необхідні сигналу, щоб завершити цикл. Частота відноситься до кількості періодів за секунду. Частота сигналу є кількістю циклів за секунду. На рис. 4.6 показано поняття періоду і частоти.

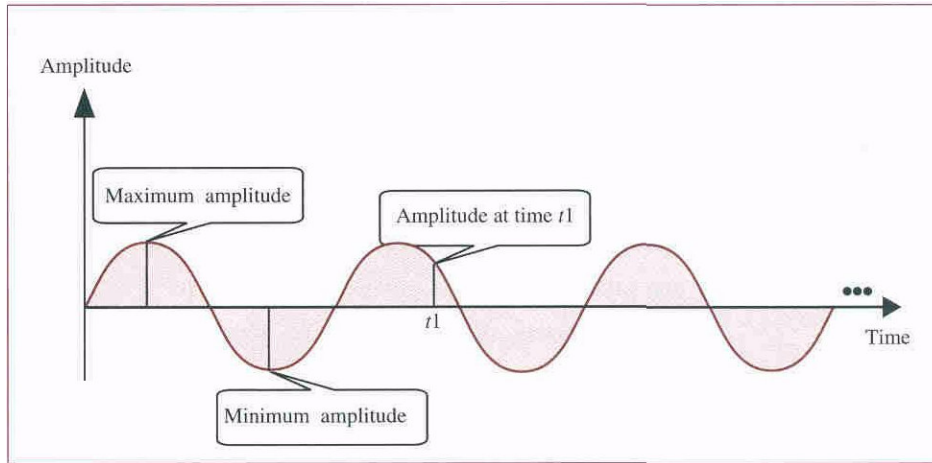


Рис. 4.5. Амплітуда

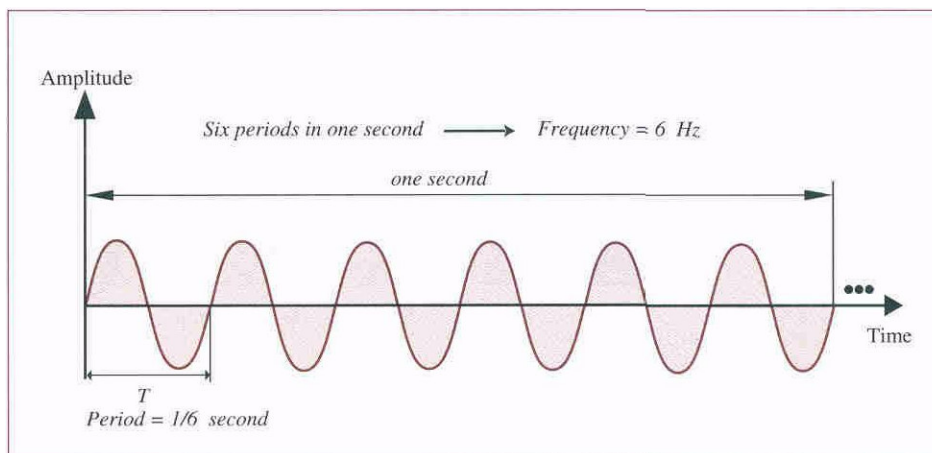


Рис. 4.6. Період і частота

Одиниця Періоду

Період виражається в секундах. У телекомунікації використовується п'ять одиниць вимірювання періоду: секунда (s), мілісекунда ($ms = 10^{-3} s$), мікросекунда ($\mu s = 10^{-6} s$), наносекунда ($ns = 10^{-9} s$), і пікосекунди ($ps = 10^{-12} s$). Див. Табл. 4.1.

Таблиця 4.1. Одиниці періодів

Одиниця	Еквівалент
Секунди	1 s
Мілісекунди (ms)	$10^{-3} s$
Мікросекунди (μs)	$10^{-6} s$
Наносекунди (ns)	$10^{-9} s$
Picoseconds (ps)	$10^{-12} s$

Приклад 4.1

Показати 100 мілісекунд в секундах, мікросекундах, наносекундах, і пікосекундах.

Рішення

Ми маніпулюємо потужностями по 10, щоб знайти відповідну одиницю. Ми замінюємо 10^{-3} секунд мілісекундами, 10^{-6} секунд мікросекундами, 10^{-9} секунд наносекундами, і 10^{-12} секунд пікосекундами.

$$100 \text{ мілісекунд} = 100 \times 10^{-3} \text{ секунд} = 0.1 \text{ секунди}$$

$$100 \text{ мілісекунд} = 100 \times 10^{-3} \text{ секунд} = 100 \times 10^3 \times 10^{-6} \text{ секунд} = 10^5 \mu\text{s}$$

$$100 \text{ мілісекунд} = 100 \times 10^{-3} \text{ секунд} = 100 \times 10^6 \times 10^{-9} \text{ секунд} = 10^8 \text{ ns}$$

$$100 \text{ мілісекунд} = 100 \times 10^{-3} \text{ секунд} = 100 \times 10^9 \times 10^{-12} \text{ секунд} = 10^{11} \text{ ps}$$

Одиниця Частоти

Частота виражається в герцах (Hz), на честь німецького фізика Генріха Рудольфа Герца. У телекомунікації використовується п'ять одиниць вимірювання частоти: герц (Hz, кілогерц (KHz = 10^3 Hz), мегагерц (Mhz = 10^6 Hz), гігагерц (GHz = 10^9 Hz), і терагерц (THz = 10^{12} Hz). Див. табл. 4.2.

Табл. 4.2. Одиниці частоти

Одиниця	Еквівалент
Герц (Hz)	1 Hz
Кілогерц (KHz)	10^3 Hz
Мегагерц (Mhz)	10^6 Hz
Gigahertz (GHz)	10^9 Hz
Terahertz (THz)	10^{12} Hz

Приклад 4.2

Виразити 14 Mhz в Hz, KHz, GHz. і THz.

Рішення

Ми маніпулюємо потужністю 10, щоб знайти відповідну одиницю. Ми замінюємо 10^3 Hz через KHz, 10^6 Hz з Mhz, 10^9 Hz з GHz, і 10^{12} Hz з THz.

$$14 \text{ Mhz} = 14 \times 10^6 \text{ Hz}$$

$$14 \text{ MHz} = 14 \times 10^6 \text{ Hz} = 14 \times 10^3 \times 10^3 \text{ Hz} = 14 \times 10^3 \text{ KHz}$$

$$14 \text{ MHz} = 14 \times 10^6 \text{ Hz} = 14 \times 10^{-3} \times 10^9 \text{ Hz} = 14 \times 10^{-3} \text{ GHz}$$

$$14 \text{ MHz} = 14 \times 10^6 \text{ Hz} = 14 \times 10^{-6} \times 10^{12} \text{ Hz} = 14 \times 10^{-6} \text{ THz}$$

Перетворення частоти в період і навпаки

Математично, взаємовідносини між частотою і періодом є протилежністю один одному; якщо дано одне, інше може бути одержане.

$$\text{Frequency} = 1/\text{Period}$$

$$\text{Period} = 1/\text{Frequency}$$

Період – це кількість часу потрібного сигналу, щоб завершити один цикл; частота – кількість герців. Частота і період – протилежність одного одному: $f = 1/T$ s $T = 1/f$.

Приклад 4.3

Хвиля синуса має частоту 6 Hz, який її період?

Рішення

Нехай T період і f частота. Тоді

$$T = 1/f = 1/6 = 0.17 \text{ секунди}$$

Приклад 4.4

Хвиля синуса має частоту 8 KHz. Який її період?

Рішення

Нехай T період і f частота. Тоді

$$T = 1/f = 1/8000 = 0.000125 \text{ секунди} = 125 \times 10^{-6} \text{ секунд} = 125\mu\text{s}$$

Приклад 4.5

Хвиля синуса завершила один цикл через 4 секунди. Яка її частота?

Рішення

Нехай T період і f частота. Тоді

$$f = 1/T = 1/4 = 0.25 \text{ Hz}$$

Приклад 4.6

Хвиля синуса завершила один цикл за $25 \mu\text{s}$. Яка її частота?

Рішення

Нехай T період і f частота. Тоді

$$f = 1/T = 1/(25 \times 10^{-6}) = 40,000 \text{ Hz} = 40 \times 10^3 \text{ Hz} = 40 \text{ KHz}$$

Більше про Частоту

Ми знаємо вже, що частота – взаємовідношення сигналу до вказаного строку і що частота форми хвилі – кількість циклів за секунду. Але з іншої точки зору частота є вимірюванням змін. Електромагнітні сигнали мають форму вібруючої форми; це означає, що вони коливаються безперервно і прогнозовано над і нижче середнього горизонтального рівня. Норма, за якою рухаються хвилі синуса від найнижчого до найвищого горизонтального – частота. Сигнал 40 Hz має половину частоти від 80 Hz сигналу; він завершує один цикл в два рази швидше від 80 Hz сигналу, так кожний цикл також займає вдвічі довше, щоб змінити від найнижчого до найвищих рівнів напруги. Частота, таким чином, хоч описана в герцах, є загальним вимірюванням норми зміни сигналу щодо часу.

Частота є нормою зміни щодо часу. Зміни в короткому діапазоні часу означають високу частоту. Зміни за довгий діапазоні часу означають низьку частоту.

Якщо значення сигналу змінюється за дуже короткий відрізок часу, частота є високою. Якщо вона змінюється за довгим відрізок часу, частота є низькою.

Дві Крайнощі

А що, коли сигнал не змінюється взагалі? А що коли він підтримує постійну напругу? В такому випадку, частота є нульовою. Концептуально, ця ідея є проста. Якщо сигнал не змінюється взагалі, він ніколи не завершить цикл, так що частота є 0 Hz.

А що, коли сигнал змінюється миттєво? А що, коли ці стрибки від одного рівня до іншого не займають час? Тоді частота є невизначеною. Іншими словами, коли сигнал змінюється миттєво, період є нульовим; з тих пір, як частота – протилежність періоду, тоді, в даному випадку, частота є $1/0$, або нескінченність.

Якщо сигнал не змінюється взагалі, частота є нульовою. Якщо сигнал змінюється миттєво, частота є нескінченна.

Фаза

Термін Фаза описує місцеположення хвилі відносно нуля. Якщо ми вважаємо хвилю як таку, що може бути зісунута назад або вперед вздовж осі часу, фаза описує розмір того переміщення. Це вказує статус першого циклу.

Фаза описує місцеположення хвилі відносно нульового часу.

Фаза виміряється в градусах або радіанах (360 градусів є 2π радіан). Зсув фази на 360 градусів відповідає переміщенню повного періоду; фазове переміщення 180 градусів відповідає переміщенню періоду половини; і фазове переміщення 90 градусів відповідає переміщенню четверті періоду (рис. 4.7).

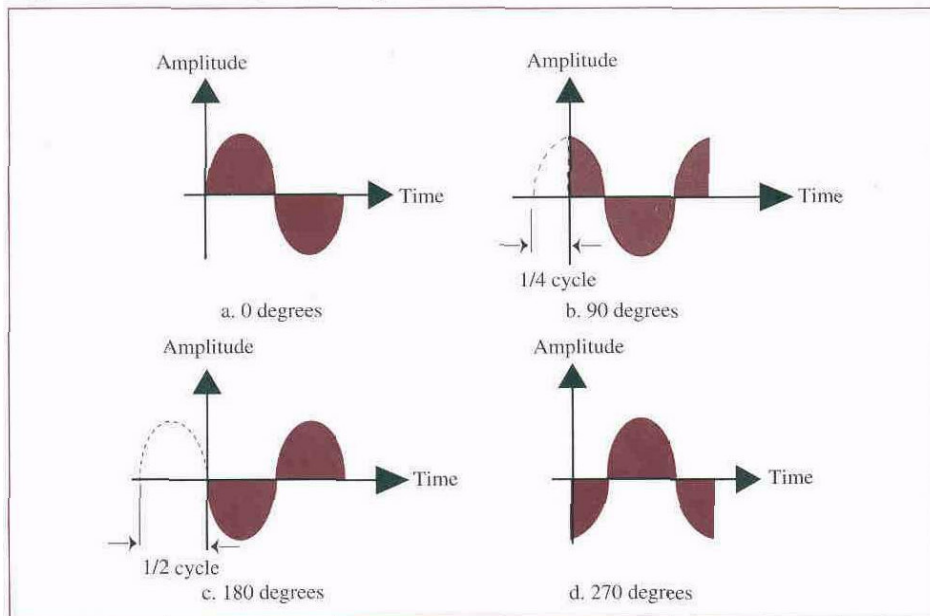


Рис. 4.7. Взаємовідношення між різними фазами

Приклад 4.7

Хвиля синуса становить $1/6$ циклу щодо нульового часу. Якою є фаза?

Рішення

Ми знаємо, що один повний цикл – 360 градусів. Таким чином, $1/6$ циклу є

$$1/6 \times 360 = 60 \text{ градусів}$$

Візуальне порівняння амплітуди, частоти, і фаза надає дані, корисні для розуміння їх функцій. Зміни у всіх трьох властивостях можуть бути введені в сигнал і електронно контрольованими. (дивіться рис. 4.8, 4.9, і 4.10).

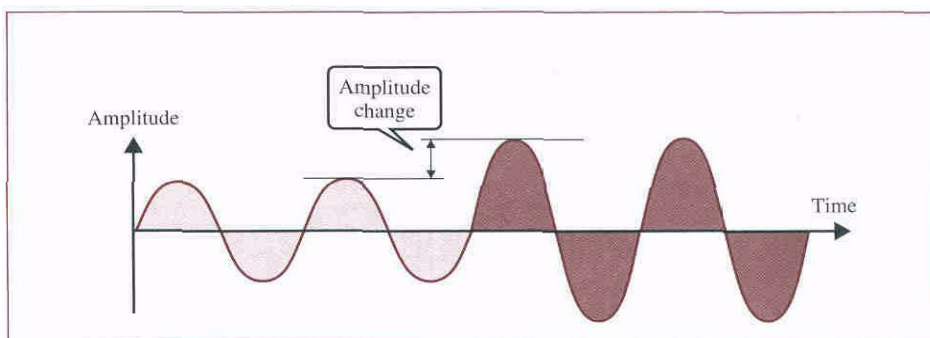


Рис. 4.8. Зміна амплітуди

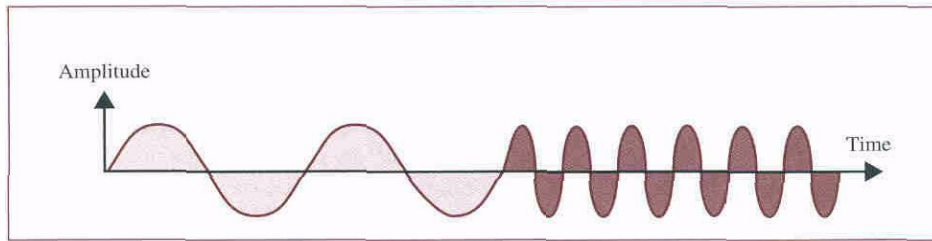


Рис. 4.9 Частотна зміна

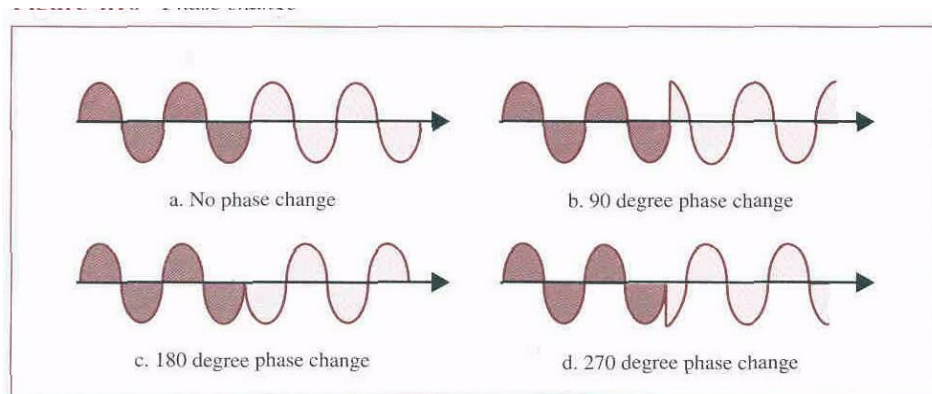


Рис. 4.10. Фазова зміна

Хвиля синуса всесторонньо визначається амплітудою, частотою, і фазою. Ми покажемо хвилю синуса, використовуючи так званий графік час-області. Графік час-область показує зміну амплітуди сигналу щодо часу (це – графік амплітуда за час). Фаза і частота ясно не вимірюються на графіку час-область.

Щоб показати взаємовідношення між амплітудою і частотою, ми можемо використати, так званий графік частота-область. На рий. 4.11 порівнюється інтервал (миттєва амплітуда щодо часу) і частотна область (максимальна амплітуда щодо частоти).

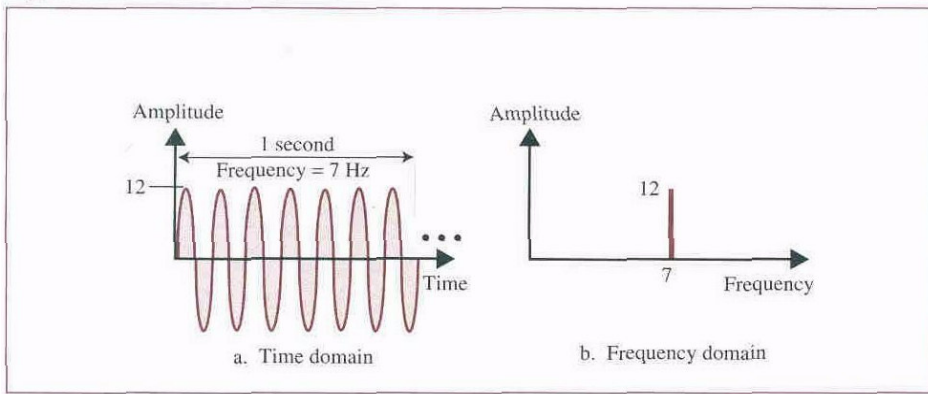


Рис. 4.11. Области часу і частоти

На рис. 4.12 дано графіків час-область і частота-область трьох сигналів із варіюванням частот і амплітуд. Порівняйте моделі в межах кожної пари, щоб дивитися який вид інформації краще підходить для передачі.

Низькочастотний сигнал в області частоти відповідає сигналу з довгим періодом в інтервалі часу і навпаки. Сигнал, який змінюється швидко в часі, відповідає високим частотам в частотній області.

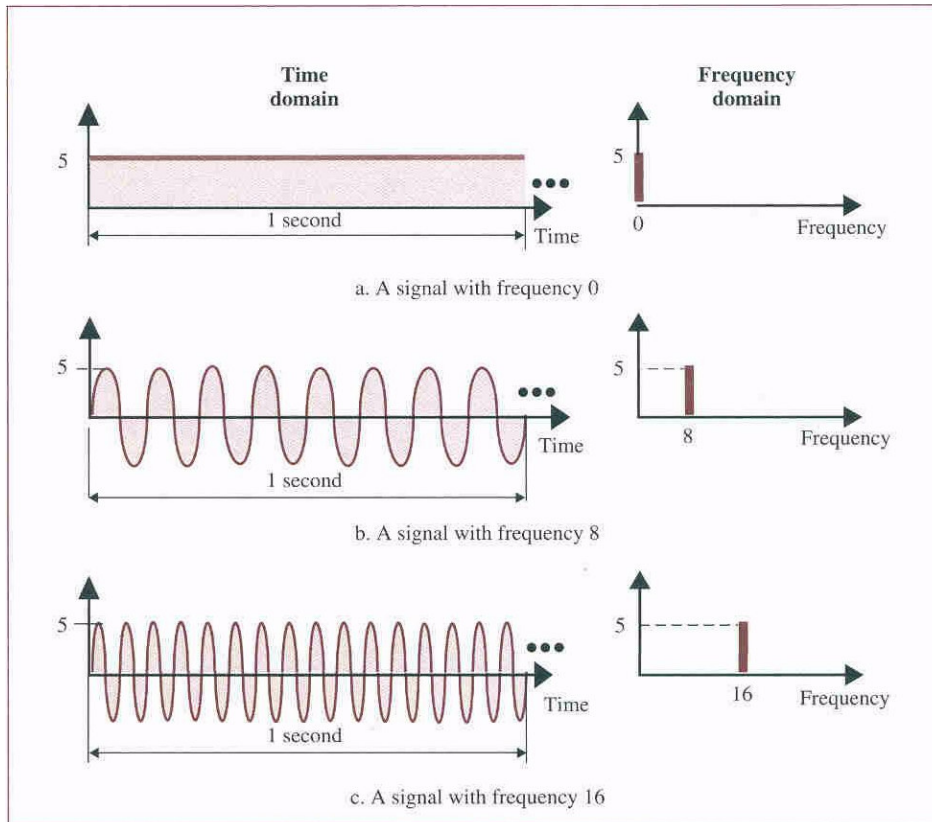


Рис. 4.12. Области часу і частоти для різних сигналів

4.4. Складні сигнали та їх характеристики

Частотний спектр та смуга пропускання Складові Сигнали

Поки що, ми зосередили увагу на простих періодичних сигналах (хвилі синуса). Але що можна сказати про періодичні сигнали, які не є хвилями синуса? Багато корисних форм хвиль не змінюються в єдиній гладкій кривій між мінімальною і максимальною амплітудою; вони стрибають, ковзають, гойдаються і занурюються. Але поки будь-яка нерегулярність є послідовною, цикл за циклом, сигнал є ще періодичним і логічно повинен бути описаним в тих же умовах, що використовуються для хвиль синуса. Фактично, може показано, що будь-який періодичний сигнал, байдуже який складний, може бути розбитий на набір хвиль синуса, кожний з яких має виміряну амплітуду, частоту, і фазу.

Щоб розкласти складовий сигнал на компоненти, є необхідним аналіз Фур'є. Проте, поняття розпаду можна побачити на простому прикладі. На рис. 4.13 показано періодичний сигнал, розкладений на дві хвилі синуса. Перша хвиля (середній графік) синуса має частоту 6, в той час коли друга синусова хвиля має частоту 0. Додавання цій двох точок крапка за крапкою приводить до верхнього графа. Можна помітити, що оригінальні сигнали виглядають як хвиля синуса, яка має, малу вісь часу зісунуту вниз. Середня амплітуда цього сигналу є ненульовою. Цей коефіцієнт вказує на присутність нульово-частотного компоненту, компоненту постійного струму (DC). Цей компонент DC відповідає за 10-одиниць зізуву направлено вгору.

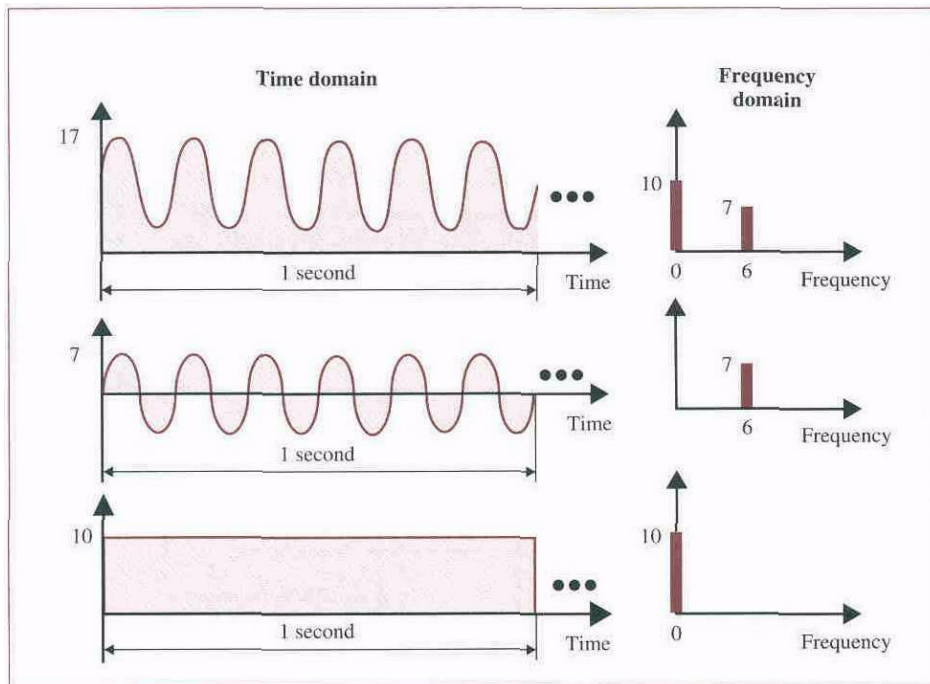


Рис. 4.13. Сигнал з компонентом DC

В контрасті до графу час-область, який ілюструє складовий сигнал як окремий об'єкт, граф частота-область показує складовий сигнал як серію складових частот. За винятком показу зіткнення кожного компонента з іншими, воно показує сигнал як набір незалежних частот.

Не дивлячись на те, що граф час-область є більш корисним для розуміння зіткнення двох сигналів один з одним, вертикальні бари графа частотної області дають більш стислий вигляд відносних частот і амплітуд складових хвиль синусу.

На рис. 4.14 показано складовий сигнал, розкладений на чотири компоненти. Цей сигнал є близьким до цифрового сигналу даних. Для точного цифрового сигналу даних, нам потрібно нескінченна кількість нерівних гармонійних сигналів (f , $3f$, $5f$, $9f$...), кожне з іншою амплітудою. Графи частотної області також показуються.

Частотний спектр і смуга пропускання

Тут слід загадати два терміни: спектр і смуга пропускання. Частотний спектр сигналу – колекція всіх складових частот, що він містить і показується використання графа частотної області. Смуга пропускання сигналу – ширина частотного спектру (рис. 4.15). Іншими словами, смуга пропускання відноситься до ряду складових частот, і частотний спектр відноситься до елементів в межах того ряду. Щоб обчислити смугу пропускання, слід відняти найнижчу частоту від найвищої частоти ряду.

Частотний спектр сигналу – комбінація всіх сигналів хвилі синуса які утворюють той сигнал.

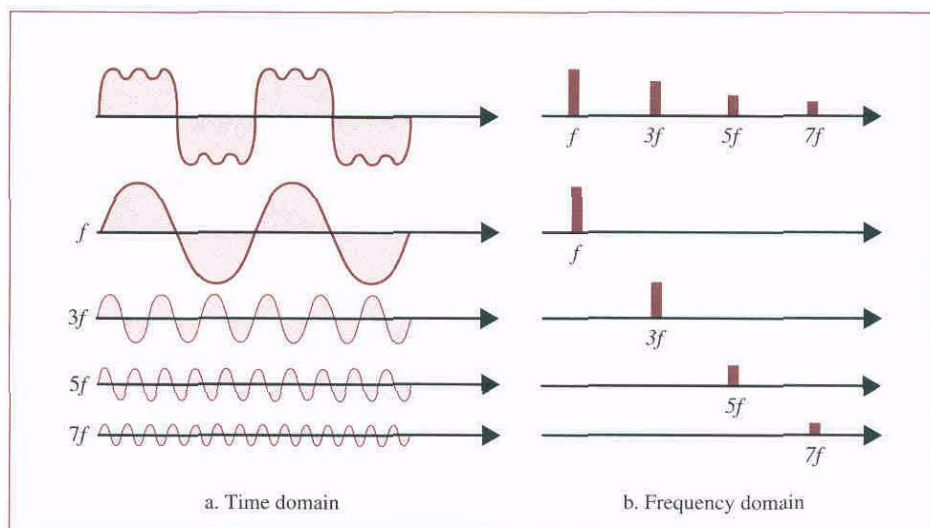


Рис. 4.14. Складові хвилі

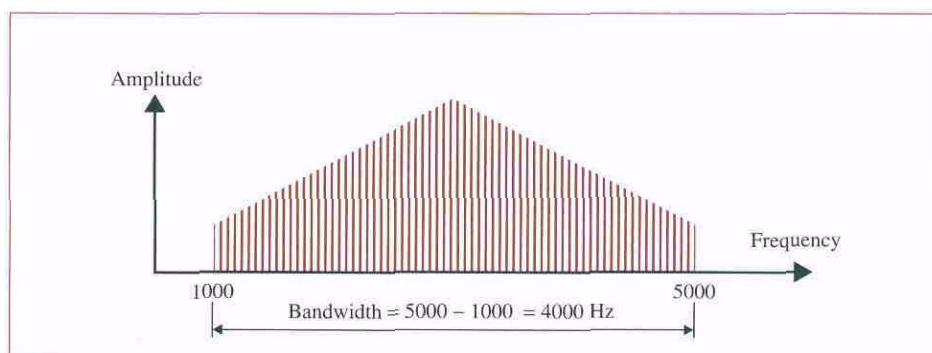


Рис. 4.15. Смуга пропускання

Приклад 4.8

Якщо періодичний сигнал розкласти на п'ять хвиль синуса з частотами 100, 300, 500, 700, і 900 Hz, що є смугою пропускання? Намалюємо спектр, припускаючи що всі компоненти мають максимальну амплітуду 10 вольтів.

Рішення

Припустимо, що f_h найвища частота, f_l найнижча частота, і b смуга пропускання. Тоді,

$$B=f_h - f_l = 900-100 = 800 \text{ Hz}$$

Спектр має тільки п'ять смужок, в 100, 300, 500, 700 і 900 (рис. 4.16).

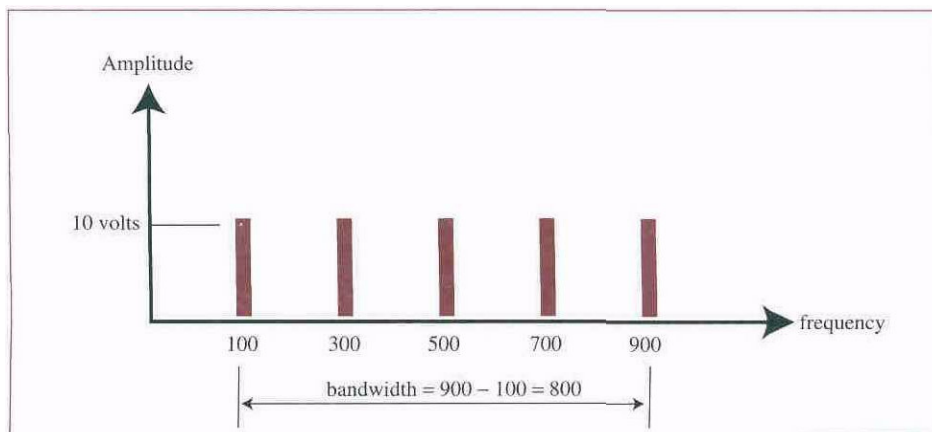


Рис. 4.16. Приклад 4.8

Приклад 4.9

Сигнал має смугу пропускання 20 Hz. Найвища частота є 60 Hz. Чим є найнижча частота? Намалуйте спектр, якщо сигнал містить всі цілочисельні частоти тієї ж амплітуди.

Рішення

Припустимо, що f_h найвища частота, f_l найнижча частота, і b смуга пропускання. Тоді,

$$B=f_h - f_l \rightarrow 20 = 60 - f_l \rightarrow f_l = 60-20 = 40 \text{ Hz}$$

Спектр містить всі цілочисельні частоти. Ми показуємо це серією смужок (дивіться рис. 4.17).

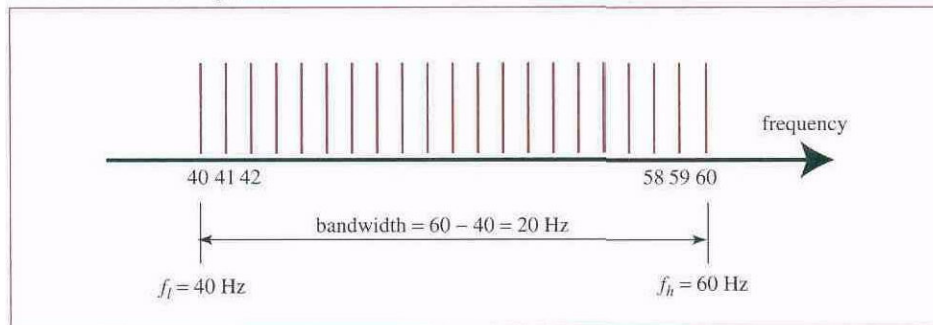


Рис. 4.17. Приклад 4.9

Сигнали з обмеженим спектром

Щоб зрозуміти, яке відношення все вищевикладене має до передачі даних, розглянемо конкретний приклад – передачу двійкового коду ASCII символу. Для цього потрібно буде 8 біт (тобто 1 байт). Задача – передати наступну послідовність біт: 01100010. На мал. 4.18, зліва зображена залежність напруги виходу від часу на передаючому комп’ютері. В результаті аналізу Фур’є для даного сигналу набуваємо наступні значення коефіцієнтів:

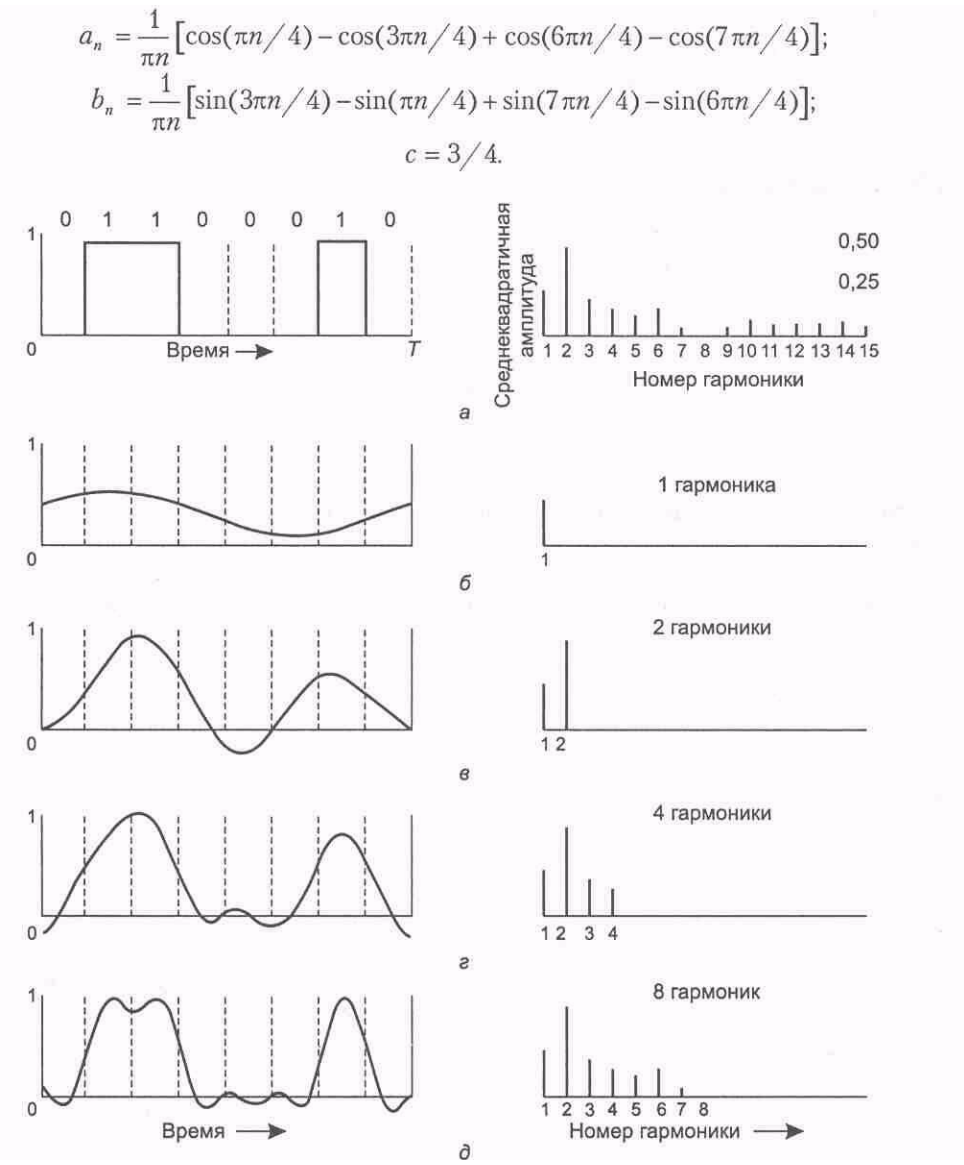


Рис 4.18. Двійковий сигнал і його середньоквадратичні гармоніки Фур'є (а); послідовні наближення до оригінального сигналу (б-д)

Середньоквадратичні амплітуди для декількох перших гармонік показані на мал. 4.18, а справа. Ці значення представляють інтерес, оскільки їх квадрати пропорційні енергії, передаваній на відповідній частоті.

Жоден канал зв'язку не може передавати сигнали без втрати потужності. Якби всі гармоніки ряду Фур'є зменшувалися при передачі в рівному ступені, то сигнал зменшувався б по амплітуді, але не спотворювався (тобто в нього була б та ж прямокутна форма, як на мал. 2.1, а). На жаль, всі канали зв'язку зменшують гармоніки ряду Фур'є в різні

ступені, тим самим спотворюючи передаваний сигнал. Як правило, амплітуди передаються без зменшення в частотному діапазоні від 0 до якоїсь частоти (що вимірюється в періодах в секунду або герцах (Гц)), при цьому високочастотна складова сигналу (вище частоти, яку називають частотою зрізу) помітно ослабляється. Цей діапазон частот називається смугою пропускання. На практиці зріз зовсім не є таким різким, тому звичайно в згадану смугу пропускання включають ті частоти, які передаються із втратою потужності, що не перевищує 50 %.

Смуга пропускання є фізичною характеристикою середовища передачі даних і залежить звичайно від конструкції, товщини і довжини носія. Іноді для навмисного зменшення смуги пропускання, доступної абонентам, в лінію включається спеціальний пристрій – фільтр. Наприклад, кабель, використовуваний в телефонії при невеликих відстанях, має смугу пропускання, рівну 1 мгц, проте телефонні компанії за допомогою частотних фільтрів урізують її, надаючи користувачам лише 3100 Гц. Такої смуги, втім, цілком вистачає для виразної передачі мови, зате за рахунок зменшення ресурсів, що витрачаються кожним абонентом, підвищується загальна ефективність системи.

Тепер подивимося, як буде виглядати сигнал, зображений на мал. 4.18, а, якщо смуга пропускання каналу буде такою, що через нього будуть проходити тільки найнижчі частоти (тобто функція $g(t)$ буде апроксимована лише декількома першими членами рядів рівняння (2.1)). На мал. 4.18, б показаний сигнал на виході каналу, проникного лише першу (основну) гармоніку сигналу. Аналогічно, мал. 4.18, в-д показують спектри і відновлені сигнали для каналів з більш широкою смугою пропускання.

При заданій швидкості передачі в бітах, рівної b біт/с, час, що вимагається для передачі, скажімо, 8 біт, буде рівним $8/b$ секунд. Таким чином, частота першої гармоніки рівна $b/8$ Гц. Звичайна телефонна лінія, часто звана мовним каналом, має штучно створену частоту зрізу близько

3000 Гц. Це обмеження означає, що номер найвищої гармоніки, що пройшла крізь телефонний канал, приблизно (зріз не дуже крутий) рівний $3000/(b/8)$ або $24\ 000/b$.

Для деяких швидкостей передачі даних ці значення показані в табл. 2.1. З приведених даних ясно, що спроба передати по мовному каналу дані на швидкості 9600 біт/с перетворить сигнал, показаний на мал. 4.18, в щось подібне рис. 4.18, в, що зробить прийом початкового потоку бітів з прийнятною якістю практично неможливим. Очевидно, що в сигналів, передаваних із швидкістю 38 400 біт/с і вище, немає жодних шансів пройти через мовний канал, навіть при повній відсутності перешкод на лінії. Іншими словами, обмеження смуги пропускання частот каналу обмежує його пропускну здатність для передачі двійкових даних, навіть для ідеальних каналів. Проте схеми, що використовують декілька рівнів напруг, існують і дозволяють досягти більш високих швидкостей передачі даних. Ми обговоримо це далі в цьому розділі.

Таблиця 2.1. Співвідношення між швидкістю передачі даних і числом гармонік

Швидкість біт/с	T, мс	1-а гармоніка, Гц	Кількість гармонік, що пропускаються
300	26,67	37,5	80
600	13,33	75	40
1200	6,67	150	20
2400	3,33	300	10
4800	1,67	600	5
9600	0,83	1200	2
19200	0,42	2400	1
38400	0,21	4800	0

Максимальна швидкість передачі даних через канал

В 1924 році американський учений Х. Найквіст (H. Nyquist) з компанії AT&T прийшов до висновку, що існує якусь гранична швидкість передачі навіть для ідеальних каналів. Він вивів рівняння, що дозволяє знайти максимальну швидкість передачі даних в безшумному каналі з обмеженою смугою пропускання частот. В 1948 році Клод Шеннон (Claude Shannon) продовжив роботу Найквіста і розширив її для випадку каналу з випадковим (тобто термодинамічним) шумом. Ми стисло розглянемо результати роботи Найквіста і Шеннона, що стали сьогодні класичними.

Найквіст довів, що якщо довільний сигнал пройшов через низькочастотний фільтр із смугою пропускання H , то такий відфільтрований сигнал може бути повністю відновлений по дискретних значеннях цього сигналу, виміряних з частотою $2H$ в секунду. Проводити вимірювання сигналу частіше, ніж $2H$ в секунду, немає сенсу, оскільки більш високочастотні компоненти сигналу були відфільтровані. Якщо сигнал складається з V дискретних рівнів, то рівняння Найквіста буде виглядати так:

$$\text{максимальна швидкість передачі даних} = 2H \log_2 V, \text{ біт/с}$$

Так, наприклад, безшумний канал з частотою пропускання в 3 кГц не може передавати двійкові (тобто дворівневі) сигнали на швидкості, вище 6000 Кбіт/с.

Отже, ми розглянули випадок безшумних каналів. За наявності в каналі випадкового шуму ситуація різко погіршується. Рівень термодинамічного шуму в каналі вимірюється відношенням потужності сигналу до потужності шуму і називається відношенням сигнал/шум. Якщо позначити потужність сигналу S , а потужність шуму – N , то відношення сигнал/шум буде рівний S/N . Звичайно сама величина відношення не вживається. Замість неї використовується її десятковий логарифм, помножений на 10: $10 \lg S/N$. Така одиниця називається децибелом (decibel, dB, дБ). Таким чином, якщо відношення сигнал/шум 10, це відповідає 10 дБ, відношення 100 рівно 20 дБ,

відношення 1000 рівно 30 дБ і т.д. Виробники стереопідсилювачів часто вказують смугу частот (частотний діапазон), в якому їх апаратура має лінійну амплітудно-частотну характеристику в межах 3 дБ. Відхилення в 3 дБ відповідає ослабленню сигналу приблизно в двічі (тому що $\log 3 = 0,5$).

Головним результатом, який отримав Шеннон, було твердження про те, що максимальна швидкість передачі даних в каналі із смугою частот H Гц і відношенням сигнал/шум, рівним S/N , можна обчислити по формулі

$$\text{максимальна швидкість передачі даних} = H \log_2(1+S/N).$$

Наприклад, канал з частотною смугою пропускання в 3000 Гц і відношенням потужностей сигналу і термального шуму в 30 дБ (звичайні параметри для аналогової частини телефонної системи) ніколи не зможе передавати більше 30 000 біт/с, незалежно від способу модуляції сигналу, тобто кількості використовуваних рівнів сигналу, частоти дискретизації і т.д. Результат, отриманий Шенноном і підкріплений постулатами теорії інформації, застосовний до будь-якого каналу з гаусівським (термальним) шумом. Спроби довести зворотне слід вважати приреченими не провал. Проте слід відмітити, що дана теорема описує верхню, теоретичну межу пропускну спроможності інформаційного каналу, і реальні системи рідко досягають його.

Характеристики ліній зв'язку

Типи характеристик і способи їх визначення

До основних характеристик ліній зв'язки відносяться:

- амплітудно-частотна характеристика;
- смуга пропускання;
- загасання;
- завадостійкість;
- перехресні наводки на ближньому кінці лінії;
- пропускну здатність;

- достовірність передачі даних;
- питома вартість.

В першу чергу розробника обчислювальної мережі цікавлять пропускна здатність і достовірність передачі даних, оскільки ці характеристики прямо впливають на продуктивність і надійність створюваної мережі. Пропускна здатність і достовірність – це характеристики як лінії зв'язку, так і способу передачі даних. Тому якщо спосіб передачі (протокол) вже визначений, то відомі і ці характеристики. Наприклад, пропускна здатність цифрової лінії завжди відома, оскільки на ній визначений протокол фізичного рівня, який задає бітову швидкість передачі даних – 64 Кбіт/с, 2 Мбіт/с тощо.

Проте не можна говорити про пропускну здатність лінії зв'язку, до того як для неї визначений протокол фізичного рівня. Саме в таких випадках, коли тільки належить визначити, який з безлічі існуючих протоколів можна використовувати на даній лінії, дуже важливими є решта характеристик лінії, такі як смуга пропускання, перехресні наведення, перешкодостійкість і інші характеристики.

Для визначення характеристик лінії зв'язки часто використовують аналіз її реакцій на деякі еталонні дії. Такий підхід дозволяє достатньо просто і однотипно визначати характеристики ліній зв'язку будь-якої природи, не вдаючись до складних теоретичних досліджень. Частіше всього як еталонних сигналів для дослідження реакцій ліній зв'язку використовуються синусоїдальні сигнали різних частот. Це пов'язано з тим, що сигнали цього типу часто зустрічаються в техніці і з їх допомогою можна уявити будь-яку функцію часу – як безперервний процес коливання звуку, так і прямокутні імпульси, що генеруються комп'ютером.

Спектральний аналіз сигналів на лініях зв'язку

З теорії гармонійного аналізу відомо, що будь-який періодичний процес можна уявити у вигляді суми синусоїдальних коливань різних частот і різних амплітуд (мал. 4.19). Кожна становляча синусоїда називається також гармонікою, а набір всіх гармонік називають спектральним розкладанням початкового сигналу. Неперіодичні сигнали можна уявити у вигляді інтеграла синусоїдальних сигналів з безперервним спектром частот. Наприклад, спектральне розкладання ідеального імпульсу (одиничної потужності і нульової тривалості) має складові всього спектру частот, від $-\infty$ до $+\infty$ (мал. 4.20).

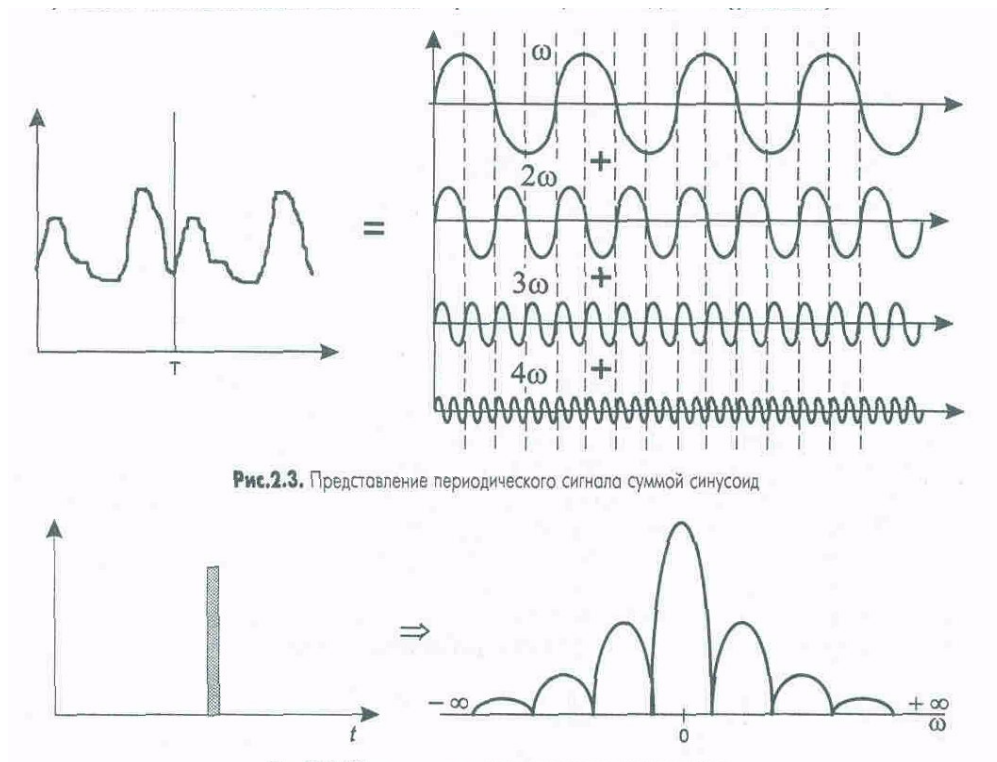


Рис.2.3. Представление периодического сигнала суммой синусоид

Рис.4.20. Спектральне розкладання ідеального імпульсу

Техніка знаходження спектру будь-якого початкового сигналу добре відома. Для деяких сигналів, які добре описуються аналітично (наприклад, для послідовності прямокутних імпульсів однакової тривалості і амплітуди), спектр легко обчислюється на основі формул Фур'є. Для сигналів довільної форми, що зустрічаються на практиці, спектр можна знайти за допомогою

спеціальних приладів – спектральних аналізаторів, які виміряють спектр реального сигналу і відображають амплітуди становлячих гармонік на екрані або роздруковують їх на принтері.

Спотворення передаючим каналом синусоїди якої-небудь частоти приводить до спотворення передаваного сигналу будь-якої форми, особливо якщо синусоїди різних частот спотворюються неоднаково. Якщо це аналоговий сигнал, що передає мову – то змінюється тембр голосу за рахунок спотворення обертонів – бічних частот. При передачі імпульсних сигналів, характерних для комп'ютерних мереж, спотворюються низькочастотні і високочастотні гармоніки, в результаті фронти імпульсів втрачають свою прямокутну форму (мал. 4.21). Внаслідок цього на приймальному кінці лінії сигнали можуть погано розпізнаватися.

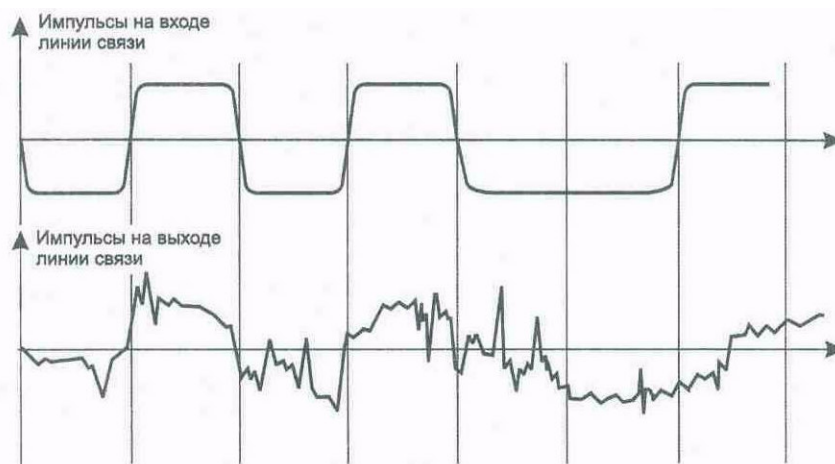


Рис. 4.21. Спотворення імпульсів в лінії зв'язку

Лінія зв'язку спотворює передавані сигнали через те, що її фізичні параметри відрізняються від ідеальних. Так, наприклад, мідні дроти завжди представляють собою деяку розподілену по довжині комбінацію активного опору, навантаження місткості і індуктивної (мал. 4.22). В результаті для синусоїд різних частот лінія буде володіти різним повним опором, а значить, і передаватися вони будуть по-різному. Волоконно-оптичний кабель також

має відхилення, що заважають ідеальному розповсюдженню світла. Якщо лінія зв'язку включає проміжну апаратуру, то вона також може вносити додаткові спотворення, оскільки неможливо створити пристрої, які б однаково добре передавали весь спектр синусоїд, від нуля до безкінечності.

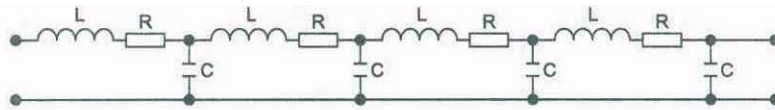


Рис. 2.6 Представлення лінії як розподіленого навантаження індуктивної місткості

Окрім спотворень сигналів, що вносяться внутрішніми фізичними параметрами лінії зв'язку, існують і зовнішні перешкоди, які вносять свій внесок в спотворення форми сигналів на виході лінії. Ці перешкоди створюють різні електричні двигуни, електронні пристрої, атмосферні явища і т.д. Незважаючи на захисні заходи, що робляться розробниками кабелів і підсилювально-комутуючої апаратури, повністю компенсувати вплив зовнішніх перешкод не вдається. Тому сигнали на виході лінії зв'язку звичайно мають складну форму (як це і показано на рис, 4.21), по якій іноді важко зрозуміти, яка дискретна інформація була подана на вхід лінії.

Амплітудно-частотна характеристика, смуга пропускання і загасання

Ступінь спотворення синусоїдальних сигналів лініями зв'язку оцінюється за допомогою таких характеристик, як амплітудно-частотна характеристика, смуга пропускання і загасання на певній частоті.

Амплітудно-частотна характеристика (мал. 4.23) показує, як затухає амплітуда синусоїди на виході лінії зв'язку в порівнянні з амплітудою на її вході для всіх можливих частот передаваного сигналу. Замість амплітуди в цій характеристиці часто використовують також такий параметр сигналу, як його потужність.



Рис. 2.23. Амплітудно-частотна характеристика

Знання амплітудно-частотної характеристики реальної лінії дозволяє визначити форму сигналу виходу практично для будь-якого вхідного сигналу. Для цього необхідно знайти спектр вхідного сигналу, перетворити амплітуду становлячих його гармонік відповідно до амплітудно-частотної характеристики, а потім знайти форму сигналу виходу, склавши перетворені гармоніки.

Не дивлячись на повноту інформації, амплітудно-частотною характеристикою, що надається, про лінію зв'язку, її використання ускладнюється тією обставиною, що отримати її вельми важко. Адже для цього потрібно провести тестування лінії еталонними синусоїдами по всьому діапазону частот від нуля до деякого максимального значення, яке може зустрітися у вхідних сигналах. Причому міняти частоту вхідних синусоїд потрібно з невеликим кроком, а значить, кількість експериментів повинна бути дуже великою. Тому на практиці замість амплітудно-частотної характеристики застосовуються інші, спрощені характеристики – смуга пропускання і загасання.

Смуга пропускання (bandwidth) – це безперервний діапазон частот, для якого відношення амплітуди сигналу виходу до вхідного перевищує деяку наперед задану межу, звичайно 0,5. Тобто смуга пропускання визначає

діапазон частот синусоїдального сигналу, при яких цей сигнал передається по лінії зв'язку без значних спотворень. Знання смуги пропускання дозволяє отримати з деякою мірою наближення той же результат, що і знання амплітудно-частотної характеристики. Як ми побачимо нижче, ширина смуги пропускання в щонайбільшому ступені впливає на максимально можливу швидкість передачі інформації по лінії зв'язку. Саме цей факт знайшов віддзеркалення в англійському еквіваленті даного терміну (width – ширина).

Загасання (attenuation) визначається як відносне зменшення амплітуди або потужності сигналу при передачі по лінії сигналу певної частоти. Таким чином, загасання представляє собою одну крапку з амплітудно-частотної характеристики лінії. Часто при експлуатації лінії наперед відома основна частота передаваного сигналу, тобто та частота, гармоніка якої має щонайбільшу амплітуду і потужність. Тому достатньо знати загасання на цій частоті, щоб приблизно оцінити спотворення передаваних по лінії сигналів. Більш точні оцінки можливі при знанні загасання на декількох частотах, відповідних декільком основним гармонікам передаваного сигналу.

Загасання A звичайно вимірюється в децибелах (дБ, decibel – dB) і обчислюється по наступній формулі:

$$A = 10 \log_{10} P_{\text{вих}}/P_{\text{вх}}$$

де $P_{\text{вих}}$ – потужність сигналу на виході лінії, $P_{\text{вх}}$ – потужність сигналу на вході лінії.

Оскільки потужність сигналу кабелю виходу без проміжних підсилювачів завжди менше ніж потужність вхідного сигналу, загасання кабелю завжди є негативною величиною.

Наприклад, кабель на витій парі категорії 5 характеризується загасанням не нижче $-23,6$ дБ для частоти 100 мгц при довжині кабелю 100 м. Частота 100 мгц вибрана тому, що кабель цієї категорії призначений для високошвидкісної передачі даних, сигнали яких мають значущі гармоніки з частотою приблизно 100 мгц. Кабель категорії 3 призначений для

низькошвидкісної передачі даних, тому для нього визначається загасання на частоті 10 мгц (не нижче $-11,5$ дБ). Часто оперують з абсолютними значеннями загасання, без вказування знаку.

Абсолютний рівень потужності, наприклад рівень потужності передавача, також вимірюється в децибелах. При цьому як базове значення потужності сигналу, щодо якого вимірюється поточна потужність, приймається значення в 1 мВт. Таким чином, рівень потужності p обчислюється за наступною формулою:

$$p = 10 \log_{10} P/1\text{мВт} \text{ [дБм]}$$

де P – потужність сигналу в міліватах, а дБм (dBm) – це одиниця вимірювання рівня потужності (децибел на 1 мВт).

Таким чином, амплітудно-частотна характеристика, смуга пропускання і загасання є універсальними характеристиками, і їх знання дозволяє зробити висновок про те, як через лінію зв'язку будуть передаватися сигнали будь-якої форми.

Смуга пропускання залежить від типу лінії і її протяжності. На мал. 4.24 показані смуги пропускання ліній зв'язку різних типів, а також найбільш часто використовувані в техніці зв'язку частотні діапазони.

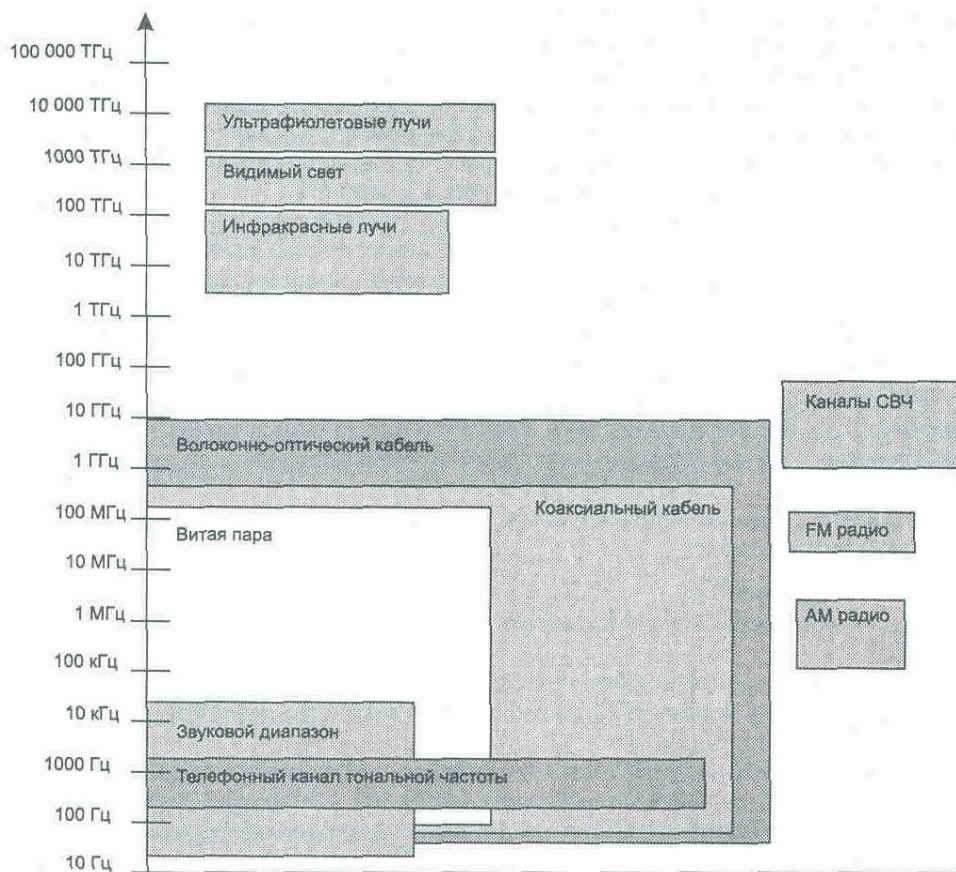


Рис. 4.24. Смуги пропускання ліній зв'язку і популярні частотні діапазони

Пропускна здатність лінії

Пропускна здатність (throughput) лінії характеризує максимально можливу швидкість передачі даних по лінії зв'язку. Пропускна здатність вимірюється в бітах в секунду – біт/с, а також в похідних одиницях, таких як кілобіт в секунду (Кбіт/с), мегабіт в секунду (Мбіт/с), гігабіт в секунду (Гбіт/с) і т.д.

ПРИМІТКА Пропускна здатність ліній зв'язку і комунікаційною мережного устаткування традиційно вимірюється в бітах за секунду, про не в байтах за секунду. Це пов'язано з тим, що дані в мережах передаються і послідовна, тобто побітно, а не паралельно, байтами, як це робиться між пристроями усередині комп'ютера. Такі одиниці вимірювання, як кілобіт, мегабіт або гігабіт, в мережних технологіях строго відповідають ступеням 10 (тобто кілобіт – це 1000 біт, а мегабіт – це 1 000 000 біт), як це прийнято у

всіх галузях науки і техніки, а не близьким до цих чисел ступеням 2, як це прийнято в програмуванні, де префікс “кіло” рівний $2^{10} = 1024$, а “мега” – $2^{20} = 1\,048\,576$

Пропускна здатність лінії зв'язку залежить не тільки від її характеристик, таких як амплітудно-частотна характеристика, але і від спектру передаваних сигналів. Якщо значущі гармоніки сигналу (тобто ті гармоніки, амплітуди яких вносять основний внесок в результуючий сигнал) потрапляють в смугу пропускання лінії, то такий сигнал буде добре передаватися даною лінією зв'язку і приймач зможе правильно розпізнати інформацію, відправлену по лінії передавачем (мал. 4.25, а). Якщо ж значущі гармоніки виходять за межі смуги пропускання лінії зв'язку, то сигнал буде значно спотворюватися, приймач буде помилятися при розпізнаванні інформації, а значить, інформація не зможе передаватися із заданою пропускну здатністю (мал. 4.25, б).

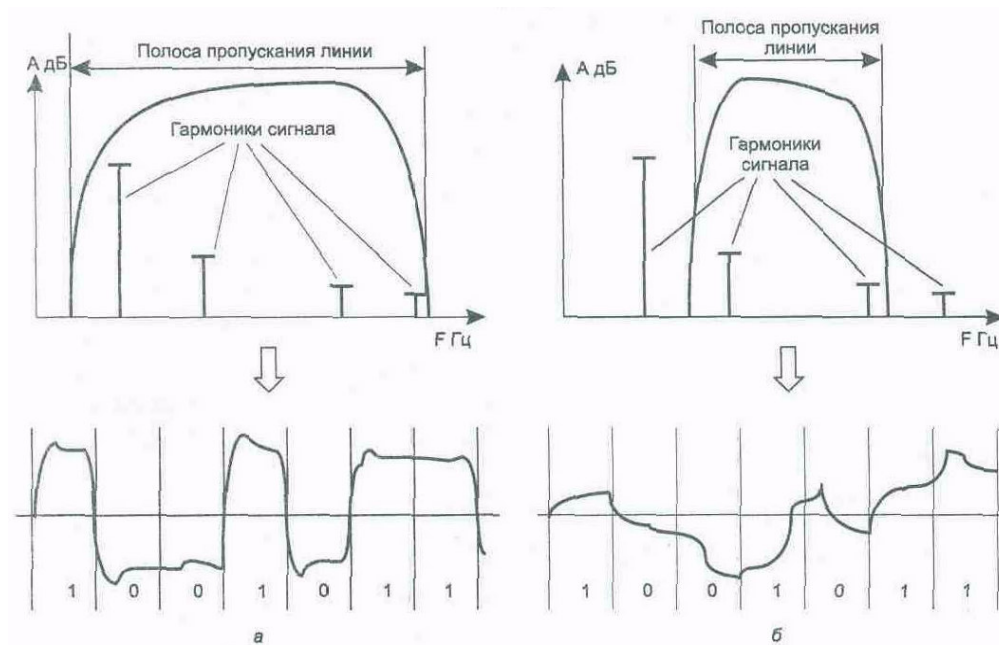


Рис. 4.25. Відповідність між смугою пропускання лінії зв'язку і спектром сигналі

Вибір способу представлення дискретної інформації у вигляді сигналів, що подаються на лінію зв'язку, називається фізичним або лінійним кодуванням. Від вибраного способу кодування залежить спектр сигналів і, відповідно, пропускна здатність лінії. Таким чином, для одного способу кодування лінія може володіти однією пропускною здатністю, а для іншого – іншою. Наприклад, віта пара категорії 3 може передавати дані з пропускною здатністю 10 Мбіт/с при способі кодування стандарту фізичного рівня 10Base-T і 33 Мбіт/с при способі кодування стандарту 100Base-T4. В прикладі, приведеному на мал. 4.25, прийнятий наступний спосіб кодування – логічна 1 уявлена на лінії позитивним потенціалом, а логічний 0 – негативним.

Теорія інформації говорить, що будь-яка помітна і непередбачувана зміна сигналу, що приймається, несе в собі інформацію. Відповідно до цього прийом синусоїди, в якій амплітуда, фаза і частота залишаються незмінними, інформації не несе, оскільки зміна сигналу хоча і відбувається, але добре передбачена. Аналогічно, не несуть в собі інформації імпульси на тактовій шині комп'ютера, оскільки їх зміни також постійні в часі. А ось імпульси на шині даних передбачити наперед не можна, тому вони переносять інформацію між окремими блоками або пристроями.

Більшість способів кодування використовують зміну якого-небудь параметра періодичного сигналу – частоти, амплітуди і фази синусоїди або ж знак потенціалу послідовності імпульсів. Періодичний сигнал, параметри якого змінюються, називають несучим сигналом або несучою частотою, якщо як такого сигналу використовується синусоїда.

Якщо сигнал змінюється так, що можна розрізнити тільки два його стани, то будь-яка його зміна буде відповідати якнайменшій одиниці інформації – біту. Якщо ж сигнал може мати більше двох помітних станів, то будь-яка його зміна буде нести декілька біт інформації.

Кількість змін інформаційного параметра несучого періодичного сигналу в секунду вимірюється у водах (baud). Період часу між сусідніми змінами інформаційного сигналу називається тактом роботи передавача.

Пропускна здатність лінії в бітах в секунду в загальному випадку не співпадає з числом бод. Вона може було як вище, так і нижче за число бод, і це співвідношення залежить від способу кодування.

Якщо сигнал має більше двох помітних станів, то пропускна здатність в бітах в секунду буде вищою, ніж число бод. Наприклад, якщо інформаційними параметрами є фаза і амплітуда синусоїди, причому розрізняються 4 стани фази в 0, 90, 180 і 270 градусів і двоє значень амплітуди сигналу, то інформаційний сигнал може мати 8 помітних станів. В цьому випадку модем, працюючий із швидкістю 2400 бод (з тактовою частотою 2400 Гц) передає інформацію із швидкістю 7200 біт/с, оскільки при одній зміні сигналу передається 3 біти інформації.

При використуванні сигналів з двома помітними станами може спостерігатися зворотна картина. Це часто стається тому, що для надійного розпізнавання приймачем призначеної для користувача інформації кожний біт в послідовності кодується за допомогою декількох змін інформаційного параметра несучого сигналу. Наприклад, при кодуванні одиничного значення біта імпульсом позитивної полярності, а нульового значення біта – імпульсом негативної полярності фізичний сигнал двічі змінює свій стан при передачі кожного біта. При такому кодуванні пропускна здатність лінії в двічі нижче, ніж число бод, передаване по лінії.

На пропускну здатність лінії робить вплив не тільки фізичне, але і логічне кодування. Логічне кодування виконується до фізичного кодування і має на увазі заміну біт початкової інформації новою послідовністю біт, несучою ту ж інформацію, але володіючій, окрім цього, додатковими властивостями, наприклад можливістю для приймальної сторони знаходити помилки в прийнятих даних. Супровід кожного байта початкової інформації

одним бітом парності – це приклад дуже часто вживаного способу логічного кодування при передачі даних за допомогою модемів. Іншим прикладом логічного кодування може служити шифрування даних, забезпечуючи їх конфіденційність при передачі через загальні канали зв'язку. При логічному кодуванні частіше всього початкова послідовність біт замінюється більш довгою послідовністю, тому пропускна здатність каналу по відношенню до корисної інформації при цьому зменшується.

Зв'язок між пропускною здатністю лінії і її смугою пропускання

Чим вище частота несучого періодичного сигналу, тим більше інформації в одиницю часу передається по лінії і тим вище пропускна здатність лінії при фіксованому способі фізичного кодування. Проте, з другого боку, із збільшенням частоти періодичного несучого сигналу збільшується і ширина спектру цього сигналу, тобто різниця між максимальною і мінімальною частотами того набору синусоїд, які в сумі дадуть вибрану для фізичного кодування послідовність сигналів. Лінія передає цей спектр синусоїд з тими спотвореннями, які визначаються її смугою пропускання. Чим більше невідповідність між смугою пропускання лінії і шириною спектру передаваних інформаційних сигналів, тим більше сигнали спотворюються і тим вірогідніше за помилку в розпізнаванні інформації приймаючою стороною, а значить, швидкість передачі інформації насправді виявляється менше ніж можна було припустити.

Зв'язок між смугою пропускання лінії і її максимально можливою пропускною здатністю, незалежно від прийнятого способу фізичного кодування, встановив Клод Шеннон:

$$C = F \log_2 (1 + P_s/P_{ш}).$$

де C – максимальна пропускна здатність лінії в бітах в секунду, F – ширина смуги пропускання лінії в герцах, P_c – потужність сигналу, $P_{ш}$ – потужність шуму.

З цього співвідношення видно, що хоча теоретичної межі пропускної спроможності лінії з фіксованою смугою пропускання не існує, на практиці така межа є. Дійсно, підвищити пропускну здатність лінії можна за рахунок збільшення потужності передавача або ж зменшення потужності шуму (перешкод) на лінії зв'язку. Обидві ці складові піддаються зміні насилу. Підвищення потужності передавача веде до значного збільшення його габаритів і вартості. Зниження рівня шуму вимагає застосування спеціальних кабелів з добрими захисними екранами, що вельми дорого, а також зниження шуму в передавачі і проміжній апаратурі, чого досягти вельми не просто. До того ж вплив потужностей корисного сигналу і шуму на пропускну здатність обмежений логарифмічною залежністю, яка росте далеко не так швидко, як прямопропорційна. Так, при достатньо типовому початковому відношенні потужності сигналу до потужності шуму в 100 разів підвищення потужності передавача в 2 рази дасть тільки 15 % збільшення пропускної спроможності лінії.

Близьким за суттю до формули Шеннона є наступне співвідношення, отримане Найквістом, яке також визначає максимально можливу пропускну здатність лінії зв'язку, але без урахування шуму на лінії:

$$C = 2F \log_2 M$$

де M – кількість помітних станів інформаційного параметра.

Якщо сигнал має 2 помітні стани, то пропускна здатність рівна подвоєному значенню ширини смуги пропускання лінії зв'язку (мал. 4.26, а). Якщо ж передавач використовує більш ніж 2 стійкі стани сигналу для кодування даних, то пропускна здатність лінії підвищується, оскільки за один такт роботи передавач передає декілька біт початкових даних, наприклад 2 біти за наявності чотирьох помітних станів сигналу (мал. 4.26, б).

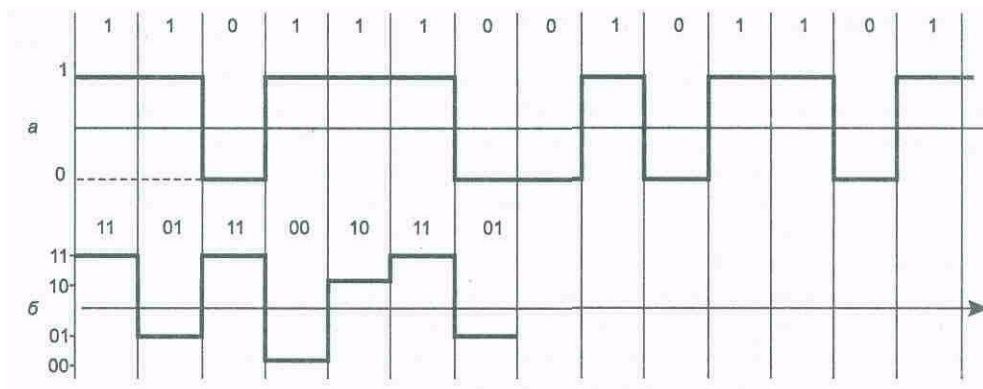


Рис. 4.26. Підвищення швидкості передачі за рахунок додаткових станів сигналу

Хоча формула Найквіста явно не урахує наявність шуму, побічно його вплив відображається у виборі кількості станів інформаційного сигналу. Для підвищення пропускної спроможності каналу хотілося б збільшити цю кількість до значних величин, але на практиці ми не можемо цього зробити через шум на лінії. Наприклад, для прикладу, приведеного на мал. 4.26, можна збільшити пропускну здатність лінії ще в двічі, використавши для кодування даних не 4, а 16 рівнів. Проте якщо амплітуда шуму часто перевищує різницю між сусідніми 16-у рівнями, то приймач не зможе стійко розпізнавати передавані дані. Тому кількість можливих станів сигналу фактично обмежується співвідношенням потужності сигналу і шуму, а формула Найквіста визначає граничну швидкість передачі даних у тому випадку, коли кількість станів вже вибрана з урахуванням можливостей стійкого розпізнавання приймачем.

Приведені співвідношення дають граничне значення пропускній спроможності лінії, а ступінь наближення до цієї межі залежить від конкретних методів фізичного кодування, що розглядаються нижче.

Завадостійкість і достовірність

Завадостійкість лінії визначає її здатність зменшувати рівень перешкод, створюваних в зовнішньому середовищі, на внутрішніх провідниках. Перешкодостійкість лінії залежить від типу використовуваного фізичного середовища, а також від екрануючих і переважних перешкоди засобів самої лінії. Якнайменше перешкодостійкими є радіолінії, доброю стійкістю володіють кабельні лінії і відмінній – волоконно-оптичні лінії, малочутливі до зовнішнього електромагнітного випромінювання. Звичайно для зменшення перешкод, що з'являються через зовнішні електромагнітні поля, провідники екранують и/или скручують.

Перехресні наведення на ближньому кінці (Near End Cross Talk – NEXТ) визначають перешкодостійкість кабелю до внутрішніх джерел перешкод, коли електромагнітне поле сигналу, передаваного виходом передавача по одній парі провідників, наводить на іншу пару провідників сигнал перешкоди. Якщо до другої пари буде підключений приймач, то він може прийняти наведену внутрішню перешкоду за корисний сигнал. Показник NEXТ, виразимий в децибелах, рівний $10 \log R_{\text{вих}}/R_{\text{нав}}$, де $R_{\text{вих}}$ – потужність сигналу виходу, $R_{\text{нав}}$ – потужність наведеного сигналу.

Чим менше значення NEXТ, тим краще кабель. Так, для витої пари категорії 5 показник NEXТ повинен бути меншим -27 дБ на частоті 100 мгц.

Показник NEXТ звичайно використовується стосовно кабелю, що складається з декількох витих пар, оскільки в цьому випадку взаємні наведення однієї пари на іншу можуть досягати значних величин. Для одинарного коаксіального кабелю (тобто складається з однієї екранованої жили) цей показник не має сенсу, а для подвійного коаксіального кабелю він також не застосовується унаслідок високого ступеня захищеності кожної жили. Оптичні волокна також не створюють скільки-небудь помітних перешкод один для одного.

У зв'язку з тим, що в деяких нових технологіях використовується передача даних одночасно по декількох витих парах, останнім часом став

застосовуватися показник PowerSUM, що є модифікацією показника NEXT. Цей показник відображає сумарну потужність перехресних наведень від всіх передаючих пар в кабелі.

Достовірність передачі даних характеризує вірогідність спотворення для кожного передаваного біта даних. Іноді цей же показник називають інтенсивністю бітових помилок (Bit Error Rate, BER). Величина BER для каналів зв'язку без додаткових засобів захисту від помилок (наприклад, кодів, що самокоректуються, або протоколів з повторною передачею спотворених кадрів) складає, як правило, 10^{-4} - 10^{-6} , в оптоволоконних лініях зв'язку – 10^{-9} . Значення достовірності передачі даних, наприклад, в 10^{-4} говорить про те, що в середньому з 10 000 біт спотворюється значення одного біта.

Спотворення біт відбуваються як через наявність перешкод на лінії, так і внаслідок спотворень форми сигналу обмеженою смугою пропускання лінії. Тому для підвищення достовірності передаваних даних потрібно підвищувати ступінь перешкодозахисної лінії, знижувати рівень перехресних наведень в кабелі, а також використовувати більш широкосмугові лінії зв'язку.

4.5. Цифрові сигнали

4.5.1 Загальні характеристики

На додаток до існування представленого аналоговим каналом, дані також можуть бути представлені цифровим сигналом. Наприклад, 1 може кодуватися як позитивна напруга і 0 як нульова напруга (рис. 4.27).

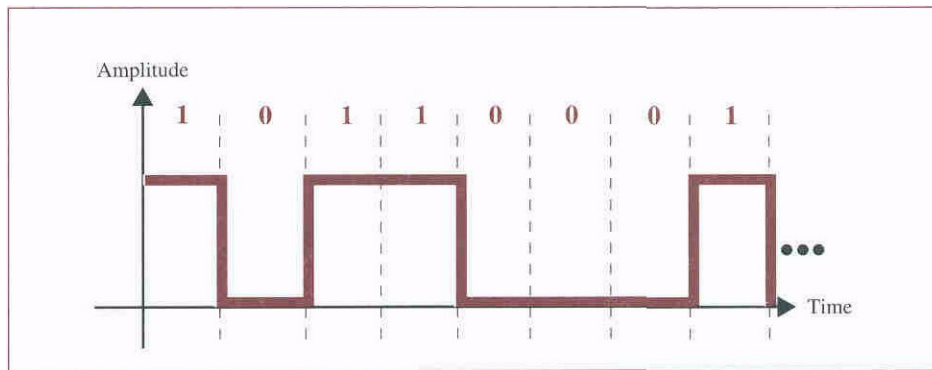


Рис. 4.27 Цифровий сигнал

Інтервал біта і швидкість передачі в бітах

Цифрові сигнали даних є неперіодичними і, тому, період або частота не є відповідними. Дві нові умови, інтервал (за винятком періоду) біта і коефіцієнт (за винятком частоти) збігу використовуються, щоб описати цифрові сигнали даних. Інтервал біта – час, що вимагається для послання одного єдиного шматка. Швидкість передачі в бітах – число інтервалів бітів за секунду. Це означає, що швидкість передачі в бітах – число бітів, посланих за одну секунду, звичайно виражається в бітах за секунду (bps). Рис. 4.28.

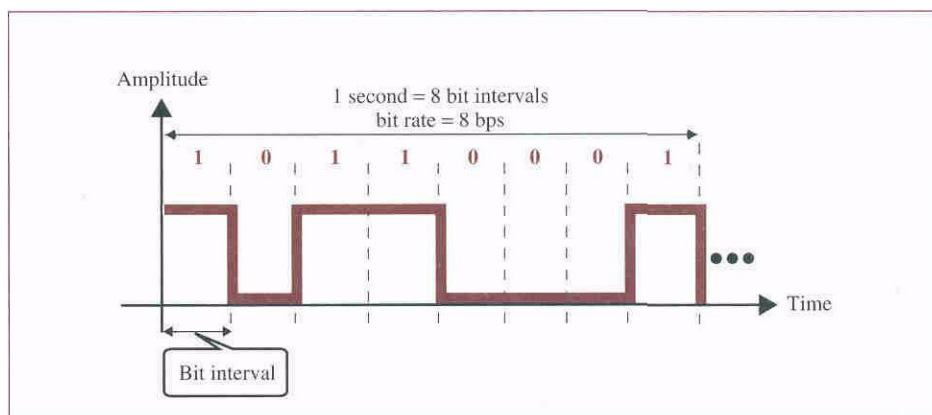


Рис. 4.28. Швидкість передачі в бітах та інтервал бітів

Приклад 4.10

Цифровий сигнал має норму 2000 bps. Якою є тривалість кожного біту (інтервал бітів)?

Рішення

Інтервал бітів – протилежність швидкості передачі в бітах.

$$\text{біт interval} = 1/(\text{bit rate}) = 1/2000 = 0.000500 \text{ секунд} = 500 \times 10^{-6} \text{ секунд} = 500 \mu\text{s}$$

Приклад 4.11

Цифровий сигнал даних має бітовий інтервал 40 мікросекунд. Яка швидкість в бітах?

Рішення

Норма бітів – протилежна до бітового інтервалу.

$$\begin{aligned} \text{bit rate} &= 1/(\text{біт інтервал}) = 1/(40 \times 10^{-6}) = 25.000 \text{ біт за секунду} = \\ &25 \times 10^3 \text{ біт за секунду} = 25 \text{ Kbps} \end{aligned}$$

4.5.2 Декомпозиція цифрового сигналу

Цифровий сигнал даних може бути розбитий на нескінченну кількість простих хвиль синуса викликаний гармоніками, кожна з іншою амплітудою, частотою, і фазою (рис. 4.29). Це означає, що коли ми посилаємо цифровий сигнал даних уздовж засобу передачі, ми посилаємо нескінченну кількість простих сигналів. Щоб одержати точну копію цифрового сигналу даних всі частотні компоненти повинні бути вірно перенесений через засіб передачі. Коли деякі з компонентів не проходяться через засіб, сигнал в одержувачі спотворюється як результат. Оскільки ніякий засіб на практиці (наприклад кабель) не є здатним до перенесення повного ряду частот, ми завжди маємо спотворення.

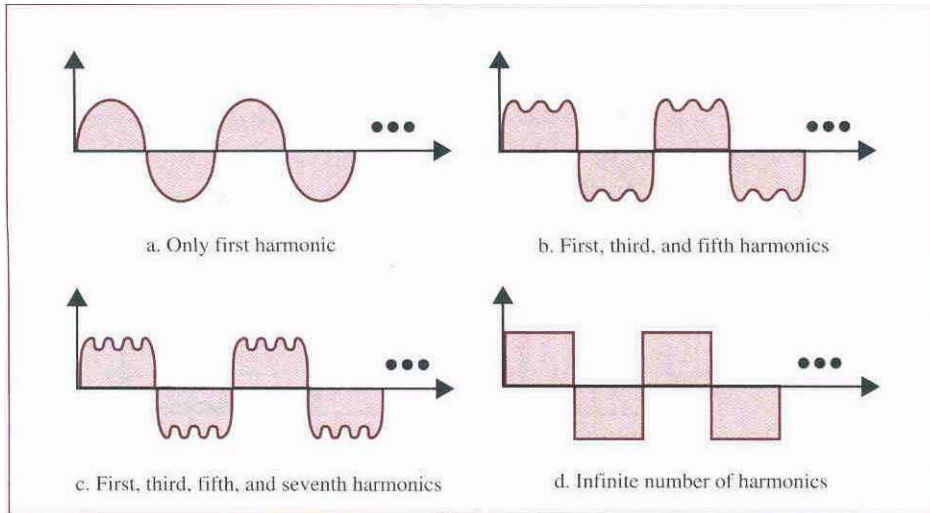


Рис. 4.29. Гармоніки цифрового сигналу даних

Незважаючи на те, що частотний спектр цифрового сигналу даних містить нескінченну кількість частот з різними амплітудами, якщо ми посилаємо тільки ті компоненти чиї амплітуди є істотними (над прийнятним порогом), ми можемо дистилювати цифровий сигнал даних з розумною точністю в одержувачі (мінімальне спотворення). Ми викликаємо цю частину нескінченного спектру істотний спектр, і смугу пропускання (рис. 4.30).

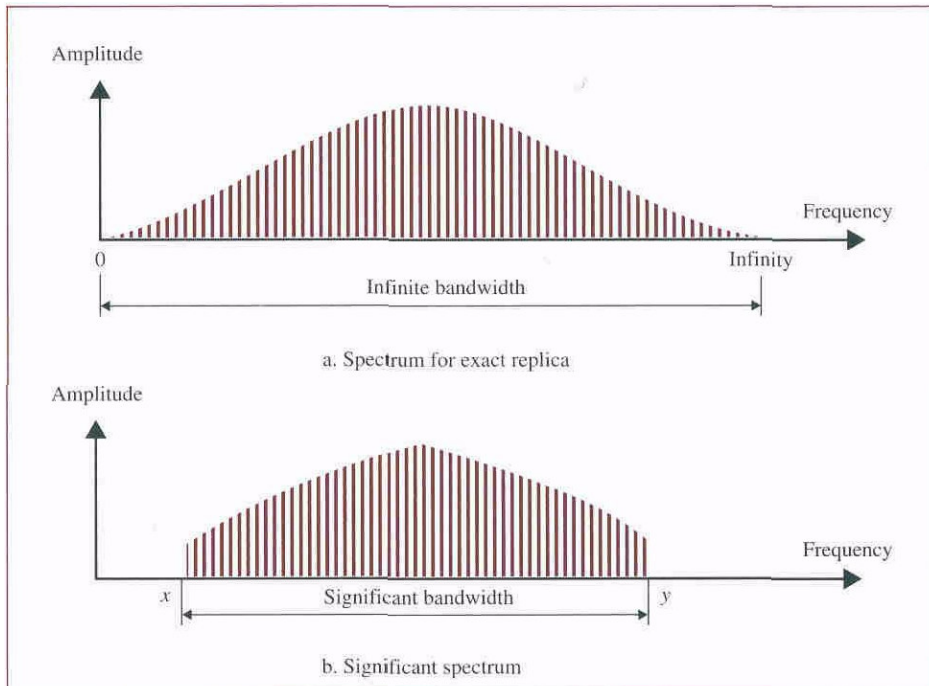


Рис. 4.30. Точний та істотний спектруми

Тема 5. Кодування і модуляція

- 5.1. Загальні відомості про методи перетворення сигналів
- 5.2. Цифрове кодування
- 5.3. Аналого – цифрове перетворення
- 5.4. Цифро – аналогове перетворення
- 5.5. Аналогова модуляція

Література

1. Forouzan
2. Таненбаум
3. Оліфер

5.1. Загальні відомості про методи перетворення сигналів

Як говорилося раніше, інформація повинна бути перетворена в сигнал перед тим, як її передають через лінії зв'язку.

Як перетворюють інформацію – залежить від первинного формату і формату, який використовується апаратними засобами зв'язку.

Простий сигнал сам собою не несе більше інформації і більше, ніж пряма строчка супроводжує слова. Сигналом потрібно маніпулювати так, щоб він містив невизначені зміни, які можуть розпізнати і відправник і приймач, як того вимагає представлення інформації. Спершу інформація повинна бути трансформована в погоджений набір нулів та одиниць, наприклад, використовуючи Американський Стандартний Код для Обміну Інформацією American Standard Code for Information Interchange (ASCII).

Дані зберігаються в комп'ютері у вигляді нулів та одиниць. Щоб бути перенесеним з одного місця в інше (всередині або за межами комп'ютера), дані звичайно перетворюються в цифрові сигнали. Це називається цифро-

цифровим перетворенням або кодуванням цифрових даних в цифровий сигнал.

Інколи потрібно перетворити аналоговий сигнал (як наприклад голос в телефонній розмові) на цифровий сигнал, наприклад, щоб зменшити вплив завад. Це називається аналогово-цифровим перетворенням або перетворенням аналогового сигналу в цифрову форму.

Часом інший, ми хочемо послати цифровий сигнал з комп'ютера через носій, розроблений для аналогового каналу. Наприклад, щоб послати дані з одного місця до іншого з використанням телефонної лінії, цифровий сигнал комп'ютера, повинен бути перетворений в аналоговий сигнал. Це називається цифро-аналоговим перетворенням або модулюванням цифрового сигналу.

Часто аналоговий канал посилається на велику відстань з використанням аналогового носія. Наприклад, голос або музика з радіостанції, які є аналоговим сигналом, передається в ефірі. Однак, частота голосу або музики не є придатною для цього виду передачі; сигнал повинен бути перенесений за допомогою вищого частотного сигналу. Це називається аналого-аналоговим перетворенням або модулюванням аналогового сигналу.

На рис. 5.1 показано ці чотири методи різних перетворень.

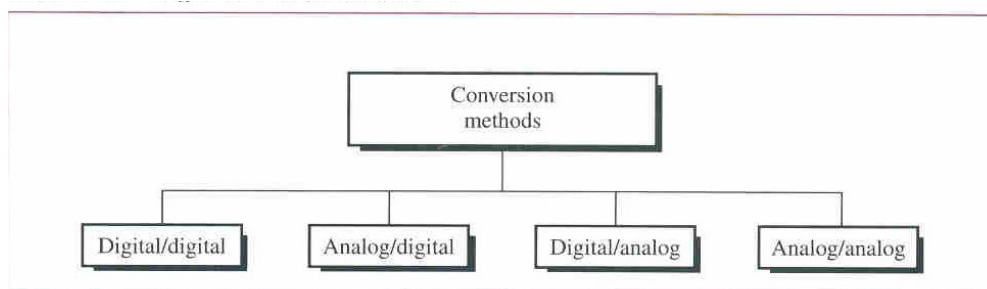


Рис. 5.1 Схеми різних перетворень

Цифрово-цифрове перетворення

Цифрово-цифрове кодування або перетворення є відображення цифрової інформації за допомогою цифрового сигналу. Наприклад, коли ви

передаєте дані з вашого комп'ютера до принтера, як первинні дані, так і передані – є цифровими. При цьому типі кодування, двійкові нулі та одиниці згенеровані за допомогою комп'ютера перетворюються на послідовність імпульсів напруги, які можуть бути передані по шині. На рис. 5.2 показано зв'язок між цифровою інформацією, цифрово-цифрові засоби кодування, і результуючий цифровий сигнал.

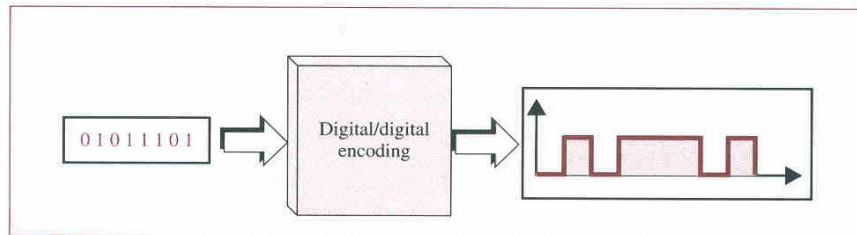


Рис. 5.2. Цифрово-цифрове кодування.

З багатьох пристроїв для цифрово-цифрового кодування, ми обговоримо тільки найбільш корисні для передачі даних. Вони попадають в три широкі категорії: однополярні, полярні та двополюсні.

Однополярне кодування є простим з використанням тільки однієї методики. Полярне кодування має три підкатегорії, NRZ, RZ, і двофазове (biphase), два з яких мають багато різновидів. Третя опція, двополюсне кодування, має три різновиди: AMI, B8ZS, і HDB3.

Методи передачі дискретних даних на фізичному рівні

При передачі дискретних даних по каналах зв'язку застосовуються два основних типи фізичного кодування – на основі синусоїдального несучого сигналу і на основі послідовності прямокутних імпульсів. Перший спосіб часто називається також модуляцією чи аналоговою модуляцією, підкреслюючи той факт, що кодування здійснюється за рахунок зміни параметрів аналогового сигналу. Другий спосіб звичайно називають цифровим кодуванням. Ці способи відрізняються шириною спектру

результуючого сигналу і складністю апаратури, необхідної для їхньої реалізації.

При використанні прямокутних імпульсів спектр результуючого сигналу виходить дуже широким. Це не дивно, якщо згадати, що спектр ідеального імпульсу має нескінченну ширину. Застосування синусоїди приводить до спектру набагато меншої ширини при тій же швидкості передачі інформації. Однак для реалізації синусоїдальної модуляції потрібна складніша і дорожча апаратура, ніж для реалізації прямокутних імпульсів.

В даний час дані, що початково мають аналогову форму – мова, телевізійне зображення – передаються каналами зв'язку в дискретному вигляді, тобто у вигляді послідовності одиниць і нулів. Процес представлення аналогової інформації в дискретній формі називається дискретною модуляцією. Терміни “модуляція” і “кодування” часто використовують як синоніми.

Аналогова модуляція

Аналогова модуляція застосовується для передачі дискретних даних каналами з вузькою смугою частот, типовим представником яких є канал тональної частоти, наданий у розпорядження користувачам телефонних мереж. Цей канал передає частоти в діапазоні від 300 до 3400 Гц, таким чином, його смуга пропускання дорівнює 3100 Гц. Хоча людський голос має набагато ширший спектр – приблизно від 100 Гц до 10 кгц – для прийнятної якості передачі мови діапазон у 3100 Гц є гарним рішенням. Строге обмеження смуги пропускання тонального каналу зв'язано з використанням апаратури ущільнення і комутації каналів у телефонних мережах.

5.2. Цифрове кодування

Однополярне (Unipolar)

Однополярне кодування є дуже простим і примітивним. Хоча його майже не використовують сьогодні, простота забезпечує легкий вступ до принципів, які розробляються із складнішими системами кодування і дозволяє нам дослідити тип проблеми, які будь-яка цифрова передавальна система повинна подолати.

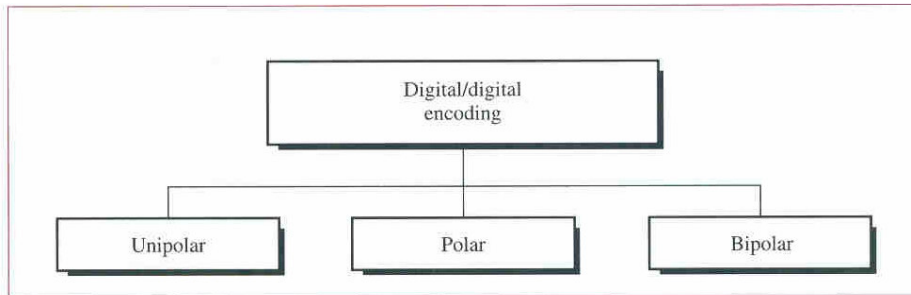


Рис. 5.3. Типи цифрово-цифрового кодування

Цифрові передавальні системи працюють за допомогою посилення імпульсів напруги вздовж засобу зв'язку, звичайно шини або кабелю. У більшості типів кодування, один рівень напруги встановлюється для двійкового 0 і другий рівень для двійкової 1. Полярність імпульсу означає, чи він є позитивним або негативним. Однополярним кодування називається через те, що використовує тільки одну полярність. Ця полярність присвоюється одному з двох двійкових рівнів, звичайно 1. Інший встановлюють, звичайно на 0 і він представляється за допомогою нульової напруги.

На рис. 5.4 показано ідею однополярного кодування. У цьому прикладі одиниці кодуються як позитивне значення і нулі кодуються, як нульове значення. На додаток можна сказати відверто, що однополярне кодування є недорогим для впровадження.

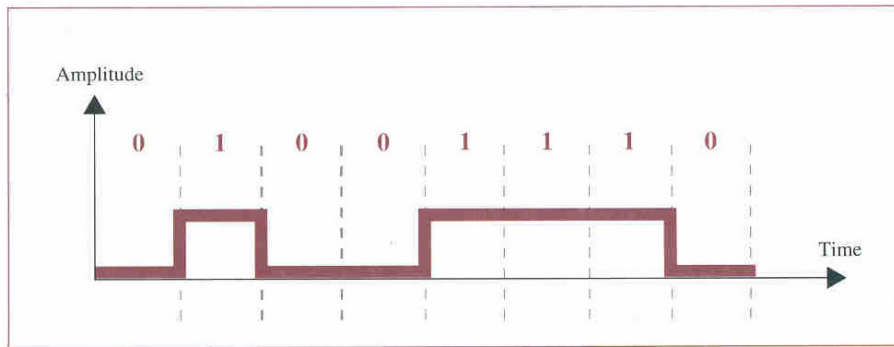


Рис. 5.4. Однополярне кодування

Однак, однополярне кодування має щонайменше дві проблеми, які зменшують його привабливість: компоненту DC і синхронізацію.

Компонента DC

Середня амплітуда індексованого однополярного сигналу є ненульовою. Це створює те, що називається компонентою постійного струму (DC) (компонент з нульовою частотою). Коли сигнал містить компоненту DC, її не можна передавати через носій, який не може підтримувати компоненти DC.

Синхронізація

Коли сигнал незмінний, приймач не може визначити початок і закінчення кожного біта. Таким чином, проблема синхронізації в однополярному кодуванні може траплятися кожного разу, коли потік даних включає велику безперервну серію одиниць або нулів. Цифрові схеми кодування використовують зміни в рівні напруги, щоб вказати на зміни в бітовому типі. Сигнальна зміна також вказує, що один біт закінчився і новий біт почався. В однополярному кодуванні, однак, серія одного виду біта, скажімо сім одиниць, відбувається не із змінами напруги, тільки нерозбита позитивна напруга, яка триває у сім разів довше ніж один одиничний біт. Поки немає зміни сигналу, щоб вказати на запуск наступного біта один за

одним, приймач залежить від таймера. Дається очікувана бітова швидкість 1000 bps, якщо приймач виявляє позитивну напругу, яка триває 0.005 секунди, він читає одну одиничку за 0.001 секунди, або п'ять 1 за секунду.

На жаль, відсутність синхронізації між відправником і таймерами приймача спотворює узгодження в часі сигналу, так, що, наприклад, п'ять одиничок може бути розтягнуто до 0.006 секунди, примушуючи приймач читати один додатковий біт. Цей один додатковий біт в потоці даних викликає після цього помилку в дешифруванні. Рішення, яке розробляється, щоб контролювати синхронізацію однополярної передачі – використовувати окрему паралельну лінію, що переносить синхронізуючий сигнал і дозволяє отримуючому пристрою розсинхронізувати таймер до того сигналу. Але дублювання кількості ліній, які використовуються для передачі збільшує вартість і стає неекономним.

Полярне

Полярне кодування використовує два рівні напруги: один позитивний і один негативний. За допомогою використання обох рівнів, в найбільш полярних методах кодування середній рівень напруги на лінії зменшується, і проблема компоненти DC однополярного кодування зменшується. У манчестерському і різницево-манчестерському коді, кожний біт складається як з позитивних, так і негативних напруг, так що компонента DC повністю ліквідується.

Із багатьох існуючих відхилень полярного кодування, ми дослідимо тільки три найбільш популярних: не повернення до нуля (NRZ), повернення до нуля (RZ), і двофазове (biphase). Кодування NRZ включає два методи: не повернення до нуля, рівневе (NRZ-L), і не повернення до нуля, інвертоване (NRZ-I). Двофазове також розпадається на два методи. По-перше, манчестерський метод використовується за допомогою ЛОМ Ethernet.

Другий різницевий манчестерський метод використовується за допомогою ЛОМ Token Ring (рис. 5.5).

Не повернення до Нуля (NRZ)

У кодуванні NRZ, рівень сигналу є завжди або позитивним або від'ємним. Нижче обговорюються два найбільш популярні методи передачі NRZ.

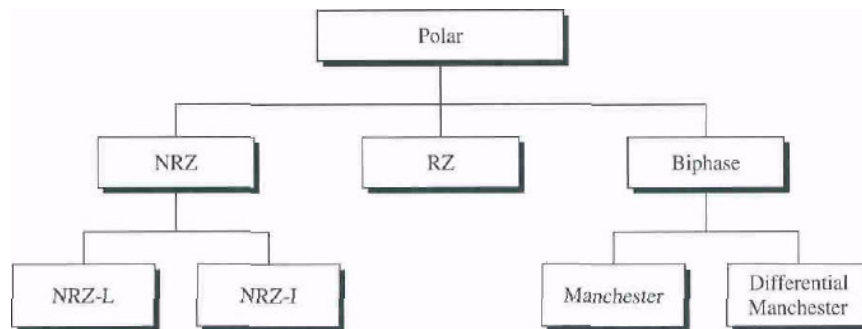


Рис. 5.5. Типи полярного кодування

В кодуванні NRZ-L, рівень сигналу залежить від типу біта, який його представляє. Позитивна напруга звичайно означає, що біт є 0, а від'ємна напруга означає, що біт є 1 (або навпаки); таким чином, рівень сигналу залежить від стану біта.

Проблема може з'явитися, коли є великий потік 0 або 1 в даних. Приймач отримує безперервну напругу і повинний визначити за допомогою таймера, скільки бітів посилається, і таймер може синхронізуватися або не синхронізуватися з таймером відправника.

Всередині NRZ-I, інверсія рівня напруги представляє 1 біт. Це є перехід між позитивною і негативною напругою, власне не напругою безпосередньо, а тим, що представляє 1 біт. 0 Біт представляється не за допомогою зміни. NRZ-I є вищим від NRZ-L завдяки синхронізації, що забезпечується за допомогою зміни сигналу кожний раз, коли зустрічається 1 біт. Існування одиниць в потоці даних дозволяє приймачу розсинхронізувати таймер до

фактичного надходження передачі. Рядок нулів може викликати проблеми, але, через те, що нулі не є такий же ймовірний, вони спричиняють меншу проблему.

На рис. 5.6 показує NRZ-L і NRZ-I із зображенням тієї ж серії бітів. У послідовності NRZ-L, позитивні і від'ємні напруги мають специфічні значення: позитивні для 0 і від'ємні для 1. В послідовності NRZ-I напруга за секунду є безглуздою. Замість цього, приймач шукає зміни від одного рівня до іншого на основі розпізнавання одиниць.

Повернення до нуля (RZ)

Оскільки часом первинні дані містять рядки послідовних нулів або одиниць, приймач може втратити позицію. Оскільки ми згадали в нашому обговоренні однополярного кодування, один шлях підтвердити синхронізацію – послати окремий сигнал узгодження в часі окремим каналом. Однак, рішенняє як дорогим, так і схильним до власної помилки. Кращий розв'язок – як-небудь включати синхронізацію в індексований сигнал, трохи схоже на рішення, забезпеченого за допомогою NRZ-I, але, здатний до обробки як стрічок нулів, так і одиниць.

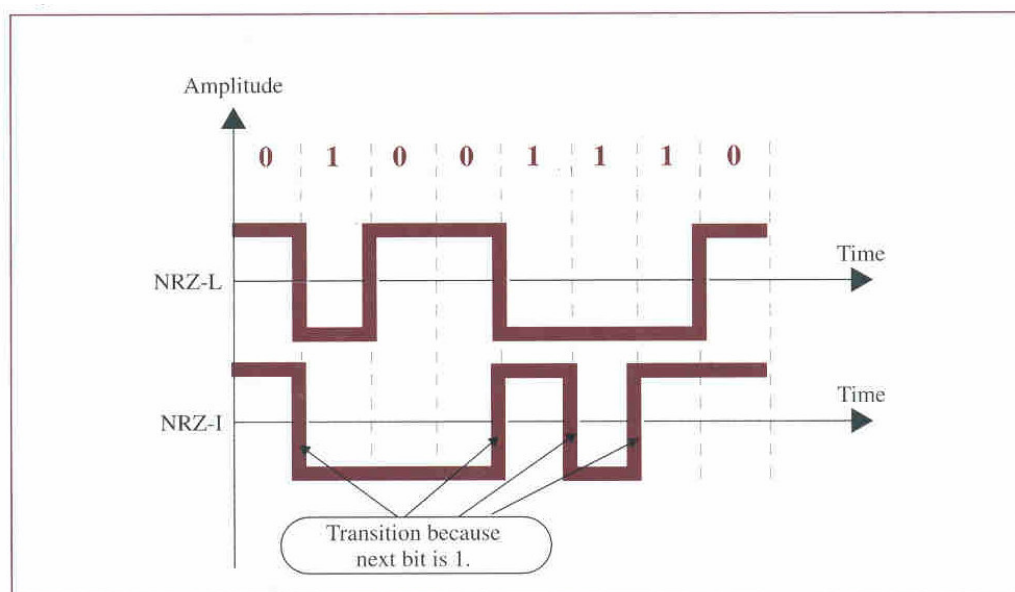


Рис. 5.6. Кодування NRZ-L і NRZ-I

Щоб виконати синхронізацію, повинна бути зміна сигналу для кожного біта. Приймач може використовувати ці зміни, щоб створювати, змінювати, і синхронізувати таймер. Як було видно вище, NRZ-I виконує це для послідовностей одиниць. Але, щоб змінюватися з кожним бітом, нам потрібно більше, ніж тільки два значення. Одне рішення є кодуванням з поверненням до нуля (RZ), який використовує три значення: позитивне, негативне і нуль. У RZ сигнал обмінюється не між бітами, але протягом кожного біта. Подібно NRZ-L, позитивна напруга означає 1 і від'ємні напруга означає 0. Але, на відміну від NRZ-L, на півдорозі через кожний бітовий інтервал, сигнал повертається до нуля. 1 біт дійсно представляється за допомогою позитивного до нуля і 0 біт він негативного до нуля, швидше, ніж за допомогою тільки позитивного або негативного. На рис. 5.7 показано принцип.

Головний недолік кодування RZ є те, це вимагає, щоб дві зміни сигналу кодували один біт і таким чином займає більшу смугу пропускання. Але три альтернативи досліджені раніше показують його найбільшу ефективність.

Двофазове

Можливо найкращим існуючим розв'язком проблеми синхронізації є двофазове кодування. У цьому методі сигналу міняється в середині бітового інтервалу, але не повертається до нуля. Замість того, це продовжується до розташованого на протилежному боці полюса. Як в RZ, ці переходи через середину інтервалу дозволяють синхронізацію.

Як згадувалось раніше, є два типи двофазового кодування, які використовуються у мережах сьогодні: манчестерський і різницевий манчестерський.

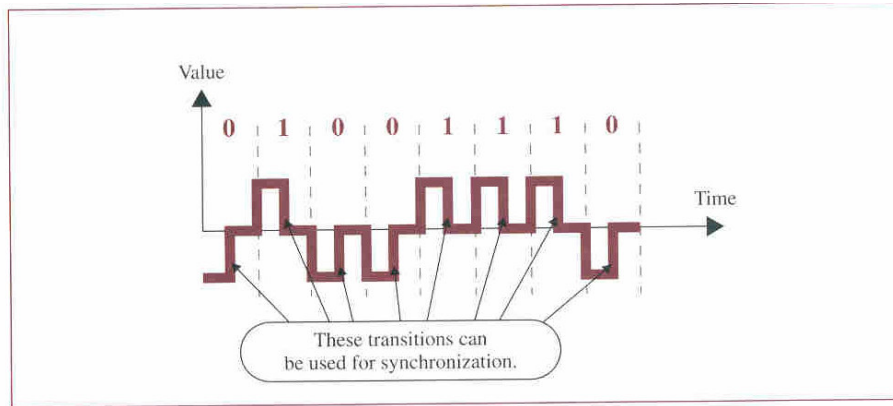


Рис. 5.7. Кодування RZ

Манчестерське кодування використовує інверсію в середині кожного бітового інтервалу як для синхронізації, так і відображення бітів. Перехід від негативного до позитивного представляє двійкову 1 і перехід від позитивного до негативного представляє двійковий 0. За допомогою використання поодинокого переходу для подвійної цілі, манчестерське кодування досягає того ж рівня синхронізації, що і RZ, але з єдиними двома рівнями амплітуди.

У різницевому манчестерському, інверсія в середині бітового інтервалу використовується для синхронізації, але наявність або відсутність додаткового переходу на початку інтервалу використовується для ідентифікації біту. Перехід означає, що двійковий 0 і жодний перехід не означає двійкової 1. різницевий манчестерський потребує, щоб дві зміни сигналу для представлення двійкового 0, але тільки один, щоб представити двійкову 1.

На рис. 5.8 показано манчестерські і різницеві манчестерські сигнали для того ж двійкового коду.

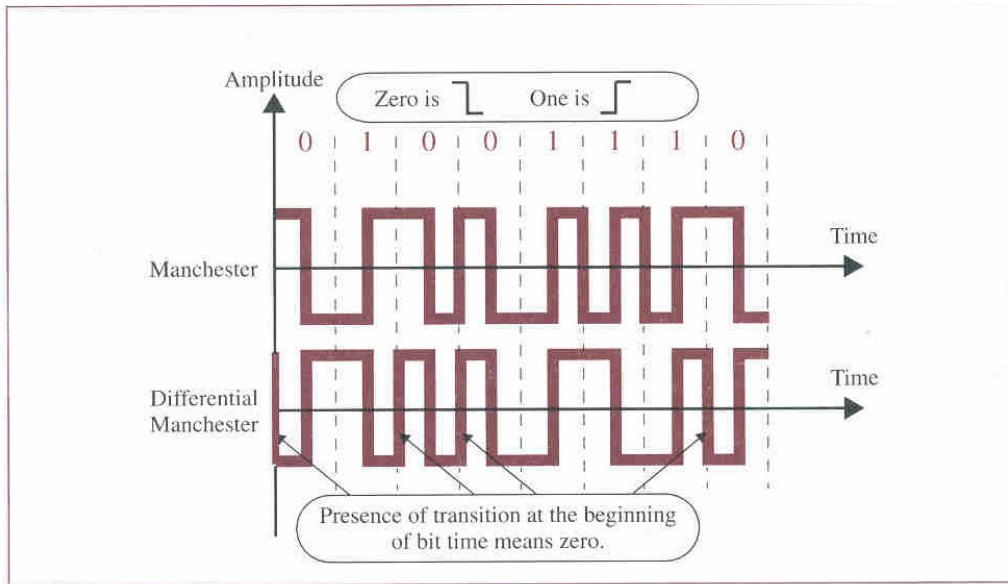


Рис. 5.8. Манчестерське і різницеве манчестерський кодування

Двополюсне

Двополюсне кодування, подібно RZ, використовує три рівні напруги: позитивний, негативний і нуль. На відміну від RZ, однак, нульовий рівень в двополюсному кодуванні використовується, щоб представити двійковий 0.

Одиниці представляються за допомогою змінених позитивних і негативних напруг. Якщо перший біт одиниці представляється за допомогою позитивної амплітуди, другий буде представлений за допомогою негативної амплітуди, третій за допомогою позитивної амплітуди, і так далі. Це чергування відбувається, навіть коли одиничні біти не є послідовними.

Три типи двополюсного кодування часто використовуються в промисловій передачі даних: AMI, B8ZS, і HDB3 (рис. 5.9).

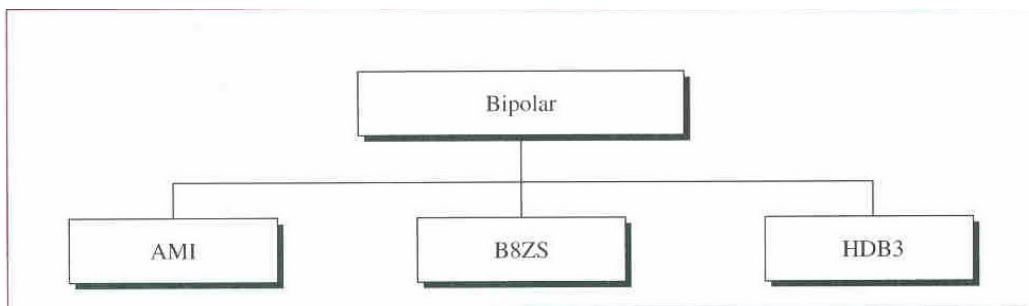


Рис. 5.9 Типи двополюсного кодування

Двополюсна Змінна Інверсія Мітки (АМІ)

Двополюсна інверсія змінної мітки (АМІ) є найпростішим типом двополюсного кодування. У назві “інверсії змінної мітки”, слово “мітка” прийшло з телеграфії і означає 1. Так що АМІ означає альтернативну інверсію 1. Нейтральна, нульова напруга представляє двійковий 0. Двійкові одиниці представляються за допомогою змінених позитивних і негативних напруг. На рис. 5.10 наведено приклад.

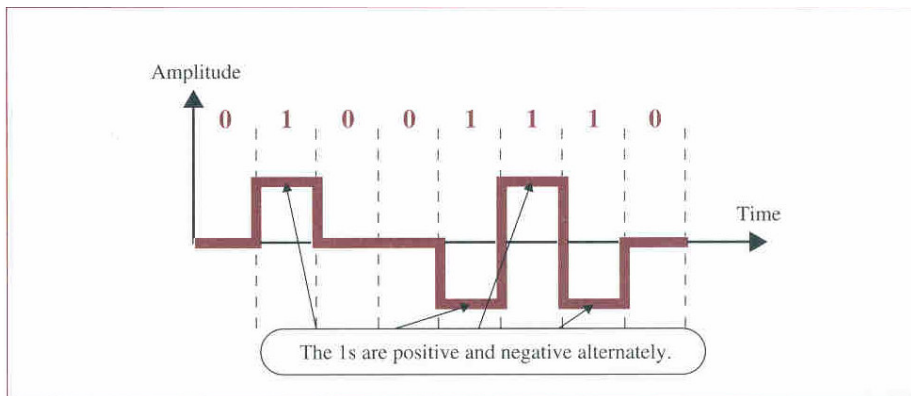


Рис. 5.10 Двополюсне кодування АМІ

Відхилення двополюсного АМІ називається псевдотрійковим, в якому двійковий 0 міняється між позитивними і від’ємними напругами.

За допомогою інверсії на кожному входженні 1, двополюсне АМІ виконує дві речі: по-перше, компонент DC є нульовим, і по-друге, довга послідовність одиниць залишається синхронізованою. Немає механізму гарантії синхронізації довгої стрічки нулів.

Два відхилення двополюсного АМІ були розроблені, щоб вирішити проблему синхронізації послідовних нулів, особливо для віддаленої передачі. Перше використовується в Північній Америці і називається двополюсна 8-нульова заміна (BSZS). Друга використовується в Європі і Японії і називається двополюсною 3 з високою щільністю розміщення (HDB3).

Обидва є застосуванням двополюсного АМІ, що змінюють первинний зразок тільки у випадку багатократної послідовності нулів.

Двополюсна 8-Нульова Заміна (B8ZS)

B8ZS прийнято в Північній Америці, щоб забезпечити синхронізацію довгих рядків нулів. У більшості ситуацій, B8ZS функціонує ідентично до двополюсного АМІ. Двополюсний АМІ змінює полюси з кожною 1, яка зустрічається. Ці зміни забезпечують синхронізацію, потрібну за допомогою приймача. Але сигнал не змінюється протягом рядка нулів, так що синхронізація часто втрачається.

Різниця між B8ZS і двополюсним АМІ відбувається кожного разу коли вісім або більше послідовних нулів зустрічаються в потоці даних. Розв'язок, забезпечений за допомогою B8ZS – спричинити штучні зміни сигналу, які називають порушеннями в стрічці нулів. Завжди, коли вісім нулів трапляються підряд, B8ZS представляє зміни в зразку, основані на полярності попередньої 1 (1 була якраз перед нулями). (Рис. 5.11.).

Якщо попередній 1 біт був позитивний, вісім нулів кодуватимуться, як нуль, нуль, нуль, позитивний, негативний, нуль, негативний, позитивний. Слід пам'ятати, що приймач шукає змінну полярність, щоб ідентифікувати 1. Коли він знаходить дві послідовних позитивних зміни оточені трьома нулями, він розпізнає зразок, як свідомо представлене і непомилкове протиріччя. Потім він шукає другу пара очікуваних протиріч. Коли він знаходить їх, приймач перетворює всі вісім бітів на нулі і повертається назад до нормального двополюсного режиму АМІ.

Якщо полярність попередньої 1 є негативною, відображення протиріч є тим же, але з оберненою полярністю. Як позитивні, так і негативні зразки показані на рис. 5.11.

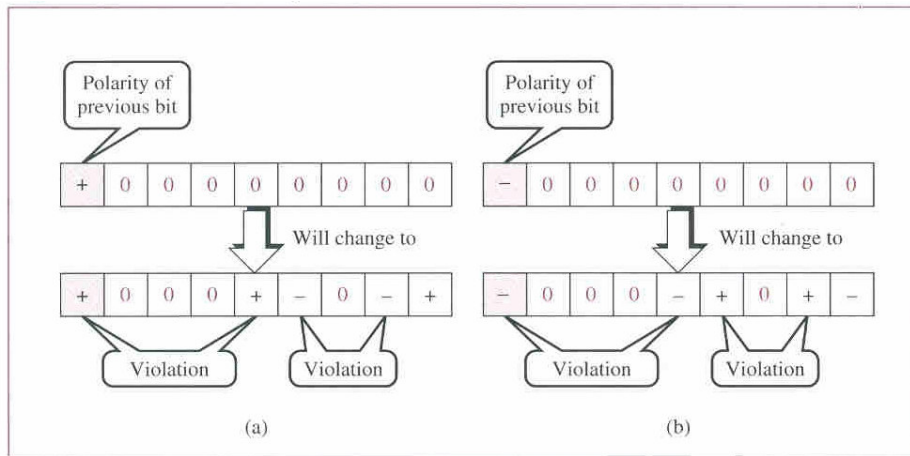


Рис. 5.11 B8ZS кодування

Двополюсний 3 з високою щільністю (HDB3)

Проблема синхронізації рядків послідовних нулів в Європі і Японії розв'язується по іншому, ніж в Сполучених Штатах. Ця конвенція з назвою HDB3 представляє зміни в двополюсному зразку АМІ кожного разу, коли зустрічаються з чотирма послідовним нулями замість очікування восьми, які потрібні у B8ZS в Північній Америці. Хоч назвою є HDB3, зразок міняється кожен раз коли є чотири нулі підряд (рис. 5.12).

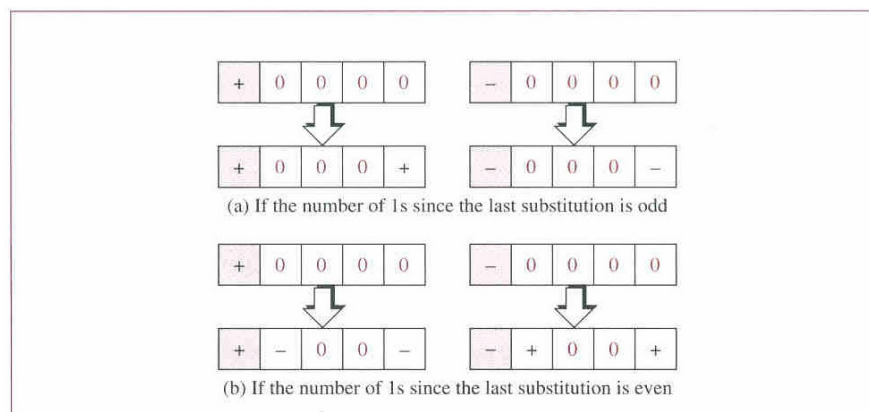


Рис. 5.12 Кодування HDB3

Як в B8ZS, зображення збудження в HDB3 базується на полярності попереднього 1 біта. Але на відміну від B8ZS. HDB3 також розглядає кількість одиниць, що відбулися в бітовому потоці після останньої заміни.

Кожного разу, коли кількість одиниць з часу останньої заміни є непарною, НОВЗ поміщає збудження замість чотирьох послідовних 0. Якщо полярність попередніх бітів була позитивною, збудження є позитивним. Якщо полярність попередніх бітів була негативна, збудження є негативним.

Кожного разу, коли кількість 1 з часу останньої заміни є рівномірною, НОВЗ поміщає збудження в позиціях як початку, так і чотирьох послідовних нулів. Якщо полярність попереднього біта була позитивна, обидва збудження є негативними. Якщо полярність попереднього біта була негативна, обидва збудження є позитивними. Всі чотири зразки показані на рис. 5.12.

Як ви можете бачити, ідея – порушити стандартний зразок шляхами, які машина може визнати, як навмисний, і, щоб використовувати ті збудження, щоб синхронізувати систему.

Приклад 5.1

Використання В8ZS, кодують бітовий потік 10000000000100. припустимо, що полярність першої 1 є позитивною.

Розв'язок

Див. рис. 5.13.

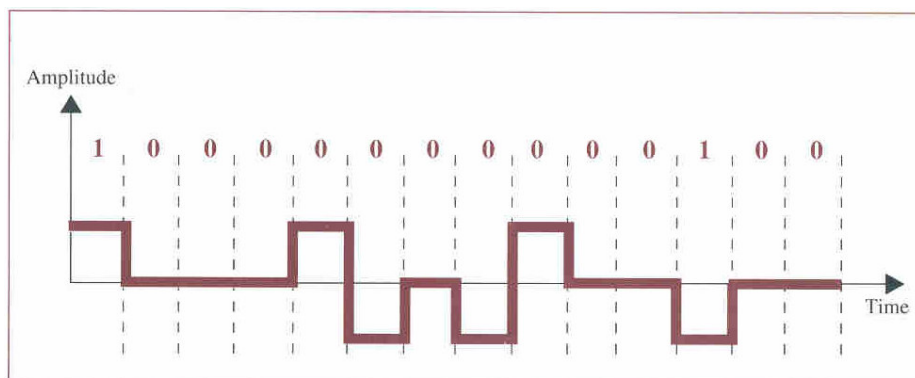


Рис. 5.13. Розв'язок прикладу 5.1

Приклад 5.2

Використовуючи HDB3, декодуйте бітовий потік 10000000000100.
Припустимо, що кількість одиниць є непарною і перша 1 є позитивною.

Розв'язок

Див. Рис. 5.14.

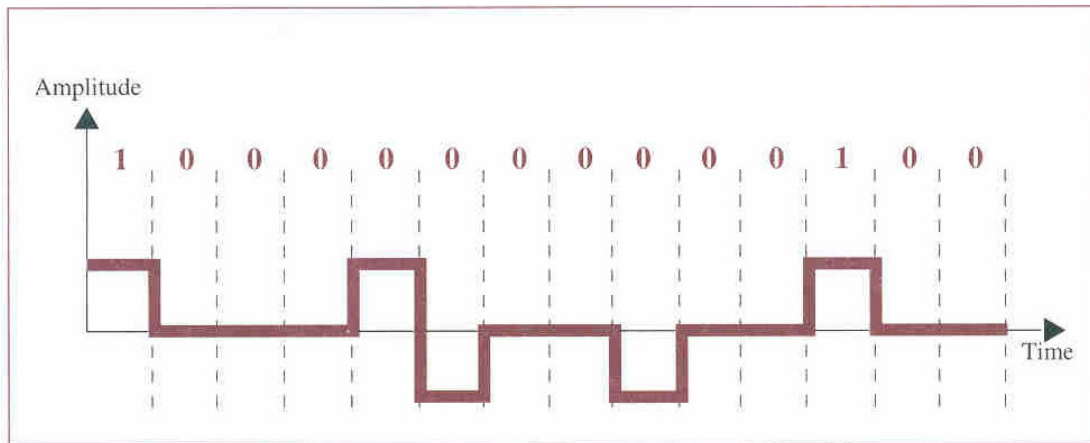


Рис. 5.14. рішення прикладу 5.2

Манчестерський код

В жодній з версій Ethernet не застосовується пряме двійкове кодування біта 0 напругою в 1В і біта 1 – напругою 5В, тому що такий спосіб приводить до неоднозначності. Якщо одна станція посилає бітовий рядок 00010000, то інша може інтерпретувати її як 10000000 чи 01000000, тому що вони не зможуть відрізнити відсутність сигналу (0В) від біта 0 (0В). Можна, звичайно, кодувати одиницю позитивною напругою +1В, а нуль – негативною напругою -1В. Але при цьому все одно виникає проблема, зв'язана із синхронізацією передавача і приймача. Різні частоти роботи їхніх системних таймерів можуть привести до розсинхронізації і невірної інтерпретації даних. У результаті приймач може втратити границю бітового інтервалу. Особливо велика ймовірність цього у випадку довгої послідовності нулів чи одиниць.

Таким чином, машині що приймає потрібний спосіб однозначного визначення початку, кінця і середини кожного біта без допомоги зовнішнього

таймера. Це реалізується за допомогою двох методів: манчестерського кодування і різницевого манчестерського кодування. У манчестерському коді кожен часовий інтервал передачі одного біта поділяється на два рівних періоди. Біт зі значенням 1 кодується високим рівнем напруги в першій половині інтервалу і низьким у другій половині, а нульовий біт кодується зворотною послідовністю – спочатку низька напруга, потім висока. Така схема гарантує зміну напруги в середині періоду бітів, що дозволяє приймачу синхронізуватися з передавачем. Недоліком манчестерського кодування є те, що воно вимагає подвійної пропускну здатності лінії стосовно прямого двійкового кодування, тому що імпульси мають половинну ширину. Наприклад, для того щоб відправляти дані зі швидкістю 10 Мбіт/с, необхідно змінювати сигнал 20 мільйонів разів на секунду. Манчестерське кодування показане на мал. 5.15, б.

Різницеве манчестерське кодування, показане на рис. 5.15, в, є варіантом основного манчестерського кодування. У ньому біт 0 кодується зміною стану на початку інтервалу, а біт 1 збереженням попереднього рівня. В обох випадках у середині інтервалу обов'язково присутній перехід. Різницева схема вимагає більш складного устаткування, зате має добрий захист від шуму. В усіх мережах Ethernet використовується манчестерське кодування завдяки його простоті. Високий сигнал кодується напругою у +0,85 В, а низький сигнал -0,85 В, у результаті чого постійна складова напруги дорівнює 0 В. Різницеве манчестерське кодування а також підрівень управління доступом до середовища в Ethernet не використовується, але використовується в інших ЛОМ (наприклад, стандарт 802.5, маркерне кільце).

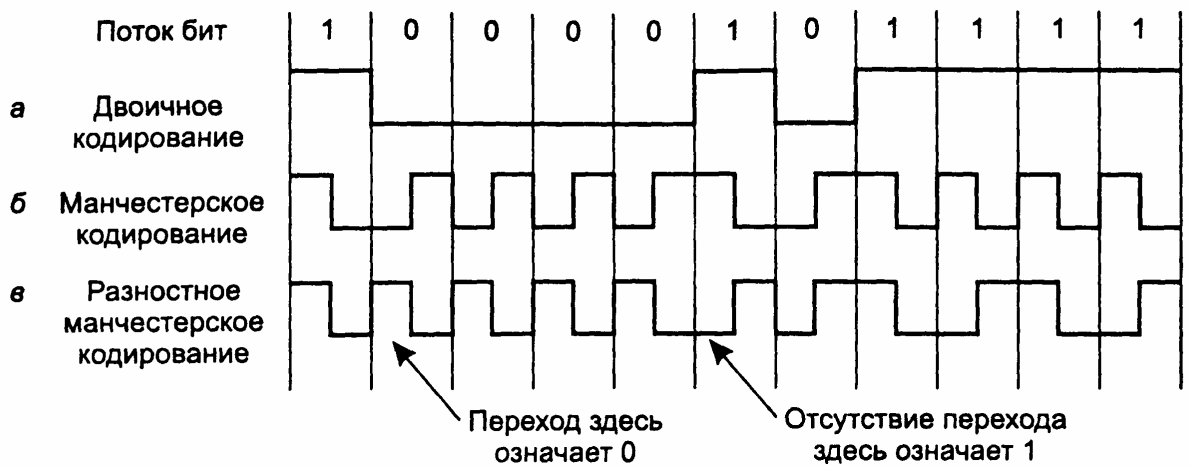


Рис. 5.15. Двійкове кодування (а); манчестерське кодування (б); різницеве манчестерське кодування (в)

Протокол підрівня управління доступом до середовища в Ethernet

Вихідна структура кадру, запропонована у свій час DIX (DEC, Intel, Xerox), показана на мал. 5.16. Кожен кадр починається з поля Preamble (преамбула, заголовок) довжиною 8 байт, яке містить послідовність 10101010. Манчестерське кодування такої послідовності бітів дає в результаті меандр із частотою 10 МГц і тривалістю 6,4 мкс, що дозволяє одержувачу синхронізувати свого таймера з таймером відправника. Далі до кінця кадру вони повинні зберігати синхронізований стан за рахунок манчестерського коду, що зберігає оцінки границь бітів.

Кадр містить дві адреси: одержувача і відправника. По стандарту дозволяються 2-байтові і 6-байтові адреси, однак параметри немодульованої передачі зі швидкістю 10 Мбіт/с передбачають тільки 6-байтові адреси. Старший біт адреси одержувача містить 0 для звичайних адрес і 1 для групових одержувачів. Групові адреси дозволяють декільком станціям приймати інформацію від одного відправника. Кадр, що відправляється груповому адресату, може бути отриманий усіма станціями, що входять у цю

групу. Такий механізм називається груповою розсилкою. Якщо адреса складається тільки з одиниць, то кадр можуть прийняти абсолютно всі станції мережі. Таким способом здійснюється широкомовлення. Різниця між груповою розсилкою і широкомовленням дуже істотна, тому варто наголосити - кадр, призначений для групової розсилки, посилається певній групі станцій Ethernet; широкомовний кадр одержують абсолютно всі станції мережі. Групова розсилка вибірковіша, але вимагає зусиль при управлінні групами. Широкомовлення - грубіша технологія, але не вимагає ніякого налаштування груп.

При амплітудній модуляції спектр складається із синусоїди несучої частоти f_c і двох бічних гармонік: $(f_c + f_t)$ і $(f_c - f_t)$ де f_t - частота зміни інформаційного параметра синусоїди, що збігається зі швидкістю передачі даних при використанні двох рівнів амплітуди (мал. 2.14, б). Частота f_t визначає пропускну здатність лінії при даному способі кодування. При невеликій частоті модуляції ширина спектра сигналу буде також невеликою (рівною $2f_t$), тому сигнали не будуть спотворюватися лінією, якщо її смуга пропускання буде чи більше дорівнює $2f_t$. Для каналу тональної частоти такий спосіб модуляції прийнятний при швидкості передачі даних не більше $3100/2=1550$ біт/с. Якщо ж для представлення даних використовуються 4 рівні амплітуди, то пропускну здатність каналу підвищується до 3100 біт/с.

При фазовій і частотній модуляції спектр сигналу виходить складнішим, чим при амплітудній модуляції, тому що бічних гармонік тут утвориться більше двох, але вони також симетрично розташовані щодо основної несучої частоти, а їх амплітуди швидко зменшуються. Тому ці види модуляції також добре підходять для передачі даних по каналу тональної частоти.

Для підвищення швидкості передачі даних використовують комбіновані методи модуляції. Найбільш розповсюдженими є методи квадратурної амплітудної модуляції (Online Amplitude Modulation, OAM). Ці

методи засновані на поєднанні фазової модуляції з 8 значеннями величин зрушення фази і амплітудної модуляції з 4 рівнями амплітуди. Однак з можливих 32 комбінацій сигналу використовуються далеко не всі. Наприклад, у кодах Трелліса припустимі всього 6, 7 чи 8 комбінацій для представлення вихідних даних, а інші комбінації є забороненими. Така надмірність кодування потрібно для розпізнавання модемом помилкових сигналів, що є наслідком перекручувань через перешкоди, що на телефонних каналах, комутирува особливо, дуже значні по амплітуді і тривалі за часом.

При цифровому кодуванні дискретної інформації застосовують потенційні та імпульсні коди.

У потенційних кодах для представлення логічних одиниць і нулів використовується тільки значення потенціалу сигналу, а його перепади, що формують закінчені імпульси, до уваги не приймаються. Імпульсні коди дозволяють представити двійкові дані або імпульсами визначеної полярності, або частиною імпульсу – перепадом потенціалу визначеного напрямку.

Вимоги до методів цифрового кодування

При використанні прямокутних імпульсів для передачі дискретної інформації необхідно вибрати такий спосіб кодування, що одночасно досягав би декількох цілей:

- мав при одній і тій же бітовій швидкості найменшу ширину спектра результуючого сигналу;
- забезпечував синхронізацію між передавачем і приймачем;
- мав здатність розпізнавати помилки;
- мав низьку вартість реалізації.

Вужчий спектр сигналів дозволяє на одній і тій же лінії (з однієї і тією же смугою пропускання) домагатися вищої швидкості передачі даних. Крім того, часто до спектра сигналу пред'являється вимога відсутності постійної складової, тобто наявності постійного струму між передавачем і приймачем.

Зокрема, застосування різних трансформаторних схем гальванічної розв'язки перешкоджає проходженню постійного струму.

Синхронізація передавача і приймача потрібна для того, щоб приймач точно знав, у який момент часу необхідно зчитувати нову інформацію з лінії зв'язку. Ця проблема в мережах вирішується складніше, ніж при обміні даними між близько розташованими пристроями, наприклад між блоками усередині комп'ютера чи між комп'ютером і принтером. На невеликих відстанях добре працює схема, заснована на окремої тактуючої лінії зв'язку (рис. 5.16), так що інформація знімається з лінії даних тільки в момент приходу тактового імпульсу. У мережах використання цієї схеми викликає труднощі через неоднорідність характеристик провідників у кабелях. На великих відстанях нерівномірність швидкості поширення сигналу може привести до того, що тактовий імпульс прийде настільки чи пізніше раніш відповідного сигналу даних, що біт даних буде пропущений чи лічений повторно. Іншою причиною, по якій у мережах відмовляються від використання тактуючих імпульсів, є економія провідників у дорогих кабелях.

Тому в мережах застосовуються так звані коди, що самосинхронізуються, сигнали яких несуть для передавача вказівки про те, у який момент часу потрібно здійснювати розпізнавання чергового біта (чи декількох біт, якщо код орієнтований більш ніж на два стани сигналу). Будь-який різкий перепад сигналу – так званий фронт – може служити вказівкою для синхронізації приймача з передавачем.

При використанні синусоїд як несучий сигнал результируючий код має властивість самосинхронізації, тому що зміна амплітуди несучої частоти дає можливість приймачу визначити момент появи вхідного коду.

Рис. 5.16. Синхронізація приймача і передавача на невеликих відстанях

Розпізнавання і корекцію перекручених даних складно здійснити засобами фізичного рівня, тому найчастіше цю роботу беруть на себе протоколи, що лежать вище: канальний, мережний, транспортний чи прикладний. З іншого боку, розпізнавання помилок на фізичному рівні заощаджує час, тому що приймач не чекає повного приміщення кадру в буфер, а відбраковує його відразу при розпізнаванні помилкових біт усередині кадру.

Вимоги, пропоновані до методів кодування, є взаємно суперечливими, тому кожний з розглянутих нижче популярних методів цифрового кодування має свої переваги і свої недоліки в порівнянні з іншими.

Потенційний код без повернення до нуля

На мал. 5.17, а показаний уже згаданий раніше метод потенційного кодування, який ще називають також кодуванням без повернення до нуля (Non Return to Zero, NRZ). Остання назва відбиває ту обставину, що при передачі послідовності одиниць сигнал не повертається до нуля протягом такту (як ми побачимо нижче, в інших методах кодування повернення до нуля в цьому випадку відбувається). Метод NRZ простий у реалізації, має добру розпізнаваність помилок (через два різні потенціали), але не має

властивості самосинхронізації. При передачі довгої послідовності одиниць чи нулів сигнал на лінії не змінюється, тому приймач позбавлений можливості визначати по вхідному сигналу моменти часу, коли потрібно в черговий раз зчитувати дані. Навіть при наявності високоточного тактового генератора приймач може помилитися з моментом знімання даних, тому що частоти двох генераторів ніколи не бувають цілком ідентичними. Тому при високих швидкостях обміну даними і довгими послідовностями одиниць чи нулів невелика неузгодженість тактових частот може привести до помилки в цілий такт і, відповідно, зчитуванню некоректного значення біта.

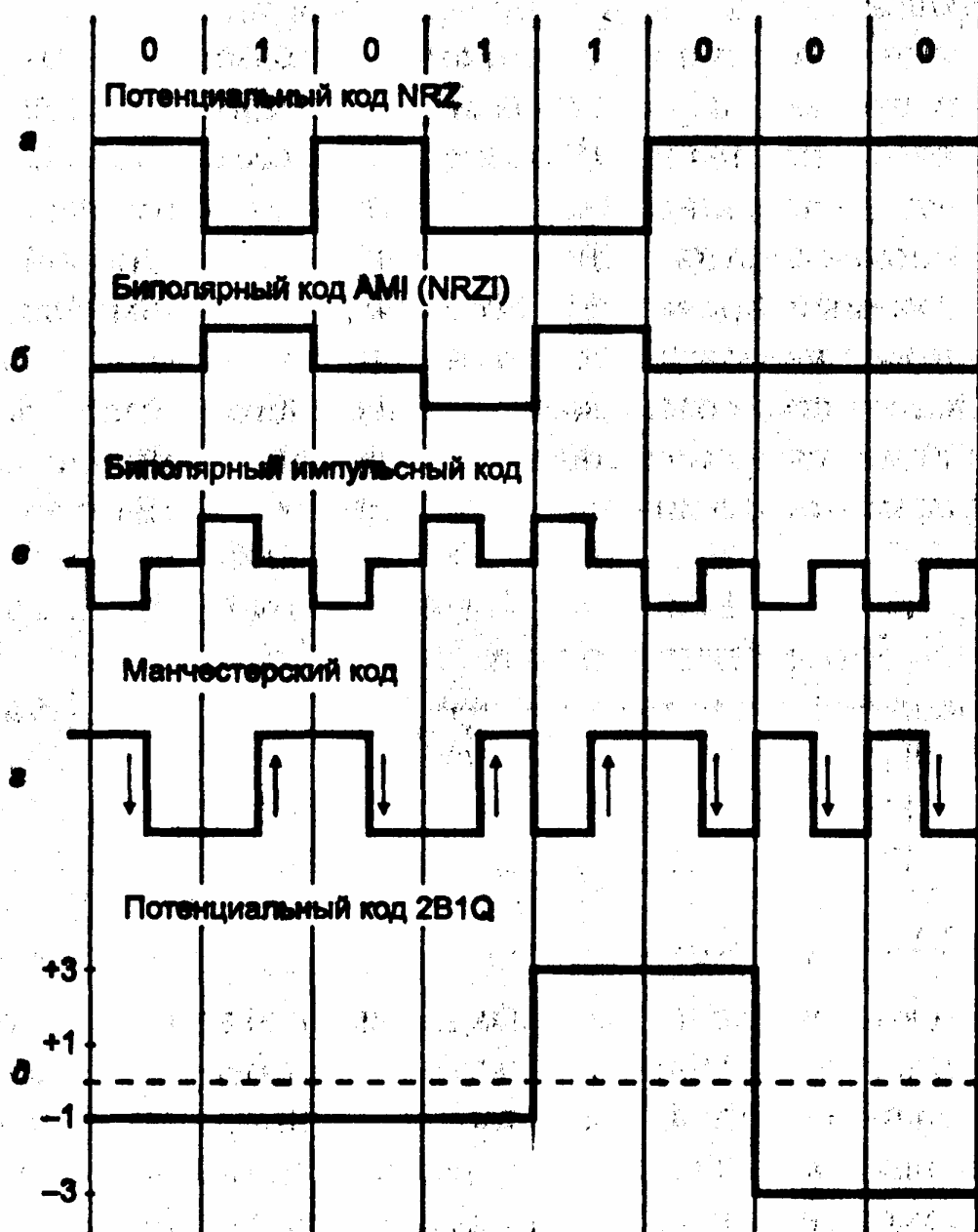


Рис. 5.17. Способы дискретного кодирования данных

Іншим серйозним недоліком методу NRZ є наявність низькочастотної складової, котра наближається до нуля при передачі довгих послідовностей одиниць чи нулів. Через це багато каналів зв'язку, що не забезпечують прямого гальванічного з'єднання між приймачем і джерелом, цей вид кодування не підтримують. У результаті в чистому виді код NRZ у мережах не використовується. Тому використовуються його різні модифікації, у яких

усувають як погану самосинхронізацію коду NRZ, так і наявність постійної складової. Привабливість коду NRZ, через яку є сенс зайнятися його поліпшенням, складається в досить низькій частоті основної гармоніки f_0 , що дорівнює $N/2$ Гц, як це було показано в попередньому розділі. В інших методів кодування, наприклад манчестерського, основна гармоніка має вищу частоту.

Метод біполярного кодування з альтернативною інверсією

Однієї з модифікацій методу NRZ є метод біполярного кодування з альтернативною інверсією (Bipolar Alternate Mark Inversion, AMI). У цьому методі (рис. 5.17,б) використовуються три рівні потенціалу – негативний, нульовий і позитивний. Для кодування логічного нуля використовується нульовий потенціал, а логічна одиниця кодується або позитивним потенціалом, або негативним, при цьому потенціал кожної нової одиниці протилежний потенціалу попередньої.

Код AMI частково ліквідує проблеми постійної складової і відсутності самосинхронізації, властиві коду NRZ. Це відбувається при передачі довгих послідовностей одиниць. У цих випадках сигнал на лінії являє собою послідовність різнополярних імпульсів з тим же спектром, що й у коду NRZ, що передає нулі, що чергуються, і одиниці, тобто без постійної складової і з основною гармонікою $N/2$ Гц (де N – бітова швидкість передачі даних). Довгі ж послідовності нулів також небезпечні для коду AMI, як і для коду NRZ – сигнал вироджується в постійний потенціал нульової амплітуди. Тому код AMI вимагає подальшого поліпшення, хоча задача спрощується – залишилося справитися тільки з послідовностями нулів.

У цілому, для різних комбінацій бітів на лінії використання коду AMI приводить до вузького спектру сигналу, ніж для коду NRZ, а значить, і до вищої пропускну здатності лінії. Наприклад, при передачі одиниць, що чергуються, і нулів основна гармоніка f_0 має частоту $N/4$ Гц. Код AMI надає

також певні можливості по розпізнаванню помилкових сигналів. Так, порушення строгого чергування полярності сигналів говорить про помилковий імпульс чи зникнення з лінії коректного імпульсу. Сигнал з некоректною полярністю називається забороненим сигналом (signal violation).

У кодї АМІ використовуються не два, а три рівні сигналу на лінії. Додатковий рівень вимагає збільшення потужності передавача приблизно на 3 дБ для забезпечення тієї ж вірогідності прийому бітів на лінії, що є загальним недоліком кодів з декількома станами сигналу в порівнянні з кодами, що розрізняють тільки два стани.

Потенційний код з інверсією при одиниці

Існує код, схожий на АМІ, але тільки з двома рівнями сигналу. При передачі нуля він передає потенціал, що був встановлений у попередньому такті (не змінює його), а при передачі одиниці потенціал інвертується на протилежний. Цей код називається потенційним кодом з інверсією при одиниці (Non Return to Zero with ones Inverted, NRZI). Цей код зручний у тих випадках, коли використання третього рівня сигналу дуже небажане, наприклад в оптичних кабелях, де стійко розпізнаються два стани сигналу – світло і темрява. Для поліпшення потенційних кодів, подібних АМІ і NRZI, використовуються два методи. Перший метод заснований на додаванні у вихідний код надлишкових біт, що містять логічні одиниці. Очевидно, що в цьому випадку довгі послідовності нулів перериваються і код стає самосинхронізованим для будь-яких переданих даних. Зникає також постійна складова, а значить, ще більш звужується спектр сигналу. Але цей метод знижує корисну пропускну здатність лінії, тому що надлишкові одиниці користувачької інформації не несуть. Інший метод заснований на попередньому “перемішуванні” вихідної інформації таким чином, щоб імовірність появи одиниць і нулів на лінії ставала близькою. Пристрої, чи

блоки, що виконують таку операцію, називаються скремблерами (scramble – смітник). При скрембюванні використовується відомий алгоритм, тому приймач, одержавши двійкові дані, передає їх на дескремблер, що відновлює вихідну послідовність біт. Надлишкові біти при цьому по лінії не передаються. Обидва методи відносяться до логічного, а не фізичного кодування, тому що форму сигналів на лінії вони не визначають.

Біполярний імпульсний код

Крім потенційних кодів у мережах використовуються й імпульсні коди, коли дані представлені повним чи імпульсом же его частиною – фронтом. Найбільш простим випадком такого підходу є біполярний імпульсний код, у якому одиниця представлена імпульсом однієї полярності, а нуль – іншої (мал. 2.16, в). Кожен імпульс триває половину такту. Такий має відмінні самосинхронізуючі властивості, але постійна складова може бути присутньою, наприклад, при передачі довгої послідовності одиниць чи нулів. Крім того, спектр у нього ширший, ніж у потенційних кодів. Так, при передачі всіх нулів чи одиниць частота основної гармоніки коду буде дорівнює N Гц, що в два рази вище основної гармоніки коду NRZ і в чотири рази вище основної гармоніки коду АМІ при передачі одиниць, що чергуються, і нулів. Через занадто широкий спектр біполярний імпульсний код використовується рідко.

Манчестерський код

У локальних мережах донедавна найпоширенішим методом кодування був так званий манчестерський код (мал. 2.16, г). Він застосовується в технологіях Ethernet і Token Ring.

У манчестерському коді для кодування одиниць і нулів використовується перепад потенціалу, тобто фронт імпульсу. При манчестерському кодуванні кожен такт поділяється на дві частини.

Інформація кодується перепадами потенціалу, що відбуваються в середині кожного такту. Одиниця кодується перепадом від низького рівня сигналу до високого, а нуль – зворотним перепадом. На початку кожного такту може відбуватися службовий перепад сигналу, якщо потрібно представити кілька одиниць чи нулів подряд. Тому що сигнал змінюється принаймні один раз за такт передачі одного біта даних, то манчестерський код має гарні самосинхронізуючі властивості. Смуга пропускання манчестерського коду вужча, ніж у біполярних імпульсних. У нього також немає постійної складової, а основна гармоніка в гіршому випадку (при передачі послідовності одиниць чи нулів) має частоту N Гц, а в кращому (при передачі одиниць, що чергуються, і нулів) вона дорівнює $N/2$ Гц, як і в кодів АМІ чи NRZ. У середньому ширина смуги манчестерського коду в півтора разу вужча, ніж у біполярного імпульсного коду, а основна гармоніка коливається поблизу значення $3N/4$. Манчестерський код має ще одну перевагу перед біполярним імпульсним кодом. В останньому для передачі даних використовуються три рівні сигналу, а в манчестерському – два.

Потенційний код 2B1Q

На мал. 2.16, д показаний потенційний код з чотирма рівнями сигналу для кодування даних. Це код 2B1Q, назва якого відбиває його суть – кожні два біти (2B) передаються за один такт сигналом, що має чотири стани (1Q). Парі біт 00 відповідає потенціал $-2,5$ В, парі біт 01 відповідає потенціал $-0,833$ В, парі 11 – потенціал $+0,833$ В, а парі 10 – потенціал $+2,5$ В. При цьому способі кодування вимагаються додаткові заходи по боротьбі з довгими послідовностями однакових пар біт, тому що при цьому сигнал перетворюється в постійну складову. При випадковому чергуванні бітів спектр сигналу в два рази вужчий, ніж у коду NRZ, тому що при тій же бітовій швидкості тривалість такту збільшується в два рази. Таким чином, за допомогою коду 2B1Q можна по однієї і тій же лінії передавати дані в два

рази швидше, ніж за допомогою коду АМІ чи NRZ. Однак для його реалізації потужність передавача повинна бути вища, щоб чотири рівні чітко розрізнялися приймачем на тлі перешкод.

5.3. Аналого-цифрове перетворення

Нам інколи потрібно перетворити в цифрову форму аналоговий сигнал. Наприклад, щоб послати людський голос на велику віддаль, нам потрібно перетворити його в цифрову форм, так як цифрові сигнали даних є менше схильними до завад. Це називається аналого-цифровим перетворенням або перетворенням в цифрову форму аналогового сигналу. Воно вимагає спрощення потенційно нескінченної кількості значень в аналоговому повідомленні так, щоб вони могли бути представлені, як цифровий потік з мінімальним пошкодженням інформації. Окремі методи для аналогово-цифрового перетворення будуть обговорені пізніше. На рис. 5.15 показано аналогово-цифровий конвертор, codec (дешифратор кодера).

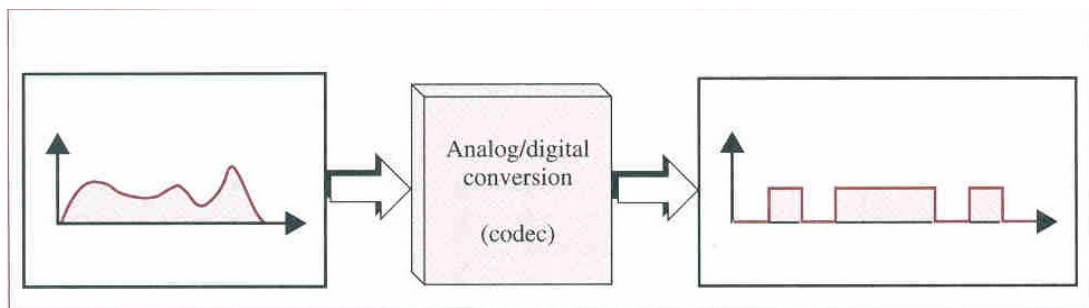


Рис. 5.15. Аналого-цифрове перетворення

Аналого-цифрове перетворення може використати будь-які цифрові сигнали даних. Структура сигналу переміщення не є проблемою. Натомість, проблемою є те, як перекласти інформацію з нескінченної кількості значень до дискретної кількості значень без втрат інформації або якості.

Модуляція Імпульсної Амплітуди (РАМ)

Перший крок в аналогово-цифровому перетворенні називається модуляція імпульсної амплітуди (РАМ). Ця техніка бере аналоговий канал, опитує його, і генерує серію імпульсів, оснований на результатах вибірки. Термін вибірка означає вимірювання амплітуди сигналу з рівними проміжками.

Метод вибірки, яка використовується в РАМ є більш корисним до інших областей розробки, ніж до передачі даних. Однак, РАМ є основою важливої аналогово-цифрової модуляції (РСМ), яку називають імпульсним методом перетворення.

У РАМ, первинний сигнал опитується з рівними проміжками, як показано на рис. 5.16. РАМ використовує викликану приклад техніки і володіння. У даному моменті, сигнальний рівень зчитується, потім зберігається. Типове значення відбувається тільки миттєво в фактичному хвильовому виразі, але узагальнюється над коротким, але вимірюваним періодом в результаті РАМ.

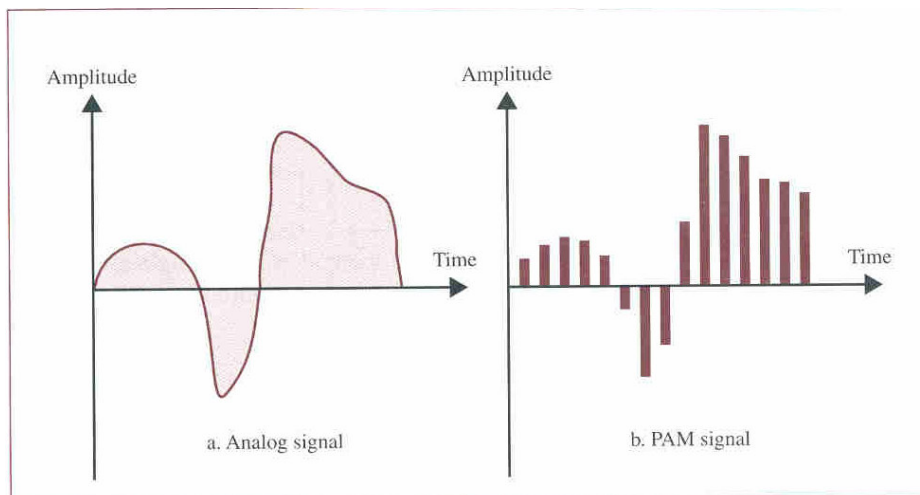


Рис. 5.16 РАМ

Причиною того, що РАМ не підходить до передачі даних, є те, що хоч він перекладає первинний хвильовий вираз до серії імпульсів, ці імпульси є нерухомими з будь-якої амплітуди (аналоговий сигнал, а не цифровий). Щоб

зробити їх цифровими, ми повинні змінити їх за допомогою використання модуляції імпульсного коду (PCM).

Модуляція Імпульсного Коду (PCM)

PCM змінює імпульси, створені за допомогою РАМ, щоб створити цифровий сигнал даних. Щоб зробити так, перший квантизує PCM імпульси РАМ. Квантування є методом присвоєння значень в специфічній області до типових екземплярів. Результат квантування показано на рис. 5.17.

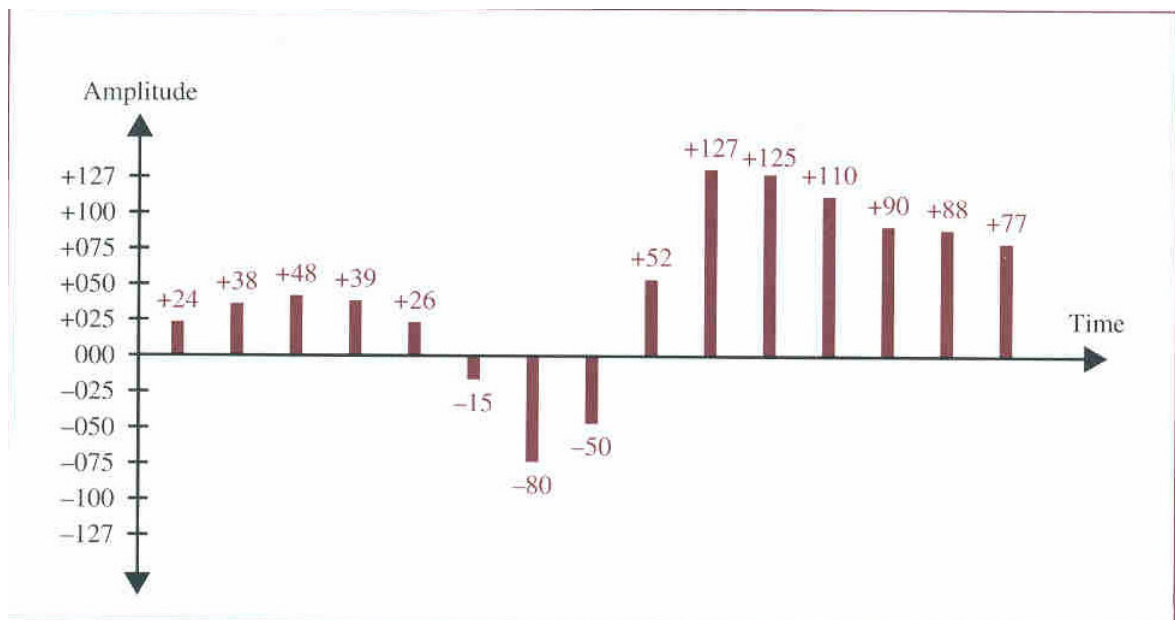


Рис. 5.17. Квантизований сигнал РАМ

На рис. 5.18 показано простий метод знака присвоєння і значення величини до прикладів квантизації. Кожне значення перекладається на двійковий еквівалент семи бітів. Восьмий біт вказує на знак.

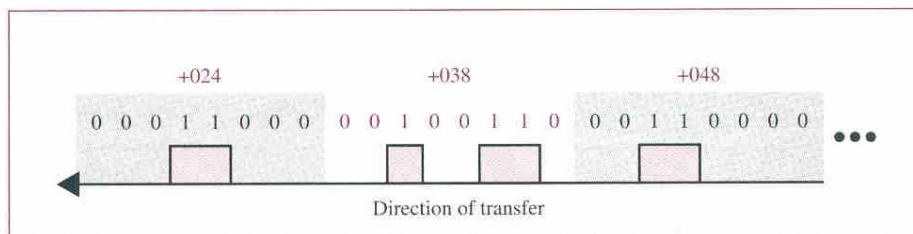
+024	00011000	-015	10001111	+125	01111101
+038	00100110	-080	11010000	+110	01101110
+048	00110000	-050	10110010	+090	01011010
+039	00100111	+052	00110110	+088	01011000
+026	00011010	+127	01111111	+077	01001101

Sign bit
 + is 0 - is 1

Рис. 5.18. Квантизація з використанням знака і величини

Двійкові розряди потім перетворюються в цифровий сигнал даних, використовуючи один з методів цифрово-цифрового кодування. На рис. 5.19 показано результат модуляції імпульсного коду первинного сигналу, який кодується остаточно в уніполярний сигнал. Показані тільки перші три типові значення.

PCM дійсно створюється особливістю чотирьох окремих процесів: РАМ, квантування, двійкове кодування, і цифрово-цифрове кодування. На рис. 5.20 показано повний процес в графічному вираженні. PCM є методом вибірки, який використовується, щоб перетворити в цифрову форму голос в Т-лінійній передачі в Північній Американській системі дистанційного зв'язку.



Цифра 5.19 PCM

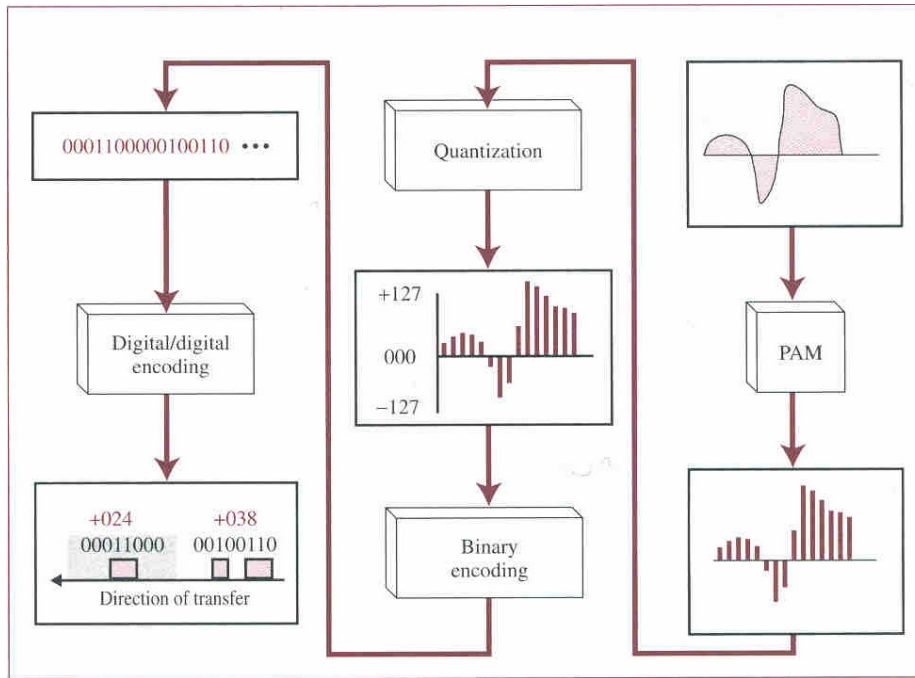


Рис. 5.20 Від аналогового каналу до цифрового коду РСМ

Вибірка коефіцієнта

Оскільки можна сказати з попередніх рисунків, точність будь-якого цифрового відтворення аналогового каналу залежить від кількості взятих прикладів. Використовуючи РАМ і РСМ, ми можемо відтворити хвильовий вираз точно за допомогою використання нескінчених прикладів, або ми можемо відтворити узагальнення напряму зміни за допомогою трьох прикладів. Очевидно, ми віддаємо перевагу кількості десь між цими двома крайностями. Так що є запитання. Скільки прикладів є достатнім?

Дійсно, потрібно зовсім небагато інформації для отримуючого пристрою, щоб відновити аналоговий канал. Відповідно до теореми Nyquist, щоб гарантувати точне відтворення первинного аналогового каналу, використовуючи РАМ, коефіцієнт вибірки повинний бути щонайменше вдвічі вищим від частоти первинного сигналу. Так, якщо ми хочемо до зразкового відображення голосу у телефоні з максимальною частотою 4000 Hz, ми потребуємо коефіцієнта вибірки 8000 прикладів за секунду.

Зразок подвійної частоти вибірки означає, що сигнал повинен бути опитаним кожних $1/2x$ секунд. Використовуючи приклад надмірних фонових лінійок голосу означає опитування кожну другу з $1/8000$. Рис. 5.21 ілюструє принцип.

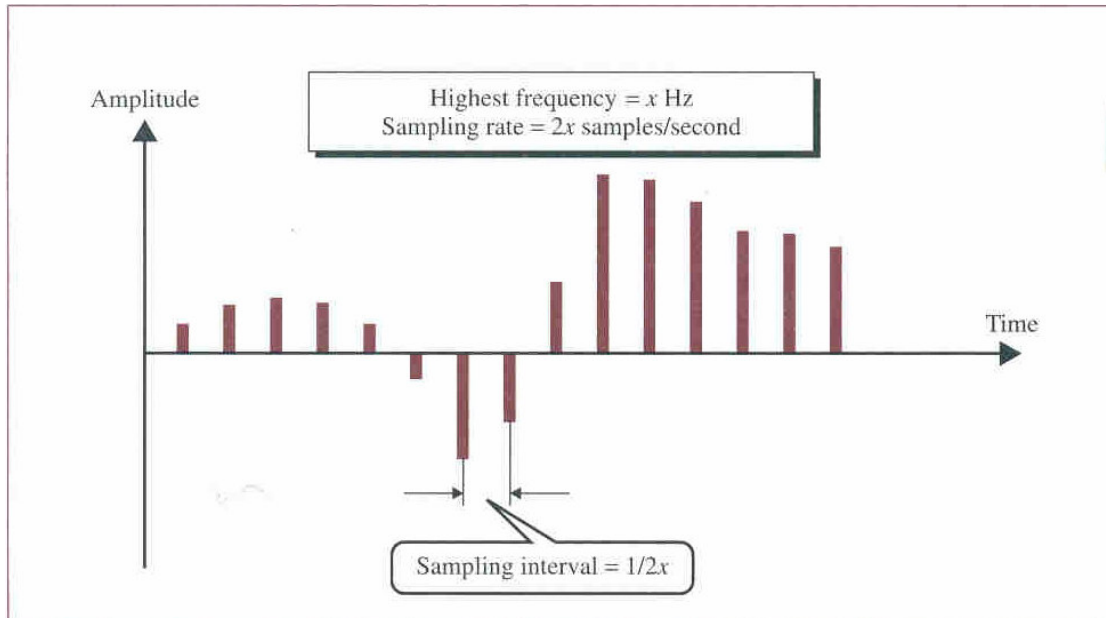


Рис. 5.21. Теорема Найквіста

Приклад 5.3

Який коефіцієнт вибірки потрібен для сигналу з пропускнуою здатністю 10,000 Hz (1,000 до 11,000 Hz)?

Розв'язок

Зразок вибірки повинний бути двічі вищим частоти сигналу:

Приклади/секунди коефіцієнта = Вибірки $2(11,000) = 22,000$

Скільки бітів за приклад?

Після того, як ми заснували коефіцієнт вибірки, ми потребуємо визначити кількість бітів, яка передається для кожного прикладу. Це залежить від рівня потрібної точності. Кількість бітів вибирається такою, що первинний сигнал може бути відтворений з бажаною точністю в амплітуді.

Приклад 5.4

Сигнал опитується. Кожен приклад вимагає щонайменше 12 рівнів точності (+0 до +5 і -0 -5). Скільки бітів повинно бути послано по кожен приклад?

Розв'язок

Ми потребуємо чотири біти: один біт для знаку і три біти для значення. Три бітове значення може представити $2^3 = 8$ рівнів (000 до 111), яке є більшим, ніж те, що ми потребуємо. Дво-бітове значення не є достатнім після $2^2 = 4$. Чотири бітове значення є завеликим, тому що $2^4 = 16$.

Швидкість передачі в бітах

Після виявлення кількості бітів за приклад, ми можемо підрахувати швидкість передачі в бітах, використовуючи наступну формулу:

Кількість x бітів коефіцієнта Вибірки швидкості = Передачі в бітах за приклад

Приклад 5.5

Ми хочемо перетворити в цифрову форму людський голос. Якою є швидкість передачі в бітах, яка набуває восьми бітів за приклад?

Розв'язок

Людський голос нормально містить частоти від 0 до 4000 Hz. Так що коефіцієнт вибірки є:

$X_{\text{зразка}} = \text{Вибірки} \cdot 4000 = 8000$ опитує/допомагає швидкість передачі в бітах може бути підрахований, як:

Кількість x бітів коефіцієнта Вибірки швидкості = Передачі в бітах за зразкова = $8000 \times 8 = 64,000$ біти/s = 64 Kbps

5.4. Цифро-аналогове перетворення

Цифрово-аналогове перетворення або цифро-аналогова модуляція є процесом зміни однієї з характеристик аналогового каналу, оснований на інформації в цифровому сигналі даних (нулі і одиниці). Коли ви передаєте дані від одного комп'ютера до іншого через телефонну лінію, наприклад,

первинні дані є цифровими, але, через те, що телефонні служби використовують аналогові канали, дані повинні бути перетворені. Цифрові дані повинні модулюватися на аналоговому каналі, яким маніпулювали, щоб бути схожим на два чіткі значення, які відповідають двійковій 1 і двійковому 0. Рис. 5.22 показує зв'язок між цифровою інформацією, цифрово-аналоговими апаратними засобами модулювання, і аналоговим каналом рівнодіючої сили.

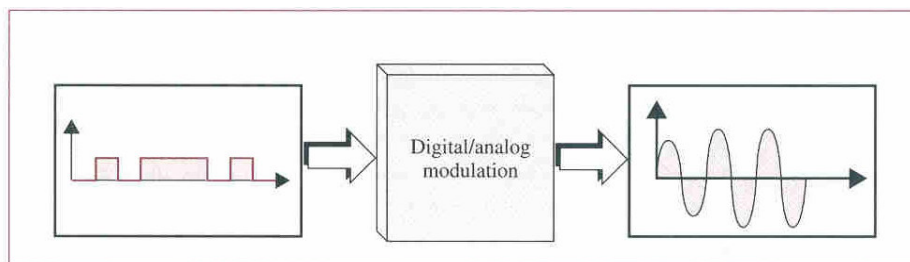


Рис. 5.22. Цифрово-аналогова модуляція

Дискретна модуляція аналогових сигналів

Однією з основних тенденцій розвитку мережних технологій є передача в одній мережі як дискретних, так і аналогових по своїй природі даних. Джерелами дискретних даних є комп'ютери та інші обчислювальні пристрої, а джерелами аналогових даних є такі пристрої, як телефони, відеокамери, звуко- і відеовідтворююча апаратура. На ранніх етапах рішення цієї проблеми в територіальних мережах усі типи даних передавалися в аналоговій формі, при цьому дискретні за своїм характером комп'ютерні дані перетворювалися в аналогову форму за допомогою модемів.

Однак у міру розвитку техніки знімання і передачі аналогових даних з'ясувалося, що передача їх в аналоговій формі не дозволяє поліпшити якість прийнятих на іншому кінці лінії даних, якщо вони істотно спотворилися при передачі. Сам аналоговий сигнал не дає ніяких указівок ні про те, що відбулося перекручування, ні про те, як його виправити, оскільки форма сигналу може бути будь-яка. Поліпшення ж якості ліній, особливо

територіальних, вимагає величезних зусиль і капіталовкладень. Тому на зміну аналоговій техніці запису і передачі звуку і зображення прийшов цифрова техніка. Ця техніка використовує так названу дискретну модуляцію вихідних безупинних у часі аналогових процесів.

Дискретні способи модуляції засновані на дискретизації безупинних процесів як по амплітуді, так і за часом (мал. 2.19). Розглянемо принципи дискретної модуляції на прикладі імпульсно-кодової модуляції, ІКМ (Pulse Amplitude Modulation, PAM), що широко застосовується в цифровій телефонії.

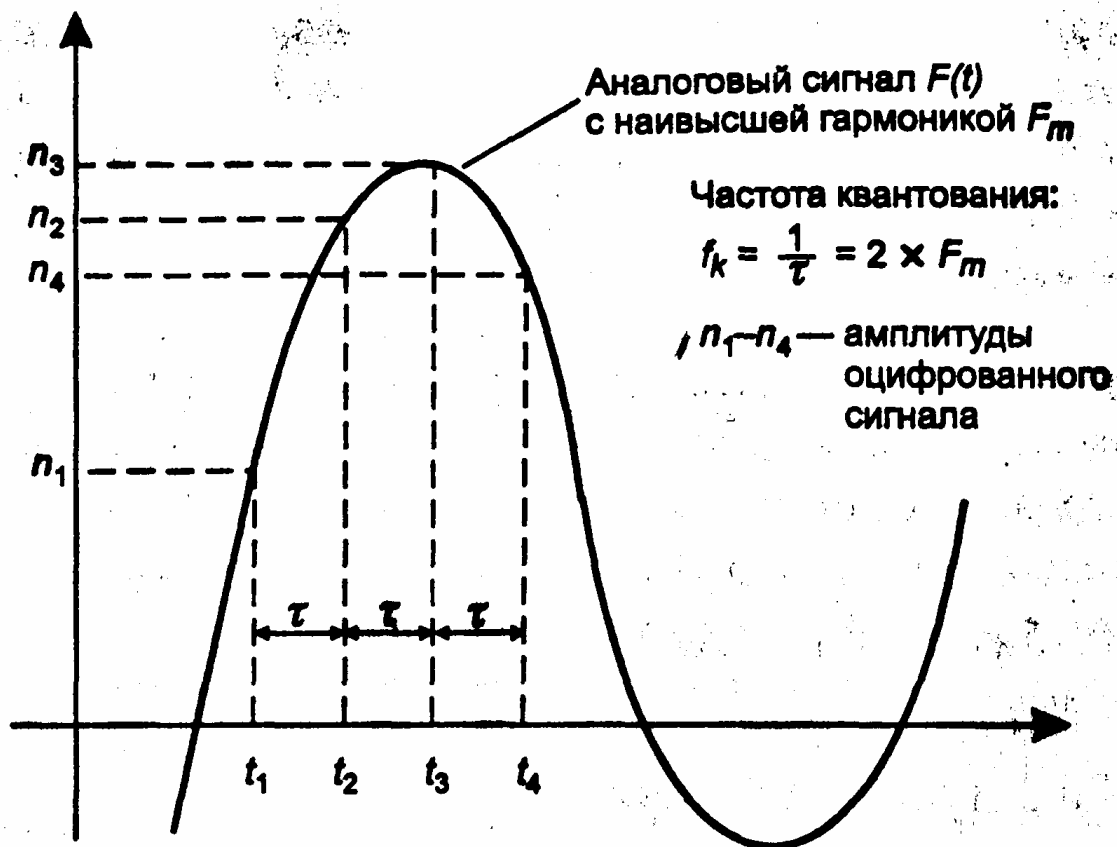


Рис. 2.19. Дискретна модуляція безупинного процесу

Амплітуда вихідної безупинної функції вимірюється із заданим періодом – за рахунок цього відбувається дискретизація за часом. Потім кожен вимір представляється у виді двійкового числа визначеної розрядності, що означає дискретизацію за значеннями функції – безперервна множина

можливих значень амплітуди заміняється дискретною кількістю її значень. Пристрій, що виконує подібну функцію, називається аналого-цифровим перетворювачем (АЦП). Після цього виміри передаються по каналах зв'язку у виді послідовності одиниць і нулів. При цьому застосовуються ті ж методи кодування, що й у випадку передачі початково дискретної інформації, тобто, наприклад, методи, засновані на кодів В825 чи 2В1Q.

На прийомній стороні лінії коди перетворюються у вихідну послідовність біт, а спеціальна апаратура, яку називають цифро-аналоговим перетворювачем (ЦАП), робить демодуляцію оцифрованих амплітуд безперервного сигналу, відновлюючи вихідну безперервну функцію часу.

Дискретна модуляції заснована на теорії відображення Найквіста – Котельникова. Відповідно до цієї теорії, аналогова безперервна функція, передана у виді послідовності її дискретних за часом значень, може бути точно відновлена, якщо частота дискретизації була в два чи більш разів вища, ніж частота найвищої гармоніки спектру вихідної функції.

Якщо ця умова не дотримується, то відновлена функція буде істотно відрізнятися від вихідної.

Перевагою цифрових методів запису, відтворення і передачі аналогової інформації є можливість контролю вірогідності переданих лічених з носія чи отриманих по лінії зв'язку даних. Для цього можна застосовувати ті ж методи, що застосовуються для комп'ютерних даних (і розглядаються більш детально далі), – обчислення контрольної суми, повторна передача перекручених кадрів, застосування кодів, що самокоректуються.

Для якісної передачі голосу в методі ІКМ використовується частота квантування амплітуди звукових коливань у 8000 Гц. Це зв'язано з тим, що в аналоговій телефонії для передачі голосу було обрано діапазон від 300 до 3400 Гц, що достатньо якісно передає всі основні гармоніки співрозмовників. Відповідно до теореми Найквіста – Котельникова для якісної передачі голосу досить вибрати частоту дискретизації, у два рази перевищуючу найвищу

гармоніку безупинного сигналу, тобто 2 x 3400-6800 Гц. Обрана в дійсності частота дискретизації 8000 Гц забезпечує деякий запас якості. У методі ІКМ звичайно використовується 7 чи 8 біт коду для представлення амплітуди одного виміру. Відповідно це дає 127 чи 256 градацій звукового сигналу, що виявляється цілком достатнім для якісної передачі голосу. При використанні методу ІКМ для передачі одного голосового каналу необхідна пропускна здатність 56 чи 64 Кбіт/с залежно від того, якою кількістю біт представляється кожен вимір. Якщо для цих цілей використовується 7 біт, то при частоті передачі вимірів у 8000 Гц одержуємо:

$8000 \times 7 = 56000$ біт/с чи 56 Кбіт/с; а для випадку 8-ми біт:

$8000 \times 8 = 64000$ біт/с чи 64 Кбіт/с.

Стандартним є цифровий канал 64 Кбіт/с, що також називається елементарним каналом цифрових телефонних мереж.

Передача безупинного сигналу в дискретному вигляді вимагає від мереж жорсткого дотримання часового інтервалу в 125 мкс (відповідно частоті дискретизації 8000 Гц) між сусідніми вимірами, тобто вимагає синхронної передачі даних між вузлами мережі. При недотриманні синхронності вхідних вимірів вихідний сигнал відновлюється невірно, що приводить до перекручування голосу, зображення чи іншої мультимедійної інформації, переданої цифровими мережами. Так, перекручування синхронізації в 10 мс може привести до ефекту "луни", а зсув між вимірами в 200 мс приводять до втрати розпізнаваності вимовлених слів. У той же час втрата одного виміру при дотриманні синхронності між іншими вимірами практично не позначається на відтвореному звукові. Це відбувається за рахунок згладжуючих пристроїв, у цифро-аналогових перетворювачах, що засновані на властивості інерційності будь-якого фізичного сигналу – амплітуда звукових коливань не може миттєво змінитися на велику величину.

На якість сигналу після ЦАП впливає не тільки синхронність надходження на його вхід вимірів, але і погрішність дискретизації амплітуд цих вимірів.

У теоремі Найквіста – Котельникова передбачається, що амплітуди функції вимірюються точно, у той же час використання для їхнього збереження двійкових чисел з обмеженою розрядністю дещо спотворює ці амплітуди. Відповідно спотворюється відновлений безупинний сигнал, що називається шумом дискретизації (по амплітуді).

Існують і інші методи дискретної модуляції, що дозволяють представити виміри голосу в більш компактній формі, наприклад у вигляді послідовності 4-бітних чи 2-бітних чисел. При цьому один голосовий канал вимагає меншої пропускної здатності, наприклад 32 Кбіт/с, 16 Кбіт/с чи ще менше. З 1985 року застосовується стандарт CCITT кодування голосу, який називають Adaptive Differential Pulse Code Modulation (ADPCM). Коди ADPCM засновані на знаходженні різниць між послідовними вимірами голосу, що потім і передаються по мережі. У коді ADPCM для збереження однієї різниці використовуються 4 біт і голос передається зі швидкістю 32 Кбіт/с. Більш сучасний метод, Linear Predicting Coding (LPC), робить виміри вихідної функції рідше, але використовує методи прогнозування напрямку зміни амплітуди сигналу. За допомогою цього методу можна понизити швидкість передачі голосу до 9600 біт/с.

Представлені в цифровій формі безперервні дані легко можна передати через комп'ютерну мережу. Для цього досить помістити кілька вимірів у кадр якої-небудь стандартної мережної технології, забезпечити кадр правильною адресою призначення і відправити адресату. Адресат повинний добути з кадру виміри і подати їх з частотою квантування (для голосу – з частотою 8000 Гц) на цифро-аналоговий перетворювач. В міру надходження наступних кадрів з вимірами голосу операція повинна повторитися. Якщо кадри будуть прибувати досить синхронно, то якість голосу може бути досить високою.

Однак, як ми уже знаємо, кадри в комп'ютерних мережах можуть затримуватися як у кінцевих вузлах (при очікуванні доступу до поділюваного середовища), так і в проміжних комунікаційних пристроях – мостах, комутаторах і маршрутизаторах. Тому якість голосу при передачі в цифровій формі через комп'ютерні мережі звичайно буває невисокою. Для якісної передачі оцифрованих безперервних сигналів – голосу, зображення – сьогодні використовують спеціальні цифрові мережі, такі як ISDN, ATM, і мережі цифрового телебачення. Тем для передачі внутрікорпоративних телефонних розмов сьогодні характерні мережі frame relay, затримки передачі кадрів яких укладаються в припустимі межі.

Асинхронна і синхронна передачі

При обміні даними на фізичному рівні одиницею інформації є біт, тому засоби фізичного рівня завжди підтримують побітову синхронізацію між приймачем і передавачем.

Канальний рівень оперує кадрами даних і забезпечує синхронізацію між приймачем і передавачем на рівні кадрів. В обов'язки приймача входить розпізнавання початку першого байта кадру, розпізнавання границь полів кадру і розпізнавання ознаки закінчення кадру.

Звичайно досить забезпечити синхронізацію на зазначених двох рівнях – бітовому і кадровому, – щоб передавач і приймач змогли забезпечити стійкий обмін інформацією. Однак при поганій якості лінії зв'язку (звичайно це відноситься до комутованих телефонних каналів) для здешевлення апаратури і підвищення надійності передачі даних запроваджують додаткові засоби синхронізації на рівні байтів.

Такий режим роботи називається асинхронним чи старт-стопним. Іншою причиною використання такого режиму роботи є наявність пристроїв, що генерують байти даних у випадкові моменти часу. Так працює клавіатура

дисплея чи іншого термінального пристрою, з якого людина вводить дані для обробки їх комп'ютером.

В асинхронному режимі кожен байт даних супроводжується спеціальними сигналами “старт” і “стоп”. Призначення цих сигналів полягає в тому, щоб, по-перше, сповістити приймач про прихід даних і, по-друге, щоб дати приймачу досить часу для виконання деяких функцій, зв'язаних із синхронізацією, до надходження наступного байта. Сигнал “старт” має тривалість в один тактовий інтервал, а сигнал “стоп” може тривати один, півтора чи два такти, тому говорять, що використовується один, півтора чи дві біти в якості стопового сигналу, хоча користувачькі біти ці сигнали не представляють.

Як говорилося раніше, хвиля синуса визначається за допомогою трьох характеристик: амплітуда, частота, і фаза. Коли ми змінюємо будь-який з цих характеристик, ми створюємо другу версію тієї хвилі. Якщо ми потім говоримо, що первинна хвиля представляє двійковою 1, відхилення можна представити двійковим 0 або навпаки. Таким чином, за допомогою зміни одного аспекту простого електричного сигналу туди і назад, ми можемо використовувати їх, щоб представити цифрові дані. Будь-які три характеристики, надруковані вище, можуть бути змінені цим шляхом, надаючи нам щонайменше три пристрої для модулювання цифрових даних в аналоговий канал: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). Крім того, є четвертий (і кращий) пристрій, який об'єднує зміни як по амплітуді, так і модуляції drature amplitude modulation (QAM). QAM є найбільш ефективною з цих опцій і використовується у всіх сучасних модемах (рис. 5.23).

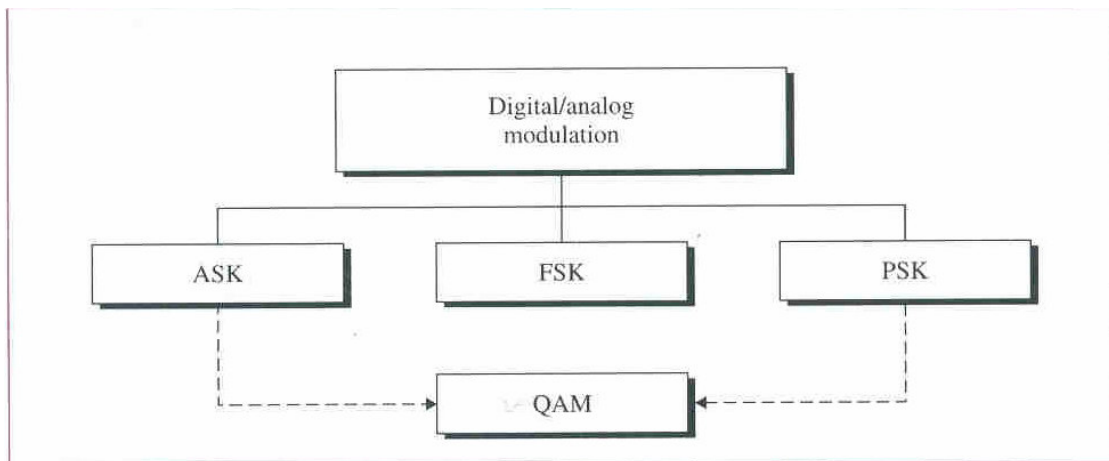


Рис. 5.23. Типи цифро-аналогової модуляції

Аспекти Цифрово-аналогового перетворення

Перед тим, як ми обговорюємо специфічні методи цифро-аналогової модуляції, повинні бути визначені дві основні проблеми: швидкість передачі в бодах/бітах і несучий сигнал.

Біт Rate і Бод Rate

Два елементи, які використовуються часто при передачі даних, швидкість передачі в бітах і швидкість в бодах. Швидкість передачі в бітах є кількість бітів, переданих протягом однієї секунди. Швидкість в бодах означає кількість сигналів за секунду, які необхідні, щоб представити ті біти. У обговореннях комп'ютерної ефективності, швидкість передачі в бітах є більш важливою – ми хочемо знати скільки часу потрібно, щоб передати кожну порцію інформації. У передачі даних, однак, ми більш стикаємося з тим, як ефективно ми можемо переміщувати ті дані з місця на місце, в порціях або блоках. Менші сигнальні елементи, яких вимагається, ефективніша система і менша пропускна спроможність, яка вимагається, щоб передати більше бітів; так що ми більш зв'язуємось з швидкістю в бодах. Швидкість в бодах визначає пропускну спроможність, якої вимагається, щоб послати сигнал.

Швидкість передачі в бітах дорівнює швидкості в бодах помноженій на кількість бітів, представлених за допомогою кожного сигналу. Швидкість в бодах дорівнює швидкості передачі в бітах, яка ділиться на кількість бітів, представлених за допомогою кожного сигнального зсуву. Швидкість Передачі в бітах є завжди більшою або рівною швидкості в бодах.

Аналогія може прояснити принцип бодів і бітів. У транспорті, бод є подібним до автомобіля, біт є подібним до пасажера. Автомобіль може перенести одного або більше пасажирів. Автомобілі переміщують з точки в точку тільки одного пасажера (шофер), тоді переміщуються 1000 пасажирів. Однак, якщо кожний автомобіль перевозить чотирьох пасажирів (carpooling), тоді переміщуються 4000 пасажирів. Зверніть увагу, що кількість автомобілів, а не кількість пасажирів, визначає потік обміну і, таким чином, потребу для ширших каналів інформації. Так само, кількість бодів визначає необхідну пропускну здатність, не кількість бітів.

Сигнал носія

У аналоговій передачі, передаючий пристрій виробляє сигнал високої частоти, що виступає як основа для інформаційного сигналу. Цей базовий сигнал називається сигнал носія або частота носія. Отримуючий пристрій налаштовується на частоту сигналу носія, який очікує його від відправника. Цифрова інформація потім модулюється на сигналі носія за допомогою модифікації однієї або більше характеристик (амплітуда, частота, фаза). Цей вид модифікації зветься, модуляція інформаційний сигнал зветься сигнал модулювання.

Amplitude Shift Keying (ASK)

У Amplitude Shift Keying (ASK), сила сигналу носія змінюється, щоб представити двійковий 1 або 0. Як частота так і константа фазового залишаються, в той час, як амплітуда змінюється. Яка напруга представляє 1

і яка представляє 0 залишається проектувальникам системи. Тривалість біта є період часу, коли визначається один біт. Амплітуда сигналу піку протягом кожної бітової тривалості є постійною і значення залежить від біта (0 або 1). Швидкість передачі, яка використовує ASK обмежується за допомогою фізичних характеристик передавального носія. Рис. 5.24 подає концептуальне зображення ASK.

На жаль, ASK передача є надзвичайно вразливою до завади. Термін завада означає ненавмисні напруги, представлені за допомогою різних явищ, як наприклад тепло або електромагнітний вступ, створений за допомогою інших джерел. Ці ненавмисні напруги об'єднуються з сигналом, щоб змінити амплітуду. 0 Може бути змінений на 1, і 1 на 0. Ви можете побачити те, як завада повинна особливо бути проблематична для ASK, який залежить виключно від амплітуди для розпізнавання. Завада звичайно впливає на амплітуду; таким чином. ASK є метод модулювання, який найбільш попадає під вплив завад.

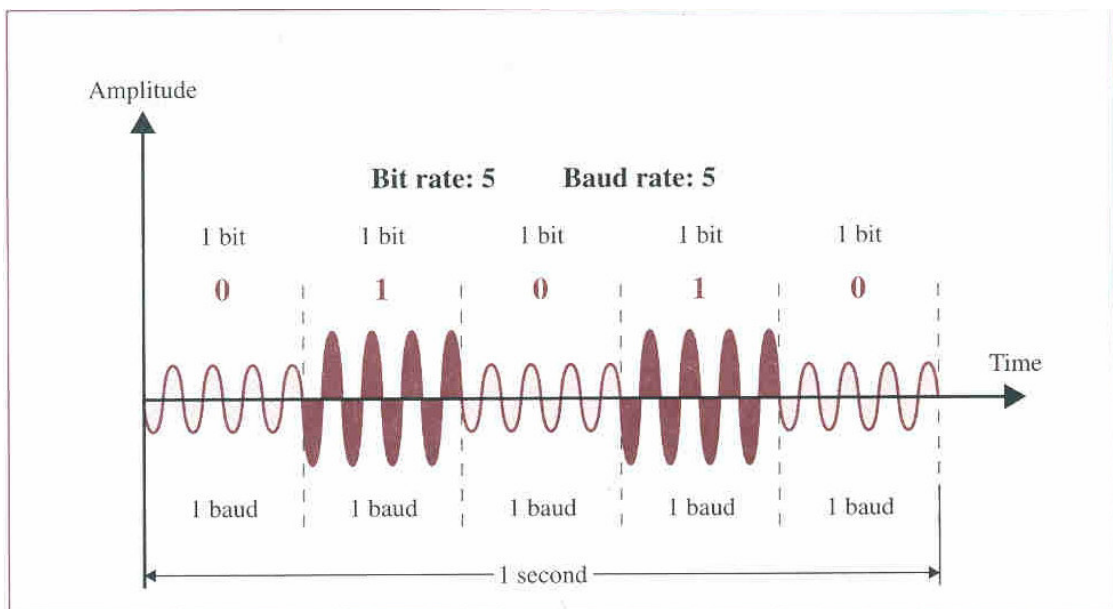


Рис. 5.24. ASK

Популярна ASK техніка називається on-off-keying (OOK). В OOK одне з бітових значень представляється не за допомогою напруги. Перевагою є спрощення в кількості енергії, яку вимагається, щоб передати інформацію.

Смуга пропускання для ASK

Як видно з попередньої лекції смуга пропускання сигналу є сумарна область частот, зайнятих за допомогою того сигналу. Коли ми розкладаємо ASK модульований сигнал, ми отримуємо спектр багатьох простих частот. Однак, найбільш суттєвий будь-хто є $f_c - N_{\text{baud}}/2$ and $f_c + N_{\text{baud}}/2$ з частотою носія, f_c в середині (рис. 5.25).

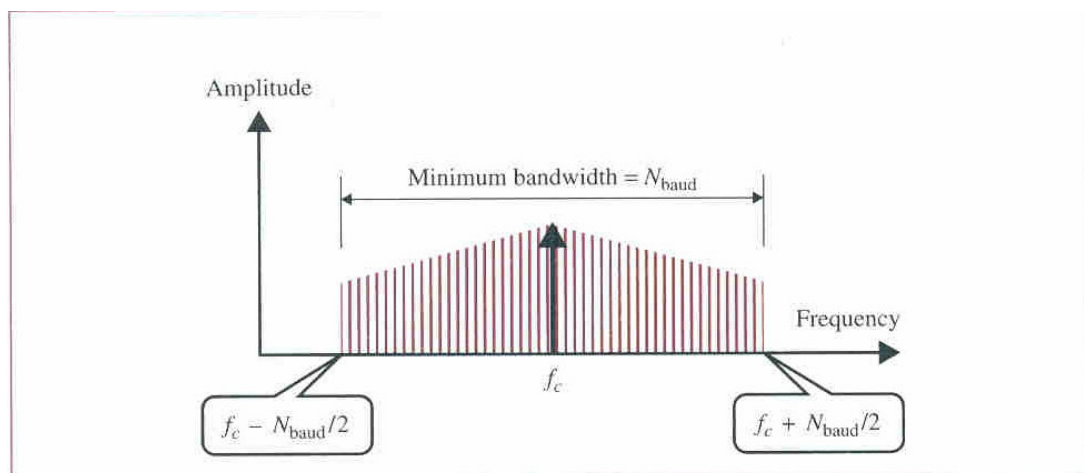


Рис. 5.25. Зв'язок між швидкістю смуги і смугою пропускання в ASK

Мінімальна смуга пропускання, яку вимагається для передачі, рівна до швидкості в бодах.

Хоч є тільки одна частота носія, процес модуляції виробляє комплексний сигнал, який є комбінація багато простих сигналів, кожного з різною частотою.

Frequency Shift Keying (FSK)

У Frequency Shift Keying (FSK), частота сигналу носія змінюється, щоб представити двійковий 1 або 0. Частота сигналу протягом кожної бітової тривалості є постійною і значення залежить від біта (0 або 1): як амплітуда піку, так і фаза залишаються постійною. Рис. 5.27 подає концептуальне зображення FSK.

FSK уникає більшості проблем ASK завад. Через те, що отримуючий пристрій шукає специфічні частотні зміни над даною кількістю періодів, він може ігнорувати перепади напруги. Коефіцієнти FSK обмеження є фізичними можливостями носія.

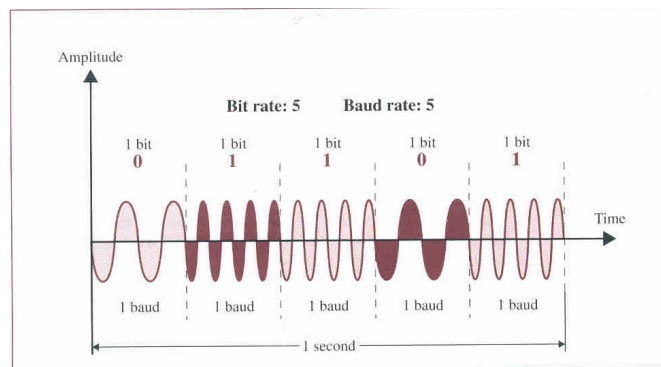


Рис. 5.27. FSK

Bandwidth для FSK

Хоч FSK переміщається між двома частотами носія, легко аналізувати, як співіснують дві частоти. Ми можемо сказати, що спектр FSK є комбінацією двох ASK спектрів, які центруються навколо спектру смуги пропускання, якої вимагається для передачі FSK, є рівним до швидкості в бодах сигналу плюс частотний зсув (різниця між двома частотами носія): $BW = \{fc1-fc0+Nbaud\}$ Рис. 5.28.

Хоч є тільки дві частоти носія, процес модуляції виробляє складений сигнал, який є комбінацією багатьох простих сигналів, кожного з різною частотою.

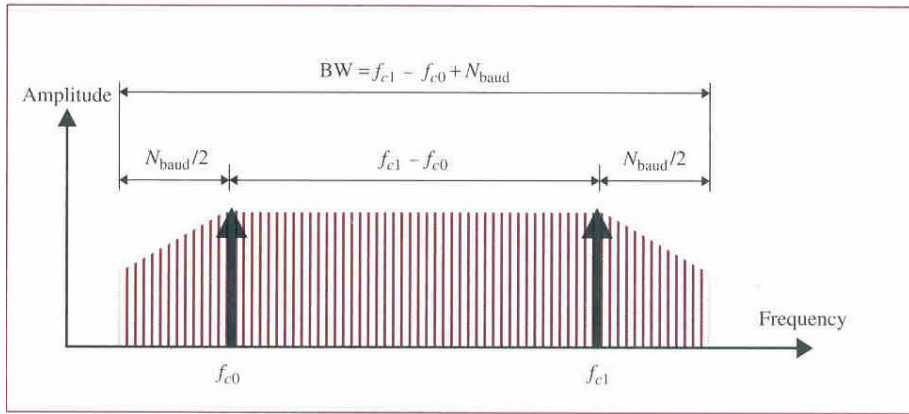


Рис. 5.28. Співвідношення між швидкістю у бодах і частотою у FSK

Phase Shift Keying (PSK)

У Phase Shift Keying (PSK), фаза носія змінюється, щоб представити двійковий 1 або 0. Як амплітуда піку, так і частотна константа залишаються, оскільки фаза змінюється. Наприклад, якщо ми починаємо з фази 0 градусів, щоб представити двійковий 0, тоді ми можемо змінити фазу на 180 градусів, щоб послати двійкову 1. Фаза сигналу протягом кожної бітової тривалості є постійною і значення залежить від біта (0 або 1). Рис. 5.29 подає концептуальне зображення PSK.

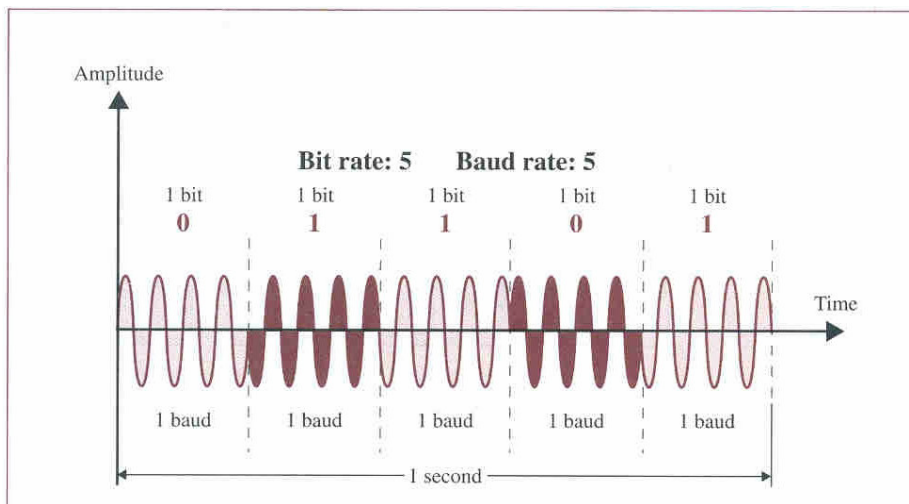
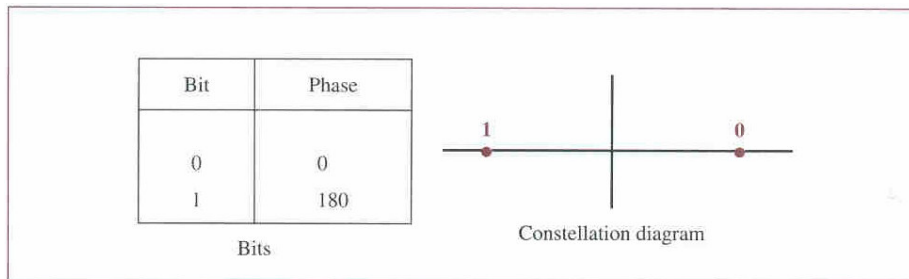


Рис. 5.29. PSK

Вищезазначений метод часто називають 2-PSK, або двійковий PSK, через те, що використовуються дві різні фази (0 і 180 градусів). Рис. 5.30 робить це наочним за допомогою сеансу зв'язку фази до бітового значення. Друга схема, за назвою сузір'я (constellation) або схема стану фази, показує той же зв'язок за допомогою ілюстрування тільки фаз.



Фігурне 5.30 PSK сузір'я (constellation)

PSK не є чутливим до завад, які впливають на ASK, ні до обмежень пропускнуої смуги FSK. Це означає, що менші відхилення в сигналі можуть бути виявлені надійно за допомогою приймача. Таким чином, замість використання тільки двох відхилень кожного сигналу, який представляє один біт, ми можемо використовувати чотири відхилення і дозволяти кожному фазовому зсуву представити два біти (рис. 5.31).

Схема сузір'я для сигналу на рис. 5.31 надається в рис. 5.32. Фаза 0 градусів в даний момент представляє 00; 90 градусів представляє 01; 180 градусів представляє 10; і 270 градусів представляє 11. Ця техніка називається 4-PSK або Q-PSK. Пара бітів, представлених за допомогою кожної фази називається двобітова конфігурація. Ми можемо передати дані два рази, як швидке використання 4-PSK, оскільки ми можемо використати 2-PSK.

Ми можемо розширити цю ідею до 8-PSK. Замість 90 градусів, ми в даний момент змінюємо сигнал за допомогою зсувів 45 градусів. З вісьмома різними фазами, кожний зсув може представити три біти (один tribit) вчасно.

(Як можна побачити, відношення кількості бітів бітового зсуву до кількості фаз є показник степеня двох. Коли ми маємо чотири можливі фази, ми можемо послати два біти – 2² дорівнює 4. Коли ми маємо вісім можливих фаз, ми можемо послати три біти – 2³ дорівнює 8). Рис. 5.33 показує зв'язки між фазовими зсувами і tribits, який кожний представляє: 8-PSK в тричі швидший, ніж 2-PSK.

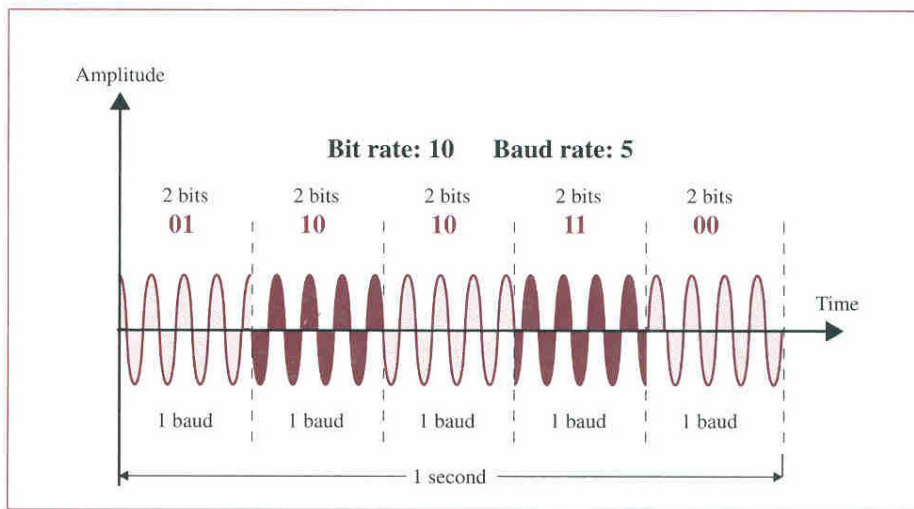


Рис. 5.31 4-PSK

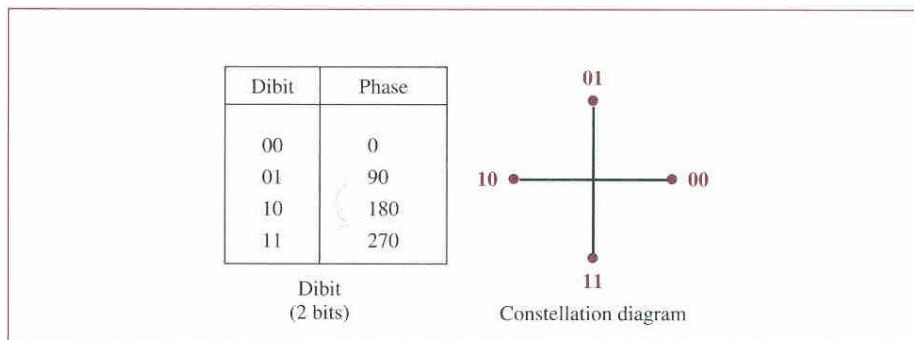


Рис. 5.32. 4-PSK характеристики

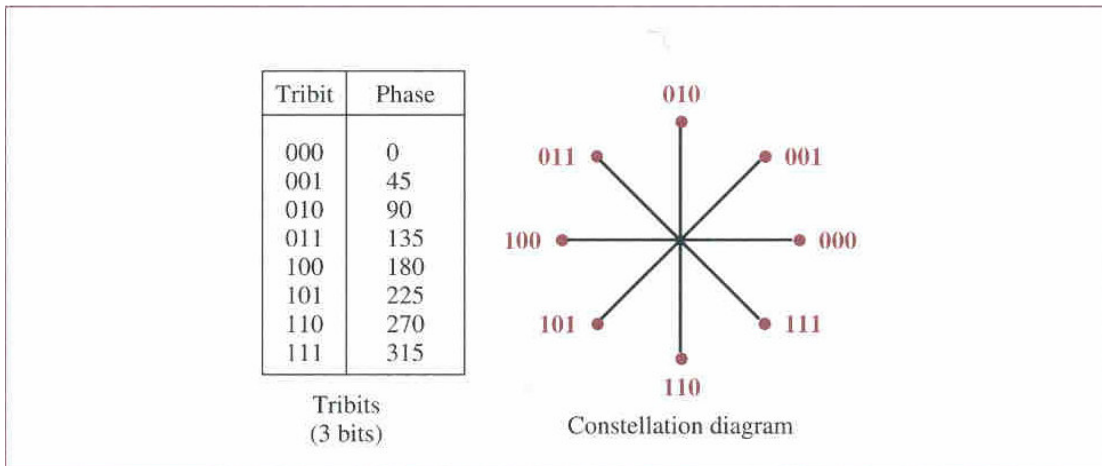


Рис. 5.33. Характеристики 8-PSK

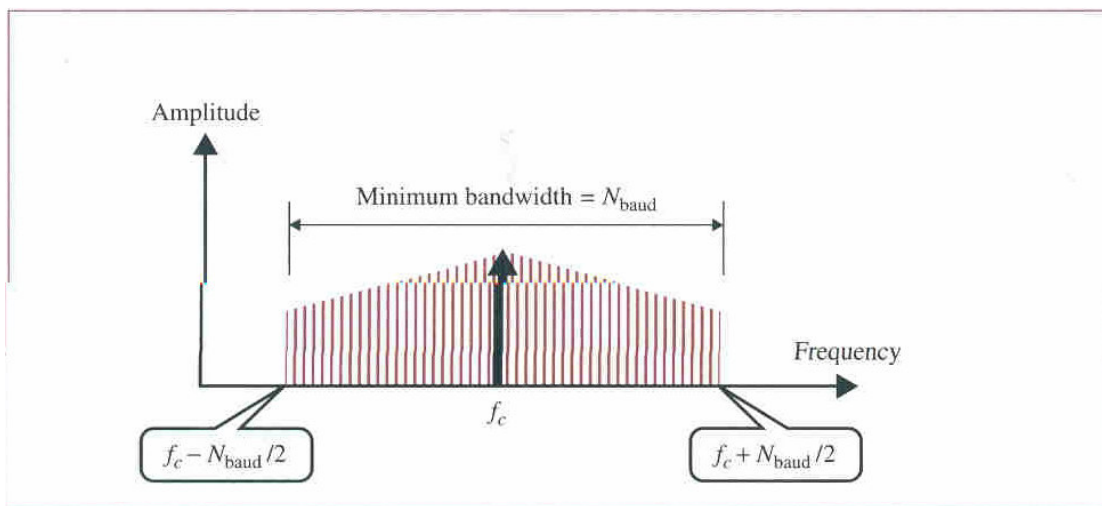


Рис. 5.34. Відношення між швидкістю передачі в бодах і пропускнуою смугою в PSK

Bandwidth для PSK

Мінімальна смуга пропускання, якої вимагається для передачі PSK, така сама, як ASK передачі – і з тих же причин. Оскільки ми бачили, максимальна швидкість передачі в бітах в передачі PSK, однак, є потенційно більша, ніж, ASK. Так, в той час, як максимальні швидкості в бодах ASK і PSK є тими ж для даної смуги пропускання, швидкості передачі в бітах PSK, які використовують ту ж смугу пропускання, можуть бути в два з лишнім рази більші (рис. 5.34).

Quadrature Amplitude Modulation (QAM)

PSK обмежується за допомогою здатності устаткування, щоб відрізнити невеликі різниці в фазі. Цей коефіцієнт обмежує потенційну швидкість передачі в бітах.

Досі, ми змінюємо тільки один трьох характеристик хвилі синуса в часі, а що буде, коли ми змінюємо два? Обмеження смуги пропускання роблять комбінації FSK з іншими змінами практично непотрібними. Але чому не об'єднують ASK і PSK? Тоді ми могли б мати відхилення x в фазі і відхилення y в амплітуді, надаючи нам можливі відхилення u x разів і відповідну кількість бітів за відхилення. Quadrature Amplitude Modulation (QAM) робить тільки те. Термінова квадратура розвивається обмеження, яких вимагається для мінімальної продуктивності і зв'язана з тригонометрією.

Можливі відхилення QAM є численними. Теоретично, будь-яка вимірна кількість змін в амплітуді може бути об'єднана з будь-якою вимірною кількістю змін в фазі. Рис. 5.35 показує дві можливі конфігурації, 4-QAM і 8-QAM. У обох випадках, кількість зсувів амплітуди є меншою, ніж кількість фазових зсувів. Через те, що зміни амплітуди є вразливими до завади і вимагають, щоб більші відмінності зсуву, ніж фазові зміни, кількість фазових зсувів, які використовуються за допомогою системи QAM є завжди більшою, ніж кількість зсувів амплітуди. Крива інтервалу часу, яка відповідає 8-QAM сигналу на рис. 5.35, показана на рис. 5.36.

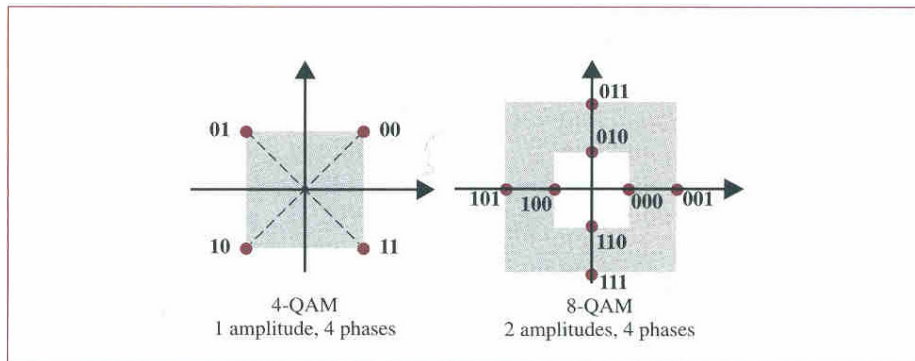


Рис. 5.35. 4-QAM сузір'я та 8-QAM

Інші геометричні зв'язки є також можливими. Три популярних 16-QAM конфігурацій показані на рис. 5.37. Перший приклад, три амплітуди і 12 фаз, завада описувачів, найкраща, через більше відношення фазового зсуву до амплітуди. Це є рекомендація ITU-T. Другий приклад, чотири амплітуди і вісім фаз, є рекомендацією OSI. Якщо ви досліджуєте діаграму старанно, ви помітите, що хоч це базується на концентричних кругах, не кожне пересічення фази і амплітуди використовується. Фактично, 4 разів 8 повинні дати 32 можливих відхилень. Але за допомогою використання тільки половини тих можливостей, вимірні відмінності між зсувами збільшуються і гарантується більша сигнальна читабельність. Крім того, окремі проекти QAM з'єднують специфічні амплітуди з специфічними фазами. Це означає, що навіть з проблемами завади, які асоціюються з переміщенням амплітуди, значення зсуву може оправитися від фазової інформації. Взагалі, таким чином, іншою перевагою QAM над ASK є нижча чутливість до завад.

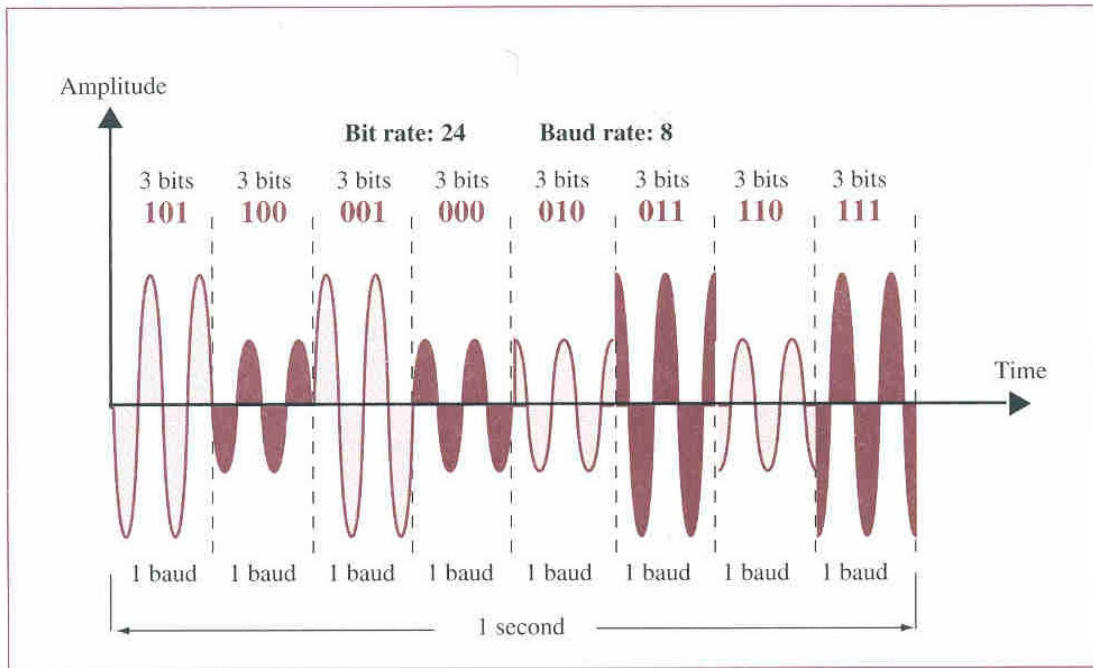


Рис. 5.36. Інтервал часу для сигналу S-QAM

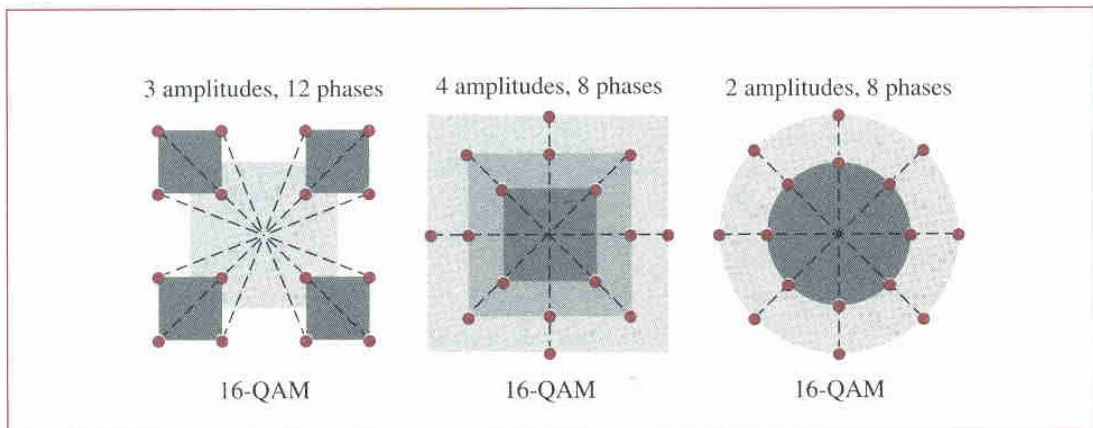


Рис. 5.37 16-QAM constellationx

Смуга пропускання для QAM

Мінімальна необхідна передача QAM для смуги пропускання так само, як вимагається для ASK і PSK передачі. QAM має ті ж переваги, що і PSK над ASK.

Бітове/Бодове порівняння

Допускаючи, що сигнал FSK телефонними голосовими лініями може послати 1200 бітів за секунду, швидкість передачі в бітах є 1200 bps. Кожний частотний зсув представляє поодиноким біт; так що це вимагає, щоб 1200 елементів цифрового сигналу послали 1200 бітів. Швидкість в бодах, таким чином, є також 1200 bps. Кожне сигнальне відхилення в 8-QAM системі, однак, представляє три біти. Так швидкість 1200 передачі в бітах bps, використання 8-QAM, має швидкість в бодах тільки 400. Оскільки на рис. 5.38 показується, система двобітової конфігурації має швидкість в бодах половину швидкості передачі в бітах, система tribit має швидкість в бодах на третину швидкості передачі в бітах, і система quadbit має швидкість в бодах на четвертину швидкості передачі в бітах.

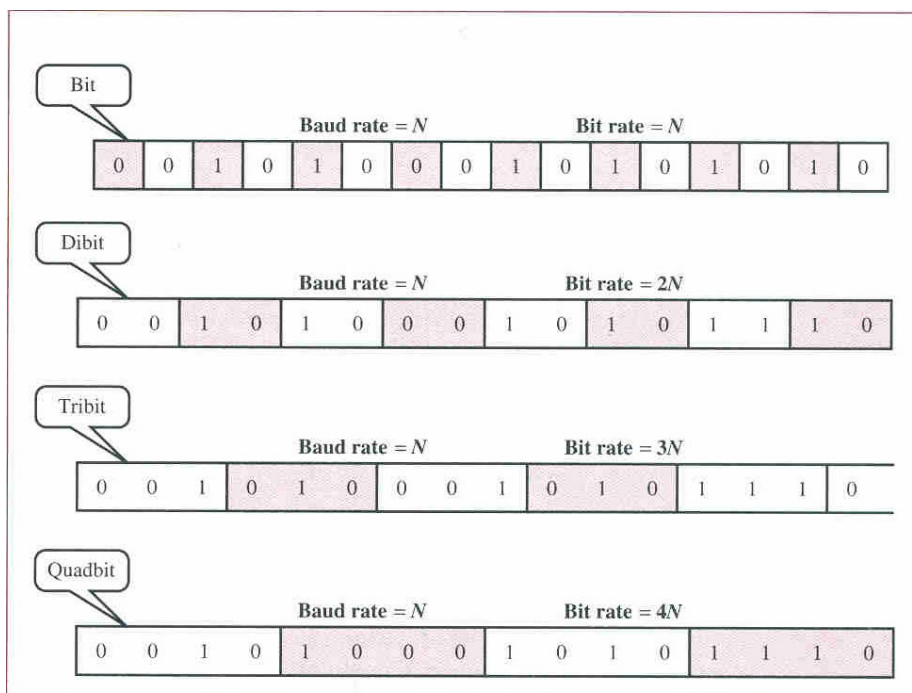


Рис. 5.38. Біт і смуга частот

Таблиця 5.1 показує порівняльний бітової і бодової швидкості для різних методів цифрово-аналогової модуляції.

Таблиця 5.1. Порівняння швидкості в бітах і бодах

Modulation	Units	Bits/Bau	Baud	Bit Rate
ASK FSK 2-PSK	Bit	1	N	N
4-PSK, 4-QAM	Dibit	2	N	2N
8-PSK, 8-QAM	Tribit	3	N	3N
16-QAM	Quadbit	4	N	4N
32-QAM	Pentabit	5	N	5N
64-QAM	Hexabit	6	N	6N
128-QAM	Septabit	7	N	7N
256-QAM	Octabit	8	N	8N

При амплітудній модуляції спектр складається із синусоїди несучої частоти f_c і двох бічних гармонік: $(f_c + f_t)$ і $(f_c - f_t)$ де f_t – частота зміни інформаційного параметра синусоїди, що збігається зі швидкістю передачі даних при використанні двох рівнів амплітуди (мал. 2.14, б). Частота f_t визначає пропускну здатність лінії при даному способі кодування. При невеликій частоті модуляції ширина спектра сигналу буде також невеликою (рівною $2f_t$), тому сигнали не будуть спотворюватися лінією, якщо її смуга пропускання буде чи більше дорівнює $2f_t$. Для каналу тональної частоти такий спосіб модуляції прийнятний при швидкості передачі даних не більше $3100/2=1550$ біт/с. Якщо ж для представлення даних використовуються 4 рівні амплітуди, то пропускну здатність каналу підвищується до 3100 біт/с.

При фазовій і частотній модуляції спектр сигналу виходить складнішим, чим при амплітудній модуляції, тому що бічних гармонік тут утвориться більше двох, але вони також симетрично розташовані щодо основної несучої частоти, а їх амплітуди швидко зменшуються. Тому ці види модуляції також добре підходять для передачі даних по каналу тональної частоти.

Для підвищення швидкості передачі даних використовують комбіновані методи модуляції. Найбільш розповсюдженими є методи квадратурної амплітудної модуляції (Quadrature Amplitude Modulation, QAM). Ці методи засновані на поєднанні фазової модуляції з 8 значеннями величин зрушення фази і амплітудної модуляції з 4 рівнями амплітуди. Однак з можливих 32 комбінацій сигналу використовуються далеко не всі.

Наприклад, у кодах Трелліса припустимі всього 6, 7 чи 8 комбінацій для представлення вихідних даних, а інші комбінації є забороненими. Така надмірність кодування потрібно для розпізнавання модемом помилкових сигналів, що є наслідком перекручувань через перешкоди, що на телефонних каналах, комутирува особливо, дуже значні по амплітуді і тривалі за часом.

Цифрове кодування

При цифровому кодуванні дискретної інформації застосовують потенційні та імпульсні коди.

У потенційних кодах для представлення логічних одиниць і нулів використовується тільки значення потенціалу сигналу, а його перепади, що формують закінчені імпульси, до уваги не приймаються. Імпульсні коди дозволяють представити двійкові дані або імпульсами визначеної полярності, або частиною імпульсу – перепадом потенціалу визначеного напрямку.

Вимоги до методів цифрового кодування

При використанні прямокутних імпульсів для передачі дискретної інформації необхідно вибрати такий спосіб кодування, що одночасно досягав би декількох цілей:

- мав при одній і тій же бітовій швидкості найменшу ширину спектра результуючого сигналу;
- забезпечував синхронізацію між передавачем і приймачем;
- мав здатність розпізнавати помилки;
- мав низьку вартість реалізації.

5.5. Аналогова модуляція

При передачі дискретних даних по каналах зв'язку застосовуються два основних типи фізичного кодування – на основі синусоїдального несучого сигналу і на основі послідовності прямокутних імпульсів. Перший спосіб

часто називається також модуляцією чи аналоговою модуляцією, підкреслюючи той факт, що кодування здійснюється за рахунок зміни параметрів аналогового сигналу. Другий спосіб звичайно називають цифровим кодуванням. Ці способи відрізняються шириною спектру результуючого сигналу і складністю апаратури, необхідної для їх реалізації.

При використанні прямокутних імпульсів спектр результуючого сигналу виходить дуже широким. Це не дивно, якщо згадати, що спектр ідеального імпульсу має нескінченну ширину. Застосування синусоїди приводить до спектра набагато меншої ширини при тій же швидкості передачі інформації. Однак для реалізації синусоїдальної модуляції потрібно складніша і дорожча апаратура, ніж для реалізації прямокутних імпульсів.

В даний час все частіше дані, що початково мають аналогову форму – мова, телевізійне зображення, – передаються по каналах зв'язку в дискретному вигляді, тобто у вигляді послідовності одиниць і нулів. Процес представлення аналогової інформації в дискретній формі називається дискретною модуляцією. Терміни "модуляція" і "кодування" часто використовують як синоніми.

Аналогова модуляція застосовується для передачі дискретних даних по каналах з вузькою смугою частот, типовим представником яких є канал тональної частоти, наданий у розпорядження користувачам публичних телефонних мереж. Типова амплітудно-частотна характеристика каналу тональної частоти представлена на рис. 2.12. Цей канал передає частоти в діапазоні від 300 до 3400 Гц, таким чином, його смуга пропускання дорівнює 3100 Гц. Хоча людський голос має набагато ширший спектр – приблизно від 100 Гц до 10 кгц, – для прийнятної якості передачі мови діапазон у 3100 Гц є гарним рішенням. Строге обмеження смуги пропускання тонального каналу зв'язано з використанням апаратури ущільнення і комутації каналів у телефонних мережах.

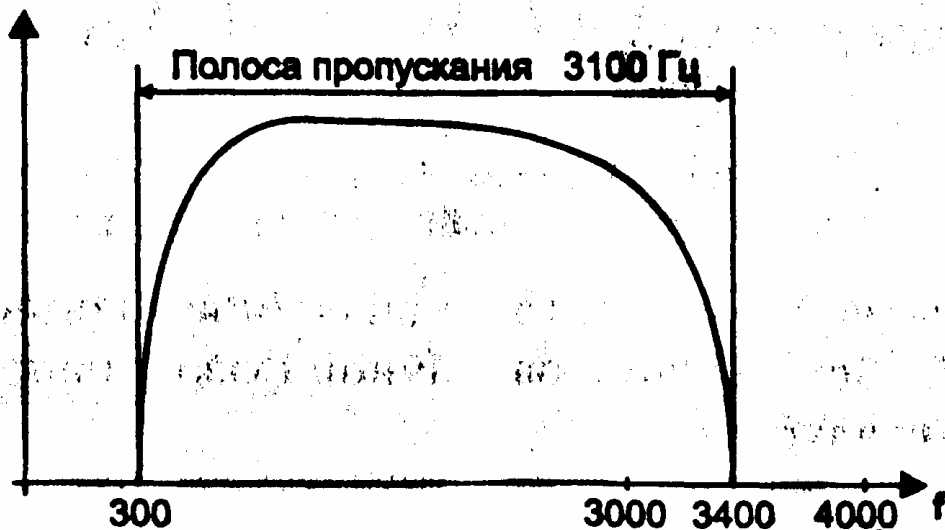


Рис. 2.12. Амплітудно-частотна характеристика каналу тональної частоти

Методи передачі дискретних даних на фізичному рівні

Пристрій, що виконує функції модуляції несучої синусоїди на стороні передавача і демодуляції на прийомній стороні, називається модем (модулятор-демодулятор).

Методи аналогової модуляції

Аналогова модуляція є таким способом фізичного кодування, при якому інформація кодується зміною амплітуди, частоти чи фази синусоїдального сигналу несучої частоти. Основні способи аналогової модуляції показані на рис. 2.13. На діаграмі (рис. 2.13, а) показана послідовність бітів вихідної інформації, представлена потенціалами високого рівня для логічної одиниці і потенціалом нульового рівня для логічного нуля. Такий спосіб кодування називається потенційним кодом, що часто використовується при передачі даних між блоками комп'ютера.

При амплітудній модуляції (рис. 2.13, б) для логічної одиниці вибирається один рівень амплітуди синусоїди несучої частоти, а для логічного нуля — іншої. Цей спосіб рідко використовується в чистому виді на

практиці через низьку завадостійкість, але часто застосовується в поєднанні з іншим видом модуляції – фазовою модуляцією.

При частотній модуляції (рис. 2.13, в) значення 0 і 1 вихідних даних передаються синусоїдами з різною частотою. Цей спосіб модуляції не вимагає складних схем у модемах і звичайно застосовується в низькошвидкісних модемах, що працюють на швидкостях 300 чи 1200 біт/с.



Рис. 2.13. Різні типи модуляції

При фазовій модуляції (рис. 2.13, г) значенням даних 0 і 1 відповідають сигнали однакової частоти, але з різною фазою, наприклад 0 і 180 градусів чи 0,90,180 і 270 градусів.

У швидкісних модемах часто використовуються комбіновані методи модуляції, як правило, амплітудна в поєднанні з фазовою.

Аналого-аналогове перетворення

Аналого-аналогове перетворення є зображення аналогової інформації за допомогою аналогового каналу. Радіо є прикладом аналого-аналогового

зв'язку. Рис. 5.39 показує зв'язок між аналоговою інформацією, апаратними засобами аналогового перетворення, і аналоговим каналом рівнодіючої сили.

Аналого-аналогова модуляція може бути виконана трьома шляхами: амплітудна модуляція (АМ), частотна модуляція (FM), і фазова модуляція (PM). Рис 5.40.

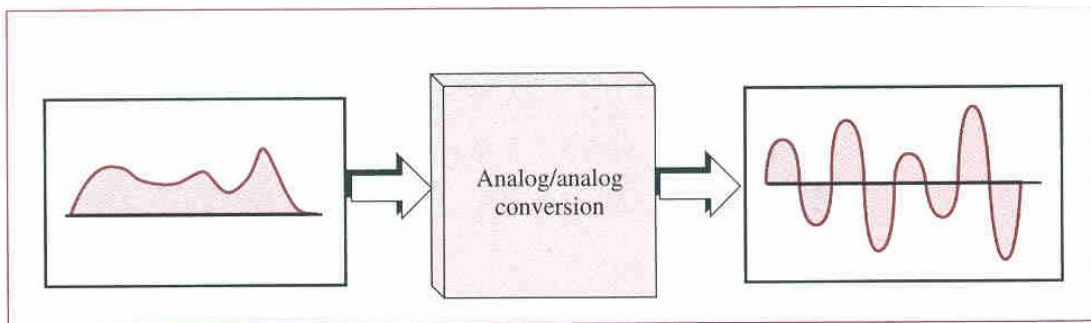


Рис. 5.39. Аналого-аналогова модуляція

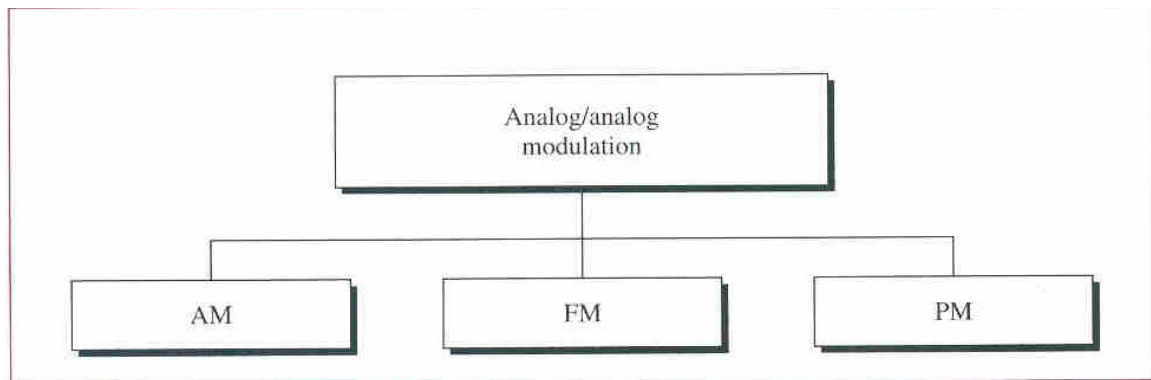


Рис. 5.40. Типи аналого-аналогової модуляції

Амплітудна модуляція (АМ)

Всередині АМ передача, сигнал носія модулюється так, щоб амплітуда змінилася з амплітудами зміни сигналу модулювання. Частота і фаза носія залишаються тією ж: тільки амплітуда змінюється, щоб співпадати з відхиленням в інформації. На рис. 5.41 показана робота цього принципу. Сигнал модулювання стає конвертом носія.

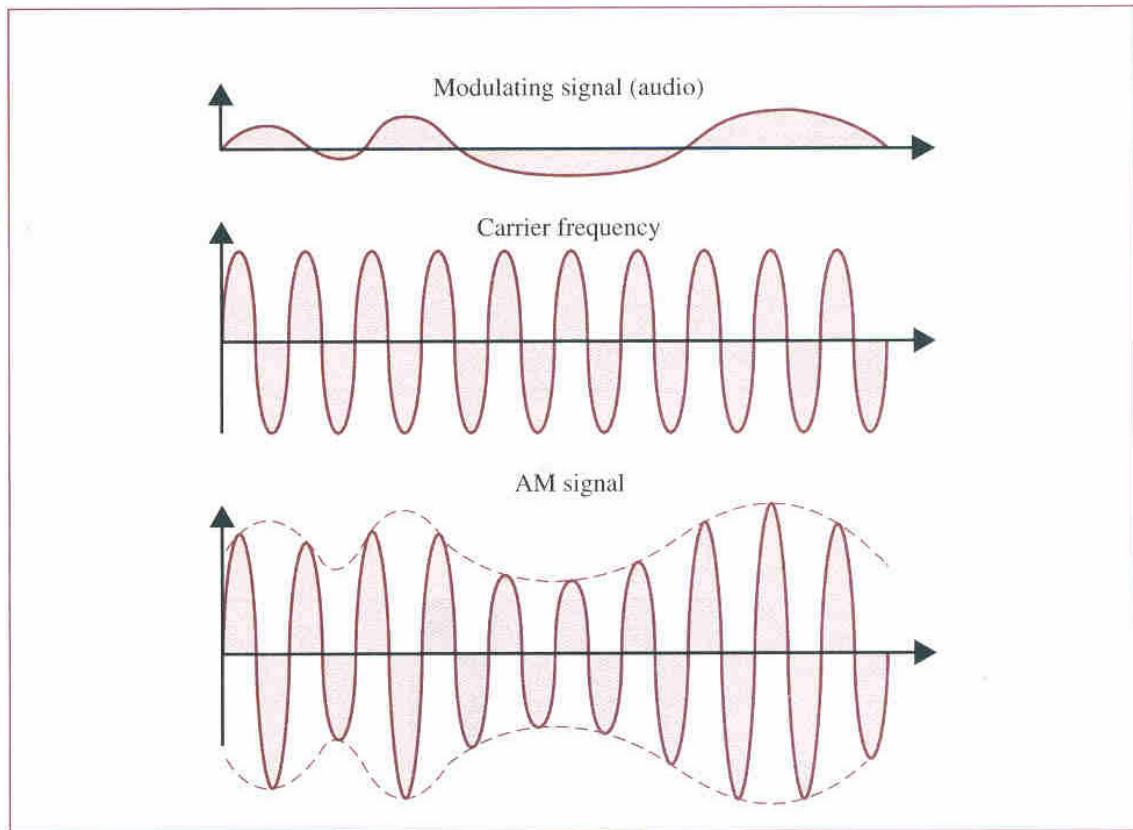


Рис. 5.41. Амплітудна модуляція

Сму́га пропускання АМ

Сму́га пропускання АМ сигнал є рівним подвійній смузі пропускання сигналу модулювання і покриває область, яка центрується навколо частоти (рис. 5.42). Затінена частина діаграми є частотним спектром сигналу.

Сму́га пропускання звукового сигналу (мова і музика) є звичайно 5 КHz. Таким чином, АМ радіостанція потребує мінімальної смуги пропускання 10 КHz. Фактично стандарт FCC дозволяє 10 КHz кожній АМ станції.

АМ станції дозволяються частоти носія між 530 і 1700 КHz (1.7 MHz). Однак, кожна частота носія станції повинна бути розділена з обох сторін щонайменше на 10 КHz (одна сму́га пропускання АМ), щоб уникнути перешкод. Якщо одна станція використовує частоту носія 1100 КHz, наступна частота станції не може бути нижча, ніж 1110 КHz (рис. 5.43).

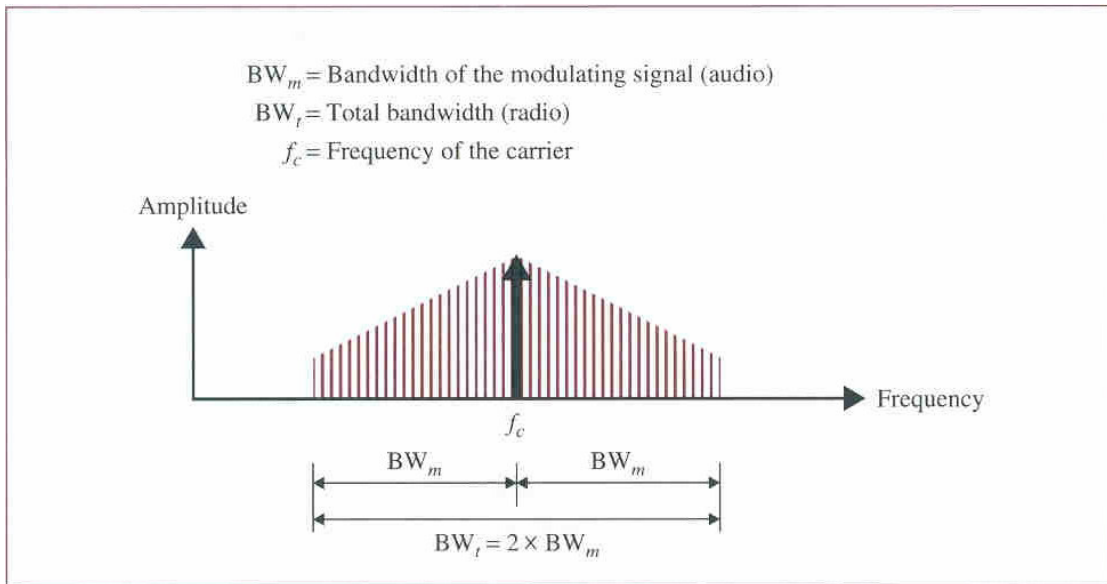


Рис. 5.42. Смуга пропускання АМ

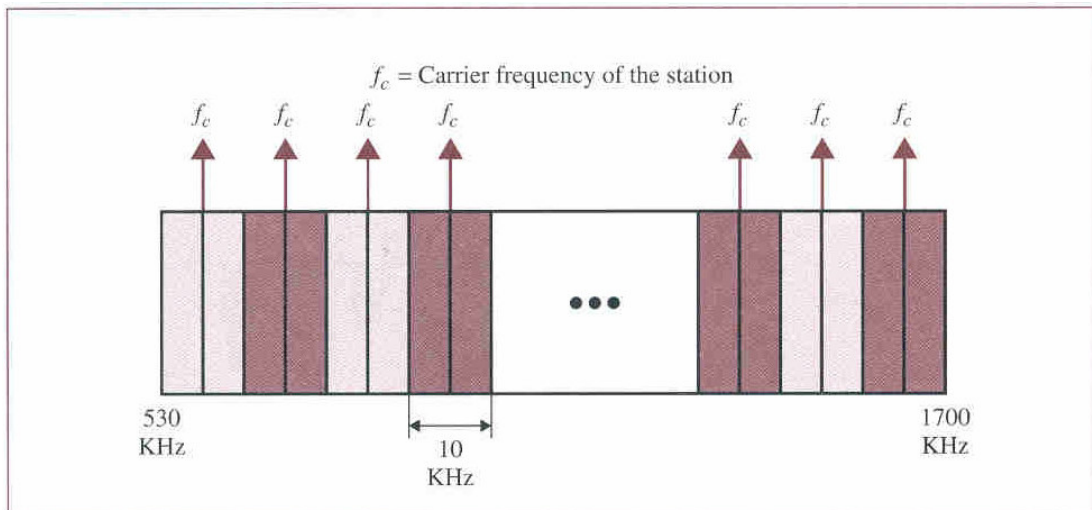


Рис. 5.43. Розподіл смуги частот АМ

Частотна Модуляція (FM)

У передачі FM, частота сигналу носія модулюється, щоб слідувати рівню (амплітуді) напруги зміни сигналу модулювання. Амплітуда піку і фаза константи сигнального залишку носія, але, як амплітуда інформаційних сигнальних змін, частота носія змінюється відповідно. Рис. 5.44 показує зв'язки модулювання сигналу носія, і сигналу FM рівнодіючої сили.

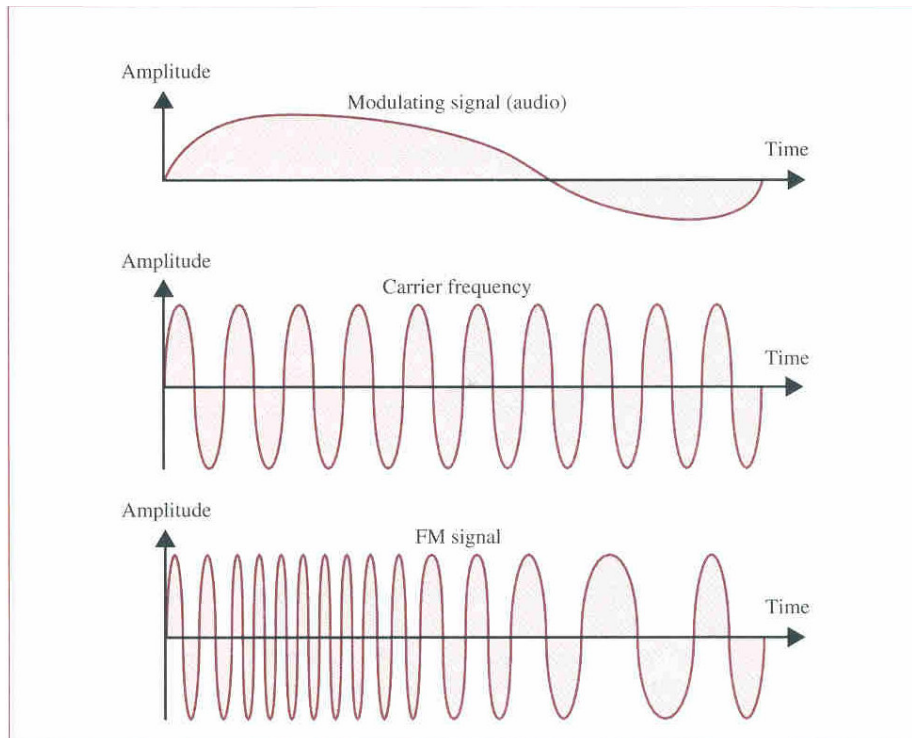


Рис. 5.44. Частотна модуляція

Смуга пропускання FM

Смуга пропускання сигналу FM є рівною до 10 разів смуги пропускання сигналу модулювання і, подібно смузі пропускання AM, покриває область, яка центрується навколо частоти носія. Рис. 5.45 показує як смугу пропускання, так і, в затіненій частині, частотний спектр сигналу FM.

Смуга пропускання звукових сигналів (мова і музика) передачі в stereo є майже 15 KHz. Кожна радіо станція FM, таким чином, потребує мінімальної смуги пропускання 150 KHz. FCC дозволяє 200 KHz (0.2 MHz) для кожної станції, щоб надати деяке місце для країв смуг частот.

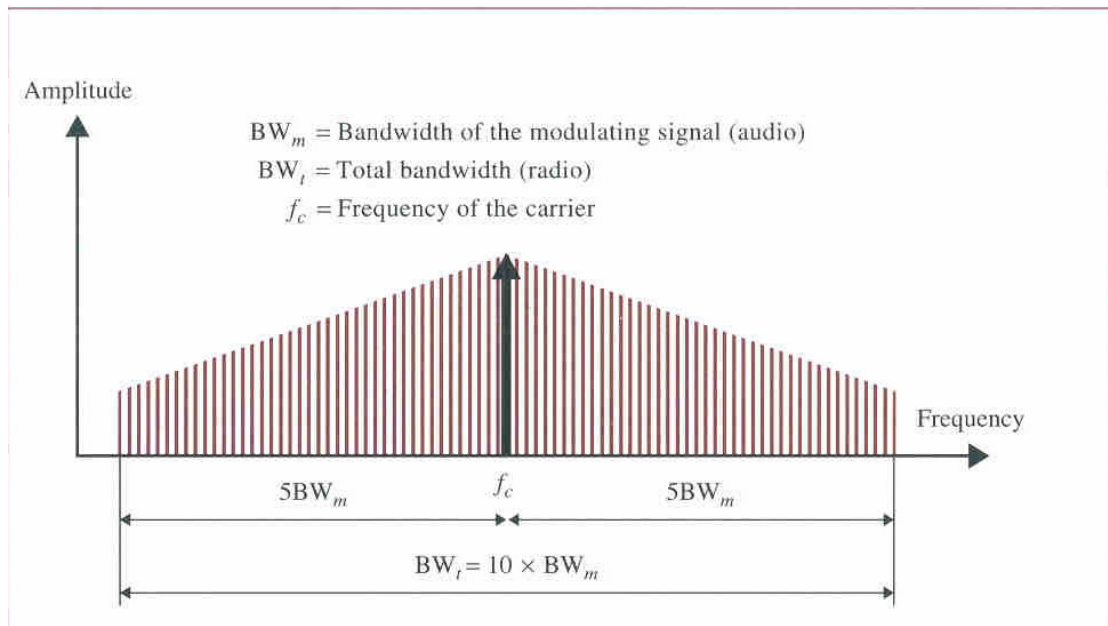


Рис. 5.45. Смуга пропускання FM

Станції FM дозволяються частоти між 88 і 108 МГц. Станції повинні бути розділені на щонайменше 200 КГц, щоб утримати їх смугу пропускання від перекриття. Щоб створити навіть більшу якість, FCC вимагає, що в даній області, можуть використовуватися тільки змінні розподіли смуги пропускання. Інші залишаються невикористаними, щоб запобігти будь-якій можливості одночасного прийому двох станцій разом. Даний діапазон з 88 до 108 МГц, як область, є 100 потенційною смугою пропускання FM в області, яких 50 може діяти в будь-який момент. Рис. 5.46 ілюструє цей принцип.

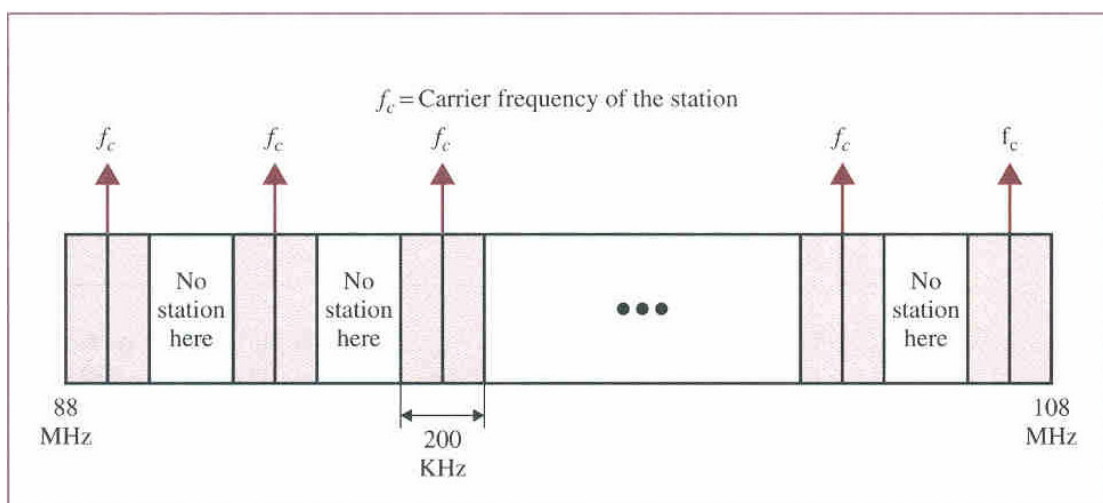


Рис. 5.26. Розподіл смуги частот FM

Фазова Модуляція (PM)

Завдяки простішим вимогам апаратних засобів, фазова модуляція (PM) використовується в деяких системах, як альтернативна частотній модуляції. У передачі PM, фаза сигналу носія модулюється, щоб слідувати рівню (амплітуді) напруги зміни сигналу модулювання. Амплітуда піку і частота сигналу носія зберігають константу, але, як амплітуда інформаційних сигнальних змін, фаза носія відповідно змінюється. Аналіз і кінцевий результат (модульований сигнал) є подібним до тих частотній модуляції.

Тема 6. Інтерфейси і модеми

6.1. Передача цифрових даних

6.2. Інтерфейс DTE-DCE

6.3. Інші стандарти інтерфейсу

6.4. Модеми

6.5. Модеми 56К

Ми вже здійснювали кодування інформації у формат для передачі, наступним кроком є дослідження самого процесу передачі. Пристрої обробки інформації генерують закодовані сигнали і зазвичай потребують підтримки для передачі їх по комунікаційним лініям. Наприклад, РС генерує цифровий сигнал, але потребує додаткового пристрою, щоб модулювати несучу частоту перед тим, як послати його телефонною лінією. Як буде здійснюватися передача закодованих даних від генеруючого пристрою до наступного пристрою? Відповідь лежить в основі поняття *інтерфейс*, який являє собою сукупність ліній зв'язку.

Так як інтерфейс зв'язує два пристрої, що не обов'язково виготовлені одним і тим самим виробником, то повинні бути наперед визначені характеристики та стандарти інтерфейсу. Характеристики інтерфейсу включають його технічні специфікації (скільки ліній зв'язку використовується для передачі сигналу), електричні специфікації (частота, амплітуда, і фаза очікуваного сигналу), і його функціональні описи. Ці характеристики цілком описуються деякими популярними стандартами і впроваджені у фізичний рівень моделі OSI.

6.1. Передача цифрових даних

Першочерговою задачею при розгляді питання передачі даних від одного пристрою до іншого є передавання лініями зв'язку, і основною задачею при

розгляді питання передавання – це потік даних. Чи посилати один біт за одиницю часу, чи групувати біти в більші групи і якщо так, то як? Передача двійкових даних через лінії зв'язку може здійснюватися або в паралельному режимі або послідовному. В паралельному режимі багато бітів посилаються з кожним синхронізуючим сигналом. В послідовному режимі один біт передається з кожним синхронізуючим сигналом. Є тільки один метод паралельної передачі даних і два методи серійної передачі: синхронний і асинхронний (див. рис. 6.1).

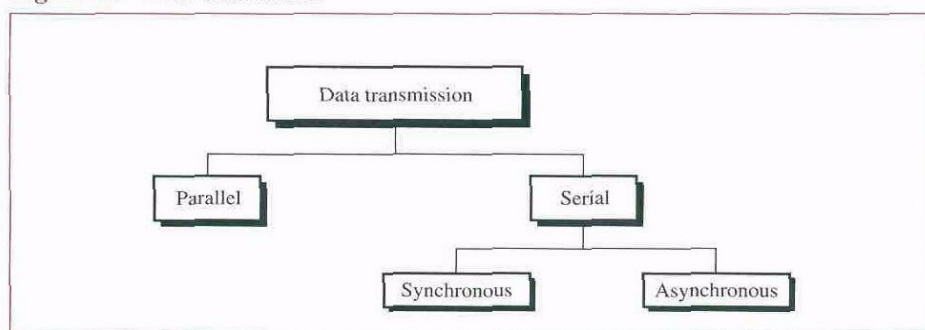


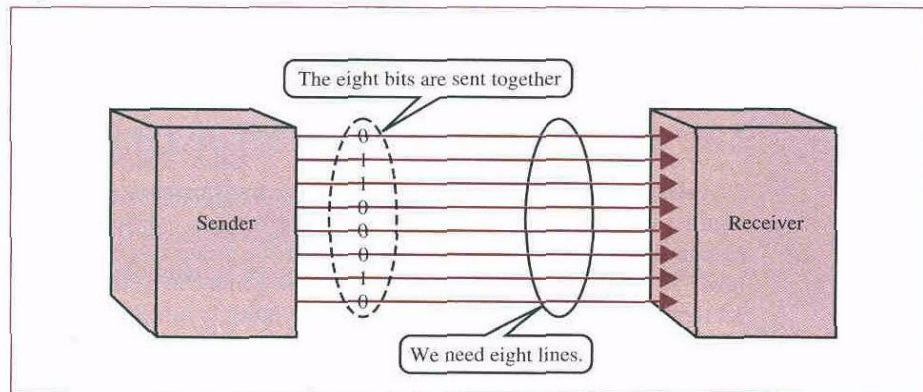
Рис. 6.1 Методи передачі даних

Паралельна передача

Двійкові дані, що складаються з 0 або 1, можуть бути організовані в групи по n бітів в кожній. Комп'ютери переважно маніпулюють певними групами даних, так як і ми спілкуємося словами, а не буквами. За допомогою групування, ми можемо послати n біт за одиницю часу замість одного. Це називається паралельною передачею.

Механізм паралельної передачі концептуально простий: використовується n ліній для передачі n бітів за одиницю часу. Таким чином, кожний біт має свою власну лінію, і всі n бітів однієї групи можуть передаватися з кожним синхронізуючим сигналом від одного пристрою до іншого. Рис. 6.2 показує, як працює паралельна передача для $n = 8$. Зазвичай, вісім ліній поєднуються в одному кабелі з конектором на кожному кінці.

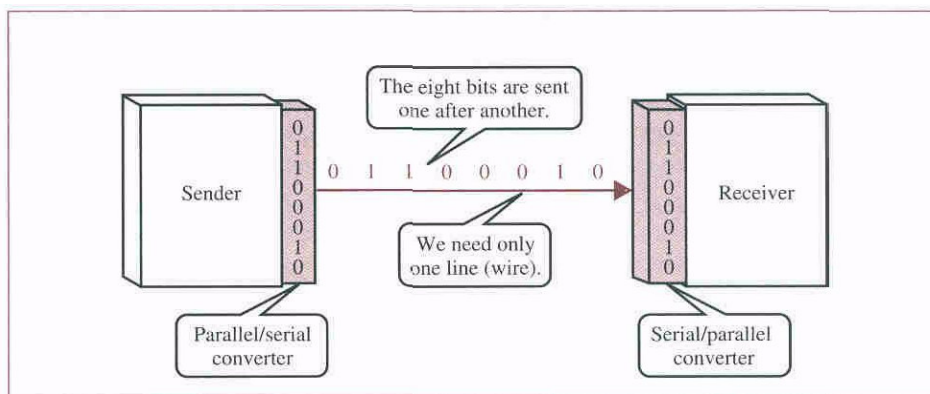
Figure 6.2 Parallel transmission



Перевага паралельної передачі - це швидкість. Паралельна передача може збільшити швидкість передачі в n разів у порівнянні з послідовною. Але є істотний недолік – вартість. Паралельна передача вимагає n ліній зв'язку тільки для того, щоб передати потік даних. Так як це дорого, то паралельна передача переважно обмежується короткими дистанціями.

Послідовна передача

В послідовній передачі один біт передається за іншим, так що потрібен тільки один канал зв'язку а не n для передачі даних між двома пристроями комунікації (див. рис. 6.3).



Перевага послідовної передачі над паралельною – потрібен тільки один канал зв'язку, тому вартість послідовної передачі відносно паралельної скорочується в n разів.

Оскільки комунікація в межах пристроїв є паралельною, то в інтерфейсі потрібні пристрої конвертації між відправником і лінією (з паралельного до послідовного) і між лінією і одержувачем (з послідовного до паралельного).

Послідовна передача здійснюється в двох режимах: асинхронний або синхронний.

Асинхронна передача

Асинхронна передача названа так, тому що непотрібен таймінг сигналу. Натомість інформація отримується і перетворюється погоджувальними шаблонами. Поки передаються ці шаблони пристрій-одержувач може зчитувати інформацію незважаючи на ритм, в якому здійснюється передача. Шаблони засновані на групуванні бітового потоку в байти. Кожна група (вісім бітів) передається по лінії як окрема одиниця. Система передачі посилає кожну групу незалежно як тільки вона готова, незважаючи на таймер.

Без імпульсу синхронізації одержувач не може використовувати таймінг, щоб передбачити, коли прийде наступна група. Щоб повідомити одержувач про прибуття нової групи, на початок кожного байта додається додатковий біт. Цей біт, зазвичай рівний 0, називається стартовим бітом. Щоб повідомити одержувача, що досягнуто кінця байта, один або більше додаткових бітів додаються до кінця байта. Ці біти, зазвичай рівні 1, називаються стоповими бітами. Отже, кожний байт збільшується в розмірі до 10 бітів як мінімум, з якого 8 - це інформація і 2 або більше - це сигнали одержувачу. Крім того, за передачею кожного байта може слідувати пауза - часовий інтервал змінної тривалості. Ця пауза може бути заповнена потоком

додаткових стопових бітів.

Стартові і стопові біти, а також пауза повідомляють одержувача про початок і кінець кожного байта і дозволяють йому синхронізуватися з потоком даних. Цей механізм називається асинхронним, тому що на рівні байтів відправник і одержувач не повинні синхронізуватися. Але в межах кожного байту одержувач повинен синхронізуватися з потоком даних. Тобто, деяка синхронізація потрібна, але тільки для тривалості окремого байту. Пристрій отримання ресинхронізується на початку кожного нового байта. Коли одержувач знаходить стартовий біт, то він встановлює таймер і починає перерахунок бітів в порядку їх надходження. Після n бітів одержувач шукає стоповий біт. Як тільки він знаходить стоповий біт, він нехтує будь-якими прийнятими імпульсами поки не знайде наступний стартовий біт.

Рис. 6.4 – це схематична ілюстрація асинхронної передачі. У цьому прикладі стартові біти рівні 0, стопові біти – 1, паузу зображено пустим часовим інтервалом, а не додатковими стоповими бітами.

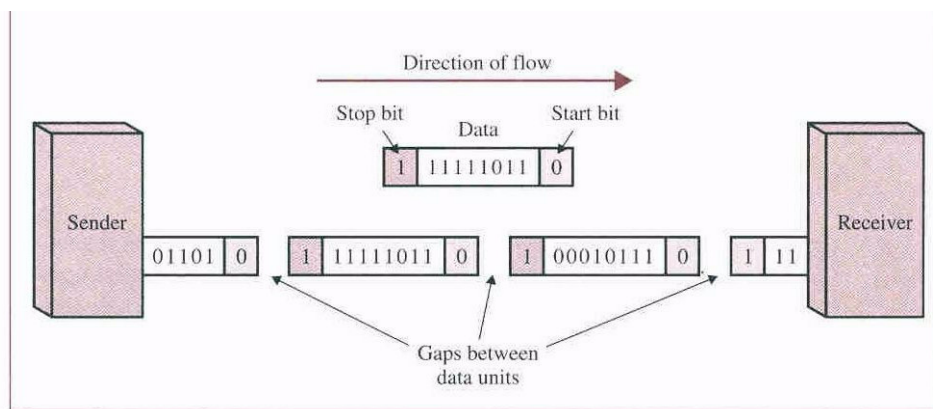


Рис. 6.4 Схема асинхронної передачі

Додавання стопових і стартових бітів і вставка пауз в бітовий потік роблять асинхронну передачу повільнішою, ніж інші форми передачі, що можуть функціонувати без додавання контрольної інформації. Але це дешево і ефективно, і ці дві переваги роблять її привабливим вибором для ситуацій

низькошвидкісної комунікації. Наприклад, під'єднання терміналу до комп'ютера – це типове застосування для асинхронної передачі. Користувач друкує тільки один символ за одиницю часу і в термінах обробки даних робить це надзвичайно повільно, залишаючи непередбачувані паузи часу між символами.

Синхронна передача

В синхронній передачі бітовий потік з'єднаний в більш довгі “фрейми”, які можуть містити багато байтів. Кожний байт, проте, подається на передачу без паузи між собою і наступним байтом. На одержувача покладається функція виділення байтів із бітового потоку з метою декодування. Іншими словами, дані передаються у вигляді неперервної стрічки 1 і 0, а одержувач виділяє з цієї стрічки окремі байти або символи, намагаючись відновити інформацію.

Рис. 6.5 надає схематичну ілюстрацію синхронної передачі. На рис. вказано межі між байтами. Фактично, ці межі не існують; відправник формує свої дані як одну довгу стрічку. Якщо відправник хоче відправити дані порціями, то паузи між цими порціями повинні наповнюватися спеціальною послідовністю. Одержувач перераховує біти в порядку їх надходження і групує їх.

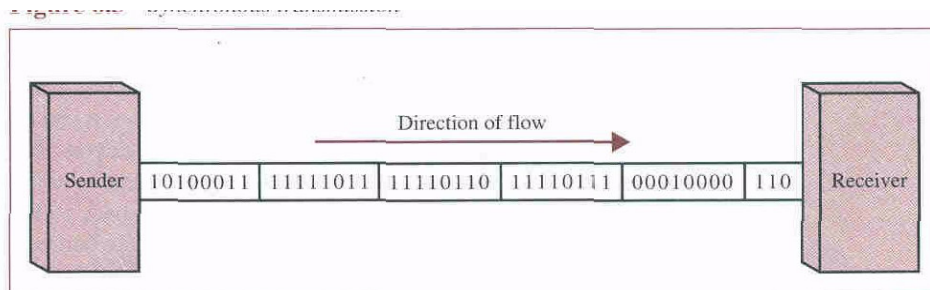


Рис. 6.5 Схема синхронної передачі

Без пауз і стартових/стопових бітів немає ніякого вбудованого

механізму, щоб допомогти одержувачу регулювати свою бітову синхронізацію всередині потоку. Тому стає дуже важливим таймінг, тому що точність прийнятої інформації залежить повністю від здатності пристрою-одержувача точно підраховувати біти, що надходять.

Перевага синхронної передачі - це швидкість. Без додаткових бітів та пауз, які потрібно вставляти на початку передачі і забирати вкінці, синхронна передача працює швидше, ніж асинхронна. З цієї причини вона більше підходить для високошвидкісних застосувань як, наприклад, передача даних від одного комп'ютера до іншого. Синхронізація байтів реалізована на каналному рівні.

6.2. Інтерфейс DTE-DCE

Потрібно прояснити дві терміни, які є важливими для комп'ютерних мереж: data terminal equipment (DTE) і data circuit-terminating equipment (DCE). Існують чотири базові функціональні одиниці для комунікацію даними: DTE і DCE на одному кінці і DCE і DTE на іншому, як показано на рис. 6.6.

DTE генерує дані і передає їх разом з необхідними управляючими символами до DCE. DCE перетворює сигнал у відповідний формат для передачі і поміщає сигнал в лінію зв'язку. Коли сигнал досягає одержувача, цей процес повторяється у зворотньому порядку.

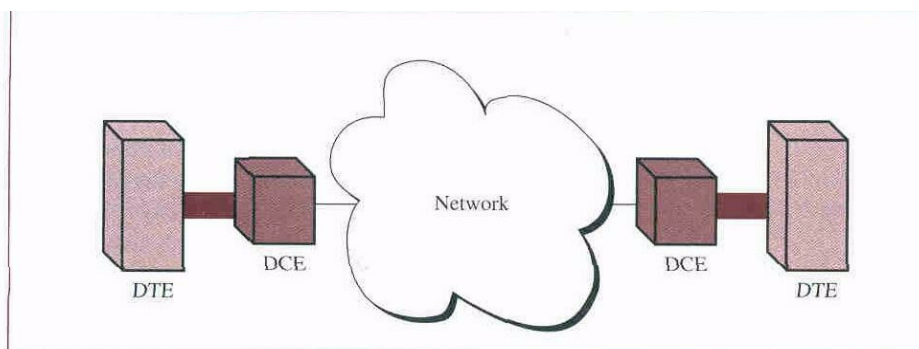


Рис. 6.6 DTE і DCE

DTE

DTE включає будь-яку одиницю, яка функціонує або як джерело, або як місце призначення при передачі двійкових цифрових даних. На фізичному рівні це може бути термінал, мікроком'ютер, комп'ютер, принтер, факс, або будь-який інший пристрій що генерує або отримує числові дані. DTE часто не комунікують безпосередньо один з одним; вони генерують і поглинають інформацію і потребують посередника, який би зв'язував їх. Уявіть собі, що DTE працює як ваш мозок, коли ви розмовляєте. Якщо ви маєте ідею, то ви хочете повідомити про це іншій людині. Ваш мозок створює ідею, але не може сам передавати її до мозку іншої людини. Але нажаль або на щастя, ми не вміємо читати думки. Натомість наш мозок передає ідею за допомогою голосових зв'язок, які здатні генерувати звукові хвилі, що передаються через повітря або телефонну лінію до вуха іншої людини і звідти до її мозку, де голосовий сигнал конвертується в інформацію.

В цій моделі, ваш мозок і мозок іншої людини – це DTE. Ваші голосові зв'язки – це DCE. Ваше вухо або вухо іншої людини – це також DCE. Повітря або телефонний дріт – це середовище передачі.

DCE

DCE включає будь-який функціональний пристрій, який передає або одержує дані у формі аналогового або цифрового сигналу через мережу. На фізичному рівні DCE бере дані, що генеруються за допомогою DTE, перетворює їх на відповідний сигнал, а потім поміщає сигнал в лінію зв'язку. Загалом DCE, що функціонують на цьому рівні, включають модеми (модулятори/демодулятори, які розглядаються в підрозділі 6.4). В будь-якій мережі DTE генерує цифрові дані і передає їх до DCE; DCE перетворює дані у форму, прийнятну для засобу передачі, і посилає конвертований сигнал іншому DCE у мережі. Другий DCE отримує сигнал, перетворює його у

форму, прийнятну для DTE і доставляє йому. Щоб зробити можливими як пересилку, так і отримання, DCE повинні використовувати той же самий метод модуляції (наприклад, FSK), що дуже схоже на ситуацію: коли ви хочете поговорити з кимось, хто розуміє тільки японську мову, ви повинні спілкуватися японською. Два DTE не повинні координуватися одним з одним, але кожний повинен координуватися з його власний DCE, а DCE повинні співпрацювати таким чином, щоб перетворення даних відбувалося без втрати їх цілісності.

Стандарти

За ці роки було розроблено багато стандартів, щоб визначити зв'язок між DTE і DCE (див. рис. 6.7). Хоча вони і відрізняються один від одного, але кожний з стандартів забезпечує модель для технічних, електричних і функціональних особливостей зв'язку.

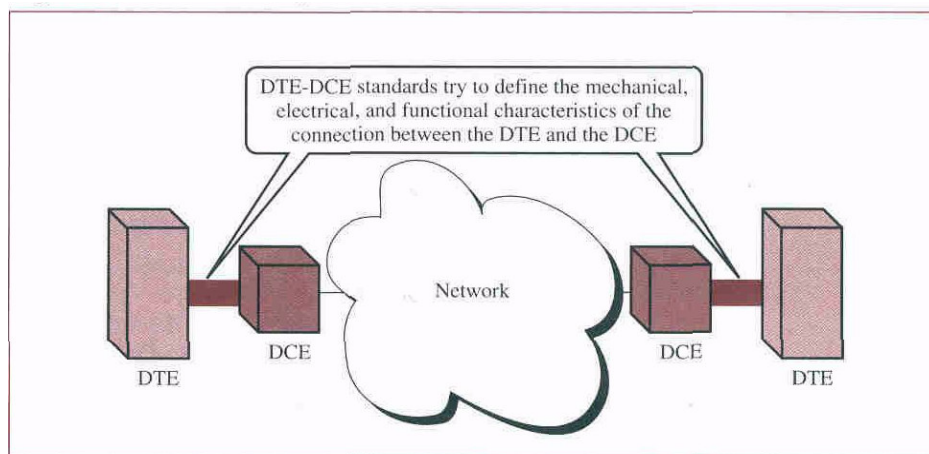


Рис. 6.7 Інтерфейс DTE-DCE

Організації, залучені в найактивніші стандарти інтерфейсу DTE-DCE, – це EIA і ITU-T. Стандарти EIA: EIA-232, EIA-442, EIA-449, і так далі. ITU-T стандарти були названі V і X серією.

Інтерфейс EIA-232

Один з найважливіших стандартів інтерфейсу, що розробляється EIA, – це EIA-232, який визначає технічні, електричні, і функціональні особливості інтерфейсу між DTE і DCE. Випущений в 1962 як стандарт RS-232, він з часом поновлювався. Сама остання версія, EIA-232-D, визначає не тільки тип конекторів, які використовуються, але і специфічний кабель, і пробки, і функціональність кожно піна.

Технічна специфікація

Технічна специфікація стандарту EIA-232 визначає інтерфейс як 25-дротовий кабель із конектором DB-25. Довжина кабелю не може перевищувати 15 метрів.

Конектор DB-25 - це пробка з 25 голками або слотами, кожний з яких був приєднаний до єдиної лінії із специфічною функцією.

За цим проектом, EIA створив можливість 25 окремих взаємодій між DTE і DCE. На практиці фактично використовуються менше, але стандарт дозволяє майбутнє включення функціональності.

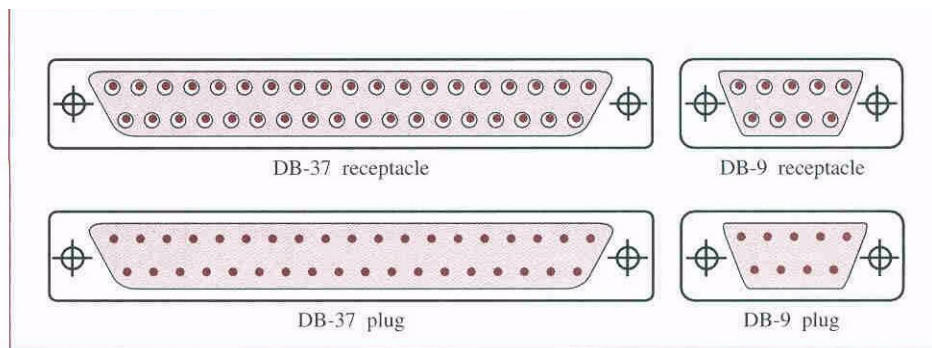
EIA-232 веде до 25-дротяного кабелю, Конектор терміну звертається до пробки з кожною лінією в кабелі, що з'єднується з голкою. З'єднувач терміну звертається до вмістища з кожною лінією в кабелі, що з'єднується з металевим машинним маслом, або футляром. В з'єднувачі DB-25, ці голки і надають трубчасту форму організовані в двох рядах, з 13 на верху і 12 на низу.

Оскільки ми подивимося в наступній секції, інша реалізація EIA-232 використовує 9-дротяний кабель з шпильковим з'єднувачем DB-9, приєднаним, щоб також закінчити.

6.3. Інші стандарти інтерфейсу

Як норма даних, так і кабельна довжина (сигнальна здатність дистанції) обмежуються EIA-232: швидкість передач даних до 20 Kbps і кабельній довжині до 50 ступень (15 метри). Щоб відповідати потребам користувачів, які вимагають більшої швидкості та/або дистанції EIA і 1TU-T ввели доповнюючі стандарти EIA-449, EIA-530, і X.21.

Механічні специфікації EIA-449 визначають комбінацію двох з'єднувачів: один із 37 пальчиками (DB-37) і один з 9 пальчиками (DB-9), для з'єднаних 46 пальчиків (рис. 6.15).



Функціональні описи EIA-449 надають подібних пальчикових властивостей DB-37 з DB-25. Головна функціональна різниця між 25- і 37-пальчиковими з'єднувачами - це те, що всі функції, що стосуються повторного каналу, були видалені з DB-37. Тому що повторний канал рідко використовується EIA-449 відділяє ті функції і поміщає їх в другому, 9-пальчиковому з'єднувачі (DB-9). Таким чином, другий канал доступний системам, які потребують цього.

Пальчикові Функції DB-37

Щоб підтримувати взаємозамінність з EIA-232, EIA-449 визначає дві категорії пальчиків, які використовуються в обміні даних, елемент управління, і таймінг інформацію (Табл. 6.1).

Таблиця 6.1. Пальчики DB-37

<i>Pin</i>	<i>Function</i>	<i>Category</i>	<i>Pin</i>	<i>Function</i>	<i>Category</i>
1	Shield		20	Receive Common	II
2	Signal rate indicator		21	Unassigned	I
3	Unassigned		22	Send data	I
4	Send data	I	23	Send timing	I
5	Send timing	I	24	Receive data	I
6	Receive data	I	25	Request to send	I
7	Request to send	I	26	Receive timing	I
8	Receive timing	I	27	Clear to send	I
9	Clear to send	I	28	Terminal in service	II

<i>Pin</i>	<i>Function</i>	<i>Category</i>	<i>Pin</i>	<i>Function</i>	<i>Category</i>
10	Local loopback	II	29	Data mode	I
11	Data mode	I	30	Terminal ready	I
12	Terminal ready	I	31	Receive ready	I
13	Receive ready	I	32	Select standby	II
14	Remote loopback	II	33	Signal quality	
15	Incoming call		34	New signal	II
16	Select frequency	II	35	Terminal timing	I
17	Terminal timing	I	36	Standby indicator	II
18	Test mode	II	37	Send common	II
19	Signal ground				

Категорія, 1 включає ті пальчики, чії функції сумісні з тими з EIA-232 (хоча якнайбільше були перейменовані). Для кожного пальчика Категорії 1, EIA-449 визначає два пальчики, один в першій колоні і один в другій колоні. Наприклад як пальчик 4, так і 22 були викликані посилають дані. Ці два пальчики мають рівноцінну функціональність пальчика 2 в EIA-232. Як пальчик 5, так і 23 були викликані посилати тімінг, і як пальчик 6, так і 24 були викликані одержувати дані. Навіть більш цікавить ці пари пальчиків є вертикально сусідніми один один в з'єднувачі, з пальчиком із другої колони, що займає положення по суті нижче його дублікату від першої колони. (Нумеруйте з'єднувач DB-37, заснований на нумерації з'єднувача DB-25, щоб бачити ці взаємозв'язки.) Ця структура - це те, що надає EIA-449 його

потужність. Як пальчики зв'язуються стане ясно пізніше в цій секції коли ми обговорюємо два змінні методи сигналізації визначений в електричних специфікаціях.

Пальчики Категорії II

Пальчики категорії II - це ті, які не мають ніякого еквівалента в EIA-232 або перевизначилися. Номери і функції цих нових пальчиків є як вказано нижче:

1. Локальний пальчик 10 використовується для локальної перевірки.
2. Видалений пальчик 14 використовується для видаленої перевірки.
3. Вибрана частота. Пальчик 16 використовується, щоб вибрати між двома різними частотними нормами.
4. Тестовий режим. Пальчик 18 використовується, щоб робити перевірку на різних рівнях.
5. Отримайте загальним. Пальчик 20 забезпечує загальний сигнальний зворотний провід для виведених з рівноваги довжин кола з DCE на DTE.
6. Термінальний в сервісі. Пальчик 28 указує до DCE, чи DTE не є оперативним.
7. Вибране резервування. Пальчик 32 дозволяє DTE, щоб запитати використання устаткування резервування в події відмови
8. Новий сигнал. Пальчик 34 доступний для додатків багаторазового показника, де первинний DTE управляє окремим повторним DTEs. Коли активізовано, пальчик 34 указує, що один DTE закінчив обмін даними і готовий починати спочатку.
9. Індикатор резервування. Пальчик 36 забезпечує сигнал підтвердження від DCE у відповідь на вибране резервування (пальчик 32).
10. Пошліть загальним. Пальчик 37 забезпечує загальний сигнальний зворотний провід для виведеного з рівноваги кола від (він DTE до

DCE).

Пальчикові функції DB-9

Таблиця 6.2 складає список пальчикових функцій з'єднувача DB-9. Примітка (з'єднувач DB-9 тут відмінний від того обговорюваного в EIA-232).

Table 6.2 DB-9 pins

<i>Pin</i>	<i>Function</i>
1	Shield
2	Secondary receive ready
3	Secondary send data
4	Secondary receive data
5	Signal ground
6	Receive common
7	Secondary request to send
8	Secondary clear to send
9	Send common

Електричні специфікації: RS-423 і RS-422

EIA-449 використовує два стандарти, щоб визначити його електричні специфікації: RS-423 (для довжин кола) і RS-422 (для урівноважених довжин кола).

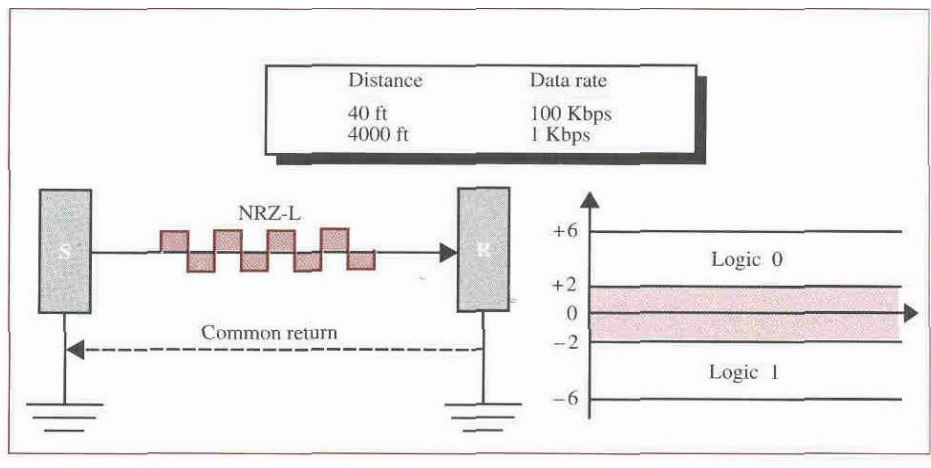
RS-423: Виведений з рівноваги режим

RS-423 - це виведена з рівноваги схемна специфікація, означаючи, що це визначає тільки одну лінію для розповсюдження сигналу.

Всі сигнали в цьому стандартному використуванні загальне повернення (або ґрунт), щоб завершити довжину кола. На рис. 6.16 подано концептуальний перегляд цього виду довжини кола також як і специфікацій для стандарту. У виведеному з рівноваги схемному режимі, виклики EIA-449 для використування тільки першого пальчика кожної пари категорії 1 і Категорії II

RS-422: Урівноважений Режим

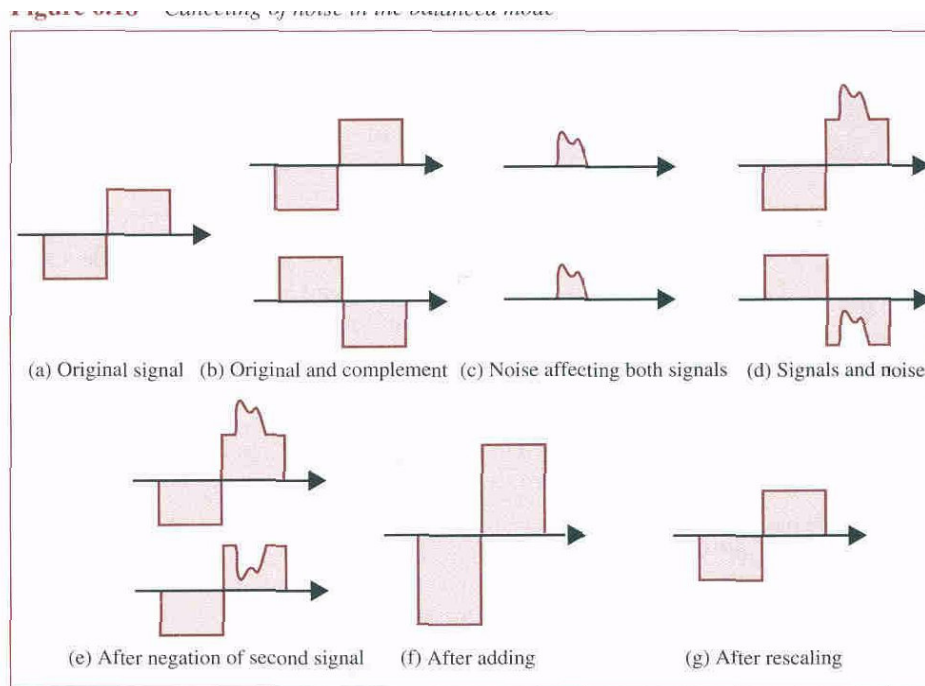
RS-422 - це урівноважена схемна специфікація, означаючи, що це визначає дві лінії для розповсюдження кожного сигналу. Сигнали знову використовують загальне повернення для повернення сигналу. На рис. 6.17 подано концептуальний перегляд і специфікації для цього стандарту. В урівноваженому режимі, EIA-449 використовує всі пари голок в Категорії 1, але не використовує голки Категорії II. Як бачите від електричних специфікацій для цього стандарту співвідношення швидкості передачі даних до дистанції набагато вище, ніж із стандарту EIA-232: 10 Mbps.



В урівноваженому режимі, дві лінії несуть ту ж передачу. Вони не, проте, несуть ідентичні сигнали. Сигнал на одній лінії - це доповнення сигналу на іншому. Коли накреслено план доповнення схоже на зображення дзеркала оригінального сигналу (рис. 6.17). Замість слухання до будь-якого фактичного сигналу, одержувач знаходить відмінності між двома. Цей механізм робить урівноважену довжину кола менш сприйнятливою до шуму виведеного з рівноваги довжини кола і покращує роботу.

Оскільки додаткові сигнали прибувають в одержувачі, вони були виконані (диференціальний підсилювач). Цей механізм віднімає другий сигнал із самого початку перед інтерпретацією. Тому що два сигнали

доповнюють один один результат віднімання - це продублююло значення першого сигналу. Наприклад, якщо в даний момент перший сигнал має напругу 5, другий сигнал матиме напругу -5. Результат віднімання, таким чином, складає $5 - (-5)$ яка рівна 10. Якщо шум, що вноситься, до передачі, стискає обидва сигнали в таким же чином (позитивний шум впливає на обидва сигнали позитивно; негативний шум впливає на обидва негативно). В результаті, шум був виключений протягом процесу віднімання (рис. 6.18). Наприклад, скажемо, два вольти шуму були введено в показчику, де перший сигнал знаходиться в 5 вольтях і його доповнення знаходиться в -5 вольтях. Доповнення спотворює перший сигнал до 7 вольтів, і другий до -3 вольтів. $7 - (-3)$ рівне 10. Ця здатність нейтралізувати результати шуму, який дозволяє вищі швидкості передач даних урівноваженої передачі.



E1A-530

E1A-449 забезпечує набагато кращу функціональність, ніж E1A-232. Проте, це вимагає з'єднувача DB-37, що промисловість відмовилася охопити через кількість інвестицій, вже помічених до DB-25. Щоб стимулювати

ухвалення нового стандарту, таким чином, EIA розробляв версію EIA-449, що пальчики DB-25 використовувань:

EIA-530

Пальчикові функції EIA-530 - це по суті ті з Категорії EIA-449 я плюс три пальчики від Категорії !! (довжини кола).

Голок EIA-232, щось нехтувало, включаючи індикатор дзвінка, сигнальний якісний детектор і сигнальний селектор норми. EIA-530 робить нуль підтримують повторну довжину кола.

X.21

X.21 - це стандарт інтерфейсу, що розробляється ІТУ-Т, щоб звернутися до багато кого з проблем, існуючих в інтерфейсах EIA, і, в той же час, мостити шлях для цілком цифрової комунікації.

Використовування каналів передач даних для елемента управління

Велика пропорція довжин кола в інтерфейсах EIA використовуються для елемента управління. Ці кола необхідні, тому що елемент управління імплементованих стандартів функціонує, оскільки відділяють сигнали. З окремою лінією контрольну інформацію зобразили тільки позитивними і негативними напругами. Але, якщо контрольні сигнали кодуються, використовуючи значущий контрольний характер від системи, як наприклад ASCII - вони можуть передаватися лініями даних.

Для цього. X.21 виключає більшість контрольних довжин кола стандартів EIA і натомість направляє їх трафік каналами передач даних. Щоб робити цю консолідацію можливою функціональності як DTE, так і DCE повинен додати схемну логіку, яка надає можливість їм перетворити контрольні коди в розрядні потоки, які можуть посилатися лінією даних. Також додаткова логіка потреби дискримінувати між контрольною

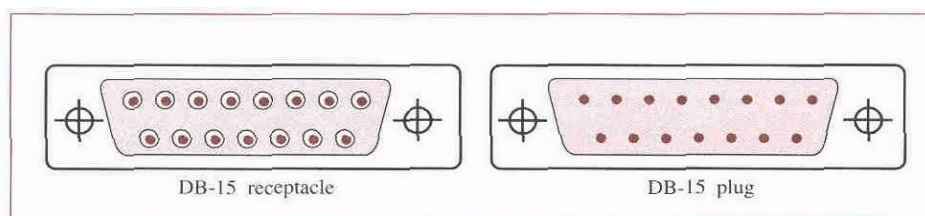
інформацією і даними по отриманню.

Цей проект дозволяє X.21, щоб не тільки використовувати менше пальчиків, але і використовуватися в цифрових телекомунікаціях, де контрольна інформація була послана від пристрою до пристрою мережі, а не тільки між DTE і DCE. Оскільки цифрова технологія з'являється ще і контрольна інформація повинна оброблятися, включаючи набір номера, повторно набираючий номер, володіння, і так далі. X.21 корисний так як переплітає, щоб з'єднати комп'ютери з аналоговими пристроями, як наприклад модеми, так і як з'єднувач між комп'ютерами і цифровими інтерфейсами, як наприклад ISDN і X.25.

X.21 розробляється, щоб працювати з урівноваженими довжинами кола в 64 Kbps, норма, яка стає промисловим стандартом.

Пальчикові функції

Малюнок 6.19 показує з'єднувач, вказаний X.21, DB-15. Оскільки ім'я вказує DB-15 - це 15-пальчиковий з'єднувач.



11. Timing байта. Інша перевага, запропонована X.21, - це таймінг лінії до синхронізації управляючого байта на додаток до синхронізації, забезпеченої стандартами EIA. За допомогою додавання імпульсу (пальчики 7 і 14) таймінг байта, X.21 покращує синхронізацію передач.
12. Елемент управління і вводу. Пальчик 3 і 5 з'єднувача DB-15 використовуються для ініціалізації, або угоди почати передачу. Пальчик 3 - це еквівалент запиту для послання. Пальчик 5 - це еквівалент

ясності для послання. Таблиця 6.3 складає список функцій для кожного пальчика.

Таблиця 6.3. Пальчики DB-15

Table 6.3 DB-15 pins

<i>Pin</i>	<i>Function</i>	<i>Pin</i>	<i>Function</i>
1	Shield	9	Transmit data or control
2	Transmit data or control	10	Control
3	Control	11	Receive data or control
4	Receive data or control	12	Indication
5	Indication	13	Signal element timing
6	Signal element timing	14	Byte timing
7	Byte timing	15	Reserved
8	Signal ground		

6.4. Модеми

Найзвичнішим типом DCE є модем. Кожен хто користувався Інтернет, заходив на офісний комп'ютер з дому або передавав інформацію телефонними лініями, мав справу з модемом. Внутрішній або зовнішній модем, асоціюється у користувачів із пристроєм, який конвертує цифрові дані комп'ютера у аналоговий сигнал для передачі телефонними лініями. Також цей пристрій конвертує інформацію, що надходить по телефону у форму зрозумілу для комп'ютера.

Термін модем - це складове слово, яке означає два функціональні пристрої: модулятор сигналів і демодулятор сигналів. Взаємозв'язок його двох частин показаний на рис. 6.20.

Модулятор перетворює цифровий сигнал у аналоговий сигнал з використанням ASK, FSK, PSK, або QAM. Демодулятор перетворює аналоговий сигнал на цифровий сигнал. Тоді як демодулятор має схожість із аналого-цифровим конвертором, він фактично не є конвертором такого типу. Це не пробує створити сигнал подібно цифровому факсу; він лише робить

процес зворотній модуляції, тобто виконує демодуляцію.

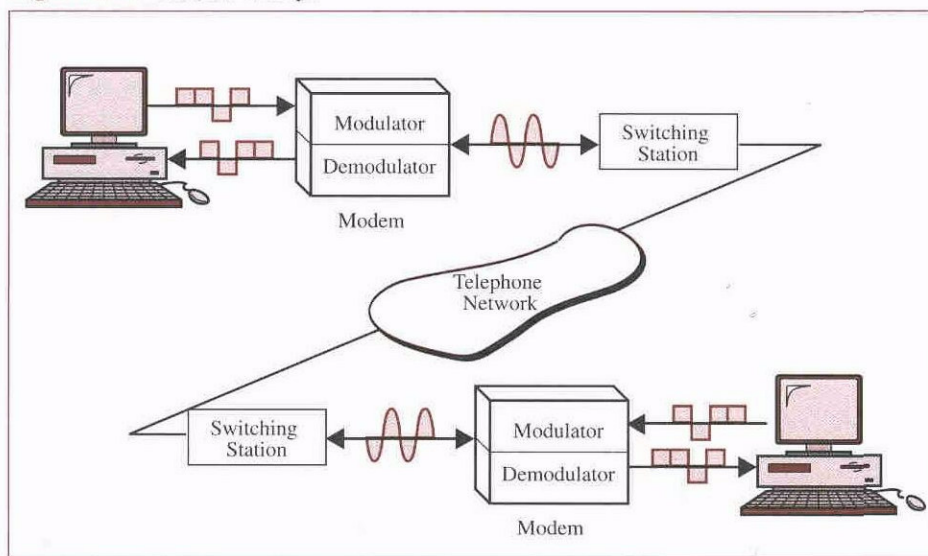


Рис. 6.20 показує взаємозв'язок модемів із комунікаційними лініями. Два PCs на кінцях - це DTEs; модеми - це DCEs. DTE створює цифровий сигнал і доставляє його модему через інтерфейс (подібно EIA-232, як обговорено раніше). Модульований сигнал отримується демодулятором іншого модему. Демодулятор використовує ASK, FSK, PSK або QAM і розшифровує його у формат зрозумілий комп'ютеру. Після цього цифровий сигнал передається до інтерфейсу комп'ютера. Кожний DCE повинен бути сумісний з обома власними DTE і з іншим DCEs.

Швидкість передачі

Можна почути описи модемів як швидкісні або низькошвидкісні, що означає, скільки бітів за секунду цей пристрій здатний передати або отримати. Але перед тим, як говорити про швидкість модемів, слід розглянути швидкість ліній передачі.

Смуга пропускання

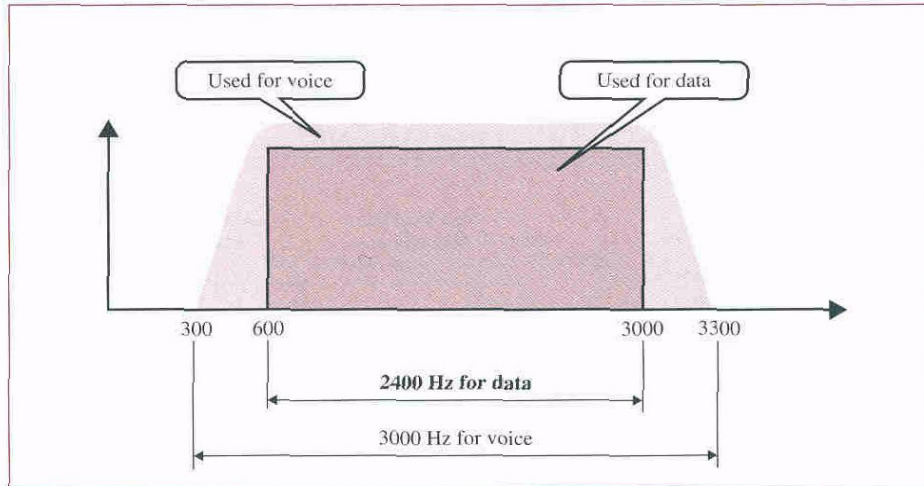
Ми визначили це поняття у лекції 4. Зараз ми можемо застосувати це

поняття до фізичних медіа, щоб бачити його результат на передачі. Швидкість передач даних залежить від виду кодування, що використовується засобом.

Середня смуга пропускання пов'язана з обмеженням фізичної властивості засобу; кожна лінія має діапазон частот, на яких може передавати інформацію. Якщо частота сигналу є дуже низькою, вона не може подолати місткість лінії. Якщо високою – вона може перешкодити індуктивності лінії. Отже ми можемо сказати кожна лінія має верхній ліміт і нижній ліміт на частотах сигналів, які може переносити.

Традиційні телефонні лінії можуть виконувати передачу на частотах між 300 гц і 3300 гц, надаючи смугу пропускання 3000 гц. Весь цей діапазон використовується для передачі голосу, де завади і спотворення можуть прийматися без втрат. Оскільки ми бачили, інформаційні сигнали вимагають гарантії вищого ступеню точності. Для безпеки, таким чином краї цього діапазону не використовуються для передачі даних. Взагалі, ми можемо сказати, що сигнал повинен бути менше, ніж смуга пропускання кабелю. Ефективні телефонної лінії, що використовується для передачі даних, складає 2400 гц, покриваючи діапазон від 600 гц до 3000 гц. Відзначимо, що сьогодні деякі телефонні лінії мають більшу смугу пропускання, ніж традиційні лінії. Проте, розробники модемів все ще орієнтуються на традиційні лінії (рис. 6.21).

Figure 6.21 Telephone line bandwidth



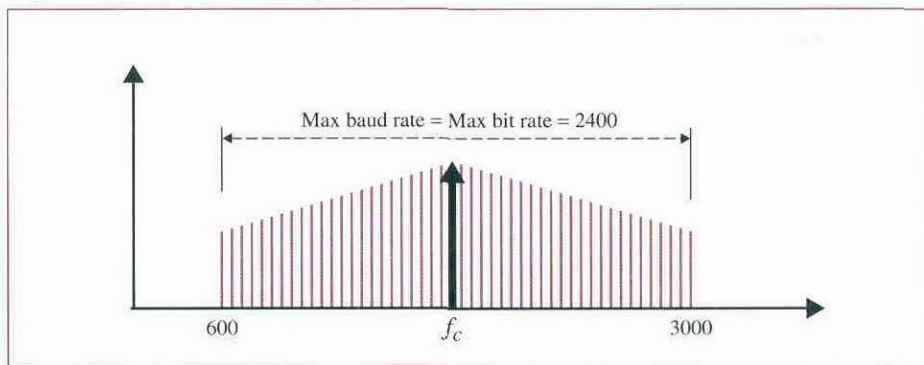
Швидкість модему

Як можна бачити, кожен вид аналогової конвертації обробляє сигнали різними способами: ASK маніпулює амплітудою, FSK маніпулює частотою, PSK маніпулює фазою, і QAM маніпулює як фазою, так і амплітудою.

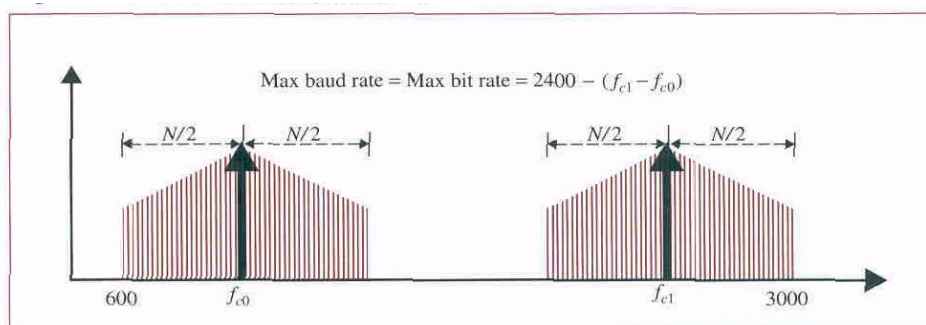
ASK

Оскільки видно з лекції 5, для ASK вимагається перетворення - рівна швидкість в бодах сигналу. Припущення, що лінія використовується одним сигналом, як би це було для сімплексної або напів-дуплексної передачі максимальна швидкість в бодах для ASK модуляції рівна повній смузі пропускання засобу передачі. Тому що ефективна смуга пропускання телефонної лінії складає 2400 гц, максимальна швидкість в бодах є також 2400. І тому що швидкість в бодах і швидкість передачі в бітах при ASK модуляції, максимальна бітова швидкість є також 2400 (рис. 6.22).

Figure 6.22 Baud rate in half-duplex ASK



Для повнодуплексної передачі, тільки половина повної смуги пропускання може використовуватися у двох напрямках. Тому максимальна швидкість для ASK передачі у дуплексному режимі 1200bps. Рис. 6.23 показує цей взаємозв'язок. Загальна доступна смуга пропускання складає 2400 гц зосереджених навкруги його власного носій. (Примітка: Деякі специфікації модему вказують напів-дуплексний режим скороченням HDX і дуплексний скороченням FDX.

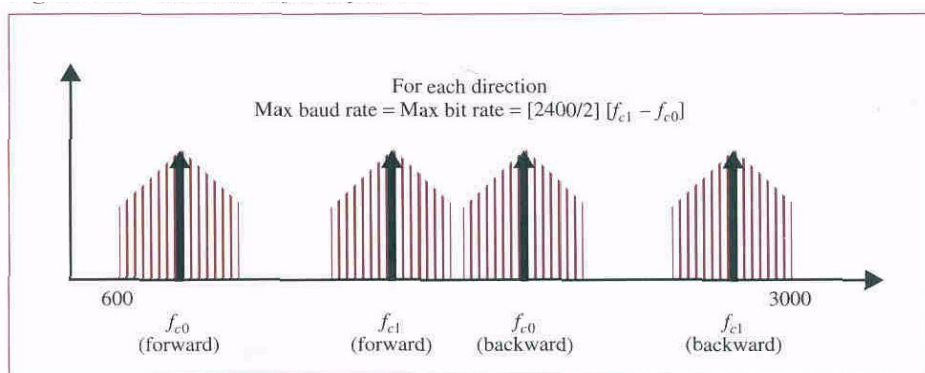


Хоча бітова швидкість ASK's дорівнює найбільш популярним видам модуляції, проблеми зашумленості роблять його непрактичним для використання в модемі.

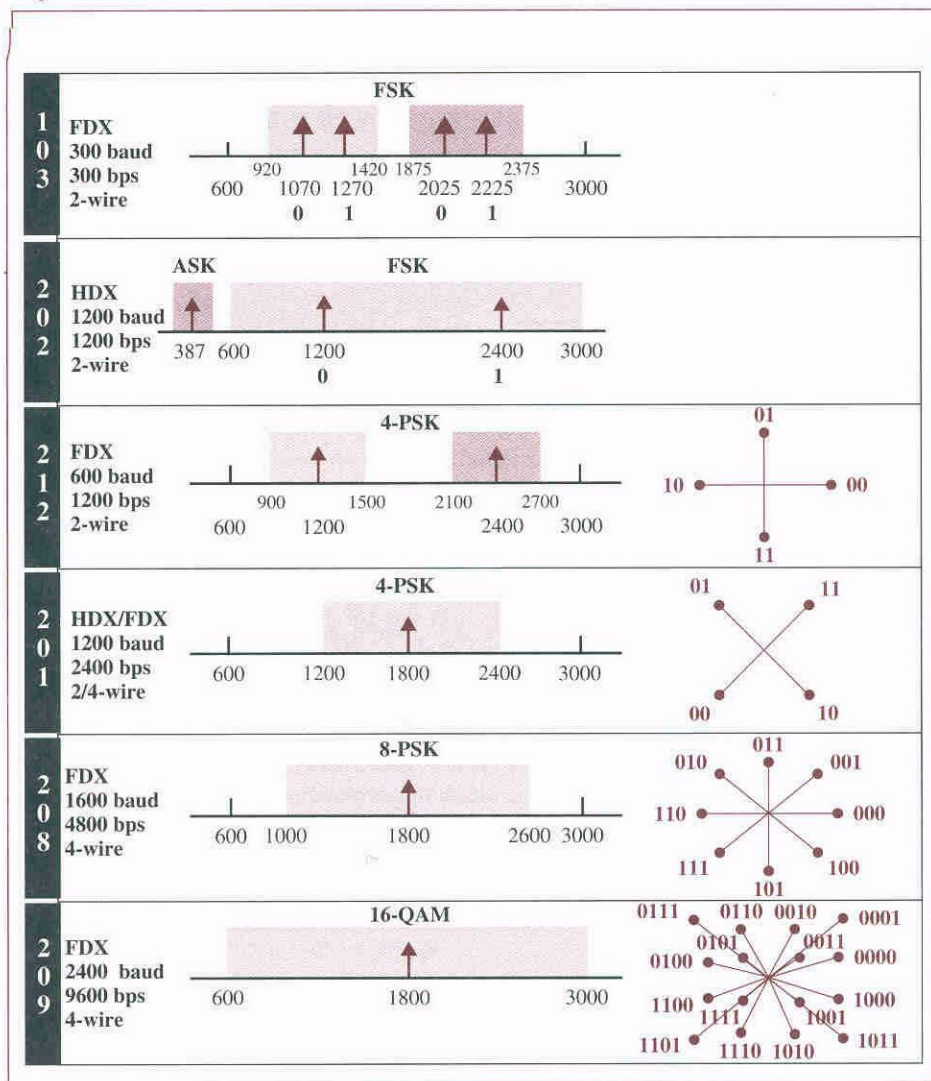
FSK

Як видно з лекції 5, для передачі FSK вимагається рівна швидкості сигналу в бодах плюс частотний зсув. Припущення, що ціла лінія використовується одним сигналом, як це робиться для сімплексної або

напівдуплексної передачі, максимальна швидкість в бодах для модуляції FSK рівна повній смузі пропускання мінус частотне переміщення. Тому що ефективна смуга пропускання телефонної лінії складає 2400 Гц, максимальна швидкість в бодах є таким чином 2400 мінус переміщення. І тому, що швидкість в бодах і швидкість передачі в бітах - це те ж в FSK модуляції максимальна швидкість передачі в бітах є також 2400 мінус частотне переміщення (рис. 6.24).



Для дуплексної передачі, тільки половина повної смуги пропускання лінії може використовувється для будь-кого напрямку. Таким чином, максимальна теоретична норма для FSK у повно-дуплексному режимі складає повну смугу пропускання мінус половина частотного зсуву. рис. 6.25.



PSK та QAM

Якщо згадати, мінімум, що вимагається для передачі PSK або QAM є таким самим, як вимагається для ASK передачі, але швидкість передачі в бітах може бути більшою залежно від кількості бітів, які можуть зображатися кожною одиницею сигналу.

Порівняння

Таблиця 6.4 підсумовує максимальну швидкість передачі в бітах по стандартних витих телефонних лініях для кожного з механізмів модуляції, що розглянуто вище. Ці цифри підсумовують традиційні дво-проводові лінії. Якщо чотири-проводові лінії використовуються швидкості передач для дуплексної передачі можуть подвоюватися. У такому разі, дві лінії можуть

використовуватися для пересилки і два для отримання даних, таким чином продублював доступний. Проте, ці цифри є теоретичними і не завжди можуть досягатися доступною технологією.

Табл. 6.4. Теоретичні швидкості передачі в бітах для модемів

Table 6.4 *Theoretical bit rates for modems*

<i>Modulation</i>	<i>Half-Duplex</i>	<i>Full-Duplex</i>
ASK	2400	1200
FSK	< 2400	< 1200
2-PSK	2400	1200
4-PSK, 4-QAM	4800	2400
8-PSK, 8-QAM	7200	3600
16-QAM	9600	4800
32-QAM	12,000	6000
64-QAM	14,400	7200
128-QAM	16,800	8400
256-QAM	19,200	9,600

Стандарти Модемів

В цій секції ми розглянемо два стандарти модему: Модеми Bell і ITU-T модеми.

Модеми Bell

Перші комерційні модеми почали вироблятися телефонною компанією Bell на початку 1970-их. Як перший і, довгий час, єдиний виробник на ринку Bell визначив розробку технології і забезпечив де-факто стандарт, на якому працювали подальші виробники. Сьогодні є десятки компаній, які виробляють сотні різних видів модемів у всьому світі. Багато моделей стали складними і потужними, але всі вони еволюціонували від оригінальних і відносно простих перших моделей від Bell. Розгляд тих перших модемів забезпечує нас розумінням основних особливостей модемів.

На рис. 6.26 показано специфікації головних модемів Bell.

Серія 103/113 Однією із ранніх комерційно доступних серій модемів

була Bell 103/113. Модеми серії Bell 103/113 діють в дуплексному режимі по два-проводових комутованих телефонних лініях. Асинхронна передача, використовує модуляцію FSK. Частоти сесії складають 1070 гц = 0 і 1270 гц - я. Частоти відповіді складають 2025 гц = 0 і 2225 гц = 1. Швидкість передач даних складає 300 bps. 113 серія - це варіація 103 серії з додатковими особливостями перевірки.

Серія 202 Модеми серії Bell 202 діють в пів-дуплексному режимі по дво-проводових комутованих телефонних лініях. Асинхронна передача використовує модуляцію FSK. Тому що 202 серії півдуплексні тільки одна пара частот передачі використовується: 1200 гц = 0, і 2400 гц = 1.

Відзначимо, що 202 серія включає частотну дію повторної передачі в будь-якому напрямі в 387 гц, використовує ASK модуляцію, з швидкістю передач даних тільки 5 bps. Цей канал використовується пристроєм отримання, щоб сказати передавачу, що є зв'язок і послати повідомлення перерви, що викликають 212 Серія, модеми серії Bell 212 мають дві швидкості. Настроювальний елемент другої швидкості дозволяє взаємозамінність з більш широкою кількістю систем. Обидві швидкості діють в дуплексному режимі над комутованими телефонними лініями. Більш повільна швидкість, 300 bps, використовує FSK модуляцію для асинхронної передачі, тільки подібно 103/113 серії. Більша швидкість, 1200 bps, може діяти або в асинхронному або синхронному режимі і використовує модуляцію 4-PSK. Тоді як 1200 bps - це та ж швидкість передач даних як досягнуто 202 серією, 212 серія досягає норми в дуплексному а не в півдуплексному режимі.

Відзначте, що за допомогою переміщення від FSK до модуляції PSK, конструктори мають більшу ефективність передачі.

В серії 202, дві частоти використовуються, щоб послати різні біти в одному напрямі. В серії 212 дві частоти зображають два різні напрямі передачі. модуляція зроблена за допомогою зміни фази на будь-якій частоті, з

кожною з чотирьох фаз переміщає зображення двох бітів.

201 Серія Модеми 201 серії діють в будь-якому півдуплексному режимі по дво-проводових комутованих лініях або дуплексний режим по чотири-проводових орендованими лініями. Повні дво-проводові лінії були присвячені по єдиному напрямку передачі. Чотири-проводові лінії дозволяють два цілком окремі канали, один в кожному напрямі, щоб обробляти через єдиний модем на кожному кінці.

Синхронна передача, використовуючи модуляцію 4-PSK, яка означає, що тільки одна частота потрібна для передачі по кожній парі ліній. Розділ передачі на дві фізично окремі лінії дозволяє кожному напрямку використовувати повну лінію.

Це означає, що по суті та ж технологія, швидкість передач даних продублювалася до 2400 bps (або 1200 бод) в як наполовину, так і дуплексні режими (2400 bps все ще половину теоретичної максимальної швидкості передач даних для модуляції 4-PSK по дво-проводових фонових лініях).

208 Серія, модеми 208 серії діють в дуплексному режимі по чотири-проводових орендованих лініями. Синхронна передача, використовує модуляцію 8-PSK. Подібно 201 серії модеми 208 серії досягають дуплексного статусу за допомогою того, що продублювали кількість ліній, що використовуються і присвятили еквівалент повної лінії по кожному напрямку передачі. Різниця тут - це те, що технологія модуляції/демодуляції зараз здатна відрізнити між вісьма різними фазовими переміщеннями. Цей модем має швидкість в бодах 1600. В трьох бітах за бод (8-PSK створює tribits), що транслює із швидкістю, щоб трохи оцінити 4800 bps.

209 серія, Модеми 209 серії діють в дуплексному режимі по чотири-проводових орендованих лініями. Синхронна передача, використовує модуляцію 16-QAM. Ці модеми досягають дуплексного статусу за допомогою того, що продублювали кількість ліній таким чином, що кожний напрям передачі має свій канал. Ця серія, проте, дозволяє використання

повної смуги пропускання кожного каналу. І тому що кожне переміщення зображає quadbit, з 16-QAM, швидкість передач даних складає 9600 bps.

Стандарти Модему ІТУ-Т

Сьогодні, багато які з найпопулярніших доступних модемів були засновані на стандартах, публікованих ІТУ-Т. Для наших цілей, ці модеми можуть поділитися на дві групи: ті, які по суті рівноцінні до прикладу модему Bell, V.21 - це подібний модем дзвону 103. Ті модеми ІТУ-Т, які є сумісною серією Bell, потрапляють в список в Таблиці 6.5 з їх еквівалентами Bell.

Таблиця 6.5. ІТУ-Т/Bell

Table 6.5 *ITU-T/Bell compatibility*

<i>ITU-T</i>	<i>Bell</i>	<i>Baud Rate</i>	<i>Bit Rate</i>	<i>Modulation</i>
V.21	103	300	300	FSK
V.22	212	600	1200	4-PSK
V.23	202	1200	1200	FSK
V.26	201	1200	2400	4-PSK
V.27	208	1600	4800	8-PSK
V.29	209	2400	9600	16-QAM

Модеми ІТУ-Т, які не мають еквівалентів в серії Bell, були описані нижче. Їх особливості показано в рис. 6.27.

V.22bis вказує, що цей модем - це друга генерація серії V.22 (bis є латинським словом двічі). V.22bis - це модем подвійної швидкості, і означає, що він може діяти на 1200, або 2400 bps. Яка швидкість використовується залежить від швидкості DCE в решті кінця обміну. Коли V.22bis одержує дані від 2400 модему bps, він діє в 2400 режимі bps для взаємозамінності.

В 1200 режимі bps, V.22bis використовує модуляцію 4-DPSK (двобітова конфігурація) в нормі передачі 600 бода. DPSK підтримує диференціальне закриття фазового переміщення на ключ, яке означає, що двійковий код визначає фазову зміну, не поточну фазу.

Правила з чотирьох двійкових кодів вказано нижче:

- 00 90 фазова зміна ступеня
- 01 0 фазова зміна ступеня
- 10 180 фазова зміна ступеня
- 11 270 фазова зміна ступеня

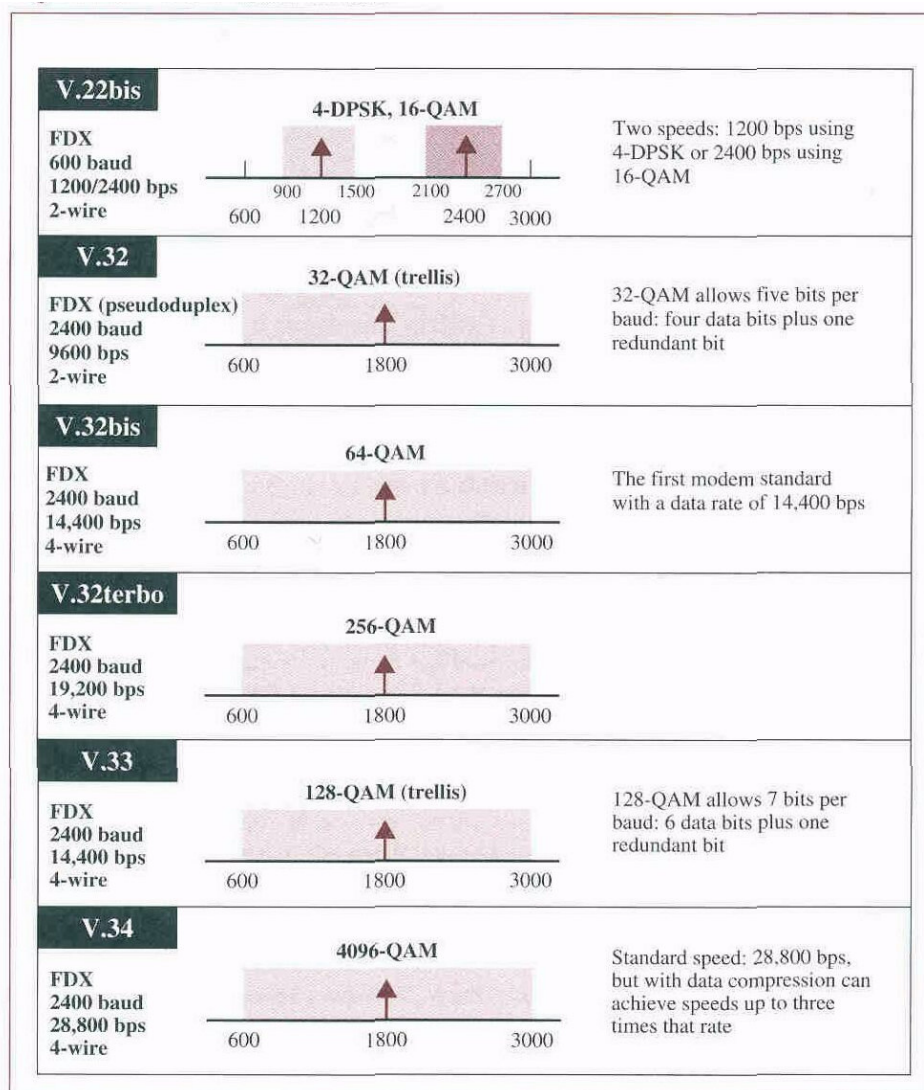
В 2400 режимі bps, V.22bis використовує 16-QAM (quadbit). Два молодші розряди в кожному quadbit модулюються, використовуючи ту ж диференціальну схему, описану вище для 1200 передачі bps. Два більшість значущих розрядів модулюються заснований на діаграмі сузір'я, показаній на рис. 6.28.

V.32 V.32 - це збільшена версія V.29, яка використовує комбіновану модуляцію і кодування техніки, викликав trellis кодовану модуляцію. Trellis є по суті QAM плюс додатковий біт. Потік даних ділиться на секції, по чотири біти. Замість quadbit, проте, quintbit (п'яти-бітова комбінація) була передана. Значення додаткового біта було вираховано від значень розрядів даних.

В будь-якій системі QAM, одержувач порівнює кожний загальноприйнятий сигнальний показчик зі всіма дійсними показчиками в сузір'ї і вибирає показчик найближчий як наявний у вигляді розрядне значення. Сигнал, спотворений шумом передачі, може набрати ближче значення до сусіднього показчика, ніж до наявного у вигляді показчика, приводячи до помилки в ідентифікації показчика і помилки в загальноприйнятих даних. Ближче показчики знаходяться в сузір'ї, більш вірогідний шум передачі, що може привести до поганої ідентифікації сигналу. За допомогою додавання додаткового розряду до кожного quadbit, кодована модуляція trellis збільшує кількість інформації, що використовується, щоб ідентифікувати кожний двійковий код і таким чином, скорочує число можливих співпадань. Для цього кодований сигнал trellis набагато менш вірогідний, ніж ясний сигнал QAM, який прочитаний неправильно, коли спотворено шумом.

Деякі виробники V.32-сумісних модемів використовують легкість trellis, щоб забезпечити функції, як наприклад виявлення помилки або виправлення помилки.

V.32 закликає до 32-QAM з швидкістю в бодах 2400. Тому що тільки чотири біти кожного зображають дані, швидкість виникнення складає $4 \times 2400 = 9600$ bps. Діаграма сузір'я показана на рис. 6.29.



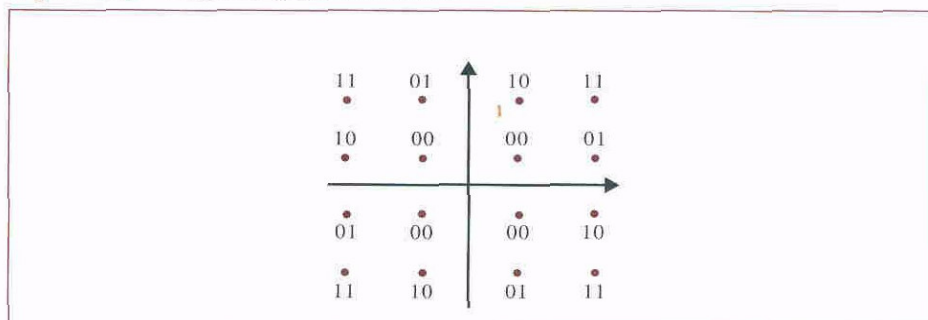
Модеми V.32 можуть використовуватися з дво-проводовою комутованою лінією в тому, що було названо псевдо-спареним режимом. псевдо-спарений був заснований на техніці під назвою ануляція луни.

V.32bis модем V.32bis був першим стандартів ІТУ-Т, щоб підтримувати 14.400 передачі bps. V.32bis використовує передачу (шість бітів за бод) 64-QAM в нормі 2400 бода ($2400 \times 6 = 14.400$ bps).

Додаткове збільшення, забезпечене V.32bis, - це включення автоматичного зворотного і передній падіння, особливості якого надають можливість модему регулювати його швидкість уверх або вниз залежно від якості лінії або сигналу. V.32terbo V.32terbo - це збільшена версія V.32bis (terbo - це каламбур на слово ter, який походить від латинського три). Це використовує 256-QAM, щоб забезпечити швидкість 19,200 bps.

V.33 V.33 також ґрунтується на V.32. Цей модем, проте, використовує кодовану модуляцію trellis, засновану на 128-QAM в 2400 боді. Кожна сигнальна зміна зображає шаблон семи бітів: шість розрядів даних і одного додаткового біта. Шість бітів даних за зміну (бод) надають цьому швидкість $6 \times 2400 = 14,400$ bps. Діаграма сузір'я для цієї схеми показана на рис. 6.30.

Figure 6.30 V.32bis 16-QAM constellation



V.34 модем V.34, V.fast, що іноді викликається, забезпечує швидкість 28,800 або 33,600 bps. Крім того, V.34 забезпечує стиснення даних, яке дозволяє швидкості передач даних із швидкість удвічі або утричі більшою за його нормальну швидкість.

V.42 стандарт V.42, прийнятий ІТУ-Т, використовує протокол, викликаний процедурою доступу посилання для модемів (LAPM). LAPM - це версія протоколу канального рівня, викликаного HDLC. Стандартні використання другого протоколу, викликаний DCEs процедурою

виправлення помилки, який дозволяє модему виправити помилки.

V.42his Після V.42. ІТУ-Т прийняв V.42bis. Цей стандарт включає всі особливості V.42, але додає Уельський метод компресії Lempel-Ziv. Модеми, що використовують цей стандарт, можуть досягти співвідношення компресії 3:1 4:1. Відзначте що швидкість передач даних модему не була збільшена; компресія дозволяє користувачу передати більше бітів за період часу.

Інтелектуальні Модеми

Мета модему - модулювати і демодулювати сигнал. Багато із сьогоднішніх модемів, проте, роблять більше. Зокрема, клас модемів під назвою інтелектуальні модеми містять програмне забезпечення, щоб підтримувати цілий ряд додаткових функцій, як наприклад автоматична відповідь і набір номера.

Інтелектуальні модеми були відразу запроваджені фірмою Hayes, Inc.

Декілька зразкових команд були надано в Таблиці 6.6.

Цей список зображає тільки малу підмножину доступних команд

Таблиця 6.6 В командах

Table 6.6 *AT commands*

<i>Command</i>	<i>Meaning</i>	<i>Parameters</i>
A	Put modem in answer mode	
B	Use V.22bis at 1200 bps	
D	Dial the number	The number to dial
E	Enable/disable echo printing	0 or 1
H	Put modem on/off hook	0 or 1
L	Adjust speaker volume	<i>n</i>
P	Use pulse dialing	
T	Use tone dialing	

6.5. Модеми 56К

Традиційні модеми мають обмеження на швидкість передачі даних

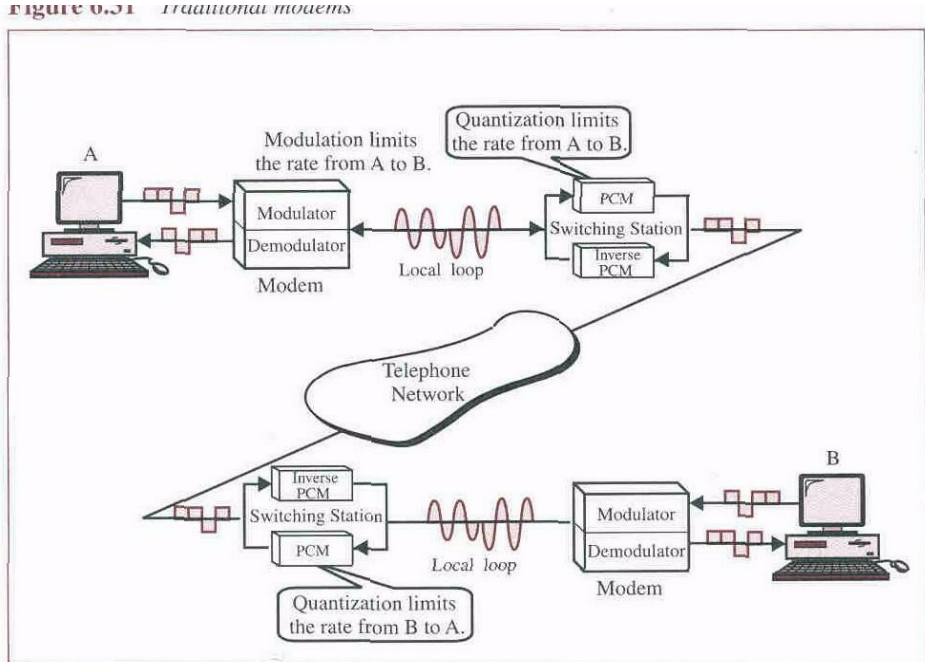
(максимум 33.6 Kbps), як детерміновано формулою Шенона. Проте, нові модеми, мають швидкість 56,000 bps, які називають 56К модемами, є уже зараз на ринку. Ці модеми можуть використовуватися, тільки якщо одна партія використовує цифрову сигналізацію (як наприклад інтернет-провайдер).

Вони несиметричні, тому що завантаження (потік даних від інтернет-провайдера до РС) є максимум 56 Kbps тоді як пересилка (потік даних з РС до інтернет-провайдера) може бути максимум 33.6 Kbps. Ці модеми порушують принцип Шенона.

Передача даних від вузла до вузла В йде такими кроками:

1. Цифрові дані модулюються модемом.
2. Аналогові дані послаються від модему до місця переключення на вузлі використання.
3. В місці переключення, аналогові дані перетворюються на цифрове використання РСМ.
4. Цифрові дані передаються через цифрову мережу телефонної компанії і попадають на місце переключення вузла В.
5. В місці переключення, цифрові дані перетворюються на аналогове використання зворотне РСМ.
6. Аналогові дані посилаються від місця переключення на вузлі В до модему, що використовує локальний цикл.
7. Аналогові дані демодулюються модемом на вузлі В.

Figure 6.31 Traditional modems



Чинник обмеження - це крок 3. Тут, аналоговий сигнал перетворюється на цифровий сигнал. Шум що походить від цього процесу, обмежує швидкість передач даних до 33.6 Kbps.

Передача даних від вузла B, виконує ті ж кроки. Знову чинник обмеження - це крок квантування з використанням РСМ.

Результат

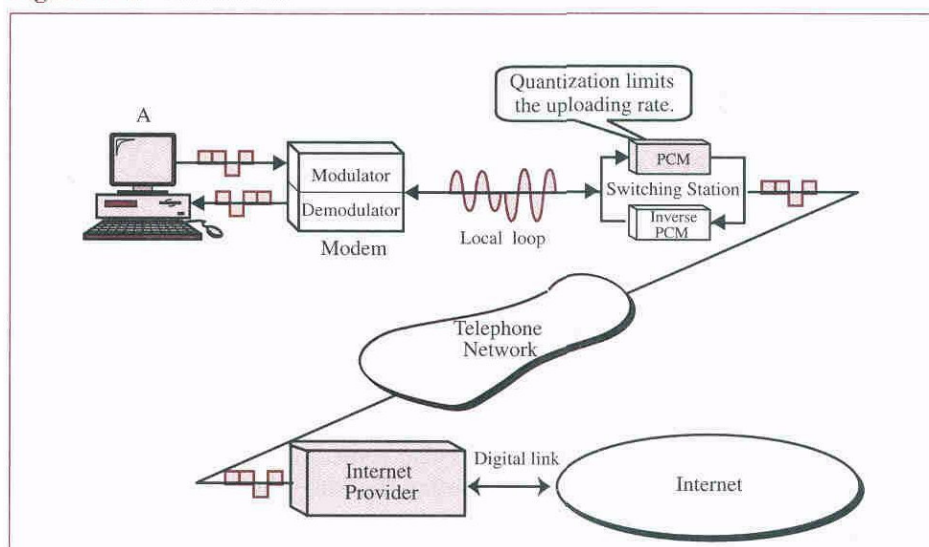
Максимальна швидкість передач даних в кожному напрямі була обмежена до 33.6 Kbps.

Якщо одна сторона - це інтернет-провайдер і сигналу не доводиться пройти через РСМ конвертор, квантування виключене в одному напрямі і швидкість передач даних може збільшуватися до 56 Kbps (рис. 6.32).

Пересилка

Передача даних від абонента до інтернет-провайдера (пересилка) слідує цим крокам:

1. Цифрові дані модулюються модемом на вузлі.
2. Аналогові дані посиляються від модему до місця переключення на вузлі, включеному в локальний цикл.
3. В місці переключення, дані перетворюються на цифрове використання PCM.



Тема 7. Передавальне середовище

- 7.1. Класифікація [1, p.187-188, 2, p.119]
- 7.2. Керовані носії передачі інформації [1, p.188]
 - 7.2.1. Витя пара [3, p.7, 2, p.120-121]
 - 7.2.2.1. Неекранована [1, p.188-191]
 - 7.2.2.2. Екранована [1, p.191-192]
 - 7.2.3. Коаксіальний кабель [2, p.121-122, 1, p.192-193]
 - 7.2.4. Оптичне волокно [2, p.122-123]
 - 7.2.4.1. Оптичне волоконна передача даних [1, p.193-194, 2, p.123-124, 1, p.196-198]
 - 7.2.4.2. Оптичне волоконні кабелі [2, p.125-127, 1, p.199-200]
- 7.3. Некеровані носії або безпроводний зв'язок [2, p.129-130]
 - 7.3.1. Електромагнітний спектр [2, p.130-133]
 - 7.3.2. Радіозв'язок [2, p.133-134]
 - 7.3.3. Зв'язок у мікрохвильовому діапазоні [2, p.134-136]
 - 7.3.4. Інфрачервоні і міліметрові хвилі [2, p.138]
 - 7.3.5. Зв'язок у видимому діапазоні [2, p.138-139]
 - 7.3.6. Супутниковий зв'язок [1, p.206-208]
 - 7.3.7. Мобільний телефонний зв'язок [2, p.187-206]
 - 7.3.8. Кабельне телебачення [2, p.206-213]
- 7.4. Погіршення передачі [1, p.211-214]
- 7.5. Продуктивність і довжина хвилі [1, p.214-217]
- 7.6. Порівняння носіїв передачі інформації [1, p.217-218]

References

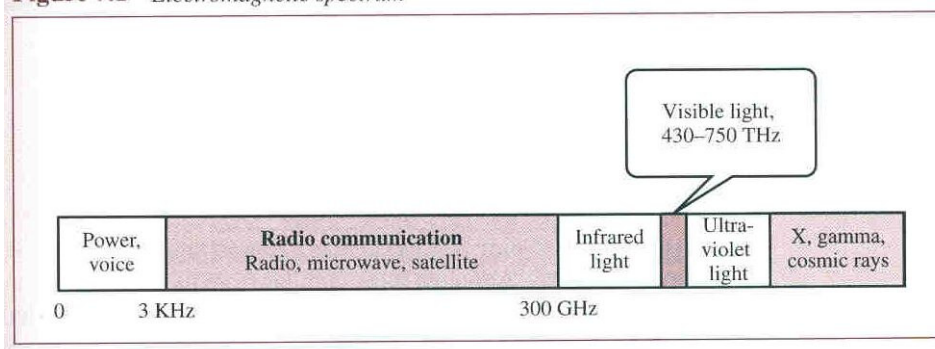
1. Fouruzan
2. Таненбаум
3. Матеріали попередньої версії

7.1. Класифікація

Як обговорювалось в лекції 4, комп'ютери та інші пристрої телекомунікації використовують сигнали для відображення даних. Ці сигнали передаються від одного пристрою до іншого у вигляді електромагнітної енергії. Електромагнітні сигнали можуть передаватися вакуум, повітря або інші засоби передачі.

Електромагнітна енергія, комбінація електричних і магнітних полів, що вібрують відносно один один, включає потужність, голос, хвилі радіо, інфрачервоне світло, видиме світло, ультрафіолетове світло, рентгенівське, гамма, і космічне випромінення. Кожен з них складає частину електромагнітного спектру (рис. 7.1). Не всі частини спектру зараз придатні до використання для телекомунікацій, також, і засоби зв'язку можуть використовувати лише декілька типів. Частоти голосового діапазону, загалом передаються кабелями, як наприклад вита пара або коаксіальний кабель. Радіочастоти можуть передаватися через повітря чи простір, але вимагають специфічних передавачів і отримувачів. Видиме світло, третій вид електромагнітної енергії, що зараз використовується для комунікацій, використовує оптоволоконний кабель.

Figure 7.1 Electromagnetic spectrum



7.1. Електромагнітний спектр

Засоби передачі можуть бути поділені на дві широкі категорії: керовані і некеровані (рис. 7.2).

Figure 7.2 Classes of transmission media

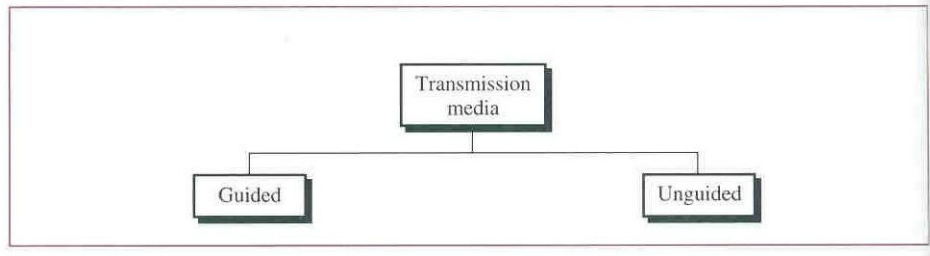


Рис. 7.2. Класи засобів передачі

7.2. Керовані носії передачі інформації

Керовані засоби, є такими, що забезпечують передачу від одного пристрою до іншого, включають виту пару, коаксіальний кабель, і оптоволоконний кабель (рис. 7.3). Сигнал, що передається по будь-якому з цих засобів, направляється фізичними обмеженнями передавального засобу. Виті пари і коаксіальний кабель використовують металеві (мідні) провідники, які приймають і, передають сигнали у формі електричного потоку. Оптоволокну - це скляний або пластичний кабель, який приймає і передає сигнали у формі світла.

Figure 7.3 Categories of guided media

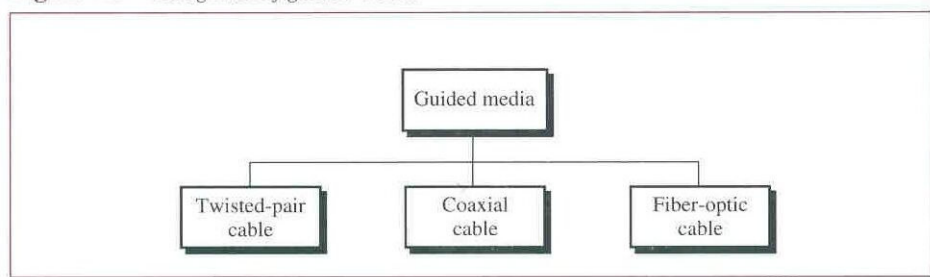


Рис. 7.3. Категорії керованих засобів

Призначенням фізичного рівня мережі є передача необробленого потоку бітів від однієї машини до іншої. Для передачі можуть використовуватися різні фізичні носії інформації, що називаються також середовищем розповсюдження сигналу. Кожний з них має характерний набір смуг пропускання, затримок, цін і простоти установки і використання. Носії можна розділити на дві групи: керовані носії, такі як мідний провід і оптоволоконний кабель, і некеровані, наприклад радіозв'язок і передача лазерному променя без кабелю. Ми розглянемо їх далі.

7.2.1. Вита пара

Витою парою (рис. 2.2) називається кабель, в якому ізольована пара провідників скручена з невеликим числом витків на одиницю довжини. Скручування провідників зменшує зовнішні електричні перешкоди при передаванні сигналів по кабелю.

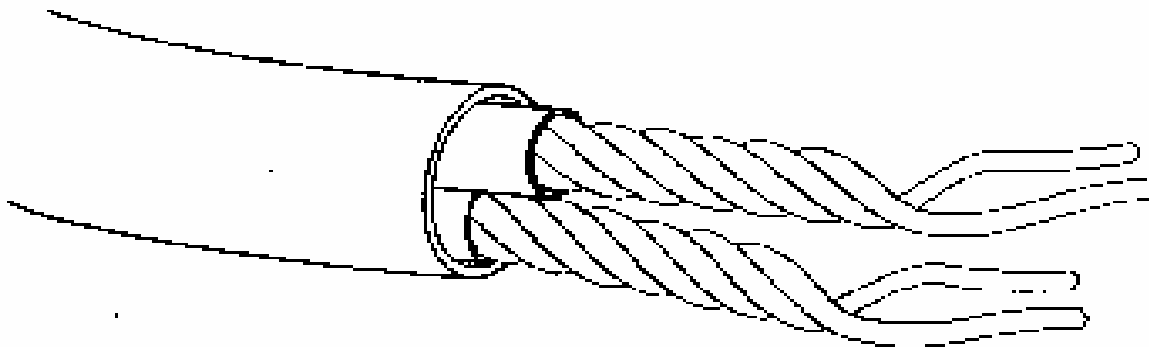


Рис. 2.2 Вита пара

Хоча швидкість передачі даних за допомогою магнітних стрічок відмінна, проте величина затримки при такій передачі дуже велика. Час передачі вимірюється хвилинами або годинами, а не мілісекундами. Для багатьох додатків потрібна миттєва реакція віддаленої системи (в

підключеному режимі). Одним з перших і дотепер часто вживаних засобів передачі є вита пара. Цей носій складається з двох ізольованих мідних провідників, звичайний діаметр яких складає 1 мм. Провідники звиваються один навкруг іншого у вигляді спіралі, чимось нагадуючи молекулу ДНК. Це дозволяє зменшити електромагнітну взаємодію декількох розташованих поряд витих пар. (Два паралельні проводи утворюють найпростішу антену, вита пара – ні.)

Найпоширенішим застосуванням виті пари є телефонна лінія. Майже всі телефони з'єднуються з телефонними компаніями за допомогою цього носія. Вита пара може передавати сигнал без ослаблення потужності на відстань, що становить декілька кілометрів. На дальших відстанях потрібні повторювачі. Велика кількість витих пар, що прокладаються на велику відстань в одному напрямі, об'єднуються в кабель, на який надягається захисне покриття. Якби пари проводів, що знаходяться усередині таких кабелів, не були звиті, то сигнали, що проходять по них, накладалися б один на одного. Телефонні кабелі діаметром декілька сантиметрів можна бачити протягнутими на стовпах.

Виті пари можуть використовуватися для передачі як аналогових, так і цифрових даних. Смуга пропускання залежить від діаметра і довжини провідника, але в більшості випадків на відстані до декількох кілометрів може бути досягнуто швидкість декілька мегабіт в секунду. Завдяки досить високій пропускну́й спроможності і невеликій ціні виті пари поширені і, швидше за все, будуть популярні і в майбутньому.

7.2.2.1. Неекранована

Вита пара буває у двох видах: незахищена і захищена.

Незахищена вита пара (UTP)

Незахищена вита пара (UTP) - це найзагальніший вид засобу телекомунікації, який використовується сьогодні. Хоча вона найчастіше використовується в телефонних системах, частотний ряд підходить для передачі як даних, так і голосу (рис. 7.4). Вита пара складається з двох провідників (звичайно, мідь), кожний з власною кольоровою ізоляцією. Кольорова ізоляція використовується для ототожнення (рис. 7.5). Кольори використовуються для як ідентифікації специфічних провідників у кабелі, так і для того, щоб вказати які дроти йдуть попарно і як вони ідентифікуються у більшій в'язці.

Figure 7.4 Frequency range for twisted-pair cable

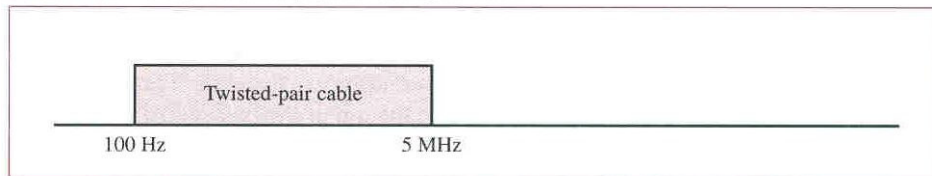


Рис. 7.4. Частотний ряд для витої пари

Figure 7.5 Twisted-pair cable

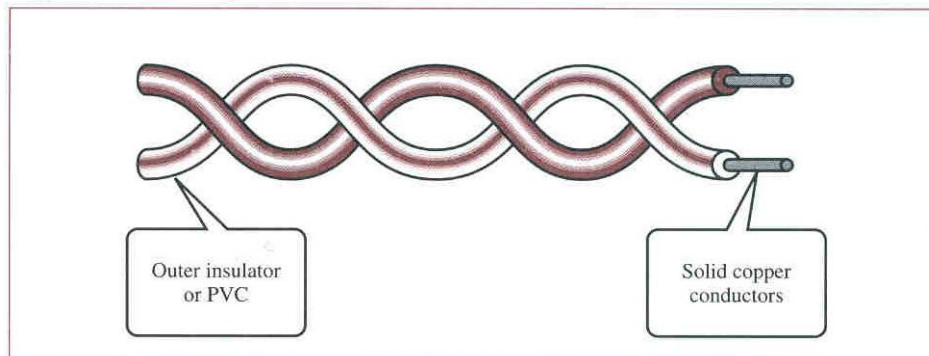


Рис. 7.5. Вита пара

В минулому, два паралельні плоскі дроти використовувалися для комунікації. Проте, електромагнітні завади від пристроїв, як наприклад двигун може створити шум у кабелі. Якщо два провідники є паралельними, дріт найближчий до джерела шуму одержує більший вплив і закінчує з

вищим рівнем напруги, ніж дрiт, що розміщений далше, що спричиняє нерівномірне навантаження і пошкоджує сигнал (рис. 7.6).

Figure 7.6 Effect of noise on parallel lines

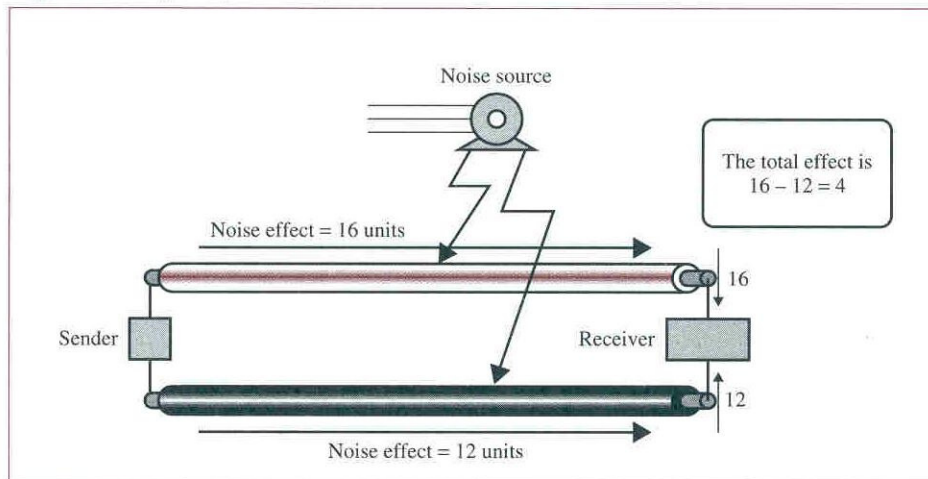


Рис. 7.6. Результат шуму на паралельних лініях

Якщо, однак, два дроти звиті один навколо одного з регулярним інтервалом (між 2 і 12 витків на фут), кожен дрiт наближається до джерела шуму половину часу і віддаляється на другу половину. Із витками, таким чином, кумулятивний результат втручання рівний на обох провідниках (рис. 7.1). Кожна секція дроту має "завантаження" 4, коли вона є на вершині витка, і 3, коли вона є знизу. Повний результат шуму в одержувачі є таким чином 0 (14- 14). Звивання не завжди виключає вплив шуму, але істотно зменшує його.

Figure 7.7 Effect of noise on twisted-pair lines

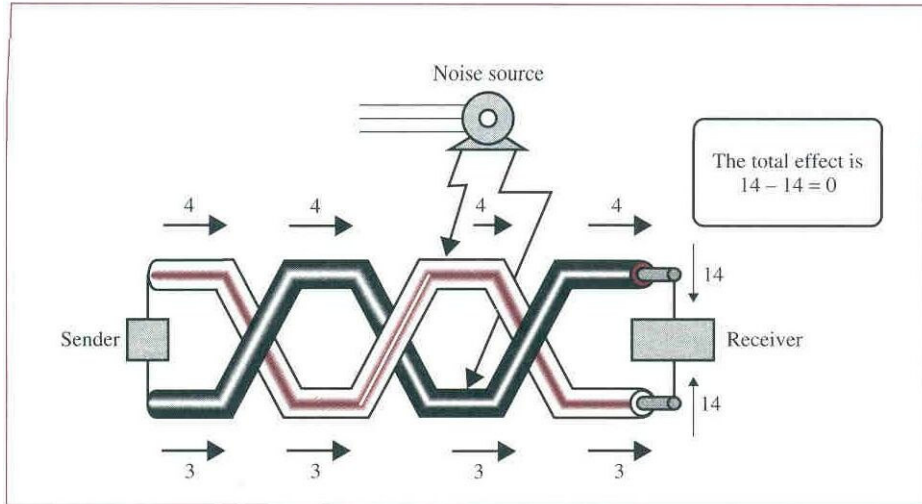


Рис. 7.7. Результат шуму на лініях з виті пари

Переваги UTP - це вартість і простота використання. UTP дешевий, гнучкий, і легкий для встановлення. Вищі типи UTP використовуються в багатьох технологіях LAN, включаючи Ethernet і Token Ring. Рис. 7.8 показує п'ять незахищених витих пар у кабелі.

Figure 7.8 Cable with five unshielded twisted pairs of wires

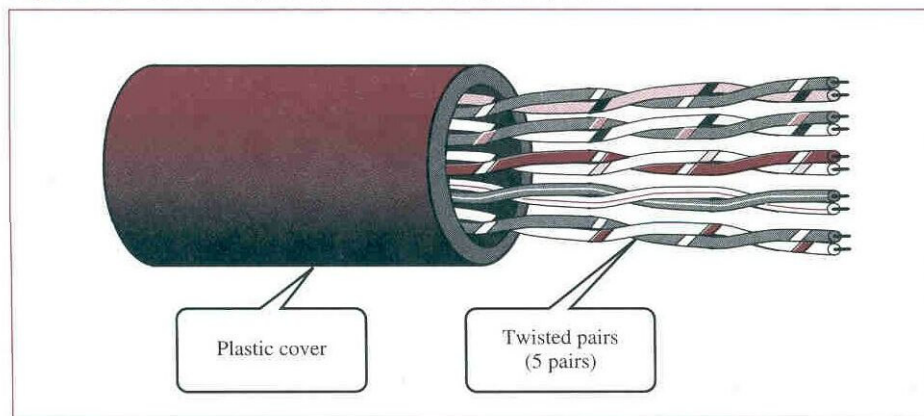


Рис. 7.8. Кабель з п'ятьма незахищеними витими парами дротів

Електронна Виробнича Асоціація (EIA) розробила стандарти для градації кабелів UTP за якістю. Категорії визначені за якістю кабелю, з 1 як

найнижчою і 5 як найвищою. Кожна категорія EIA є відповідною для певних використань, і не підходить для інших:

- Категорія 1. Основна вита пара, що використовується в телефонних системах. Цей рівень якості добрий для передачі голосу, але неадекватний для швидкісної комунікації даних
- Категорія 2. Наступна градація, відповідна для голосу і для передачі даних зі швидкістю до 4 Mbps
- Категорія 3. Вимагає як мінімум три витки на фут і може використовуватися для передачі даних аж до 10 Mbps. Є зараз стандартним кабелем для більшості телефонних систем.
- Категорія 4. Повинна мати як мінімум три витки на фут, а також інші умови, щоб мати можливу норму передачі до 16 Mbps
- Категорія 5. Використовують для передачі даних аж до 100 Mbps.

Конектори UTP UTP найпростіше підключати до мережевих пристроїв через розетку подібну до телефонної. Конектори мають штекер і розетку. Штекер вставляють в розетку і фіксують спеціальним зажимом (під назвою ключ), який утримує їх на місці. Кожний дрот в кабелі зв'язаний з одним проводом (або голкою) в з'єднувачі. Найчастіше використовують конектори RJ45 з вісьма провідниками, один для кожного проводу з чотирьох витих пар (рис. 7.9).

Figure 7.9 UTP connection

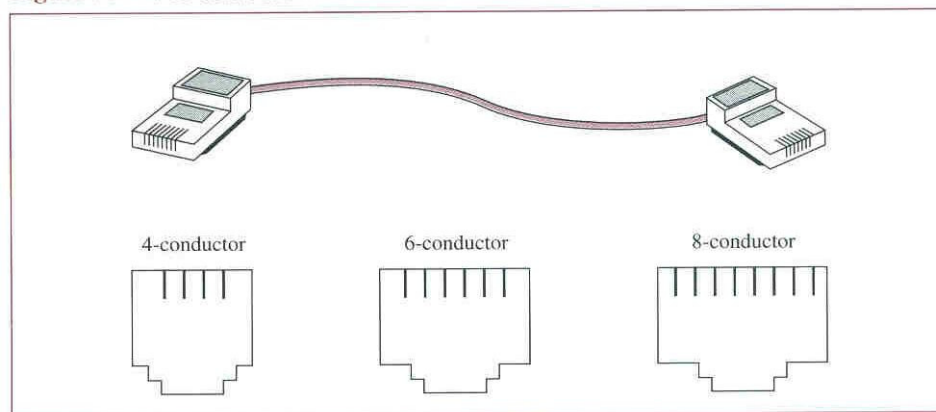


Рис. 7.9. Зв'язок UTP

2.2.2. Екранована

Захищена вита пара (STP)

Захищена вита пара (STP) має металеве або плетене покриття, яке огортає кожну пару ізольованих провідників (рис. 7.10). Кожух оберігає від проникнення електромагнітного шуму. Це також може виключити феномен за назвою crosstalk, який є результатом впливу одного кола(або каналу) на інше коло. Це відбувається, коли одна лінія (діє як свого роду приймаюча антени) приймає сигнали іншої лінії (діє як свого роду передаюча антена). Цей результат може бути видно під час телефонних розмов, коли абонент може чути інші розмови у фоні. Захист кожної пари у витій парі може виключити найбільший crosstalk.

Figure 7.10 *Shielded twisted-pair cable*

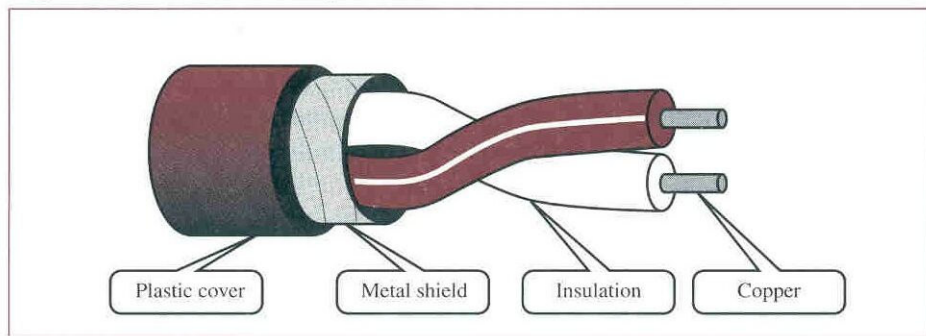


Рис. 7.10. Захищені виті пари

STP має ті ж якісні характеристики і використовує ті ж з'єднувачі що й UTP, але захист повинен з'єднуватися із заземленням. Матеріали і виробничі вимоги роблять STP дорожчим, ніж UTP, менш сприйнятливим до шуму.

7.2.3. Коаксіальний кабель

Іншим поширеним засобом передачі даних є коаксіальний кабель. Він краще екранований, ніж вита пара, тому може забезпечити передачу даних на більші відстані з вищими швидкостями. Широко застосовуються два типи кабелів. Один з них, 50-омний, звичайно використовується для передачі виключно цифрових даних. Інший тип кабелю, 75-омний часто застосовується для передачі аналогової інформації, а також в кабельному телебаченні. В основі такого розподілу лежать швидше історичні, ніж технічні чинники (наприклад, перші дипольні антени мали імпеданс 300 Ом, і простіше всього було використовувати вже існуючі перетворювачі з відношенням імпедансу 4:1).

Коаксіальний кабель складається з ізольованого твердого мідного проводу, розташованого в центрі кабелю. Поверх ізоляції натягнутий циліндричний провідник, звичайно виконаний у вигляді дрібної мідної сітки. Він покритий зовнішнім захисним шаром ізоляції (пластиковою оболонкою). Вид кабелю в розрізі показано на рис. 2.3.

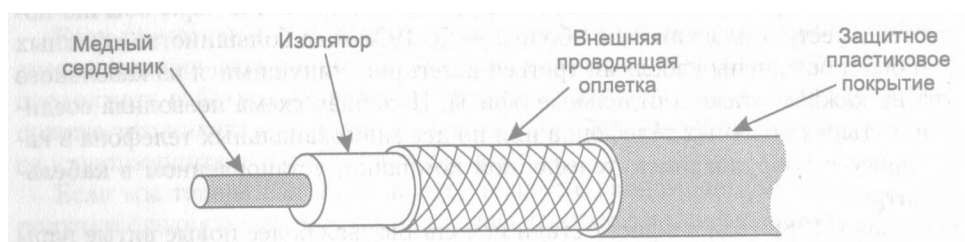


Рис. 2.3. Коаксіальний кабель

Конструкція і спеціальний тип екранування коаксіального кабелю забезпечують високу пропускну спроможність і відмінну завадостійкість. Максимальна пропускну спроможність залежить від якості, довжини і співвідношення сигнал/шум лінії. Сучасні кабелі мають смугу пропускання близько 1 ГГц. Коаксіальні кабелі широко застосовувалися в телефонних

системах, але тепер на лініях великої довжини їх все частіше замінюють оптоволоконними кабелями. Проте коаксіальні кабелі все ще широко використовуються для кабельного телебачення, а також в деяких регіональних мережах.

Коаксіальний кабель переносить сигнали вищих частотних рядів, ніж вита пара, тому що ці два засоби конструюються цілком по різному. Замість двох проводів, коаксіал має центральне провідникове ядро або провідник (звичайно мідь), оточений у ізоляцією, яка обгорнута зовнішнім металевим покриттям, або комбінацією двох (також звичайно мідь). Зовнішнє металеве покриття діє як щит проти шуму. Так і як другий провідник, який утворює коло. Цей зовнішній провідник також оточений у ізоляцією, і цілий кабель захищений пластиковою ізоляцією (рис. 7.12).

Коаксіальні кабельні стандарти

Різні коаксіальні кабельні проекти розподілені по категоріях рейтингами Radio Government (RG). Кожний номер RG означає унікальний набір фізичних специфікацій, включаючи калібр внутрішнього провідника, товщини і виду внутрішнього ізолятора, конструкції щита, розміру і виду зовнішнього кожуха для провідника.

Кожний кабель, визначений рейтингами RG, пристосований для функції, що спеціалізується. Нижче перелічено кілька загальних:

- RG-8. Використовують в товстому Ethernet.
- RG-9. Використовують в товстому Ethernet.
- RG-11. Використовують в товстому Ethernet.
- RG-58. Використовують в тонкому Ethernet.
- RG-59. Використовують для ТБ.

Figure 7.12 Coaxial cable

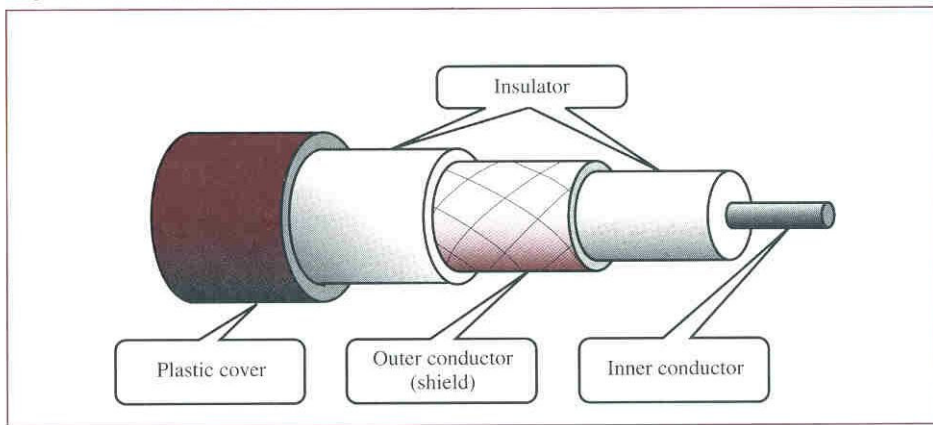


Рис. 7.12. Коаксіальний кабель

Коаксіальні кабельні з'єднувачі

За останні роки, цілий ряд з'єднувачів були розроблені для використання з коаксіальним кабелем, звичайно виробниками, що шукають специфічні рішення до специфічних вимог продукту. Декілька проектів з'єднувача, що найбільш широко використовуються, стали стандартизованими. Найзагальніший з них названий з'єднувачем барреля через подібність його форми. Із з'єднувачів барреля, найпопулярніший є штиковим з'єднувачем (BNC), який вставляється і фіксується напівповоротом. Інші види з'єднувачів барреля необхідно закручувати разом і тому вимагає більше зусилля, або вставляється без замикання, що є менш безпечним. Всі коаксіальні з'єднувачі мають єдину голку, що стирчить по центру штекера котра вставляється в розетку. Коаксіальні з'єднувачі близькі до з'єднань кабельного ТБ і VCR.

Два інші види з'єднувачів, є Т-конектори і термінатори. Т-конектор (використовують в тонкому Ethernet) дозволяє відгалуження від головної лінії. Кабель може відгалуздитися, щоб з'єднати окремі термінали. Термінатори потрібні для шинних топологій, де один головний кабель діє, як основа з гілками до окремих пристроїв, але не має завершального пристрою.

Якщо головний кабель залишається без приладу, будь-який сигнал, передається ехом назад, і заважає оригінальному сигналу. Термінатор поглинає хвилю і виключає зворотне ехо.

7.2.4. Оптичне волокно

Швидкий розвиток комп'ютерних технологій викликає відчуття гордості у багатьох представників цієї індустрії. Перший персональний комп'ютер фірми ІВМ, створений в 1981 році, працював з тактовою частотою 4,77 МГц. Через 20 років цей показник виріс до 2 ГГц. Приріст множника склав 20 за десятиліття. Не так вже погано.

За той же період швидкість передачі даних виросла з 56 Кбіт/с (ARPANET) до 1 Гбіт/с (сучасний оптичний зв'язок), це означає зростання в 125 разів за кожні 10 років. При цьому вірогідність помилки при передачі зменшилася з 10^{-5} на біт майже до нуля.

В даний час процесори починають наближатися до своїх фізичних меж. Швидкість світла подолати неможливо, непросто розв'язати і проблему відведення теплової енергії. Існуюча нині оптичне волокно технологія, навпаки, може розвивати швидкість передачі даних аж до 50 000 Гбіт/с (50 Тбіт/с), і при цьому багато фахівців зайнято пошуком досконаліших матеріалів. Сьогоднішня практична межа в 10 Гбіт/с обумовлена нашою нездатністю швидше перетворювати електричні сигнали в оптичні і назад, хоча в лабораторних умовах вже досягнута швидкість 100 Гбіт/с на одинарному волокні.

В гонці комп'ютерів і засобів зв'язку перемогли останні. Думка про практично нескінченну смугу пропускання (при ненульовій вартості, зрозуміло) ще не засвоєна до кінця поколінням учених-комп'ютерників, привчених мислити в категоріях низьких обмежень Найквіста і Шеннона, що накладаються на мідний провід. Нова точка зору повинна полягати в тому,

що всі комп'ютери безнадійно повільні, і мережам слід за всяку ціну уникати обчислень незалежно від того, яка частина смуги пропускання при цьому буде втрачена. В даному розділі ми розглянемо технологію передачі даних по оптичному волокну.

7.2.4.1. Оптичне волоконна передача даних

До цього місця, ми обговорили провідні (металеві) кабелі, які передають сигнали у формі струму. Оптичне волокно, з другого боку, виготовляється зі скла або пластмаси і передає сигнали у формі світла. Щоб зрозуміти оптичне волокно нам необхідно дослідити окремі аспекти природи світла.

Природа світла

Світло є формою електромагнітної енергії. Воно передається найшвидше у вакуумі: 300,000 км/с. Швидкість залежить від густини речовини через яку передається світло (чим вища густина, тим менша швидкість).

Оптичне волоконна система передачі даних складається з трьох основних компонентів: джерела світла, носія, по якому розповсюджується світловий сигнал, і приймача сигналу, або детектора. Світловий імпульс приймають за одиницю, а відсутність імпульсу – за нуль. Світло розповсюджується в надтонкому скляному волокну. При попаданні на нього світла детектор генерує електричний імпульс. Приєднавши до одного кінця оптичного волокна джерело світла, а до іншого – детектор, ми отримаємо однонаправлену систему передачі даних. Система приймає електричні сигнали і перетворює їх в світлові імпульси, що передаються по волокну. На іншій стороні відбувається зворотне перетворення в електричні сигнали.

Така передаюча система б була даремна, якби світло по дорозі розсівалося і втрачало свою потужність. Проте в даному випадку використовується один цікавий фізичний закон. Коли промінь світла переходить з одного середовища в інше, наприклад, із скла (розплавленого і застиглому кварцу) в повітря, промінь відхиляється (ефект рефракції або заломлення) на межі скло–повітря, як показано на рис. 2.4. а. Тут ми бачимо, що промінь світла падає під кутом α , виходячи під кутом β . Співвідношення кутів падіння і віддзеркалення залежить від властивостей суміжних середовищ (зокрема, від їх коефіцієнтів заломлення). Якщо кут падіння перевершує деяку критичну величину, промінь світла цілком відражається назад в скло, а в повітря ніщо не проходить. Таким чином, промінь світла, падаючий на межу середовищ під кутом, що перевищує критичний, виявляється замкнутим усередині волокна, як показано на рис. 2.4, б, і може бути переданий на велику відстань майже без втрат.

На рис. 2.4, б показано тільки один спійманий промінь світла, проте оскільки будь-який промінь світла з кутом падіння, що перевищує критичний, відражатиметься від стінок волокна, то і безліч проміння одночасно відражатиметься під різними кутами. Про кожний промінь говорять, що він має деяку моду, а оптичне волокно, що має властивістю передавати відразу декілька променів, називається багатомодовим. Проте якщо зменшити діаметр волокна до декількох довжин хвиль світла, то волокно починає діяти подібно хвилеводу, і світло може рухатися тільки по прямій лінії, без віддзеркалень від стінок волокна. Таке волокно називається одномодовим. Воно коштує дорожче, але може використовуватися при передачі даних на великі відстані. Сьогоднішні одномодові волоконні лінії можуть працювати із швидкістю 50 Гбіт/с на відстані до 100 км. В лабораторіях були досягнуті і вищі швидкості, правда, на менших дистанціях.

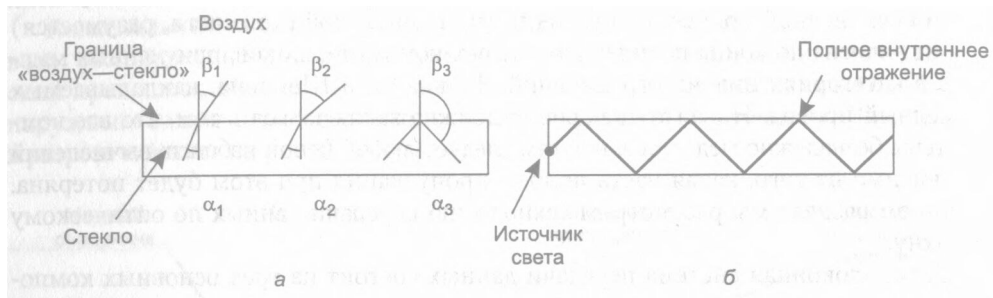


Рис. 2.4. Три приклади заломлення променя світла, падаючого під різними кутами на межі кварцового волокна і повітря (а); промінь світла, спійманий повним внутрішнім віддзеркаленням (б)

Методи розповсюдження

Поточна технологія підтримує два методи для розповсюдження світла вздовж оптичних каналів, кожний вимагає волокно з різними фізичними особливостями: багатомодовий і єдиний метод. Багатомодовий, по черзі, може виконуватися в двох формах: індексний кроку або градуйований індексний (рис. 7.16).

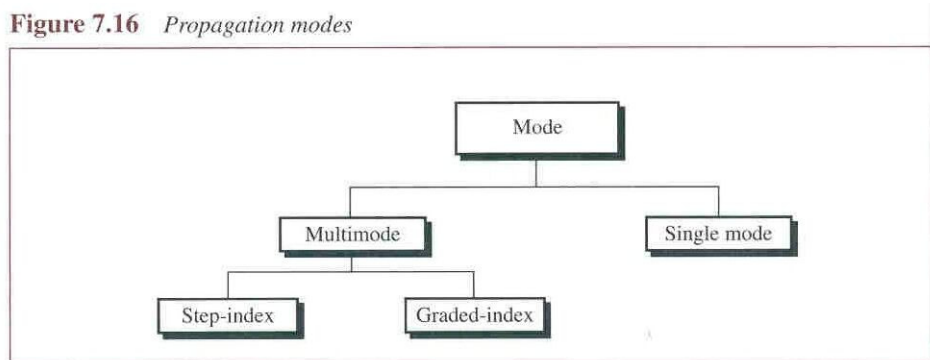


Рис. 7.16. Методи розповсюдження

Багатомодовий

Багатомодовий названий так, тому що багаторазові промені легко рухаються від початку через ядро в різні сторони. Як ці промені переміщуються в межах кабелю залежить від структури ядра.

В багатомодовому індексному волокні, густина ядра зберігає константу від центру до країв. Пучок світла переміщається через цю постійну густина по прямій лінії, поки досягає інтерфейсу ядра і cladding. В інтерфейсі, є раптова зміна до нижчої густини, яка змінює ситуацію руху променя. Індексний термін кроку залежить від раптовості цієї зміни.

Різні промені (або пучки) показано на рис. 7.17, рухаються через індексне волокно. Деякі промені посередині рухаються по прямих лініях через ядро і досягають місця призначення без відображення або заломлення. Деякі промені завдають удару інтерфейсу ядра і cladding менша ситуація, ніж критична ситуація; ці промені пронизують cladding і втрачаються. Ще інші ударяються об край ядра в більших ситуаціях, ніж критична ситуація і відбиваються назад в ядро і в сторони, підстрибують туди і сюди, поки досягають місця призначення.

Figure 7.17 Multimode step-index fiber

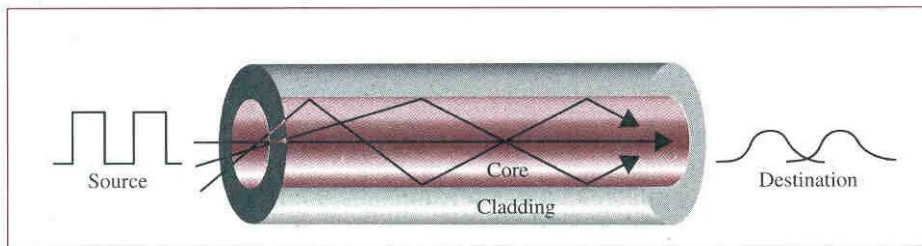


Рис. 7.17. Мультимодове волокно з індексним кроком

Кожен промінь відбивається на кут рівний до кута падіння. Чим більший кут падіння, тим ширша ситуація відображення. Промінь з меншим кутом падіння вимагатиме, щоб більше стрибків передавалися на ту ж дистанцію, ніж промінь з більшим кутом падіння. Тому, промінь з меншою випадковою ситуацією повинен передаватися далі, щоб досягти місця призначення. Ця різниця в довжині шляху означає, що різні промені прибувають в місце призначення по різному. Оскільки ці різні промені перекомбінуються в одержувачі, вони приводять до сигналу, який є не

точною точною копією того сигналу, який був переданий. Такий сигнал спотворюється затримками розповсюдження. Це спотворення обмежує норму доступних даних і робить мультимодовий індексний кабель неадекватним для певних точних додатків.

Іншим видом волокна, за назвою мультимодове розміщено-індексне волокно, зменшує це спотворення передачі сигналу через кабель. Слово індекс тут означає індекс відбиття. Оскільки ми бачили вище, індекс рефракції пов'язаний з густиною. Розміщено-індексне волокно, таким чином, є одним із способів зміни густини. Густина найвища в центрі ядра і зменшується поступово до краю. На рис. 7.18 показано зіткнення цієї мінливої густини на розповсюдженні легких променів.

Figure 7.18 Multimode graded-index fiber

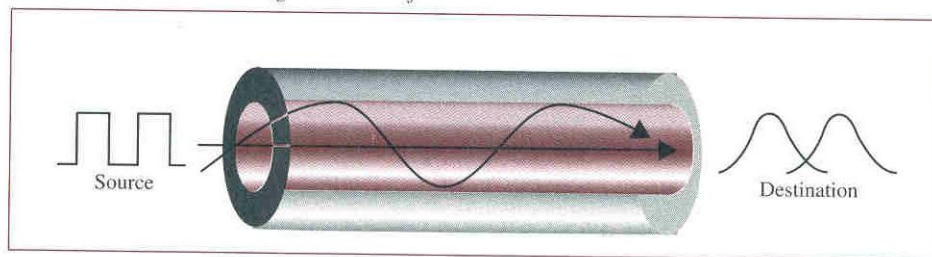


Рис. 7.18. Мультимодове розміщено-індексне волокно

Сигнал вводиться в центрі ядра. Від цієї точки, тільки горизонтальні промені рухаються по прямій лінії через постійну густину в центрі. Промені в інших ситуаціях переміщуються через середовище із постійно змінною густиною. Кожна різниця густини примушує кожен промінь заломлюватися по кривій. Крім того, варіюючи рефракцію варіюється дистанція руху кожного променя в даний періоді часу, приведення до різних променів, пересічних в регулярних інтервалах. Обережне розміщення одержувача в одному з цих перетинів дозволяє сигналу реконструюватися з більшою точністю.

Єдиний метод використовує індексний крок у волокні і надзвичайно легко фокусує джерело, що промені лімітують малий ряд ситуацій близько до горизонталі. Єдиний метод використовує набагато менший діаметр, ніж й багатомодових волокнах, і з реально нижчою густиною (індекс рефракції). Зменшення в густині приводить до критичної ситуації, яка є близькою до 90 градусів, щоб робити розповсюдження променів майже горизонтально. В даному випадку, розповсюдження різних променів майже ідентичне і затримки є незначними. Всі промені прибувають в місці призначення "разом" і можуть перекомбінуватися без спотворення сигналу (рис. 7.19).

Figure 7.19 Single-mode fiber

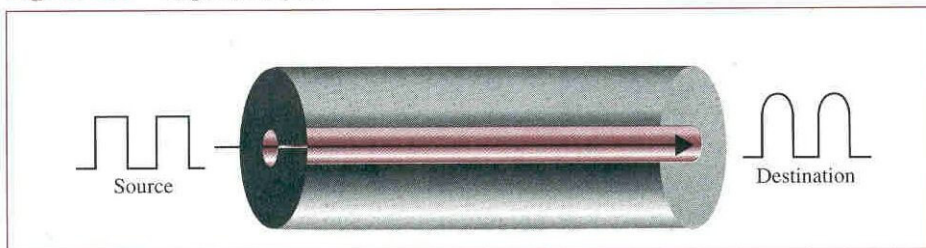


Рис. 7.19. Єдиний метод

7.2.4.2. Оптиволоконні кабелі

Структура оптиволоконного кабелю схожа з описаною раніше структурою коаксіального проводу. Різниця полягає лише в тому, що в першому немає екрануючої сітки. На рис. 2.6, а показана окрема оптиволоконна жила. В центрі її розташовується скляна сердечина, по якій розповсюджується світло. В багатомодовому оптиволоконні діаметр сердечника складає 50 мкм, що приблизно рівно товщині людського волоса. Сердечник в одномодовому волокні має діаметр від 8 до 10 мкм.

Сердечник покритий шаром скла з нижчим, ніж у сердечника, коефіцієнтом заломлення. Він призначений для більш надійного запобігання виходу світла за межі сердечника. Зовнішнім шаром служить пластикова

оболонка захищаюча скло. Оптиволоконні жили звичайно групуються в пучки, захищені зовнішньою оболонкою. На рис. 2.6, б показаний трижильний кабель.



Рис. 2.6. Видгляд одиночного волокна збоку (а); поперечний перетин трижильного кабелю (б)

Звичайно кабелі прокладають в ґрунт на глибину близько 1 м, де їх можуть випадково пошкодити гризуни або екскаватор. Біля побережжя трансокеанічні кабелі укладаються в траншеї спеціальним механізмом. На великій глибині їх звичайно просто кладуть на дно, де їх можуть зачепити риболовецькі траулери або перегризти акули.

З'єднання відрізків кабелю може здійснюватися трьома способами. По-перше, на кінець кабелю може прикріплюватися спеціальний роз'єм, за допомогою якого кабель вставляється в оптичну розетку. Подібне з'єднання приводить до втрати 10-20 % сили світла, зате воно дозволяє легко змінити конфігурацію системи.

По-друге, вони можуть механічно зрощуватися – два акуратно відрізаних кінця кабелю укладаються поряд один з одним і затискаються спеціальною муфтою. Поліпшення проходження світла досягається вирівнюванням кінців кабелю. При цьому через з'єднання пропускається світло, і задачею є добитися максимальної відповідності потужності вихідного сигналу потужності вхідного. Одне механічне зрощення кабелів

займає у досвідченого монтажника мереж близько 5 хвилин і дає в результаті втрату 10 % потужності світла.

По-третє, два кабелі можуть бути сплавлені разом. Сплавне з'єднання майже так само добре, як і суцільний кабель, але навіть при такому методі відбувається невелике зменшення потужності світла.

У всіх трьох типах з'єднань в точці з'єднання можуть виникнути віддзеркалення, і відображене світло може інтерферувати з сигналом.

Для передачі сигналу по оптоволоконному кабелю можуть використовуватися два типи джерела світла: світловипромінюючі діоди (LED, Light Emitting Diode) і напівпровідникові лазери. Вони володіють різними властивостями, як показано в табл. 2.2. Їх довжина хвилі може бути набудований за допомогою інтерферометрів Фабри–Перо (Fabry–Perot) або Маха–Цандера (Mach–Zehnder), встановлюваних між джерелом і кабелем. Інтерферометри Фабри–Перо є простими резонансними поглибленнями, що складаються з двох паралельних дзеркал. Світло падає перпендикулярно дзеркалам, поглиблення відбирає ті довжини хвиль, які укладаються в його розмір ціле число раз. Інтерферометри Маха–Цандера розділяють світло на два промені, які проходять різну відстань і знову з'єднуються на виході. Синфазними на виході інтерферометра виявиться проміння строго визначеної довжини.

Таблиця 2.2. Порівняльні характеристики світлодіодів і напівпровідникових лазерів

Характеристика	Светодиод	Полупроводниковый лазер
Скорость передачи данных	Низкая	Высокая
Тип волокна	Многомодовые	Многомодовые или одномодовые
Расстояние	Короткое	Дальнее
Срок службы	Долгий	Короткий
Чувствительность к температуре	Невысокая	Значительная
Цена	Низкая	Высокая

Приймальний кінець оптичного кабелю є фотодіодом, генерувальним електричним імпульсом, коли на нього падає світло. Звичайний час спрацьовування фотодіода – близько 1 нс, що обмежує швидкість передачі даних 1 Гбіт/с. Термальний шум також має місце, тому імпульс світла повинен бути досить потужним, щоб його можна було знайти на фоні шуму. При достатній потужності імпульсу можна добитися малої частоти помилок.

Джерела світла для оптоволоконна

Як видно – ціль оптоволоконного кабелю – передавати і направляти пучок світла від джерела до приймача. Для передачі і походження передавач повинен бути обладнаний джерелом світла і приймач – світлочутливим осередком (під назвою фотодіод), здатний до трансляції світла у вигляді придатному до сприйняття комп'ютером. Джерело світла може бути або світлодіодом light-emitting diode (LED) або діодом лазерної ін'єкції (ILD). LED є дешевшим джерелом, але вони забезпечують нефокусоване світло, який вдаряється в межі каналу по всій дистанції. Для цього LED обмежені до використання на короткі дистанції.

Лазери, з іншого боку, можуть фокусуватися до дуже вузького ряду, контролюючи кут падіння. Сигнали лазера охороняють характеристики сигналу на значних дистанціях.

Опто-волоконні конектори

Конектори для оптоволоконного кабелю повинні бути такими точними як кабель безпосередньо. З металевими засобами, не вимагається, щоб зв'язки були точні, поки обидва провідники знаходяться у фізичному контакті. З оптичним волокном, з другого боку, будь-яке неспівпадання одного сегменту ядра або з іншим сегментом або з фотодіодом призводить до відраження сигналу назад до відправника, і будь-яка різниця в розмірі двох сполучених каналів приводить до зміни сигналу. Крім того, зв'язок повинен

бути завершений не надміру щільно. Розрив між двома ядрами призводить до розсіяного сигналу; надмірно щільний зв'язок може стиснути два ядра і змінити відображення.

Даючи ці вимоги, виробники розробили окремі з'єднувачі, які як точно, так і легко використовувати. Всі популярні з'єднувачі - це баррель, сформований і входив в штекери і розетки. Кабель обладнаний штекером, який замикає провідники в розетці пристрою.

Переваги оптичного волокна

Головні переваги оптоволокна над витю парою і коаксіальним кабелем - це опір шуму, менші втрати сигналу і вища смуга пропускання.

Опір шуму. Тому що оптоволокно використовує освітлення швидше, ніж електрику, шум не є коефіцієнтом. Зовнішнє світло, яке може дати завади, блокуване від каналу зовнішньою ізоляцією.

- Менші спотворення сигналу. Відстань оптоволокна є істотно більшою від інших приведених засобів. Сигнал може передаватися на багато кілометрів без вимоги перезапису.
- Вища смуга пропускання. Оптоволокно може підтримувати набагато вищу смугу пропускання (і швидкість передачі даних), ніж вита пара або коаксіальний кабель. Зараз, швидкості передач даних і утилізація смуги пропускання через оптоволокно є обмеженими не засобом передачі, але генерацією сигналу і доступною технологією прийому.

Недоліки оптоволокна

Головні недоліки оптоволокна - це вартість, інсталяція, підтримка і крихкість.

- Вартість. Оптоволокно – дороге, тому що будь-які домішки або недосконалість в ядрі можуть спотворити сигнал, він повинен бути якісним. Також, джерело світла лазера може коштувати тисячі доларів,

порівняних з сотнями доларів для генераторів електричних сигналів.

- Інсталяція/підтримка. Будь-яка грубість або розкол в ядрі оптичного кабелю легко поширюється і змінює сигнал. Всі з'єднання повинні поліруватися і прецизійно об'єднуватися. Всі зв'язки повинні відмінно вирівнюватися і відповідати розміру ядра і повинні забезпечити цілковиту світлонепроникність. Металеві медіа, можуть робитися за допомогою різання і гофрування і використовувати відносно прості інструменти.
- Крихкість. Скловолокло легше розбити, ніж дрiт, що робить його меншим придатним для додатків, де апаратна потрібна мобільність .

Оскільки виробники устаткування поліпшили оптоволокло і витрати падають, високі швидкості передачі даних і імунітет до шуму зробили оптоволокло популярнішим.

7.3. Некеровані носії або безпроводний зв'язок

У наш час з'являється вся більша кількість інформаційних „наркоманів” – людей з потребою постійно знаходитися в підключеному режимі (on-line). Таким користувачам ніякі кабельні з'єднання, будь то вита пара, коаксіальний кабель або оптичне волокло, не підходять. Їм потрібно отримувати дані безпосередньо на переносні комп'ютери, лаптопи, ноутбуки, електронні записники, кишенькові комп'ютери, палмтопи і комп'ютери, вбудовані в наручні годинники. Коротше кажучи, вони вважають за краще користуватися пристроями, не прив'язаними до наземної інфраструктури. Для таких користувачів безпроводний зв'язок є необхідністю. В даному розділі ми познайомимося з основами безпроводного зв'язку, оскільки у нього є ряд інших важливих застосувань, окрім надання доступу в Інтернет охочим побродити по ньому, лежачи на пляжі.

Існує думка, що в майбутньому залишаться тільки два типи зв'язку – оптоволоконний і безпроводний. Всі стаціонарні (тобто не переносні) комп'ютери, телефони, факси тощо, з'єднуюватимуться оптоволоконними кабелями, а всі переносні – за допомогою безпроводного зв'язку.

При деяких обставинах безпроводний зв'язок може мати свої переваги і для стаціонарних пристроїв. Наприклад, якщо прокладка оптоволоконного кабелю ускладнена природними умовами (гори, джунглі, болота тощо), то безпроводний зв'язок може виявитися бажаним. Слід зазначити, що сучасний безпроводний зв'язок зародився на Гавайських островах, де людей розділяли великі простори Тихого океану і звичайна телефонна система виявилася неефективною.

7.3.1. Електромагнітний спектр

Рух електронів породжує електромагнітні хвилі, які можуть розповсюджуватися в просторі (навіть у вакуумі). Це явище було передбачено британським фізиком Джеймсом Клерком Максвелом (James Clerk Maxwell) в 1865 році. Перший експеримент, при якому їх можна було спостерігати, поставив німецький фізик Генріх Герц (Heinrich Hertz) в 1887 році. Число коливань електромагнітних коливань в секунду називається частотою, і вимірюється в герцах (на честь Генріха Герца). Відстань між двома послідовними максимумами (або мінімумами) називається довжиною хвилі. Ця величина традиційно позначається грецькою буквою λ (лямбда).

Якщо в електричний ланцюг включити антену відповідного розміру, то електромагнітні хвилі можна з успіхом приймати приймачем на деякій відстані. На цьому принципі засновані всі безпроводні системи зв'язку.

У вакуумі всі електромагнітні хвилі розповсюджуються з однією і тією ж швидкістю, незалежно від їх частоти. Ця швидкість називається швидкістю світла. Її значення приблизно рівно $3 \cdot 10^8$ м/с, або близько одного фута (30 см) за наносекунду. (Можна було б перевизначити, скориставшись таким

збігом, фут, ухваливши, що він рівний відстані, яку проходить електромагнітна хвиля у вакуумі за 1 нс. Це було б логічніше, ніж вимірювати довжини розміром чобота якогось давно померлого короля.) В міді або склі швидкість світла складає приблизно 2/3 від цієї величини, крім того, залежить від частоти. Швидкість світла сучасна наука вважає верхньою межею швидкостей. Швидше не може рухатися ніякий об'єкт або сигнал.

Величини f , λ і c (у вакуумі) зв'язані фундаментальним співвідношенням

$$\lambda f = c \quad (2.2)$$

Оскільки c є константою, то, знаючи f , ми можемо визначити λ , і навпаки. Існує мнемонічне правило, яке свідчить, що $\lambda f \approx 300$, якщо λ вимірюється в метрах, а f – в мегагерцах. Наприклад, хвилі з частотою 100 МГц мають довжину хвилі близько 3 м, 1000 МГц відповідають 0,3 м, а довжині хвилі 0,1 м відповідає частота 3000 МГц.

На рис. 2.9 зображено електромагнітний спектр. Радіо, мікрохвильовий, інфрачервоний діапазони, а також видиме світло можуть бути використані для передачі інформації за допомогою амплітудної, частотної або фазової модуляції хвиль. Ультрафіолетове, рентгенівське і гамма-випромінювання б були навіть краще завдяки їх високим частотам, проте їх складно генерувати і модулювати, вони погано проходять крізь будівлі і, крім того, вони небезпечні для всього живого. Діапазони, перераховані в нижній частині рис. 2.9, є офіційними назвами ІТУ, заснованими на довжинах хвиль. Так, наприклад, низькочастотний діапазон (LF, Low Frequency) охоплює довжини хвиль від 1 км до 10 км (що приблизно відповідає діапазону частот від 30 кГц до 300 кГц). Скорочення LF, MF і HF позначають Low Frequency (низька частота), Medium Frequency (середня частота) і High Frequency (висока частота) відповідно. Очевидно, при призначенні діапазонам назв ніхто не припускав, що використовуватимуться частоти вище 10 МГц, тому більш високі діапазони

отримали назви VHF (very high frequency – дуже висока частота), UHF (ultrahigh frequency – ультрависока частота, УВЧ), SHF (superhigh frequency – надвисока частота, СВЧ), EHF (Extremely High Frequency – надзвичайно висока частота) і THF (Tremendously High Frequency – жахливо висока частота). Вище за останній діапазон імена поки не придумані, але якщо слідувати традиції, з'являться діапазони Неймовірно (Incredibly), Дивовижно (Astonishingly) і Жахливо (Prodigiously) високих частот (ITF, ATF і PTF).

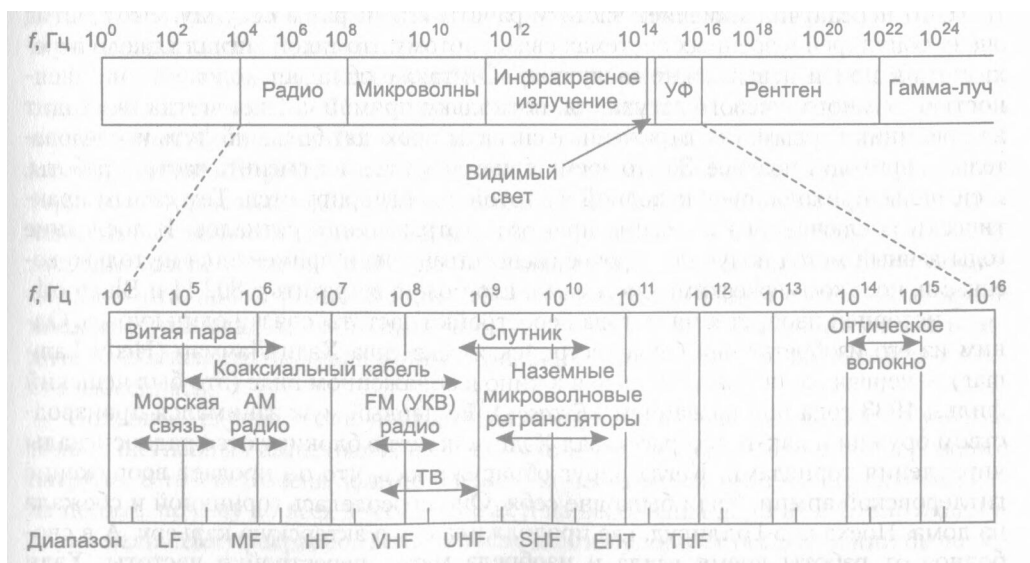


Рис. 2.9. Електромагнітний спектр і його застосування в зв'язку

Кількість інформації, яку може переносити електромагнітна хвиля, пов'язана з частотним діапазоном каналу. Сучасні технології дозволяють кодувати декілька біт на герц на низьких частотах. За деяких умов це число може зростати восьмикратно на високих частотах. Таким чином, по коаксіальному кабелю із смугою пропускання 750 МГц можна передавати декілька гігабіт за секунду. З рис. 2.9 повинно бути зрозуміло, чому розробники мереж так люблять оптоволоконний зв'язок.

Знаючи ширину діапазону довжин хвиль $\Delta\lambda$, ми можемо обчислити відповідний їм діапазон частот Δf і швидкість передачі даних, яку може забезпечити даний діапазон. Чим ширше діапазон, тим вище швидкість

передачі даних. Наприклад, розглянемо 1,30-мікронний діапазон, зображений на рис. 2.5. Тут ми маємо $\lambda = 1,3 \cdot 10^{-6}$ і $\Delta\lambda = 0,17 \cdot 10^{-6}$, так що Δf приблизно рівно 30 ТГц. Тоді, скажімо, при 8 біт/Гц ми одержуємо 240 Тбіт/с.

Більшість систем зв'язку використовує вузькі смуги частот (тобто $\Delta f/f < 1$), що дозволяє забезпечити упевнений прийом сигналу (велике співвідношення ват/герц). Проте іноді використовуються і широкі смуги. При цьому можливі два варіанти. Коли застосовується розширений спектр з перебудовою частоти, то передавач змінює частоту роботи сотні раз в секунду. Цей метод дуже популярний у військових системах зв'язку, тому що такий сигнал важко перехопити і майже неможливо заглушити. Він також має добру захищеність від багатопроменевого загасання, оскільки прямий сигнал завжди приходиться на приймач першим. Всі відображені сигнали проходять більший шлях і, отже, приходять пізніше. За цей час приймач встигає змінити частоту роботи, і сигнали, що приходять з початковою частотою, ним ігноруються. Тим самим практично виключається накладення прямого і відображеного сигналів. За останні роки даний метод отримав широке розповсюдження і застосовується не тільки військовими, але і комерційними системами. Його можна зустріти в 802.11 і Bluetooth.

Ще один метод, що використовує широкую смугу частот, називається розширеним спектром з прямою послідовністю. Він теж стає з часом все більш популярним. Зокрема, цей метод використовується в деяких мобільних телефонах другого покоління, і до третього покоління він стане домінуючим в цій сфері завдяки добрій ефективності саме такого спектру, завадостійкій та іншим властивостям. В деяких безпроводних ЛОМ цей метод працює, тому далі ми ще повернемося до цієї теми.

А поки ми розглядатимемо тільки засоби зв'язку з вузькою частотною смугою. Ми обговоримо питання використання різних областей спектру, починаючи з радіозв'язку.

7.3.2. Радіозв'язок

Радіохвилі просто згенерувати, вони можуть подолати великі відстані, проходити крізь стіни і огинати будівлі, тому їх галузь застосування досить широка. Радіозв'язок встановлюють як в приміщеннях, так і зовні будівель. Крім того, радіохвилі можуть розповсюджуватися одночасно у всіх напрямках, тому для низьких частот не вимагається прицілювання антен передавача і приймача.

В деяких випадках така властивість радіохвиль є зручною, але іноді вона небажане. В 1970-х роках компанія General Motors вирішила оснастити нові автомобілі «кадилак» керованою за допомогою комп'ютера системою антиблокування гальм. Коли водій натискував на педаль гальма, комп'ютер, щоб гальма не заблокували, видавав серію імпульсів команд включення і виключення гальм. Одного прекрасного дня поліцейський, патрулюючий шосе в штаті Огайо, вирішив зв'язатися з своєю ділянкою за допомогою нової портативної радіостанції. При цьому їдучий поряд з ним «кадилак» раптово став скакати, як дикий кінь. Коли офіцер зупинив машину, водій присягнувся, що не робив ніяких дій і що машина раптом просто збісилася.

Подібні випадки стали повторюватися: «кадилаки» іноді божеволіли, але тільки на головних автострадах штату Огайо і лише під наглядом дорожнього патруля. Протягом дуже довгого часу компанія General Motors ніяк не могла зрозуміти, чому у всіх інших штатах і на невеликих дорогах в Огайо «кадилаки» поводитися чудово. Тільки після довгих наполегливих досліджень було знайдене, що проводка «кадилака» була прекрасною антеною для частот, що використовуються новою радіосистемою дорожнього патруля штату Огайо.

Властивості радіохвиль залежать від частоти. При роботі на низьких частотах радіохвилі добре проходять крізь перешкоди, проте потужність сигналу в повітрі різко падає у міру віддалення від передавача. Співвідношення потужності і віддаленості від джерела виражається

приблизно так: $1/r^2$. На високих частотах радіохвилі взагалі мають тенденцію розповсюджуватися виключно по прямій лінії і відображатися від перешкод. Крім того, вони поглинаються, наприклад, дощем. Радіосигнали будь-яких частот схильні перешкодам з боку двигунів з іскрами у щітках і іншого електричного устаткування.

Завдяки здатності радіохвиль розповсюджуватися на великі відстані взаємні перешкоди, що викликаються одночасно працюючими користувачами, є серйозною проблемою. Тому всі держави ведуть дуже строгий облік власників радіопередавачів, за одним виключенням (обговорюваним далі).

В діапазонах VLF радіохвилі LF і MF розповсюджуються уздовж поверхні землі, як показано на рис. 2.10, а. Ці хвилі можна піймати радіоприймачем на відстані близько 1000 км, якщо використовуються низькі частоти, і на дещо менших відстанях, якщо частоти вище. Радіомовлення з амплітудною модуляцією (AM) використовує діапазон середніх хвиль (MF), з цієї причини, наприклад, передачі середньохвильової радіостанції Бостона не чутні в Нью-Йорку. Радіохвилі цих діапазонів легко проникають крізь будівлі, унаслідок чого переносні радіоприймачі працюють і в приміщеннях. Основною перешкодою для використання цих діапазонів для передачі даних є їх відносно низька пропускна спроможність (див. рівняння (2-3).

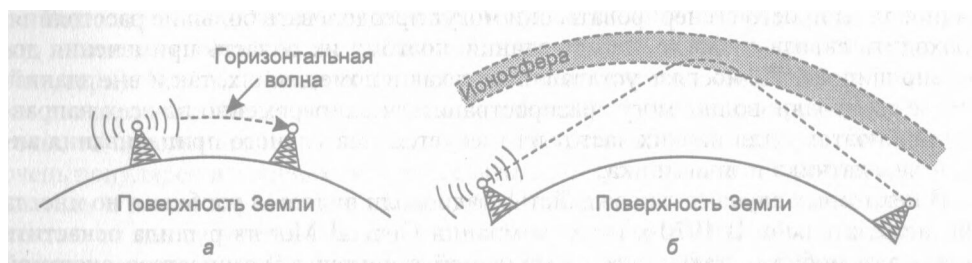


Рис. 2.10. Хвилі діапазонів VLF, LF і MF огинають нерівності поверхні Землі (а); хвилі діапазону HF відображаються від іоносфери (б)

Радіохвилі діапазонів HF і VHF поглинаються землею. Проте ті з них, які доходять до іоносфери, що є шаром заряджених частинок, розташованим на висоті від 100 до 500 км, відображаються нею і посиляються назад до поверхні Землі, як показано на рис. 2.10, б. За певних атмосферних умов сигнал може відобразитися кілька разів. Радіоаматори використовують такі діапазони частот для телекомунікації. Військові також здійснюють зв'язок в діапазонах HF і VHF.

7.3.3. Зв'язок у мікрохвильовому діапазоні

На частотах вище 100 МГц радіохвилі розповсюджуються майже по прямій, тому можуть бути сфокусовані у вузькі пучки. Концентрація енергії у вигляді вузького пучка за допомогою параболічної антени (ніби всім відомої супутникової телевізійної тарілки) приводить до поліпшення співвідношення сигнал/ шум, проте для подібного зв'язку передаюча і приймаюча антени повинні бути досить точно направлені один на одного. Крім того, подібна спрямованість дозволяє використовувати декілька передавачів, встановлених в ряд, сигнали від яких приймаються також встановленими в ряд приймальними антенами без взаємних перешкод. До винаходу оптоволоконного зв'язку подібні мікрохвильові антени протягом десятків літ склали основу міжміського телефонного зв'язку. Насправді компанія MCI, один з основних конкурентів AT&T, побудувала цілу систему мікрохвильового зв'язку з передачею сигналу від однієї башти до іншої. Відстань між антенами складала десятки кілометрів. Ця технологія знайшла віддзеркалення навіть в назві компанії: аббревіатура оператора міжміського зв'язку MCI спочатку розшифровувалася як Microwave Communications, Inc. З тих пір, втім, MCI вже встигла перейти на оптоволоконні мережі і об'єдналася з компанією WorldCom.

Мікрохвилі розповсюджуються строго по прямій, тому при дуже великому віддаленні антен один від одного на шляху проходження сигналу

може виявитися земна поверхня (наприклад, так трапиться, якщо поставити передавач в Сан-Франциско, а приймач – в Амстердамі). Чим вищі башти ретрансляцій, тим більша може бути відстань між ними. Максимальну відстань між повторювачами можна дуже грубо оцінити як корінь квадратний з їх висоти. Так, при висоті ретрансляторів 100 м відстань між ними може бути близько 80 км.

На відміну від радіохвиль з нижчими частотами, мікрохвилі погано проходять крізь будівлі. Крім того, навіть при точному фокусуванні променя на приймальній антені при проходженні крізь простір промінь досить значно розширюється в діаметрі. Частина хвиль може відобразитися атмосферними шарами, завдяки чому на своєму шляху до приймальної антени відображені хвилі пройдуть більшу відстань, ніж прямі. Це означає, що перші відрізнятимуться від останніх по фазі, що може привести до ослаблення сигналу. Такий ефект називається багатопроменевим загасанням і досить часто є серйозною проблемою. Наявність цього ефекту залежить від погоди і від частоти. Деякі оператори зв'язку тримають близько 10 % своїх каналів вільними і тимчасово перемикаються на них у разі виникнення багатопроменевого загасання на якій-небудь частоті.

Потреби у все більшому діапазоні частот примушують постійно удосконалювати технологію, завдяки чому для зв'язку використовуються все більш високі частоти. Діапазони частот до 10 ГГц тепер застосовуються досить широко, проте при частотах вище 4 ГГц з'являється нова проблема: поглинання водою. Довжина хвиль при такій частоті складає всього декілька сантиметрів, і такі хвилі сильно поглинаються дощем. Такий ефект може бути вельми корисний для тих, хто хоче спорудити величезну зовнішню мікрохвильову піч, щоб смажити пролітаючих пташок, проте він є серйозною проблемою в області радіозв'язку. Поки що єдиним рішенням є відключення ліній зв'язку, що перетинаються смугою дощу, і перемикання на обхідні шляхи.

Мікрохвильовий радіозв'язок став настільки широко використовуватися в міжміській телефонії, стільникових телефонах, телемовленні і інших областях, що почав сильно відчуватися брак ширини спектру. Даний зв'язок має ряд переваг перед оптоволоконном. Головне з них складається в тому, що не потрібно прокладати кабель, відповідно, не потрібно платити за арендувати землі на шляху сигналу. Достатньо купити маленькі ділянки землі через кожні 50 км і встановити на них вежі ретрансляцій, обійшовши, таким чином, телефонні кабельні системи. Саме тому корпорації MCI вдалося швидко впровадитися в ринок міжміського зв'язку. Компанія Sprint пішла іншим шляхом: вона була утворена Південною Тихоокеанською залізницею (South Pacific Railroad), яка вже володіла правами на велику ділянку шляху і просто закопувала кабель поряд із залізничним полотном.

Крім того, мікрохвильовий зв'язок є недорогим. Установка двох примітивних веж (це можуть бути просто великі стовпи на чотирьох розтяжках) з антенами на кожній з них, швидше за все, обійдеться дешевше, ніж прокладка 50 км кабелю в перенаселеній міській місцевості або в горах. Це може бути також дешевшим, ніж арендувати оптоволоконної лінії у телефонної компанії, особливо якщо телефонна компанія ще не повністю розплатилася за мідний кабель, який вона вже змінила на оптоволоконний.

7.3.4. Інфрачервоні і міліметрові хвилі

Інфрачервоне і міліметрове випромінювання без використання кабелю широко застосовується для зв'язку на невеликих відстанях. Дистанційні пульти управління для телевізорів, відеомагнітофонів і стереоапаратури використовують інфрачервоне випромінювання. Вони відносно направлені, дешеві і легко встановлювані, але мають один важливий недолік: інфрачервоне випромінювання не проходить крізь тверді об'єкти (спробуйте встати між телевізором і пультом). Ми почали з розгляду довгих

радіохвиль і поступово просуваємося до видимого світла, і вже інфрачервоні хвилі мало нагадують радіохвилі і поводяться, як світло.

З другого боку, той факт, що інфрачервоні хвилі не проходять крізь стіни, є також і позитивним. Адже це означає, що інфрачервона система в одній частині будівлі не інтерферуватиме з подібною системою в сусідній кімнаті – ви, на щастя, не зможете управляти з свого пульта телевізором сусіда. Крім того, це підвищує захищеність інфрачервоної системи від прослуховування в порівнянні з радіосистемою. З цієї причини для використання інфрачервоної системи зв'язку не потрібна державна ліцензія, на відміну від радіозв'язку (окрім діапазонів ISM). Зв'язок в інфрачервоному діапазоні застосовується в настільних обчислювальних системах (наприклад, для зв'язку ноутбуків з принтерами), але все таки не грає суттєвої ролі в телекомунікації.

7.3.5. Зв'язок у видимому діапазоні

Ненаправлені оптичні сигнали використовувалися протягом декількох століть. Герой американської війни за незалежність Пол Ревер (Paul Revere) в 1775 році в Бостоні використовував двійкові оптичні сигнали, інформуючи з дзвіниці Старої Північної церкви (Old North Church) населення про прибуття англійців. Більш сучасним додатком є з'єднання локальних мереж в двох будівлях за допомогою лазерів, встановлених на дахах. Зв'язок за допомогою когерентних хвиль лазера є суто однонаправленим, тому для двостороннього зв'язку необхідно на кожному даху встановити по лазеру і по фотодетектору. Така технологія дозволяє організувати зв'язок з дуже високою пропускною спроможністю при дуже низькій ціні. Крім того, така система досить просто вмонтовується і, на відміну від мікрохвильового зв'язку, не вимагає ліцензії FCC (Федеральної комісії зв'язку США).

Вузкий промінь є сильною стороною лазера, проте він створює і деякі проблеми. Щоб потрапити міліметровим променем в мішень діаметром 1 мм

на відстані 500 м, потрібне снайперське мистецтво найвищої проби. Звичайно на лазери встановлюються лінзи для невеликого роз фокусування променя.

Недоліком лазерного променя є також нездатність проходити крізь дощ або густий туман, хоча в сонячні ясні дні він працює чудово (рис. 2.12). Цей ефект можна спостерігати неозброєним оком в жаркий день на шосе або над гарячим радіатором автомобіля. Борючись з цим ефектом, астрономи розташовують свої телескопи високо в горах, подалі від атмосфери.

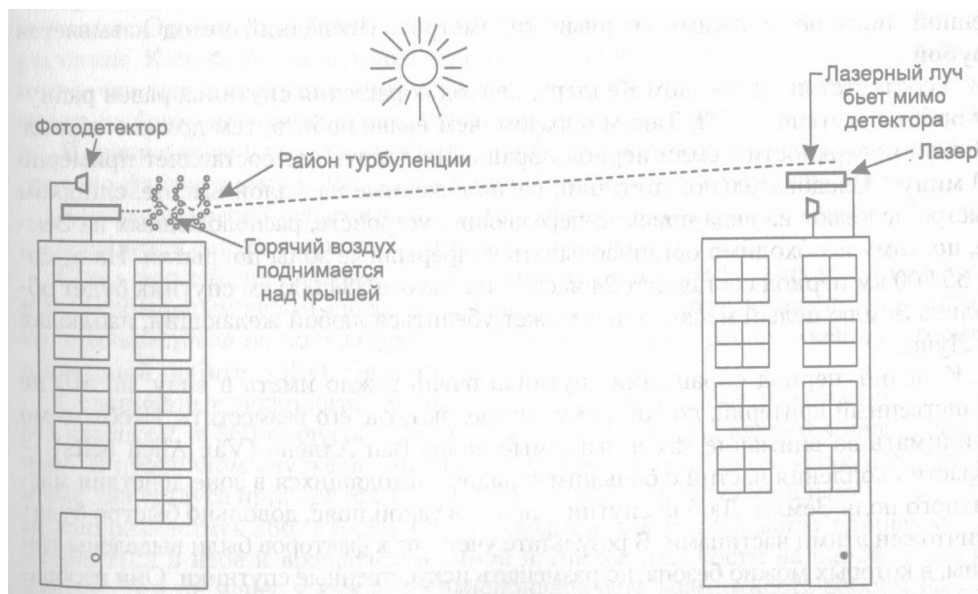


Рис. 2.12. Конвекційні потоки заважають працювати лазерній системі. На малюнку зображена двонаправлена система з двома лазерами

7.3.6. Супутниковий зв'язок

Передача супутника подібна до мікрохвильовій передачі при якій один з учасників є супутником, що виведений на орбіту землі. Принцип є таким самим, як наземний мікрохвильовий, із супутником який діє подібно до супервисокої антени і повторювача repeater (рис, 7.34). Хоча сигнал передачі супутника повинен передаватися прямими лініями, обмеження, нав'язані дистанції кривизною землі, зменшені. На цьому шляху, зміни супутника

доставляють мікрохвильові сигнали до континентів і океанів одним стрибком.

Figure 7.33 *Horn antenna*

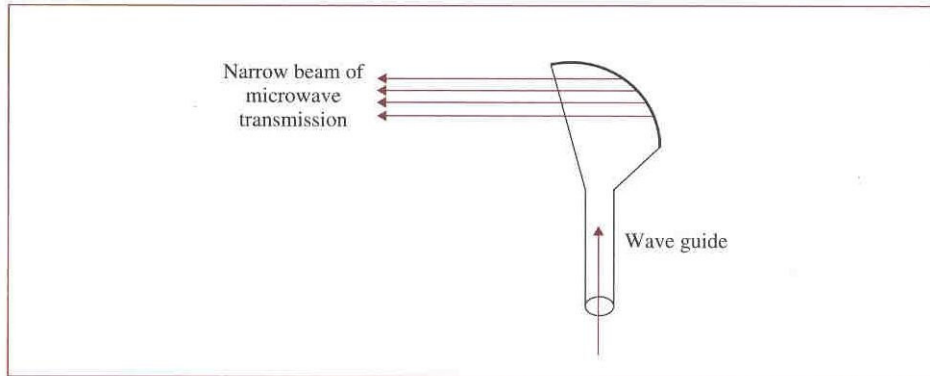


Рис. 7.33. Антена Horn

Figure 7.34 *Satellite communication*

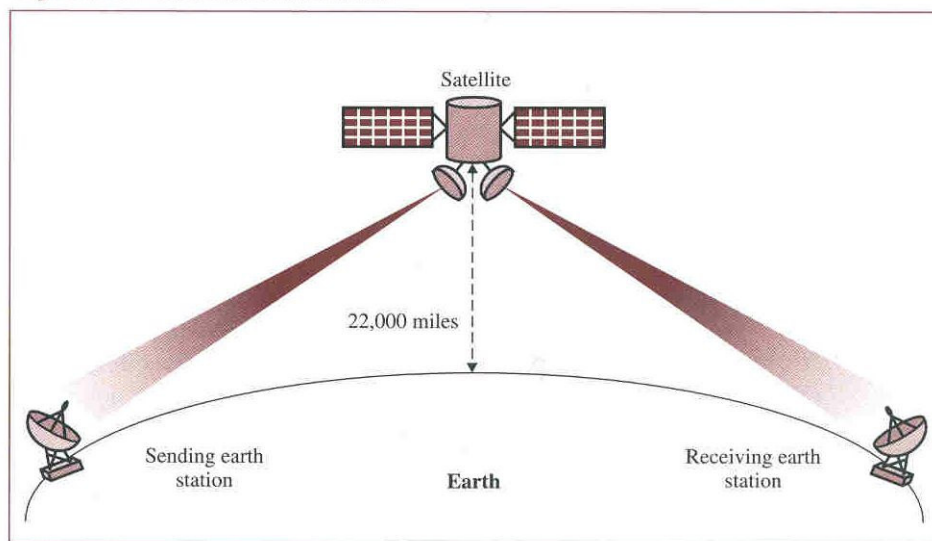


Рис. 7.34. Зв'язок через супутник

Мікрохвильовий супутник може забезпечити здатність передачі назад і вперед до будь-якої точки на землі на будь-яку віддаль. Ця перевага робить високоякісну комунікацію доступною до нерозвинених частин світу без вимоги величезних інвестицій на створення інфраструктури. Супутники є

надзвичайно дорогими, але аренда часу або частот може бути відносно дешевою.

Геосинхронні супутники Geosynchronous

Розповсюдження вимагає, щоб пересилаюча і приймаюча антени були підключені одночасно (одна антена повинна мати іншу в полі зору). Тому, супутник, що рухається, швидше або повільніше, ніж обертання землі корисний тільки на короткі періоди часу (точно так, як поламаний годинник точно показує час двічі на день). Щоб гарантувати постійну комунікацію, супутник повинен переміщуватися на тій же швидкості як і земля таким чином, що він, здається, зависає над однією точкою. Такі супутники називаються геосинхронними geosynchronous.

Тому що орбітальна швидкість залежить на віддалі від планети, тільки одна орбіта може бути геосинхронною. Ця орбіта лежить в екваторіальній площині і є приблизно 22,000 миль від поверхні землі.

Але один геосинхронний супутник не може охоплювати цілу землю. Один супутник на орбіті має контакт з величезною кількістю місць, але кривизну землі видно з багатьох місць ззовні планети. Це мінімум три супутники, рівновіддалені від одного одного на геосинхронній орбіті, щоб забезпечити глобальну передачу. На рис. 7.35 показано три супутники розміщені на 120 градусів один від одного на геосинхронній навкруг екватора. Вигляд з від Північного полюса.

Figure 7.35 Satellites in geosynchronous orbit

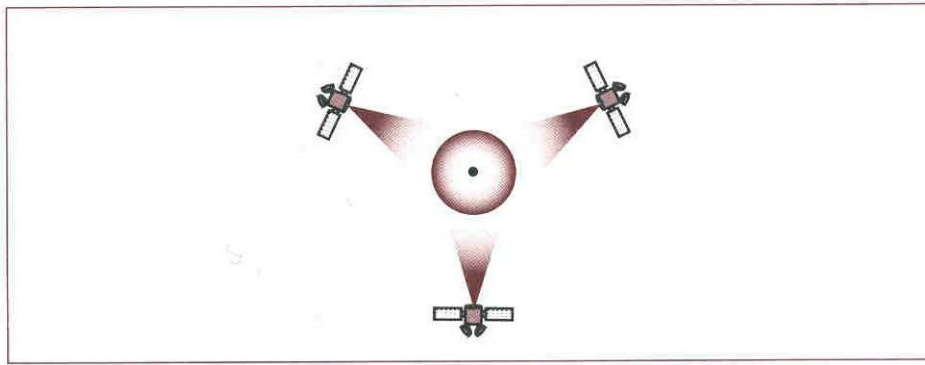


Рис. 7.35. Супутники на геосинхронній орбіті

Частотні діапазони для зв'язку через супутник

Частоти зарезервовані для мікрохвильової дуги комунікацій супутника в гігагерцах (GHz). Кожен супутник посилає і одержує у двох різних групах. Передача від землі до супутника називається uplink. Передача від супутника до землі називається downlink. В таблиці 7.2 дано назви і частоти для кожного ряду.

Таблиця 7.2. Частотні діапазони супутника

Band	Downlink	Uplink
C	3.7 to 4.2 GHz	5.925 to 6.425 GHz
Ku	11.7 to 12.2 GHz	14 to 14.5 GHz
Ka	17.7 to 21 GHz	27.5 to 31 GHz

7.3.7. Мобільний телефонний зв'язок

Традиційна телефонна система (навіть якщо вона одного прекрасного дня повністю перейде на багатогігабітний оптоволоконний кабель) ніколи не зможе задовольнити потреби величезної групи користувачів – людей, що

знаходяться в дорозі. Люди хочуть отримати можливість бути на зв'язку буквально скрізь: в автомобілі, літаку, басейні і т.д. Через декілька років не залишиться такої точки на Землі, звідки не можна було б подзвонити по телефону, послати e-mail і вийти в Інтернет. Принаймні, люди чекають саме цього. Отже, інтерес до безпроводної телефонії продовжуватиме рости. В наступних розділах ми розглянемо подробиці, що стосуються цієї теми.

Безпроводні телефони бувають двох типів: домашні радіотелефони і мобільні телефони (іноді звані стільниковими телефонами). Радіотелефони є пристроями, що складаються з базової станції і однієї або декількох переносних трубок. Вони призначені для використання усередині житла або в безпосередній близькості від нього. Їх ніколи не об'єднують в мережі, тому надалі ми їх розглядати не будемо. Натомість ми більш детально розглянемо мобільні системи зв'язку, які використовуються як для передачі мови, так і для обміну даними.

На даний момент можна виділити вже три різні покоління мобільних телефонів, що здійснюють:

- 1) аналоговий голосовий зв'язок;
- 2) цифровий голосовий зв'язок;
- 3) цифровий голосовий зв'язок і обмін даними (Інтернет, електронна пошта і т. д.).

Хоча велика частина нашого обговорення буде присвячена технічному влаштуванню цих систем, не можна не відзначити той цікавий факт, що величезний вплив на процес розвитку технологій цього типу надали політичні і економічні рішення. Перша мобільна система була запропонована американською компанією AT&T, яка, з відома комісії FCC, встановила мобільний зв'язок на всій території Сполучених Штатів. В результаті ціла країна знайшла єдину (аналогову) систему зв'язку, і мобільний телефон, куплений, наприклад, в Каліфорнії, успішно працював в Нью-Йорку. А в

Європі все вийшло навпаки: коли туди прийшов мобільний зв'язок, кожна країна кинулася розробляти власні системи, внаслідок чого програли все.

Проте Європа в чомусь навчилася на своїх помилках, і з появою цифрових систем державні телефонні служби об'єдналися, щоб створити єдиний стандарт (GSM), по якому могли б працювати будь-які європейські мобільні телефони. На той час в США держава вийшла з бізнесу, пов'язаного із стандартизацією, тому нові цифрові мобільні системи стали турботою комерційних структур. Це привело до того, що різні виробники стали випускати різнотипні мобільні телефони, і в США з'явилися дві основні (і одна трохи менше) несумісні цифрові мобільні телефонні системи.

Не дивлячись на початкове лідерство США, Європа зараз обійшла Штати по популярності мобільного зв'язку. Однією з причин є, звичайно, єдина європейська система. Ще одна причина досить забавна. Вона пов'язана з телефонними номерами. В США не розрізняються номери мобільних і стаціонарних телефонів. Тому немає ніякої можливості взнати, набираючи номер, наприклад, (212) 234-5678, потрапите ви на міський телефон (дешевий або взагалі безкоштовний дзвінок) або на стільниковий (дорогий дзвінок). Щоб люди не нервували кожного разу, гадаючи, куди вони дзвонять, телефонні компанії примусили абонентів стільникового зв'язку платити за вхідні дзвінки. Але багато кого таке рішення відлякало – люди стали боятися витратити велику суму грошей на один тільки прийом вхідних дзвінків. В Європі у мобільних телефонів номер починається з особливого коду (звичайно це число в районі 800-900), тому його відразу можна взнати. Значить, можна встановити звичайне правило, прийняте в телефонії: платить той хто телефонує (за винятком міжнародних дзвінків, де платять обидва).

Третій чинник, що зробив великий вплив на популярність мобільних систем, – це широке розповсюдження телефонів з передплатою розмов (до 75 % в деяких регіонах). Їх можна купити в багатьох магазинах, і це не представляє особливий складності. Вони можуть бути заряджений,

наприклад, на 20 або 50 євро, а при зниженні балансу до нуля їх можна «перезарядити» за допомогою секретного PIN-коду. Тепер такі мобільні телефони є у будь-якого підлітка, і батьки можуть бути на зв'язку з своїм чадом, не побоюючись при цьому, що він самостійно наговорить по телефону на кругленьку суму. Якщо мобільний телефон використовується лише епізодично, то це обходиться практично безкоштовно, оскільки майже завжди можна знайти тариф, на якому відсутня абонентна платня або платня за вхідні дзвінки.

Мобільні телефони першого покоління: аналогова передача мови

Проте досить про політику і бізнес. Поговоримо про технології. Почнемо наш розгляд з найперших з них. Мобільні радіотелефони епізодично застосовувалися в морському судноплаванні і військовому зв'язку в перші десятиріччя ХХ століття. В 1946 році в Сент-Луї була встановлена перша система автомобільних телефонів. Вона мала один великий передавач, розташований на даху високої будівлі, і єдиний канал прийому і передачі даних. Щоб почати розмову, потрібно було натискувати на кнопку, яка включала передавач і відключала приймач. Такі системи, відомі як тангентні, існували в деяких містах ще в кінці 50-х. СВ-радіо, системи, що використовуються у таксі і поліцейських машинах, часто використовують цю ж технологію.

В 1960-х роках з'явилася вдосконалена система мобільного телефонного зв'язку, IMTS (Improved Mobile Telephone System). Вона також використовувала потужний (200-ват) передавач, встановлений на вершині гори, але вже мала два частотні канали: один для відправки, інший – для прийому даних. Тому мікрофонна кнопка вже не була потрібна. Завдяки розділенню вхідних і вихідних каналів користувачі мобільних телефонів не могли чути чужі розмови (на відміну від тангентних систем, що використовуються у таксі).

IMTS підтримувала 23 канали в діапазоні від 150 до 450 МГц. Через невелике число каналів користувачам часто довго доводилося чекати звільнення лінії. До того ж через сильну потужність передавача суміжні системи повинні були розташовуватися на відстані декількох сотень кілометрів один від одного щоб уникнути інтерференції сигналів. Загалом, через низьку місткість ця система була визнана непрактичною.

Вдосконалений мобільний телефонний зв'язок (AMPS)

Все змінилося з появою системи вдосконаленого мобільного телефонного зв'язку, AMPS (Advanced Mobile Phone System), винайденою компанією Bell Labs і вперше встановленої в США в 1982 році. Вона також використовувалася в Англії, де називалася TACS, і в Японії – під ім'ям MCS-L1. Не дивлячись на те що зараз ця система вже пішла в минуле, ми все ж таки її розглянемо, оскільки багато її фундаментальних властивостей були напряму успадковувано її цифровим послідовником, D-AMPS (для сумісності із старим устаткуванням).

В будь-якій мобільній телефонній системі географічний регіон обхвату ділиться на стільники (звідси іноді вживана назва – «стільникові телефони»). В AMPS розмір стільників складає звичайно від 10 до 20 км; в цифрових системах стільники ще дрібніші. Кожний стільник працює на своїх частотах, не пересічних з сусідніми. Лежача в основі телефонної системи AMPS ідея розбиття території на відносно невеликі осередки і використання одних і тих же частот в різних (але не сусідніх) осередках дає цій системі значно великі можливості в порівнянні з більш ранніми системами. Тоді як в системі IMTS на території діаметром 100 км для кожного дзвінка була потрібна своя частота, система AMTS в тій же області могла складатися із ста десятикілометрових стільників і підтримувати від 5 до 10 дзвінків на одній і тій же частоті в сильно видалених один від одного осередках. Крім того, невеликі розміри стільників означають меншу потужність, потрібну для

передавачів, а значить, і меншу вартість пристроїв. Телефонні трубки мають вихідну потужність близько 0,6 Вт, передавачі в автомобілях – близько 3 Вт, що є максимальною потужністю, яку дозволяє Федеральна комісія зв'язку США (Federal Communication Commission, FCC).

Ідея повторного використання частоти проілюстрована на рис. 2.35, а, Стільники мають форму, близьку до кола, проте на моделі їх легше представити у вигляді шестикутників. В лівій частині малюнка всі стільники одного розміру. Вони з'єднані в групи по сім стільників. Кожна буква відповідає певному набору частот. Зверніть увагу на те, що між осередками з однаковими наборами частот розташовується буфер приблизно в два осередки вширшки, в якому дані частоти не використовуються – це забезпечує добре розділення сигналів однакових частот і низький рівень перешкод.

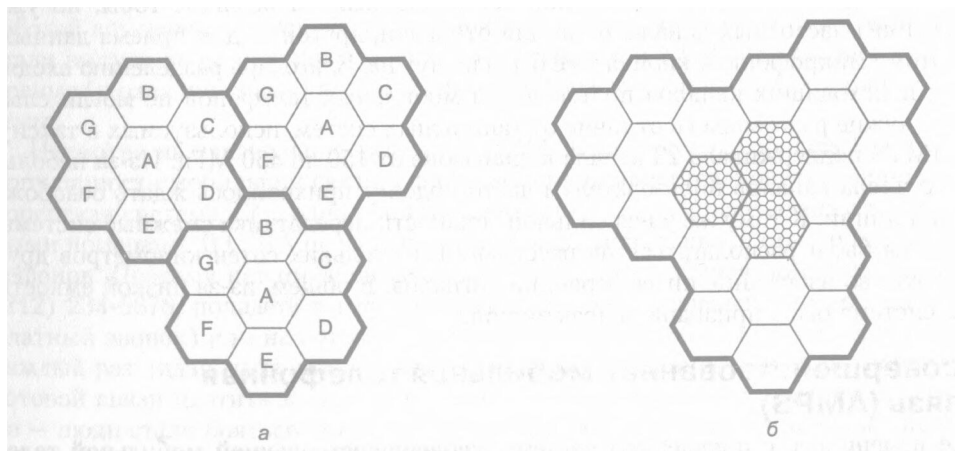


Рис. 2.35. Повторне використання частоти (а); розбиття на мікростільники (б)

Головна задача полягає в тому, щоб знайти відповідні піднесеності для розміщення антен базових станцій. Для вирішення цієї проблеми багато операторів зв'язку уклали договори з Римською католицькою церквою, оскільки останній належить значна кількість високих будов в різних країнах. Зручно і те, що всі вони знаходяться під єдиним управлінням.

Якщо в якому-небудь регіоні кількість користувачів зростає настільки, що система переповнюється, то потужність передавачів зменшується, а переповнені стільники розбиваються на стільники меншого розміру (мікростільники), як показано на рис. 2.35, б.

В центрі кожного осередку розташовується базова станція (БС), з якою зв'язуються всі телефони, що знаходяться в її зоні дії. Базова станція складається з комп'ютера і приймача/передавача, сполученого з антеною. В невеликих системах всі базові станції сполучені з одним пристроєм, званім MTSO (Mobile Telephone Switching Office – комутатор мобільних телефонів) або MSC (Mobile Switching Center – мобільний комутаційний центр). Великій системі може бути потрібно декілька комутаторів, які з'єднуються з комутатором другого рівня, і т.д. Комутатори мобільних телефонів є аналогами крайових телефонних станцій і справді з'єднуються хоча б з одним крайовим комутатором звичайної телефонної системи. Комутатори мобільних телефонів зв'язуються з базовими станціями, один з одним і з комутатором телефонною сіттю загального користування (PSTN, Public Switched Telephone Network), побудованою на основі комутації пакетів.

В кожний момент часу мобільний телефон логічно знаходиться в зоні дії одного осередку і управляється базовою станцією цього осередку. Коли телефон фізично покидає осередок, його базова станція помічає ослаблення сигналу і опитує всі навколишні станції, наскільки добре вони чують сигнал цього телефону. Потім базова станція передає управління даним телефоном осередку, одержуючому від неї найсильніший сигнал, таким чином визначаючи осередок, в який перемістився мобільний телефон. Після цього телефон інформується про перехід у ведення нової БС, і якщо у цей момент ведеться розмова, телефону буде запропонований перемкнутися на новий канал (оскільки в сусідніх стільниках однакові частотні канали не використовуються). Подібний процес називається передачею (handoff) і займає близько 300 мс. Призначення каналу здійснює комутатор мобільних

телефонів MTSO, що є центральним нервом системи. Базові станції є всього лише радіоретрансляторами.

Передача може здійснюватися двома способами. При м'якій передачі телефон переходить у ведення нової базової станції ще до відходу із старої. При цьому не відбувається навіть короткочасного пропадання зв'язку. Недоліком такого методу є те, що у момент переходу з однієї на іншу телефон повинен працювати одночасно на двох частотах. Телефони першого і другого покоління цього робити не уміють.

При жорсткій передачі стара базова станція обриває зв'язок з телефоном ще до того, як нова узяла його під свою опіку. Якщо остання не може протягом якогось часу налагодити зв'язок з телефоном (наприклад, унаслідок відсутності вільних частот), то розмова може обірватися. Користувач, звичайно, помітить це, але нічого не поробиш – так іноді трапляється при використуванні даної технології.

Канали

Система AMPS використовує 832 дуплексні канали, кожний з яких складається з пари сімплексних каналів. 832 сімплексні канали передачі розташовуються в діапазоні від 824 до 849 МГц, і ще 832 сімплексні канали прийому – від 869 до 894 МГц. Ширина кожного каналу складає 30 кГц. Таким чином, для розділення каналів в системі AMPS використовується частотне ущільнення.

В діапазоні 800 МГц довжина радіохвиль складають близько 40 см. Такі радіохвилі розповсюджуються строго по прямій лінії. Вони поглинаються деревами і відображаються від поверхні землі і будівель. Може трапитися так, що сигнал з мобільного телефону досягне базової станції по прямому шляху, але, крім того, з невеликим запізненням потрапить на ту ж станцію, відобразившись від землі або будівлі. Такий ефект може привести до появи

луни або спотворення сигналу (багатопроменеве загасання). Іноді можна почути віддалену розмову, що відобразилася кілька разів.

Всі 832 канали можна розділити на чотири категорії:

1. Управляючі канали (від бази до мобільного телефону) для управління системою.
2. Пейджінгові канали (від бази до мобільного телефону) для передачі повідомлень мобільним користувачам.
3. Канали доступу (двонаправлені) для встановлення з'єднання і призначення каналів.
4. Канали даних (двонаправлені) для передачі голосу, факсу або даних.

Для управління резервується 21 канал. Вони прошиваються в програмованому пристрої (ППЗУ) кожного телефону, що запам'ятовує. Оскільки одні і ті ж частоти не можуть використовуватися в сусідніх стільниках, те число голосових каналів, доступних в межах одного осередку, значно менше 832 – звичайно близько 45.

Управління викликом

Кожний мобільний телефон в системі AMPS забезпечується 32-розрядним порядковим номером і 10-значним телефонним номером, які записуються в ППЗУ телефону. Телефонний номер складається з 3-значного коду області, що займає 10 біт, і 7-значного номери абонента, займаючі 24 біти. При включенні телефон сканує запрограмований список з 21 управляючого каналу, в якому він шукає найсильніший сигнал.

Потім телефон передає в ефір свій 32-розрядний порядковий номер і 34-розрядний телефонний номер. Як і вся управляюча інформація в системі AMPS, цей пакет посилається в цифровій формі кілька разів із застосуванням завадостійкого кодування, хоча самі голосові канали є аналоговими.

Коли базова станція чує цей сигнал, вона передає повідомлення комутатору MTSO, який фіксує появу нового користувача, а також інформує

«домашній комутатор» абонента про його нове місцеположення. Звичайно мобільний телефон реєструється приблизно кожні 15 хвилин.

Щоб подзвонити з мобільного телефону, його власник включає телефон, вводить номер і натискає клавішу SEND. При цьому телефон посилає набраний телефонний номер разом з своїми ідентифікаторами по каналу доступу. Якщо при цьому відбувається колізія, то телефон повторює спробу пізніше. Коли базова станція одержує запит, вона інформує про це комутатор. Якщо той хто дзвонить є клієнтом оператора зв'язку, якому належить даний комутатор (або одного з її партнерів), тоді комутатор шукає для нього вільний канал. Якщо такий канал знаходиться, то номер цього каналу посилається назад по управляючому каналу. Потім мобільний телефон автоматично перемикається на вибраний голосовий канал і чекає, поки той, кому дзвонять, відповість.

Вхідні дзвінки обробляються інакше. Базова станція знаходиться в режимі очікування, телефони постійно прослуховують пейджинговий канал, чекаючи адресованих їм повідомлень. Коли поступає дзвінок на мобільний телефон (із звичайного або іншого мобільного телефону), то пакет посилається на «домашній комутатор», якому повинне бути відоме поточне місцезнаходження абонента. Цей пакет пересилається на базову станцію в його поточному осередку, який посилає по пейджинговому каналу повідомлення типу: «Елемент 14, ви тут?». При цьому телефон, якому дзвонять, по управляючому каналу відповідає: «Так». Тоді базова станція його повідомляє: «Елемент 14, вам дзвінок по каналу 3». Після цього стільниковий телефон перемикається на канал 3 і починає видавати звукові сигнали (або програвати мелодію, яку власнику подарували на день народження).

Друге покоління мобільних телефонів: цифрова передача голосу

Перше покоління стільникових телефонних систем було аналоговим. Друге покоління є цифровим. Як не було ніяких чітких стандартів в першому поколінні мобільних телефонів, так не з'явилися вони і до другого покоління. Зараз використовуються чотири системи другого покоління: D-AMPS, GSM, CDMA і PDC. Далі ми обговоримо перші три з них. PDC знайшла застосування тільки в Японії і є, насправді, модифікацією D-AMPS, направленою на збереження сумісності з японським аналоговим устаткуванням першого покоління. Назва PCS (Personal Communications Services – персональна служба зв'язку) іноді використовується в літературі по маркетингу і означає систему другого покоління (цифрову, розуміє). Спочатку так називався телефон, що працює в діапазоні 1900 МГц, втім, зараз відмінності майже стиралися.

D-AMPS – цифровий вдосконалений мобільний зв'язок

Другим поколінням AMPS є повністю цифрова система D-AMPS. Вона описується міжнародним стандартом IS-54 і його послідовником – IS-136. Система D-AMPS була розроблена так, щоб вона могла успішно співіснувати з AMPS і мобільні телефони першого і другого покоління могли працювати одночасно в одному і тому ж стільнику.

Зокрема, D-AMPS використовує ті ж 30-герцові канали, що і AMPS. Вони розташовуються в тому ж діапазоні, тобто може вийти так, що якийсь канал буде аналоговим, а сусідні з ним канали – цифровими. Залежно від конкретного набору телефонів в даному осередку її комутатор визначає, які канали цифрові, які аналогові, і може динамічно міняти їх тип залежно від того, які телефони потрапляють або виходять із зони дії базової станції осередку. Коли D-AMPS була представлена як нова служба, для неї був виділений додатковий діапазон, з розрахунком на збільшення навантаження. Вихідні канали розташували на частотах 1850-1910 МГц, а відповідні вхідні канали – на частотах 1930-1990 МГц. Як і в AMPS, канали парні. В цій смузі

довжина хвиль складає 16 см, тому стандартна антена розміром в четверть довжини хвилі буде розміром всього лише 4 см, що дає можливість створити більш компактні телефони. Проте багато телефонів D-AMPS можуть використовувати обидва діапазони (як 850, так і 1900 МГц), що дозволяє використовувати збільшений набір доступних каналів.

В мобільному телефоні системи D-AMPS голосовий сигнал захоплюється мікрофоном, оцифровується і стискається при допомозі складнішої моделі, ніж дельта-модуляція і схема прогнозу, які ми вивчали раніше. Метод компресії в даному випадку враховує особливості людського голосу, стискаючи мову із стандартних 56 Кбіт/с (PCM-кодування) до 8 Кбіт/с і навіть менше. Стиснення проводиться спеціальною схемою, званою вокодером, прямо в телефоні, а не на базовій або комутаційній станції. Це зменшує розміри інформації, яку необхідно передати в ефір. При використуванні стаціонарної телефонії немає ніякого значення в стисненні даних в самому телефонному апараті, оскільки зменшення трафіку в локальній лінії ніяк не впливає на загальну місткість системи.

Коли ж йдеться про мобільний зв'язок, то в оцифровці і стисненні даних в самій трубці є значна вигода: достатньо сказати, що три абоненти D-AMPS можуть одночасно використовувати одну і ту ж пару частотних каналів за рахунок мультиплексування з розділенням часу. Кожна пара частот підтримує швидкість 25 кадрів/с (40 мс на кадр). Кадри складаються з шести часових інтервалів по 6,67 мс, як показано на рис. 2.36 для самої низькочастотної каналної пари.



Рис. 2.36. Канал D-AMPS з трьома абонентами (а); канал D-AMPS з шістьма абонентами (б)

Кожний кадр обслуговує трьох користувачів, які по черзі займають вихідний і вхідний канали. Під час першого кадрового інтервалу (рис. 2.36, а), наприклад, користувач 1 може передавати дані на базову станцію, а в цей час користувач 3 може приймати дані. Кадровий інтервал складається з 324 біт, з них 64 використовуються для організації захисного інтервалу, синхронізації і функцій управління. Таким чином, користувачу надається 260 біт. З них 101 використовується для виправлення помилок при передачі по зашумленному ефіру, тому в чистому вигляді для корисних даних залишається лише 159 біт. При швидкості 50 інтервалів в секунду пропускна спроможність, доступна для передачі стислої мовної інформації, складає близько 8 Кбіт/с, тобто 1/7 стандартної пропускної спроможності GSM. Використовування поліпшених алгоритмів стиснення може дозволити укласти мову в 4 Кбіт/с, в цьому випадку один кадр може використовуватися одночасно шістьма абонентами, як показано на рис. 2.36, б. З погляду операторів мобільного зв'язку, можливість стиснення даних в 3-6 разів щодо AMPS – це велика перемога. Цим пояснюється популярність «персональних служб зв'язку». Звичайно, якість звуку при 4 Кбіт/с не порівняти з 56 Кбіт/с, проте деякі оператори, проте, рекламують високоякісний звук, який можна нібито порівняти із звуком Hi-Fi апаратури. Але повинне бути очевидний, що канал 8 Кбіт/с ніколи не дасть навіть якості стародавнього модему на 9600

біт/с. Структура управління D-AMPS досить складна. Не вдаючись в подробиці, можна сказати, що групи з 16 кадрів формують суперкадр, і деяка частина службової інформації з'являється обмежена кількість раз в суперкадрі. Використовуються шість основних управляючих каналів: конфігурація системи, управління в реальному і модельному (не реальному) часі, пейджингові функції, відповіді на запити доступу і короткі повідомлення. Але концептуально робота D-AMPS не відрізняється від роботи AMPS. Коли телефон включений, він знаходиться у контакті з базовою станцією, повідомляючи про себе і прослуховуючи управляючий канал на предмет вхідних дзвінків. Знайшовши новий телефон, комутатор інформує домашню базу абонента про його місцезнаходження, завдяки чому дзвінки можуть бути коректно маршрутизовані.

Системи AMPS і D-AMPS розрізняються методом передачі сигналу телефону з однієї базової станції на іншу. В AMPS цим займається комутатор, не використовуючи ніяких мобільних пристроїв. Як видно з рис. 2.36, в D-AMPS третину часу мобільний телефон займається не передачею і не прийомом інформації. Він використовує порожні кадрові інтервали для вимірювання якості лінії. Коли він знаходить, що сигнал пропадає, то інформує комутатор, який розриває з'єднання з поточною базовою станцією. В цей час телефон може спробувати знайти станцію із сильнішим сигналом. Як і в AMPS, на передачу йде близько 300 мс. Метод, що використовується в D-AMPS, називається передачею за допомогою телефону, MAHO (Mobile Assisted HandOff).

GSM – глобальна система мобільного зв'язку

Система D-AMPS широко поширена в США і (в дещо зміненій формі) в Японії. Решта світу використовує систему під назвою GSM (Global System For Mobile Communications – глобальна система мобільного зв'язку). Втім, GSM починає проникати і в США. В першому наближенні, система GSM

подібна D-AMPS. І та, і інша – стільникові системи. І там, і там застосовується частотне ущільнення. Кожний телефон передає дані на одній частоті, а одержує – на іншій (остання вище першою: 80 МГц в D-AMPS і 55 МГц в GSM). В обох системах пари частотних каналів розбивається за допомогою часового ущільнення на кадрові інтервали, що використовуються декількома абонентами. Проте канали GSM значно ширше за канали AMPS (200 кГц проти 30 кГц) і обслуговують щодо мало додаткових користувачів (8 проти 3), внаслідок чого в GSM швидкість передачі даних одним користувачем виявляється набагато вища, ніж в D-AMPS.

Далі ми розглянемо лише основні властивості GSM. А друкарський варіант стандарту GSM займає понад 5000 (sic!) сторінок. Основна частина тексту відноситься до опису інженерних аспектів системи, зокрема, пристрої приймачів, оброблювальних багатопроменеве розповсюдження сигналів, синхронізації приймачів і передавачів.

Отже, кожна смуга частот має ширину 200 кГц. Система GSM має 124 пари сімлексних каналів, як показано на рис. 2.37. Ширина пропускання кожного сімлексного каналу складає 200 кГц. Канал підтримує 8 окремих з'єднань за допомогою часового ущільнення. Кожній активній в даний момент базовій станції призначений один кадровий інтервал на пару каналів. Теоретично, кожний стільник може мати до 992 каналів, проте багато хто з них свідомо робить неприступними, щоб уникнути конфліктів з сусідніми стільниками. На рис. 2.36 вісім заштрихованих кадрових інтервалів належать одному і тому ж з'єднанню, по чотири в кожному напрямі. Прийом і передача відбуваються в різних інтервалах, оскільки апаратура GSM не може працювати одночасно в двох режимах, і на перебудову потрібен якийсь час. Якщо мобільній станції привласнений діапазон 980,4/935,4 МГц і кадрового інтервалу 2 хочуть здійснити передачу на базову станцію, він скористається нижнім набором заштрихованих інтервалів (а також подальшими),

розміщуючи в кожному з них порцію даних. Так продовжуватиметься до тих пір, поки не будуть послані всі дані.

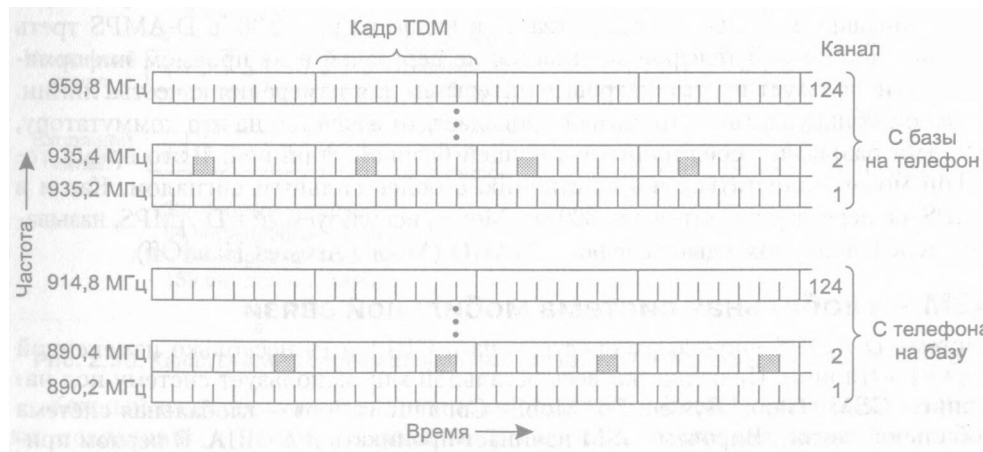


Рис. 2.37. GSM має 124 частотні канали, в кожному з них 8-інтервальна система з розділенням часу

Інтервали TDM, зображені на рис. 2.37, є частиною складної ієрархічної системи кадрів. Кожний інтервал має специфічну структуру, як і їх групи. Спрощена ієрархія зображена на рис. 2.38. Ми бачимо тут, що інтервал TDM складається з 148-бітового кадру даних, який займає канал на 577 мкс (включаючи захисний інтервал завдовжки 30 мкс). Кадри даних починаються і закінчуються трьома нулями, це робиться для їх розмежування. В них також входять 57-бітові інформаційні (Information) поля, в кожному з яких присутній контрольний біт перевірки вмісту (голос/дані). Між інформаційними полями є 26-бітове поле синхронізації (Sync), яке використовується приймачем для синхронізації з межею кадру передавача.

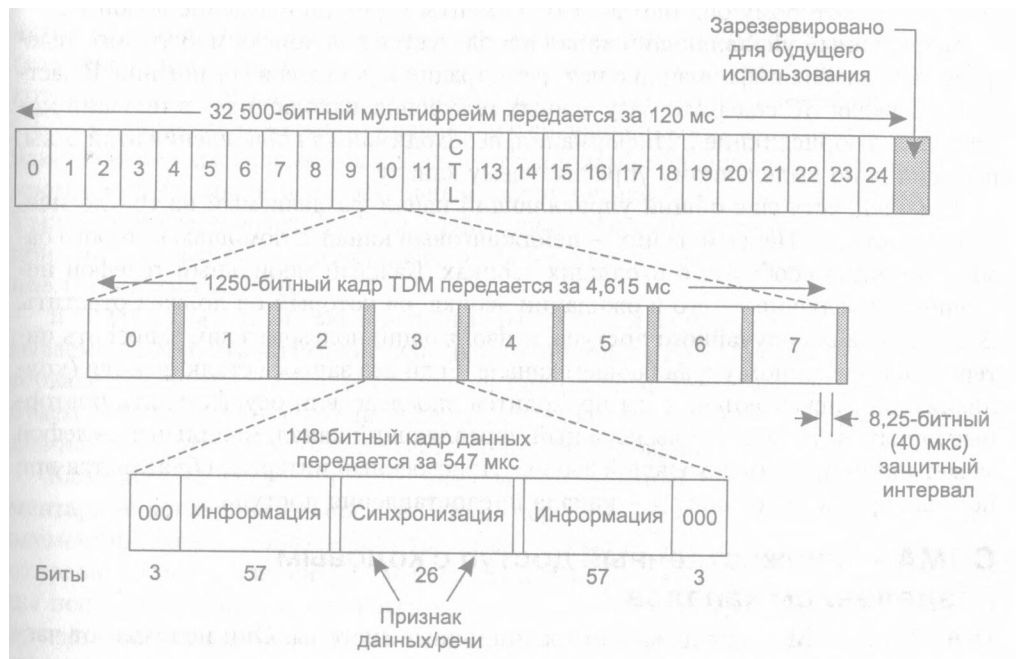


Рис. 2.38. Частина ієрархічної структури кадрів GSM

Кадр даних передається за 547 мкс, але передавачу дозволяється посилати дані тільки через кожні 4,615 мс, оскільки він ділить канал з сьомма іншими станціями. Загальна швидкість кожного каналу складає 270 883 біт/с. Вона ділиться між 8 користувачами. Разом виходить 33,854 Кбіт/с, що більш ніж в два рази перевищує 16,2 Кбіт/с D-AMPS (324 біти 50 разів в секунду). Проте, як і в AMPS, на невідгідні витрати витрачається велика частина пропускної спроможності, і у результаті на одного користувача доводиться 24,7 Кбіт/с (перед початком виправлення помилок). Після виправлення помилок залишається 13 Кбіт/с, за допомогою яких потрібно передати голос. Це вже майже в два рази краще, ніж D-AMPS (за рахунок використання відповідно збільшеної пропускної спроможності).

Як видно на рис. 2.38, 8 кадрів даних утворюють один кадр TDM, а 26 кадрів TDM утворюють мультикадр 120-мілісекунди. В мультикадрі дванадцятий інтервал використовується для службової цілі, а двадцять п'ятий зарезервований для майбутнього використання, тому для призначеного для користувача трафіку залишається тільки 24 інтервали.

Проте, на додаток до 26-інтервального мультифрейму, показаного на рис. 2.38, використовується ще і 51-інтервальный мультифрейм (не показаний на малюнку). Деякі інтервали потрібні для управляючих каналів. Широкомовний управляючий канал є безперервним потоком, що виходить з базової станції, в якому містяться її ідентифікаційна інформація і статус каналу. Всі мобільні пристрої проводять моніторинг потужності сигналу, по якому вони визначають моменти переходу у ввід нової.

Виділений управляючий канал використовується для пошуку мобільного телефону, оновлення інформації про нього, реєстрації і установок з'єднання. Зокрема, кожна БС містить базу даних телефонів, що знаходяться у нинішній момент під її юрисдикцією. Інформація, необхідна для оновлення цієї бази, передається по виділеному управляючому каналу.

Нарешті, є ще загальний управляючий канал, що розділяється на три логічні підканали. Перший з них – пейджинговий канал, за допомогою якого базова станція повідомляє про вхідні дзвінки. Кожний мобільний телефон постійно прослуховує його в очікуванні дзвінка, на який він повинен відповісти. Другий – канал випадкового доступу, що дозволяє користувачам запитати інтервал у виділеному управляючому каналі. Якщо два запити стикаються (колізія), вони спотворюються, і їм доводиться згодом здійснювати повторні спроби. Використовуючи виділений управляючий канал, мобільний телефон може ініціювати вихідний дзвінок. Привласнений інтервал оголошується за допомогою третього підканалу – каналу надання доступу.

CDMA – множинний доступ з кодовим розділенням каналів

D-AMPS і GSM – це досить традиційні системи. Вони використовують частотне і часове ущільнення для розділення спектру на канали і розділення каналів на інтервали. Проте є ще одна система з цієї серії під назвою CDMA (Code Division Multiple Access – множинний доступ з кодовим розділенням

каналів), яка працює абсолютно по-іншому. Коли CDMA була вперше запропонована, реакція представників відповідної промисловості нагадувала реакцію королеви Ізабелли, коли до неї прийшов Колумб і сказав, що він досяг Індії, попливши в напрямі, протилежному потрібному. Так чи інакше, завдяки завзятості єдиної компанії, Qualcomm, CDMA тепер признається не тільки повноцінною системою мобільного зв'язку, але і кращай з існуючих систем третього покоління. Вона також використовується в США при роботі з устаткуванням другого покоління, конкуруючи з D-AMPS. Наприклад, персональна служба зв'язку Sprint використовує CDMA, а AT&T Wireless – D-AMPS. CDMA описується міжнародним стандартом IS-95, і іноді на цю систему посилаються саме таким чином. Також використовується назва торгової марки – cdmaOne.

Так, CDMA повністю відрізняється від AMPS, D-AMPS і GSM. Замість розділення доступного частотного діапазону на сотні вузьких каналів в CDMA кожна станція може при передачі весь час користуватися повним спектром частот. Одночасний множинний доступ забезпечується за рахунок застосування теорії кодування. CDMA також відмінняє думку про те, що кадри, що одночасно прийшли, повинні псуватися. Натомість передбачається, що сигнали додаються лінійно.

Перш ніж розбирати алгоритм роботи, розглянемо наступну аналогію. Уявіть собі зал очікування в аеропорту. Безліч пар жваво розмовляють. Часове ущільнення можна порівняти з ситуацією, коли всі люди знаходяться в центрі залу і говорять по черзі. Частотне ущільнення ми порівняємо з ситуацією, при якій люди знаходяться в різних кутках і ведуть свої розмови, які не чутні іншим. Це відбувається одночасно, але незалежно. Для CDMA краще всього підходить порівняння з ситуацією, коли все в центрі залу, проте кожна пара використовує свою мову спілкування. Франкомовні перемивають кісточки всім іншим, сприймаючи чужі розмови як шум. Таким чином,

ключовою ідеєю CDMA є виділення корисного сигналу при ігноруванні всього іншого. Далі йде злегка спрощений опис технології CDMA.

В CDMA кожний бітовий інтервал розбивається на t коротких періодів, званих елементарними сигналами, або чіпами (chip). Звичайно в бітовому інтервалі поміщаються 64 або 128 елементарних сигналів. В нашому прикладі ми допускати, що бітовий інтервал містить тільки 8 елементарних сигналів на біт, і це треба сприймати лише як спрощення.

Кожній станції відповідає унікальний m -бітний код, що називається елементарною послідовністю. Щоб передати 1 біт, станція посилає свою елементарну послідовність. Щоб передати битий із значенням 0, потрібно відправити замість елементарної послідовності її доповнення (всі одиниці послідовності міняються на нулі, а всі нулі – на одиниці). Ніяких інших комбінацій передавати не дозволяється. Таким чином, якщо $t = 8$ і станції привласнена 8-бітова елементарна послідовність 00011011, то біт із значенням «1» передається кодом 00011011 (що відповідає елементарній послідовності), а біт із значенням «0» передається кодом 11100100 (доповнення елементарної послідовності).

Виправдати збільшене в t раз кількість інформації, яка необхідна передавати (щоб швидкість склала b біт/с, потрібно відправляти tb елементарних сигналів в секунду), можна тільки за рахунок збільшення в t раз пропускної спроможності. Таким чином, CDMA є однією з форм зв'язку з розширеним спектром (передбачається, що ніяких змін в методах модуляції і кодування не проводилося). Якщо є смуга шириною 1 МГц, на якій працюють 100 станцій, то при частотному ущільненні кожна з них отримала б свої 10 кГц і працювала б із швидкістю 10 Кбіт/с (припустимо, використовується 1 біт/Гц). При CDMA всі станції використовують всю ширину діапазону (1 МГц), так що швидкість передачі елементарних сигналів складає 1 Мчіп/с. При кодуванні одного біта елементарними послідовностями, число яких

менше 100, ефективна пропускна спроможність CDMA вище, ніж FDM, причому проблема розміщення каналів вирішена.

З педагогічних міркувань зручніше використовувати біполярний запис і двійковий 0 позначати -1, а двійкову 1 позначати +1. В дужках показуватимемо елементарні послідовності. Так, одиничний біт для станції А виглядатиме як (-1 -1 -1 +1 +1 -1 +1 +1). На рис. 2.39, а ми покажемо елементарні послідовності чотирьох станцій. На рис. 2.39, б зображені вони ж, але в біполярній нотації.

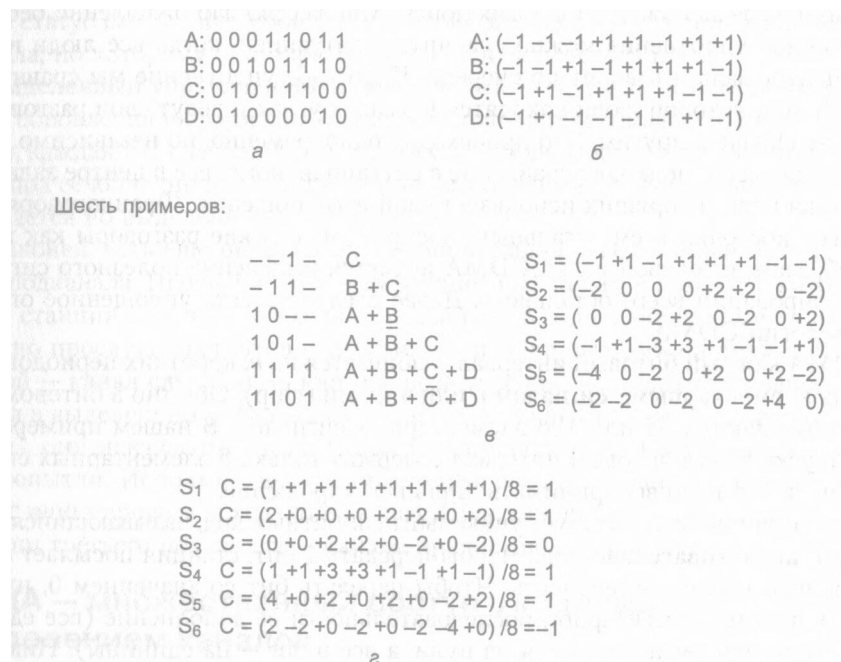


Рис. 2.39. Двійкові елементарні послідовності для чотирьох станцій (а); біполярні елементарні двійкові послідовності (б); шість прикладів передачі (в); відновлення сигналу станції З (г)

Кожна станція має власну унікальну елементарну послідовність. Позначимо символом S вектор довжини t для станції S , а символом S – доповнення 5. Всі елементарні послідовності попарно ортогональні. Ми маємо на увазі, що нормований скалярний твір двох різних елементарних послідовностей S і T (пишеться $S \gg T$) рівно 0. Відомо, як генерувати такі

послідовності за допомогою методу, відомого як коди Уолша. Використовуючи математичний запис, можна виразити сказане раніше таким чином:

Просто кажучи, скільки однакових пар, стільки і різних. Цю властивість ортогональності ми строго доведемо трохи пізніше. Зверніть увагу: якщо $S^*T = 0$, то-и S^*T також рівно 0. Нормований скалярний твір будь-якої елементарної послідовності на саму себе рівно 1.

Це дійсно так, оскільки кожний з t доданків суми рівно 1, тому вся сума рівна t . Зверніть також увагу на те, що $S \cdot S = -1$.

Протягом кожного бітового інтервалу станція може або передавати 1, посилаючи свою елементарну послідовність, або передавати 0, посилаючи доповнення до послідовності, або може мовчати і нічого не передавати. Припустимо, що всі станції синхронізувалися в часі, тобто всі послідовності почали передаватися в один і той же момент.

Коли дві або більш станції намагаються здійснити одночасну передачу, їх біполярні сигнали лінійно складаються. Наприклад, якщо при передачі одного елементарного сигналу три станції послали +1, а одна послала -1, то в результаті вийде +2. Можна розглядати це як складання напруг: три станції мають на виході +1 В, а одна має на виході -1 В. В результаті складання одержуємо +2 В.

На рис. 2.39, в зображено шість прикладів передачі, в якій одночасно беруть участь одна або декілька станцій. В першому прикладі С передає одиничний біт, тому ми просто одержуємо елементарну послідовність цієї станції. В другому прикладі і В, і С передають одиничні біти, внаслідок чого ми одержуємо суму їх біполярних послідовностей, а саме:

$$(-1 -1 + 1 -1 + 1 + 1 + 1 -1) + (-1 + 1 -1 + 1 + 1 + 1 -1 -1) = (-2 0 0 0 +2 +2 0 -2).$$

В третьому прикладі станція А посилає 1, а станція В посилає 0. Інші мовчать. В четвертому прикладі А і С посилають 1, тоді як В посилає 0. В

п'ятому прикладі всі чотири станції посилають 1. Нарешті, в останньому випадку A, B і D посилають одиничний біт, а C посилає нульовий. Зверніть увагу на те, що кожної з шести послідовностей (від S_1 до S_6), представлених на рис. 2.39, в, відповідає один бітовий інтервал.

Щоб відновити початковий бітовий потік кожної із станцій, приймач повинен наперед знати елементарні послідовності всіх передавачів, з якими він працює. Відновлення здійснюється шляхом обчислення нормованого скалярного твору прийнятої послідовності (тобто лінійної суми сигналів всіх станцій) і елементарної послідовності тієї станції, чий початковий сигнал відновлюється. Якщо прийнята елементарна послідовність S і приймач намагається зрозуміти, що передала станція з елементарною послідовністю Z , то проводиться обчислення нормованого скалярного твору $S * C$.

Щоб зрозуміти, як це все працює, давайте уявимо собі ці дві станції, A і C. Нехай обидва передають одиничний біт, тоді як станція B передає нульовий біт. Приймач одержує суму сигналів, яка рівна $S = A + B + C$ і обчислює добуток:

$$S * C = (A + B + C) * C = A * C + B * C + C * C = 0 + 0 + 1 = 1$$

Перші два доданки рівні нулю, тому що всі пари елементарних послідовностей ретельно підбиралися такими, щоб вони були ортогональними, див. вираз (2.4). Тепер повинне бути зрозумілий, чому ця умова повинна бути накладений на елементарні послідовності.

Можна уявити собі цю задачу і по-іншому. Припустимо, приймач отримав замість суми сигналів окремі сигнали. В цьому випадку приймач обчислюватиме скалярні твори кожного з них по окремо, а результати складати. Завдяки властивості ортогональності, всі скалярні твори, окрім $C * C$, рівні 0. Складання з подальшим обчисленням скалярного твору рівносильно підсумовуванню скалярних творів.

Звернемося знову до шести прикладів, показаних на рис. 2.39, в. Конкретний результат декодування цих послідовностей представлений на

рис. 2.39, р. Допустимий, приймач зацікавлений у витяганні потоку бітів, посланого станцією С, зі всіх шести послідовностей S_1 - S_6 . Для цього він обчислює кожний біт шляхом підсумовування парних творів прийнятої послідовності (5) і вектора С (див. рис. 2.39, б), потім розподіли результату на 8 (оскільки $t = 8$ в даному випадку). Як бачите, кожного разу знаходиться вірний біт. Це так само просто, як говорити по-французьки!

В ідеальній системі CDMA без шуму місткість (тобто допустима кількість станцій) може бути скільки завгодно великою, як і місткість ідеального безшумного каналу Найквіста може збільшуватися за рахунок підвищення кількості біт на відлік. На практиці, звичайно ж, фізичні обмеження дуже сильно зменшують місткість системи. По-перше, ми припускали, що всі послідовності синхронізовані за часом. На самій же справі точну синхронізацію забезпечити неможливо. Єдине що можна зробити, – це організувати форсування приймачем відправки з боку передавача достатньо довгої елементарної послідовності, по якій приймач міг би здійснити синхронізацію. Вся решта (несинхронізовані) посилки при цьому розглядається як випадковий шум. Якщо їх не дуже багато, базовий алгоритм декодування працює непогано. З накладенням елементарних послідовностей на шумовий фон зв'язана досить обширна теорія. Як неважко здогадатися, чим довше елементарна послідовність, тим вище вірогідність її коректного детектування на фоні шуму. Для підвищення надійності бітова послідовність може використовувати код з корекцією помилок. Елементарні послідовності ніколи не використовують корекцію помилок.

Ще одним очевидним допущенням, яким ми користувалися в наших міркуваннях, є припущення про те, що потужності всіх станцій такі ж, як сприймані приймачем. Система CDMA звичайно використовується в безпроводному зв'язку, де завжди присутня базова стаціонарна станція і безліч мобільних станцій, розташованих на різних відстанях від неї. Рівні потужності, сприймані приймачем, звичайно, залежать від того, наскільки

далеко знаходяться передавачі. Добрим евристичним правилом є правило компенсації потужностей: чим слабший сигнал, що приймається мобільним телефоном від базової станції, тим потужнішим повинен бути його вихідний сигнал. Іншими словами, мобільна станція, що одержує слабкий сигнал від базової станції, посилатиме потужніший сигнал, ніж станція, що одержує потужний сигнал з БС. Потужності можуть також контролюватися базовими станціями, що видають команди мобільним станціям збільшити або зменшити свою потужність.

Ще ми припускали, що приймач знає, хто відправляє йому дані. У принципі, маючи достатньо потужну обчислювальну можливість, базова станція може слухати одночасно всіх відправників і виконувати алгоритм декодування паралельно для всіх передавачів. Але про це простіше говорити, ніж реалізовувати. В CDMA є ще багато складних речей, які ми опустили в нашій короткій розповіді. Проте, це добре продумана схема, яка все ширше застосовується в безпроводному зв'язку. Стандартною смугою CDMA є 1,25 МГц (проти 30 кГц в D-AMPS і 200 кГц в GSM), і в цій смузі система може обслуговувати набагато більше користувачів, ніж будь-яка інша система. При цьому кожному користувачу надається пропускна спроможність, яка, принаймні, не гірше, ніж в GSM, а часто навіть краще.

Мобільні телефони третього покоління: цифрова мова і дані

Яким буде майбутнє мобільній телефонії? Давайте спробуємо розібратися. Розвитком цієї галузі рухає велику кількість чинників. По-перше, об'єм передаваних даних вже перевищує об'єм передаваної мови в стаціонарних мережах, і перший показник росте експоненціально, тоді як останній росте досить повільно. Багато експертів передрікають таке ж майбутнє і мобільним мережам: трафік даних перевищить голосовий трафік. По-друге, комп'ютерна індустрія і індустрія телефонії і розваг вже стали повністю цифровою і швидко об'єднуються. Багато хто захоплюється

компактністю і малою вагою портативного пристрою, який виступає як телефон, програвач компакт-дисків, DVD-програвач, терміналу для електронної пошти, володіє веб-інтерфейсом, можливостями текстового редактора, включає електронні ігри і багато що інше. З його допомогою можна без жодних дротів в будь-якій точці миру отримати високошвидкісний доступ в Інтернет. Все це називається третім поколінням мобільної телефонії.

Ще в 1992 році міжнародний союз телекомунікацій, ІТУ, зробив спробу конкретизувати і реалізувати ці мрії і випустив проект під назвою ІМТ-2000, де ІМТ означало «міжнародний мобільний зв'язок» (International Mobile Telecommunications). Що стосується числа 2000, то воно було потрібне для трьох речей: по-перше, воно указувало на рік, в якому замислювалося ввести в дію цей проект; по-друге, саме на такій частоті (в мегагерцах) повинна була працювати система; по-третє, передбачалося встановити таку ширину смуги (в кілогерцах).

Жоден з трьох пунктів здійснений не був. В 2000 році система реалізована не була. ІТУ рекомендував урядам всіх країн зарезервувати частоту 2000 МГц (2 ГГц) для міжнародного роумінгу. Рекомендацію виконав тільки Китай. Нарешті, в якийсь момент усвідомили, що неможливо виділити кожному користувачу пропускну спроможність в 2 Мбіт/с, особливо враховуючи особливу мобільність багато кого з них (просто нереально з достатньо високою швидкістю здійснювати передачу з однієї базової станції на іншу). Більш реалістично виглядає виділення 2 Мбіт/с стаціонарним абонентам, які сидять удома (в цьому випадку така система буде серйозним конкурентом ADSL), 384 Кбіт/с для людей, які не поспішаючи прогулюються по парку, і 144 Кбіт/с – для зв'язку з абонентами, що рухаються в автомобілях. Проте, навкруги 3G, як називають третє покоління мобільного зв'язку, кипить бурхлива діяльність. Третє покоління ще не виправдало повною мірою ті надії, які з ним пов'язували, проте незабаром поза сумнівом виправдає.

Ось основні сервіси, для надання яких замислювалася мережа ІМТ-2000:

- Високоякісна передача мови.
- Обмін повідомленнями (заміна e-mail, факсу, SMS, чату і т. д.).
- Мультимедіа (програвання музики, відео, фільмів, телебачення і т. д.).

Доступ в Інтернет (включаючи проглядання сторінок з аудіо- і відеоінформацією). Як додаткові послуги можуть бути відеоконференції, телепрезентації, групові електронні ігри, мобільна комерція (використовування мобільного телефону для оплати покупок). Більш того, всі ці сервіси повинні бути доступний по всьому світу (з автоматичним з'єднанням через супутник в тих місцях, де стаціонарна мережа відсутня) на основі постійного підключення і з гарантованою якістю обслуговування.

ITU замислював ІМТ-2000 як єдину технологію, щоб виробники могли випустити універсальний пристрій, який можна було б продавати по всьому світу (як комп'ютери і програвачі компакт-дисків і не в приклад мобільним телефонам і телевізорам). Одна стандартна технологія сильно спрощує життя операторам зв'язку і привертає клієнтів. Війна форматів (так вийшло з Betamax і VHS в світі відеозапису), яка спочатку сприймалася як вид конкуренції, виявилася несприятливою для бізнесу.

Було висунуто декілька технічних пропозицій, згодом деякі відсіялися і залишилися дві основні технології. Перша з них називається широкосмуговим CDMA (W-CDMA, Wideband CDMA) і була запропонована фірмою Ericsson. Система використовує розширення спектру із застосуванням коду прямої послідовності, такий метод ми вже описували раніше. Смуга пропускання складає 5 МГц і призначена для міжмережевого обміну з мережами стандарту GSM, хоча система не має зворотної сумісності з GSM. Зате вона володіє властивістю, яка дозволяє користувачу при виході із стільника W-CDMA і вході в осередок GSM не переривати дзвінок. Ця система була просунута Європейським Союзом, який назвав її UMTS

(Universal Mobile Telecommunications System – універсальна система мобільного зв'язку).

Другим претендентом стала система CDMA2000, запропонована Qualcomm. В ній також використовується принцип розширення спектру із застосуванням коду прямої послідовності, та і взагалі її можна розглядати як розширення IS-95 (між іншим, є зворотна сумісність з цим стандартом). Смуга пропускання має ширину 5 МГц, проте CDMA2000 не призначена для міжмережевої взаємодії з GSM, і передача з'єднання при переході в осередок GSM (або D-AMPS) не здійснюється. Серед інших технічних відмінностей від W-CDMA варто відзначити іншу швидкість проходження елементарних посилок, інші кадровий інтервал, спектр і спосіб синхронізації, що використовується.

Якби інженерів з Ericsson і Qualcomm посадили за стіл переговорів і поставили б задачу виробити єдину систему, вони, напевно, справилися б з цим. Врешті-решт, базовий принцип обох систем – це CDMA на каналі із смугою 5 МГц. Неначебно ніхто не збирається битися на дуелі через швидкість елементарних посилок. Біда в тому, що справжньою проблемою, як завжди, є зовсім не інженерне рішення, а політика. Європі була потрібна система, що уміє працювати з GSM; Сполученим Штатам була потрібна система, сумісна з однією з вже існуючих там систем (IS-95). Кожна сторона підтримувала свою компанію (Ericsson знаходиться в Швеції, Qualcomm – в Каліфорнії). Врешті-решт, обидві компанії виявилися залучені в множинні тяжби, пов'язані з патентами на технологію CDMA.

В березні 1999 року судові розгляди закінчилися тим, що Ericsson погодилася придбати інфраструктуру Qualcomm. Компанії також погодилися на єдиний стандарт 3G, проте з безліччю несумісних функцій, які, втім, у великій мірі пов'язані з документацією, а не з технічними відмінностями. Не дивлячись на всі розбіжності, незабаром з'являться служби і пристрої 3G.

Про системи 3G написано багато, причому відгуки в основному захоплені. Більшість пише про три покоління мобільного зв'язку в тому дусі, що це найбільше досягнення з часів винаходу хліборізки.

Поки бояри борються в спробах прийти до угоди по системах 3G, деякі оператори зв'язку вже роблять перші боязкі кроки у напрямі 3G, пропонуючи, що називається, 2,5G, хоча більш точно б назвати це 2,1G. Одна така система називається EDGE (Enhanced Data rates for GSM Evolution – підвищені швидкості передачі для розвитку GSM) і є звичайний GSM із збільшеним числом біт на бод. Проблема полягає в тому, що чим більше битов використовується, тим більше вірогідність помилок. Тому в EDGE застосовуються дев'ять різних схем модуляції і корекції помилок. Відрізняються вони один від одного відсотком пропускної спроможності, що виділяється на виправлення помилок, що виникають унаслідок підвищеної швидкості.

Ще однією системою «другого з половиною покоління» є GPRS (General Packet Radio Service – загальні послуги пакетного радіозв'язку) – пакетна мережа на базі D-AMPS або GSM. Вона дозволяє обмінюватися IP-пакетами по голосових каналах стільникового зв'язку. При роботі GPRS деякі часові інтервали на деяких частотах резервуються під пакетний трафік. Число і розташування цих інтервалів можуть динамічно змінюватися базовою станцією залежно від співвідношення голосового і інформаційного трафіку в осередку.

Доступні часові інтервали діляться на дещо логічних каналів, що використовуються для різної мети. Базова станція визначає, в яких інтервалах розташовуються ці канали. Один канал призначений для передачі пакетів з базовою на мобільну станцію, причому кожний пакет має поле індикації місця свого призначення. Щоб послати IP-пакет, мобільна станція запрошує один або декілька часових інтервалів, посылаючи на БС відповідний запит. Якщо запит приходить непошкодженим, назад відсилається інформація про

частоту і інтервал, в якому можна передавати IP-пакет. Як тільки на базову станцію прибуває пакет, вона по звичайному кабельному з'єднанню пересилає його в Інтернет. Оскільки система GPRS працює лише як надбудова над існуючою голосовою системою, її можна розглядати в кращому разі як часову затичку, яка не знадобиться, коли буде введений в дію 3G.

Навіть не дивлячись на те, що 3G дотепер не реалізований в повному об'ємі, багато дослідників розглядають його появу як факт, що вже відбувся, і тому не дуже цікавляться проблемами його вивчення. 4G характеризуватиметься високою пропускною спроможністю, повсюдною застосовністю, повною інтеграцією з кабельними мережами, особливо IP, адаптивним управлінням ресурсами і частотним спектром, програмним радіо і високою якістю обслуговування в області мультимедіа.

З другого боку, повсюдно встановлюється така велика кількість точок доступу до безпроводних ЛОМ стандарту 802.11, що багато хто розглядає 3G не як факт, а як мертвонароджене покоління систем, що відбувся. На думку багато кого, людям не складе труднощів залишатися на зв'язку, просто переміщаючись від однієї такої точки доступу до іншої. Сказати, що дана галузь знаходиться у стадії бурхливих змін – значить не сказати нічого. Подивимося, що буде літ через п'ять. Швидше за все, зміниться дуже багато що.

7.3.8. Кабельне телебачення

Ми вже вивчили більш менш детально стаціонарні і безпроводні телефонні системи. Вони, безумовно, гратимуть важливу роль в мережних технологіях майбутнього. Проте, популярнішою стає альтернативна стаціонарна мережна система, а саме кабельне телебачення. Багато хто вже дістає доступ в Інтернет і телефонні послуги з кабельних мереж, і їх оператори прагнуть розширити споживацький ринок. В наступних розділах

ми обговорюватимемо кабельне телебачення як мережну структуру і як альтернативу телефонній системі, яку ми тільки що вивчили.

Абонентне телебачення

Кабельне телебачення вперше з'явилося в кінці 1940-х років і було способом поліпшити прийом сигналу у віддалених селищах і гірській місцевості. Система спочатку складалася з великої антени, розташованої на вершині горба і приймаючої телевізійний сигнал, підсилювача, що називається розподільним пристроєм, і коаксіального кабелю, по якому сигнал доставлявся безпосередньо до абонентів, як показано на рис. 2.40.

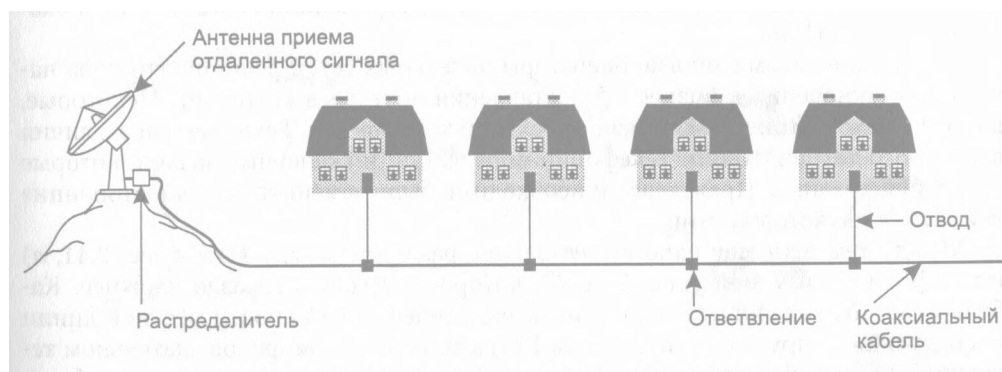


Рис. 2.40. Перша система кабельного телебачення

Спочатку така система називалася абонентним телебаченням, або телебаченням з колективною антеною. Її могло утримувати навіть яке-небудь маленьке приватне сімейне підприємство. Будь-який підприємець, трошки знайомий з електронікою, міг встановити у себе в населеному пункті устаткування, і йому залишалося тільки знайти клієнтів, готових оплачувати послуги. У міру зростання числа абонентів необхідно було додавати кабелі і підсилювачі. Передача була виключно односторонньою: від розподільника до користувачів. До 1970 року з'явилися тисячі незалежних систем.

В 1974 році корпорація Time заснувала новий канал під назвою «Домашня квиткова каса», який був кабельним кіно. Потім з'явилися інші

подібні тематичні канали: спортивний, кулінарний, новин і т.д. Це привело до двох змін в даній галузі. По-перше, крупні корпорації стали скуповувати існуючі кабельні системи і прокладати свої кабелі для залучення нових клієнтів. По-друге, з часом з'явилася необхідність в об'єднанні систем, часто розташованих в різних містах, з метою підстави нових кабельних каналів. Різні кабельні компанії стали об'єднувати свої мережі, організовуючи єдині регіональні і національні мережі. Приблизно те ж саме відбувалося вісімдесяти роками раніше з телефонними мережами. Ізольовані один від одного телефонні станції стали об'єднуватися, що дозволило організувати міжміські дзвінки.

Кабельний Інтернет

Протягом довгих літ кабельна система розширялася, і звичайні кабелі між містами стали замінюватися оптоволоконними з високою пропускнуою спроможністю. Приблизно те ж саме стало відбуватися в телефонній мережі. Система, що використовує оптичне волокно на довгих магістралях і коаксіальний кабель для підведення сигналу до будинків, отримала назву HFC (Hybrid Fiber Coax – комбінована оптокоаксіальна кабельна система). Електрооптичні перетворювачі, що реалізують інтерфейс між оптичною і електричною частинами мережі, називаються оптовузлами. Оскільки пропускна спроможність оптичних кабелів набагато вище, ніж коаксіальних, один оптовузел може обслуговувати декілька низькошвидкісних ліній. Частина сучасної системи HFC показана на рис. 2.41, а.

Останнім часом багато операторів кабельних мереж вирішили, що пора почати проникнення в бізнес надання доступу в Інтернет. Деякі, втім, схотіли зайнятися також кабельною телефонією. Технічні відмінності кабельного телебачення і телефонії визначили інженерні задачі, які належало вирішити. Перш за все необхідно було замінити всі односторонні підсилювачі двосторонніми.

Тим часом є ще одна істотна відмінність між HFC (рис. 2.41, а) і телефонною системою (рис. 2.41, б), яке усунути набагато складніше. Кабель може бути один на декілька будинків, а телефонний провід місцевої лінії в кожну квартиру підводиться свій. Коли йдеться про широкоповне телебачення, особливої різниці немає. Всі телепрограми розповсюджуються по кабелю, і не важливо, 10 або 10 000 абонентів будуть підключені до нього. Але коли один і той же кабель використовується для доступу в Інтернет, то один клієнт, що викачує дуже великий файл, потенційно може тим самим віднімати істотну частину пропускну спроможності у всіх інших. Чим більше користувачів, тим жорсткіша конкуренція між ними в цьому значенні. В телефонній системі такого ні: передача великого файлу по каналу ADSL ніяк не впливає пропускну спроможність сусіднього каналу. З другого боку, пропускну спроможність коаксіального кабелю багато вище, ніж виті пари.

Як же була розв'язана ця проблема? Досить просто: довгі кабелі були розділені на короткі ділянки, напряду що підключаються до оптовузла. Доступна смуга пропускання на ділянці від розподільника до кожного оптовузла дуже велика, і, оскільки в одному сегменті кабелю звичайно не буває великого числа абонентів, трафік цілком керований. Звичайний кабельний сегмент охоплює 500-2000 будинків, проте все більше людей підключається до кабельного Інтернету, тому іноді потрібне більш дрібне розбиття, що приводить до появи додаткових оптовузлов.

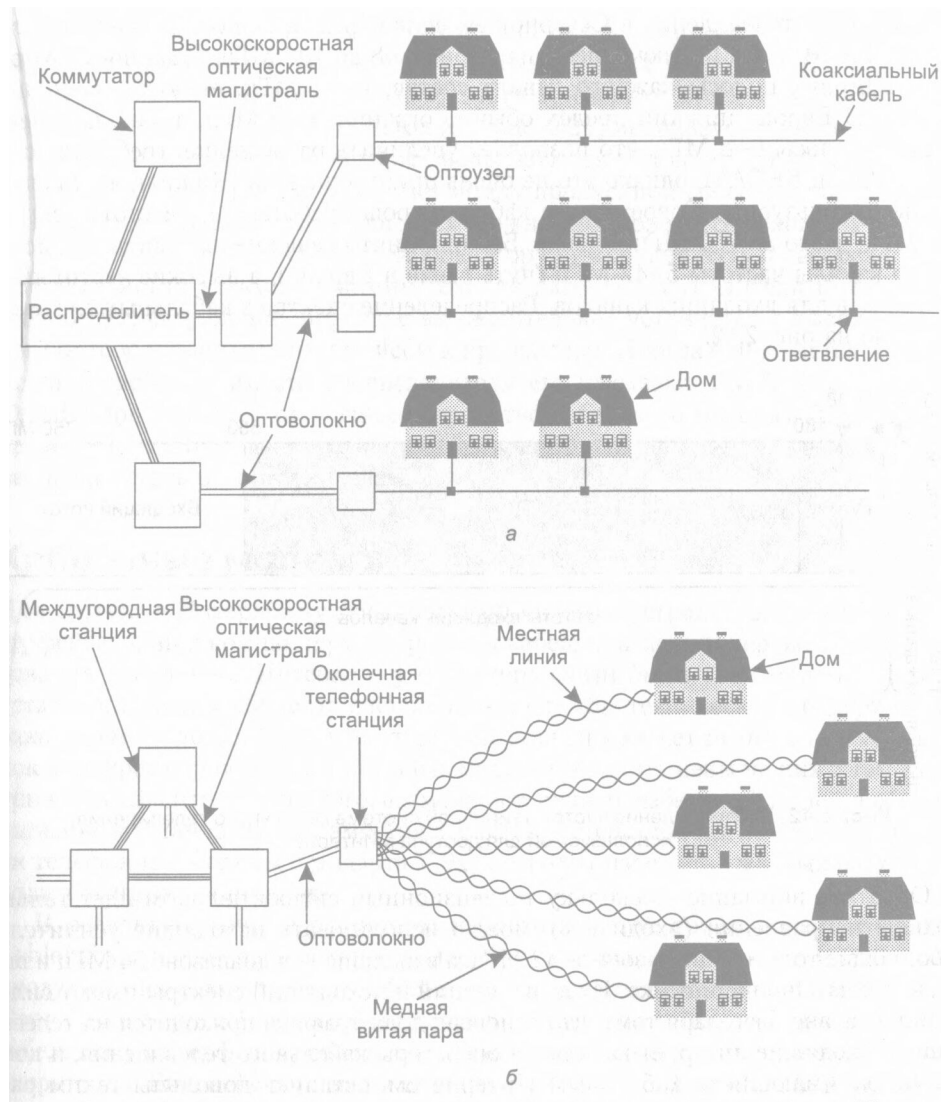


Рис. 2.41 . Кабельне телебачення (а); стаціонарна телефонна система (б)

Розподіл спектру

Якщо викинути всі телевізійні канали і використати кабельну інфраструктуру виключно для доступу в Інтернет, це приведе до появи великого числа незадоволених користувачів, тому ніхто так не робить. Більш того, в більшості міст існують певні обмеження, що не дозволяють так зробити, навіть якщо яка-небудь компанія і схоче. Значить, потрібно було знайти якийсь спосіб сумісного існування телевізійного сигналу і цифрових даних на одному кабелі.

Кабельне телебачення в Північній Америці традиційно займає частоти з 54 до 550 МГц (за винятком діапазону з 88 до 108 МГц, відданих FM-радіо). Ширина смуги кожного каналу складає 6 МГц, включаючи захисні смуги. В Європі нижня межа звичайно обмежена 65 МГц, а канали мають ширину смуги 6-8 МГц, що дозволяє збільшити дозвіл, що вимагається системам PAL і SECAM, проте це не дуже принципово. Нижня частина спектру не використовується. Сучасні кабелі добре працюють на частотах понад 550 МГц, часто до 750 МГц і вище. Було ухвалено рішення виділити під вихідні канали частоти 5-42 МГц (трохи вище в Європі), а високі частоти використовувати для вхідних каналів. Розподіл спектру в кабельних системах показаний на рис. 2.42.

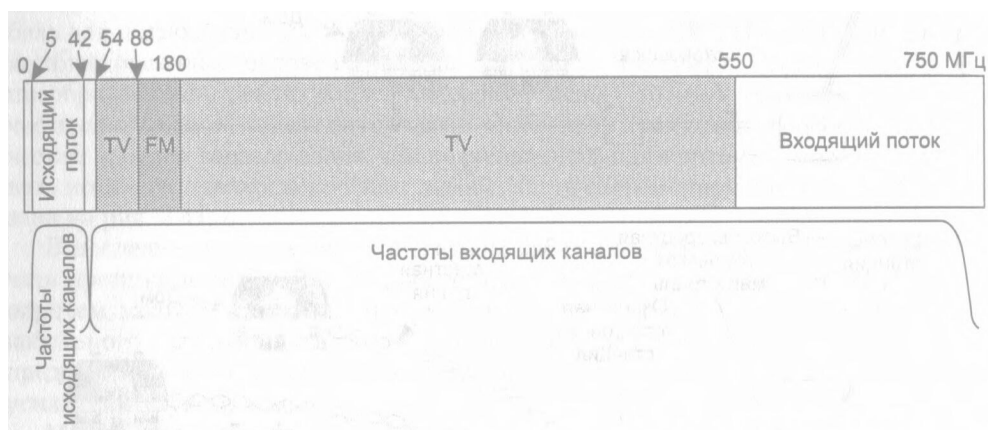


Рис. 2.42. Розподіл частот в типовій системі кабельного телебачення, що використовується для доступу в Інтернет

Зверніть увагу: оскільки телевізійний сигнал цілком йде тільки в одному напрямі (що входить), можна використовувати вихідні підсилювачі, що працюють тільки в діапазоні 5-42 МГц, а що входять – в діапазоні 54 МГц і вище, як показано на малюнку. Отже, вхідний і вихідний спектри мають сильний дисбаланс завдяки тому, що основна частка трафіку доводиться на телебачення і вхідні інтернет-канали. І оператори кабельного телебачення, і компанії, що займаються кабельним Інтернетом, залишилися задоволені

таким розподілом. Як ми вже говорили, телефонні компанії часто пропонують асиметричний DSL-сервіс, хоча у них немає особливих технічних підстав, щоб так робити.

Довгі коаксіальні кабелі не краще за місцеві телефонні лінії, коли йдеться про передачу цифрових даних. Тому тут також потрібна аналогова модуляція. Звичайно застосовується схема, при якій беруться кожних 6 або 8 МГц вхідного каналу і модулюються за допомогою QAM-64 або (якщо кабель відмінної якості) QAM-256. При каналі шириною 6 МГц і методі QAM-64 ми одержуємо швидкість близько 36 Мбіт/с. Якщо відняти невігідні витрати, чиста швидкість передачі даних складе 27 Мбіт/с. При використуванні QAM-256 чиста швидкість підвищується до 39 Мбіт/с. Європейські значення на третину вищі.

Для вихідних потоків навіть QAM-64 не дуже підходить. Дуже багато на відповідних частотах перешкод від мікрохвильових пристроїв, СВ-радіостанцій і інших джерел. Виходячи з цього застосовують більш повільну, але надійну схему – QPSK. Цей метод (див. рис. 2.21) використовує всього лише два біти на бод замість 6 або 8, які використовуються методами QAM на вхідному потоці. Таким чином, асиметрія між пропускною спроможністю вхідних і вихідних каналів навіть вище, ніж можна припустити виходячи з рис. 2.42.

Окрім оновлення підсилювачів, оператору потрібно відновити і розподільний пристрій на вході системи. Замість латентного підсилювача потрібно поставити інтелектуальний цифровий обчислювальний пристрій з високошвидкісним оптоволоконним інтерфейсом до провайдера. Іноді обновляється навіть ім'я цього пристрою: замість розподільника його називають CMTS (Cable Modem Termination System – крайовий пристрій кабельного модему). Далі ми утримаємося від такого значного оновлення і як і раніше називатимемо розподільник розподільником.

Кабельні модеми

Для доступу в Інтернет потрібен кабельний модем – пристрій, що має два інтерфейси: один до комп'ютера, другий – до кабельної мережі. В перші роки існування кабельного Інтернету у оператора зв'язку були свої модеми, які встановлювалися у абонента фахівцем служби технічної підтримки. Проте потім стало зрозуміло, що відкритий стандарт може дозволити створити ринок конкурентоздатних кабельних модемів, понизити ціни на них і тим самим привернути клієнтів. Більш того, можливість купити кабельний модем в звичайному магазині і встановити його самостійно (як користувачі завжди встановлювали телефонні модеми стандарту V.9x) дозволить уникнути жахливих витрат на оплату виїзду фахівця.

В результаті багато операторів кабельних мереж об'єдналися з фірмою CableLabs з метою вироблення стандарту на кабельні модеми і тестування продукції на сумісність. Модеми стандарту DOCSIS (Data Over Cable Service Interface Specification – специфікація передачі даних по кабельному інтерфейсу), що з'явився, зараз тільки починають замінювати власні модеми операторів. Європейська версія стандарту називається EuroDOCSIS. Проте не всім операторам подобається ідея вільного продажу стандартних кабельних модемів – дуже вже добрі гроші вони одержують за здачу в аренду модемів своїм клієнтам. Відкритий стандарт, що породив десятки фірм – виробників кабельних модемів, що продають їх в магазинах, веде до кінця подібної практики.

Інтерфейс між модемом і комп'ютером досить традиційний. Звичайно, Ethernet із швидкістю 10 Мбіт/с (іноді USB). Кабельні модеми скоро будуть нагадувати звичайні внутрішні модеми і розмірами, і способом установки.

Другий інтерфейс складніший. Чимала частина стандарту присвячена радіоінженерним рішенням, але обговорення цього питання виходить за рамки даної лекції. Єдине, що необхідно відзначити, це те, що, як і ADSL-модеми, кабельні модеми знаходяться на постійному підключенні. Вони

встановлюють з'єднання зразу ж після подачі живлення і постійно підтримують його, оскільки оператори кабельних мереж не стягують платню за час на лінії.

Щоб краще зрозуміти, як відбувається робота кабельного модему, розглянемо, що відбувається при його включенні. Модем починає прослуховувати вхідний канал у пошуках спеціального пакету, час від часу посланого розподільником. В ньому повідомляються системні параметри для модемів, котрі тільки що включилися в роботу. Після виявлення даного пакету новий модем оголошує про свою появу по одному з вихідних каналів. Розподільник відповідає, привласнюючи модему вхідний і вихідний канали. Втім, початковий розподіл каналів може бути динамічно змінений розподільником, якщо він вирішить, що необхідно збалансувати навантаження.

Потім модем визначає, на якій відстані від розподільника він знаходиться. Для цього посилається спеціальний пакет і обчислюється час, через який приходить відповідь. Цей процес називається вимірюванням дальності. Модему необхідно знати ці дані, щоб налагодити роботу вихідних каналів і правильно синхронізуватися. Час роботи ділиться на міні-інтервали. Кожний вихідний пакет повинен уміщатися в один або декілька сусідніх міні-інтервалів. Розподільник анонсує кожний початок циклу міні-інтервалів, проте цей «стартовий постріл» модеми чують не одночасно, оскільки вони знаходяться на різних відстанях. Знаючи своє видалення від розподільника, модем може обчислити, коли насправді був посланий прийнятий їм сигнал початку міні-інтервалу. Довжина міні-інтервалу залежить від мережі. Звичайно об'єм корисної інформації в ньому рівний 8 байт.

Під час ініціалізації розподільник також привласнює модему міні-інтервал для запиту пропускнуої спроможності вихідного каналу. Як правило, одному і тому ж міні-інтервалу запиту відповідає декілька модемів, що приводить до конкуренції між ними. Коли комп'ютер хоче відіслати пакет

даних, він передає його модему, який запрошує необхідну кількість міні-інтервалів для нього. Якщо запит прийнятий, то розподільник посилає підтвердження по вхідному каналу. В підтвердженні модем повідомляється, які міні-інтервали зарезервовані для нього. Після цього пакет відправляється, починаючи з першим «своїм міні-інтервалом». Використовуючи спеціальне поле заголовка, можна повідомити про необхідність передати додаткові пакети.

Якщо ж один і той же міні-інтервал хочуть отримати декілька станцій одночасно, то ніякого підтвердження не висилається, а ці станції можуть повторити спробу тільки через випадковий проміжок часу. Якщо при повторній спробі знову виникла колізія, то випадковий проміжок подвоюється.

Вхідні канали управляються не так, як вихідні. По-перше, відправник в цьому випадку тільки один – розподільник, тому не виникає ніякої боротьби за лінію і немає необхідності в міні-інтервалах, які, насправді, є різновидом статистичного часового ущільнення. По-друге, трафік вхідного каналу звичайно набагато вище, ніж вихідного, тому використовуються пакети фіксованого розміру – 204 байти. Частина пакету – код корекції помилок Ріда–Соломона плюс ще деяка службова інформація. Власне дані займають в пакеті 184 байти. Ці числа були вибрані з міркувань сумісності з цифровим телебаченням, що використовує MPEG-2, так що телевізійний і вхідний інформаційний канали мають один і той же формат. Логічна структура з'єднання показана на рис. 2.43.

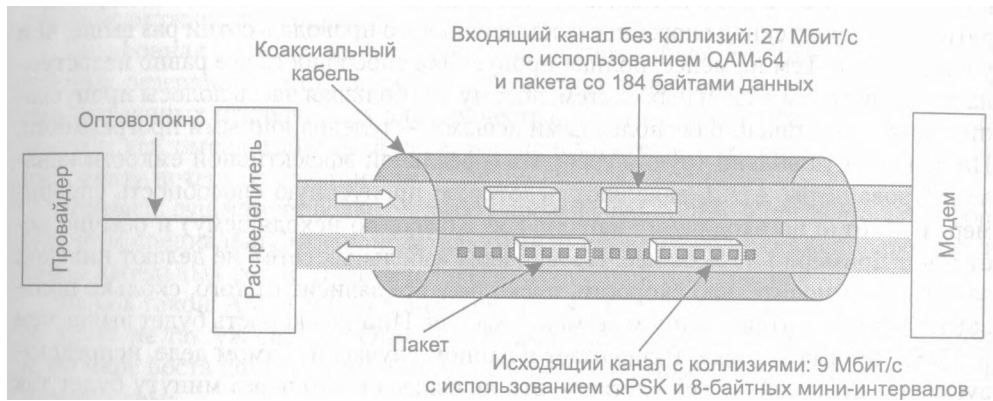


Рис. 2.43. Типова схема вхідного і вихідного каналів, прийнята в США

Повернемося до ініціалізації модему. Коли він закінчив вимірювання дальності і отримав вихідний сигнал, вхідний канал і міні-інтервали, він може почати передавати пакети. Перший пакет, який він посилає, адресований провайдеру і містить запит на отримання IP-адреси, яка привласнюється динамічно з використанням протоколу DHCP. Також у розподільника запрошується точний час доби.

Наступний крок пов'язаний із захистом даних. Оскільки кабель – це ресурс, кожний охочий може прочитувати трафік, що проходить мимо нього, що спільно використовується. Щоб запобігти небажаному доступу до інформації сусіда (буквально), всі дані передаються в зашифрованій формі в обох напрямках. Частина процедури ініціалізації включає обмін ключами шифру. На перший погляд здається неможливою задачею непомітної передачі ключа при світлі дня і величезному скупченні народу.

Нарешті, модему потрібно ідентифікувати себе по захищеному каналу. Після цього ініціалізація вважається завершеною. Користувач може з'єднатися провайдером і починати роботу.

7.4. Погіршення передачі

Засоби передачі недосконалі. Недосконалість викликає пошкодження в сигналі, посланому по лінії. Це означає, що сигнал на початку і кінці лінії, не

є тим же. Те що послано не є тим, що отримано. Три види пошкоджень звичайно мають місце; затування, спотворення, і шум (рис. 7.38).

Figure 7.38 Impairment types

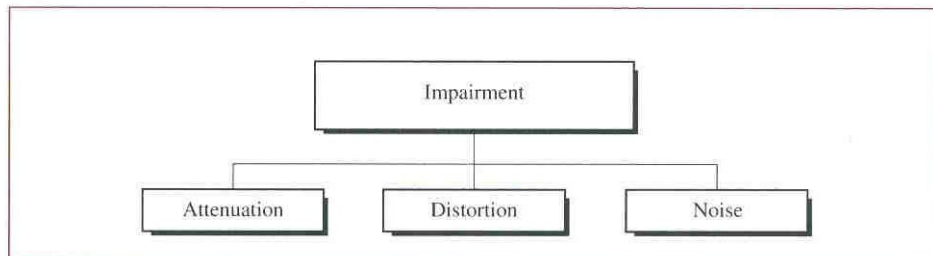


Рис. 7.38. Типи пошкодження

Затування

Затування є втратою засобів енергії. Коли сигнал, простий або складний, передається через лінію, він втрачає частину енергії таким чином, що не може подолати опір лінії. От чому провід, що переносить електричні сигнали, гріється, але не дуже. Частина електричної енергії сигналу перетворюється в теплову енергію. Щоб компенсувати ці втрати, використовують підсилювачі (рис. 7.39 показує результат виснаження і розширення сигналу).

Figure 7.39 Attenuation

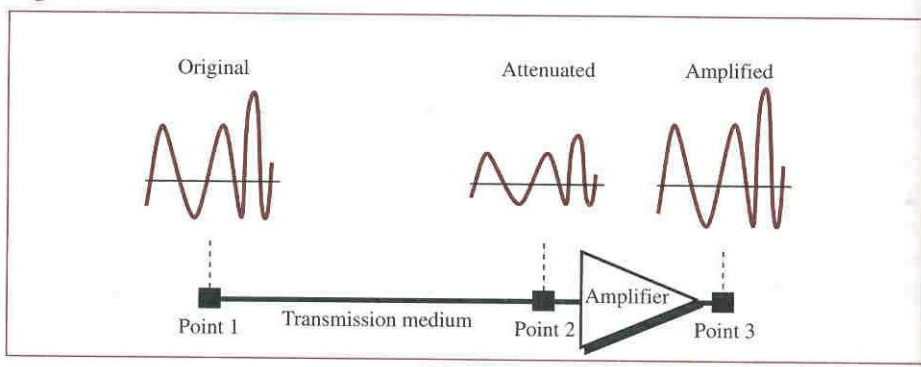


Рис. 7.39. Затування

Децибели

Щоб показати, що сигнал втратив або придбав силу, інженери використовують поняття децибела. Децибел (dB) виміряє відносні сили двох сигналів або сигналу в двох різних точках. Слід відзначте, що dB негативний, якщо сигнал ослаблений і позитивний, якщо сигнал збільшений.

Спотворення

Спотворення означає, що сигнал змінює форму або вигляд. Спотворення відбувається в складовому сигналі, складеному з різних частот. Кожний сигнальний компонент має власну швидкість розповсюдження через засіб і, таким чином, власну затримку прибутті до місця призначення. На рис. 7.41 показано результат спотворення на складовому сигналі.

Figure 7.41 Distortion

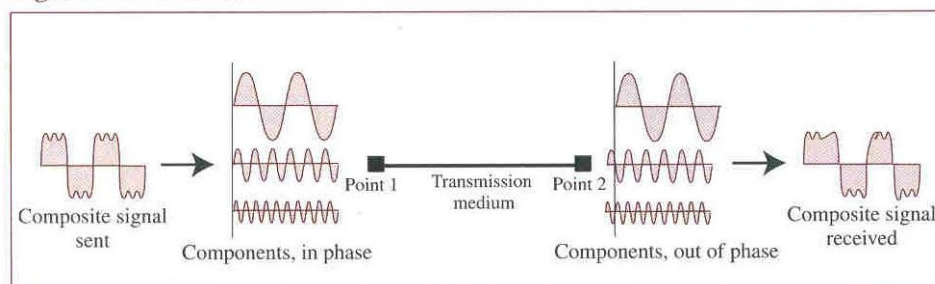


Рис. 7.41. Спотворення

Шум

Шум - це інша проблема. Окремі види шуму, як наприклад тепловий шум, вимушений шум, crosstalk, і шум імпульсу може псувати сигнал. Тепловий шум - це випадковий рух електронів в дроті, який створює додатковий сигнал, відмінний від посланого відправником. Вимушений шум прибуває від джерел, як наприклад двигуни і прилади. Ці пристрої діють, як антена пересилки і як антена отримання. Crosstalk є результатом впливу одного проводу на інший. Один провід діє як передаюча антена, а інший як приймаюча антена. Шум імпульсу - це шпилька (сигнал з високою енергією

за дуже короткий період часу) який приходить від енергетичних ліній, блискавки тощо. На рис. 7.42 показує результат впливу шуму на сигнал.

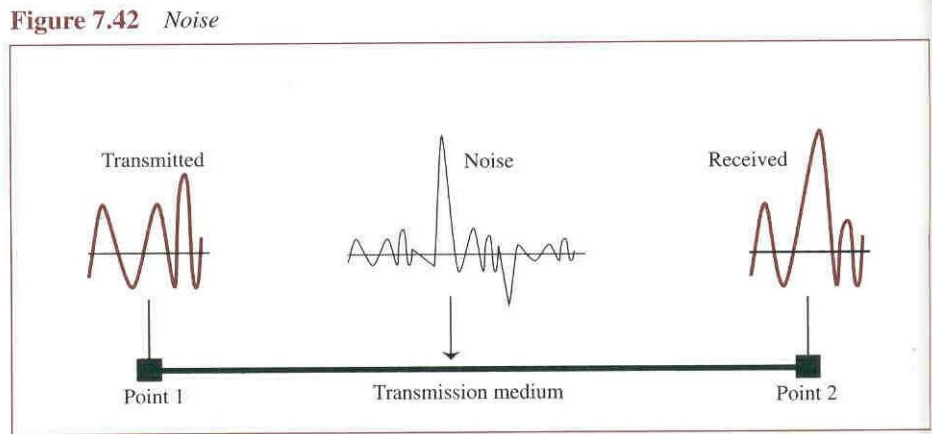


Рис. 7.42. Шум

7.5. Продуктивність і довжина хвилі

Засоби передачі - це дороги якими подорожують дані. Щоб виміряти продуктивність засобів передачі, ми можемо використовувати три поняття: пропускна здатність (throughput), швидкість розповсюдження, і час розповсюдження.

Пропускна здатність (Throughput)

Пропускна здатність є вимірюванням того, як швидко дані можуть пройти через точку. Іншими словами, якщо ми розглядаємо будь-яку точку в засобі передачі як стіну через яку проходить розряд, пропускна здатність є кількістю бітів, які можуть пройти цю стіну один за другим. На рис. 7.43 показано це поняття.

Figure 7.43 Throughput

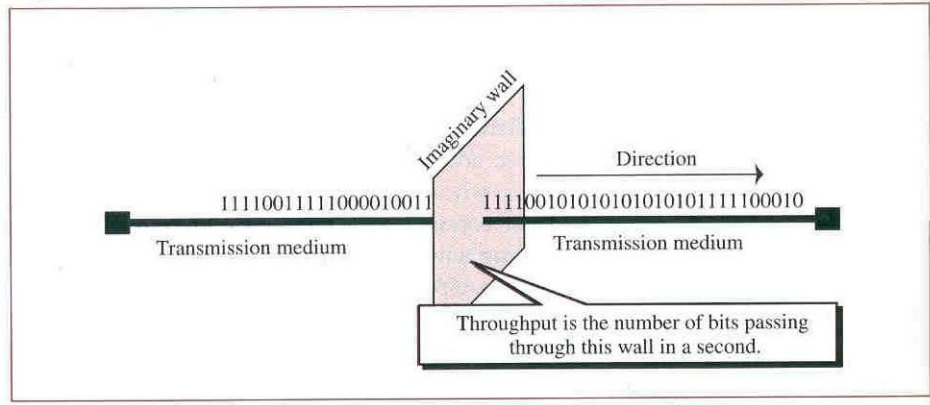


Рис. 7.43. Пропускна здатність

Швидкість розповсюдження

Швидкість розповсюдження вимірює дистанцію яку сигнал або біт може пройти через лінії один за одним. Швидкість розповсюдження електромагнітних сигналів залежить від засобу і частоти сигналу. Наприклад, у вакуумі, легко розповсюджується з швидкістю 3×10^8 м/с. Майже те ж у витій парі. Проте, в коаксіальних і оптоволоконних кабелях швидкість складає 2×10^8 м/с для частот в ряді від МГц до GHz.

Час розповсюдження

Час розповсюдження виміряє час, що вимагається для сигналу (або біта), щоб пройти від однієї точки засобу передачі до іншого. Час розповсюдження обчислюється за допомогою розподілу дистанції на швидкість розповсюдження.

$$\text{Час розповсюдження} = \text{Дистанція} / \text{Швидкість розповсюдження}$$

На рис. 7.44 показано поняття.

Figure 7.44 Propagation time

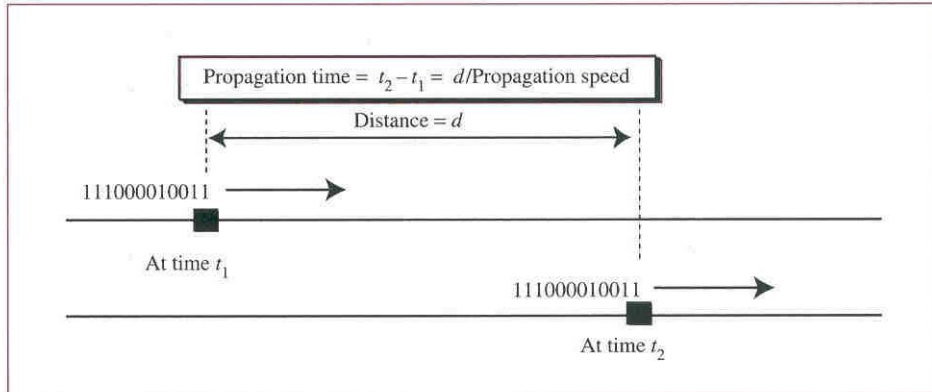


Рис. 7.44. Час розповсюдження

Час розповсюдження звичайно нормалізовані до кілометрів. Наприклад, час розповсюдження для виті пари, нормалізованої до кілометрів, є

Час розповсюдження - $1000 \text{ м} / (3 \times 10^8 \text{ м/с}) = 3.33 \times 10^{-6} \text{ с/м} = 3.33 \text{ нс/км}$

Для коаксіального або волоконного очного кабелю, це є звичайно

Час розповсюдження = $1000 \text{ м} / (2 \times 10^8 \text{ м/с}) = 5 \times 10^{-6} \text{ с/м} = 5 \text{ нс/км}$

Довжина хвилі

Довжина хвилі - це інша особливість сигналу, що передається через засіб передачі. Довжина хвилі прив'язує період або частоту простої хвилі синуса до швидкості розповсюдження засобу. Іншими словами, поки частота сигналу незалежна від засобу, довжина хвилі залежить як від частоти, так і засобу. Хоча довжина хвилі може зв'язуватися з електричними сигналами, це звичайно, щоб використовувати довжини хвилі, коли говориться про передачу світла в оптичному волокні. Довжина хвилі - це дистанція що її простий сигнал може пройти за один період часу (рис. 7.45).

Figure 7.45 Wavelength

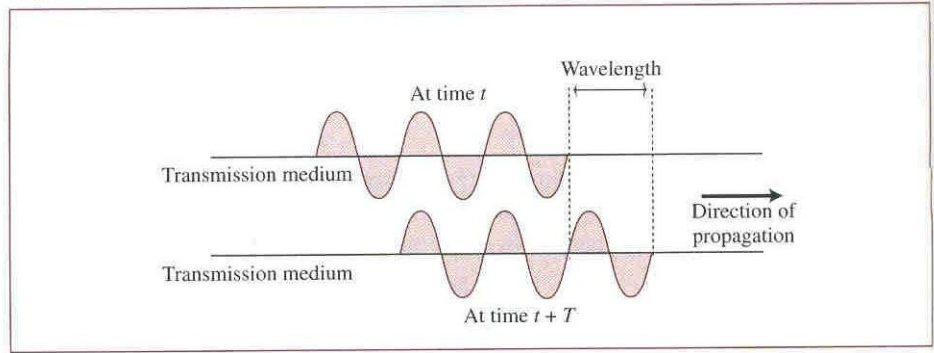


Рис. 7.45. Довжина хвилі

Довжина хвилі може обчислюватися за даною швидкістю розповсюдження і періодом сигналу

Довжина хвилі = Період \times швидкість розповсюдження

Проте часові періоди і частоти пов'язані один з одним, ми можемо також сказати

Довжина хвилі = швидкості розповсюдження \times (1/частоту) = Швидкість розповсюдження/частоту

Довжина хвилі звичайно вимірюється в мікрометрах (мікрони) замість метрів. Наприклад, довжина хвилі червоного світла (частота = 4×10^{14}) в повітрі є

$$\lambda = v/f = (3 \times 10^8) / (4 \times 10^{14}) = 0.75 \times 10^{-6} \text{ m} = 0.75 \text{ мкм}$$

В коаксіальному або оптоволоконному кабелі, проте, довжина хвилі нижча (0.5), тому що швидкість розповсюдження в кабелі є менш ніж в повітрі.

7.6. Порівняння носіїв передачі інформації

При оцінюванні придатності специфічного засобу до специфічного додатку, п'ять коефіцієнтів повинні бути на увазі: вартість, швидкість, затухання, електромагнітне завади і безпека.

- Вартість. Це вартість матеріалів, плюс установка.
- Швидкість. Швидкість - це максимальне число бітів за секунду, які засіб може передати надійно. Серед інших коефіцієнтів, швидкість варіюється з частотою (вища частота може передати більше бітів за секунду), з фізичним розміром засобу та/або устаткування передачі, і з станом провідника.
- Затухання. Як обговорювалось раніше, затухання - це тенденція електромагнітного сигналу, щоб ослаблюватись або спотворюватись над відстані. Протягом передачі, енергія сигналу може поглинутись або розсіятись засобом безпосередньо. Наприклад, опір дроту може зменшити енергію сигналу і віддати її у формі тепла.
- Електромагнітне завади (ЕМІ). Електромагнітні завади (ЕМІ) - це сприйнятливність засобу до зовнішньої електромагнітної енергії, що впливає на зв'язок, який заважає розуміти сигнал. Близькі результати ЕМІ статичні (звукові) і сніг (візуальні)
- Безпека. Це захист проти підслуховування. Наскільки легко для неавторизованого пристрою прослуховувати зв'язок? Деякі засоби, подібно широкомовному радіо і незахищеній витій парі, легко перехоплюються. Інші, подібно оптоволоконному кабелю є більш безпечними.

Таблиця 7.3 порівнює різні засоби, засновані на якостях, перерахованих вище.

Таблиця 7.3. Продуктивність засобів передачі

Table 7.3 *Transmission media performance*

<i>Medium</i>	<i>Cost</i>	<i>Speed</i>	<i>Attenuation</i>	<i>EMI</i>	<i>Security</i>
UTP	Low	1–100 Mbps	High	High	Low
STP	Moderate	1–150 Mbps	High	Moderate	Low
Coax	Moderate	1 Mbps–1 Gbps	Moderate	Moderate	Low
Optical fiber	High	10 Mbps–2 Gbps	Low	Low	High
Radio	Moderate	1–10 Mbps	Low–high	High	Low
Microwave	High	1 Mbps–10 Gbps	Variable	High	Moderate
Satellite	High	1 Mbps–10 Gbps	Variable	High	Moderate
Cellular	High	9.6–19.2 Kbps	Low	Moderate	Low

Тема 8. Мультиплексування

1. Загальні відомості
2. Частотне мультиплексування
3. Поділ по довжині хвилі
4. Часове мультиплексування
5. Застосування мультиплексування: телефонні системи, цифрові абонентські лінії

Література

[Forouzan, Таненбаум, Оліфер]

8.1. Загальні відомості

Кожного разу, коли спроможність передачі пристроїв зв'язку двох засобу більша, ніж потреби передачі пристроїв, зв'язок може бути розподіленим, подібно до того, як велика труба води може доставляти воду до кількох будинків відразу. Мультиплексування є набором устаткування, яке дозволяє одночасну передачу багаторазових сигналів через єдиний канал зв'язку.

Якщо зростає використання телекомунікацій і передачі даних, так зростає і трафік. Ми можемо пристосуватися до цього зростання за допомогою продовження індивідуальні ліній зв'язку щоразу, коли потрібний новий канал, або підвищити місткість передатчиків і використати існуючі, щоб нести багаторазові сигнали.

Сьогоднішні технології включають засоби з високою смугою пропускання (high-смуга пропускання), як наприклад коаксіальний кабель, оптичне волокно, мікрохвилі та супутники. Кожний з них має потужність передачі вищу ніж потрібно для передачі середнього сигналу. Якщо потужність передатчика більша, ніж потрібно пристроям передачі,

марнується резерв виробничих потужностей. Ефективна система збільшує утилізацію всіх засобів. Крім того, дорога технологія, часто стає ефективною по вартості тільки тоді, коли канали передачі розподілені.

На рис. 8.1 показано два можливі шляхи зв'язку чотирьох пар пристроїв. В 8.1а, кожна пара має власну лінію. Якщо повна потужність кожної лінії не використовується, частина тієї потужності втрачається. На 8.1б, передачі між парами мультимплексні; ті ж чотири пари розподіляють потужність єдиної лінії зв'язку.

Багато до одного / один до багатьох

В мультимплексній системі, n пристроїв розподіляють потужність одної лінії зв'язку. На рис. 8.1б показано основний формат мультимплексної системи. Чотири пристрої з лівого боку направляють потоки передачі до мультимплексора мультимплексор (MUX), який об'єднує їх в єдиний потік (багато до одного). В приймачі потік об'єднується в демультимплексорі демультимплексор (DEMUX), який розділяє потік на складові частини передачі (один до багатьох) і направляє їх до пристроїв отримувачів.

На рис. 8.1б слово “шлях” означає фізичну лінію зв'язку. Слово “канал” означає частину шляху, який виконує передачу між даною парою пристроїв. Один шлях може мати багато (n) каналів.

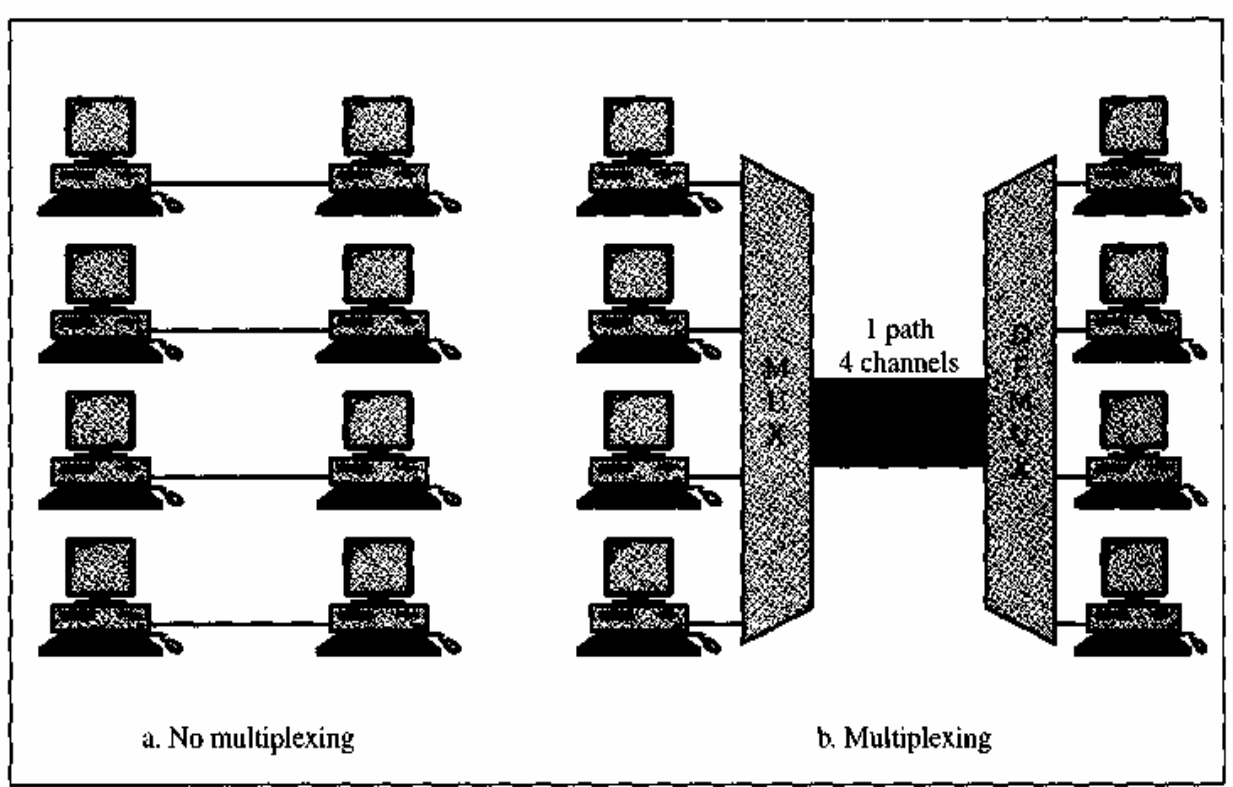


Рис. 8.1. Мультиплексування проти відсутності мультиплексування

Сигнали мультиплексуються з використанням трьох основних методів: частотного мультиплексування (FDM), часове мультиплексування (TDM), і поділ по довжині хвилі (WDM).

TDM в подальшому сприяє поділу на синхронний TDM (звичайно називається TDM) і асинхронний TDM, який також називається статистичний TDM чи концентратором (див. рис. 8.2).

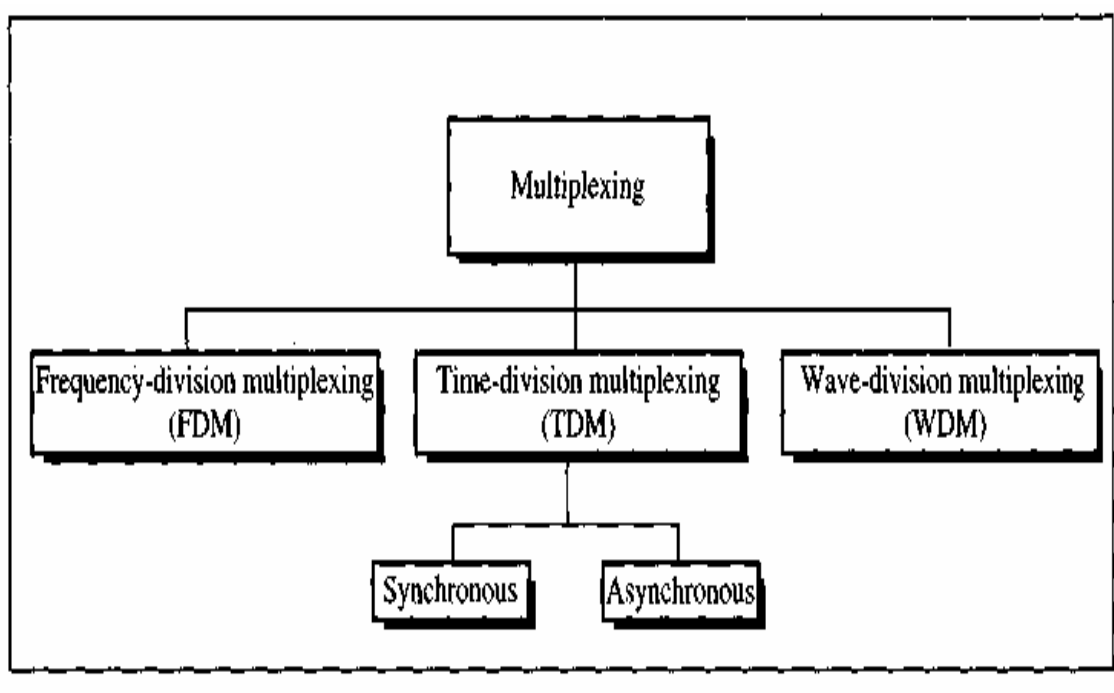


Рис. 8.2 Категорії мультиплексування

8.2. Частотне мультиплексування (Frequency-Division Multiplexing FDM)

Частотне мультиплексування (FDM) - це аналогова техніка, яка може застосовуватися, коли смуга пропускання передатчика більша, ніж комбінована смуга пропускання сигналів, які мають бути передані. В FDM, сигнали, що генеруються кожним пристроєм пересилки, модулюють різними частотами носія. Ці модульовані сигнали потім з'єднуються в єдиний складовий сигнал, який може бути переданий передатчиком. Частоти носія розділяються достатньою смугою пропускання, щоб пристосувати модульований сигнал. Ці діапазони смуг пропускання - це канали, через які передаються різні сигнали. Канали повинні відділятися полосами невикористаних смуг пропускання (guard bands), щоб запобігти перекриттю сигналів. Крім того, частоти носія не повинні заважати оригінальним частотам даних.

На рис 8.3 представлений концептуальний вигляд FDM. Згідно цього рисунка, шлях передачі поділений на три частини, кожне представляє собою канал, здатний нести одну передачу. Як аналогію, можна уявити собі точку,

де три вузькі вулиці зустрічаються, щоб сформувати шосе з трьома рядами. Кожна з трьох вулиць відповідає вузькій дорозі шосе. Всі автомобілі, що переїжджають на шосе від однієї з вулиць, все ще маю власну вузьку дорогу і можуть подорожувати без заважання автомобілям в інших вузьких дорогах.

Figure 8.3 *FDM*

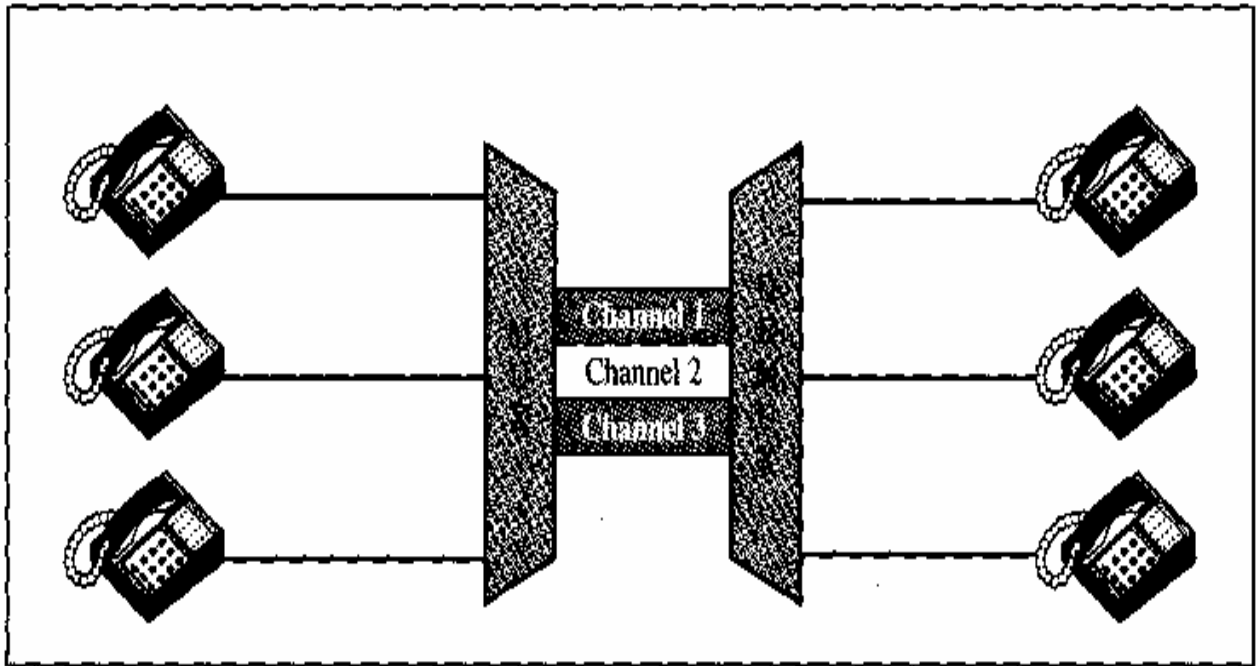


Рис. 8.3. FDM

Потрібно зауважити, що рис. 8.3 показує шлях, який поділяється просторово на окремі канали, фактичний поділ каналу досягається частотою швидше, ніж простором.

Процес FDM

Рис. 8.4 – це концептуальна ілюстрація часової області процесу мультиплексування. FDM є аналоговим процесом і ми показуємо чи використовуються тут телефони, як вхідні і вихідні пристрої. Кожний телефон генерує сигнал подібного частотного діапазону. Усередині

мультиплексора ці подібні сигнали модулюються на різні частоти носія (f_1 , f_2 , and f_3).

Результуючі модульовані сигнали потім з'єднуються в єдиний складовий сигнал, який був посланий передавачем, що має достатню смугу пропускання.

Рис. 8.5 - це ілюстрація частотної області для того ж поняття (Горизонтальна вісь цього малюнка означає частоту, не час. Всі три частоти носія існують в той же час в межах смуги пропускання.) В FDM, сигнали модулюються на різні несучі частоти (f_1 , f_2 , and f_3), використовуючи АМ або ФМ модуляцію. Як зазначено в розділі 5, модулюючи один сигнал в інший, одержуємо в результаті смугу пропускання щонайменш в двічі більшу від оригіналу. Щоб дозволити більш ефективного використання шляху, фактична смуга пропускання може зменшуватись за допомогою подавлення половини смуги.

Figure 8.4 FDM multiplexing process, time domain

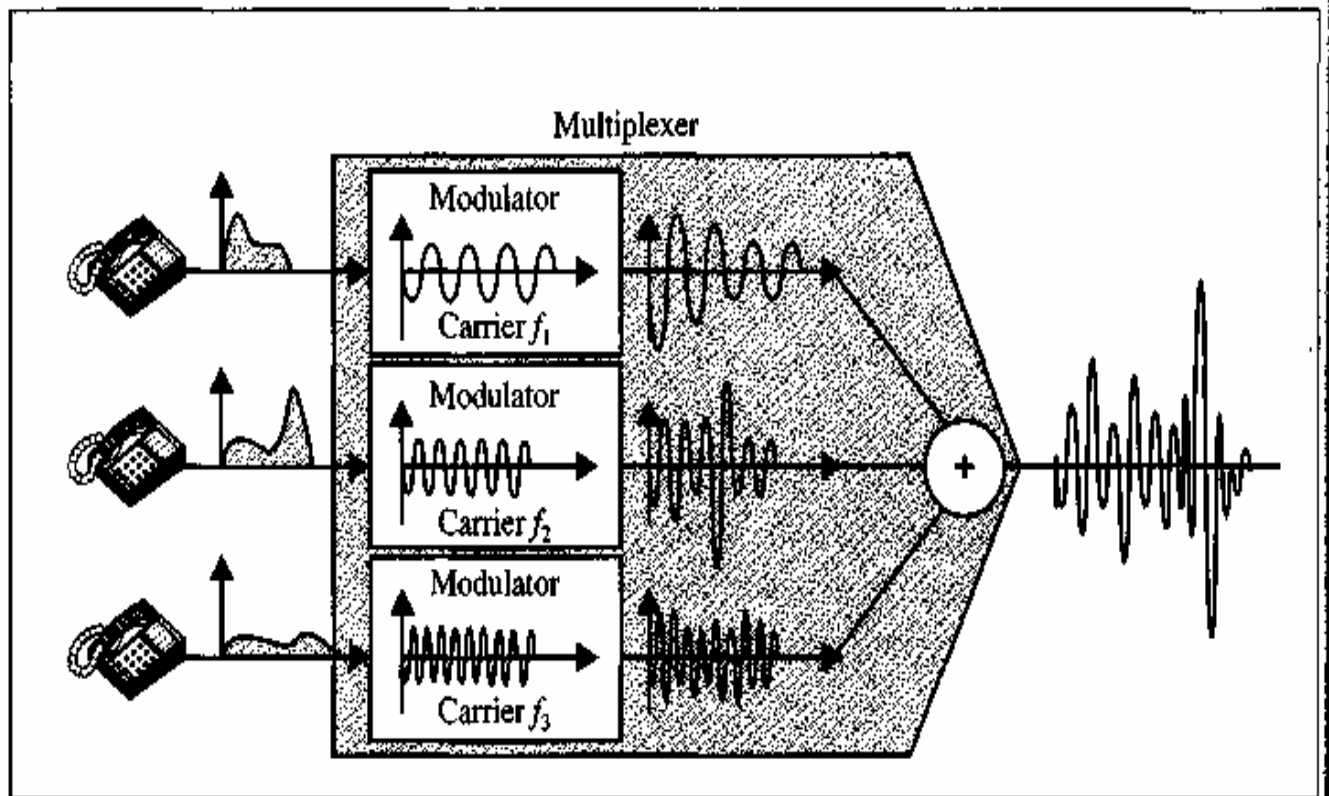
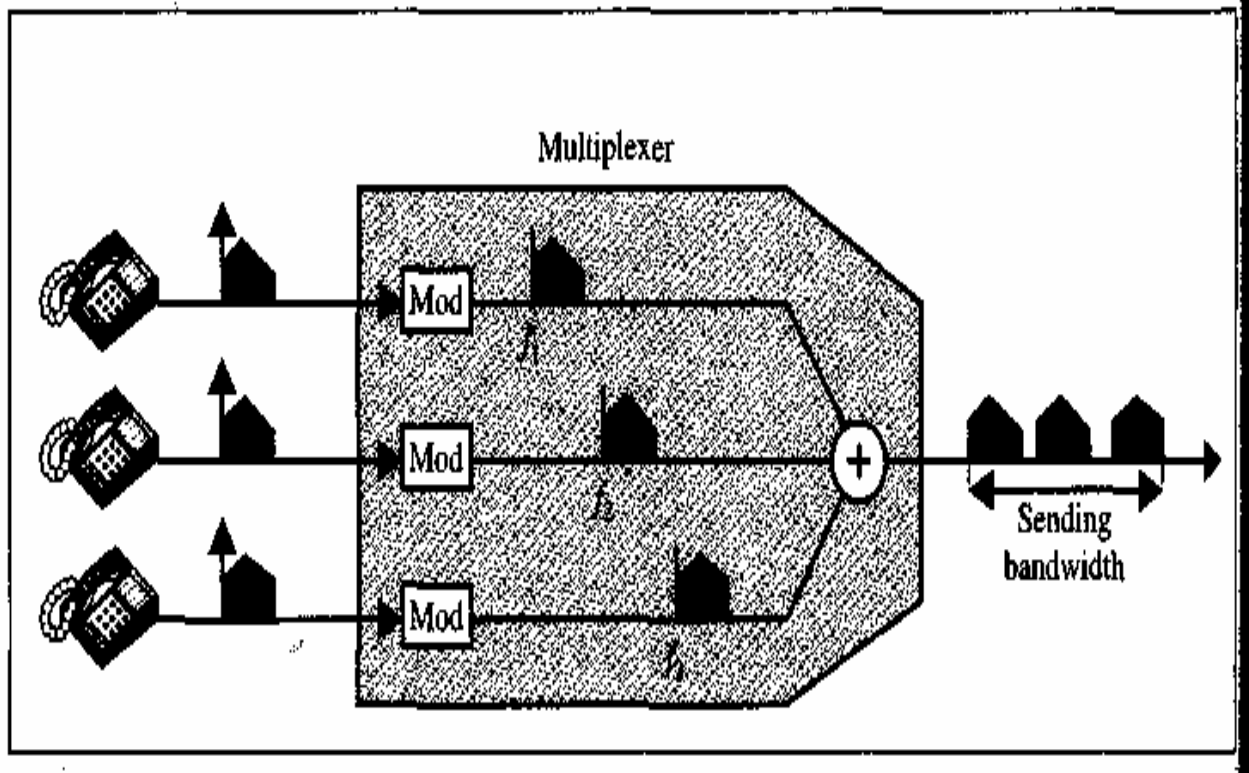


Figure 8.5 *FDM multiplexing process, frequency domain*



Демультимплексування

Демультимплексор використовує серію фільтрів для декомпозиції мультимплексного сигналу в складові сигнали. Індивідуальні сигнали потім передаються демодулятором, який відділяє їх від їх носіїв і передає їх до одержувачів, що очікують. Рис. 8.6 є ілюстрацією часової області мультимплексування FDM, як знову використовує три телефони, як пристрої комунікації. Частотна область того ж прикладу приведена на рис. 8.7.

Figure 8.6 *FDM demultiplexing process, time domain*

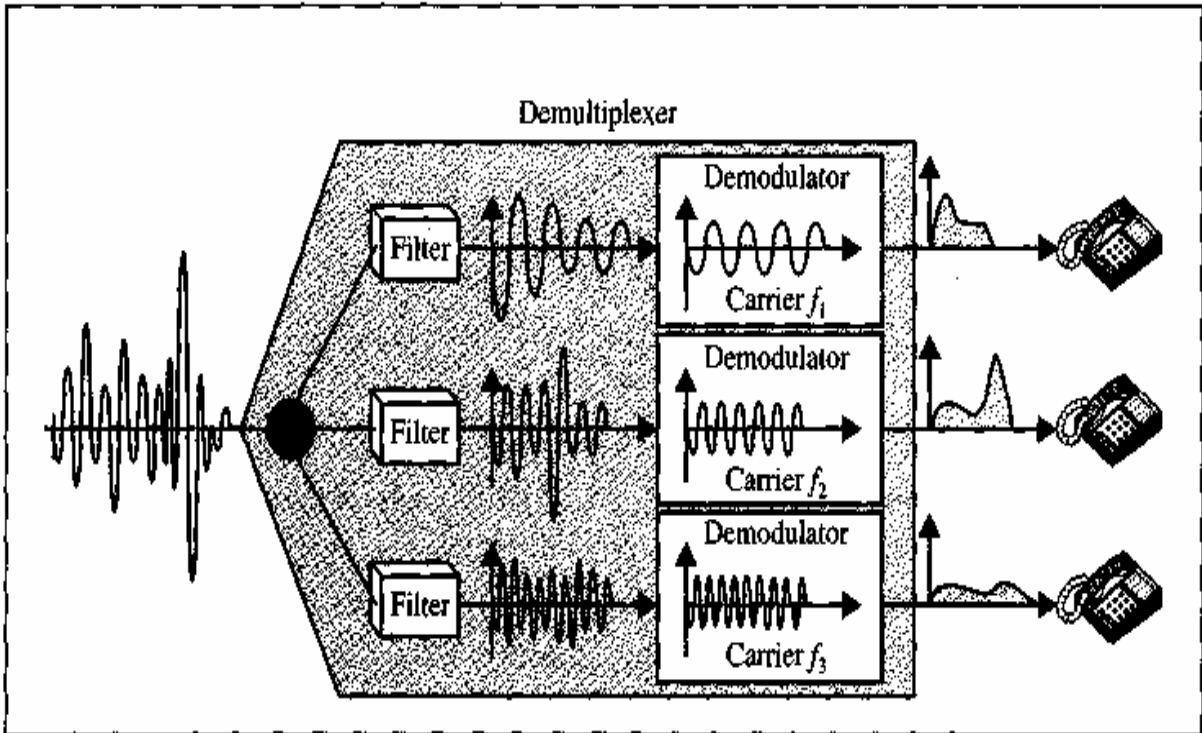
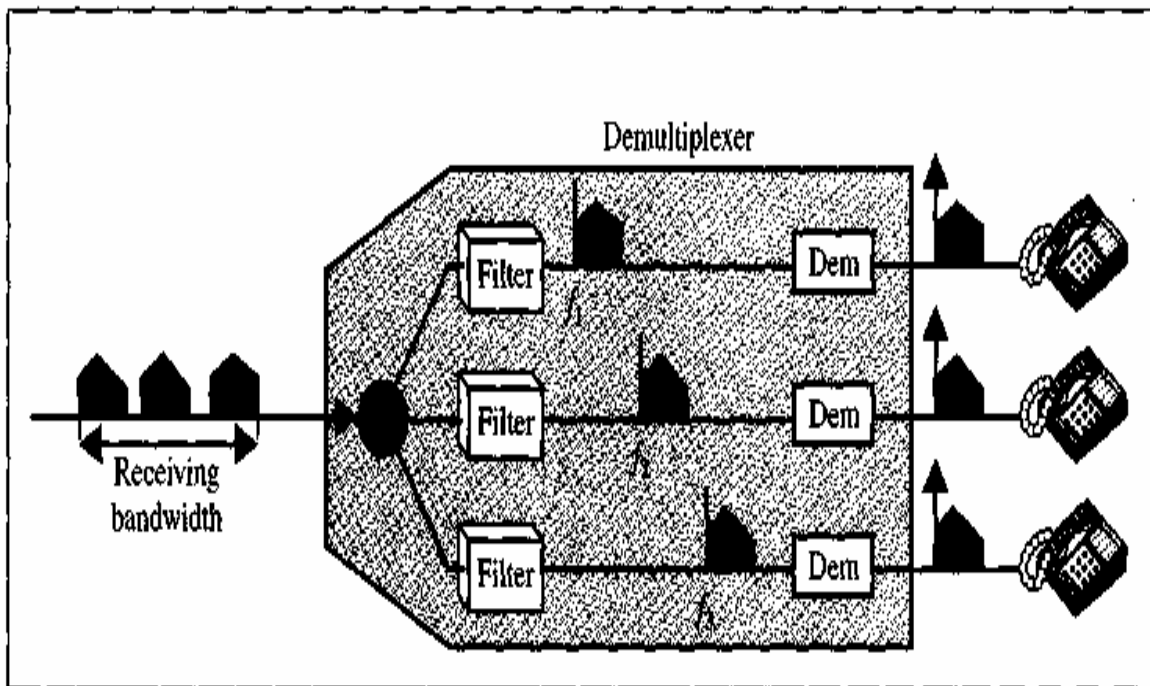


Figure 8.7 *FDM demultiplexing, frequency domain*



Комутація каналів на основі частотного мультиплексування

Технологія частотного мультиплексування каналів (FDM) була розроблена для телефонних мереж, але застосовується вона і для інших видів мереж, наприклад мереж кабельного телебачення.

Розглянемо особливості цього виду мультиплексування на прикладі телефонної мережі.

Мовні сигнали мають спектр шириною приблизно в 10 000 Гц, проте основні гармоніки вкладаються в діапазон від 300 до 3400 Гц. Тому для якісної передачі мови достатньо утворити між двома співбесідниками канал із смугою пропускання в 3100 Гц, який і використовується в телефонних мережах для з'єднання двох абонентів. В той же час смуга пропускання кабельних систем з проміжними підсилювачами, які сполучають телефонні комутатори між собою, звичайно складає сотні кілогерців, а іноді і сотні мегагерц.

Проте безпосередньо передавати сигнали декількох абонентних каналів по широкосмуговому каналу неможливо, оскільки всі вони працюють в одному і тому ж діапазоні частот і сигнали різних абонентів змішаються між собою так, що розділити їх буде неможливо.

Для розділення абонентних каналів характерна техніка модуляції високочастотного несучого синусоїдального сигналу низькочастотним мовним сигналом. Ця техніка подібна техніці аналогової модуляції при передачі дискретних сигналів модемами, тільки замість дискретного початкового сигналу використовуються безперервні сигнали, породжувані звуковими коливаннями. В результаті спектр модульованого сигналу переноситься в інший діапазон, який симетрично розташовується відносно несучої частоти і має ширину, приблизно співпадаючу з шириною модулюючого сигналу.

Якщо сигнали кожного абонентного каналу перенести в свій власний діапазон частот, то в одному широкосмуговому каналі можна одночасно передавати сигнали декількох абонентних каналів.

На входи FDM-комутатора поступають початкові сигнали від абонентів телефонної мережі. Комутатор виконує перенесення частоти кожного каналу в свій діапазон частот. Звичайно високочастотний діапазон ділиться на смуги, які відводяться для передачі даних абонентних каналів. Щоб низькочастотні складові сигналів різних каналів не змішувалися між собою, смуги роблять шириною в 4 кГц, а не в 3,1 кГц, залишаючи між ними проміжок страховки в 900 Гц.

В каналі між двома FDM-комутаторами одночасно передаються сигнали всіх абонентних каналів, але кожний з них займає свою смугу частот. Такий канал називають ущільненим.

Вихідний FDM-комутатор виділяє модульовані сигнали кожної несучої частоти і передає їх на відповідний вихідний канал, до якого безпосередньо підключений абонентний телефон.

В мережах на основі FDM-комутації прийнято декілька рівнів ієрархії ущільнених каналів. Перший рівень ущільнення утворюють 12 абонентних каналів, які складають базову групу каналів, що займає смугу частот шириною в 48 кГц з межами від 60 до 108 кГц.

Другий рівень ущільнення утворюють 5 базових груп, які складають супергрупу, із смугою частот шириною в 240 кГц і межами від 312 до 552 кГц. Супергрупа передає дані 60 абонентних каналів тональної частоти. Десять супергруп утворюють головну групу, яка використовується для зв'язку між комутаторами на великих відстанях. Головна група передає дані 600 абонентів одночасно і вимагає від каналу зв'язку смугу пропускання шириною не менше 2520 кГц з межами від 564 до 3084 кГц.

Комутатори FDM можуть виконувати як динамічну, так і постійну комутацію. При динамічній комутації один абонент ініціює з'єднання з іншим абонентом, посилаючи в мережу номер абонента, що викликається.

Комутатор динамічно виділяє даному абоненту одну з вільних смуг свого ущільненого каналу. При постійній комутації за абонентом смуга в 4

кГц закріплюється на тривалий термін шляхом настройки комутатора по окремому входу, неприступному користувачам.

Принцип комутації на основі розділення частот залишається незмінним і в мережах іншого вигляду, міняються тільки межі смуг, що виділяються окремому абонентному каналу, а також кількість низькошвидкісних каналів в ущільненому високошвидкісному.

8.3. Поділ по довжині хвилі WDM

Мультиплексування (WDM) поділу по довжині хвилі є концептуально тим самим, як FDM, за винятком того, що мультиплексування і демультиплексування залучають легкі сигнали, передані через волокно-оптичні канали. Ідея є тією ж: ми об'єднуємо різні сигнали різних частот. Проте, різниця є в тому, що частоти дуже високі.

Рисунок 8.8 дає концептуальний перегляд WDM мультиплексора і демультиплексора. Дуже вузькі полоси світла від різних джерел з'єднуються, щоб утворити більш широку полосу світла. В одержувачі, сигнали відділяються демультиплексором.

Таке може викликати здивування про механізм WDM. Хоча технологія дуже комплексна, ідея дуже проста. Ми хочемо об'єднати багаторазові прості джерела в одному єдиному промені світла в мультиплексорі й потім назад розділити в демультиплексорі. Об'єднання і розбиття простих джерел легко обробляють призмою. Згідно з основами фізики призма згинає пучок світла, відповідно до кута нахилу і частоти. Використовуючи цей механізм, мультиплексор може об'єднати окремі вхідні пучки світла, кожний з яких містить вузьку групу частот, в один вихідний пучок більш широкої групи частот. Демультиплексор може повернути назад цей процес. Рисунок 8.9 показує загальне представлення.

Figure 8.8 WDM

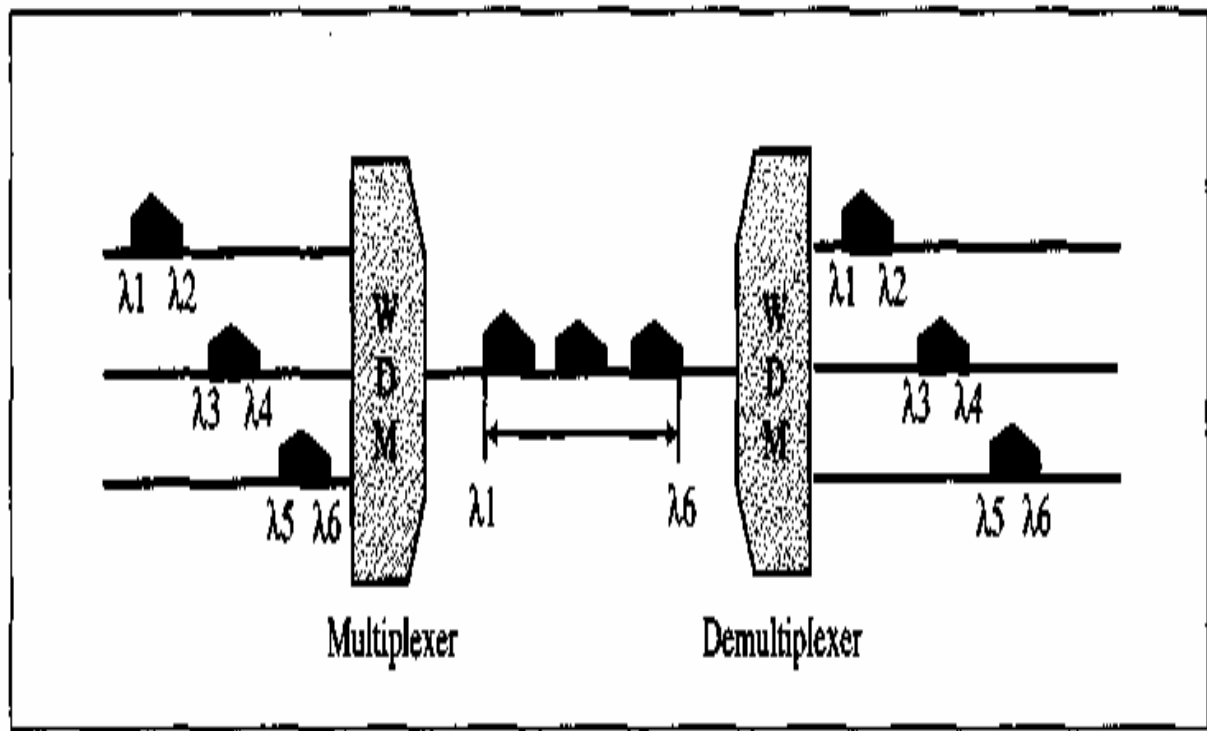
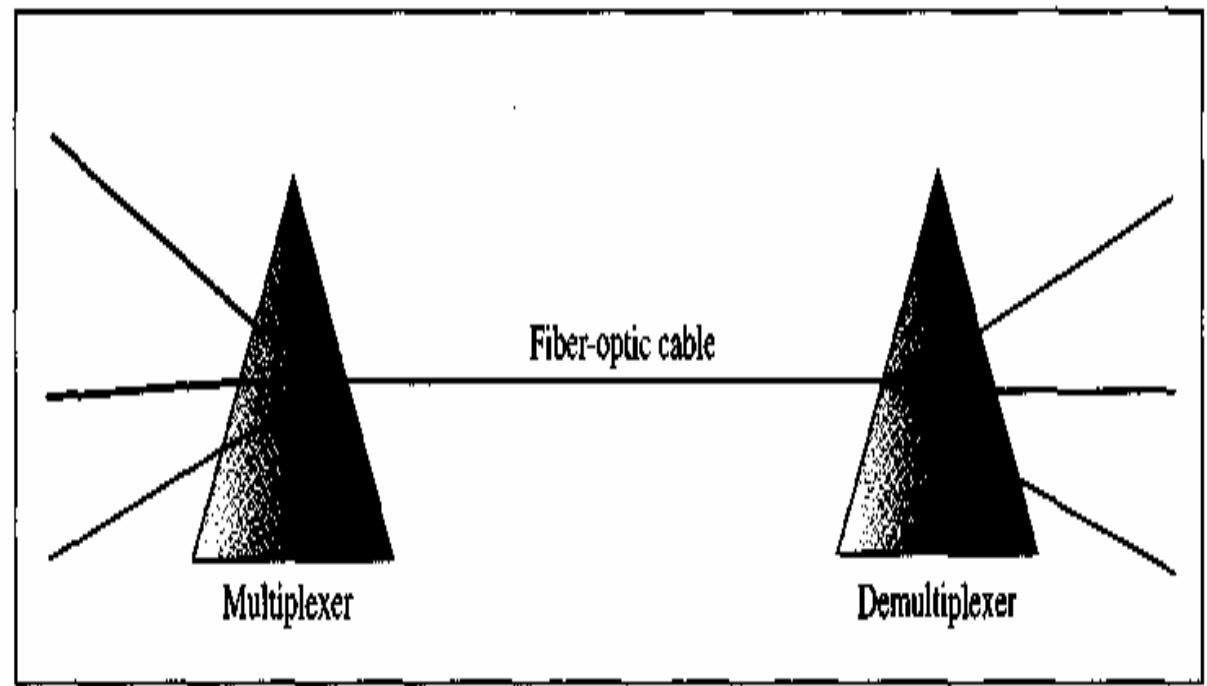


Figure 8.9 Prisms in WDM multiplexing and demultiplexing



Забезпечення дуплексного режиму роботи на основі технологій FDM, TDM і WDM

Залежно від напрямку можливої передачі даних способи передачі даних по лінії зв'язку діляться на наступні типи:

- сімплексний – передача здійснюється по лінії зв'язку тільки в одному напрямі;
- напівдуплексний – передача ведеться в обох напрямках, але поперемінно в часі. Прикладом такої передачі служить технологія Ethernet
- дуплексний – передача ведеться одночасно в двох напрямках. Дуплексний режим – найбільш універсальний і продуктивний спосіб роботи каналу.

Найпростішим варіантом організації дуплексного режиму є використання двох незалежних фізичних каналів (двох пар провідників або двох світодіодів) в кабелі, кожний з яких працює в сімплексному режимі, тобто передає дані в одному напрямі. Саме така ідея лежить в основі реалізації дуплексного режиму роботи в багатьох мережних технологіях, наприклад Fast Ethernet або ATM.

Іноді таке просте рішення виявляється неприпустимим або неефективним. Частіше за все це відбувається в тих випадках, коли для дуплексного обміну даними є всього один фізичний канал, а організація другого пов'язана з великими витратами.

Наприклад, при обміні даними за допомогою модемів через телефонну мережу у користувача є тільки один фізичний канал зв'язку з АТС – двохрантова лінія, і проводити другу навряд чи доцільно. В таких випадках дуплексний режим роботи організовується на основі розділення каналу на два логічні підканали за допомогою техніки FDM або TDM.

Модеми для організації дуплексного режиму роботи на двохранвній лінії застосовують техніку FDM. Модеми, що використовують частотну модуляцію, працюють на чотирьох частотах: дві частоти – для кодування

одиниць і нулів в одному напрямі, а ще дві частоти – для передачі даних у зворотному напрямі.

При цифровому кодуванні дуплексний режим на двохранівній лінії організовується за допомогою техніки TDM. Частина тайм-слотів використовується для передачі даних в одному напрямі, а частина – для передачі в іншому напрямі. Звичайно тайм-слоти протилежних напрямів чергують, через що такий спосіб іноді називають передачею «пінг-понгу». TDM-розділення лінії характерне, наприклад, для цифрових мереж з інтеграцією послуг (ISDN) на абонентних двохранівних закінченнях.

У волоконно-оптичних кабелях при використуванні одного оптичного волокна для організації дуплексного режиму роботи застосовується передача даних в одному напрямі за допомогою світлового пучка однієї довжини хвилі, а в зворотному – іншої довжини хвилі. Така техніка відноситься до методу FDM, проте для оптичних кабелів вона отримала назву розділення по довжині хвилі (Wave Division Multiplexing, WDM). WDM застосовується і для підвищення швидкості передачі даних в одному напрямі, звичайно використовуючи від 2 до 16 каналів.

8.4. Часове мультиплексування (TDM)

Часове мультиплексування (TDM) - це цифровий процес, який може застосовуватися, коли місткість передавального середовища більша, ніж діапазон передачі даних, що вимагається пристроями передачі і отримання. В такому випадку можуть трапитись багаторазові передачі.

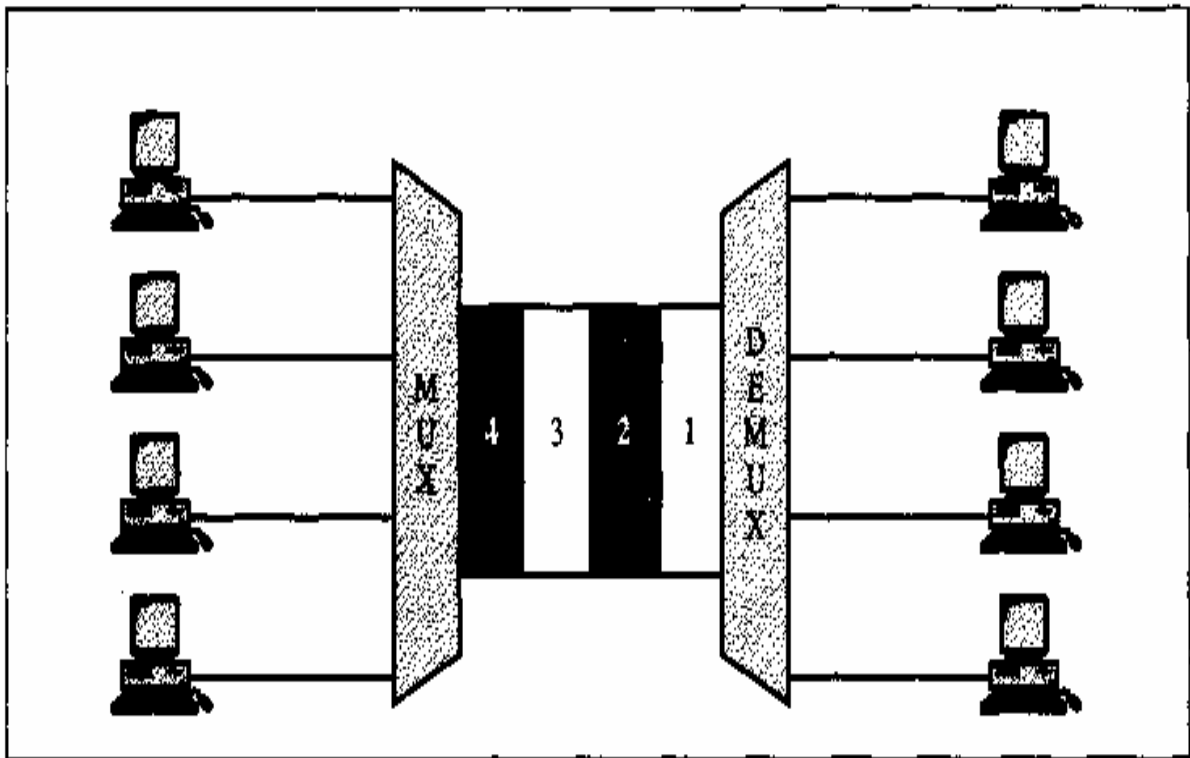
Рис. 8.10 дає концептуальне представлення TDM. Потрібно зазначити, що той же передатчик використовується як і в FDM; проте, передатчик показано поділений на частини за часом, а не за частотою.

На рисунку TDM, частини сигналів 1, 2, 3, і 4 займають передавач послідовно. Як аналогію, можна уявити собі лижний підйомник, що працює в декілька переходів. Кожний запуск має власну лінію і лижники в кожній лінії

повертається по черзі на підйомнику. Оскільки кожний стілець досягає верху гори, лижник, що їхав, легко звільняється і їде на лижах вниз.

TDM може виконуватися двома шляхами: синхронний TDM і асинхронний TDM.

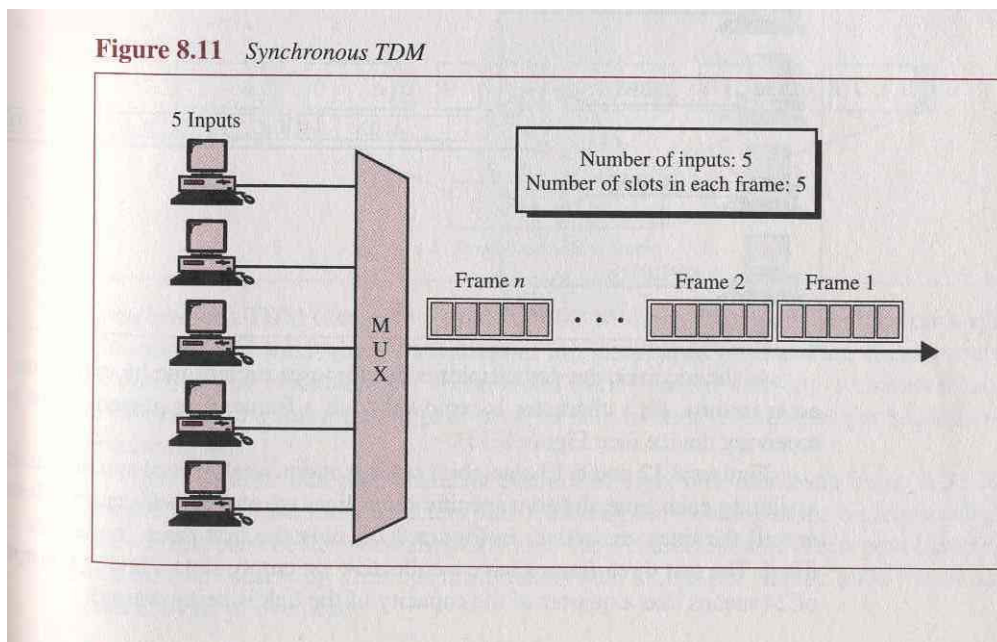
Figure 8.10 TDM



Синхронний TDM

В синхронному поділі в часі, термін синхронний термін має інше значення від того, що використовується в інших областях телекомунікацій. Тут синхронизування означає, що мультиплексор локалізує точно в цей момент часу слот до кожного пристрою весь час, немає значення чи має пристрій щось-небудь для передачі. Часовий слот А, наприклад, призначений для пристрою А сам і не може бути використаний будь-яким іншим пристроєм. Кожного разу, коли виділений слот часу активізується, пристрій має нагоду послати частину даних. Якщо пристрій не в змозі передати або не має даних для посилання, слот часу залишається порожнім.

Фрейми. Часові слоти групуються у фрейми. Фрейм складається з одного повного циклу слотів часу, включаючи один або більше слотів, прикріплених до кожного пристрою пересилки (див. рис. 8.11). В системі з n вхідними лініями, кожний фрейм має як мінімум n слотів, кожен з яких локалізований для несення даних від специфічної вхідної лінії. Якщо всі вхідні пристрої які сумісно використовують передатчик, передають на тій же швидкості дані, кожний пристрій має один фрейм на слот. Проте, є можливим пристосування різних швидкостей передачі даних. Передача з двома слотами на фрейм призведе до двічі швидшого прибуття даних.



Прорізи часу, призначені до даного пристрою, займають те ж розташування в кожному фреймі і складають даний канал пристрою. На рис. 1.11 ми показуємо п'ять вхідних ліній, які мультиплексуються на єдину лінію, що використовує синхронний TDM. В цьому прикладі, всі входи мають ту ж швидкість передачі даних, так що число слотів часу в кожному фреймі рівне кількості вхідних ліній.

Перемикання

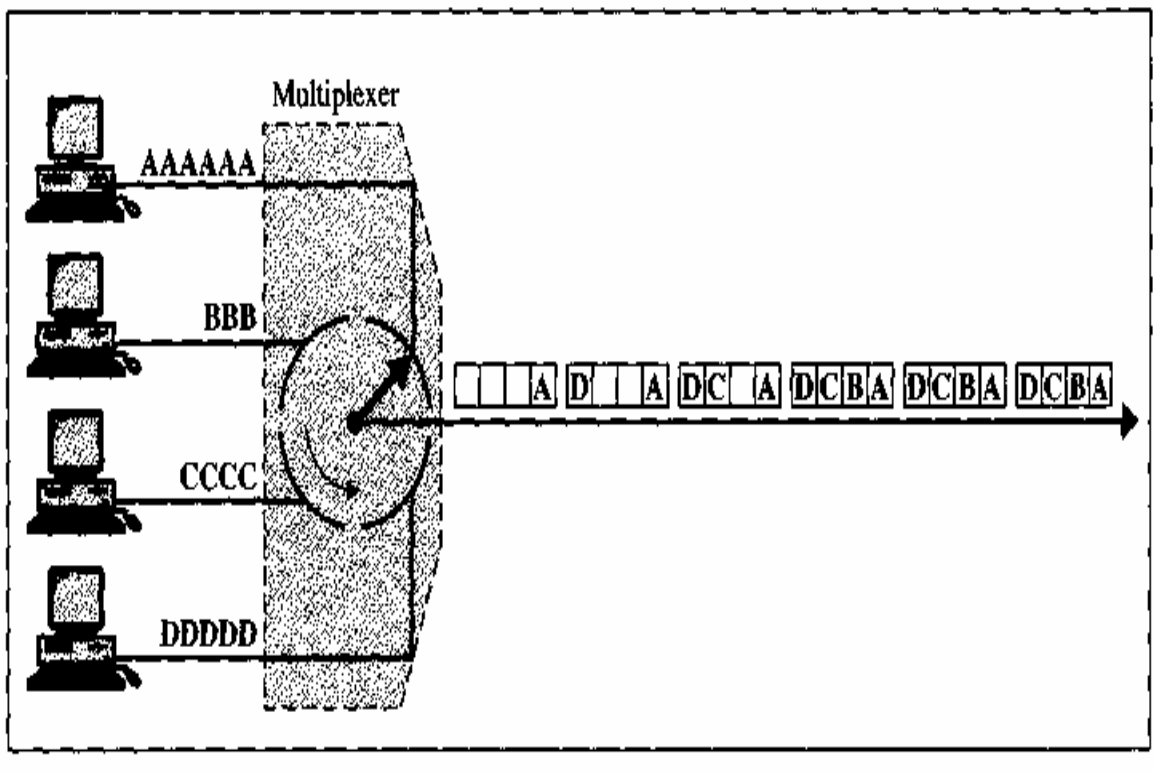
Синхронний TDM можна порівнювати із перемикачем, який дуже швидко обертається. Оскільки перемикач відкривається перед пристроєм, цей

пристрій має нагоду послати конкретизовану кількість (x бітів) даних на канал. Перемикач рухається від пристрою до пристрою зі стабільною швидкістю і у певному порядку.

Перемикач може бути зроблено бітом, байтом, або будь-яким іншим елементом даних. Іншими словами, мультиплексор може взяти один байт з кожного пристрою, потім інший байт від кожного пристрою, і так далі. В даній системі, перешаровані одиниці завжди будуть того ж розміру.

Рис. 8.12 показує перешарування і будівництво фрейма. В прикладі, ми перешарували різні передачі символом (рівному одному байту кожний), але поняття є те саме для елементів даних будь-якої довжини. Як бачите, кожний пристрій пересилає різний повідомлення. Мультиплексор перешаровує різні повідомлення і формує їх в фрейми перед відправленням їх на передавач.

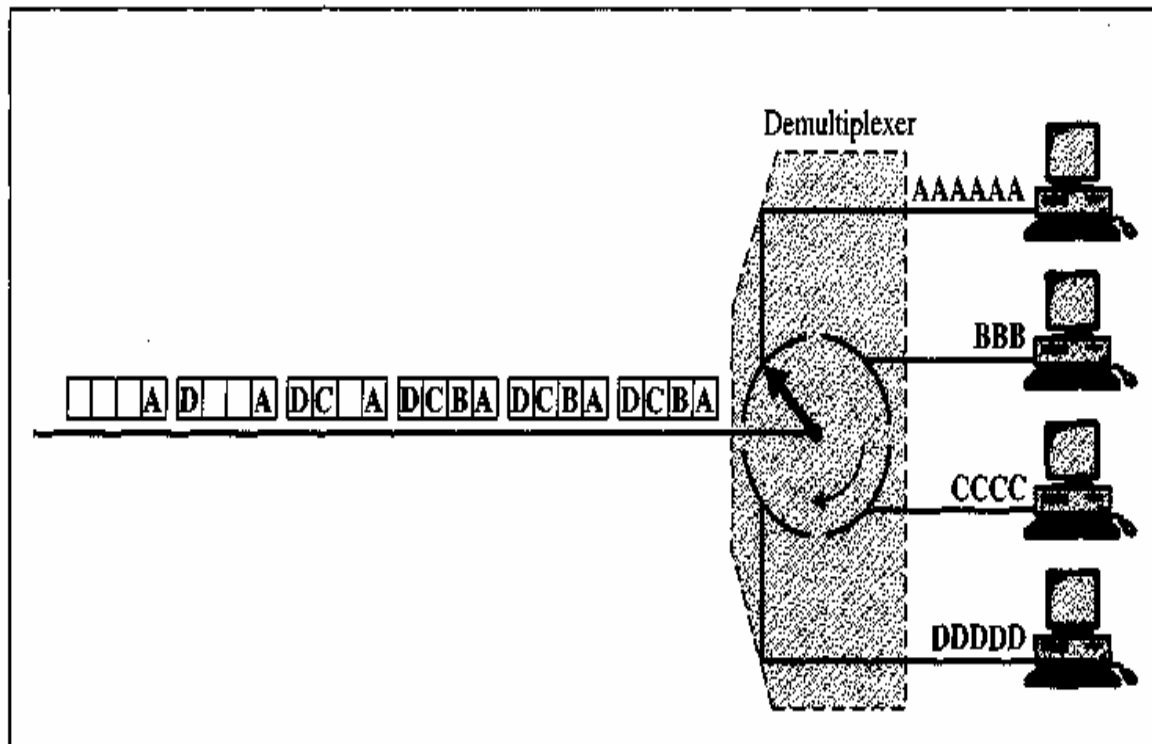
Figure 8.12 Synchronous TDM, multiplexing process



В одержувачі, демультіплексор розділяє кожний фрейм за допомогою витягання кожного символу по черзі. Коли символ видалений з фрейма, він передається відповідному пристрою отримування (див. рис. 8.13).

Рис. 8.12 і 8.13 також показують головну слабкість синхронного TDM. Призначаючи кожного разу слот до специфічної вхідної лінії, ми закінчуємо з порожніми слотами кожного разу коли не всі лінії активні. На рис. 1.12, тільки перші три фрейми є цілком заповнені. Останні три фрейми мають шість спільних порожніх слотів. Наявність 6 порожніх слотів із 24 означає, що четверть місткості передавача витрачається.

Figure 8.13 *Synchronous TDM, demultiplexing process*

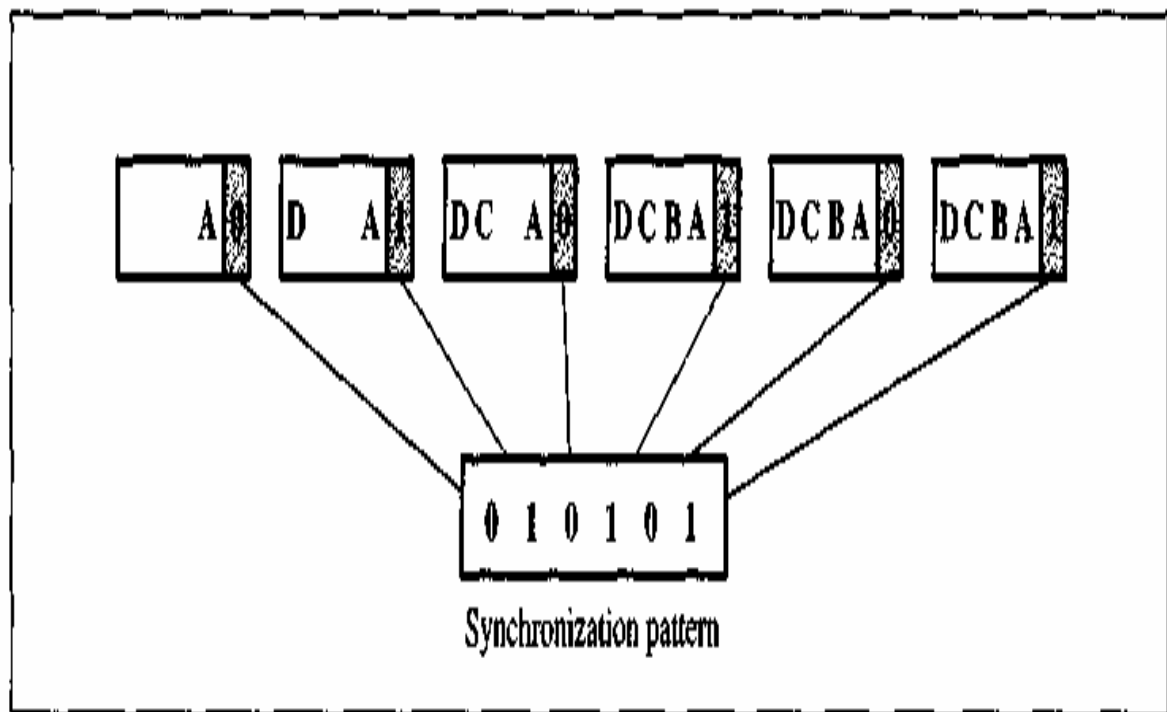


Формування бітів

Виходячи з того, що порядок часових слотів в синхронній системі TDM не змінюється від фрейма до фрейма, дуже маленька надлишкова інформація необхідна, щоб увійти до кожного фрейма. Порядок отримань говорить демультіплексору куди перенаправляти кожного разу слот, так що ніяка адресація непотрібна. Різні коефіцієнти, проте, можуть викликати часову

несумісність. Для цього, один або більше бітів синхронізації звичайно збільшуються для кожного фрейма. Ці біти, що називаються фреймовими **бітами**, слідуєть шаблону, фрейм до фрейма, що дозволяє демультимплексору виконувати синхронізацію з вхідним потоком, таким чином це може відділити слоти часу точно. В більшості випадків, ця інформація синхронізації складається з одного біта за фрейм, між 0 і 1 (010101010), як показано на рис. 8.14.

Figure 8.14 Framing bits

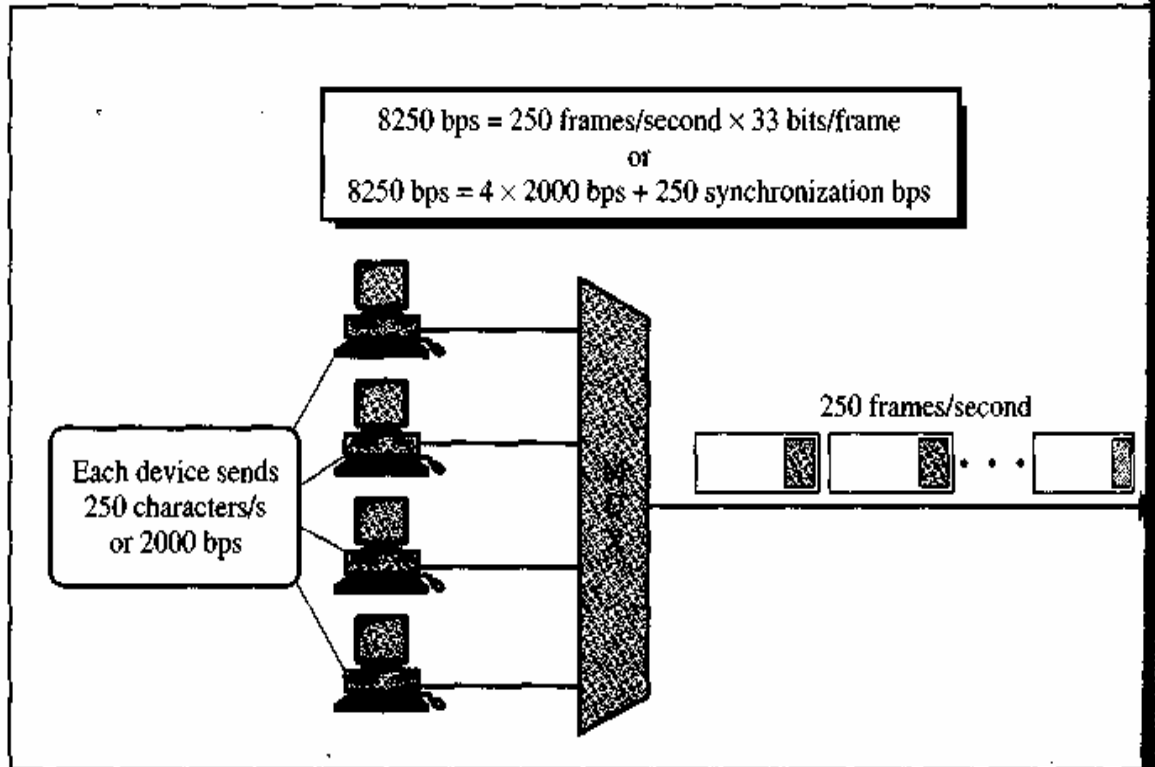


Приклад синхронного TDM

Уявимо собі, що ми маємо чотири вхідні джерела на синхронному передавачі TDM, де передачі перешаровують символом. Якщо кожне джерело створює 250 символів за секунду, і кожний фрейм несе 1 символ від кожного джерела, шлях передачі повинен здатний нести 250 фреймів за секунду (див. рис. 8.15). Якщо ми припускаємо, що кожний символ складається з восьми бітів, потім кожний фрейм - це 33 біти: 32 біти для

чотирьох символів плюс 1 фреймовий біт. Проглядаючи взаємозв'язки бітів, ми бачимо, що кожний пристрій створює 2000 bps (250 символи з 8 бітами на символ), але лінія несе 8250 bps (250 фрейми з 33 бітами за фрейм): 8000 бітів даних і 250 бітів службової інформації.

Figure 8.15 *Data rate calculation for frames*



Вставка біта. Як зазначалося раніше, є можливим з'єднувати пристрої з різним синхронним TDM. Наприклад, пристрій А використовує одноразовий слот, поки прилад В використовує два. Число слотів у фреймі і вхідних лініях, до яких залишитися приєднатись, є сталим в даній системі, але пристрої з різними швидкостями передачі даних контролюються різне число цих слотів. Пам'ятайте: довжина часового слоту є сталою, однак, різні швидкості передачі даних повинні ділитись на ціле число. Наприклад, ми можемо пристосувати пристрій, який є в 5 разів швидший від інших пристроїв, надаючи йому п'ять слотів до одного для кожного з решти пристроїв. Ми, однак, не можемо пристосувати пристрій, який є в п'ять з

половиною разів швидший за допомогою цього методу, тому що ми не можемо вводити половину слоту у фрейм.

Асинхронний TDM

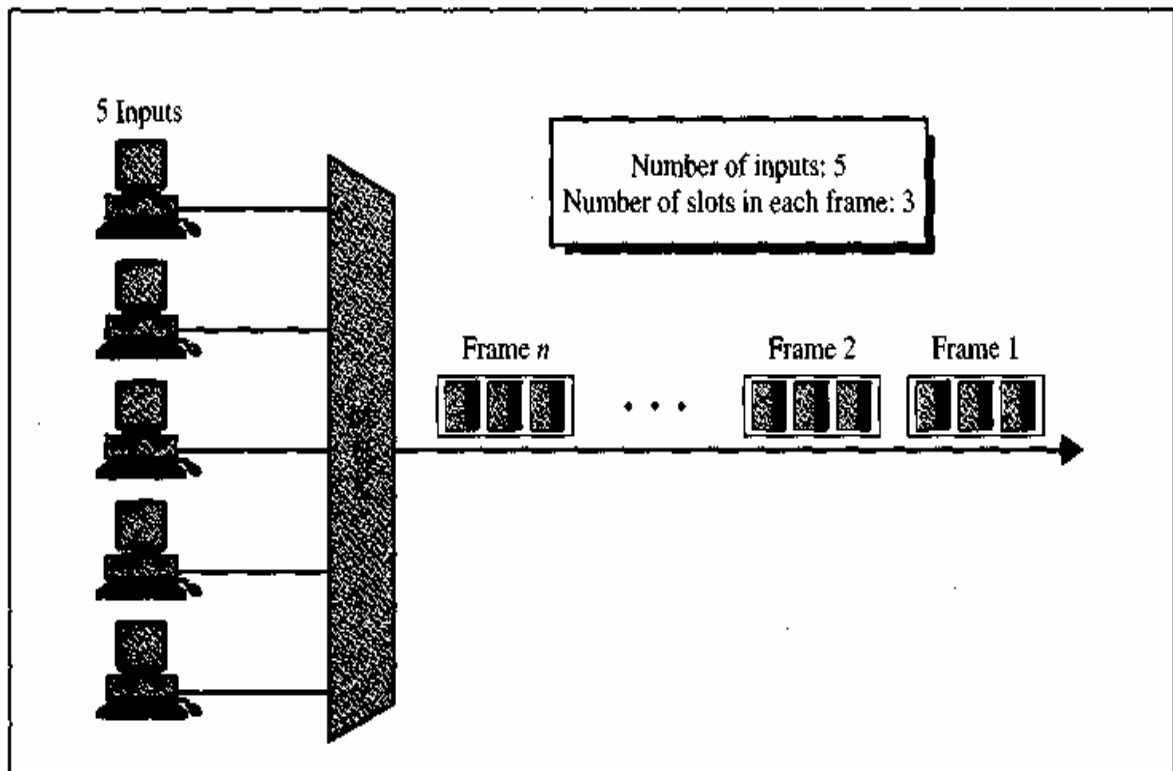
Оскільки ми бачили в попередній секції, синхронний TDM не гарантує, що вся місткість передатчика використовується. Фактично, це більш вірогідно, що тільки частина всього часу використовується в даний момент. Оскільки часові слоти чітко визначені і виправлені, коли під'єднаний пристрій J не передає, відповідний слот виявляється порожнім. Наприклад, уявіть собі, що ми мультиплексували вихідні ідентичні комп'ютери в єдину лінію. Використовуючи синхронний TDM, швидкість повинна скласти як мінімум в 20 разів більше швидкості кожної вхідної лінії. Але що, коли тільки 10 комп'ютерів використовується в даний час? Половина місткості лінії втрачається.

Асинхронне ущільнення в часі, або статистичне ущільнення в часі, розроблено, щоб уникати цього виду недоліку. Як з *“синхронним”* терміном, термін *“асинхронний”* трохи відрізняється в мультиплексуванні, ніж в інших областях передач даних. Тут це означає гнучкість.

Подібно синхронному TDM, асинхронний TDM дозволяє цілому ряду вхідних ліній більш низької швидкості мультиплексуватись до єдиної лінії вищої швидкості. На відміну від синхронного TDM, в асинхронному TDM повна швидкість вхідних ліній може бути більшою, ніж місткість шляху.

В синхронній системі, якщо ми маємо n вхідних ліній, фрейм містить виправлене число як мінімум n слотів часу. В асинхронній системі, якщо ми маємо n вхідних ліній, фрейм містить не більше ніж m слотів, з m менше ніж n (див. рис. 8.16). В цьому випадку, асинхронний TDM підтримує те ж число вхідних ліній як синхронний TDM з більш низькою місткістю. Або, на тому ж передатчику, асинхронний TDM може підтримувати більше пристроїв, ніж синхронний TDM.

Figure 8.16 Asynchronous TDM

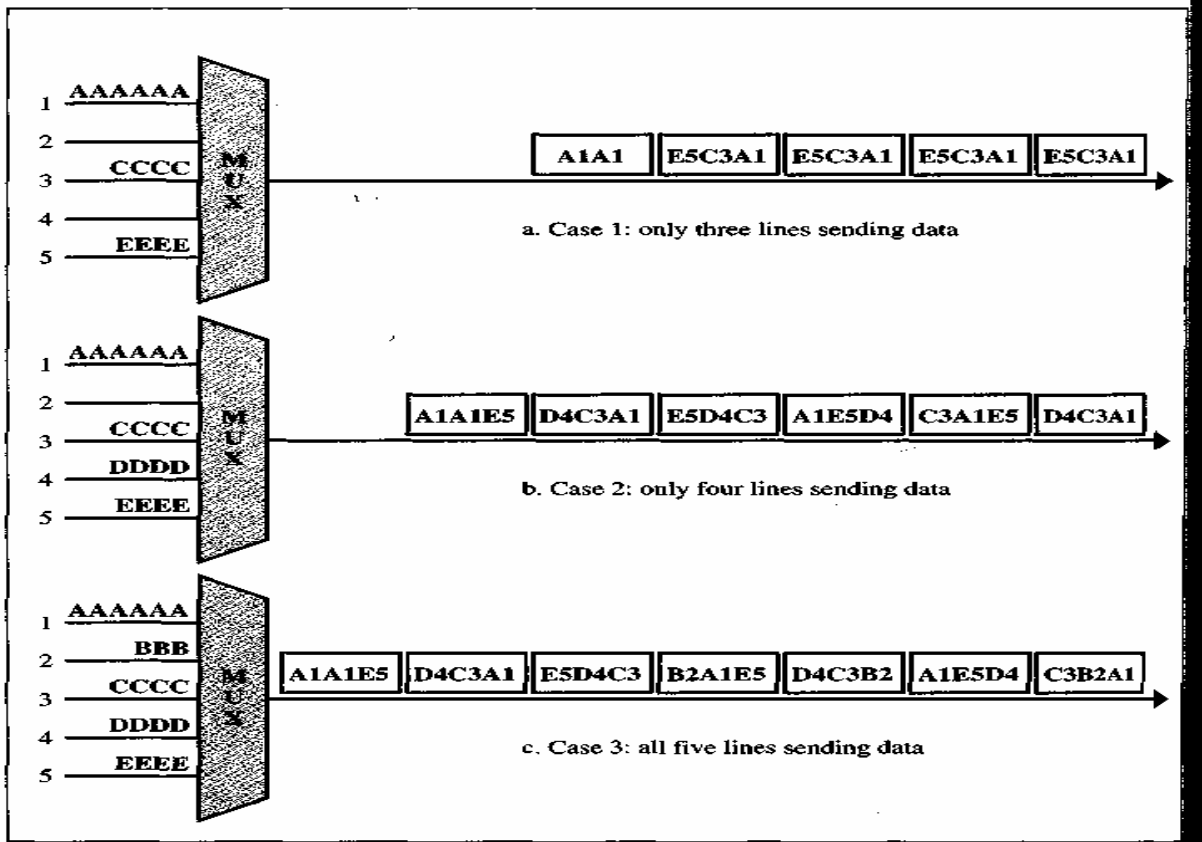


Число слотів часу в асинхронному фреймі (m) TDM засновано на статистичному аналізі числа вхідних ліній, які, ймовірно, передаються в будь-якому даному часі. Швидше, ніж чітко призначені, кожний проріз доступний до будь-якої з приєднаних вхідних ліній, які мають дані на відсилку. Мультиплексор сканує вхідні лінії, приймає частини даних, поки фрейм наповнений, а потім посилає фрейм через передатчик. Якщо не є достатньо даних, щоб заповнити фрейм всіх слотів, переданий фрейм тільки частково заповнюється; тому повна місткість передатчика не може складати 100 відсотків часу, що використовується. Але здатність локалізувати слоти часу динамічно пов'язана з більш низьким співвідношенням слотів часу до вхідних ліній, що дуже зменшує ймовірність і ступінь збою.

Рис. 8.17 показує систему, де п'ять комп'ютерів відкрило канал зв'язку, використовуючи асинхронний TDM. В цьому прикладі, розмір фрейма - це три прорізи. Малюнок показує, як мультиплексор обробляє три рівні трафіку.

В першому випадку, тільки три з п'яти комп'ютерів мають дані для відправлення (середній сценарій для цієї системи, як вказують факти, що розмір фрейма трьох слотів був вибраний). В другому випадку, чотири лінії відсилають дані, більші на одне число, ніж число слотів на фрейм. В третьому випадку, всі лінії пересилають дані. В кожному випадку, мультиплексор сканує пристрої в порядку В з 1 до 5, наповнюючи слоти часу по мірі надходження даних для передачі.

Figure 8.17 Examples of asynchronous TDM frames



В першому випадку, три активні вхідні лінії відповідають трьом слотам у фреймі В. Для перших чотирьох фреймів, входи симетрично розповсюджується серед всіх з'єднаних пристроїв. П'ятим фреймом, проте, пристрої 3 і 5 завершили свої передачі, але пристрій 1 ще має два символи для передачі. Мультиплексор збирає дані А від пристрою 1, сканує вниз лінію без пошуку іншої передачі, і повертається пристрою 1, щоб забрати останнє А. Там не існує ніяких даних, щоб наповнити заключний слот,

мультиплексор тоді передає п'ятий фрейм з тільки двома наповненими слотами.

В системі синхронного TDM, шість фреймів п'яти часових слотів, кожен буде потрібен для передачі всіх даних – загалом 30 часових слотів. Але тільки 14 з тих слотів мали бути заповнені, залишаючи лінію невикористану для більш ніж половини невикористаного часу. З асинхронною системою, показаною тут, тільки один переданий фрейм частково порожній. Протягом решти часу передачі, повна місткість передатчика задіюється.

В другому випадку, є ще одна активна вхідна лінія, яка має слоти слоти в кожному фреймі. В цей час, поки мультиплексор сканує від 1 до 5, фрейм наповнюється раніше всі лінії будуть перевірені. Перший фрейм, таким чином, переносить дані від пристроїв 1,3, і 4, але не 5.

Мультиплексор продовжує сканування, поміщаючи першу частину передачі 5-го пристрою в перший слот наступного фрейма, потім повертається назад до верху лінії і вставляє другу частину даних 1-го пристрою в другий слот, і так далі. Як бачите, коли число активних відправників не дорівнює числу слотів у фреймі, слоти часу не наповнені симетрично. Пристрій 1, в цьому прикладі, займає перший слот в першому фреймі, другий слот в другому фреймі, і так далі.

У випадках 2 і 3, якщо швидкість лінії рівна трьом вхідним лініям, дані, що мають бути передані, прибудуть швидше, ніж мультиплексор зможе доставит їх передатчику. У такому разі, буфер потрібен, щоб запам'ятати дані, поки мультиплексор буде готовий.

Адресація і Службова інформація

У випадках 2 і 3 в згаданому вище прикладі ілюструється головну слабкість асинхронного TDM: звідки демультіплексор знає, якому слоту належить яка вихідна лінія? В синхронному TDM, пристрій, до якого дані в

слоті часу належати, вказує місцеположення часового слоту у фреймі. Але в асинхронному TDM, дані від даного пристрою можуть знаходитися в першому слоті одного фрейма і в третьому наступного. У відсутності виправлених позиційних взаємозв'язків, кожного разу слот повинен нести адресу, що повідомляє демультимплексору, як направити дані. Ця адреса тільки для локального використання, приєднується мультимплексором і відкидається демультимплексор одразу після прочитання. На рис. 8.17 адреса конкретизується цифрою.

Часові слоти змінної довжини. Асинхронний TDM може пристосувати трафік зміною швидкостей передач даних за допомогою варіювання довжини слотів часу. Станції, що передають дані на більш високій швидкості, можуть отримати більш довгий слот. Управління полями змінної довжини вимагає, щоб службові біти були приєднані до початку кожного слоту часу щоб вказати довжину майбутньої частини даних. Ці додаткові біти також збільшують надлишкову інформацію і є ефективними тільки з більшими прорізами часу.

Комутація каналів на основі розділення часу

Комутація на основі техніки розділення частот розроблялася з розрахунку на передачу безперервних сигналів, що представляють голос. При переході до цифрової форми представлення голосу була розроблена нова техніка мультимплексування, що орієнтується на дискретний характер передаваних даних.

Ця техніка носить назву мультимплексування з розділенням часу. Рідше використовується і інша її назва – техніка синхронного режиму передачі. Рис. 2.28 пояснює принцип комутації каналів на основі техніки TDM.

Апаратура TDM-мереж – мультимплексори, комутатори, демультимплексори – працює в режимі розділення часу, по черзі обслуговуючи протягом циклу своєї роботи всі абонентні канали. Цикл

роботи устаткування TDM рівний 125 мкс, що відповідає періоду проходження вимірів голосу в цифровому абонентному каналі. Це значить, що мультиплексор або комутатор встигає вчасно обслужити будь-який абонентний канал і передати його черговий вимір далі по мережі. Кожному з'єднанню виділяється один квант часу циклу роботи апаратури, званий також тайм-слотом. Тривалість тайм-слота залежить від числа абонентних каналів, обслуговуваних мультиплексором TDM або комутатором.

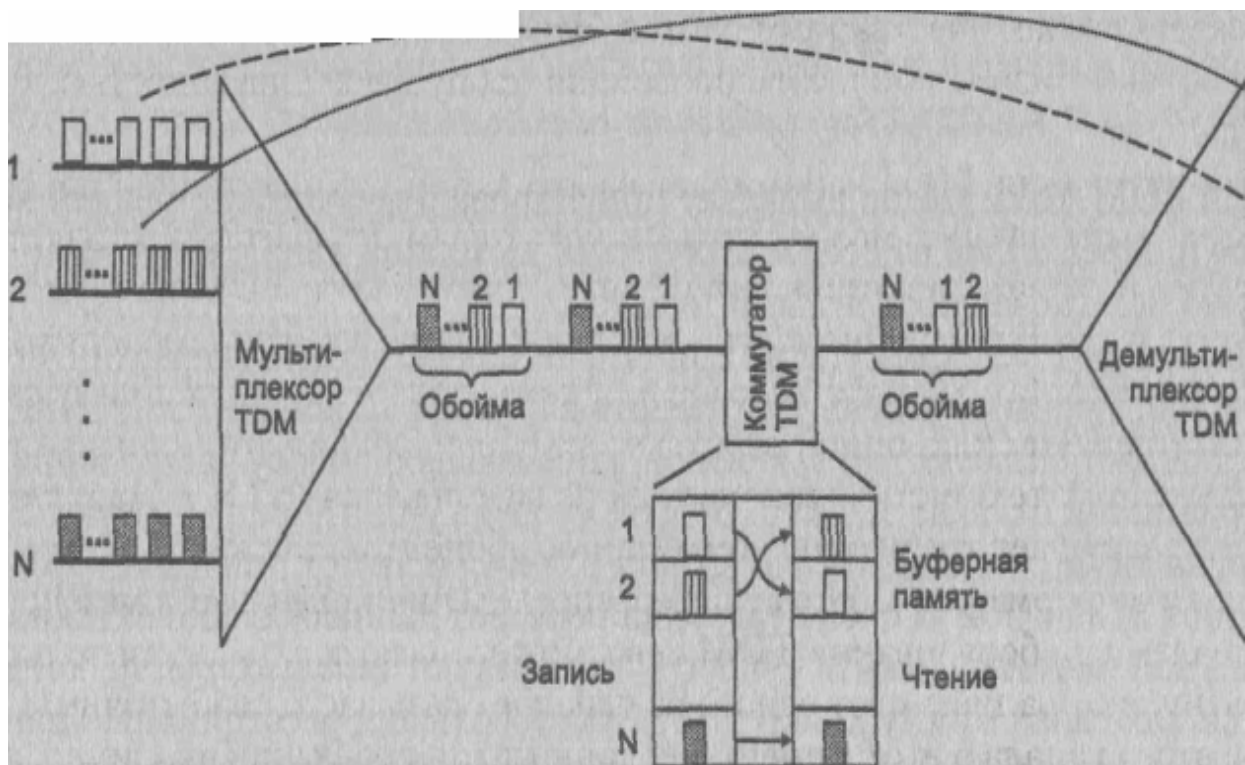


Рис. 2.28. Комутація на основі розділення каналу в часі

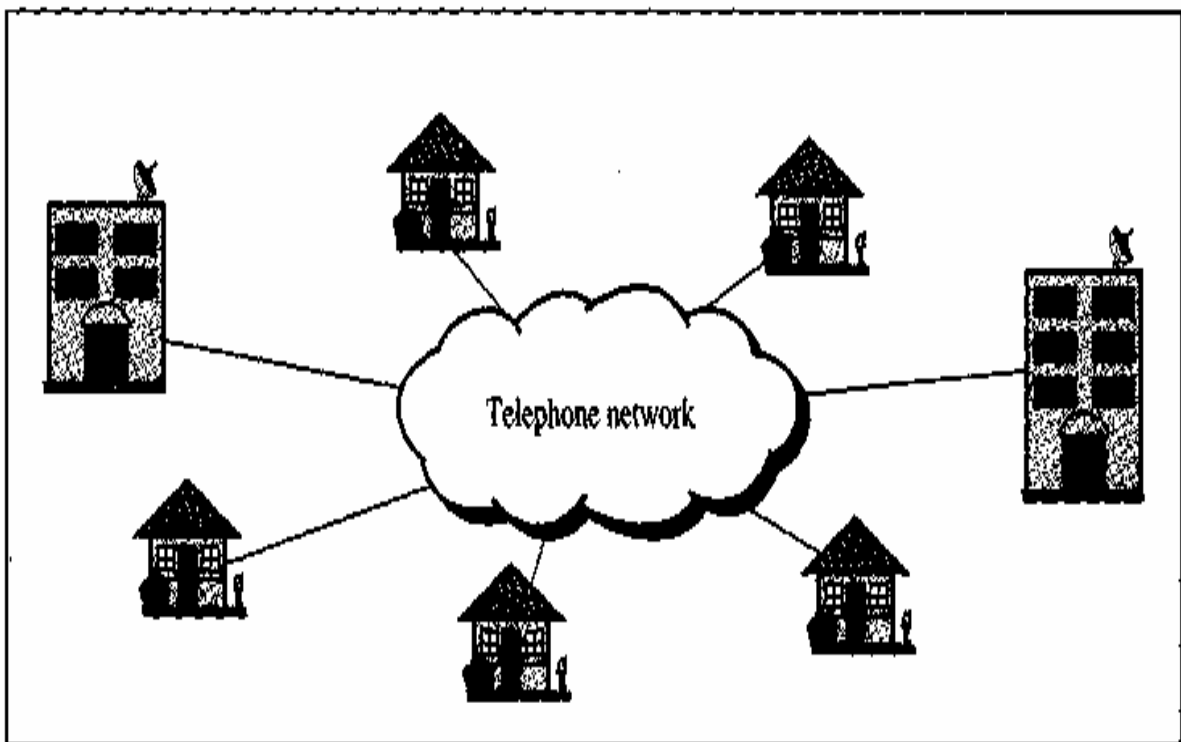
Мультиплексор приймає інформацію по N вхідних каналах від кінцевих абонентів, кожний з яких передає дані по абонентному каналу із швидкістю 64 Кбіт/с – 1 байт кожні 125 мкс. В кожному циклі мультиплексор виконує наступні дії:

- прийом від кожного каналу чергового байта даних;
- складання з прийнятих байтів ущільненого кадру, званого також обоймою.

8.5. Додаток мультиплексування: телефонна система

Мультиплексування на протязі довгого часу є дуже важливий інструмент телефонної індустрії. Погляд в деякі основи телефонного зв'язку допоможе нам зрозуміти технології як FDM так і TDM. Звичайно, різні частини світу використовують різні системи. Ми зосередимося тільки на системі, що використовується в Північній Америці. Північно-американська телефонна система включає багато **загальних носіїв**, що надають локальні і віддалені послуги абонентам. Ці носії включають локальні компанії, як наприклад Pacific Bell і віддалені постачальники, як наприклад AT&T, MCI, і Sprint (див. рис. 8.19).

Figure 8.19 Telephone network

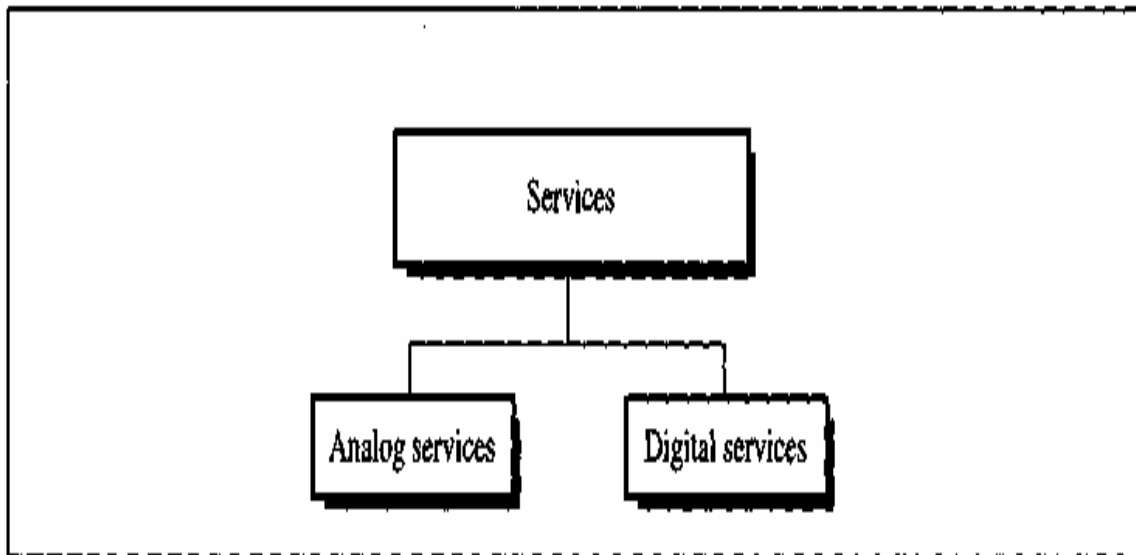


Загальні Сервіси Носіїв і Ієрархія

Телефонні компанії розпочалися із забезпечення їх абонентів аналоговими послугами, які використовували аналогові мережі. Більш пізня технологія дозволила введення цифрових послуг і мереж. На сьогодні,

Американські провайдери півночі перебувають в процесі зміни їх службових ліній від аналогових до цифрових. Передбачають, що незабаром вся мережа буде цифрова. Зараз, проте, обидва види послуг доступні - як FDM так і TDM знаходяться у використанні (див. рис. 8.20).

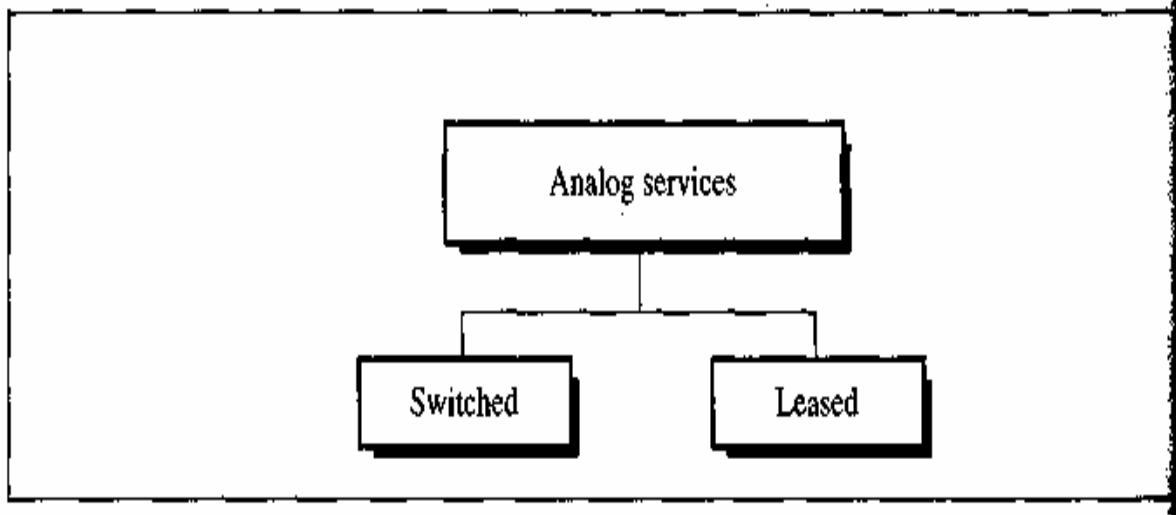
Figure 8.20 *Categories of telephone services*



Аналогові Послуги

З Багатьох аналогових послуг, доступних абонентам, є два які будуть тут обговорюватись: послуги переключення і послуги аренди (див. рис. 8.21)

Figure 8.21 *Categories of analog services*

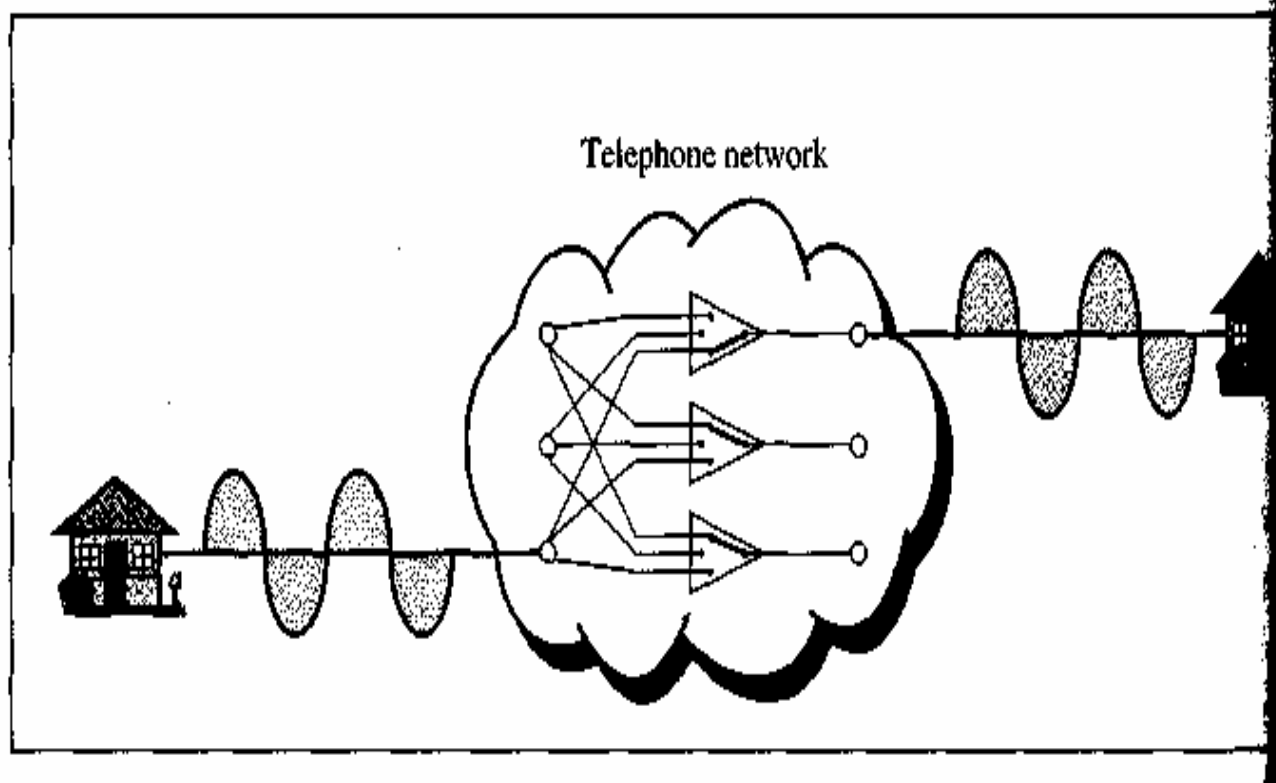


Сервіс Аналогового переключення

Сервіс Аналогового переключення - це комутований сервіс, що найбільш близький до dial-up і використовує домашній телефон. Він використовує двох-дротовий (чи спеціальний, чотирьох-дротовий) кабель, щоб з'єднати абонента з мережею з можливістю зворотного обміну. Такий зв'язок називається локальним циклом. Така мережа називається, private switched telephone network (PSTN). Сигнал на локальному циклі є аналоговим, і смуга пропускання є звичайно в діапазоні 4000 Гц.

З комутованими лініями, коли користувач набирає номер, виклик декілька разів перемикається, за обміном. Відповідні перемикачі очікують, щоб пов'язати лінію з тою особою, що викликається. Перемикач з'єднує дві лінії протягом виклику (див. рис. 8.22).

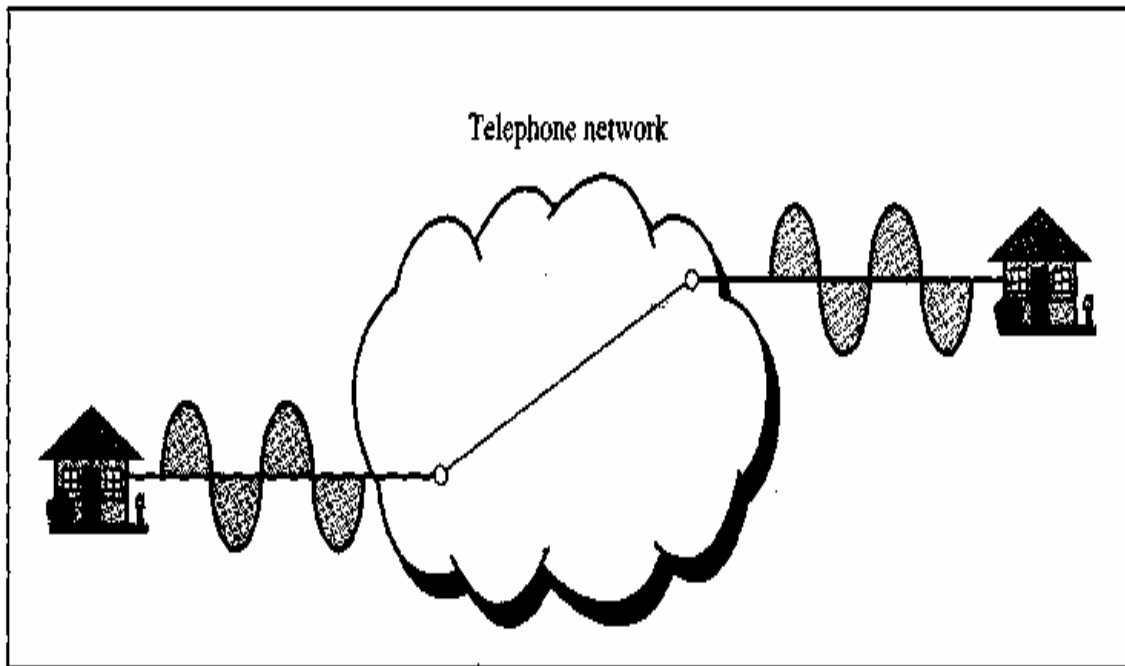
Figure 8.22 *Analog switched service*



Сервіс Аналогового Арендування

Сервіс Аналогового Арендування пропонує замовникам можливість арендувати лінію, яка постійно з'єднується з іншим замовником. Зв'язок також ще проходить через перемикачі в телефонній мережі, які є єдиною лінією, тому що перемикач завжди закритий; ніякий набір номера не потрібен (див. рис. 8.23).

Figure 8.23 *Analog leased service*



Аналогова Ієрархія

Щоб збільшити ефективність їх інфраструктури, телефонні компанії мають традиційні мультиплексні сигнали від більш низьких смуг пропускання на вищі смуги пропускання. В цьому випадку, багато комутованих або арендованих ліній можуть об'єднуватися в вузчі, але більші канали. Для аналогових ліній використовується FDM.

Одна з цих ієрархічних систем використовуються в AT&T, і створена із груп, супергруп, головних груп, і гігантських груп (див. рис. 8.24).

В цій аналоговій ієрархії, 12 голосових каналів мультиплекуються на вищу смугу пропускання, щоб створити групу. (Щоб законсервувати смугу

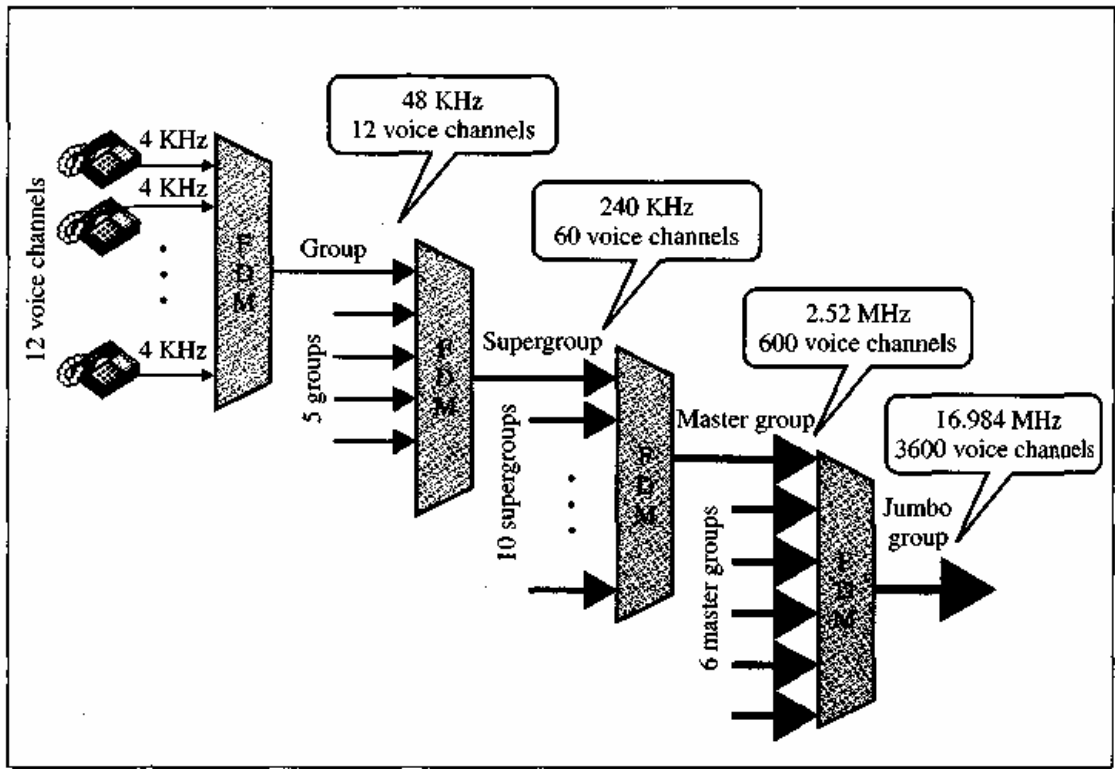
пропускання, АТ&Т використовує устаткування модуляції, які подавляють носій і відновлюють їх потім на демультимплексуванні). Група має 48 КHz смугу пропускання і підтримує 12 каналів голосу.

В наступному рівні, аж до п'яти груп може бути мультимплексовані, щоб створити складовий сигнал під назвою супергрупа. Супергрупа має смугу пропускання 240 КHz і підтримує аж до 60 каналів голосу. Супергрупи можуть бути зроблені або п'яти груп, або 60 незалежних каналів голосу.

В наступному рівні, 10 супергруп мультимплексується, щоб створити головну групу. Головна група повинна мати 2.40 мГц смугу пропускання, але потреба сторожових потоків між каналами збільшує необхідну смугу пропускання до 2.52 мГц. Головні групи підтримують аж до 600 каналів голосу.

Остаточо, шість головних груп можуть об'єднуватися в гігантській групі. Гігантська група повинна мати 15.12 мГц (6 мГц x 2.52), але збільшена до 16.984 мГц, щоб дозволити сторожові потоки між головними групами.

Figure 8.24 Analog hierarchy



Цифрові Послуги

Недавно телефонні компанії почали пропозицію цифрових послуг їх абонентам. Однією перевагою є те, що цифрові послуги менш чутливі, ніж аналогові послуги, до шуму і інших форм завад. Телефонна лінія діє подібно антені і збиратиме як під час аналогової, так і під час цифрової передачі завади. В аналогових передачах, як сигнал так і завади аналогові і не можливо їх легко відділити. В цифровій передачі, з іншого боку, є цифровий сигнал даних, але інтерфейс ще аналоговий.

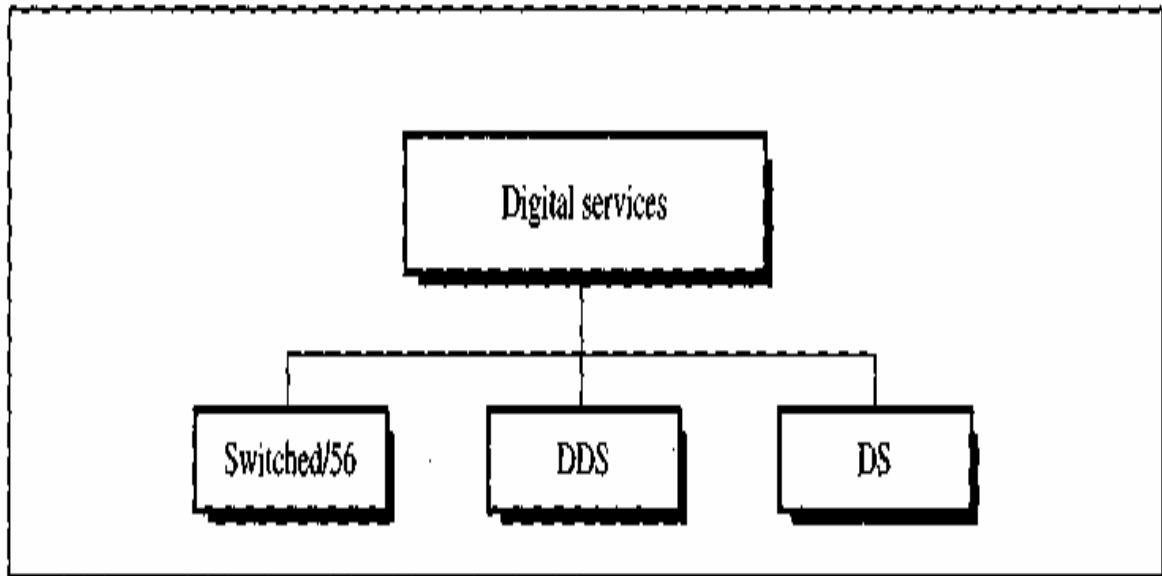
Сигнал таким чином може бути відділений легко. Інша перевага цифрової передачі - це нижча вартість. Це тому, що потрібно диференціювати тільки два або три рівні напруги замість безперервного діапазону значень, отже цифрова електроніка менш витратна ніж відповідне аналогове устаткування.

Ми розглянемо три різні види цифрових послуг: switched/56, DDS, and DS (див. рис. 8.25).

Сервіс Switched/56

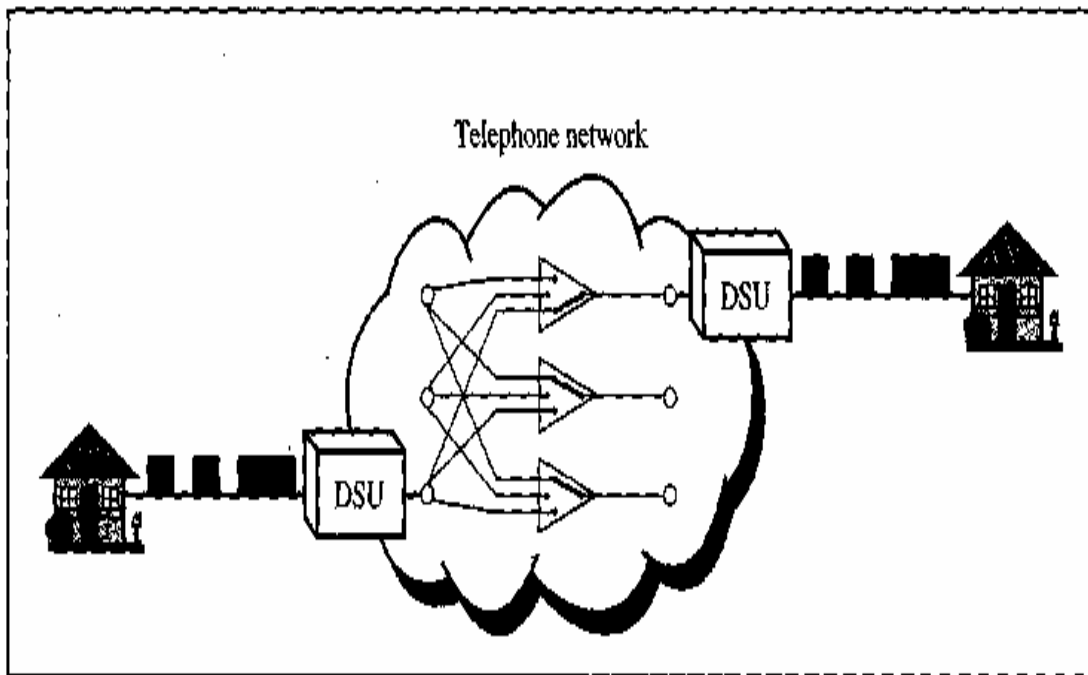
Switched/56 є цифровою версією комутованої лінії аналога. Це - переключений цифровий сервіс, який дозволяє швидкість передачі даних аж до 56 Kbps. Щоб спілкуватися через цей сервіс, обидві сторони повинні підписатися. Відвідувач з нормальною телефонною службою не може з'єднуватися з телефоном або комп'ютером із switched/56, навіть якщо використовує модем.

Figure 8.25 *Categories of digital services*



Оскільки лінія в сервісі switched/56 вже цифрова, абонентам не потрібні модеми, щоб передати цифрові дані. Проте, вони роблять потребу в іншому пристрої під назвою **цифрова службова одиниця (DSU)**. Цей пристрій змінює норму цифрових даних, створених пристроєм абонента до 56 Kbps, і кодує їх у форматі, що використовується постачальником послуги (див. рис. 8.26). DSU часто входить в процес набору номера (DSU з номеронабирачем).

Figure 8.26 *Switched/56 service*

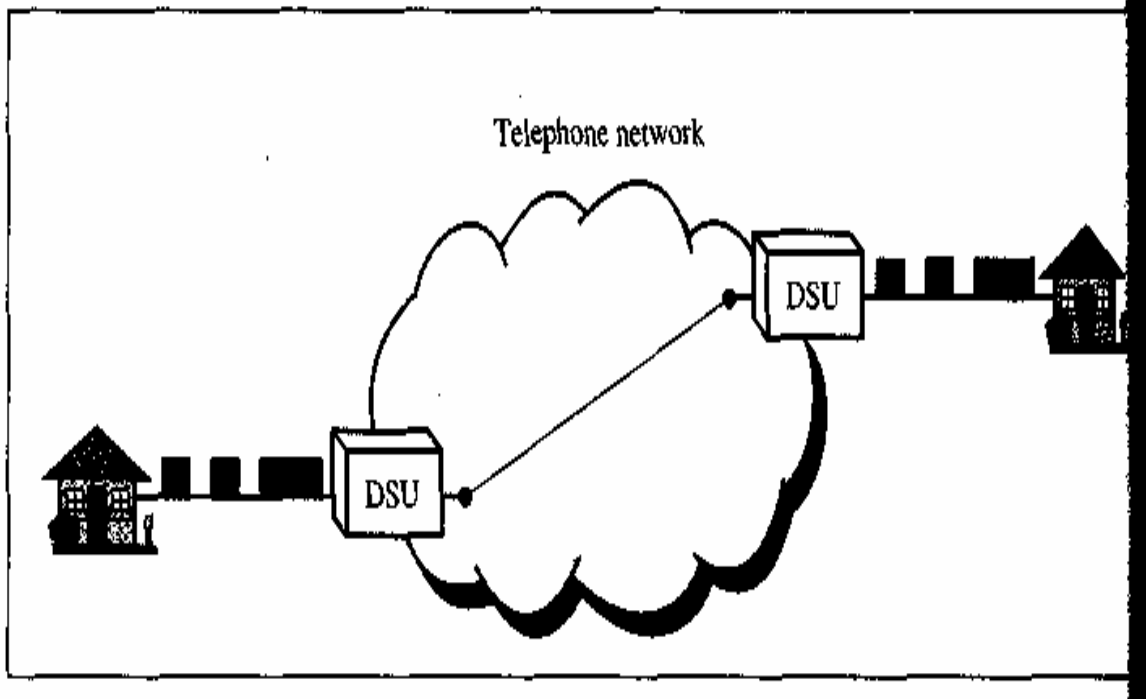


Сервіс Цифрових Даних (DDS)

Сервіс цифрових даних (DDS)- це цифрова версія аналогової арендованої лінії; це є цифрова арендована лінія з максимальною швидкістю передачі даних 64 Kbps.

Подібно switched/56, DDS вимагає використання DSU. DSU для цього сервісу дешевше, ніж вимагається для switched/56, тому що не потрібна подушка набору(див. рис. 8.27).

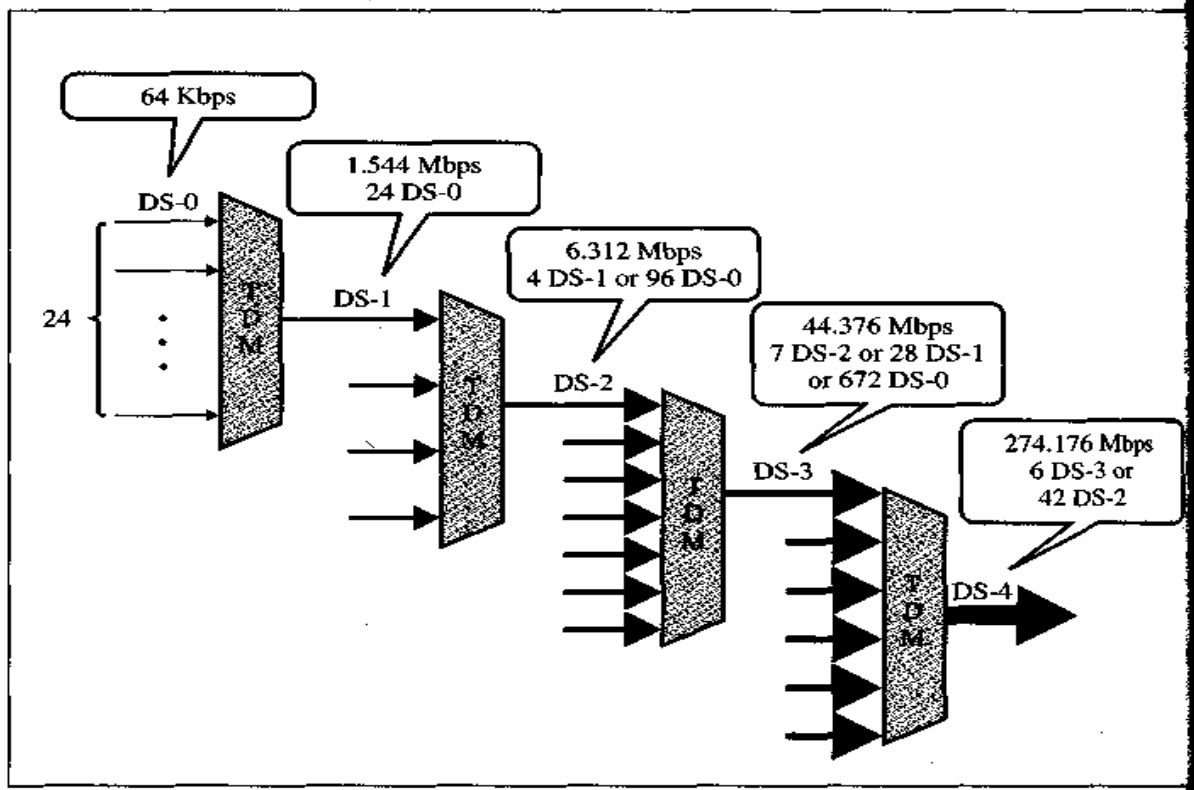
Figure 8.27 *DDS service*



Сервіс Цифрового Сигналу Даних (DS)

Після послуг switched/56 і DDS, телефонні компанії потребували розвитку ієрархії цифрових послуг подібно тому, що використовується для аналогових послуг. Він був **сервісом цифрового сигналу (DS) даних**. DS є ієрархією цифрових сигналів даних. Рисунок 8.28 показує швидкості передачі даних, підтримувані кожним рівнем.

Figure 8.28 DS hierarchy



Сервіс DS-0 має схожість DDS. Це є єдиний цифровий канал 64 Kbps.

DS-1 є сервісом 1.544-Mbps; 1.544 Mbps складає 24 разів 64 Kbps плюс 8 Kbps. Він може використовуватися як єдиний сервіс для передачі 1.544-Mbps, або до 24 мультіплексних каналів DS-0, або нести будь-яку іншу комбінацію, бажану для користувача, в межах 1.544-Mbps.

DS-2 є сервісом 6.312-Mbps; 6.312 Mbps складає 96 разів 64 Kbps плюс 168 Kbps. Він може використовуватися як єдиний сервіс для передачі 6.312-Mbps, або до 4 мультіплексних каналів DS-1, 96 каналів DS-0, або комбінації цих типів сервісів.

DS-3 є сервісом 44.376-Mbps; 44.376 Mbps складає 672 разів 64 Kbps плюс 1.368 Mbps. Може використовуватися як єдиний сервіс для передачі 44.376-Mbps, або до 7 мультіплексних каналів DS-2, 28 каналів DS-1 channels, 672 DS-0, або комбінації цих службових типів.

DS-4 є сервісом 274.176-Mbps; 274.176 складає 4032 разів 64 Kbps плюс 16.128 Mbps надлишкової інформації. Це може бути до 6 мультиплексних каналів DS-3, 42 каналів DS-2 channels, 168 DS-1, 4032 каналів DS-0, або комбінації цих службових типів.

Лінії T

DS-0, DS-1, і так далі є назвами послуг. Щоб виконувати ті послуги, телефонні компанії використовують **лінії T** (T-1 до T-4). Це є лінії з місткостями, які точно відповідають до швидкостей передач даних DS-1 до послуг DS-4 (див. табл. 8.1).

Table 8.1 *DS and T line rates*

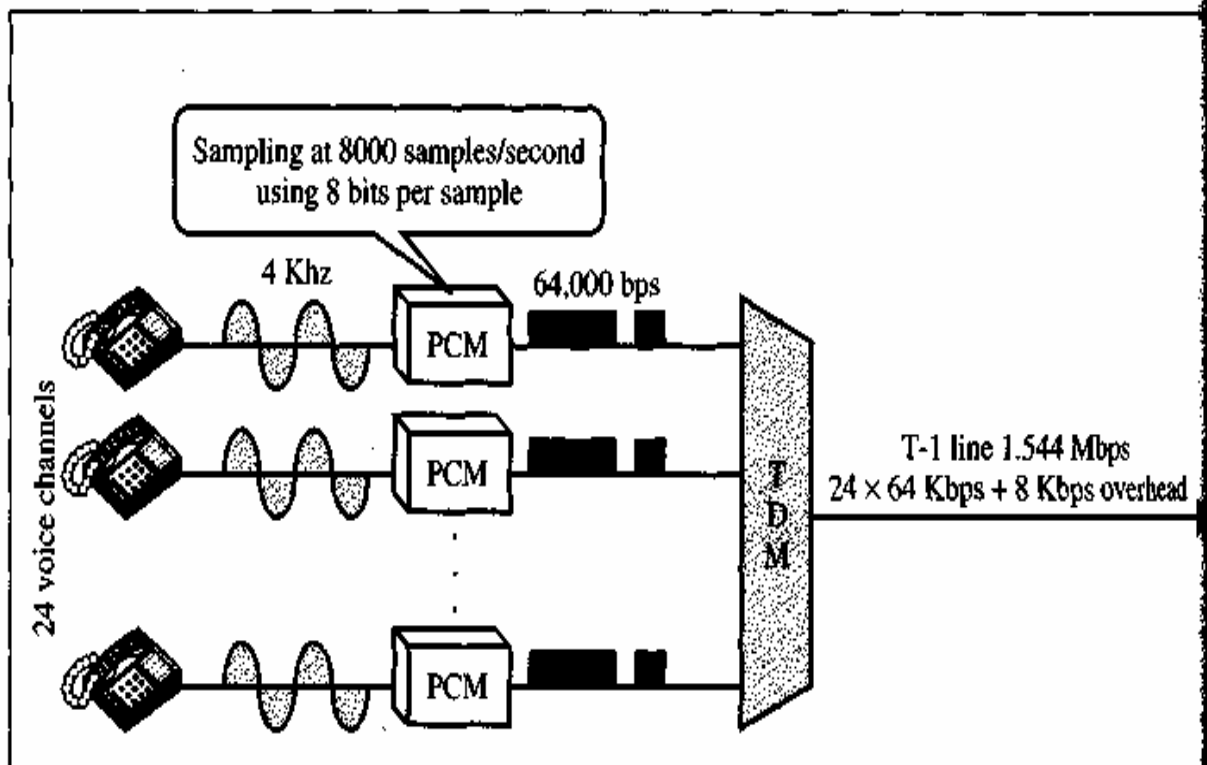
<i>Service</i>	<i>Line</i>	<i>Rate (Mbps)</i>	<i>Voice Channels</i>
DS-1	T-1	1.544	24
DS-2	T-2	6.312	96
DS-3	T-3	44.736	672
DS-4	T-4	274.176	4032

T-1 використовується, щоб виконувати DS-1, T-2 використовується, щоб виконувати DS-2, і так далі. Як бачите з Таблиці 1.1, DS-0 не є фактично запропонованим як сервіс, але він визначений як основа для довідки. Телефонні компанії вірять, що замовнику потрібен рівень сервісу, який може бути знайдений в DS-0, можуть замінити DDS.

Лінії Т для Аналогової передачі Т-лінії - це цифрові лінії, розроблені для передачі цифрових даних, голосу, або звукових сигналів. Проте, вони також можуть використовуватися для аналогової передачі (регулярні телефонні зв'язки).

Можливість використання ліній Т як аналогових носіїв відкрила нове покоління послуг для телефонних компаній. Раніше, коли організація хотіла 24 окремі телефонні лінії, було потрібно проводити 24 парних кабелів від компанії до центрального пункту. Сьогодні така ж організація може об'єднати 24 лінії в одній лінії Т-1 і виконати тільки лінію Т-1 до пункту. Рис. 8.29 показує, як 24 канали голосу можуть бути мультиплексовані на одну лінію Т-1.

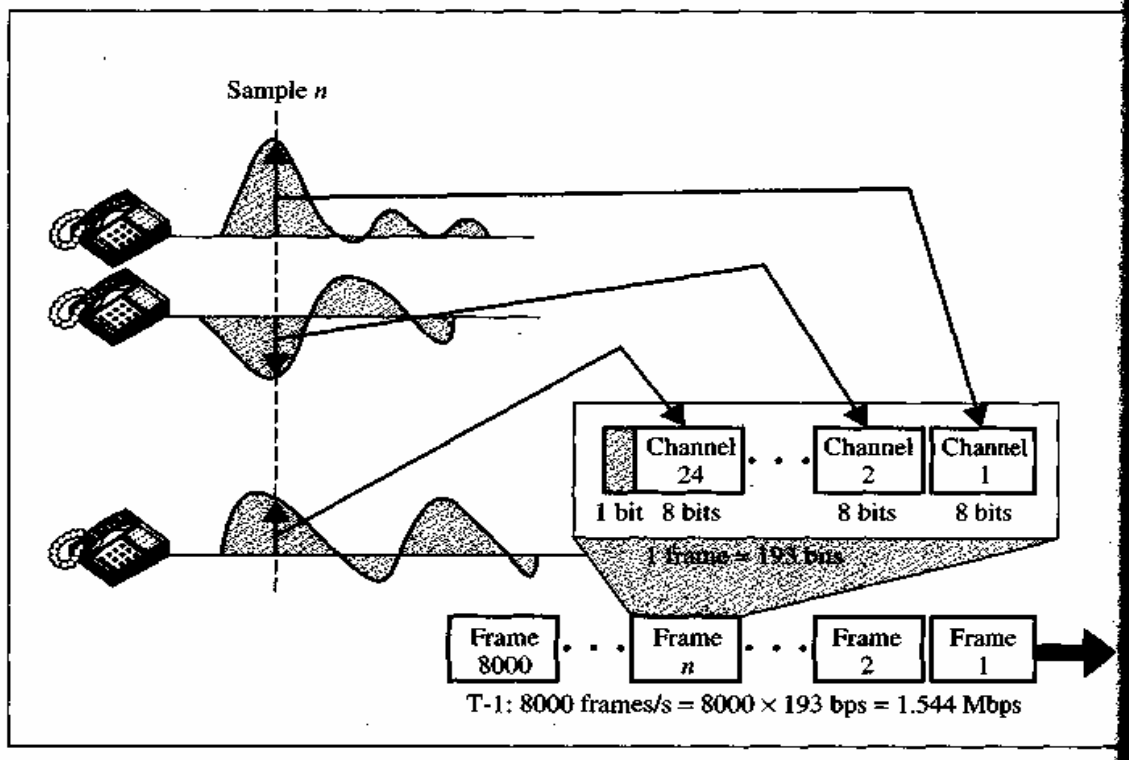
Figure 8.29 T-1 line for multiplexing telephone lines



Фрейм Т-1. Як зазначалось вище, DS-1 вимагає 8 Кbps надлишкової інформації. Щоб зрозуміти як порахувати кількість надлишкової інформації, ми повинні розглянути формат 24-голосового фрейму В.

Фрейм, що використовується на лінії T-1, - це звичайно 193 біти, що діляться на 24 слоти кожен 8 біт плюс 1 додатковий біт для синхронізації ($24 \times 8 + 1 = 193$); подивіться Рисунок 8.30. В іншому випадку кожен слот містить 1 сигнальний сегмент від кожного каналу; 24 сегменти - це фрейм перешарування. Якщо лінія T-1 несе 8000 фреймів за секунду, швидкість передачі даних - 1.544 MtB ($193 \times 8000 = 1.544 \text{ Mbps}$) – місткість лінії.

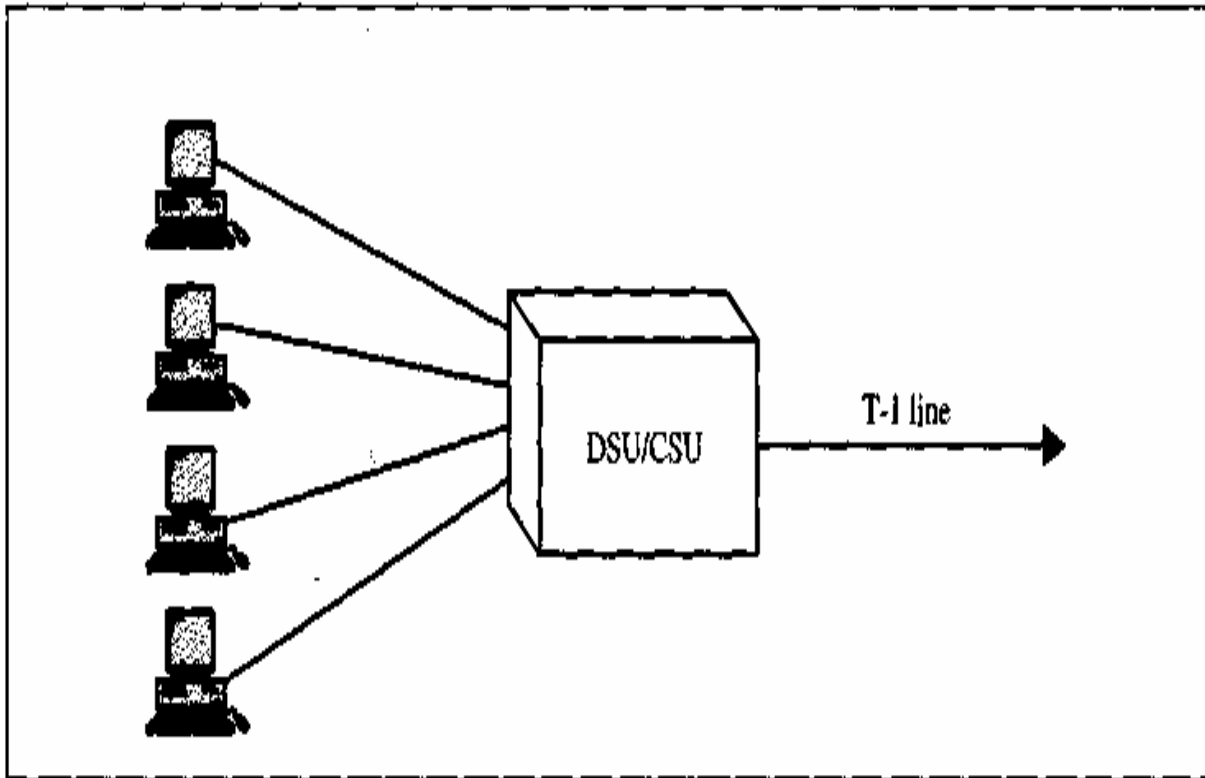
Figure 8.30 T-1 frame structure



Фракційні Лінії Т. Багатьом абонентам може не бути потрібна повна місткість лінії Т. Щоб пристосувати цих замовників, телефонні компанії розробили Фракційні послуги лінії Т, які дозволяють окремим абонентам відкрити одну лінію мультиплексуванням для передачі.

Наприклад, малому бізнесу може бути потрібно тільки четверта частина місткості лінії T-1. Для цього можна направити передачу через пристрій під назвою **цифрова одиниця сервісу/кальняльна одиниця сервісу (DSU/CSU)**. Цей пристрій дозволяє поділити місткість лінії на чотири перешаровані канали (див. рис. 8.31).

Figure 8.31 *Fractional T-1 line*



Лінії E

Європейці використовують версію ліній T під назвою **лінії E**. Дві системи візуально ідентичні, але їх місткості відрізняються. Таблиця 1.2 показує лінії E і їх місткості.

Table 8.2 *E line rates*

<i>Line</i>	<i>Rate (Mbps)</i>	<i>Voice Channels</i>
E-1	2.048	30
E-2	8.448	120
E-3	34.368	480
E-4	139.264	1920

Цифрова абонентська лінія (DSL)

Приклади мультиплексування, демультіплексування, і модуляція - це сім'я DSL технологій. Цифрова лінія (DSL) абонента - це більш нова технологія, що використовує існуючі мережі телекомунікацій, як наприклад локальна телефонна лінія для передачі даних, голосу, відео, і мультимедіа.

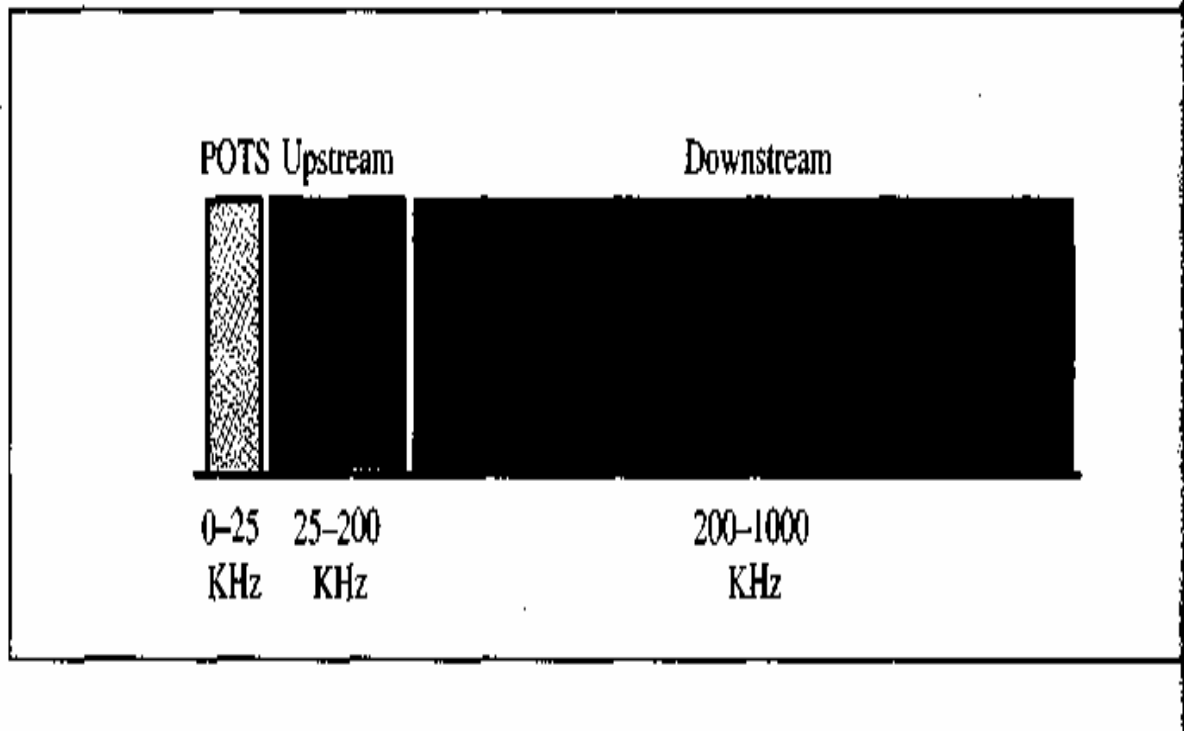
DSL є сім'єю технологій; п'ять з них обговорюватиметься тут: AMRADSL, HDSL, VDSL, і SDSL.

ADSL

Телефонні компанії встановили швидкохідні цифрові широкі мережі для зв'язку між їх центральними офісами. **Асиметрична абонентська цифрова лінія (ADSL)** несиметрична, що дозволяє використовувати вищі швидкості передачі даних в бітах в напрямі за течією (від телефонного центрального офісу до вузла абонента), ніж проти течії напрям (від вузла абонента до центрального офісу). Вони хочуть до швидко одержувати файли з Інтернету, але вони звичайно мають малі файли, як наприклад - поштове повідомлення, для відправки.

ADSL ділить смугу пропускання витої пари (один мегагерц) на t М полос. Перша полоса, між 0 і 25 КHz, використовується для регулярного телесервісу (відомого як стара телефонна служба). Друга полоса, звичайно між 25 і 200 КHz, - це комунікація, що використовує потокове з'єднання. Третя полоса, звичайно 200 КHz до 1 мгц, - це комунікація використовує завантаження. Деякі реалізації частково перекривають вихідний потік upstream, щоб забезпечити більшу смугу пропускання в напрямі за течією. Рис. 8.32 показує полоси.

Figure 8.32 Bands for ADSL



Устаткування Модуляції

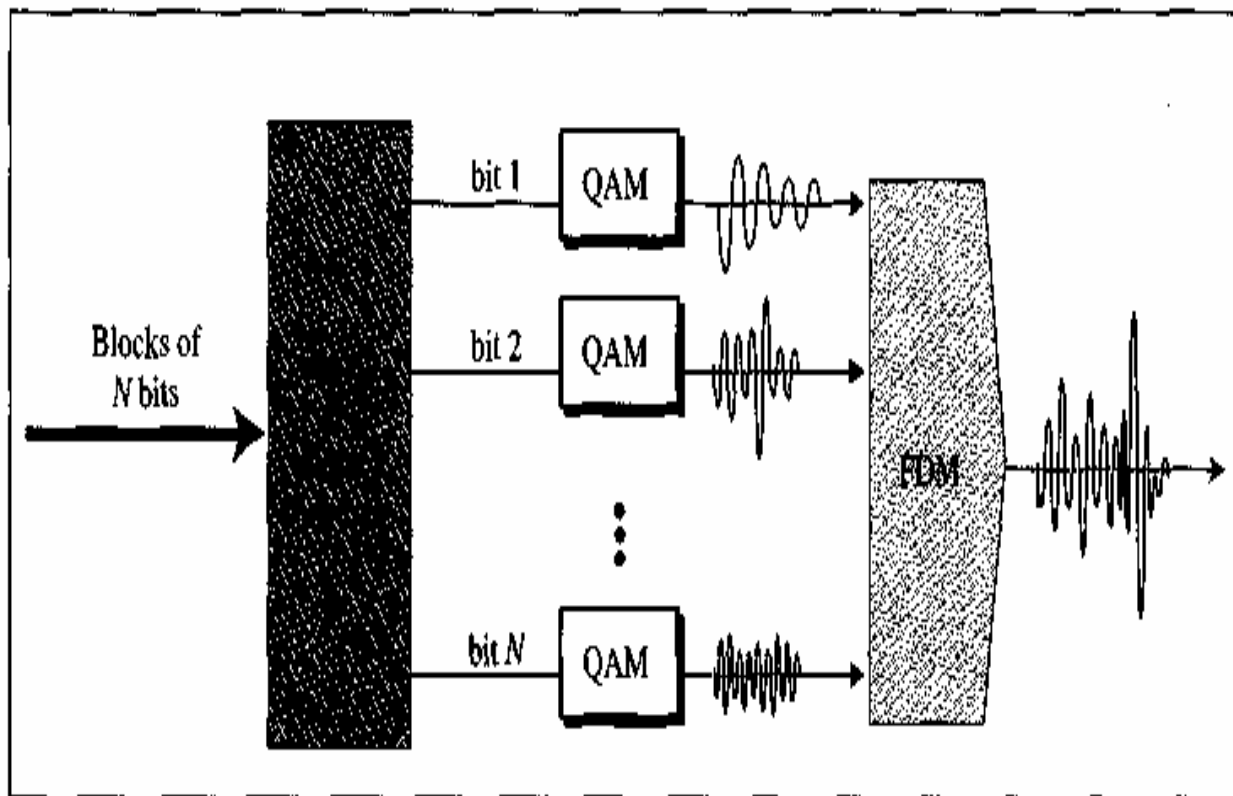
Більшість реалізацій ADSL оригінально використовувала техніку модуляції яка називається carrier-less amplitude/phase (CAP). Пізніше, інша техніка модуляції, відома як дискретний багатотон (discrete multitone) (DMT) була стандартизована ANSI.

BCAP Carrierless amplitude/phase (CAP) - це техніка модуляції, яка подібна QAM, але з однією важливою різницею: сигнал носія виключений. Техніка, проте, більш комплексна, ніж QAM і не стандартизувалася.

DMT The discrete multitone technique (DMT) об'єднує QAM і FDM. Доступна смуга пропускання для кожного напрямку ділиться на канали 4-KHz, кожний має власну частоту носія.

Рис. 8.33 показує поняття DMT з каналами N . Біти, створені джерелом, пройдені через послідовно-паралельний конвертор, де блок бітів N ділиться на паралельні шляхи A , кожен складанється з одного біта. Сигнали QAM, створені з кожного шляху, частотно мультиплекуються разом і результат відправляється в лінію.

Figure 8.33 DMT



Стандарт ANSI визначає норму 60 Kbps для кожного каналу 4-KHz, який означає модуляцію QAM з 15 бітами за бод.

Розташований вгору за течією канал звичайно займає 25 каналів, з бітовою частотою 25×60 Kbps, або 1.5 Mbps. Звичайно, швидкість передачі в бітах в цьому діапазоні змінюється від 64 Kbps до 1 Mbps через шуми.

За течією канал звичайно займає 200 каналів, з бітовою частотою 200×60 Kbps, або 12 Mbps. Звичайно, швидкість передачі в бітах в цьому діапазоні змінюється від 500 Kbps до 8 Mbps через шуми.

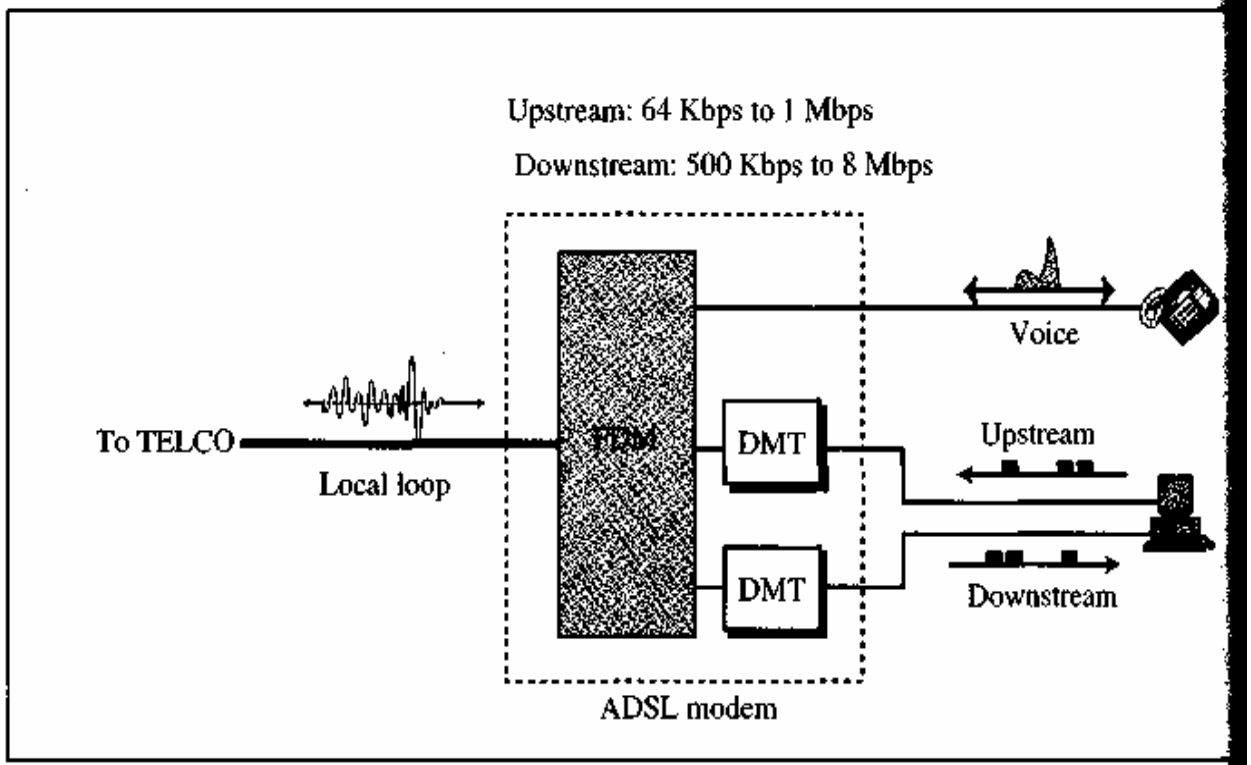
Рисунок 8.34 показує ADSL і швидкості передачі в бітах в кожному напрямі.

RADSL

Адаптивна несиметрична цифрова лінія (RADSL) абонента (rate adaptive asymmetrical digital subscriber line)- це технологія, заснована на ADSL. Вона дозволяє різні швидкості передачі даних залежно від виду комунікації:

- Голос;
- Дані;
- Мультимедіа
- і так далі.

Figure 8.34 *ADSL modem*



HDSL

The high bit rate digital subscriber line (HDSL) була розроблена Bellcore (тепер Ncordia) як альтернатива до лінії T-1 (1.544 Mbps). Використання лінії T-1 AMI дуже сприйнятливим до виснаження у високих частотах. Це обмежує лінію lengthBT-1 до 1 Км. Для міжміських зв'язків необхідний підсилувач.

Швидкість передачі даних майже 2 Mbps може досягатися без повторювачів на відстані аж до 0.6 км. HDSL використовує дві виті пари, щоб досягти дуплексної передачі.

SDSL

Симетрична (або єдина лінія) цифрова лінія (SDSL) абонента є такою ж, як HDSL але використовує одну єдину виту-пару, доступну до більшості

абонентів і досягає тієї ж швидкості передачі даних як HDSL. Техніка *під назвою ануляція* створює дуплексну передачу.

VDSL

Надвисокошвидкісна цифрова абонентська лінія (The very high bit rate digital subscriber line), альтернативний підхід до подібного ADSL, використовує коаксіальний, оптичний кабель, або виту пару для коротких дистанцій до 1800 метрів). Техніка модуляції є DMT з бітовою швидкістю від 50 до 55 М вхідного потоку і від 1.5 до 2.5 Mbps вихідного.

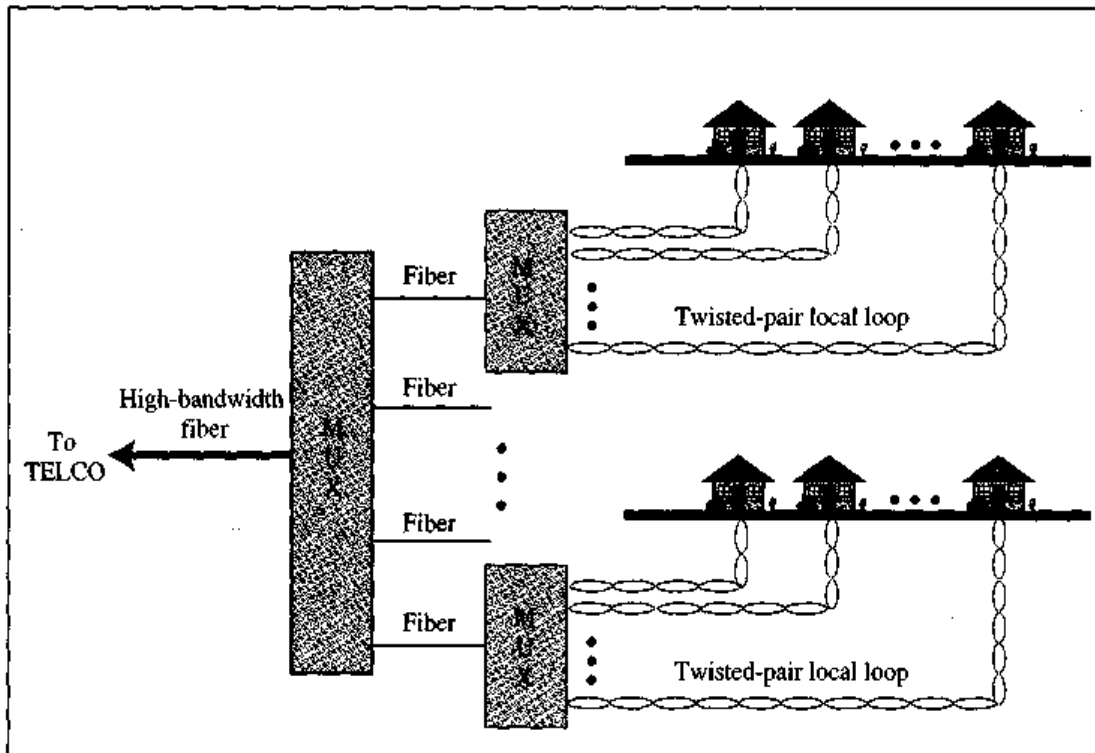
FTTC

Оптичне волокно має багато переваг, серед них опір шуму і висока місткість смуги пропускання. Проте, порівняють з іншими видами кабелю, це дуже дороге. Телефон і компанії кабельного ТБ придумали метод, названий **fiber to the curb** (FTTC), щоб зменшити витрати. Оптичне волокно прокладається від центрального офісу телефонної компанії або від головного офісу кабельної компанії до вузла. Від вузла до абонента - це менш дорога вита-пара або коаксіальний кабель.

FTTC в Телефонній Мережі

Телефонна система використовує оптичні кабелі для зв'язку і мультиплексування різних каналів голосу. Мідна вита пара, що приєднується від абонентів, мультиплексується в блоках з'єднання і перетворюються на оптичні сигнали. Оптичні сигнали в місці переключення мультиплексуються, використовуювання WDM, щоб створити більш широкі оптичні сигнали смугу пропускання для оптичних сигналів (рис. 8.35).

Figure 8.35 FTTC in the telephone network

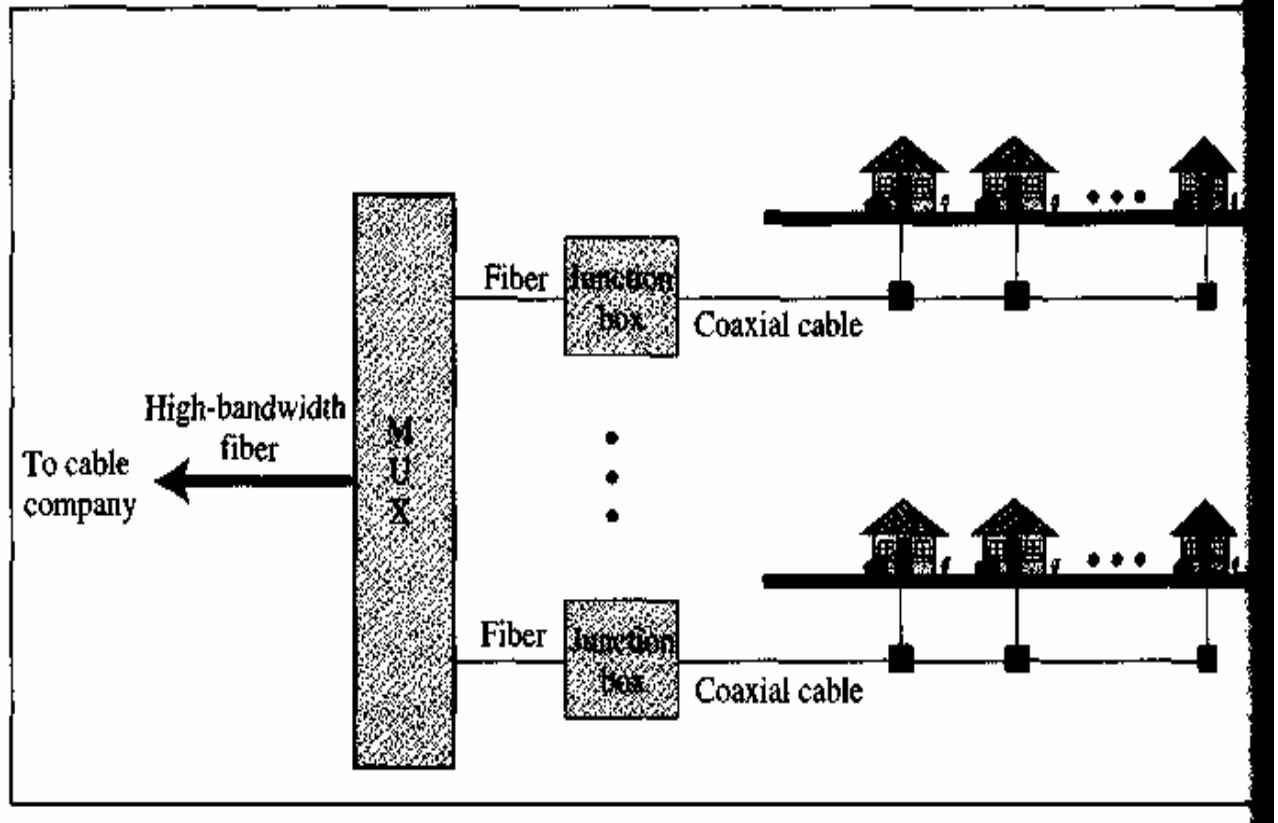


112

ТТС в Мережі Кабельного ТБ

Система кабельного ТБ використовує оптичні кабелі для з'єднання і мультиплексування різних кабельних каналів. Коаксіальні кабелі, що прибувають від індивідуальних абонентів, мультиплексуються в блоках з'єднання і перетворюються на оптичні сигнали. Оптичні сигнали в місці переключення мультиплексуються, використовуючи WDM, щоб створити більш широкі оптичні сигнали смуги пропускання (див. рис. 8.36).

Figure 8.36 FTTC in the cable TV network



Тема 9: Організація рівня передачі даних і виявлення/корекція помилок

9.1. Ключові аспекти організації передачі даних

9.1.1 Функції і структура кадру

9.1.2 Сервіси для мережевого рівня

9.1.3 Формування кадру

9.1.4 Обробка помилок

9.1.5 Управління потоком

9.2. Виявлення і корекція помилок

9.2.1 Типи помилок

9.2.2 Методи виявлення помилок

9.2.3 Корекція помилок

9.1. Ключові аспекти організації передачі даних

9.1.1 Функції і структура кадру

Рівень передачі даних повинен виконувати ряд специфічних функцій. До них відносяться:

- забезпечення строго обкресленого службового інтерфейсу для мережного рівня;
- обробка помилок передачі даних;
- управління потоком даних, затоплення повільних приймачів швидкими передавачами, що виключає.

Для цих цілей канальний рівень бере пакети, отримані з мережного рівня, і вставляє їх в спеціальні кадри для передачі. В кожному кадрі міститься заголовок, поле даних і кінцевик. Структура кадру показана на рис. 3.1. Управління кадрами – це основа діяльності рівня передачі даних. В наступних розділах ми більш детально вивчимо позначені вище питання.

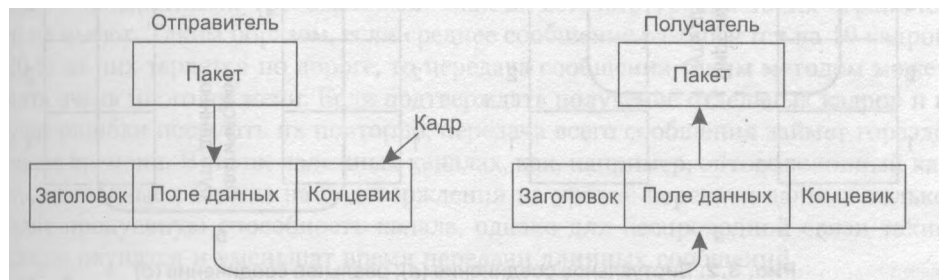


Рис. 1. Взаємодія між пакетами і кадрами

Хоча цей розділ і присвячена детальному розгляду рівня передачі даних і відповідних протоколів, багато питань, обговорюваних тут, такі як контроль помилок і контроль потоку, відносяться також до транспортних і інших протоколів. Насправді, в багатьох мережах ці функції є прерогативою верхніх рівнів і взагалі не відносяться до рівня передачі даних. З другого боку, не так вже це важливо, тому що основні принципи все одно залишаються незмінними. Аргументом на користь розгляду їх саме в світлі рівня передачі даних є те, що тут вони предстають в найпростішій формі і їх легко показати в деталях.

9.1.2 Сервіси для мережевого рівня

Задача рівня передачі даних полягає в наданні сервісів мережному рівню. Основним сервісом є передача даних від мережного рівня передаючої машини мережному рівню приймаючої машини. На передаючій машині працює процес, який передає біти з мережного рівня на рівень передачі даних для передачі їх за призначенням. Робота рівня передачі даних полягає в передачі цих бітів на приймаючу машину так, щоб вони могли бути передані мережному рівню приймаючої машини, як показано на рис. 3.2, а. Насправді дані передаються по шляху, показаному на рис. 3.2, б, проте простіше уявляти собі два рівні передачі даних, що зв'язуються один з одним за допомогою протоколу передачі даних. З цієї причини протягом цього розділу використовуватиметься модель, зображена на рис. 3.2, а.

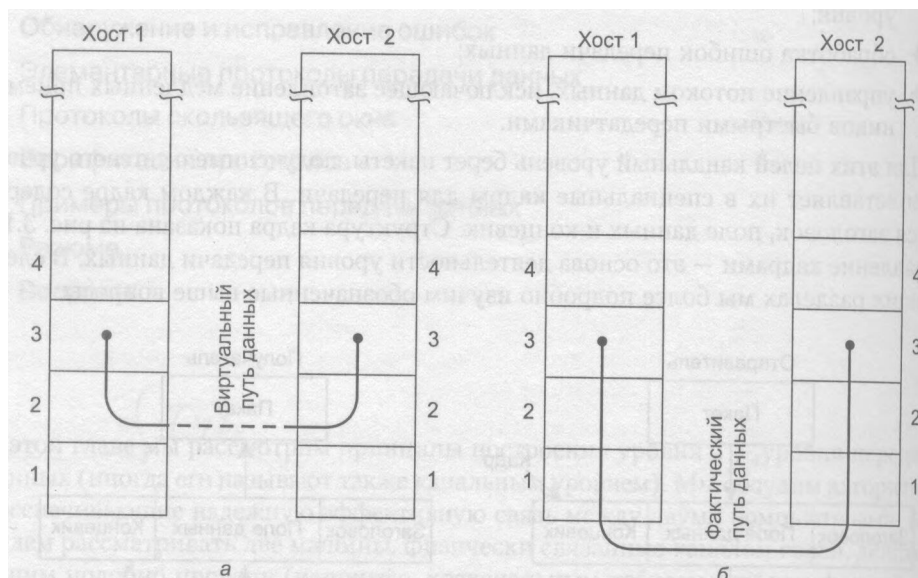


Рис. 2. Віртуальне з'єднання (а); реальне з'єднання (б)

Рівень передачі даних може надавати різні сервіси. Їх набір може бути різним в різних системах. Звичайно можливі наступні варіанти.

1. Сервіс без підтверджень, без установки з'єднання.
2. Сервіс з підтвердженнями, без установки з'єднання.
3. Сервіс з підтвердженнями, орієнтована на з'єднання.

Розглянемо ці варіанти по черзі.

Сервіс без підтверджень і без установки з'єднання полягає в тому, що передаюча машина посилає незалежні кадри приймаючій машині, а приймаюча машина не посилає підтверджень про прийом кадрів. Ніякі з'єднання наперед не встановлюються і не розриваються після передачі кадрів. Якщо який-небудь кадр втрачається через шум в лінії, то на рівні передачі даних не робиться ніяких спроб відновити його. Даний клас сервісів прийнятний при дуже низькому рівні помилок. В цьому випадку питання, пов'язані з відновленням втрачених при передачі даних, можуть бути залишені верхнім рівням. Він також застосовується в лініях зв'язку реального часу, таких як передача мови, в яких краще отримати спотворені дані, ніж отримати їх з великою затримкою. Сервіс без підтверджень і без установки з'єднання використовується в рівні передачі даних в більшості локальних мереж.

Наступним кроком у бік підвищення надійності є сервіс з підтвердженнями, без установки з'єднання. При його використуванні з'єднання також не встановлюється, але отримання кожного кадру підтверджується. Таким чином, відправник знає, чи дійшов кадр до пункту призначення в цілості. Якщо протягом встановленого інтервалу часу підтвердження не поступає, кадр посилається знову. Така служба корисна у разі використування каналів з великою вірогідністю помилок, наприклад, в безпроводних системах.

Слід зазначити, що надання підтверджень є швидше оптимізацією, ніж вимогою. Мережний рівень завжди може послати пакет і чекати підтвердження його доставки. Якщо за встановлений період часу підтвердження не буде отримано відправником, повідомлення може бути вислано ще раз. Проблема при використуванні даної стратегії полягає в тому, що кадри звичайно мають жорстке обмеження максимальної довжини, пов'язане з апаратними вимогами. Пакетів мережного рівня таких обмежень не мають. Таким чином, якщо середнє повідомлення розбивається на 10 кадрів і 20 % з них втрачається по дорозі, то передача повідомлення таким методом може зайняти дуже багато часу. Якщо підтверджувати отримання окремих кадрів і у разі помилки посилати їх повторно, передача всього повідомлення займе набагато менше

часу. В таких надійних каналах, як, наприклад, оптоволоконний кабель, невідгідні витрати на підтвердження на рівні передачі даних тільки пропускну спроможність каналу, проте для безпроводного зв'язку такі витрати окупляться і зменшать час передачі довгих повідомлень.

Найскладнішим сервісом, який може надавати рівень передачі даних, є орієнтована на з'єднання служба з підтвердженнями. При використуванні даного методу джерело і приймач, перш ніж передати один одному дані, встановлюють з'єднання. Кожний посланий кадр нумерується, а каналний рівень гарантує, що кожний посланий кадр дійсно прийнятий на іншій стороні каналу зв'язку. Крім того, гарантується, що кожний кадр був прийнятий всього один раз і що всі кадри були отримані в правильному порядку. В службі без встановлення з'єднання, навпаки, можливо, що при втраті підтвердження один і той же кадр буде посланий кілька разів і, отже, кілька разів отриманий. Орієнтований на з'єднання сервіс надає процесам мережного рівня еквівалент надійного потоку бітів.

При використуванні орієнтованого на з'єднання сервісу передача даних складається з трьох різних фаз. В першій фазі встановлюється з'єднання, при цьому обидві сторони ініціалізували змінні і лічильники, необхідні для стеження за тим, які кадри вже прийняті, а які – ще ні. В другій фазі передаються кадри даних. Нарешті, в третій фазі з'єднання розривається і при цьому звільняються всі змінні, буфери і інші ресурси, що використалися під час з'єднання.

Розглянемо типовий приклад: глобальна мережа, що складається з маршрутизаторів, сполучених від вузла до вузла виділеними телефонними лініями. Коли кадр прибуває на маршрутизатор, апаратура перевіряє його на наявність помилок (за допомогою методу, який ми вивчимо трохи пізніше) і передає кадр програмному забезпеченню рівня передачі даних (яке може бути упроваджений в мікросхему мережної карти). Програма рівня передачі даних перевіряє, чи той це кадр, який очікувався, і якщо так, то передає пакет, що зберігається в полі корисного навантаження кадру, програмі маршрутизації. Програма маршрутизації вибирає потрібну лінію, що виходить, і передає пакет

назад програмі рівня передачі даних, який передає його далі по мережі. Проходження повідомлення через два маршрутизатори показано на рис. 3.3.

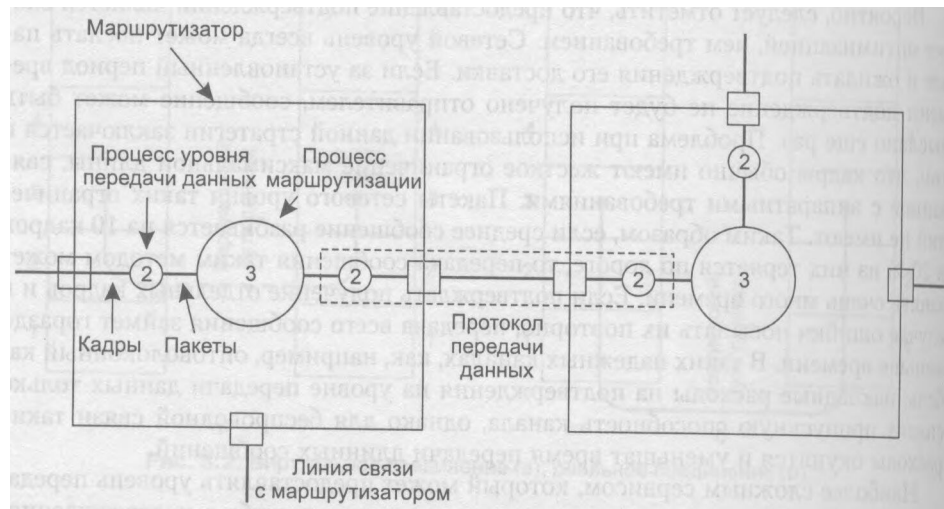


Рис. 3. Протокол передачі даних

Програми маршрутизації часто вимагають правильного виконання роботи, тобто їм потрібне надійне з'єднання з впорядкованими пакетами на всіх лініях, що сполучають маршрутизатори. Такі програми звичайно не люблять, якщо доводиться дуже часто турбуватися про втрачені пакети. Зробити ненадійні лінії надійними або хоча б досить хорошими – задача рівня передачі даних, показаного на малюнку пунктирним прямокутником. Хоча на малюнку показано декілька копій програми рівня передачі даних, насправді всі лінії зв'язку обслуговуються однією копією програми з різними таблицями і структурами даних для кожної лінії.

9.1.3 Формування кадру

Для надання сервісу мережному рівню рівень передачі даних повинен використовувати сервіси, що надаються йому фізичним рівнем. Фізичний рівень приймає необроблений потік бітів і намагається передати його за призначенням. Цей потік не застрахований від помилок. Кількість прийнятих біт може бути менше, рівно або більше числа переданих біт; крім того, значення прийнятих бітів можуть відрізнитися від значень переданих. Рівень передачі даних повинен знайти помилки і, якщо потрібно, виправити їх.

Звичайно рівень передачі даних розбиває потік бітів на окремі кадри і рахує для кожного кадру контрольну суму. (Алгоритми підрахунку контрольних сум обговорюватимуться далі в цьому розділі.) Коли кадр прибуває в пункт призначення, його контрольна сума підраховується знову. Якщо вона відрізняється від тієї, що міститься в кадрі, то рівень передачі даних розуміє, що при передачі кадру відбулася помилка, і вживає заходів (наприклад, ігнорує зіпсований кадр і посилає передаючій машині повідомлення про помилку).

Розбиття потоку бітів на окремі кадри є складнішою задачею, чим це може показатися на перший погляд. Один із способів розбиття на кадри полягає у вставці тимчасових інтервалів між кадрами, подібно тому, як вставляються пропуски між словами в тексті. Проте мережі рідко надають гарантії збереження тимчасових параметрів при передачі даних, тому можливо, що ці інтервали при передачі зникнуть або, навпаки, будуть додані нові інтервали.

Оскільки для відмітки початку і кінця кадру покладатися на тимчасові параметри дуже ризиковано, були розроблені інші методи. В даному розділі ми розглянемо чотири методи маркіровки меж кадрів.

1. Підрахунок кількості символів.
2. Використовування сигнальних байтів з символічним заповненням.
3. Використовування стартових і стопових бітів з бітовим заповненням.
4. Використовування заборонених сигналів фізичного рівня.

Перший метод формування кадрів використовує поле в заголовку для вказівки кількості символів в кадрі. Коли рівень передачі даних на приймаючому комп'ютері бачить це поле, він знає, скільки символів буде передано, і таким чином визначає, де знаходиться кінець кадру. Цей прийом проілюстрований на рис. 3.4, *а* для чотирьох кадрів розміром 5, 5, 8 і 8 символів відповідно.

Недолік такої системи в тому, що при передачі може бути спотворений сам лічильник. Наприклад, якщо розмір другого кадру з числа 5 стане через помилку в каналі числом 7, як показано на рис. 3.4, *б*, то приймаюча машина втратить синхронізацію і не зможе знайти початок наступного кадру. Навіть

якщо контрольна сума не співпаде (швидше за все) і приймаючий комп'ютер зрозуміє, що кадр прийнятий невірно, то він все одно не зможе визначити, де початок наступного кадру. Запрошувати повторну передачу кадру також марно, оскільки приймаючий комп'ютер не знає, скільки символів потрібно пропустити до початку повторної передачі. З цієї причини метод підрахунку символів тепер практично не застосовується.



Рис. 4. Потік символів: без помилок (а); з однією помилкою (б)

Другий метод формування кадрів вирішує проблему відновлення синхронізації після збою за допомогою маркіровки початку і кінця кожного кадру спеціальними байтами. У минулому стартові і стопові байти відрізнялися один від одного, але останнім часом більшість протоколів перейшла на використання в обох випадках одного і того ж байта, званого **прапором**. Це показано на рис. 3.5, а як FLAG. Таким чином, якщо приймач втрачає синхронізацію, йому необхідно просто знайти байт прапора, за допомогою якого він розпізнає кінець поточного кадру. Два байти сусідніх прапорів говорять про те, що кінчився один кадр і почався інший.

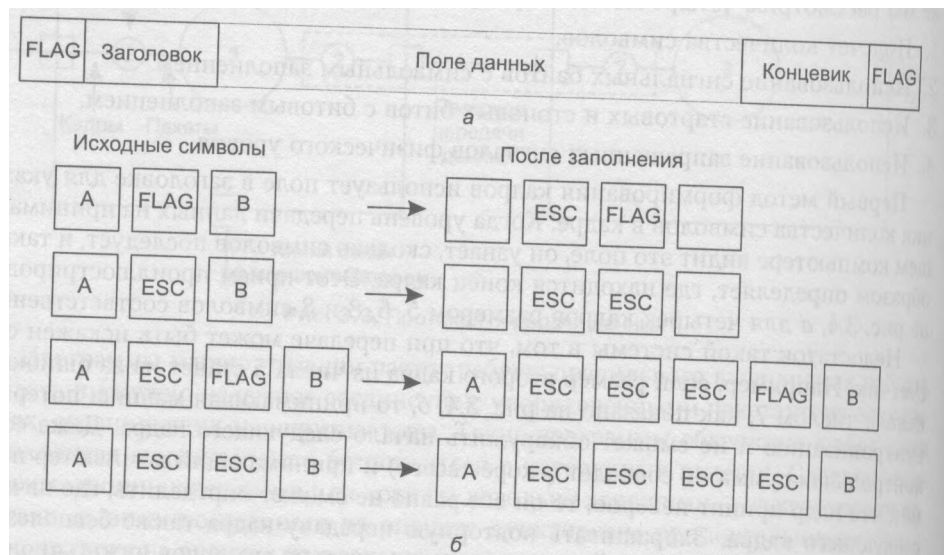


Рис. 5. Кадр, обмежений байтами прапорів (а); чотири приклади байтових послідовностей до і після символного заповнення (б)

Цей метод іноді приводить до серйозних проблем при передачі бінарних даних, таких як об'єктні коди програм або числа з плаваючою комою. В передаваних даних запросто може зустрітися послідовність, що використовується як байт прапора. Виникнення такої ситуації, швидше за все, зіб'є синхронізацію. Одним із способів рішення проблеми є додавання спеціального escape-символу (знака перемикання коду, ESC) безпосередньо перед випадково що співпав з байтом прапора усередині кадру. Рівень передачі даних одержувача спочатку прибирає ці escape-символи, потім передає кадр на мережний рівень. Такий метод називається символним заповненням. Таким чином, справжній прапор можна відрізнити від «підробленого» по наявності або відсутності перед ним ESC.

Наступне логічне питання: а що, якщо і символ ESC випадково виявиться серед інших даних? Рішення таке ж: вставити перед цим фіктивним escape-символом теперішній час. Тоді будь-хто одиночний ESC буде частиною escape-послідовності, а подвійний указуватиме на те, що службовий байт випадково опинився в потоці даних. Деякі приклади показані на рис. 3.6, б. У будь-якому випадку, байтова послідовність після її очищення від вставних символів в точності співпадає з початковою.

Схема символного заповнення, показана на рис. 3.5, – це трохи спрощена модель протоколу PPP, за допомогою якого більшість домашніх комп'ютерів з'єднується з інтернет-провайдером. Ми вивчимо PPP в цьому розділі.

Головний недолік цього методу полягає в тому, що він тісно пов'язаний з 8-бітовими символами. Тим часом не у всіх кодуваннях один символ відповідає 8 бітам. Наприклад, UNICODE використовує 16-бітове кодування. У міру розвитку мережних технологій недоліки використання довжини символного коду в механізмі формування кадрів ставали все очевиднішими. Тому було потрібно створення нової техніки, що допускає використання символів довільного розміру.

Новий метод дозволяє використовувати кадри і набори символів, що складаються з будь-якої кількості бітів. От як це реалізується. Кожний кадр починається і завершується спеціальною послідовністю бітів, 01111110 (насправді це все той же байт прапора). Якщо в бітовому потоці передаваних даних зустрінеться п'ять що йдуть підряд одиниць, рівень передачі даних автоматично вставить у вихідний потік нульовий біт. Бітове заповнення аналогічно символному, при якому в кадр перед випадково що зустрівся серед даних прапором вставляється escape-символ.

Коли приймаюча сторона зустрічає п'ять одиниць підряд, за якими слідує нуль, вона автоматично видаляє цей нуль. Бітове заповнення, як і символне, є абсолютно прозорим для мережного рівня обох комп'ютерів. Якщо послідовність прапора бітів (01111110) зустрічається в даних користувача, вона передається у вигляді 011111010, але в пам'яті приймаючого комп'ютера зберігається знову в початковому вигляді: 01111110. На рис. 3.6 наведений приклад бітового заповнення.

Завдяки бітовому заповненню межі між двома кадрами можуть бути безпомилково розпізнані за допомогою послідовності прапора. Таким чином, якщо приймальна сторона втратить межі кадрів, їй потрібно всього лише відшукати в отриманому потоці бітів байт прапора, оскільки він зустрічається тільки на межах кадрів і ніколи – в даних користувача.

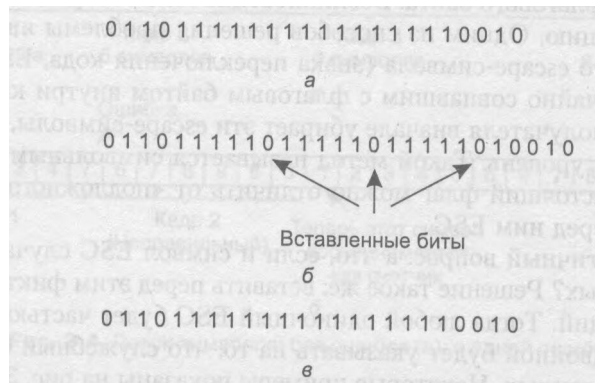


Рис. 6. Бітове заповнення: початкові дані (а); дані на лінії (б); дані, збережені в пам'яті після видалення вставних бітів (в)

Нарешті, останній метод формування кадрів прийнятний тільки в мережах, в яких фізичний носій володіє деякою надмірністю. Наприклад, деякі локальні мережі кодують один біт даних двома фізичними бітами. Звичайно біт 1 кодується парою високого і низького рівнів сигналів (негативний перепад), а біт 0 – навпаки, парою низького і високого рівнів (позитивний перепад). В такій схемі кожний передаваний біт даних містить в середині перехід, завдяки чому спрощується розпізнавання меж бітів. Комбінації рівнів сигналів (низький–низький і високий–високий) не використовуються для передачі даних, але використовуються як обмежувачі кадрів в деяких протоколах.

Багато протоколів передачі даних для підвищення надійності застосовують комбінацію лічильника символів з іншим методом формування кадру. Коли прибуває кадр, для виявлення його кінця використовується лічильник. Кадр сприймається як правильний тільки в тому випадку, якщо відповідний роздільник присутній в потрібній позиції і співпадає контрольна сума. В іншому випадку сканується вхідний потік, в якому шукається наступний роздільник.

9.1.4 Обробка помилок

Розв'язавши проблему маркіровки початку і кінця кадру, ми стикаємося з новою проблемою: як гарантувати доставку мережному рівню приймаючої машини всіх кадрів і при цьому розташувати їх в правильному порядку.

Припустимо, що відправник просто посилає кадри, не перевіряє про те, чи дійшли вони до адресата. Цього було б достатньо для сервісу без підтверджень і без встановлення з'єднання, але не для орієнтованого на з'єднання сервісу з підтвердженнями.

Звичайно для гарантування надійної доставки постачальнику посилається інформація про те, що відбувається на іншому кінці лінії. Протокол вимагає від одержувача посылати назад спеціальні управляючі кадри, позитивні або негативні повідомлення, що містять, про отримані кадри. Отримавши позитивне повідомлення, відправник визнає, що посланий їм кадр успішно отриманий на тому кінці лінії. Негативне повідомлення, навпаки, означає, що з кадром щось трапилося і його потрібно передати знову.

Крім того, посланий кадр може через несправність устаткування або якоїсь небудь перешкоди (наприклад, шуму) пропасти повністю. В цьому випадку приймаюча сторона його просто не отримає і, відповідно, ніяк не прореагує, а відправник може вічно чекати позитивної або негативної відповіді і так нічого і не отримати.

Щоб уникнути зависань мережі у разі повної втрати кадрів, використовуються таймери рівня передачі даних. Після посылки кадру включається таймер і відлічує інтервал часу, достатній для отримання приймаючим комп'ютером цього кадру, його обробки і посылки назад підтвердження. В нормальній ситуації кадр правильно приймається, а підтвердження посилається назад і вручається відправнику, перш ніж закінчиться встановлений інтервал часу, і лише після цього таймер відключається.

Проте якщо або кадр або підтвердження втрачається по шляху, встановлений інтервал часу закінчиться, і відправник отримає повідомлення про можливу проблему. Найпростішим рішенням для відправника бути послати кадр ще раз. Проте при цьому виникає небезпека отримання одного і того ж кадру кілька разів рівнем передачі даних приймаючого комп'ютера і повторної передачі його мережному рівню. Щоб цього не трапилося, необхідно

послідовно пронумерувати послані кадри, так щоб одержувач міг відрізнити повторно передані кадри від оригіналів.

Питання управління таймерами і порядковими номерами, що гарантують, що кожний кадр доставлений мережному рівню приймаючого комп'ютера рівно один раз, не більше і не менше, є дуже важливою частиною задачі, вирішуваною рівнем передачі даних. Далі в цьому розділі ми детально вивчимо методи управління на серії прикладів, що поступово ускладнюються.

9.1.5 Управління потоком

Ще один важливий аспект розробки рівня передачі даних (а також більш високих рівнів) пов'язаний з питанням про те, що робити з відправником, який постійно бажає передавати кадри швидше, ніж одержувач здатний їх одержувати. Така ситуація може виникнути, якщо біля передаючої сторони опиняється більш могутній (або менш завантажений) комп'ютер, ніж у приймаючої. Відправник продовжує посилати кадри на високій швидкості до тих пір, поки одержувач не виявиться повністю ними завалений. Навіть при ідеально працюючій лінії зв'язку в певний момент одержувач просто не зможе продовжувати обробку всіх кадрів, що прибувають, і почне їх втрачати.

В даний час застосовуються два підходи. При першому, що називається управлінням потоком із зворотним зв'язком, одержувач посилає відправнику інформацію, що дозволяє останньому продовжити передачу або, принаймні, повідомляти про те, як йдуть справи у одержувача. При другому підході, управлінні потоком з обмеженням, в протокол вбудовується механізм, що обмежує швидкість, з якою передавачі можуть передавати дані. Зворотний зв'язок з одержувачем відсутній. В цьому розділі ми розглянемо тільки підхід із зворотним зв'язком, оскільки другий підхід ніколи не застосовується на рівні передачі даних (втім, ми повернемося до нього на чолі 5).

Відомі різні схеми контролю потоку із зворотним зв'язком, але більшість з них використовує один і той же принцип. Протокол містить чітко визначені правила, що визначають, коли відправник може посилати наступний кадр. Ці правила часто забороняють пересилку кадру до тих пір, поки одержувач не

дасть дозволу, або явно, або неявно. Наприклад, при установці з'єднання одержувач може сказати: «ви можете послати мені зараз *n* кадрів, але не посилайте наступні кадри, поки я не попрошу вас продовжувати». В даному розділі ми розглянемо різні механізми, засновані на цьому принципі.

9.2. Виявлення і корекція помилок

Мережі повинні бути здатними передавати дані від одного пристрою до іншого з певною точністю. Система, яка не може гарантувати, що дані, отримані приймачем, є ідентичними даним, переданим передавачем, є по суті непотрібною. Та все ж іноді дані, що передаються від джерела до місця призначення, можуть зіпсуватися під час передачі. Фактично, більш вірогідно, що деяка частина повідомлення буде змінена в дорозі, ніж що повний вміст прибуде непошкодженим. Багато факторів, шум лінії, можуть змінити або знищити один або більше бітів даного пакету даних. Надійні системи повинні мати механізм для виявлення і виправлення таких помилок.

Виявлення помилки і виправлення виконуються або на каналному або на транспортному рівнях моделі OSI.

9.2.1 Типи помилок

Кожного разу, коли електромагнітний сигнал передається від однієї точки до іншої, він підлягає непередбаченому втручанню тепла, магнетизму та інших форм електрики. Це втручання може змінити форму або додати шуми в сигнал. Якщо сигнал несе кодовані двійкові дані, такі зміни можуть змінити значення даних. В однобітій помилці, 0 міняється на 1 або 1 на 0. У критичній помилці біти багаторазово змінюються (див. рис. 9.1).

Figure 9.1 Types of errors

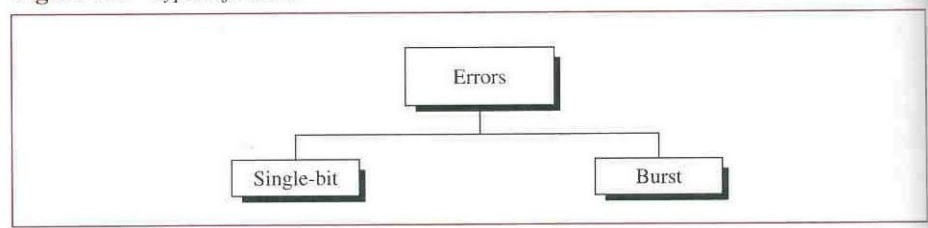


Рис. 7. Типи помилок

Однобітова помилка

Однобітова помилка, означає, що тільки один біт даного елемента (як наприклад байт, символ, елемент даних, або пакет) даних змінений з 1 на 0 або з 0 на 1.

Рис. 9.2 показує результат однобіткової помилки в елементі даних. Для розуміння зміни, можна уявити, що кожна група восьми бітів – це символ ASCII з бітом 0, доданим вліво. На рисунку, було послано 00000010 (ASCII STX), що означало початок тексту, але було отримано 00001010 (ASCII LF), що означає лінію.

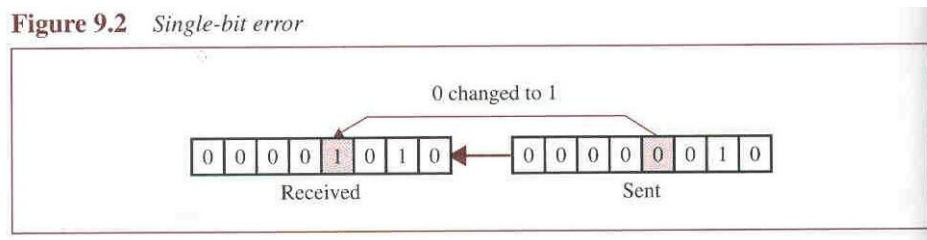


Рис. 8. Однобіткова помилка

Однобіткові помилки – це мало ймовірний вид помилки в серійній передачі даних. Припустимо, що відправник посилає дані на швидкості 1 Mbps. Це означає, що кожен біт триває тільки 1/1.000.000 секунди. Для того, щоб трапилась помилка, потрібно лише щоб шуми тривали 1/1.000.000 секунди (як правило, завади тривають набагато довше).

Проте, однобіткова помилка, може трапитися, якщо ми пересилаємо дані, використовуючи паралельну передачу. Наприклад, якщо вісім ліній використовуються, щоб послати всі вісім бітів одного байта одночасно і одна з ліній зашумлена, один біт може бути зіпсованим. В даному випадку, було послано ряд 0100010001000011, але було отримано 0101110101000011. Слід відзначити, що виникнення помилки не обов'язково означає, що помилки відбуваються в послідовних бітах. Пошкодження тривало від самого початку зіпсованого біта до останнього зіпсованого біта. Деякі біти між ними можуть бути не спотвореними.

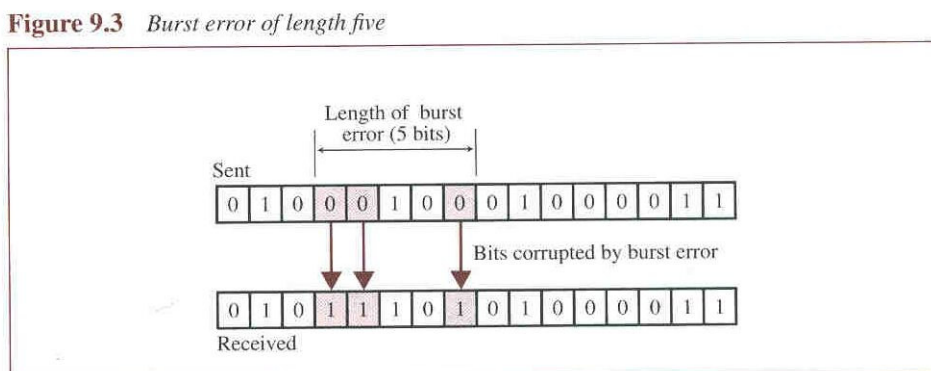


Рис. 9. Burst-помилка з довжиною 5

Найбільш ймовірно, що Burst помилка трапляється в серійній передачі. Тривалість шуму загалом довша, ніж тривалість біта, це означає, що коли шум впливає на дані, він впливає на багато бітів. Кількість бітів, що використовуються, залежить від швидкості передачі даних і тривалості шуму. Наприклад, якщо ми пересилаємо дані з швидкістю 1 Kbps, шум на 1/100 секунди може впливати на 10 бітів; якщо ми пересилаємо дані з швидкістю 1 Mbps, той же шум може впливати на 10000 бітів.

9.2.2 Методи виявлення помилок

Навіть якщо ми знаємо, які види помилок можуть відбуватися, чи розпізнаємо ми, коли вони відбудуться? Якщо ми маємо копію передачі для порівняння, то, звичайно, розпізнаємо. Але що, коли ми не маємо копії оригіналу? Потім ми не матимемо ніякої можливості дізнатись, чи трапилась помилка, поки ми розшифрували передачу і не скористалися значенням оригіналу. Для створення машини, щоб перевіряти на помилки дані, такий шлях буде повільний, дорогий, і сумнівного значення.

Надлишковість

Один механізм виявлення помилки, який повинен задовольнити цим вимогам, повинен бути здатним послати кожний елемент даних двічі. Пристрій отримання повинен бути здатним робити побітове порівняння між двома версіями даних. Будь-яка відмінність повинна вказати на помилку, і відповідний механізм виправлення міг би бути задіяний на місці. Ця система повинна бути цілком точною, але вона буде також повільнішою. Не тільки повинен дублюватися час передачі, але й повинна додаватися службова інформація, щоб порівняти кожний біт одиниці з оригінальним бітом.

Поняття включення додаткової інформації в передачі виключно для мети порівняння – це позитивно. Але замість повторення повного потоку даних, більш коротка група бітів може приєднуватися до кінця кожної одиниці. Ця техніка називається надлишковістю, тому що додаються додаткові біти надлишкової інформації; вони відкидаються, як тільки підтверджується точність передачі.

На рис. 9.4 показано процес використання надлишкових бітів, щоб перевірити точність елемента даних. Коли потік даних згенеровано, він проходить через пристрій, який аналізує це, і додає надлишкові біти для відповідного контролю коду. Елемент даних, збільшений окремими бітами (на ілюстрації, сім), передається від передавача до приймача. Приймач виконує повний потік функції перевірки. Якщо загальноприйнятий розрядний потік передав критерії перевірки, частина елемента даних приймається і надлишкові біти відкидаються.

Figure 9.4 Redundancy

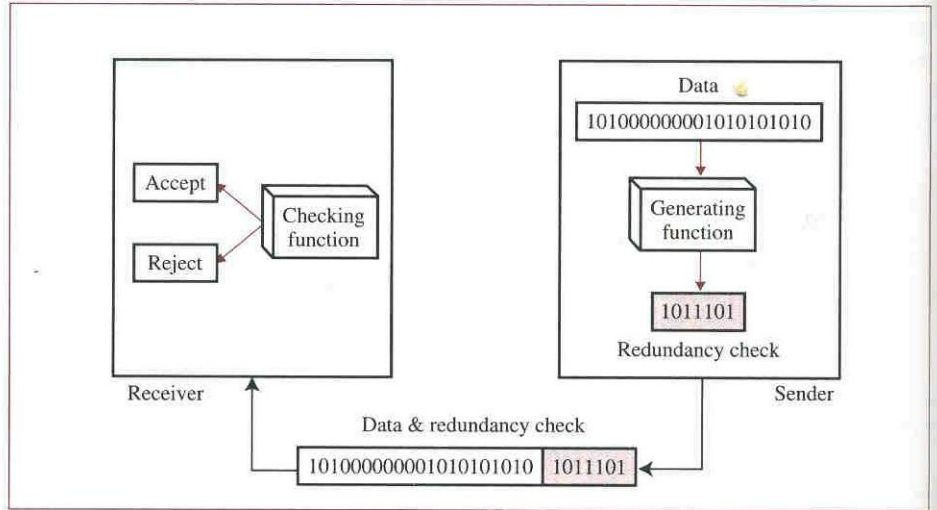


Рис. 10. Надлишковість

Чотири види контролю за допомогою надлишкових кодів використовуються в передачах даних: контроль VRC (також званий як контроль парності), контроль LRC, циклічний контроль CRC, і контрольна сума за допомогою надлишкових кодів. Перші три, VRC, LRC, і CRC, звичайно виконуються на фізичному рівні для використання на каналному рівні. Четвертий, контрольна сума, використовується перш за все верхніми рівнями (див. рис. 9.5).

Figure 9.5 Detection methods

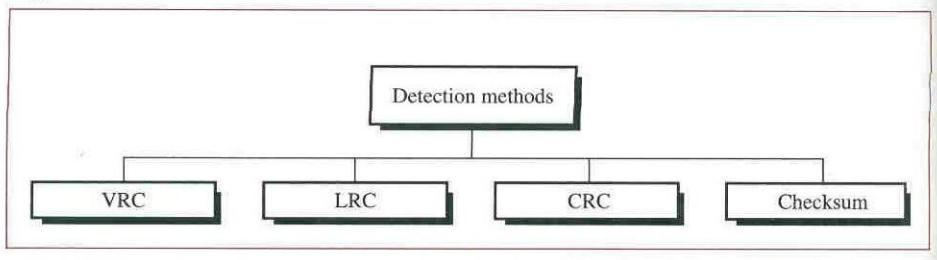


Рис. 11. Методи виявлення помилок

Контроль за допомогою надлишкових кодів (VRC)

Найзагальніший і найдешевший механізм для виявлення помилки – це контроль (VRC) за допомогою надлишкових кодів, який часто називається контроль парності. Відповідно до цієї техніки, надлишковий біт, що відповідає за розряд парності, приєднується до кожного елемента даних таким чином, що повне число знаходиться в одиниці (включаючи розряд парності).

Припустимо, потрібно передати двійковий елемент даних 1100001 [ASCII (97)], див. рис. 9.6. Додавання разом кількості 1-ць дає нам 3, непарне число. Перед передачею ми пропускаємо елемент даних через генератор паритету. Генератор паритету перераховує 1-ці і приєднує біт (1 в даному випадку) парності до кінця. Повне число 1-ць є тепер чотири. Система передає ціле розширене число через передавальну мережу. Коли воно досягає місця призначення, одержувач виконує перевірку всіх восьми бітів функцією парності. Якщо одержувач бачить 11100001, він перераховує чотири 1-ці, що є рівні номеру, і елемент даних проходить. Але що, коли елемент даних пошкоджений в дорозі? Якщо замість 11100001 одержувач бачить 11100101? Інформатор паритету перераховує 1-ці, одержує 5, непарне число, і тут одержувач знає, що помилку могли внести в дані де завгодно і таким чином відкидає цілу одиницю.

Figure 9.6 Even parity VRC concept

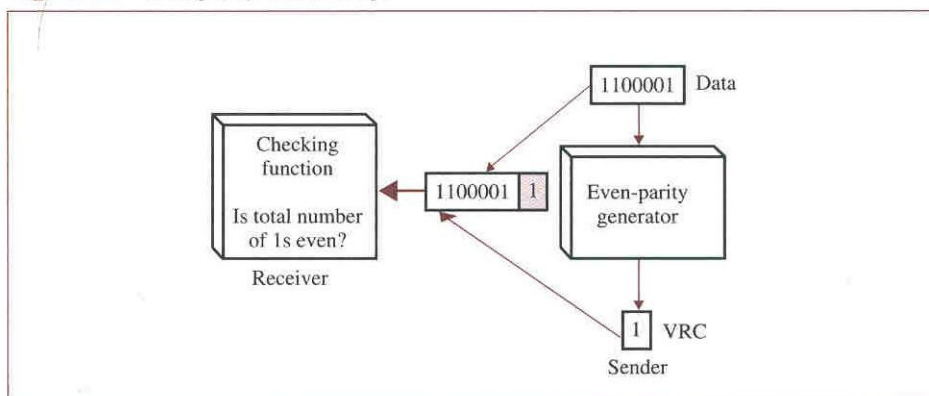


Рис. 12. Концепція VRC

Відзначимо, що ради простоти, ми обговорюємо тут перевірку на парність, де число 1-ць повинно бути парною кількістю. Деякі системи можуть використовувати перевірку на непарність, де число 1-ць повинно бути непарним. Принцип є тим же, а обчислення іншим.

Контроль за допомогою надлишкових кодів (LRC)

В контролі (LRC) за допомогою надлишкових кодів, блок бітів організований в таблиці (ряди і стовпчики). Наприклад, замість пересилки блоку 32 бітів, ми організуємо їх в таблицю, виконану в чотири ряди і вісім стовпців, як показано на рис. 9.7. Тоді ми обчислюємо розряд парності для кожного стовпчика і створюємо новий ряд з восьми бітів, які є розрядами парності для цілого блоку. Слід відзначити, що перший розряд парності в п'ятому ряду вираховується із використанням всіх перших бітів. Другий розряд парності вираховується із використанням всіх других бітів, і так далі.

Figure 9.7 LRC

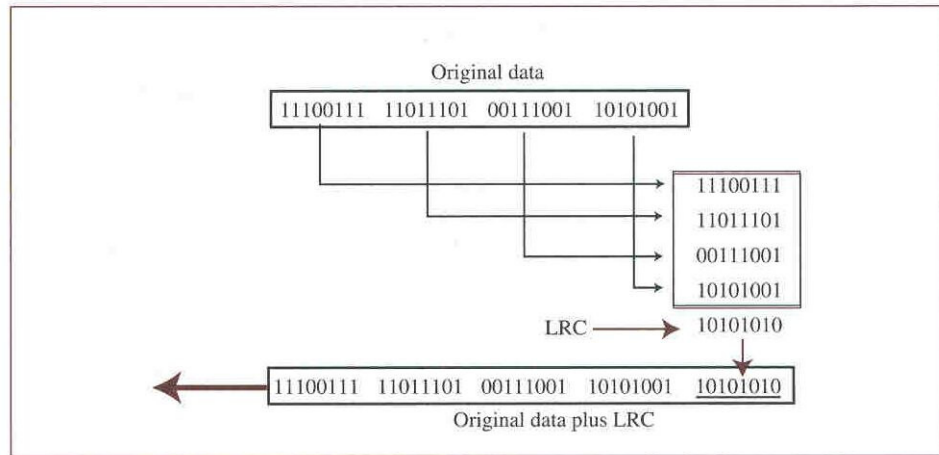


Рис. 13. LRC

Циклічний контроль за допомогою надлишкових кодів (CRC)

Третя і найбільш функціональна технологія є перевірка циклічного надлишкового коду (CRC). На відміну від VRC і LRC, які засновані на доповненні, CRC заснований на двійковому поділі. В CRC замість додавання бітів разом, щоб досягти бажаного паритету, додається послідовність надлишкових бітів, які називаються CRC. Ця послідовність приєднується до кінця елемента даних таким чином, що елемент даних можна точно поділити на секунди, визначені наперед двійковим числом. В місці призначення, елемент даних, що поступає, ділиться на той же номер. Якщо на цьому кроці не виникає ніякого залишку, прийнятий елемент даних, вважається непошкодженим і таким чином приймається. Залишок вказує, що елемент даних пошкоджений при передачі дорозі і таким чином повинен відкидатися.

Біти надлишковості, що використовуються CRC, одержують за допомогою розподілу елемента даних на визначеного наперед дільника; залишок є CRC. В

дійсності, CRC повинен мати дві якості: він повинен мати точно на один біт менше, ніж дільник, і приєднання до кінця рядка даних повинно робити розрядну послідовність здатною ділитися дільником.

Як теорія, так і додатки виявлення помилки CRC прості. Єдина складність знаходиться в отриманні CRC. Для того, щоб прояснити цей процес, ми почнемо з короткого перегляду і додамо ускладнимо його по ходу. На рис. 9.8 показано три початкові кроки.

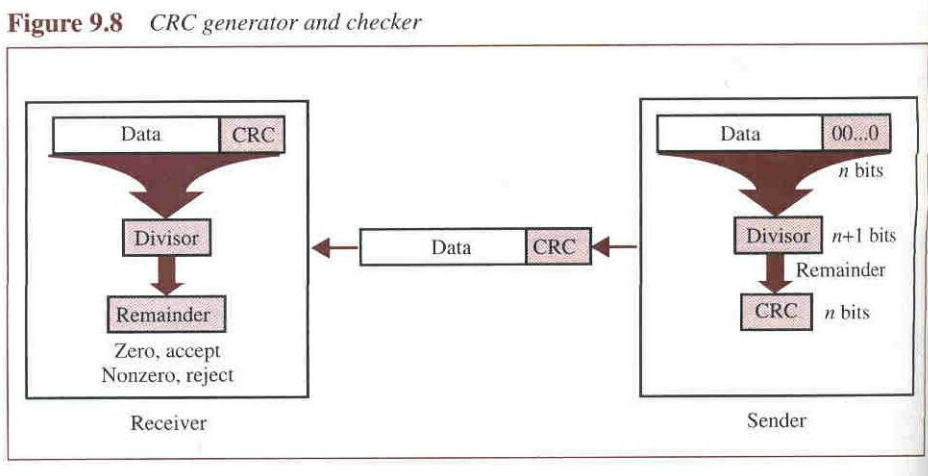


Рис. 14. CRC

Спершу, рядок 0 n приєднується до елемента даних. Кількість n є на один меншою, ніж кількість бітів у наперед визначеному дільнику, який має n + 1 біти.

Далі, наново розтягнутий елемент даних ділиться на дільника, що використовує процес, який називається двійковим діленням. Залишком, одержаним від цього ділення, є CRC.

На третьому кроці CRC з n бітів, отриманих на кроці 2, замінює приєднані 0 в кінець елемента даних. Слід відзначити, що CRC може складатися зі всіх 0-лів.

Елемент даних прибуває до одержувача даних спочатку, потім перевіряється CRC. Одержувач обходиться з цілим рядком як із одиницею: ділить його тим же дільником, який використовувався, щоб знайти залишок CRC.

Якщо рядок даних прибуває без помилки, перевірка CRC дає залишок нуля і переданий елемент даних. Якщо рядок змінений при передачі, ділення дає залишок відмінний від нуля і елемент даних не проходить.

Генератор CRC використовує ділення за модулем 2. На рис. 9.9 показано цей процес. На першому кроці, чотирьохбітовий дільник віднімає із самого початку чотири біти діленого. Кожний біт дільника віднімається від відповідного біта діленого без врахування старшого одиничного розряду. У нашому прикладі, дільник, 1101 віднімає із самого початку чотири біти діленого, 1001, одержуючи 100 (ведучий 0 залишку відкидається).

Figure 9.9 Binary division in a CRC generator

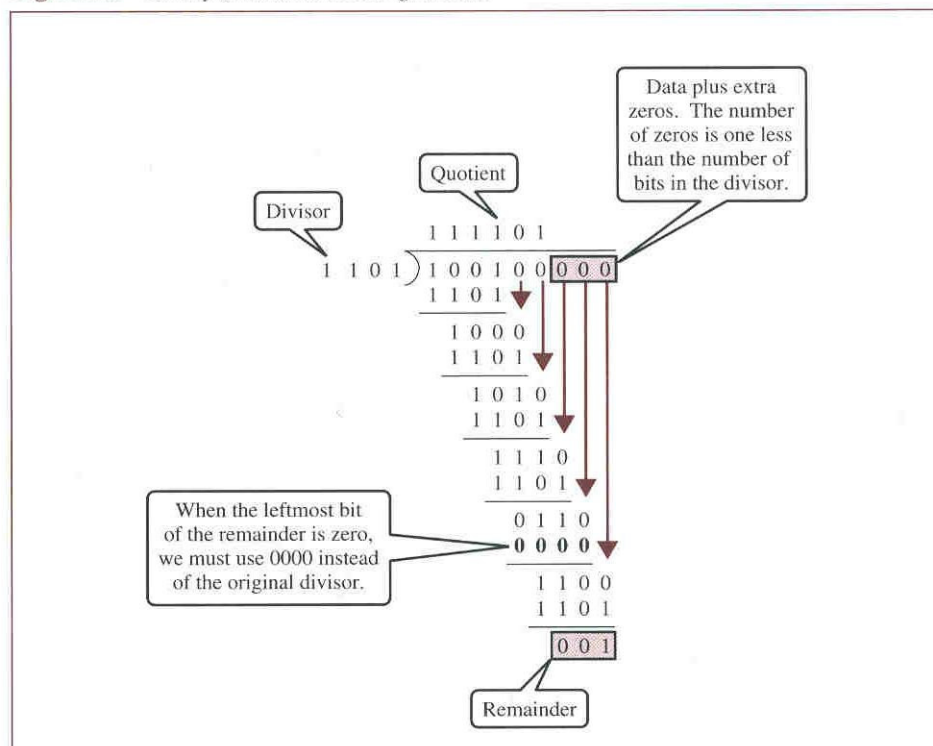


Рис.15. Двійкове ділення в CRC-генераторі

Наступний невикористаний біт від діленого тоді знесеться, щоб зробити число бітів в залишку рівним до числа бітів в дільнику. Наступний крок, таким чином, є 1000-1101, що дає 101, і так далі.

В цьому процесі, дільник завжди починає з 1; дільник може відніматись від частини попереднього діленого/залишку, яке рівне йому за довжиною; дільник може тільки відніматися від діленого/залишку, чий крайній лівий розряд складає 1. Іноді лівий біт діленого/залишок складає 0, рядок 0-лів, тієї ж довжини як дільник, замінюється дільником в тому кроці процесу. Наприклад, якщо дільник займає чотири біти, він замінюється чотирма 0-лями. (слід пам'ятати, що ми оперуємо з двійковими кодами, а не з кількісними значеннями; 0000 не є тим самим, що й 0.) Це обмеження означає, що, на будь-якому кроці, крайнє ліве віднімання буде або 0 – 0 або 1 – 1, обидва з яких дорівнюють 0. Так, після віднімання, крайній лівий розряд

залишку – це початковий нуль, який відкидається, і наступний невикористаний біт діленого зноситься, щоб заповнити залишок. Слід відзначити, що тільки перший біт залишку відкидається – якщо другий біт є також 0. Процес повторюється, поки, поки повне дільник не буде виділений.

Перевірка CRC

Функції перевірки CRC точно подібні генератору. Після отримання даних, приєднаних з CRC, робиться ділення за модулем 2. Якщо залишок – це всі 0-лі, CRC упускається і дані приймаються; інакше, прийнятий потік бітів відкидається і дані повторно відправляються. Рис. 9.10 показує той же процес ділення в одержувачі. Ми припускаємо, що немає помилки. Залишок – це всі 0-лі і прийняті дані.

Figure 9.10 Binary division in CRC checker

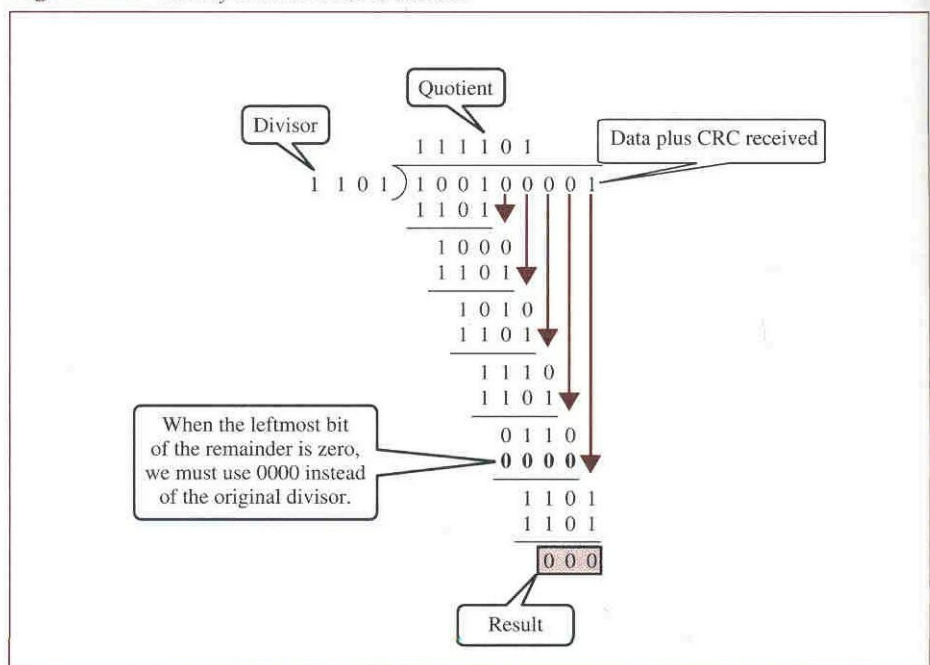


Рис. 16. Двійкове ділення в пристрої CRC-перевірки

Многочлени

Генератор CRC (дільник) найчастіше зображають, не як рядок 1 і 0, але як алгебраїчний многочлен. Багаточленний формат корисний із двох причин: він короткий і може використовуватися із математичним доведенням.

Многочлен повинен вибиратися так, щоб мати як мінімум наступні властивості:

- Він не має повинен ділитися на x .
- Він має ділитися на $(x + 1)$.

Перша умова гарантує, що всі набори помилки, які дорівнюють ступеню многочлена, знайдено. Друга умова гарантує, що всі набори помилок, які впливають на непарне число бітів, знайдено.

Figure 9.11 A polynomial

$$x^7 + x^5 + x^2 + x + 1$$

Рис. 17. Стандартні поліноми

Продуктивність

CRC є дуже дієвим методом виявлення помилки. Якщо дільник вибраний згідно наперед визначених правил, CRC може знайти всі набори помилок, які впливають на непарне число бітів.

- CRC може знайти всі набори помилок довжиною менші чи рівні ступеню многочлена.
- CRC може знайти з дуже високою вірогідністю набори помилок більшої довжини, ніж ступінь многочлена.

Контрольна сума

Метод виявлення помилки, що використовується протоколами вищого рівня, називається контрольною сумою. Подібно VRC, LRC, і CRC, контрольна сума заснована на понятті надлишковості.

Генератор контрольної суми

У відправнику, генератор контрольної суми підрозділяє елемент даних на рівні сегменти з n бітів (звичайно 16). Ці сегменти, додані разом, використовують одну складну арифметику таким чином, що результат – це також n бітів. Той результат (сума) потім доповнюється і приєднується до кінця оригінального елемента даних як біти надлишковості, що називається “поле контрольної суми”. Розширений елемент даних передається через мережу. Отже, якщо сума сегменту даних складає T , контрольна сума буде $-T$ (див. рис. 9.14 і 9.15).

Figure 9.14 Checksum

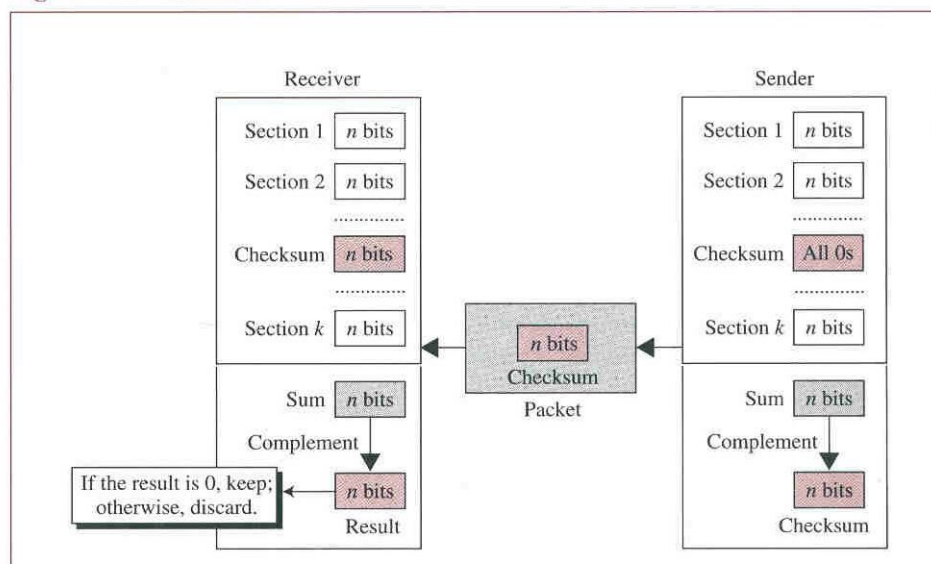


Рис. 18. Контрольна сума

Figure 9.15 Data unit and checksum

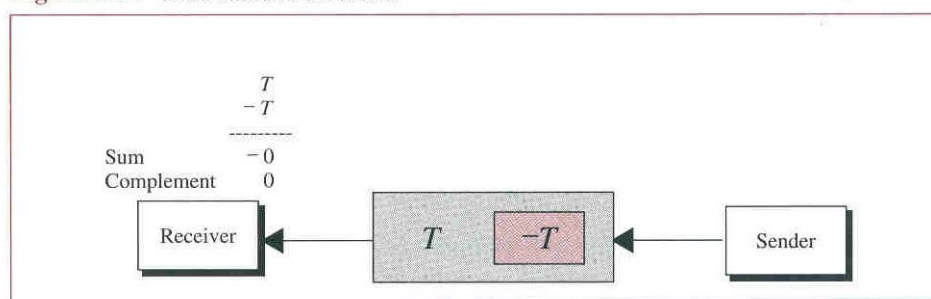


Рис. 19. Одиниця даних і контрольна сума

Перевірка контрольної суми

Одержувач ділить елемент даних, як вказано вище, і додає всі сегменти разом та доповнює результат. Якщо розширений елемент даних непошкоджений, повне значення, знайдене за допомогою додавання сегментів даних і поле контрольної суми повинне бути рівним нулю. Якщо результат не нульовий, пакет містить помилку і одержувач відкидає його.

Відправник виконує наступні кроки:

- Пакет ділиться на k секцій, кожна з них містить n бітів.
- Всі секції додаються разом, використовуючи єдине доповнення, щоб отримати суму.
- Сума доповнена і буде контрольною сумою.
- Контрольна сума відсилається з даними.

Одержувач виконує наступні кроки:

- Пакет ділиться на k секцій, кожна з n бітів
- Всі секції додаються разом, використовуючи єдине доповнення, щоб отримати суму.
- Сума доповнена.
- Якщо результат – рівний нулю, дані прийняті, інакше – ними нехтують.

Продуктивність

Контрольна сума знаходить всі помилки, що залучають непарне число бітів, як і більшість помилок, що залучають парне число бітів. Проте, якщо один або більше бітів сегменту пошкоджено і відповідний біт або біти протилежного значення в другому сегменті також пошкоджені, суми тих стовпців не зміняться і одержувач не знайде спотворення. Якщо остання цифра одного сегменту складає 0 і вона змінюється на 1 при передачі, тоді остання 1 в іншому сегменті має змінитися на 0, таким чином подібна помилка буде невизначеною. В LRC два 0 можуть одночасно змінитися на 1-ці без зміни паритету, тому що трансформації не враховувались. Контрольна сума зберігає всі трансформації; отже, навіть якщо два 0 зміняться на 1-ці це не змінить значення їх власного стовпця, але це змінить значення наступного вищого стовпця.

9.2.3 Корекція помилок

Канальний рівень повинен знаходити помилки передачі даних, пов'язані із спотворенням бітів в прийнятому кадрі даних або з втратою кадру, і по можливості їх коректувати.

Велика частина протоколів каналного рівня виконує тільки першу задачу – виявлення помилок, вважаючи, що коректувати помилки, тобто повторно передавати дані, що містили спотворену інформацію, повинні протоколи верхніх рівнів. Так працюють такі популярні протоколи локальних мереж, як Ethernet, Token Ring і інші. Проте існують протоколи каналного рівня, наприклад які самостійно вирішують задачу відновлення спотворених або втрачених кадрів.

Очевидно, що протоколи повинні працювати найбільш ефективно в типових умовах роботи мережі. Тому для мереж, в яких спотворення і втрати кадрів є дуже

рідкісними подіями, розробляються протоколи типу Ethernet, в яких не передбачаються процедури усунення помилок. Дійсно, наявність процедур відновлення даних вимагала б від кінцевих вузлів додаткових обчислювальних витрат, які в умовах надійної роботи мережі були б надлишковими.

Навпаки, якщо в мережі спотворення і втрати трапляються часто, то бажано вже на каналному рівні використовувати протокол з корекцією помилок, а не залишати цю роботу протоколам верхніх рівнів. Протоколи верхніх рівнів, наприклад транспортного або прикладного, працюючи з великими тайм-аутами, відновлять втрачені дані з великою затримкою. В глобальних мережах перших поколінь, наприклад мережах X.25, які працювали на ненадійних каналах зв'язку, протоколи каналного рівня завжди виконували процедури відновлення втрачених і спотворених кадрів.

Тому не можна вважати, що один протокол кращий від іншого тому, що він відновлює помилкові кадри, а інший протокол – ні. Кожний протокол повинен працювати в тих умовах, для яких він розроблений.

Механізми, які ми охопили до цього, знаходять помилки, але не виправляють їх. Виправлення помилки може проводити двома шляхами. В одному, коли помилка відкрита, одержувач може змушувати відправника ретранслювати повний елемент даних. В іншому, одержувач може використовувати виправляючий код помилки, який автоматично виправляє певні помилки.

Розробники мереж створили дві основні стратегії для боротьби з помилками. Даний метод ґрунтується на додаванні до пакету даних певної поточної інформації. В одному випадку цієї інформації повинно бути достатньо, щоб виявити, які дані повинні були прийти. В іншому випадку надлишкової інформації повинно бути достатньо тільки для того, щоб одержувач зрозумів, що відбулася помилка (без вказування її типу) і запитав повторну передачу. Перша стратегія використовує коди, що називаються коректуючими, або коди з виправленням помилок. Друга – код з виявленням помилок. Використання коду з виявленням помилок часто називають прямим виправленням помилок.

Кожна стратегія займає свою, так би мовити, нішу. У високонадійних каналах, таких як оптоволокно, дешевше використовувати код з виявленням помилок і просто наново передавати випадкові пошкоджені блоки. Проте, безпроводні

з'єднання, в яких може виникати безліч помилок, частіше використовують коди з надлишковістю, достатньою для того, щоб приймач міг визначити, які дані повинні були прийти. Це надійніше, ніж покладатися на повторну передачу, яка теж, можливо, пройде з помилками.

Теоретично, можливо, виправити будь-які помилки двійкового коду автоматично. Кількість бітів, що вимагаються, для виправлення багатобітову помилку чи набір помилок, така велика, що в більшості випадків недоцільно застосовувати цей метод. В зв'язку з цим, виправлення помилок обмежено до одно, дво чи трьох бітової помилки.

Виправлення однобітової помилки

Поняття, що лежить в основі виправлення помилки, може бути найдоступнішим для розуміння за допомогою розгляду найпростішого варіанту: однобітової помилки.

Як ми бачили раніше, однобітові помилки можуть виявлятися доповненням надлишкового (паритетного) біту до елемента даних (VRC). Єдиний додатковий біт може знайти однобітову помилку в будь-якій послідовності бітів, тому що результат повинен відрізнитися між тільки двома умовами: помилка або не помилка. Біт має два стани (0 і 1). Ці два стани достатні для такого рівня виявлення.

Але що, коли ми хочемо і знайти, і виправити однобітові помилки? Два стани достатні, щоб знайти помилку, але не виправити її. Помилка відбувається, коли одержувач читає біт 1 як 0 або біт 0 як 1. Щоб виправити помилку, одержувач просто змінює значення зміненого біта. Щоб зробити так, потрібно знати який біт є помилковим. Секрет виправлення помилки, полягає в тому, щоб правильно виявити недійсний біт або біти.

Наприклад, щоб виправити однобітову помилку в символі ASCII, код виправлення помилки повинен визначити, який із семи бітів змінився. В даному випадку, нам доведеться розрізнити між вісьмома різними станами: немає помилки, помилка в біті 1, помилка в біті 2, і так далі, аж до помилки в біті 7.

Біти надлишковості

Щоб вирахувати число бітів надлишковості (r), які вимагаються, щоб виправити дану кількість розрядів даних (m), ми повинні знайти взаємозв'язок між m і r . На рис 9.16 показано n біт даних r бітами надмірності, доданими до даних. Довжина коду – це $m+r$.

Figure 9.16 Data and redundancy bits

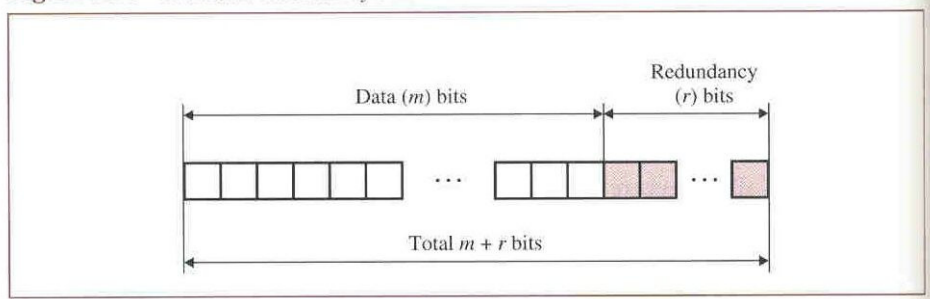


Рис. 20. Дані і надлишкові біти

Якщо знаходиться повне число бітів в одиниці передачі $n+r$, треба, щоб було вказано як мінімум $m+r+1$ різних станів. Одиначний стан означає відсутність помилки і стани $m+r$ локалізують помилку в кожній з позицій $m+r$.

Отже, стани $m+r+1$ стани можуть бути відкриті за допомогою r біт; і r біти можуть вказати 2^r різних станів. Таким чином, 2^r повинен бути рівний або більший, ніж $m+r+1$:

$$2^r > m+r+1$$

Значення r може визначатися за допомогою включення в значення m (оригінальна довжина переданого елемента даних). Наприклад, якщо значення m складає 7 (як в однобітовому коді ASCII), щонайменше значення r , яке може задовольнити це рівняння, складає 4:

$$2^4 > 7+4+1$$

В таблиці 9.1 показано деякі можливі значення m і відповідні значення r .

Number of Data Bits (m)	Number of Redundancy Bits (r)	Total Bits ($m + r$)
1	2	3
2	3	5
3	3	6
4	3	7
5	4	9
6	4	10
7	4	11

Коди Хемінга (Hamming Code)

Поки що ми розглянули число бітів, що вимагаються для покриття можливих однобітових помилкових станів при передачі. Але як маніпулювати тими бітами, щоб визначити, в якому стані відбулася помилка? Техніка, розроблена R.W.Hamming забезпечує практичне рішення.

Визначення місцеположення надлишкових бітів

Код Хемінга може звернутися до елементів даних будь-якої довжини і використовує взаємозв'язок між даними і бітами надлишковості, що обговорювались вище. Наприклад, семибітовий код ASCII, що вимагає чотири біти надлишковості, які можуть додаватися до кінця одиниці даних. На рис. 9.17 ці біти розміщені в місцеположеннях 1, 2, 4, і 8 (місцеположення в послідовності 11-ти). Для ясності в прикладах нижче ми звертаємося до бітів r1, r2, r4, і r8.

Figure 9.17 Positions of redundancy bits in Hamming code

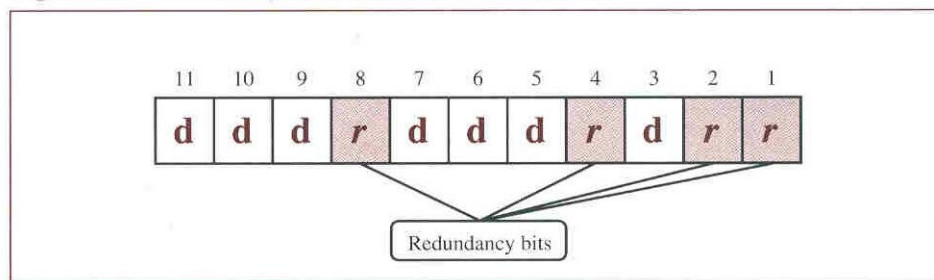


Рис. 21. Позиції надлишкових бітів у коді Хемінга

В коді Хемінга, кожний біт r – це біт VRC для однієї комбінації розрядів даних: d є бітом VRC для однієї комбінації розрядів даних, r є бітом VRC для іншої комбінації розрядів даних, і так далі. Комбінації, що використовуються, щоб вирахувати кожний з чотирьох r значень для послідовності семибітових даних.

Кожний розряд даних може включатися за більш, ніж одне обчислення VRC. В послідовностях вище, наприклад, кожний з оригінальних розрядів даних входить в як мінімум дві множини, в той час, як r біти входять в тільки один (див. рис. 9.18).

Figure 9.18 Redundancy bits calculation

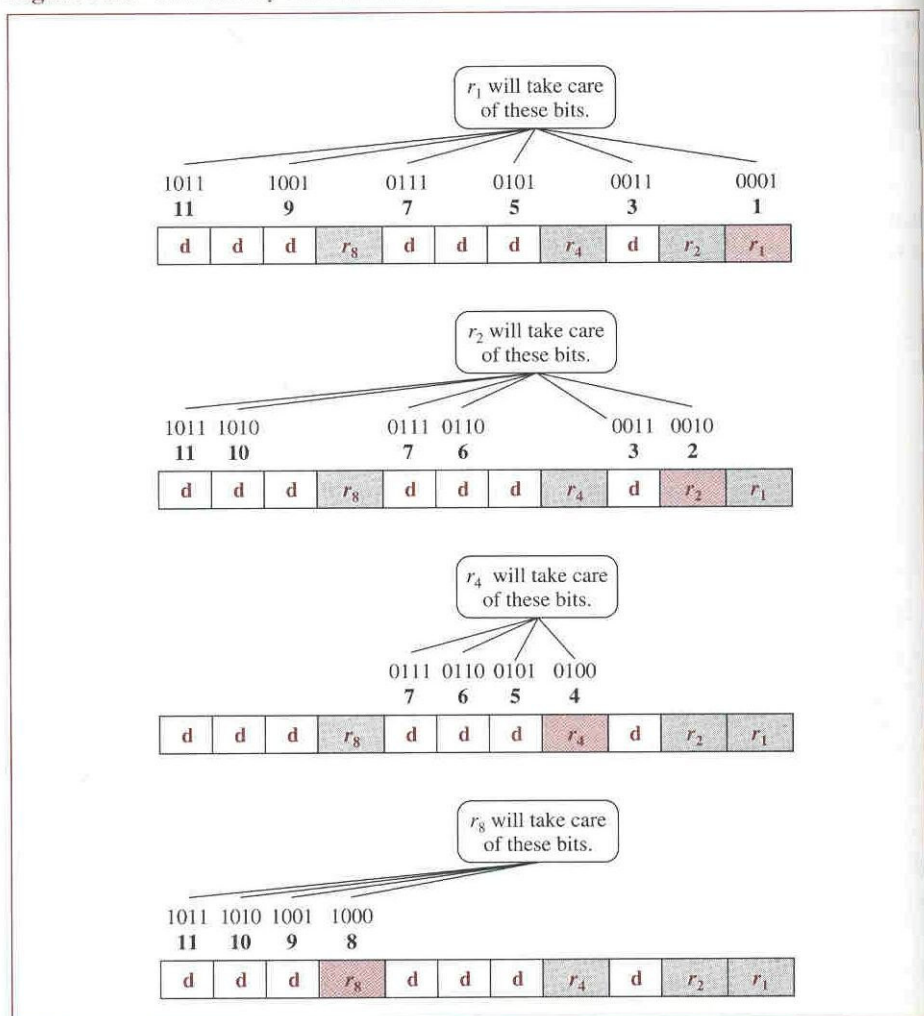


Рис. 22. Обчислення надлишкових бітів

Обчислення значень r

На рис. 9.19 показано реалізацію коду Хемінга для символу ASCII. На першому кроці, ми розміщуємо кожен біт оригінального символу у відповідному місцеположенні з 11 бітів. На подальших кроках, ми обчислюємо рівні значення для парних розрядних комбінацій. Значення паритету для кожної комбінації – це значення відповідних r біт, Наприклад, значення r вираховується, щоб забезпечити перевірку парності для комбінації бітів 3, 5, 7, 9, і 11. Значення r_2 вираховується, щоб забезпечити перевірку парності бітами 3, 6, 7, 10, і 11, і так далі. Заключний 11-розрядний код відсилається через лінію передачі.

Figure 9.19 Example of redundancy bit calculation

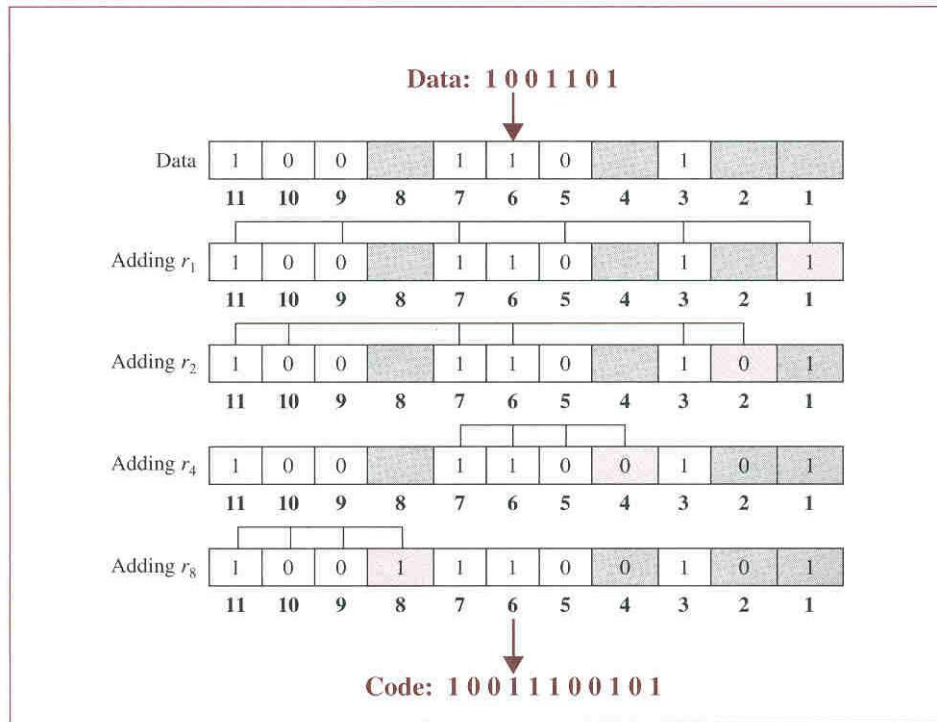


Рис. 23. Приклад розрахунку надлишкових бітів

Уявіть собі, що згадана вище передача отримана, біт під номером 7 змінений з 1 на 0 (див. рис. 9.20).

Одержувач отримує передачу і перераховує чотири нових VRCs, використовуючи той же набір бітів, що використовуються відправником плюс розряд парності для кожної множини (див. рис. 9.21). Потім він асемблює нові значення паритету в двійковому числі в порядку позицій (r_8, r_4, r_2, r_1). В нашому прикладі, цей крок дає нам двійкове число 0111 (7 в десятковій системі), яке є точним розташуванням біта помилки.

Figure 9.20 Single-bit error

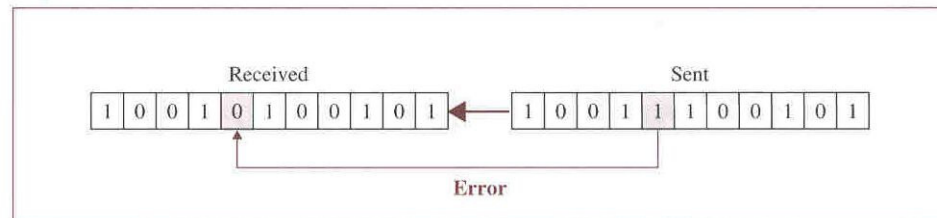


Рис. 24. однобітова помилка

Тема 10. Протоколи передачі даних і структура стандартів IEEE 802.x

10.1. Протоколи канального рівня

10.1.1. Асинхронні протоколи (ADLP)

10.1.2. Синхронні ПРОТОКОЛИ

10.1.2.1. Символьно-орієнтовані протоколи

10.1.2.2. Біт-орієнтовані протоколи

10.2. Структура стандартів IEEE 802.x

10.1. Протоколи канального рівня

Взагалі, термін протокол відноситься до набору правил або домовленостей для виконання певної задачі. При передачі даних, цей термін використовується у вузькому значенні, і означає набір правил або специфікацій, що використовується для реалізації одного або більше рівнів моделі OSI. Ми вже стикалися з інтерфейсом EIA 232-D, який є протоколом, що використовується на фізичному рівні в моделі OSI.

Протокол передачі даних – це набір правил або специфікацій, що використовуються для реалізації одного або більше рівнів моделі OSI.

Протоколи канального рівня (DLP) – це набори специфікацій, що використовуються для реалізації канального рівня. Тому вони містять правила для контролю за лінією, контролю за потоком даних і обробки помилок.

Протокол канального рівня – це набір специфікацій, що використовуються для реалізації канального рівня.

DLP можна поділити на дві підгрупи: асинхронні і синхронні протоколи (див. рис. 1). Асинхронні DLP (ADLP) маніпулюють з кожним символом в бітовому потоці незалежно. Синхронні DLP (SDLP) беруть цілий бітовий потік і розділяють його на символи однакового розміру.

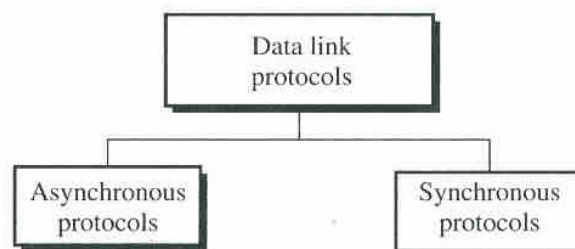
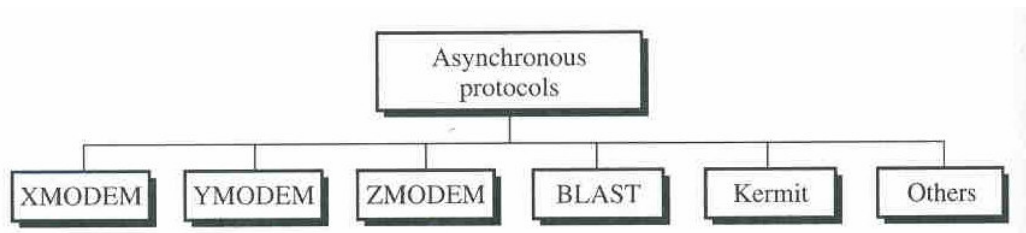


Рис. 1 Категорії DLP

10.1.1. Асинхронні протоколи (ADLP)

Цілий ряд ADLP був розроблений за останні десятиріччя, деякі з яких показані на рис. 2. Сьогодні, ці протоколи використовуються переважно в модемах. Завдяки властивій ADLP повільності (походить від обов'язкових доповнень початкових і кінцевих бітів та розширених інтервалів між фреймами), асинхронна передача на каналному рівні замінюється синхронними механізмами вищої швидкодії.

Рис. 2 Асинхронні протоколи



ADLP нескладні і недорогі. Як вже обговорювалося в Розділі 6, в асинхронній передачі елемент даних передається без часової координації між відправником і отримувачем. (i) Отримувач може не знати точно, коли був посланий елемент даних; він тільки повинен визначити початок і кінець даного елемента. Це досягається шляхом використання додаткових бітів (початкові і кінцеві) при створенні елемента даних.

Асинхронні протоколи, що використовуються перш за все в модемах, встановлюють початкові та кінцеві біти і проміжки змінної довжини між символами.

Розроблено велику різноманітність ADLP; але ми розглянемо тільки декілька з них.

XMODEM

В 1979 Ward Christiansen розробив протокол передачі файлів по телефонній лінії для комунікації між РС. Цей протокол, зараз відомий як **XMODEM**, - це напів-спарений ARQ протокол зупинки-і-очікування. Фрейм з його полями показано на рис. 3.

Перше поле – це однобітний початок заголовку (SOH). Друге поле - це двохбітний заголовок. Перший байт заголовку, номер послідовності, містить номер фрейму. Другий байт заголовку використовується для перевірки правильності

порядкового номера. Поле даних фіксованої довжини містить 128 байт даних (двійкових, логічних, ASCII, текстових та ін.). Останнє поле, CRC, для перевірки поля даних на помилки.

В цьому протоколі, передача даних починається з пересилки фрейму NAK від отримувача до відправника. Кожного разу, коли відправник посилає фрейм, він повинен чекати на підтвердження (ACK) перед тим, як послати наступний фрейм. Якщо натомість отримано NAK, то наперед посланий фрейм посилається знову. Фрейм також може також бути пересланий, якщо не отримано відповіді через вказаний період часу. Окрім NAK або ACK, відправник може отримати сигнал відміни (CAN), який перериває передачу.

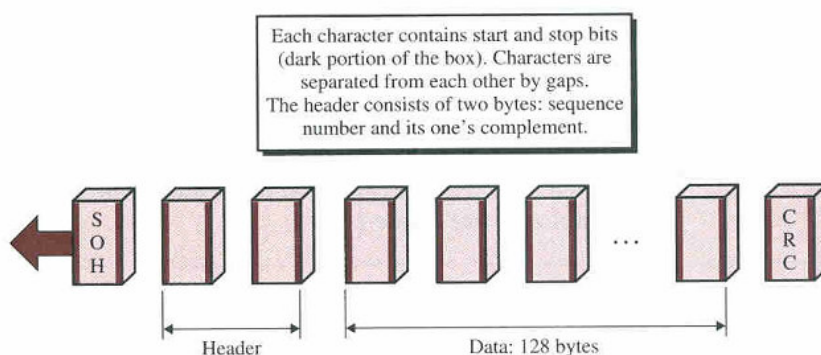


Рис. 3 Фрейм XMODEM

YMODEM

YMODEM - це протокол, який подібний до XMODEM, але має наступні відмінності:

- Елемент даних складає 1024 байти.
- Два CANs посилаються для переривання передачі.
- Для обробки помилок використовується ITU-T CRC-16.
- Декілька файлів можуть посилатися одночасно.

ZMODEM

ZMODEM - це більш новий протокол, який об'єднує особливості як XMODEM, так і YMODEM.

BLAST

Блокова асинхронна передача (BLAST) більш потужна, ніж XMODEM. Це повнодуплексний контроль за потоком даних з рухомим вікном. Це дозволяє передачу даних і двійкових файлів.

Kermit

Kermit, що розроблений в Columbia University, – це зараз найбільш розповсюджений асинхронний протокол. Цей протокол передачі файлів за функціонуванням подібний до XMODEM, коли відправник чекає NAK перед тим, як розпочати передачу. Kermit дозволяє передачу управляючих символів як текст, що реалізується у два кроки. Спочатку, управляючий символ, який використовується як текст, перетворюється в друкований символ за допомогою додавання фіксованого числа до його ASCII коду. По-друге символ # додається попереду перетвореного символу. Таким чином, управляючий символ, що використовується як текст, передається двома символами. Коли одержувач зустрічає символ #, це знає, що він повинен упускатися, і що наступний символ є управляючим. Якщо відправник хоче послати символ #, то він відправить два з них. Відзначте, що Kermit - це програма емуляції терміналу як і протокол передачі файлів.

1.2. Синхронні протоколи

Швидкість синхронної передачі робить її кращим вибором над асинхронною передачею, для технологій LAN, MAN і WAN. Протоколи, що управляють синхронною передачею, можна розділити на два класи: символно-орієнтовані протоколи і біт-орієнтовані протоколи (див. рис. 4).

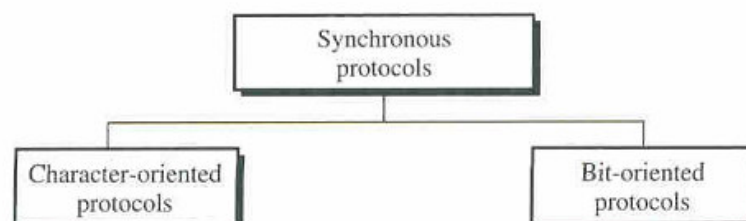


Рис. 4. Синхронні протоколи

Символьно-орієнтовані протоколи (або **байт-орієнтовані протоколи**) інтерпретують фрейм передачі або пакет як послідовність символів, кожний з яких

складається з одного байта (вісім бітів). Вся контрольна інформація знаходиться у формі існуючої системи кодування символу (наприклад, символи ASCII).

Біт-орієнтовані протоколи інтерпретують фрейм передачі або пакет як послідовність індивідуальних бітів, що робить значимим їхнє розміщення у фреймі і їхнє зіставленням з іншими бітами. Контрольна інформація в може бути одним або кількома бітами залежно від інформації, що міститься у пакеті.

У символно-орієнтованому протоколі фрейм або пакет інтерпретується як серія символів. В біт-орієнтованому протоколі фрейм або пакет інтерпретується як серії бітів.

1.2.1. Символьно-орієнтовані протоколи

З причин, які розглянуто нижче в цій секції, символно-орієнтовані протоколи не такі ефективні як біт-орієнтовані протоколи і тому вони зараз рідко використовуються. Проте вони є легкими для розуміння і використовують ту ж саму логіку і організацію як біт-орієнтовані протоколи. Розуміння символно-орієнтованих протоколів забезпечує основу для кращого розуміння біт-орієнтованих протоколів.

У всіх даних протоколах зв'язку, контрольна інформація додається до потоку даних або як окремі контрольні фрейми, або як доповнення до існуючих фреймів даних. В символно-орієнтованих протоколах, ця інформація знаходиться у формі кодових слів, узятих з існуючих наборів символів, як наприклад ASCII або EBCDIC. Ці багаторозрядні символи несуть інформацію про дисципліну лінії, управління потоком, і контроль помилки. Серед існуючих символно-орієнтованих протоколів найбільш відомий двійкова синхронна комунікація (binary synchronous communication) фірми IBM.

Двійкова синхронна комунікація (BSC)

Двійкова синхронна комунікація (BSC) - це популярний символно-орієнтований протокол каналного рівня, що був розроблений IBM в 1964 р. Він може використовуватися як в двоточкових так і багатоточкових конфігураціях, підтримує напів-дуплексну передачу, використовуючи метод управління потоком ARQ “зупинка-і-очікування” і контроль помилок. BSC не підтримує дуплексну передачу або протокол “ковзаючого вікна”.

Популярним символно-орієнтованим протоколом канального рівня є двійкова синхронна комунікація (BSC), особливістю якої є напів-дуплексна передача з ARQ “зупинка-і-очікування”. Він розроблений фірмою IBM.

Управляючі символи

Таблиця 11.1 дає список стандартних *управляючих символів*, які використовуються у фреймі BSC. Треба відзначити, що в цьому протоколі не використовується символ ACK. Пам’ятайте, що BSC використовує ARQ “зупинка-і-очікування”; підтвердження повинні бути або ACK 0, або ACK 1, щоб конкретизувати чергування фреймів даних.

Таблиця 1 Управляючі символи для BSC

<i>Character</i>	<i>ASCII Code</i>	<i>Function</i>
ACK 0	DLE and 0	Good even frame received or ready to receive
ACK 1	DLE and 1	Good odd frame received
DLE	DLE	Data transparency marker
ENQ	ENQ	Request for a response
EOT	EOT	Sender terminating
ETB	ETB	End of transmission block; ACK required
ETX	ETX	End of text in a message
ITB	US	End of intermediate block in a multiblock transmission
NAK	NAK	Bad frame received or nothing to send
NUL	NULL	Filler character
RVI	DLE and <	Urgent message from receiver
SOH	SOH	Header information begins
STX	STX	Text begins
SYN	SYN	Alerts receiver to incoming frame
TTD	STX and ENQ	Sender is pausing but not relinquishing the line
WACK	DLE and ;	Good frame received but not ready to receive more

Коди ASCII

Символи в таблиці 11.1 зображаються по різному в певних системах кодування, і не всі вони доступні в кожній системі. Якою б не була система, не всі управляючі символи можуть зображатися єдиним символом. Часто вони повинні відображатися двома або трьома символами. Також в таблиці 11.1 показано коди ASCII.

Фрейми BSC

Протокол BSC ділить передачу на фрейми. Якщо фрейм використовується тільки з метою управління, то він називається *управляючим фреймом*. Управляючі фрейми використовуються для обміну інформацією між пристроями комунікації, наприклад, щоб встановити зв'язок, щоб управляти потоком передачі, контролювати обробку помилок і роз'єднати пристрої при закінченні сеансу. Якщо фрейм містить частину або все повідомлення, тоді це *фрейм даних*. Фрейми даних використовуються для передачі інформації, але вони можуть також містити контрольну інформацію, що стосується даних (див. рис. 5).

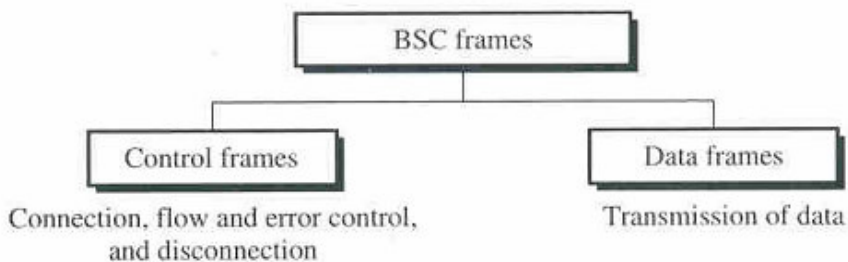


Рис. 5 Фрейми BSC

Фрейми даних

Рис. 6 показує формат простого фрейму даних. Стрілка показує напрям передачі. Фрейм починається з двох або більше символів синхронізації (SYN). Ці символи попереджають одержувача про надходження нового фрейму і забезпечують бітовий зразок, що використовується одержувачем, щоб синхронізувати свій таймінг з таймінгом пристрою-відправника. Код ASCII для SYN – це 00101110. Початковий (восьмий) біт цього байта зазвичай заповнюється додатковим 0. Два символи SYN мають такий вигляд: 0001011000010110.

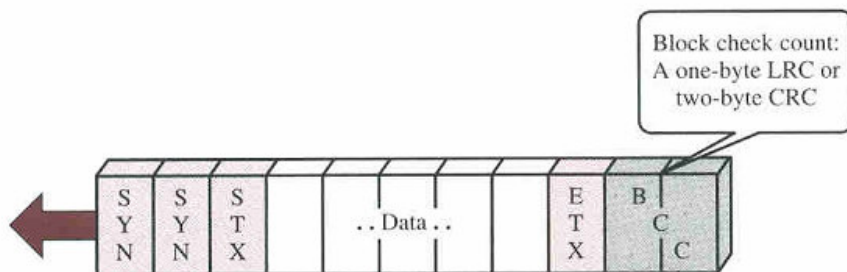


Рис. 6 Простий фрейм даних BSC

Після двох символів синхронізації йде символ початку тексту (STX). Цей символ сигналізує одержувачу, що контрольна інформація закінчується і наступний

байт - це дані. Дані або текст можуть складатися з чисел або символів. Символ кінця тексту (ETX) розділяє текст і наступні управляючі символи.

Нарешті, один або два символи під назвою *контрольна сума блоку (block check count – BCC)* включаються для виявлення помилок. Поле BCC може бути *односимвольним контролем з використанням надлишкових кодів (longitudinal redundancy check – LRC)* або *двохсимвольним циклічним контролем з використанням надлишкових кодів (cyclic redundancy check – CRC)*.

Поля заголовку фрейма: Вищеописаний зразок фрейму використовується рідко. Зазвичай, потрібно включати також адресу пристрою-одержувача, адреси пристрою-відправника й ідентифікаційні номери фреймів (0 або 1) для ARQ “зупинка-і-очікування” (див. рис. 7). Ця інформація міститься в спеціальному полі – *заголовок (header)*, – яке починається із символу початку заголовку (SOH). Заголовок починається після символів SYN і перед STX; все, що отримано після символу SOH, але перед STX, це інформація заголовку.

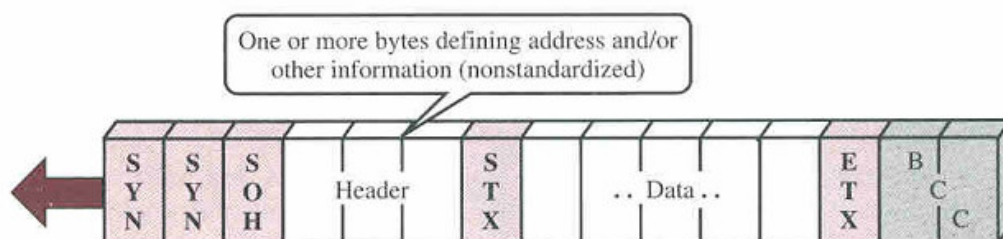


Рис. 7 Фрейм BSC із заголовком

Багатоблокові фрейми: вірогідність помилки в блоці тексту зростає із збільшенням довжини фрейму. Чим більше бітів у фреймі, тим більша вірогідність, що один з них буде зіпсований в процесі передачі, і більша вірогідність, що зміни в окремих бітах взаємовиключать один одного і зроблять процес виявлення помилок важким. З цієї причини, текст в повідомленні часто ділиться між окремими блоками. Кожний блок, крім останнього, починається символом STX і закінчується символом проміжного текстового блоку (ITB). Останній блок починається з STX, але вже закінчується символом ETX. Одразу ж після кожного ITB чи ETX йде поле BCC. Таким чином, одержувач може перевірити на помилки кожний блок окремо, отже, зростає вірогідність виявлення помилок. Проте, якщо якийсь блок містить помилку, потрібно повторно переслати увесь фрейм. Після того, як було досягнуто ETX і перевірено останній BCC, одержувач посилає єдине підтвердження для всього

фрейму. Рис. 8 показує структуру багатоблокового фрейму; який, наприклад, включає два блоки. Але на практиці фрейми можуть мати більш ніж два блоки.

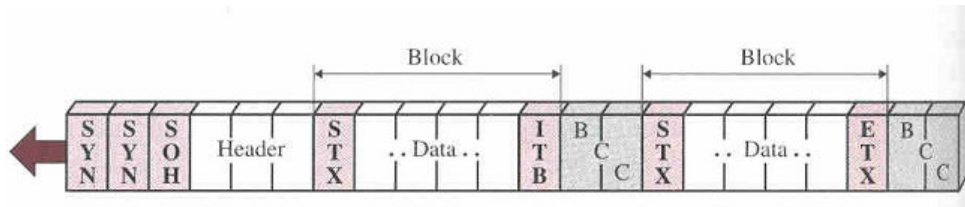
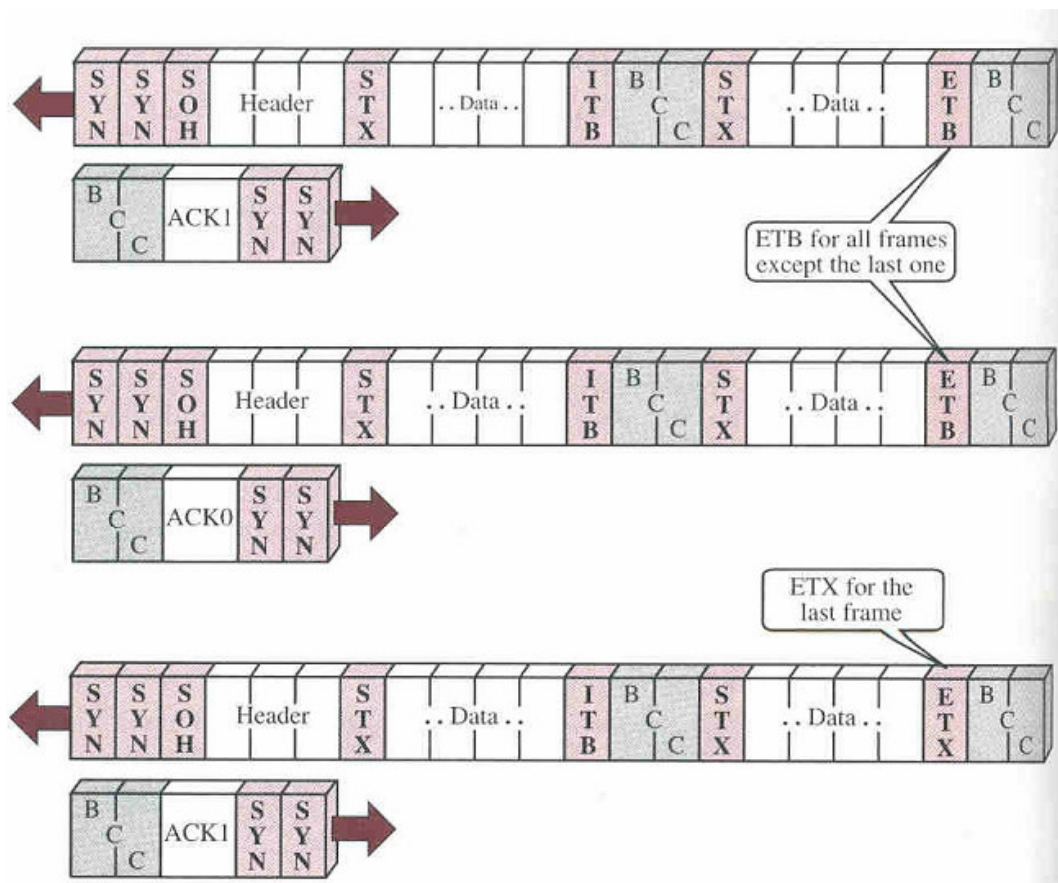


Рис. 8 Багатоблоковий фрейм

Передача багатоблокових фреймів: В прикладах, досліджених вище, один фрейм несе ціле повідомлення. Після кожної фрейму, повідомлення закінчується і управління лінією передається до вторинного пристрою (напівдуплексний метод). Деякі повідомлення, проте, можуть бути занадто довгими, щоб передаватися у формат одного фрейму. В таких випадках відправник може розбити повідомлення не тільки на блоки, але й на фрейми. Декілька фреймів можуть нести продовження єдиного повідомлення. Щоб повідомити одержувача, що кінець фрейму не є кінцем передачі, символ ETX у всіх фреймах, крім останнього, замінюється символом кінця передачі блоку (ETB). Одержувач повинен підтвердити кожний фрейм окремо, але не повинен приймати управління лінією зв'язку, поки не зустрине ETX в останньому фреймі (див. рис. 9).



Управляючі фрейми

Не треба ототожнювати управляючий фрейм з управляючим символом. Управляючий фрейм використовується одним пристроєм, щоб направити команди або попросити інформацію від іншого пристрою. Управляючий фрейм містить управляючі символи, але не містить даних; він несе інформацію, що безпосередньо стосується функціонування каналного рівня. Рис. 10 показує основний формат управляючого фрейму BSC.

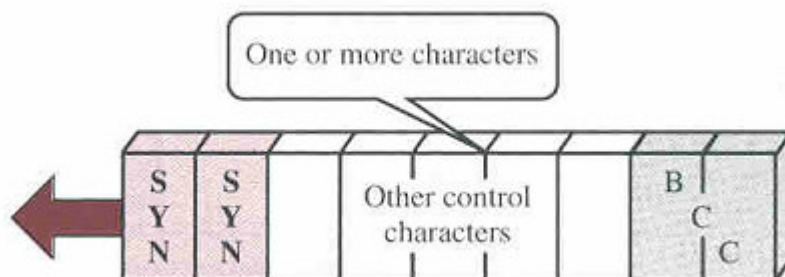


Рис. 10 Управляючий фрейм BSC

Управляючі фрейми обслуговують три цілі: встановлення зв'язку, підтримка потоку і обробки помилок протягом передачі даних і завершення зв'язку (див. рис. 11).

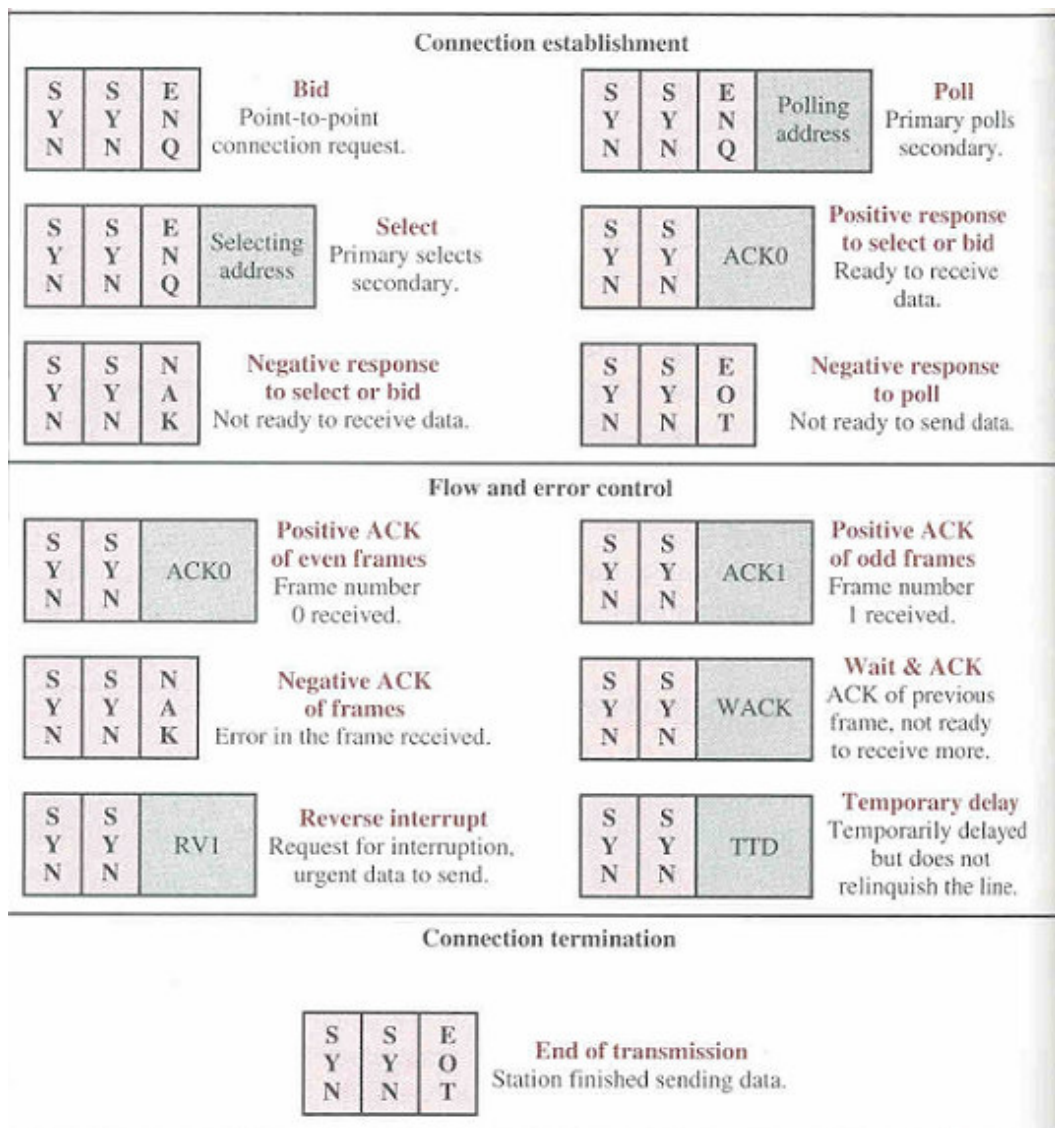


Рис. Управляючі фрейми

Незалежність даних

Спочатку BSC розроблявся тільки для передачі текстових повідомлень (слова або малюнки, складені з буквено-цифрових символів). Проте, сьогодні споживач переважно хоче передавати двійкові послідовності, які містять нетекстову інформацію і команди, наприклад, програми і графічну інформацію. На жаль, повідомлення цього виду можуть створювати проблеми при передачі за допомогою BSC. Якщо текстове поле повідомлення включає восьми-бітову комбінацію, яка схожа на управляючий символ BSC, то одержувач інтерпретує її так, що спотворюється зміст повідомлення. Наприклад, одержувач, який отримав двійковий код 0000011, може інтерпретувати його як символ ETX. З того, що ми знаємо про управляючі фрейми, кожного разу, коли одержувач знаходить ETX, він очікує, що наступні два байти є BCC і починає перевірку на наявність помилок. Але код

0000011 в цьому випадку виступає як дані, а не як управляюча інформація. Конфлікт між контрольною інформацією і даними спричинений відсутністю незалежності даних.

Протокол має бути незалежним, тобто він повинен нести будь-яку комбінацію бітів, яка представляє дані, без їхнього конфлікту з управляючою інформацією.

Незалежність даних при їх передачі означає здатність послати будь-яку комбінацію бітів, які представляють дані.

Незалежність даних в BSC досягається **заповненням байта (byte stuffing)**. Цей процес включає два етапи: позначення незалежної текстової області за допомогою символів DLE і вставка перед будь-яким символом DLE в межах незалежної області додаткового символу DLE.

Щоб визначити незалежну область, ми вставляємо один символ DLE тільки перед символом STX на початку текстового поля та інший тільки перед символом ETX (або ITB, або ETB) в кінці текстового поля. Перший DLE говорить одержувачу, що текст може містити управляючі символи і ними можна нехтувати. Останній DLE говорить одержувачу, що незалежна область закінчилася.

Проблеми можуть все ще виникати, якщо незалежна область містить символ DLE як текст. В такому разі, ми вставляємо додатковий DLE перед кожним DLE в межах тексту. Рис. 12 показує приклад незалежного фрейму.

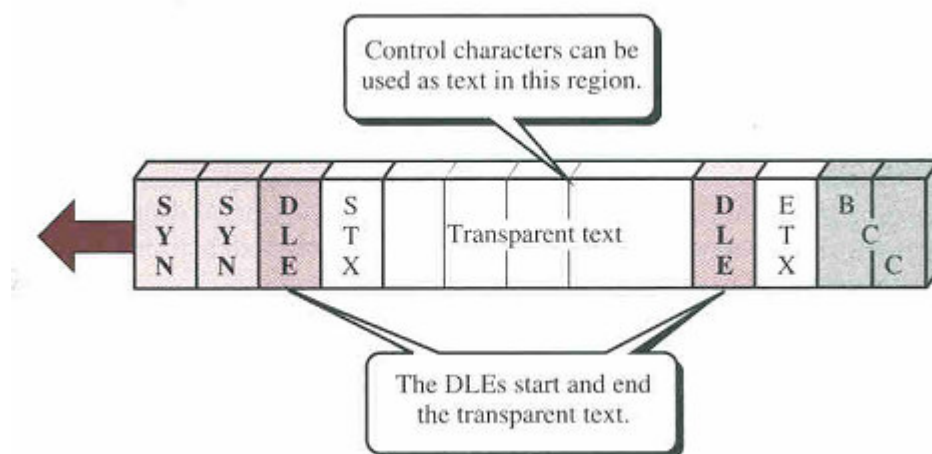


Рис. 12 Заповнення байта

1.2.2. Біт-орієнтовані протоколи

В символно-орієнтованих протоколах, біти групуються у вигляді певних шаблонів – символів. Біт-орієнтовані протоколи можуть запакувати більше

інформації в більш короткі фрейми і уникнути проблем незалежності даних, які є в символно-орієнтованих протоколах.

Враховуючи переваги, які мають біт-орієнтовані протоколи, і відсутність обмежень, притаманних існуючим системам кодування (подібно ASCII), не дивно, що за останні два десятиріччя було розроблено багато різних біт-орієнтованих протоколів, кожний з яких намагався стати стандартом (див. рис. 13). Більшість цих протоколів були комерційними і розроблялися виробниками для підтримки їх власної продукції. Один з них, **HDLC**, є проектом ISO і він став основою для всіх біт-орієнтованих протоколів, які використовуються зараз.

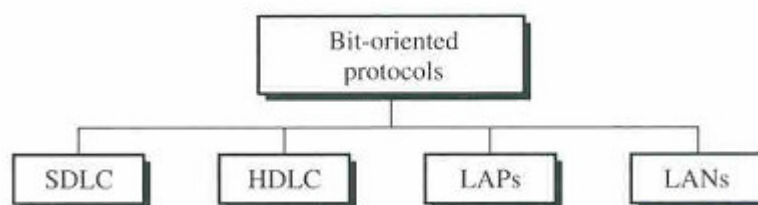


Рис. 13 Біт-орієнтовані протоколи

У 1975 IBM почала розробку біт-орієнтованих протоколу з **синхронним управлінням каналом зв'язку (SDLC)** і намагалася через ISO зробити SDLC стандартом. В 1979 ISO створює протокол з **високорівневим управлінням каналом зв'язку (HDLC)**, який був заснований на SDLC. Ухвалення HDLC комісіями ISO, призвело до його прийняття і розширення іншими організаціями. ІТУ-Т була однією з перших організацій, яка використала стандарт HDLC. З 1981 ІТУ-Т розробила серію протоколів **доступу до зв'язку (link access protocols – LAP)**: LAPB, LAPD, LAPM, LAPX, і т.п.), які повністю відповідають HDLC. Інші протоколи (такі як Frame Relay, PPP та ін.) розроблялися ІТУ-Т і ANSI, і також наслідували HDLC, як це робили більшість протоколів управління доступом до LAN. Коротше кажучи, всі біт-орієнтовані протоколи, які використовуються сьогодні, наслідують HDLC. Отже, вивчивши HDLC, можна зрозуміти роботу інших.

Всі біт-орієнтовані протоколи зв'язані з протоколом високорівневого управління каналом зв'язку (HDLC), який розроблений ISO. HDLC підтримує напівдуплексні і дуплексні режими в двоточкових і багатоточкових конфігураціях.

HDLC

HDLC - це біт-орієнтований протокол канального рівня, розроблений для підтримки як напівдуплексного, так і дуплексного режиму для двоточкових і багатоточкових зв'язків. Системи, що використовують HDLC, можуть характеризуватися типами станції, конфігураціями і режимами відповіді.

Типи станцій

HDLC виділяє три типи станцій: первинний (primary), вторинний (secondary) і змішаний (combined).

Первинна (головна) станція в HDLC функціонує так само, як і первинний пристрій управління потоком даних. Первинна станція - це пристрій в двоточковій або багатоточковій конфігурації, який має повний контроль над зв'язком. Первинна станція відправляє команди **вторинним станціям**. Первинна станція генерує команди; вторинна – відповіді.

Змішана станція може давати як команди, так і відповіді. Комбінована станція - це один з набору сполучених рівнорангових пристроїв, який запрограмований поводитися або як первинна, або як вторинна станція, в залежності від характеру і напрямку передачі.

В HDLC є станції трьох типів: первинна, вторинна і змішана. Первинна станція посилає команди. Вторинна станція – відповіді. Змішана станція посилає як команди, так і відповіді.

Конфігурації

Слово **Конфігурація** звертається до взаємозв'язку апаратних пристроїв у лінії зв'язку. Первинні, вторинні і змішані станції можуть бути сконфігуровані так: незбалансована, симетрична і збалансована конфігурація (див. рис. 14). Будь-яка з цих конфігурацій підтримує напівдуплексну і дуплексну передачу.

Незбалансована конфігурація (також “головний/підлеглий”) - це коли один пристрій первинний, а всі інші є повторними. Незбалансовані конфігурації можуть бути двоточкові, коли сполучені між собою тільки два пристрої; але частіше використовуються багатоточкові, де одна первинна станція управляє декількома вторинними.

Симетрична конфігурація - кожна фізична станція на лінії зв'язку складається з двох логічних станцій: первинної і вторинної. Окремі лінії зв'язують первинну складову однієї фізичної станції з вторинною складовою іншої фізичної станції. Симетрична конфігурація функціонує, як незбалансована конфігурація, за винятком того, що управління зв'язком може передаватися між двома станціями.

Збалансована конфігурація – коли обидві станції в двоточковій топології є змішаного типу. Станції з'єднані єдиною лінією, управління якою може здійснюватися будь-якою станцією.

HDLC не підтримує збалансовану конфігурацію для багатоточкової топології. Для цього необхідно винайти медіа протоколи управління доступом для LAN.

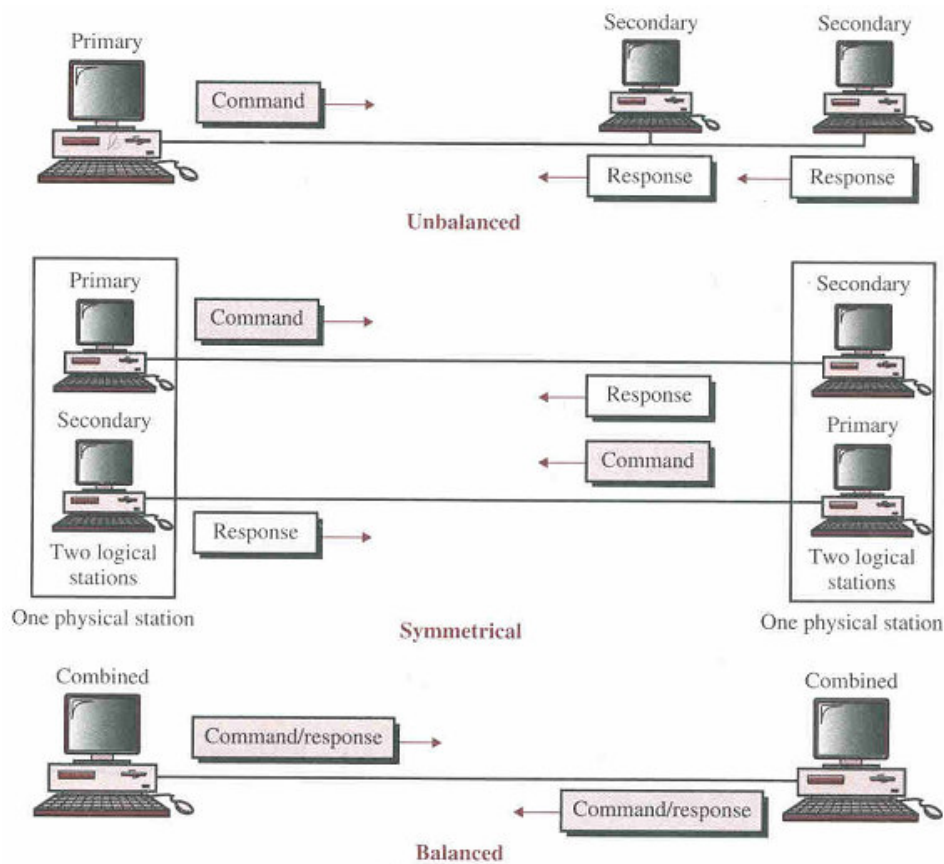


Рис. 14 Типи конфігурацій HDLC

Режими комунікації

В HDLC *режим* - це взаємозв'язок між двома пристроями, залученими до обміну даними; режим описує, хто управляє зв'язком. Обміни в незбалансованих конфігураціях завжди проводяться в нормальному режимі відповіді. Обміни в симетричних або збалансованих конфігураціях можуть проводитися у режимі, що використовує фрейм, який доставляє команди (U-frame). HDLC підтримує

три режими комунікації між станціями: нормальний режим відповіді (NRM), асинхронний режим відповіді (ARM) й асинхронний збалансований режим (ABM).

Нормальний режим відповіді (normal response mode - NRM) відноситься до стандартного взаємозв'язку “первинний/вторинний”. В цьому режимі, вторинний пристрій перед передачею повинен отримати дозвіл на це від первинного пристрою. Як тільки дозвіл отримано, вторинний може ініціювати передачу одного або більше фреймів даних.

В асинхронному режимі відповіді (asynchronous response mode - ARM), вторинний пристрій може ініціювати передачу без дозволу від первинного кожного разу, коли канал незавантажений. ARM не змінює при цьому взаємозв'язок “первинний/вторинний”. Всі передачі від вторинного пристрою (навіть до іншого вторинного на тій самій лінії) повинні бути зроблені до первинного для переключення до станції-одержувача.

В асинхронному збалансованому режимі (asynchronous balanced mode - ABM) всі станції рівні, і тому використовуються тільки комбіновані двоточкові станції. Також комбінована станція може ініціювати передачу з іншими комбінованими станціями без отримання дозволу. Рис. 15 показує взаємозв'язок між цими режимами і типами станцій.

Режими:

Нормальний режим відповіді (NRM)

В асинхронному режимі відповіді (ARM)

В асинхронному збалансованому режимі (ABM)

	NRM	ARM	ABM
Station type	Primary & secondary	Primary & secondary	Combined
Initiator	Primary	Either	Any

Рис. 15 Режими HDLC

Фрейми

Щоб забезпечити гнучкість необхідну для підтримки всіх варіантів, що можливі в описаних вище режимах і конфігураціях, HDLC визначає три види

фреймів: інформаційні **фрейми (I-frames)**, **управляючі фрейми (S-frames)**, і **ненумеровані фрейми (U-frames)**; див. рис. 16. Кожний вид фрейму працює як конверт для передачі певного виду повідомлення. I-frames використовуються для передачі призначених користувачу даних і контрольної інформації, що стосується цих даних. S-frames використовуються тільки для передачі контрольної інформації, що перш за все стосується потік каналного рівня і обробки помилок. U-frames зарезервовані для управління системою. Інформація, яка передається за допомогою U-frames, безпосередньо призначена для управління зв'язком. Кожний фрейм в HDLC може містити аж до шести полів: поле з прапорцем (ознакою) початку, поле адреси, управляюче поле, інформаційне поле, поле фрейму перевірки послідовності (frame check sequence - FCS) і поле з прапорцем закінчення. При передачі багатьох фреймів прапорець кінця одного фрейму може дублювати прапорець початку наступного фрейму.

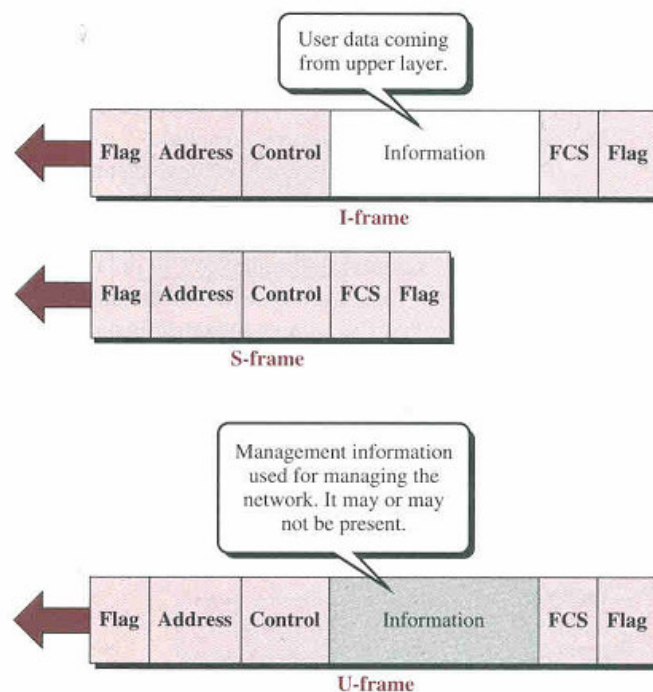


Рис. 16 Типи фреймів HDLC

Поле прапорця

Поле прапорця у фреймі HDLC - це восьми-розрядна послідовність з бітовим шаблоном 01111110, який ідентифікує як початок, так і кінець фрейму, і служить як шаблон синхронізації для одержувача. Рис. 17 показує розміщення двох полів з прапорцями в I-frame.

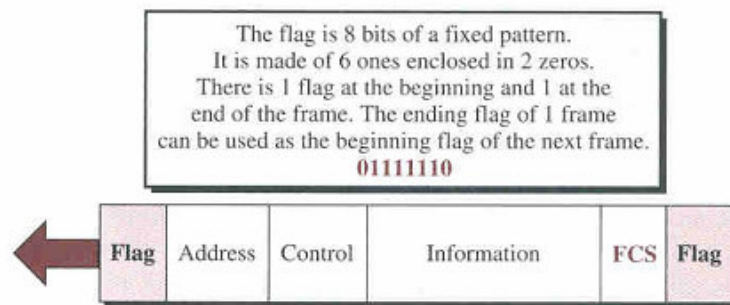


Рис. 17 Поле прапорця HDLC

Поле прапорця в HDLC є найбільш схожим на управляючий символ, і тому може неправильно зчитатися одержувачем. Поле прапорця також може потенційно спричинити проблему незалежності даних. Як тільки станція знаходить прапорець і визначає, що фрейм адресований до неї, вона починає отримання передачі і чекає наступного прапорця, який означає кінець фрейму. Можливо, що бітова послідовність, чи це контрольна інформація, чи дані, може містити 01111110. Якщо такий шаблон зустрінеться в даних, наприклад, то одержувач міг би припустити, що кінець фрейму був досягнутий (із згубними результатами).

Щоб гарантувати, що прапор не з'являється де-небудь в фреймі, HDLC використовує процес під назвою **бітове заповнення (bit stuffing)**. Кожного разу, коли відправник хоче передати бітову послідовність, що містить більш ніж п'ять послідовних 1, він вставляє (заповнює) один надлишковий 0 після п'ятої 1. Наприклад, послідовність 01111111000 стає 0111110111000. Цей надлишковий 0 вставляється не дивлячись чи шостий біт є 1 чи ні. Його присутність говорить одержувачу, що поточна послідовність не є прапорцем. Як тільки одержувач побачив надлишковий 0, він упускається і відновлюється початковий бітовий потік.

Бітове заповнення - це процес додавання одного надлишкового 0 кожного разу, коли в даних зустрічається п'ять послідовних 1, таким чином, щоб одержувач не перепував дані з прапорцем.

Рис. 18 показує бітове заповнення відправником і бітове видалення одержувачем. Відзначте, що навіть якщо ми маємо 0 після п'яти 1, все одно відбувається вставка додаткового 0. Цей 0 буде видалений одержувачем.

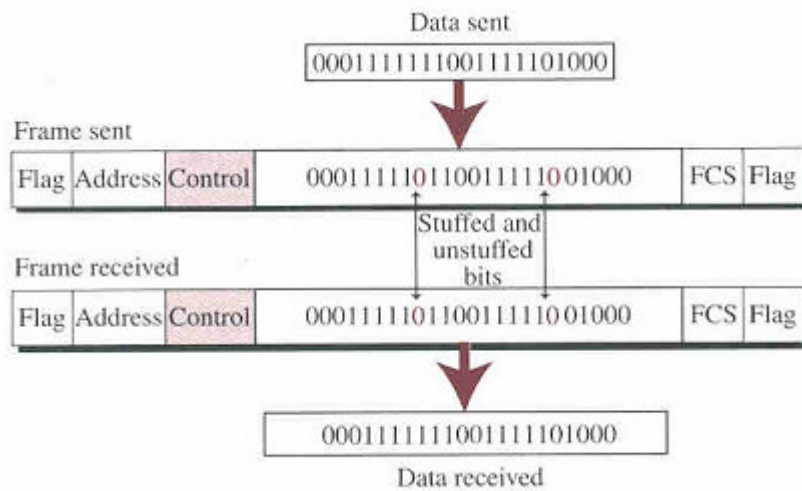


Рис. 18 Бітове заповнення і видалення

За винятком трьох виключень, бітове заповнення потрібне кожного разу, коли п'ять 1 зустрічаються послідовно. Виключення є тоді, коли бітова послідовність дійсно є прапорцем, коли передача переривається, і коли канал переводиться в режим простою. Діаграма на рис. 19 показує дії, які виконує одержувач, щоб ідентифікувати і відкинути надлишковий біт. Поки одержувач читає біти, він підраховує 1. Коли він знаходить п'ять послідовних 1 після 0, він перевіряє наступний (сьомий) біт. Якщо сьомий біт є 0, то одержувач визнає його як заповнений біт і відкидає, обнулюючи при цьому свій лічильник. Якщо сьомий біт 1, то одержувач перевіряє восьмий біт. Якщо восьмий біт 0, то послідовність визнається прапорцем і відповідно обробляється. Якщо восьмий біт це 1, то одержувач продовжує підрахунок. Послідовність, що включає 7-14 послідовних 1, означає відміну передачі. Якщо 15 і більше – то канал в режимі простою.

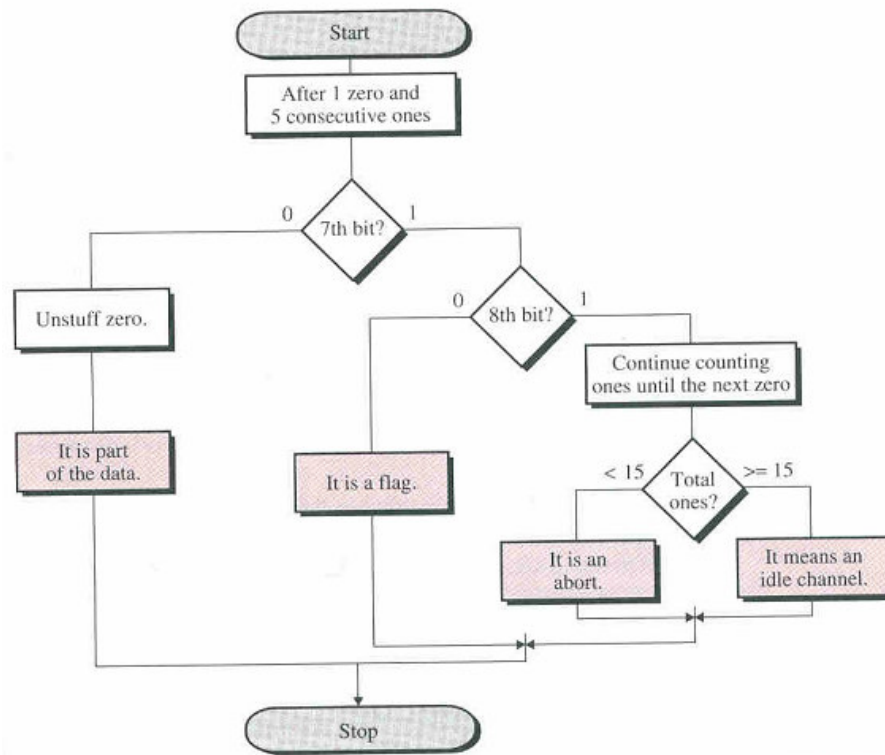


Рис. 19 Бітове заповнення в HDLC

Поле адреси

Друге поле фрейму HDLC містить адресу вторинної станції, яка є джерелом або місцем призначення фрейму (або станція діє як вторинна у випадку комбінованих станцій). Якщо первинна станція створює фрейм, то це поле містить “кому”-адресу. Якщо вторинна станція створює фрейм, то це поле містить “від кого”-адресу. Поле адреси може бути одним або декількома байтами, залежно від потреб мережі. Один байт може ідентифікувати до 128 станцій (тому що один біт використовується для іншої мети). Більші мережі вимагають декілька байт для адресації. Рис. 20 показує розміщення поля адреси відносно решти частин фрейму.

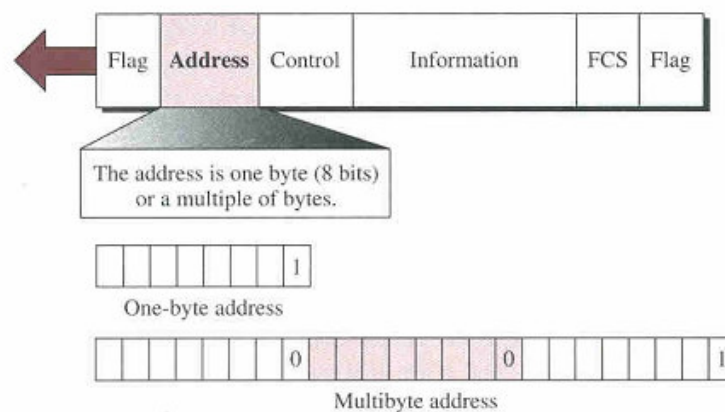


Рис. 20 Поле адреси HDLC

Якщо поле адреси це тільки один байт, то останній біт завжди рівний 1. Якщо адреса складається з декількох байтів, то всі байти крім останнього закінчуються 0; тільки останній – 1. Закінчення кожного проміжного байту 0, вказує одержувачу, що поле адреси містить декілька байтів.

Управляюче поле

Управляюче поле - це одно- або дво-байтовий сегмент фрейму, що використовується для управління потоком. Спочатку обговорюється однобайтовий сегмент, а потім двобайтовий (розширений режим).

Управляючі поля розрізняються в залежності від типу фрейму. Якщо перший біт управляючого поля 0, то це I-фрейм. Якщо перший біт 1, а другий 0, то це S-фрейм. Якщо перші два біти рівні 1, то це U-фрейм. Управляючі поля всіх трьох видів фреймів містять біт опитування/висновку (**poll/final – P/F bit**).

I-фрейм містить два 3-бітові потоки і послідовності обробки помилок, які називаються N(S) і N(R). N(S) конкретизує кількість посланих фреймів (його власний ідентифікаційний номер). N(R) вказує на кількість очікуваних фреймів в двосторонньому обміні: тому N(R) - це поле підтвердження. Якщо останній отриманий фрейм не містив помилок, то номер N(R) буде рівний номеру наступного фрейму в послідовності. Якщо останній фрейм не був отриманий коректно, то номер N(R) - це номер пошкодженого фрейму, чим вказується на необхідність його повторної передачі.

Управляюче поле S-фрейму містить поле N(R), але в ньому відсутнє поле N(S). S-фрейми використовуються, щоб повернути N(R), коли одержувач не має для передачі власних даних. В іншому випадку підтвердження міститься в управляючому полі I-фрейму. S-фрейми не передають дані, і тому не потребують N(S) для їх ідентифікації. Два біти, що передують біту P/F в S-фреймі, використовуються для того, щоб пересилати закодований потік і інформацію для обробки помилок.

U-фрейми не мають ні N(S), ні N(R), тому що вони не призначені для обміну даними користувача або підтвердженнями. Натомість, U-фрейми мають два поля коду. Ці коди використовуються, щоб визначити вид U-фрейму і його функцію

(наприклад, встановити режим обміну). Управляючі поля всіх трьох видів фреймів показано на рис. 21.

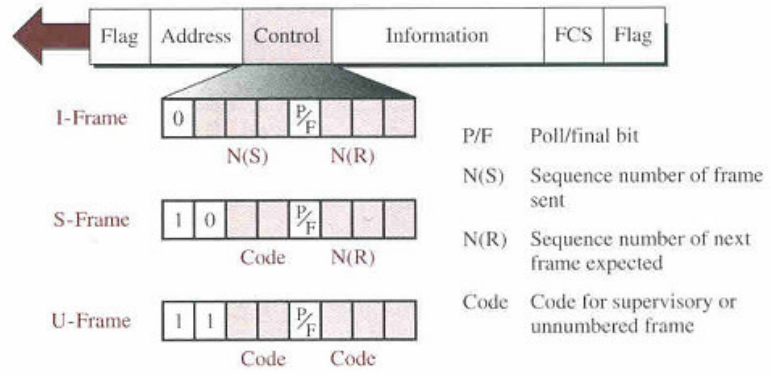


Рис. 21 Управляючі поля HDLC

10.2. Структура стандартів IEEE 802.x

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

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

Стандарти сімейства IEEE 802.x охоплюють тільки два нижні рівні семирівневої моделі OSI – фізичний і канальний. Це зв'язано з тим, що саме ці рівні найбільшою мірою відображають специфіку локальних мереж. Старші ж рівні, починаючи з мережним, в значній мірі мають загальні риси як для локальних, так і для глобальних мереж.

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

- логічної передачі даних (Logical Link Control, LLC);
- управління доступом до середовища (Media Access Control, MAC).

Рівень MAC з'явився через існування в локальних мережах розподіленого середовища передачі даних. Саме цей рівень забезпечує

коректне сумісне використання загального середовища, надаючи її відповідно до певного алгоритму в розпорядження тієї або іншої станції мережі. Після того, як доступ до середовища отриманий, нею може користуватися більш високий рівень – рівень LLC, організуючий передачу логічних одиниць даних, кадрів інформації, з різним рівнем якості транспортних послуг. В сучасних локальних сітках отримали розповсюдження декілька протоколів рівня MAC, що реалізують різні алгоритми доступу до середовища, що розділяється. Ці протоколи повністю визначають специфіку таких технологій, як Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

Рівень LLC відповідає за передачу кадрів даних між вузлами з різним ступенем надійності, а також реалізує функції інтерфейсу з прилеглим до нього мережним рівнем. Саме через рівень LLC мережний протокол запрошує у канального рівня потрібну йому транспортну операцію з потрібною якістю. На рівні LLC існує декілька режимів роботи, відмінних наявністю або відсутністю на цьому рівні процедур відновлення кадрів у разі їх втрати або спотворення, тобто відмінних якістю транспортних послуг цього рівня.

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

Стандарти IEEE 802 мають достатньо чітку структуру, приведену на рис. 3.1:

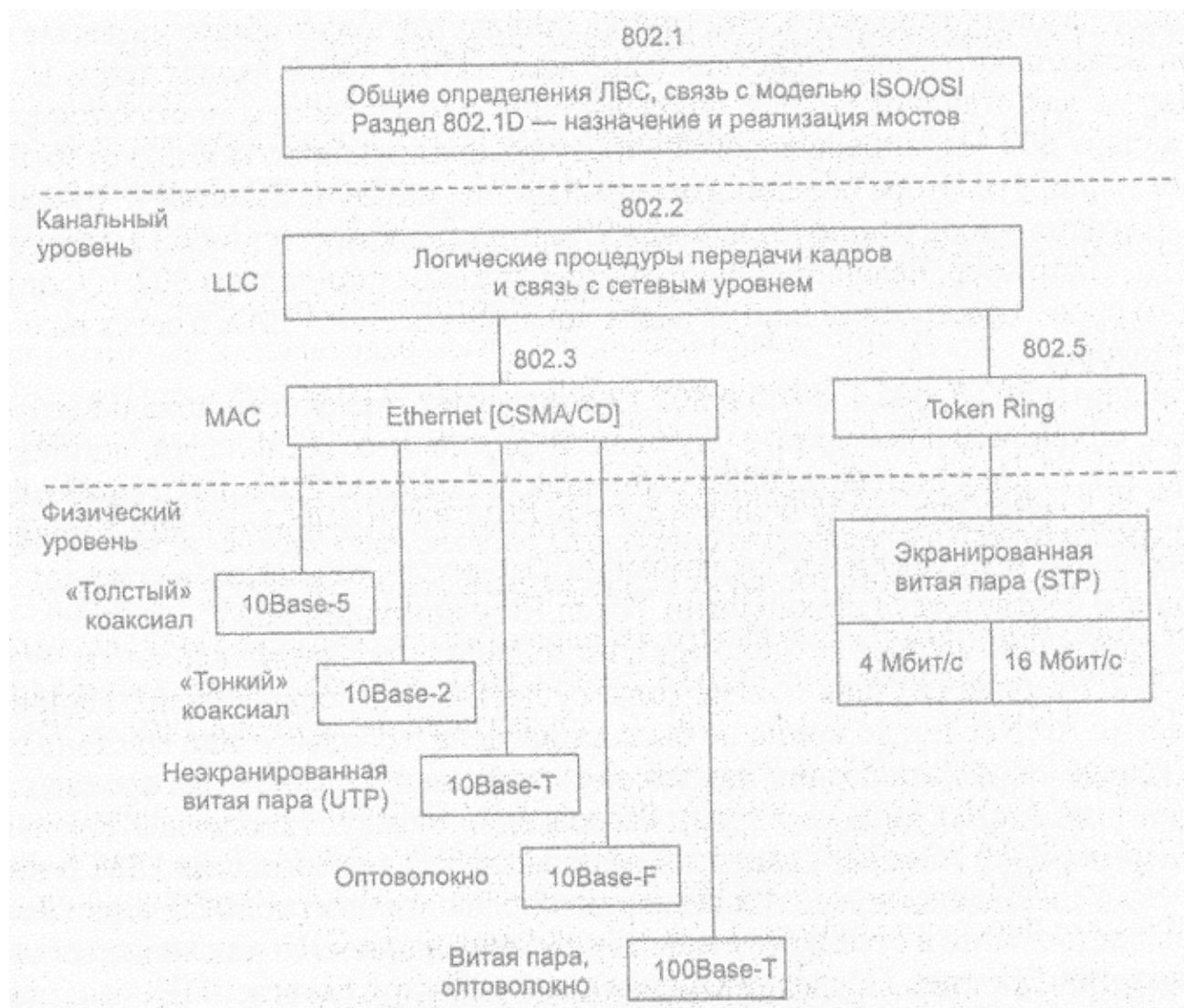


Рис. 3.1. Структура стандартів IEEE 802.x

Ця структура з'явилася в результаті великої роботи, проведеної комітетом 802 по виділенню в різних фірмових технологіях загальних підходів і загальних функцій, а також узгодженню стилів їх опису. В результаті каналний рівень був розділений на два згадані підрівні. Опис кожної технології розділений на дві частини: опис рівні MAC і опис фізичного рівня. Як видно з рис., практично у кожній технології єдиному протоколу рівня MAC відповідає декілька варіантів протоколів фізичного рівня (на рис. в цілях економії місця приведені тільки технології EtherNet і

Token Ring, але все сказане справедливо також і для решти технологій, таких як ArcNet, FDDI, 100VG-AnyLAN).

Над канальним рівнем всіх технологій зображений загальний для них протокол LLC, що підтримує декілька режимів роботи, але незалежний від вибору конкретної технології. Стандарт LLC займається підкомітетом 802.2. Навіть технології, стандартизовані не в рамках комітету 802, орієнтуються на використання протоколу LLC, визначеного стандартом 802.2, наприклад протокол FDDI, стандартизований ANSI.

Осібнo стоять стандарти, що розробляються підкомітетом 802.1. Ці стандарти носять загальний для всіх технологій характер. В підкомітеті 802.1 були розроблені загальні визначення локальних мереж і їх властивостей, визначений зв'язок трьох рівнів моделі IEEE 802 з моделлю OSI. Але найбільш практично важливими є стандарти 802.1, які описують взаємодію між собою різних технологій, а також стандарти по побудові складніших мереж на основі базових топологій. Ця група стандартів носить загальну назву стандартів міжмережевої взаємодії (internetworking). Сюди входять такі важливі стандарти, як стандарт 802.ID, що описує логіку роботи моста/комутатора, стандарт 802.1H, визначаючий роботу транслуючого моста, який може без маршрутизатора об'єднувати мережі Ethernet і FDDI, Ethernet і Token Ring і т.п. Сьогодні набір стандартів, розроблених підкомітетом 802.1, продовжує рости. Наприклад, недавно він поповнився важливим стандартом 802.1Q, визначаючим спосіб побудови віртуальних локальних мереж VLAN в мережах на основі комутаторів.

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

Corporation, а стандарт 802.5 в основному відповідає технології Token Ring компанії IBM.

Початкові фірмові технології і їх модифіковані варіанти – стандарти 802.x у ряді випадків довгі роки існували паралельно. Наприклад, технологія ArcNet так до кінця не була приведена у відповідність із стандартом 802.4 (тепер це робити пізно, оскільки десь приблизно з 1993 року виробництво устаткування ArcNet було згорнуто). Розбіжності між технологією Token Ring і стандартом 802.5 теж періодично виникають, оскільки компанія IBM регулярно вносить удосконалення в свою технологію і комітет 802.5 відображає ці удосконалення в стандарті з деяким запізненням. Виняток становить технологія Ethernet. Останній фірмовий стандарт Ethernet DIX був прийнятий в 1980 році, і з тих пір ніхто більше не робив спроб фірмового розвитку Ethernet. Всі новини в сімействі технологій Ethernet вносяться тільки в результаті ухвалення відкритих стандартів комітетом 802,3.

Більш пізні стандарти спочатку розроблялися не однією компанією, а групою зацікавлених компаній, а потім передавалися у відповідний підкомітет IEEE 802 для затвердження. Так відбулося з технологіями Fast Ethernet, 100VG-AnyLAN, Gigabit Ethernet. Група зацікавлених компаній утворювала спочатку невелике об'єднання, а потім у міру розвитку робіт до нього приєднувалися інші компанії, так що процес ухвалення стандарту носив відкритий характер.

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

802.1 – Internetworking – об'єднання мереж;

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

802.3 – Ethernet з методом доступу CSMA/CD;

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

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

802.6 – Metropolitan Area Network, MAN – мережі мегаполісів;

802.7 – Broadband Technical Advisory Group – технічна консультаційна група по широкосмуговій передачі;

802.8– Fiber Optic Technical Advisory Group – технічна консультаційна група по волоконно-оптичних мережах;

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

802.10– Network Security – мережна безпека;

802.11– Wireless Networks – безпроводні мережі;

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

Тема 11. Проблема розподілу каналу і протоколи колективного доступу

11.1. Проблема розподілу каналу

11.1.1 Статичний розподіл каналу в локальних і регіональних мережах

11.1.2 Динамічний розподіл каналу в локальних і регіональних мережах

11.2. Протоколи колективного доступу

11.2.1 Протокол ALOHA

11.2.2 Протокол вільного доступу з контролем несучої

11.2.2.1 Наполегливий і ненаполегливий CSMA

11.2.2.2 CSMA з виявленням конфліктів

11.2.3 Протоколи без зіткнень

11.2.3.1 Протокол бітової карти

11.2.3.2 Двійковий зворотній відлік

11.2.4 Протоколи з обмеженою конкуренцією

11.2.4.1 Загальні відомості

11.2.4.2 Протокол адаптивного проходу по дереву

11.2.5 Протоколи вільного доступу зі спектральним розподілом

11.2.6 Протоколи безпроводових локальних мереж

11.2.6.1 Загальні відомості

11.2.6.2 Протоколи MACA і MACAW

11.1. Проблема розподілу каналу

Всі мережні технології можуть бути розділені на дві категорії: використовуючі з'єднання від вузла до вузла і мережі із застосуванням ширококомовлення. Цей розділ присвячений ширококомовним мережам і їх протоколам.

Головною проблемою будь-яких ширококомовних мереж є питання про те, як визначити, кому надати канал, якщо користуватися ним одночасно хочуть декілька комп'ютерів. Для прикладу уявіть собі конференцію, в якій беруть участь шести чоловік, причому кожний використовує свій телефон. Всі вони сполучені таким чином, що кожний може чути всіх інших. Мабуть, що коли один з них закінчить свою мову, відразу двоє або троє почнуть говорити одночасно, тим самим створивши ніякову ситуацію. При особистій зустрічі подібним проблемам запобігає зовнішніми засобами, наприклад підняттям руки для отримання дозволу говорити. Коли доступний лише один канал, визначити, хто може говорити наступним, значно важче. Для вирішення цієї проблеми розроблено багато протоколів, які і обговорюватимуться в даному розділі. В літературі ширококомовні канали іноді називають **каналами з множинним доступом**, або **каналами з довільним доступом**.

Протоколи, що застосовуються для визначення того, хто говоритиме наступним, відносяться до підрівня рівня передачі даних, званому MAC (Medium Access Control – управління доступом до середовища). Підрівень MAC особливо важливий в локальних мережах, оскільки майже всі вони використовують канал множинного доступу. В глобальних мережах, навпаки, застосовуються двоточкові з'єднання. Виключенням є тільки супутникові мережі. Оскільки канали множинного доступу тісно пов'язані з локальними мережами, в даному розділі в основному описуватимуться локальні мережі, а також деякі питання, напряму не пов'язані з темою підрівня MAC.

Технічно підрівень управління доступом до середовища є нижньою частиною рівня передачі даних, тому доцільніше було б вивчити спочатку його, а потім протоколи «крапка– крапка, розглянуті на чолі 3. Проте,

більшості людей зрозуміти протоколи, що включають багато учасників, легше після того, як добре вивчені протоколи з двома учасниками. З цієї причини при розгляді рівнів ми злегка відхилилися від строгого проходження від низу до верху по ієрархічним сходам.

Центральною проблемою, обговорюваною в цій темі, є розподіл одного широкомовного каналу між численними користувачами, що претендують на нього. Спочатку ми у загальних рисах розглянемо статичні і динамічні схеми розподілу каналу. Потім обговоримо декілька конкретних алгоритмів.

11.1.1 Статичний розподіл каналу в локальних і регіональних мережах

Традиційним способом розподілу одного каналу – наприклад, телефонного кабелю – між численними конкуруючими користувачами є FDM (Frequency Division Multiplexing – частотне ущільнення). За наявності N користувачів смуга пропускання ділиться на N діапазонів однакової ширини (див. мал. 2.27), і кожному користувачу надається один з них. Оскільки при такій схемі біля кожного опиняється свій особистий частотний діапазон, то конфлікту між користувачами не виникає. При невеликій кількості абонентів, кожному з яких потрібна постійна лінія зв'язку (наприклад, комутатори операторів зв'язку), частотне ущільнення надає простий і ефективний механізм розподілу.

Проте при великій і постійно змінній кількості відправників даних або пульсуючому трафіку частотне ущільнення не може забезпечити достатньо ефективний розподіл каналу. Якщо кількість користувачів в який-небудь момент часу менше числа діапазонів, на які роздільний спектр частот, то велика частина спектру не використовується і витрачається даремно. Якщо, навпаки, кількість користувачів виявиться більше числа доступних діапазонів, то деяким доведеться відмовити в доступі до каналу, навіть якщо абоненти, вже що захопили його, майже не використовуватимуть пропускну спроможність.

Проте навіть якщо припустити, що кількість користувачів можна якимсь способом утримувати на постійному рівні, те розділення каналу на статичні

підканали все одно є неефективним. Основна проблема тут полягає в тому, що якщо якась частина користувачів не користується каналом, то ця частина спектру просто пропадає. Вони самі при цьому займають лінію, не передаючи нічого, і іншим не дають передати дані. Крім того, в більшості комп'ютерних систем трафік є надзвичайно нерівномірним (цілком звичайним є відношення пікового трафіку до середнього як 1000:1). Отже, велику частину часу велика частина каналів не використовується.

Те, що характеристики статичного частотного ущільнення виявляються невдалими, можна легко продемонструвати на прикладі простих обчислень теорії масового обслуговування. Спершу злічимо середній час затримки T для каналу з пропускною спроможністю C бит/с, по якому прибувають X кадрів в секунду. Довжина кадрів є випадковою величиною з експоненціально розподіленою густиною вірогідності, середнє значення якої рівно $1/\lambda$ біта на кадр. При таких параметрах швидкість прибуття складає X кадрів в секунду, а швидкість обслуговування – μC кадрів в секунду. Теорія масового обслуговування говорить про те, що пуассонівський час прибуття і обслуговування рівний

$$T = \frac{1}{\mu C - \lambda}.$$

Хай, наприклад, пропускна спроможність C рівна 100 Мбіт/с, середня довжина кадру $1/\lambda = 10\,000$ біт, швидкість прибуття кадрів $X = 5000$ кадрів в секунду. Тоді $T = 200$ мкс. Зверніть увагу: якби ми не врахували затримки при формуванні черги і просто порахували, скільки часу потрібно на передачу кадру завдовжки 10 000 біт по мережі з пропускною спроможністю 100 Мбіт/с, то отримали б неправильну відповідь: 100 мкс. Це число прийнятне лише за відсутності боротьби за канал.

Тепер давайте розділимо канал на N незалежних підканалів, у кожного з яких буде пропускна спроможність C/N бит/с. Середня вхідна швидкість в кожному підканалі тепер буде рівна X/N кадрів в секунду. Знайшовши нове значення середньої затримки T , отримаємо:

$$T_{\text{FDM}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT. \quad (1)$$

Це означає, що при використанні частотного ущільнення значення середньої затримки стало в N раз гірше за значення, яке було б в каналі, якби всі кадри були якимсь чарівним чином організовані в одну загальну чергу.

Ті ж самі аргументи застосовні і до тимчасового ущільнення (TDM, Time Division Multiplexing – мультиплексна передача з тимчасовим розділенням). Кожному користувачу в даному випадку статично виділяється N -й інтервал часу. Якщо інтервал не використовується абонентом, то він просто пропадає. З тим же успіхом можна розділити мережі фізично. Якщо узяти 100-мегабітну мережу і зробити з неї десять 10-мегабітних, статично розподіливши по них користувачів, то в результаті середня затримка зросте з 200 мкс до 2 мс.

Таким чином, жоден статичний метод розподілу каналів не годиться для пульсуючого трафіку, тому далі ми розглянемо динамічні методи.

11.1.2 Динамічний розподіл каналу в локальних і регіональних мережах

Перш ніж приступити до розгляду численних методів розподілу каналів, слід ретельно сформулювати вирішувану проблему. В основі всіх розробок в даній області лежать наступні п'ять допущень.

1. Станційна модель. Модель складається з N незалежних **станцій** (комп'ютерів, телефонів, персональних засобів зв'язку і т. д.), в кожній з яких програма користувача формує кадри для передачі. Станції іноді називають **терміналами**. Вірогідність формування кадру в інтервалі часу Δt рівна $\lambda \Delta t$, де λ є константою (швидкість прибуття нових кадрів). Як тільки кадр сформований, станція блокується і ніщо не робить, поки кадр не буде успішно переданий.

2. Припущення про єдиний канал. Єдиний канал доступний для всіх. Всі станції можуть передавати і приймати дані по ньому. З погляду апаратури всі станції вважаються рівними, хоча програмно протокол може

встановлювати для них різні пріоритети.

3. Допущення про колізії. Якщо два кадри передаються одночасно, вони перекриваються за часом, в результаті сигнал спотворюється. Така подія називається конфліктом, або колізією. Всі станції можуть знаходити конфлікти. Спотворений унаслідок конфлікту кадр повинен бути переданий повторно. Інших помилок, окрім тих, які викликані конфліктами, ні.

4а. Безперервний час. Передача кадрів може початися у будь-який момент часу. Не існує ніяких синхронізуючих імпульсів, які ділили б час на дискретні інтервали.

4б. Дискретний час. Час розділений на дискретні інтервали (такти). Передача кадру може початися тільки з початком такту. Один часовий інтервал може містити 0, 1 або більш кадрів, що відповідає вільному інтервалу, успішній передачі кадру або колізії.

5а. Контроль несучої. Станції можуть визначити, вільна або зайнята лінія, до її використання. Якщо канал зайнятий, станції не намагатимуться передавати кадри по ньому, поки він не звільниться.

5б. Відсутність контролю несучої. Станції не можуть визначити, вільна або зайнята лінія, поки не спробують її використовувати. Вони просто починають передачу. Тільки потім вони можуть визначити, чи була передача успішною.

По приведених раніше допущення слід сказати декілька слів. Перше допущення затверджує, що станції незалежні і працюють з постійною швидкістю. Також неявно передбачається, що у кожній станції є тільки один користувач або програма, тому поки станція заблокована, вона не проводить ніякої роботи. Складніші моделі розглядають багатопрограмні станції, які можуть працювати в заблокованому стані, проте і аналіз подібних станцій набагато складніше.

Допущення про єдиний канал є, насправді, центральним в даній моделі. Ніяких зовнішніх каналів зв'язку немає. Станції не можуть тягнути руки, повертаючи до себе увагу і переконуючи вчителя запитати їх.

Допущення про колізії також є основним, хоча в деяких системах (особливо в системах з розширеним спектром) дане допущення звучить не так строго, що приводить до несподіваних результатів. Крім того, в деяких локальних мережах, наприклад в мережі *token ring* (маркерне кільце), застосовується механізм дозволу колізій, реалізований за рахунок спеціальних пакетів - маркерів, що передаються від станції до станції. Поміщати в канал кадр може тільки той, у кого в даний момент знаходиться маркер. Далі ми обговоримо модель моноканалу з конкуренцією і колізіями.

Для часу існує два альтернативні допущення. В одних системах час може бути безперервним (4а), в інших – дискретним, тому ми розглянемо обидва варіанти.

Аналогічно цьому, контроль несучої також реалізований не у всіх системах. Станції локальних мереж звичайно знають, коли лінія зайнята, проте в беспровідних мережах контролю несучої нема, тому що окремо взята станція не може «чути» всі інші через різницю частотних діапазонів. Станції провідних мереж з контролем несучої можуть припиняти власну передачу, знайшовши колізію. Зверніть увагу на слово «несуча». В даному випадку воно означає електричний сигнал, що розповсюджується по каналу.

11.2. Протоколи колективного доступу

Відомі багато алгоритмів колективного доступу. В наступних розділах будуть розглянуті найцікавіші алгоритми і дані приклади їх вживання.

11.2.1 Протокол ALOHA

В 70-х роках Норман Абрамсон (Norman Abramson) і його колеги з Гавайського університету розробили новий елегантний метод рішення проблеми розподілу каналів. Їх праці згодом стали основою багатьох досліджень (Abramson, 1985). Хоча в роботі Абрамсона, що отримала назву ALOHA, використовувався широкомовний радіозв'язок із стаціонарними передавачами, основна ідея застосовна до будь-якої системи, в якій незалежні користувачі змагаються за право використання одного загального каналу.

В даному розділі ми розглянемо дві версії системи ALOHA: чисту і дискретну. Вони відрізняються тим, чи ділиться час на дискретні інтервали, протягом яких передаються кадри, чи ні. В чистій системі ALOHA не потрібна загальна синхронізація часу, а в дискретній потрібен.

Чиста система ALOHA

В основі системи ALOHA лежить проста ідея: дозволити користувачам передачу, як тільки у них з'являються дані для відсилання. Звичайно, при цьому будуть зіткнення, і кадри, що зіткнулися, будуть зруйновані. Проте завдяки властивості зворотного зв'язку широкомовної системи відправник завжди може встановити, чи дійшов його кадр до одержувача або був зруйнований. Для цього йому потрібно просто прослуховувати канал, як це робить вся решта користувачів. В локальних мережах зворотний зв'язок миттєвий, а в супутникових системах існує затримка в 270 мс, і лише після цього відправник може взнати, наскільки

успішною була передача. Якщо кадр був знищений, відправник просто вичікує деякий випадковий час і намагається переслати цей кадр знову. Час очікування повинен бути випадковим. В іншому випадку при рівних фіксованих інтервалах часу очікування колізії повторюватимуться знову і знову. Системи, в які декількох користувачів використовують один загальний канал у такий спосіб, що час від часу виникають конфлікти, називаються **системами з конкуренцією**.

На рис. 1 показаний приклад формування кадрів в системі АЛОНА. Всі кадри на нашому малюнку мають один розмір, оскільки при цьому пропускна спроможність системи зроблена максимальною саме за рахунок фіксованого розміру кадрів.



Рис. 1. В чистій системі АЛОНА кадри передаються в абсолютно довільний час

Коли два кадри одночасно намагаються зайняти канал, вони стикаються і знищуються. Навіть якщо тільки один перший біт другого кадру перекривається останнім бітом першого кадру, обидва кадри знищуються

повністю. При цьому обидва кадри буде передано пізніше повторно. Контрольна сума не може (і не повинна) відрізняти повну втрату інформації від часткової. Втрата є втрата.

Найцікавішим в даній ситуації є питання про ефективність каналу системи АЛОНА. Іншими словами, яка частина всіх передаваних кадрів здатна уникнути колізій за будь-яких обставин? Спочатку розглянемо нескінченну безліч інтерактивних користувачів, що сидять за своїми комп'ютерами (станціями). Користувач завжди знаходиться в одному з двох станів: введення з клавіатури і очікування. Спочатку всі користувачі знаходяться в стані введення. Закінчивши набір рядка, користувач перестає вводити текст, чекаючи відповіді. В цей час станція передає кадр, що містить набраний рядок, і опитує канал, перевіряючи успішність передачі кадру. Якщо кадр переданий успішно, користувач бачить відповідь і продовжує набір. В осоружному випадку користувач чекає, поки кадр не буде переданий.

Хай «час кадру» означає інтервал часу, потрібний для передачі стандартного кадру фіксованої довжини (тобто довжину кадру, ділену на швидкість передачі даних). На даний момент ми припускаємо, що нескінченна кількість користувачів породжує нові кадри, розподілені по Пуасону з наступним середнім значенням: N кадрів за час кадру. (Допущення про нескінченну кількість користувачів необхідне для того, щоб гарантувати, що величина N не стане зменшуватися у міру блокування користувачів.) Якщо $N > 1$, це означає, що співтовариство користувачів формує кадри з більшою швидкістю, ніж може бути передано по каналу, і майже кожний кадр страждатиме від зіткнень. Ми припускатимемо, що $0 < JV < 1$.

Крім нових кадрів, станції формують повторні передачі кадрів, потерпілих від зіткнень. Допустимий також, що вірогідність до спроб передачі старих і нових кадрів за час кадру також має пуасонівський розподіл з середнім значенням G за час кадру. Очевидно, що $G \wedge N$. При малому завантаженні каналу (тобто при $N \ll Q$)

зіткнень буде мало, тому буде мало і повторних передач, тобто $G \cdot N$. При великому завантаженні каналу зіткнень буде багато, а отже, $G > N$. Яка б ні було навантаження, продуктивність каналу S буде рівна пропонованому завантаженню G , помноженому на вірогідність успішної передачі, тобто $S = GP_0$, де P_0 – вірогідність того, що кадр не постраждає в результаті колізії.

Кадр не постраждає від колізії в тому випадку, якщо протягом інтервалу часу його передачі не буде послано більше жодного кадру, як показано на рис. 2. За яких умов затінений кадр буде переданий без пошкоджень? Хай t – цей час, що вимагається для передачі кадру. Якщо який-небудь користувач сформує кадр в інтервалі часу між t_0 і $t_0 + 1$, то кінець цього кадру зіткнеться з початком затіненого кадру. При цьому доля затіненого кадру вирішена наперед ще до того, як буде посланий його перший біт, проте, оскільки в чистій системі ALOHA станції не прослуховують канал до початку передачі, у них немає способу взнати, що канал зайнятий і по ньому вже передається кадр. Аналогічним чином будь-який інший кадр, передача якого почнеться в інтервалі від $t_0 + 1$ до $t_0 + 2t$, зіткнеться з кінцем затіненого кадру.

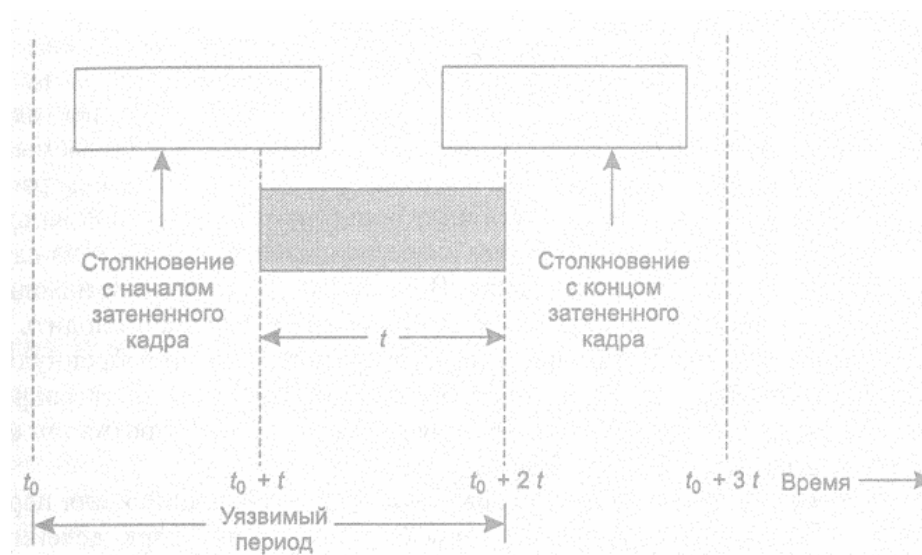


Рис. 2. Небезпечний інтервал часу для затіненого кадру

Вірогідність того, що протягом часу кадру буде сформовано δ_0 кадрів, можна обчислити по формулі розподілу Пуассона:

$$\text{Pr}[k] = \frac{G^k e^{-G}}{k!}. \quad (2)$$

Таким чином, вірогідність формування нуля кадрів протягом цього інтервалу часу рівна e^{-G} . Середня кількість кадрів, сформованих за інтервал часу завдовжки в два кадри, рівно $2G$. Вірогідність того, що ніхто не почне передачу протягом всього небезпечного періоду, рівна $P_0 = e^{-2G}$. Враховуючи, що $S = GP_0$, одержуємо:

$$S = Ge^{-2G}.$$

Залежність продуктивності каналу від пропонованого трафіку показана на рис. 3. Максимальна продуктивність досягає значення $S = 1/2e$, що приблизно рівно 0,184 при $G = 0,5$. Іншими словами, краще, на що ми можемо сподіватися, – це використовувати канал на 18 %. Цей результат дещо розчаровує, проте у разі, коли кожний передає, коли хоче, важко чекати стовідсоткового успіху.

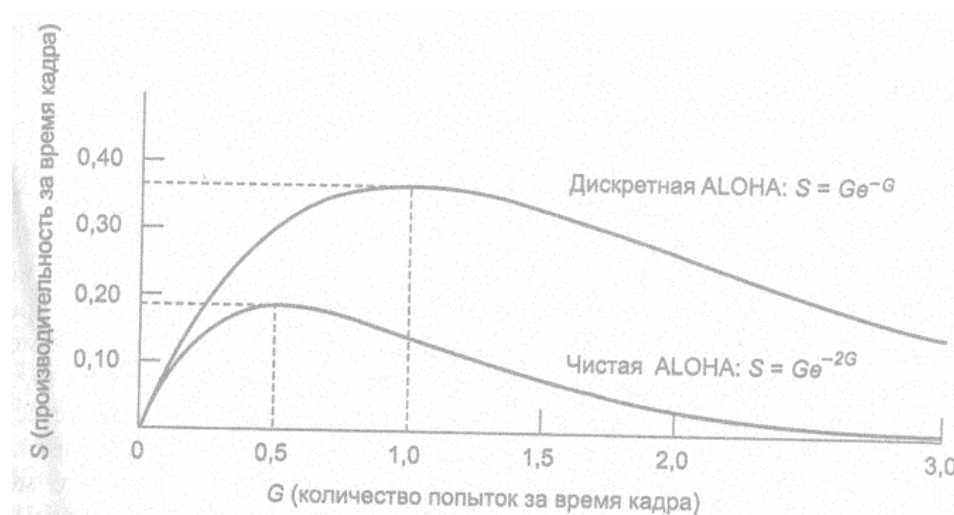


Рис. 3. Залежність продуктивності каналу від пропонованого трафіку для систем ALOHA

Дискретна система ALOHA

В 1972 р. Роберті (Roberts) опублікував опис методу, що дозволяє подвоїти продуктивність систем ALOHA (Roberts, 1972). Його пропозиція полягала в розділенні часу на дискретні інтервали, відповідні часу одного кадра. При такому підході користувачі повинні згодитися з певними тимчасовими обмеженнями. Одним із

способів досягнення синхронізації є установка спеціальної станції, що випускає синхронізуючий сигнал на початку кожного інтервалу.

В системі Робертса, відомій під назвою **дискретна ALOHA**, на відміну від **чистої системи ALOHA** Абрамсона, комп'ютер не може починати передачу відразу після натиснення користувачем клавіші Enter. Натомість він повинен дочекатися початку нового такту. Таким чином, безперервна чиста система ALOHA перетворюється на дискретну. Оскільки небезпечний часовий інтервал тепер стає в два рази коротше, вірогідність відсутності передачі по каналу за той же інтервал часу, протягом якого передається тестовий кадр, рівна e^{-c} . В результаті одержуємо:

$$S = Ge^{-G}. \quad (3)$$

Як видно з рис. 3, дискретна система ALOHA має пік при $G = 1$. При цьому продуктивність каналу складає $S = 1/e$, що приблизно рівно 0,368, тобто в два рази більше, ніж в чистій системі ALOHA. Для дискретної системи ALOHA в оптимальній ситуації 37 % інтервалів будуть порожніми, 37 % – з успішно переданими кадрами і 26 % – з кадрами, що зіткнулися. При збільшенні кількості спроб передачі в одиницю часу G кількість порожніх інтервалів зменшується, але збільшується кількість конфліктних інтервалів. Щоб побачити, наскільки швидко росте кількість конфліктних інтервалів, розглянемо передачу тестового кадру. Вірогідність того, що він уникне зіткнення, рівна e^{-c} . Фактично, це вірогідність того, що вся решта користувачів мовчатиме протягом даного тактового інтервалу. Таким чином, вірогідність зіткнення рівна $1 - e^{-G}$. Вірогідність передачі кадру рівно за до спроб (тобто після до - 1 зіткнення, за якими послідує успішна передача), рівна

$$P_k = e^{-G}(1 - e^{-G})^{k-1}.$$

Очікуване число спроб передачі для одного кадру рівно

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1-e^{-G})^{k-1} = e^G.$$

Оскільки число спроб передачі для одного кадру E експоненціально за висить від кількості спроб передачі в одиницю часу G , невелике збільшення навантаження в каналі може сильно понизити його продуктивність.

Дискретна система ALOHA надзвичайно важлива з однієї причини, яка на перший погляд не здається очевидною. Вона з'явилася в 1970-х роках, застосовувалася в деяких експериментальних системах, потім була майже забута. Коли був винайдений метод доступу в Інтернет по кабельних мережах, знов виникла проблема розподілу єдиного каналу між великим числом конкуруючих абонентів. Тоді з полиць дістали заповорошені описи дискретної ALOHA. Не раз вже було так, що цілком працездатні протоколи і методи виявлялися незатребуваними з політичних причин (наприклад, коли яка-небудь крупна компанія висловлювала бажання, щоб всі на світі використовували виключно її продукцію), проте після багатьох літ яка-небудь мудра людина згадувала про існування одного стародавнього методу, здатного розв'язати сучасну проблему. З цієї причини ми вивчимо в цьому розділі ряд елегантних протоколів, які зараз широко не використовуються, але за просто можуть виявитися запитаними в майбутньому – якщо, звичайно, про їх існування знатиме достатня кількість розробників мереж. Зрозуміло, ми вивчимо і що використовуються в даний час протоколи.

11.2.2 Протокол вільного доступу з контролем несучої

В дискретній системі ALOHA максимальний коефіцієнт використання каналу, який може бути досягнутий, рівний $1/e$. Такий скромний результат недивний, оскільки станції передають дані, коли хочуть, не

вважаючись з тим, що роблять решту станцій. В такій системі неминуче виникає велика кількість колізій. Проте в локальних мережах можна організувати процес таким чином, що станції враховуватимуть поведінку один одного. За рахунок цього можна досягти значення коефіцієнта використання каналу значно більшого, ніж $1/e$. В даному розділі ми розглянемо деякі протоколи, що дозволяють поліпшити продуктивність каналу.

Протоколи, в яких станції прослуховують середовище передачі даних і діють відповідно до цього, називаються **протоколами з контролем несучої**. Було розроблено багато таких протоколів. Кляйнрок (Kleinrock) і Тобаги (Tobagi) в 1975 році детально досліджували декілька таких протоколів. Далі ми розглянемо декілька версій протоколів з контролем несучої.

11.2.2.1 Наполегливий і ненаполегливий CSMA

Перший протокол з опитуванням несучої, який ми розглянемо, називається **“наполегливий протокол” CSMA** (Carrier Sense Multiple Access - множинний доступ з контролем несучої). Коли у станції з’являються дані для передачі, вона спочатку прослуховує канал, перевіряючи, вільний він або зайнятий. Якщо канал зайнятий, тобто по ньому передає яка-небудь інша станція, станція чекає, поки він звільниться. Коли канал звільняється, станція передає кадр, Якщо відбувається зіткнення, станція чекає протягом випадкового інтервалу часу, потім знову прослуховує канал і, якщо він вільний, намагається передати кадр ще раз. Такий протокол називається протоколом CSMA з наполегливістю 1, оскільки станція передає кадр з вірогідністю 1, як тільки знайде, що канал вільний.

Затримка розповсюдження сигналу робить сильний вплив на продуктивність даного протоколу. Існує невелика вірогідність того, що як тільки станція почне передачу, інша станція також виявиться готовою до

передачі і опитає канал. Якщо сигнал від першої станції ще не встиг досягти другої станції, друга станція вирішить, що канал вільний, і також почне передачу, результатом чого буде колізія. Чим більше час розповсюдження сигналу, тим вище вірогідність зіткнень і нижче продуктивність протоколу.

Навіть при нульовій затримці розповсюдження сигналу все одно будуть зіткнення. Якщо дві станції прийдуть в стан готовності в той час, коли передає якась третя станція, обидва чекатимуть, поки вона не закінчить передачу, після чого самі одночасно стануть передавати, і в результаті відбудеться зіткнення. Якби вони не були такі нетерплячі, кількість зіткнень була б меншою. Проте навіть така система значно краще за чисту систему ALOHA, оскільки обидві станції утримуються від передачі, поки передає третя станція. Очевидно, що завдяки цьому продуктивність системи з опитом несучої повинна бути вище навіть ніж у дискретної системи ALOHA.

Другим протоколом з опитом несучої є **ненаполегливий протокол CSMA**. В даному протоколі зроблена спроба стримати прагнення станцій починати передачу, як тільки звільняється канал. Перш ніж почати передачу, станція опитує канал. Якщо ніхто не передає в даний момент по каналу, станція починає передачу сама. Проте якщо канал зайнятий, станція не чекає звільнення каналу, постійно прослуховуючи його і намагаючись захопити відразу, як тільки він звільниться, як в попередньому протоколі. Натомість станція чекає протягом випадкового інтервалу часу, а потім знову прослуховує лінію. Очевидно, даний алгоритм повинен привести до кращого використання каналу і до великих інтервалів очікування, ніж протокол CSMA з наполегливістю 1.

Нарешті, третій протокол, який ми розглянемо, це **протокол CSMA з наполегливістю p** . Він застосовується в дискретних каналах і працює таким чином. Коли станція готова передавати, вона опитує канал. Якщо канал

вільний, вона з ймовірністю q починає передачу. З вірогідністю $q=1-p$ вона відмовляється від передачі і чекає початку наступного такту. Цей процес повторюється до тих пір, поки кадр не буде переданий або яка-небудь інша станція ^{1е} почне передачу. В останньому випадку станція поводить себе так само, як у разі зіткнення. Вона чекає протягом випадкового інтервалу часу, після чого починає все знову. Якщо при першому прослуховуванні каналу він виявляється зайнятий, станція чекає наступного інтервалу часу, після чого застосовується той же алгоритм. На рис. 4 показана розрахункова залежність продуктивності каналу пропонованого потоку кадрів для всіх трьох протоколів, а також для чистої дискретної систем ALOHA.

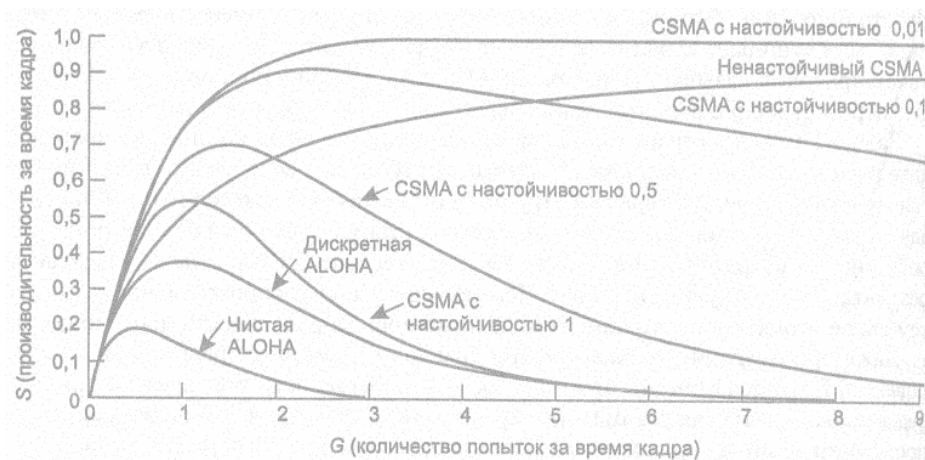


Рис. 4. Порівняння використання каналу залежно від його завантаження для різних протоколів колективного доступу

11.2.2.2 CSMA з виявленням конфліктів

Наполегливий і ненаполегливий протоколи CSMA, поза сумнівом, є покращаннями системи ALOHA, оскільки вони гарантують, що ніяка станція не почне передачу, якщо вона визначить, що канал вже зайнятий. Ще одним кроком вперед є припинення станцією передачі, якщо з'ясується, що відбувся конфлікт. Іншими словами, якщо дві станції, знайшовши, що канал вільний, одночасно почали передачу, вони практично негайно знаходять зіткнення. Замість того щоб намагатися продовжувати передачу своїх кадрів, які все одно вже не можуть бути прийняті одержувачами, їм слід припинити передачу. Таким чином економиться час і поліпшується продуктивність каналу. Такий протокол, званий CSMA/CD (Carrier-Sense Multiple Access with Collision Detection – множинний доступ з контролем несучої і виявленням конфліктів), широко застосовується в локальних мережах в підрівні MAC. Зокрема, він є основою надзвичайно популярних ЛВС Ethernet, тому ми приділимо якийсь час більш менш докладному розгляду CSMA/CD.

В протоколі CSMA/CD, так само як і в багатьох інших протоколах локальних мереж, застосовується концептуальна модель, показана на рис. 5. У момент часу t_0 одна із станцій закінчила передачу кадру. Вся решта станцій, готових до передачі, тепер може спробувати передати свої кадри. Якщо дві або більш станцій одночасно почнуть передачу, то відбудеться зіткнення. Зіткнення можуть бути знайдені по потужності або тривалості імпульсу сигналу, що приймається, порівняно з передаваним сигналом.

Знайшовши колізію, станція припиняє передачу, чекає випадкового періоду часу, після чого намагається знову за умови, що до цього моменту не почала передачу інша станція. Таким чином, наша модель протоколу CSMA/CD складатиметься з чергування періодів конкуренції і передачі, а також періодів простою каналу (коли всі станції мовчать).

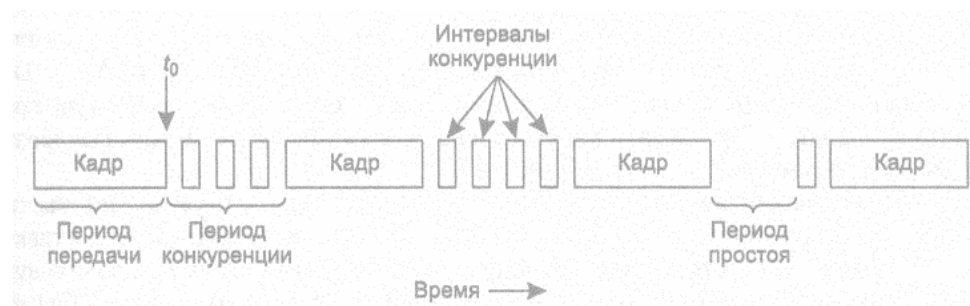


Рис. 5. Протокол CSMA/CD може знаходитися в одному з трьох станів: конкуренції, передачі і простою

Розглянемо більш детально алгоритм боротьби за право передачі по каналу. Припустимо, дві станції одночасно почали передачу у момент часу t_0 . Скільки знадобиться часу на те, щоб вони зрозуміли, що відбулося зіткнення? Від відповіді на це питання залежить довжина періоду конкуренції, а отже, величина затримки і продуктивність каналу. Мінімальний час виявлення конфлікту рівно часу розповсюдження сигналу від однієї станції до іншої.

Виходячи з цих міркувань, можна припустити, що станція, яка не чує зіткнення протягом часу, потрібного для проходження сигналу по всьому кабелю, може бути упевнений, що їй вдалося захопити кабель. Під терміном «захопити» мається на увазі, що вся решта станцій знає, що ця станція передає, і не будуть самі намагатися передавати. Проте такий висновок невірний. Розглянемо наступний сценарій. Хай час, необхідний для проходження сигналу між двома найдальшими станціями, рівно τ . У момент часу t_0 одна із станцій починає передачу. Через інтервал часу $\tau - \varepsilon$, за мить до того, як сигнал досягне найдальшої станції, та станція також починає передавати. Звичайно, майже миттєво вона знаходить зіткнення і зупиняється, але сплеск шуму, викликаний зіткненням, досягає передаючої станції тільки через інтервал часу $2\tau - \varepsilon$ з моменту початку передачі.

Іншими словами, станція не може бути упевнений в тому, що захопила канал, до тих пір, поки не пройде інтервал часу 2τ з моменту початку передачі. З цієї причини для моделювання інтервалу конкуренції ми використовуємо дискретну систему ALOHA з шириною інтервалу 2τ . В коаксіальному кабелі завдовжки 1 км τ приблизно рівне 5 мкс. Для простоти ми припускати, що кожний інтервал часу 2τ містить всього 1 біт. Як тільки канал захоплений, станція може передавати з будь-якою швидкістю, не обов'язково 1 біт за 2τ .

Слід зазначити, що виявлення зіткнення є *аналоговим* процесом. Апаратура станції повинна прослуховувати кабель під час передачі. При цьому, якщо те, що вона чує, відрізняється від того, що вона передає, станція розуміє, що відбулося зіткнення. Спосіб кодування сигналу повинен дозволяти визначати зіткнення (наприклад, зіткнення двох сигналів в Про У в явному вигляді не так просто знайти). З цієї причини використовується спеціальне кодування.

Передаюча станція повинна постійно прослуховувати канал, виявляючи сплески шуму, які можуть означати зіткнення. З цієї причини CSMA/CD з моноканалом вважається напівдуплексною системою. Станція не може одночасно передавати і приймати кадри, оскільки задіяний механізм зворотного зв'язку для визначення зіткнень.

Щоб уникнути неправильного розуміння питання слід також відзначити, що жоден протокол підрівня MAC не може гарантувати надійну доставку. Навіть за відсутності зіткнень одержувач може не отримати правильну копію кадру з різних причин (наприклад, через брак місця в буфері або пропущеного переривання).

11.2.3 Протоколи без зіткнень

Хоча в протоколі CSMA/CD зіткнення не можуть відбуватися після того, як станція захоплює канал, вони можуть траплятися в період конкуренції. Ці зіткнення знижують продуктивність системи, особливо при великій довжині кабелю (тобто при великих t) і коротких кадрах. Метод CSMA/CD виявляється не універсальним. В даному розділі ми розглянемо протоколи, які вирішують проблему боротьби за право зайняти канал, причому роблять це навіть без періоду конкуренції.

В описуваних далі протоколах передбачається наявність N станцій, у кожної з яких є постійна унікальна адреса в межах від 0 до $N-1$. То, що деякі станції можуть частина часу залишатися пасивними, ролі не грає. Також передбачається, що затримка розповсюдження сигналу нехтує мала. Головне питання зберігається: якій станції буде наданий канал після передачі даного кадру? Ми як і раніше використовуватимемо модель, зображену на рис. 5, з її дискретними інтервалами конкуренції.

11.2.3.1 Протокол бітової карти

В першому протоколі без зіткнень, який ми розглянемо, що називається основним методом бітової карти, кожний період конкуренції складається рівно з N дочасових інтервалів. Якщо у станції 0 є кадр для передачі, вона передає одиничний біт під час 0-го інтервалу. Іншим станціям не дозволяється передача в цей час. Під час інтервалу 1 станція 1 також повідомляє, чи є у неї кадр для передачі, передаючи біт 1 або 0. В результаті до закінчення інтервалу N *все* N станцій знають, хто хоче передавати. У цей момент вони починають передачу відповідно до свого порядку номерів (рис. 6).

Оскільки всі знають, чия черга передавати, зіткнень немає. Після того, як остання станція передає свій кадр, що всі станції відстежують, прослуховуючи лінію, починається новий період подачі заявок з N інтервалів. Якщо станція переходить в стан готовності (одержує кадр для передачі) відразу після того, як вона відмовилася від передачі, це значить, що їй не повезло і вона **повинна чекати наступного циклу. Протоколи, в яких намір передавати оголошується всім перед самою передачею, називаються протоколами з резервуванням.**



Рис. 6. Базовий протокол бітової карти

Оцінимо продуктивність такого протоколу. Для зручності вимірюватимемо час в одиницях інтервалів періоду подачі заявок, при цьому кадр даних складається з d одиниць часу. При слабкому завантаженні каналу біт-карта буде просто повторюватися знову і знову, зрідка перемежаючись кадрами.

Розглянемо цю ситуацію з погляду станції з невеликим номером, наприклад, 0 або 1. Зазвичай в той момент, коли у неї виникає необхідність в передачі, поточний інтервал часу вже знаходиться десь **в середині** біт-карти. В середньому станція чекатиме $N/2$ інтервалів до закінчення поточного періоду резервування і ще N інтервалів наступного (свого) періоду резервування, не рахуючи кадрів, передаваних між двома цими періодами, перш ніж вона зможе почати передачу.

Перспективи станцій з великими номерами більш веселкові. В середньому час очікування передачі складе половину циклу ($N/2$ однобітових інтервалів). Станціям з великими номерами рідко доводиться чекати наступного циклу. Оскільки станціям з невеликими номерами доводиться чекати в середньому $1,5N$ інтервалів, а станціям з великими номерами – $N/2$ інтервалів, середній час очікування для всіх станцій складає N інтервалів. При низькому завантаженні каналу його продуктивність легко злічити. Невигідні витрати на кадр складають N біт, і при довжині кадру в d біт ефективність рівна $d/(N + d)$.

При сильній завантаженості каналу, коли всі станції хочуть щось передати, період подачі заявок з N чергує з N кадрами. При цьому невідні витрати на передачу одного кадру складають всього один біт, а ефективність рівна $d/(d + 1)$. Середній час затримки для кадру буде рівний сумі часу очікування в черзі усередині своєї станції і додаткових $N(d + 1)/2$ однобітових інтервалів, коли він потрапить в початок своєї внутрішньої черги.

11.2.3.2 Двійковий зворотній відлік

Недоліком базового протоколу біт-карти є накладні витрати в 1 біт на станцію. Використовуючи двійкову адресу станції, можна поліпшити ефективність каналу. Станція, охоча зайняти канал, оголошує свою адресу у вигляді бітового рядка, починаючи із старшим бітом. Передбачається, що всі адреси станцій мають однакову довжину. Біті адреси в кожній позиції логічно складаються (логічне АБО). Ми називатимемо цей протокол протоколом з **двійковим зворотнім відліком**. Він використовується в мережі Datakit (Fraser, 1987). неявно передбачається, що затримки розповсюдження сигналу нехтує малі, тому станції чують затверджені номери практично миттєво.

Щоб уникнути конфліктів слід застосувати правило арбітражу: як тільки станція з 0 в старшому біті адреси бачить, що в сумарній адресі цей 0 замінився одиницею, вона здається і чекає наступного циклу. Наприклад, якщо станції 0010, 0100, 1001 і 1010 конкурують за канал, то в першому бітовому інтервалі вони передають біти 0, 0, 1 і 1 відповідно. В цьому випадку сумарний перший біт адреси буде рівний 1. Отже, станції з номерами 0010 і 0100 вважаються тими, що програли, а станції 1001 і 1010 продовжують боротьбу.

Наступний біт у обох станцій, що залишилися, рівний 0 – таким чином, обидва продовжують. Третій біт рівний 1, тому станція 1001 здається. Переможцем виявляється станція 1010, оскільки її адреса найбільша. Вигравши торги, вона може почати передачу кадру, після чого почнеться новий цикл торгів. Схема протоколу показана на рис. 7. Даний метод припускає, що пріоритет станції напряму залежить від її номера. В деяких випадках таке жорстке правило може грати позитивну, в деяких – негативну роль.

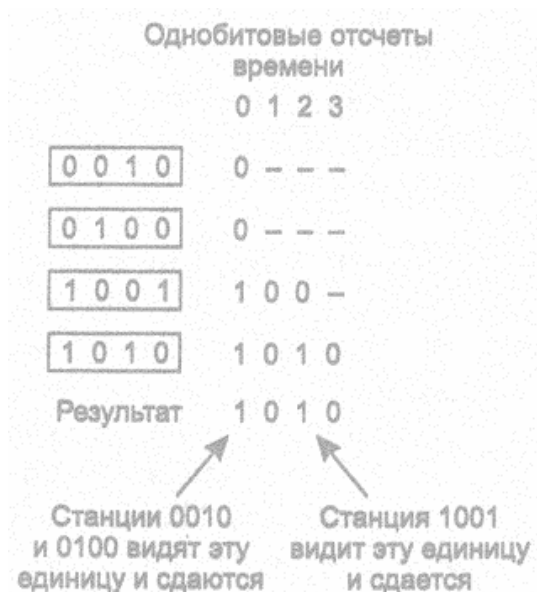


Рис. 7. Протокол з двійковим зворотним відліком. Прочерк означає мовчання

Ефективність використання каналу при цьому методі складає $d/(d+\log_2 N)$. Проте можна так хитро вибрати формат кадру, що його перше поле міститиме адресу відправника, тоді навіть ці $\log_2 N$ біт не пропадуть дарма і ефективність складе 100 %.

Мок (Mok) і Уард (Ward) в 1979 році описали варіант протоколу із зворотним відліком, в якому використовувався паралельний, а не послідовний інтерфейс. Вони також запропонували використовувати віртуальні номери станцій. Після кожної передачі станції, яка успішно послала кадр, привласнюється віртуальний номер 0, тим самим дається можливість захоплення каналу станціями, які мовчать дуже довго. Наприклад, якщо станції *З, Я, D, А, G, В, Е, F* мали пріоритети 7, 6, 5, 4, 3, 2, 1 і 0 відповідно, тоді при успішній передачі станції *D* вона поміщається в кінець списку, одержуючи номер 0. Пріоритети старших станцій *З* і *Я* залишаються незмінними (7 і 6), а пріоритети решти станцій збільшуються на 1 (наприклад, пріоритет *А* був 4, а став 5). Таким чином, на наступному циклі формується такий список: *З, Н, А, G, В, Е, F, D*. Тепер станція *D* зможе отримати доступ до каналу, тільки якщо він більше нікому не потрібен.

Двійковий зворотний відлік є прикладом простого, елегантного і ефективного протоколу, який ще належить відкрити наново розробникам майбутніх мереж. Хочеться сподіватися, що коли-небудь він займе свою нішу в мережних технологіях.

11.2.4 Протоколи з обмеженою конкуренцією

11.2.4.1 Загальні відомості

Отже, ми розглянули дві основні стратегії надання доступу до каналу в кабельних мережах: змагання, як в CSMA, і безконфліктні методи. Кожну стратегію можна оцінити по двох важливих параметрах: часу затримки при низькому завантаженні каналу і ефективності каналу при великому завантаженні. В умовах низького завантаження конфлікти (тобто чиста або дискретна системи ALOHA) переважно, оскільки час затримки в таких системах менше. У міру зростання завантаженості каналу системи із зіткненнями стають всі менш привабливими, оскільки зростають не вигідні витрати, пов'язані з конфліктами. Для безконфліктних протоколів справедливо зворотне. При низькому навантаженні у них досить високий час затримки, але у міру збільшення навантаження ефективність використання каналу не зменшується, як у конфліктних протоколів, а навпаки, зростає.

Очевидно, було б непогано об'єднати кращі властивості обох стратегій і отримати протокол, що використовує різні стратегії при різній завантаженості каналу. Такі протоколи ми називатимемо **протоколами з обмеженою конкуренцією**. Вони насправді існують, і їх розглядом ми завершимо вивчення мереж з опитом носія.

Дотепер ми розглядали тільки симетричні протоколи колективного доступу, в яких кожна станція намагається отримати доступ до каналу з рівною вірогідністю p . Цікаво, що продуктивність всієї системи може бути поліпшений при використуванні асиметричного протоколу, в якому станціям призначається різна вірогідність.

Перш ніж приступити до розгляду асиметричних протоколів, давайте стисло розглянемо продуктивність в симетричному випадку. Припустимо, що do станцій борються за доступ до каналу. Вірогідність передачі кожної станції в кожний інтервал часу рівна p . Вірогідність того, що якась станція успішно отримає доступ до каналу на даний інтервал часу, рівна $kp(l - p)^{k-1}$. Щоб знайти оптимальне значення вірогідності p , продиференціюємо даний вираз по p , прирівняємо результат до нуля і вирішимо отримане рівняння щодо p . В результаті ми отримаємо, що якнайкраще значення p рівно $1/k$. Замінюючи у формулі p на $1/k$, одержуємо вірогідність успіху при оптимальному значенні p :

$$P[\text{успех при оптимальной вероятности } p] = \left(\frac{k-1}{k}\right)^{k-1}. \quad (4)$$

Залежність цієї вірогідності від кількості готових станцій графічно показана на рис. 8. Для невеликого числа станцій значення вірогідності успіху є непоганим, проте як тільки кількість станцій досягає хоча б п'яти, вірогідність знижується майже до асимптотичної величини, рівної $1/e$.

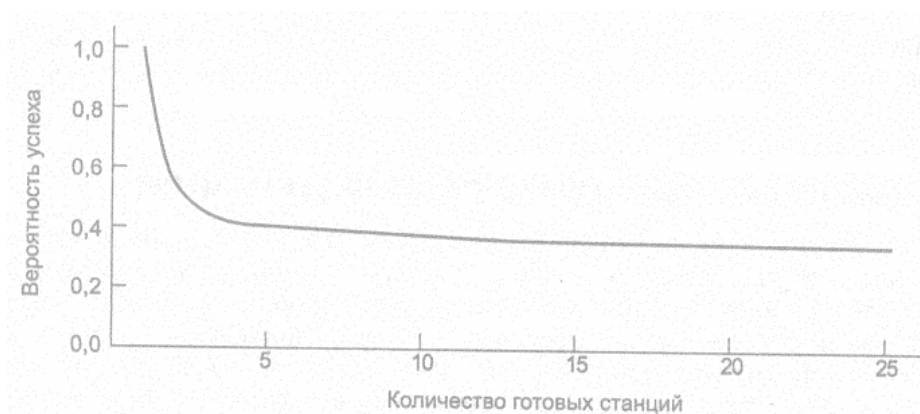


Рис. 8. Вірогідність отримання доступу до каналу в симетричному протоколі

З малюнка очевидно, що вірогідність отримання доступу до каналу для якої-небудь станції можна збільшити, тільки понизивши конкуренцію за канал. Цим займаються протоколи з обмеженою конкуренцією. Вони спочатку ділять всі станції на групи (необов'язково непересічні). Змагатися за інтервал 0 дозволяється тільки членам групи 0. Якщо хтось з них виграє, він одержує канал і передає по ньому кадр. Якщо ніхто з них не хоче передавати або відбувається зіткнення, члени групи 1 змагаються за інтервал 1, і т.д. При відповідному розбитті на групи конкуренція за кожний інтервал часу зменшується, що збільшує вірогідність його успішного використання (див. ліву частину графіка).

Питання в тому, як розбивати станції на групи. Перш ніж обговорювати загальний випадок, розглянемо декілька окремих випадків. В одному з крайніх випадків в кожній групі буде по одній станції. Таке розбиття гарантує повну відсутність конфліктів, оскільки на кожний інтервал часу претендуватиме тільки одна станція. Подібні протоколи вже розглядалися раніше (наприклад, протокол з двійковим зворотним відліком). Ще одним особливим випадком є розбиття на групи, що складаються з двох станцій. Вірогідність того, що обидві станції одночасно почнуть передачу протягом одного інтервалу, рівна p^2 , і при малих значеннях p цим значенням можна нехтувати. По мірі збільшення кількості станцій в групах ймовірність зіткнень буде зростати, однак довжина біт-карти, необхідної щоб перенумерувати всі групи, буде зменшуватися. Іншим граничним випадком буде одна група, до якої увійдуть всі станції (тобто дискретна система ALOHA). Нам потрібен механізм динамічного розбиття станцій на групи з невеликою кількістю крупних груп при слабкій завантаженості каналу і великій кількості дрібних груп (можливо, навіть що складаються з однієї станції кожна), коли завантаженість каналу висока.

11.2.4.2 Протокол адаптивного проходу по дереву

Одним з простих способів динамічного розбиття на групи є алгоритм, розроблений під час Другої світової війни в армії США для перевірки солдатів на сифіліс (Dorfman, 1943). Брався аналіз крові у N солдатів. Частина кожного зразка поміщалася в одну загальну пробірку. Цей змішаний зразок перевірявся на наявність антитіл. Якщо антитіла не виявлялися, всі солдати в даній групі оголошувалися здоровими. В осоружному ж випадку група ділилася пополам, і кожна половина групи перевірялася окремо. Подібний процес продовжувався до тих пір, поки розмір групи не зменшувався до одного солдата. В комп'ютерній версії даного алгоритму (Carpanakis, 1979) станції розглядаються у вигляді листя двійкового дерева, як показано на рис. 9. В першому тимчасовому інтервалі змагання за право передачі беруть участь всі станції. Якщо кому-небудь це вдається, то на цьому роботі алгоритму закінчується. Якщо ж відбувається зіткнення, то до другого етапу змагань допускається тільки половина станцій, а саме станції, що відносяться до вузла 2 дерева. Якщо одна із станцій успішно захоплює канал, то наступне змагання влаштовується для другої половини станцій (що відносяться до вузла 3 дерева). Якщо знову відбувається конфлікт, то до наступного інтервалу часу серед тих, що змагаються залишається вже четверть станцій, що відносяться до вузла 4.

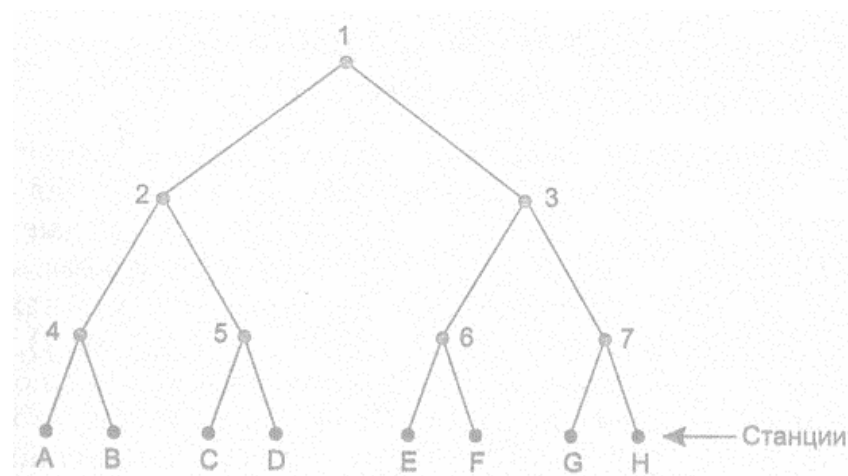


Рис. 9. Дерево з восьми станцій

Таким чином, якщо зіткнення відбувається під час інтервалу 0, то все дерево сканується на одиничну глибину для пошуку готових станцій. Кожний однобітовий слот асоціюється з певним вузлом дерева. Якщо відбувається зіткнення, пошук продовжується для лівого і правого дочірніх вузлів. Якщо кількість станцій, що претендують на передачу, рівно нулю або одиниці, пошук в даному вузлі дерева припиняється.

При сильній завантаженості каналу навряд чи варто починати пошук готової станції з вузла 1, оскільки шансів, що всього одна станція зі всіх претендуватиме на канал, мало. З тієї ж причини можуть бути пропущені також вузли 2 і 3. А на якому рівні дерева слід починати опит в загальному випадку? Очевидно, що чим сильніше завантаженість каналу, тим на більш низькому рівні дерева повинен починатися пошук готових станцій. Припускаємо, що кожна станція досить точно може оцінити q (кількість готових на даний момент станцій), відстежуючи недавній трафік.

Пронумеруємо рівні дерева на рис. 9 – вузол 1 на рівні 0, вузли 2 і 3 на рівні 1 і т.д. Звернете увагу на те, що кожний вузол на рівні i *включає* 2^i частину від всіх станцій. Якщо q *готових* станцій розподілені рівномірно, то очікуване їх число нижче за вузол на рівні i *рівно* $2^i q$. *Інтуїтивно* ясно, що оптимальним рівнем для початку пошуку буде той, на якому середнє число конкуруючих в інтервалі станцій *рівно* 1, тобто рівень, на якому $2^i q = 1$, Звідси $i = \log_2 q$.

Були розроблені численні удосконалення базового алгоритма—в частковості, деякі деталі обговорюються у Бертсекаса (Bertsekas) і Гал-лагера (Gallager) у виданні 1992 року. Наприклад, розглянемо випадок, при якому передавати хочуть тільки станції G і H . *На* вузлі 1 відбудеться конфлікт, тому буде перевірений вузол 2. Він виявиться порожнім. Вузол 3 перевіряти немає значення, оскільки там гарантований буде зіткнення. (Нам відомо, що під вузлом 1 знаходяться 2 або більш станцій, а оскільки під вузлом 2 немає жодної станції, то всі вони повинні бути під вузлом 3.) Тому перевірку вузла 3 можна пропустити і відразу перевірити вузол 6. Оскільки під вузлом 6 ніщо не виявилось, то перевірку вузла 7 також можна пропустити і перевірити вузол 6.

11.2.5 Протоколі вільного доступу зі спектральним розподілом

Ще один метод розподілу каналу полягає в його розбитті на підканали за допомогою частотного, тимчасового або змішаного розділення і динамічного розподілу підканалів в міру необхідності. Подібні схеми часто застосовуються в оптоволоконних локальних мережах, при цьому можлива одночасна передача по каналу на різних довжинах хвиль (тобто частотах). В даному розділі ми розглянемо один такий протокол (Humblet і ін., 1992).

Простіше всього побудувати цілком оптичну локальну мережу за допомогою комутатора «пасивна зірка» (див. рис. 8). Значення полягає в тому, що два оптичні волокна від кожної станції вплавляються в скляний циліндр. По одному волокну світло потрапляє в циліндр, а по іншому він з циліндра потрапляє в інше волокно. Світло, що виходить в циліндр з одного волокна, освітлює весь циліндр і потрапляє у все що виходять з нього волокна. Пасивні зірки можуть об'єднувати до декількох сотень станцій.

Для реалізації одночасної передачі спектр ділиться на канали (діапазони довжин хвиль), як показано на мал. 2.27. В протоколі **WDMA** (Wavelength Division Multiple Access – множинний доступ із спектральним розділенням) кожної станції виділяється два канали. Вузкий канал забезпечує отримання станцією управляючої інформації, а широкий канал – передачу даних станцією.

Кожний канал ділиться на групи тимчасових інтервалів, як показано на рис. 10. Хай кількість інтервалів в управляючому каналі рівно m , а кількість інтервалів в каналі даних – $n + 1$, з яких n інтервалів використовуються для даних, а останній інтервал – для повідомлення станцією про свій стан (головним чином про те, які інтервали в обох каналах вільні). В обох каналах послідовність інтервалів повторюється нескінченно, при цьому інтервал 0 позначається спеціальним чином, щоб всі могли його розпізнати. Всі канали синхронізуються одними глобальними годинами.

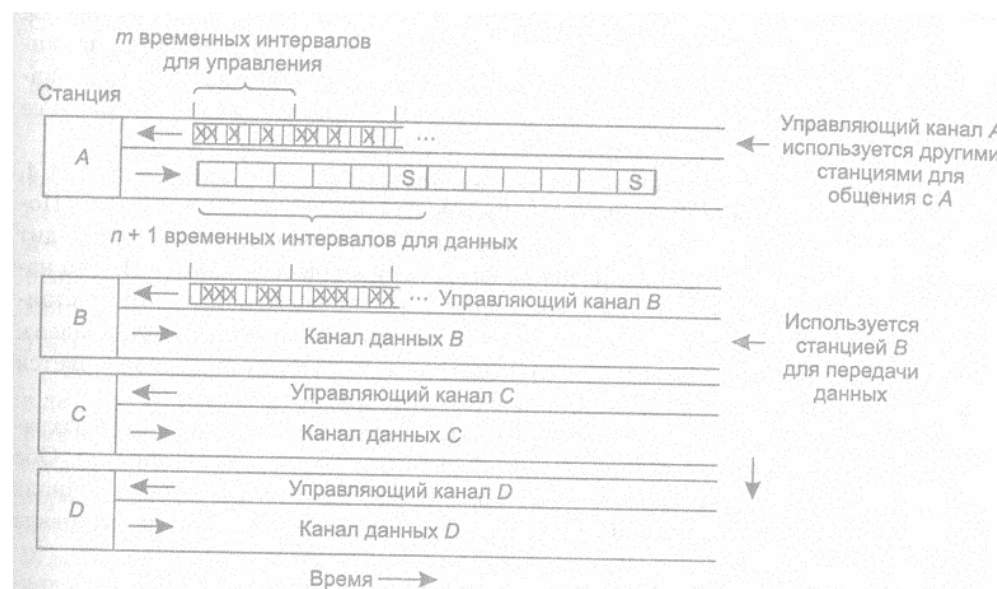


Рис. 10. Множинний доступ із спектральним розділенням

Протоколом підтримуються три класи трафіку: 1) орієнтований на з'єднання з постійною швидкістю передачі даних, наприклад, нестисле відео; 2) орієнтований на з'єднання із змінною швидкістю передачі даних, наприклад, передача файлів; 3) дейтаграмний трафік, як, наприклад, UDP-пакети. Для двох орієнтованих на з'єднання протоколів ідея полягає в тому, що якщо станція *A* хоче зв'язатися із станцією *B*, вона спочатку повинна вставити кадр CONNECTION REQUEST (запит на з'єднання) у вільний інтервал управляючого каналу *B*. Если станція *B* згодна, зв'язок відбувається по каналу даних *A*.

У кожній станції є два передавачі і два приймачі.

1. Приймач з фіксованою довжиною хвилі для прослуховування свого управляючого каналу.

2. Передавач з довжиною хвилі, що настраюється, для передачі по управляючому каналу іншої станції.
3. Передавач з фіксованою довжиною хвилі для передачі кадрів даних.
4. Приймач з довжиною хвилі, що настраюється, для прийому кадрів даних. Іншими словами, кожна станція прослуховує свій управляючий канал

Для отримання запитів, але повинна настроюватися на довжину хвилі передавача для отримання даних. Налаштування довжини хвилі здійснюється за допомогою інтерферометра Фабри–Перо або Маха–Цандера, відсікаючого всі довжини хвиль, які не входять в необхідний діапазон.

Розглянемо тепер, як станція *A* встановлює канал зв'язки класу 2 із станцією *B*, *наприклад*, для перенесення файлів. Спочатку станція *A* *настроює* свій приймач даних на канал даних станції *B* і чекає інтервалу стану. В цьому інтервалі повідомляється, які управляючі інтервали вільні в даний момент, а які зайняті. Так, на мал. 4.10 ми бачимо, що з восьми управляючих інтервалів станції *У* *вільні* тільки інтервали 0, 4 і 5. Решта інтервалів зайнята (помічені хрестиками).

Станція *A* вибирає один з вільних інтервалів, *наприклад*, інтервал 4, і вставляє в нього своє повідомлення із запитом на зв'язок (CONNECTION REQUEST). Оскільки станція *B* постійно прослуховує свій управляючий канал, вона бачить запит і дозволяє встановлення зв'язку, призначаючи інтервал 4 станції *A*. *Это* призначення оголошується в інтервалі стану управляючого каналу. Коли станція *A* бачить це призначення, вона розуміє, що односторонній зв'язок встановлений. Якщо станція *A* запрошувала двосторонній зв'язок, той же алгоритм повторюється з тією різницею, що тепер станція *B* запрошує зв'язок у станції *A*.

Може трапитися так, що станції *A* і *C* одночасно намагатимуться захопити інтервал 4 станції *B*. В цьому випадку інтервал не дістанеться нікому. Обидві станції помітять це, відстежуючи інтервал стану в

управляючому каналі станції *B*. Після цього станції *A* і *C* чекають протягом випадкового інтервалу часу і спробують ще раз.

Таким чином, у кожній станції є безконфліктний спосіб послати іншій станції коротке управляюче повідомлення. Щоб переслати файл, станція *A* посилає станції *B* управляюче повідомлення приблизно такого змісту: «будь ласка, прогляньте мої вихідні дані в інтервалі 3. Там для вас є кадр даних». Отримавши управляюче повідомлення, станція *B* настраює свій приймач на вихідний канал станції *A*, щоб прочитати інформаційний кадр. Залежно від протоколу більш високого рівня, станція *B* може використовувати той же самий механізм, щоб при необхідності послати назад підтвердження.

Проблема може виникнути, якщо станції *A* і *C* одночасно сполучені із станцією *B* і при цьому обидва раптово запропонують станції *B* подивитися в інтервал 3. Станції *B* доведеться вибрати випадковим способом одну із станцій, при цьому інша передача буде втрачена.

Для трафіку з постійною швидкістю передачі даних використовується один з різновидів цього протоколу. Коли станція *A* просить про надання зв'язку, вона одночасно із запитом говорить щось таке: «можна я посылатиму вам кадр в інтервалі 3?» Якщо станція *B* може прийняти його (тобто інтервал 3 вільний), встановлюється з'єднання з гарантованою пропускнуною спроможністю. В осоружному випадку станція *A* може спробувати змінити свою пропозицію, вибравши інший вільний інтервал.

Для трафіку третього типу (дейтаграма) використовується ще один варіант протоколу. Замість того щоб вставляти запит CONNECTION REQUEST в тільки що знайдений управляючий інтервал (4), станція пише повідомлення DATA FOR YOU IN SLOT 3 («дані для вас в інтервалі 3»), Якщо станція *У* вільна під час

наступного інтервалу 3, передача буде успішною. В іншому випадку кадр з даними втрачається. При такому зв'язку з'єднання не потрібне.

Можливо декілька варіантів реалізації всього протоколу. Наприклад, замість того щоб надавати кожній станції свій управляючий канал, можна розподілити один управляючий канал між всіма станціями. Кожній станції надається блок інтервалів в кожній групі; таким чином, декілька віртуальних каналів ефективно мультиплекуються в одному фізичному.

Крім того, для кожної станції можна використовувати тільки один приймач і один передавач, що настроюється, що настроюється. Для цього кожний канал станції ділиться на m управляючих інтервалів, за якими слідуватиме $n + 1$ інформаційний інтервал. Недоліком такого підходу є те, що відправникам доведеться довше чекати управляючого інтервалу, і подальші кадри даних теж зсунуться далі, оскільки між ними розташовуються управляючі кадри.

Розроблено і реалізовано безліч WDMA-протоколів, що розрізняються в деталях. У деяких один канал управління, у інших – дещо. В деяких затримка розповсюдження враховується, в деяких – ні. Одні враховують час настройки, інші – ні. Протоколи також розрізняються складністю обробки, пропускною спроможністю і масштабованістю. Завдяки великому числу частот, що використовуються, систему іноді називають **DWDM** (Dense Wavelength Division Multiplexing – мультиплексування по довжині хвилі високої густини). Додаткову інформацію див. в (Bogineni і ін., 1993; Chen, 1994; Goralski, 2001; Levine and Akyildiz, 1995).

11.2.6 Протоколи безпроводових локальних мереж

11.2.6.1 Загальні відомості

Із зростанням частки переносних комп'ютерів і засобів зв'язку росте і потреба в їх з'єднанні із зовнішнім світом. Навіть найперші мобільні телефони могли зв'язуватися з іншими телефонами. У перших портативних комп'ютерів такої здатності не було, проте незабаром широке розповсюдження отримали модеми. Щоб перейти в підключений режим (on-line), комп'ютер було слід приєднати до телефонної розетки. Необхідність підключення до фіксованої мережі означала, що комп'ютери були переносними, але не мобільними. Щоб називатися мобільними, портативні комп'ютери повинні використовувати для зв'язку радіо (або інфрачервоні хвилі). В цьому випадку їх власники зможуть читати і посилати листи по електронній пошті, знаходячись в автомобілі або на катері. Систему, що складається з портативних комп'ютерів, що спілкуються по радіо, можна розглядати як безпроводну локальну мережу – ми вже обговорювали це в розділі «Беспроводніє ЛВС: 802.11». Властивості таких мереж відрізняються від властивостей звичайних локальних мереж, таким мережам потрібні спеціальні протоколи управління доступом до носія (MAC). В даному розділі ми познайомимося з деякими з цих протоколів. Докладніше про безпроводні локальні мережі можна прочитати в (Geier, 2002; O'Hara and Petrick, 1999).

Звичайна конфігурація безпроводних локальних мереж має на увазі наявність офісної будівлі з наперед розміщеними в ньому базовими станціями (званими також точками доступу). Всі базові станції сполучені один з одним мідним дротом або оптоволоконним кабелем. Якщо потужність передавачів базових станцій і переносних комп'ютерів набудована так, що діапазон прийому складає близько 3-4 м, то кожна кімната стає сотою, а вся будівля перетворюється на велику стільникову систему, подібну традиційній стільниковій телефонній системі,

описаній на чолі 2. На відміну від звичайної стільникової системи, у кожного стільника в даному випадку всього один канал, покриваючий весь доступний частотний діапазон і працюючий зі всіма станціями, що знаходяться в ньому. Звичайно пропускна спроможність такого каналу складає від 1 до 2 Мбіт/с.

В подальших міркуваннях для простоти ми допустимо, що всі передавачі працюють в якомусь фіксованому діапазоні. Коли приймач потрапляє в зону прийому двох активних передавачів, результуючий сигнал спотворюється і стає даремний, тому тут ми більше не розглядатимемо системи типу CDMA. Важливо розуміти, що в деяких безпроводних ЛВС не всі станції знаходяться в межах досяжності один одного, що приводить до виникнення різного роду складнощів. Крім того, при установці безпроводних мереж в приміщенні присутність стін між станціями може зробити найсильніший вплив на ефективний діапазон кожної станції.

Можна наївно спробувати застосувати в локальних безпроводних мережах протокол CSMA (Carrier-Sense Multiple Access – множинний доступ з опитом несучої) – просто прослуховувати ефір і здійснювати передачу тільки тоді, коли він ніким не зайнятий. Проте проблема полягає в тому, що насправді має значення інтерференція на приймачі, а не на передавачі, тому цей протокол тут не годиться. Щоб наочно побачити суть проблеми, розглянемо рис. 11, де показано чотири безпроводні станції. Для нашої проблеми не має значення, яка з них є базовою, а яка – переносний. Потужність передавачів така, що інтерферувати можуть тільки сусідні станції, тобто А з В, С з В і Д але не з А.



Рис. 11. Безпроводна локальна мережа: *A* передає (а); *B* передає (б)

Спочатку розглянемо, що відбувається, коли станція *A* передає станції *pro*, як зображено на рис. 11, а. Якщо станція *C* опитує канал, то вона не чути станцію *A*, оскільки та розташована дуже далеко, і може прийти до невірної висновку про те, що канал вільний і що можна посилати дані. Якщо станція *C* почне передавати, вона інтерферуватиме із станцією *B* і спотворить кадр, передаваний станцією *A*. *Проблема*, що полягає в тому, що одна станція не може чути можливого конкурента, оскільки конкурент розташований дуже далеко від неї, іноді називається **проблемою прихованої станції**.

Тепер розглянемо зворотню ситуацію: станція *B* передає станції *A*, як показано на рис. 11, б. Станція *C* при опиті каналу чує виконувану передачу і може помилково припустити, що вона не може передавати дані станції *D*, коли насправді така передача створила б перешкоди тільки в зоні від станції *B* до станції *C*, де в даний момент не ведеться прийом. Така ситуація іноді називається **проблемою засвіченої станції**.

Проблема полягає в тому, що перш ніж почати передачу, станції необхідно знати, чи є яка-небудь активність поблизу приймача. Протокол CSMA же всього лише може повідомити про активність навкруги станції, що опитує канал. У разі передачі по дроту всі сигнали досягають всіх станцій, тому у всій системі одночасно тільки одна станція може вести передачу. В системі з використанням радіозв'язку, радіус передачі і прийому якої обмежений невеликими зонами, одночасно можуть передавати декілька станцій, якщо тільки вони передають різним приймаючим станціям, що знаходяться достатньо далеко один від одного.

Можна уявити собі це питання і по-іншому. Припустимо, в офісній будівлі у кожного працівника є безпроводний портативний комп'ютер. І ось, наприклад, Лінда хоче відправити повідомлення Марку. Комп'ютер

Лінди контролює те, що відбувається навкруги нього, і, не знайшовши ніякої активності, починає передачу. В кімнаті, де знаходиться Марк, при цьому може виникнути колізія через те, що хтось третій передає йому дані одночасно з Ліндою. Її комп'ютер, природно, цього знайти не може.

11.2.6.2 Протоколи MACA і MACAW

Одним з перших протоколів, розроблених для безпроводних локальних мереж, є **MACA** (Multiple Access with Collision Avoidance – множинний доступ із запобіганням зіткнень) (Кагп, 1990). Ідея, що лежить в основі цього протоколу, полягає в тому, що відправник примушує одержувача передати короткий кадр, щоб навколишні станції могли почути цю передачу і утриматися від дій на якийсь час, що вимагається для прийому великого інформаційного кадру. Протокол MACA проілюстрований на мал. 4.12.

Розглянемо ситуацію, в якій станція *A* передає станції *B*. Станція *A* починає з того, що посилає станції *B* кадр RTS (Request To Send – запит на передачу), як показано на мал. 4.12, *a*. Цей короткий кадр (30 байт) містить довжину кадру даних, який послідує за ним. Потім станція *B* відповідає кадром CTS (Clear To Send – дозвіл передачі), як показано на рис. 12,б. Кадр CTS також містить довжину інформаційного кадру (скопійовану з кадру RTS). Приймавши кадр CTS, станція *A* починає передачу.

Тепер подивимося, як реагують станції, які чують передачу одного з цих кадрів. Будь-яка станція, яка чує кадр RTS, знаходиться близько до станції *A* і тому повинна берегти мовчання, поки кадр CTS не буде прийнятий станцією *A*. Станції, що чують кадр CTS, знаходяться поблизу від станції *B*, отже, повинні утриматися від передачі, поки станція *B* не отримає кадр даних, довжину якого вони можуть взяти з кадру CTS.

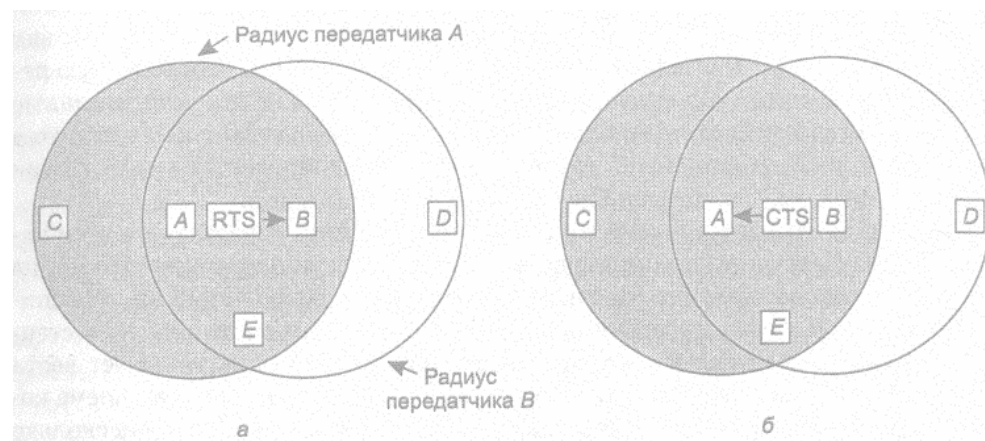


Рис. 12. Протокол MACA: станція *A* посилає кадр RTS станції *B* (а); станція *б* відповідає кадром CTS станції *A* (б)

На рис. 12 станція *C* знаходиться в зоні станції *A*, але не входить в зону станції *B*. *Поэтому* вона чує кадр RTS, передаваний станцією *A*, але не чує кадр CTS, яким відповідає станція *B*. *Поскольку* вона не інтерферує з кадром CTS, вона не зобов'язана утримуватися від передачі у той час, поки пересилається інформаційний кадр. Станція *D*, навпаки, знаходиться близько від станції *B*, але далеко від станції *A*. *Вона* не чує кадру RTS, але чує кадр CTS, а це означає, що вона знаходиться поблизу станції, що збирається прийняти кадр з даними. Тому їй не можна вести передачу, поки цей кадр не буде переданий. Станція *E* чує обидва управляючі повідомлення і так само, як і станція *D*, повинна берегти мовчання, поки не буде завершена передача інформаційного кадру.

Не дивлячись на всі запобіжні засоби, конфлікти все одно можуть відбутися. Наприклад, станції *B* і *З* можуть одночасно послати кадри RTS станції *A*. *При* цьому кадри зіткнуться і не буде прийнятий. В цьому випадку передавачі, не почувши кадр CTS у встановлений термін, чекають випадкового часу і після цього

повторюють спробу. Алгоритм витримки часу, що використовується у разі конфлікту, називається двійковим експоненціальним відкатом, і ми вивчимо його, коли розглядатимемо мережу Ethernet.

Грунтуючись на вивченні моделі протоколу МАСА, Бхаргаван (Bharghavan) з товариші в 1994 році здійснили тонку настройку протоколу МАСА, щоб поліпшити його продуктивність. Новий протокол був названий МАСАW (МАСА for Wireless – МАСА для безпроводних мереж). Спершу дослідники помітили, що без підтверджень на рівні передачі даних втрачені кадри не передавалися повторно, поки їх брак не знаходив транспортний рівень. Для вирішення цієї проблеми був введений кадр підтвердження (АСК), яким одержувач відповідав на кожний успішно прийнятий кадр даних. Крім того, було використано властивість протоколу CSMA – станції навчилися прослуховувати ефір і утримуватися від передачі кадру RTS, якщо поряд вже хтось передавав такий же кадр тій же станції. Також було вирішено зв'язати алгоритм витримки часу (у разі конфлікту) не з окремою станцією, а з потоком даних, тобто з парою станцій «джерело – приймач». Ця зміна протоколу дуже поліпшила його. Нарешті, був доданий механізм обміну між станціями інформацією про перевантаження. Крім того, алгоритм витримки часу у разі конфлікту був дещо пом'якшений, що поліпшило продуктивність системи.

Тема 12. Мережа Ethernet.

- 12.1. Загальні відомості.
- 12.2. Кабелі Ethernet.
- 12.3. Манчестерський код.
- 12.4. Протокол підрівня управління доступом до середовища в Ethernet.
- 12.5. Алгоритм двійкової експоненціальної „відміни”
- 12.6. Продуктивність мережі стандарту 802.3
- 12.7. Комутуючі мережі Ethernet.

12.1. Загальні відомості

Отже, ми в цілому закінчили обговорення загальних питань, протоколів розподілу каналу, що стосуються. Прийшов час перейти до практичних додатків, зокрема, до локальних мереж. Як вже було сказано в розділі «Ethernet», IEEE свого часу розробив серію стандартів IEEE 802, що описують локальні і регіональні мережі. Деякі стандарти вижили, деякі – ні (див. табл. 1.4). Люди, віруючі в реінкарнацію, вважають, що одним з членів Асоціації стандартів IEEE є Чарльз Дарвін, відбраковууючий слабі технології, що знов народився.. Загалом, дійсно вижили найсильніші. Найбільш важливі стандарти 802.3 (Ethernet) і 802.11 (безпроводні ЛОМ). Про 802.15 (Bluetooth) і 802.16р (безпроводні регіональні мережі) говорити всерйоз поки не доводиться. В стандартах 802.3 і 802.11 фізичні рівні і рівні управління доступом до середовища (MAC) розрізняються. Проте вже підрівні управління логічним з'єднанням (LLC, визначений стандартом 802.2) схожі, що дозволяє організувати єдине сполучення з мережним рівнем. Ми вже представили у загальних рисах Ethernet в розділі «Ethernet» (розділ 1) і

не більше повторюватимемо цей матеріал. Натомість ми відразу звернемося до розгляду таких технічних деталей побудови мереж Ethernet, як протоколи, а також нові технології високошвидкісної (гігабітної) мережі Ethernet. Оскільки Ethernet і IEEE 802.3 – це одне і те ж, то багато хто використовує обидві назви. Ми теж говоритимемо то «Ethernet», то «IEEE 802.3».

12.2. Кабелі Ethernet

Оскільки саме слово Ethernet пов'язано з кабелем (ether – ефір, середовище розповсюдження сигналу), то саме з цього ми і почнемо обговорення. В мережах Ethernet звичайно використовуються чотири типи кабелю, показані в табл. 4.1.

Історично склалося так, що кабель 10BaseS («товстий Ethernet») став першим носієм даних в мережах 802.3. Він зовні нагадував жовтий садовий шланг для поливання рослин, і через кожні 2,5 м була маркіровка місць під'єднання відведень. (Стандарт 802.3 не вимагає, щоб колір кабелю був саме жовтим, але рекомендує це.) З'єднання звичайно робляться на основі відгалужувачів «зуб вампіра»-, Зуб відгалужувача надзвичайно акуратно вводиться на половину товщини внутрішньої жили кабелю. Позначення 10Base5 говорить про наступне: швидкість роботи – 10 Мбіт/с, сигнал немодульований (BASE-band signaling), максимальна довжина сегменту – 500 м. Отже, перша цифра назви – це швидкість в мегабітах в секунду. Потім слідує слово Base (іноді його пишуть заголовними буквами – BASE), вказуюча на те, що сигнал передається на базовій частоті, тобто без модуляції. Колись був розроблений широкосмуговий варіант 10Broad36, але він так і не з'явився на світовому ринку і практично зник. Нарешті, якщо йдеться про коаксіальний кабель, то після слова Base слідує закруглена до 100-метрових одиниць максимальна довжина мережного сегменту.

Таблиця 1. Найпоширеніші типи кабелів Ethernet

Таблиця 4.1. Наиболее распространенные типы кабелей Ethernet

Название	Тип	Максимальная длина сегмента	Узлов на сегмент	Преимущества
10Base5	Толстый коаксиальный	500 м	100	Первый кабель; ныне устарел
10Base2	Тонкий коаксиальный	185 м	30	Не нужны концентраторы
10Base-T	Витая пара	100 м	1024	Низкая цена
10Base-F	Оптоволокно	2000 м	1024	Лучший вариант при прокладке между зданиями

На зміну товстому Ethernet прийшов кабель типу 10Base2 («тонкий Ethernet»), який, на відміну від шлангоподібного 10Base5, чудово згинається. Для відведень замість зубастих відгалужувачів використовуються стандартні BNC-конектори, за допомогою яких легко утворюються T-подібні з'єднання. BNC-конектори простіші у використуванні і надійніші. Крім того, вони набагато дешевші, і їх зручніше монтувати. Недоліком є менша, ніж у 10Base5, максимальна довжина сегменту – 185 м, тобто на сегмент можна «посадити» не більше 30 машин.

Виявлення обривів кабелю, надмірної довжини сегментів, виходу з ладу відгалужувачів і з'єднувачів є основною проблемою обох типів кабелів. Були розроблені спеціальні методики, що дозволяють вирішити вказані задачі. Основна ідея така: по каналу передається імпульс певної форми. Якщо він зустрічає на своєму шляху яку-небудь перешкоду або кінець кабеля, утворюється ехо, яке приходить назад до відправника. Ретельно

вимірявши часовий інтервал між відправкою імпульсу і приходом еха, можна локалізувати несправність. Такий метод називається вимірюванням відображеного сигналу.

Задачі пошуку обривів кабелю привели до створення систем із зміненою схемою підключення, в якій від кожної станції кабель йде до центрального концентратора (хаба), де станції з'єднуються один з одним електронікою. Звичайно при цьому використовуються традиційні для телефонії виті пари, головним чином тому що більшість офісних приміщень вже обладнана відповідною проводкою з великим запасом. Така схема називається IOBase-T. Концентратори не буферизують вхідний трафік. Далі ми обговоримо поліпшені системи з використанням комутаторів (switch), що зберігають дані у власному буфері.

Всі три схеми підключення представлено на рис. 13. В 10Base5 приймач-передавач зовні обжимає кабель так, щоб його контактна голка стикалася з внутрішньою жилою. Він містить електронні компоненти, що дозволяють знаходити несучу і колізії. При цьому, знайшовши колізію, приймач-передавач розсилає по всьому кабелю спеціальний пакет, що повідомляє про збій. Таким чином гарантується, що вся решта приймачів-передавач теж зрозуміє, що відбулося зіткнення.

В схемі 10Base5 відгалужувальний кабель сполучає приймач-передавач з інтерфейсною платою (мережною картою) комп'ютера. Довжина цього кабелю може досягати 50 м. Він складається з п'яти незалежних ізольованих витих пар. Дві виті пари використовуються для передачі даних від комп'ютера і до комп'ютера. Ще по двох витих парах передаються управляючі сигнали. П'ята, не завжди використовується пара дозволяє комп'ютеру управляти живленням приймача-передавач. Деякі приймачі-передавач можуть обслуговувати до восьми комп'ютерів, що зменшує необхідну кількість прийому-передачі.

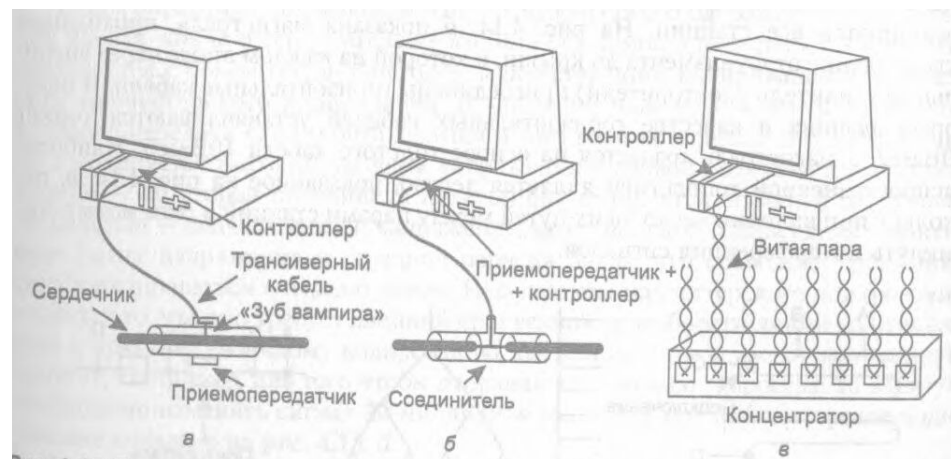


Рис. 13. Три типи кабельних з'єднань стандарту 802.3:10Base5(a); 10Base2(b); 10Base-T(s)

Трансіверний кабель закінчується на мережній платі, встановленій усередині комп'ютера. Мережна карта містить мікросхему контролера, що посилає кадри приймачу-передавач і приймаючу кадри у прийом-передачу. Контролер відповідає за правильний формат збору даних в кадри, а також за підрахунок контрольних сум вихідних кадрів і перевірку контрольних сум вхідних кадрів. Деякі контролери також управляють пулом буферів для кадрів, що приходять, і чергою буферів кадрів, що передаються, прямим доступом до пам'яті комп'ютера і іншими питаннями, пов'язаними з мережею.

В системі 10Base2 з'єднання з кабелем є звичайним Т-подібним пасивним BNC-конектором. Електроніка приймача-передавач розташовується на платі контролера, і у кожній станції звичайно є свій приймач-передавач.

В системі 10Base-T ніякого загального кабелю немає, є тільки концентратор (ящик, набитий електронікою), до якого кожна машина приєднана за допомогою свого власного кабелю. В такій конфігурації додавання і вилучення станції здійснюються простіше, а обрив кабелю виявляється досить легко. Недоліком системи 10Base-T є обмеження максимальної довжини кабелю завдовжки 100 м, в кращому разі 200 м, якщо використовуються високоякісні виті пари (категорії 5). Проте системи 10Base-T швидко стали домінувати в мережах Ethernet завдяки легкості їх установки і можливості використання вже існуючої стандартної телефонної проводки. Більш швидка версія системи 10Base-T (100Base-T) обговорюватиметься далі.

Четвертий можливий варіант кабелю для мереж Ethernet називається 10Base-F і побудований на основі оптоволоконного кабелю. Такий кабель досить дорогий внаслідок високої ціни з'єднувачів і термінаторів, проте він має відмінне відношення сигнал/шум і до того ж дозволяє сполучати дуже віддалені один від одного концентратори.

На рис. 14 зображено чотири способи прокладки кабелів в будівлі. На рис. 14, а єдиний кабель прокладається від кімнати до кімнати, і до нього під'єднуються всі станції. На рис. 14, б показана магістраль, що проходить крізь будівлю від фундаменту до даху, до якого на кожному поверсі через спеціальні підсилювачі (повторювачі) приєднані горизонтальні кабелі. В деяких будівлях як горизонтальні кабелі встановлюються тонкі 10Base2, а магістраль створюється на основі товстого кабелю 10Base5. Найпоширенішою топологією є дерево, показане на рис. 14, в, оскільки за наявності декількох шляхів між парами станцій в мережі може виникнути інтерференція сигналів.

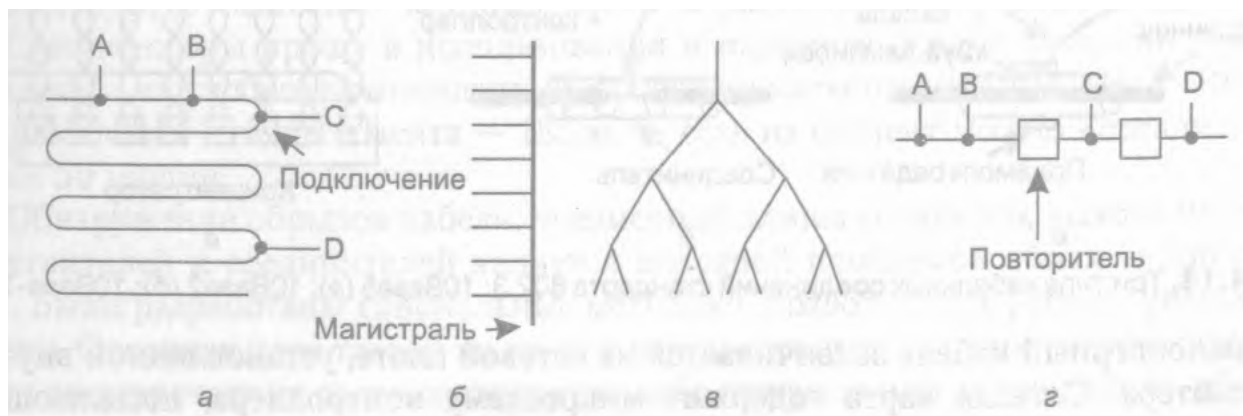


Рис. 14. Кабельна топологія: лінійна (а); магістраль (б); дерево (с); сегментована (г)

Всі версії стандарту 802.3 мають обмеження по довжині кабелів. Для побудови мереж великих розмірів декілька кабелів з'єднуються повторювачами, як показано на рис. 14, р. Повторювач – це пристрій фізичного рівня. Він приймає, підсилює (регенерує) і передає сигнали в обох напрямках. З погляду програмного забезпечення, ряд кабелів, сполучених повторювачами, не відрізняється від суцільного кабелю (відмінність полягає тільки в часовій затримці, пов'язаній з повторювачами). Система може складатися з великої кількості сегментів кабелю і повторювачів, проте два приймачі-передавач повинні бути на відстані не більше 2,5 км, між ними повинно бути не більше чотирьох повторювачів.

12.3. Манчестерський код

В жодній з версій Ethernet не застосовується пряме двійкове кодування біта 0 напругою 0В і біт 1 – напругою 5В, оскільки такий спосіб приводить до неоднозначності. Якщо одна станція посилає бітовий рядок

00010000, то інша може інтерпретувати її як 10000000 або 01000000, оскільки вони не зможуть відрізнити відсутність сигналу (0В) від біта 0 (0В). Можна, звичайно, кодувати одиницю позитивною напругою +1 В, а нуль – негативною напругою -1 В. Але при цьому все одно виникає проблема, пов'язана з синхронізацією передавача і приймача. Різні частоти роботи їх системного годинника можуть привести до розсинхронізації і невірної інтерпретації даних. В результаті приймач може втратити межу бітового інтервалу. Особливо велика ймовірність цього у разі довгої послідовності нулів або одиниць.

Таким чином, приймаючій машині потрібен спосіб однозначного визначення початку, кінця і середини кожного біта без допомоги зовнішнього таймера. Це реалізується за допомогою двох методів: манчестерського кодування і різницевого манчестерського кодування. В манчестерському коді кожний часовий інтервал передачі одного біта ділиться на два рівні періоди. Біт із значенням 1 кодується високим рівнем напруги в першій половині інтервалу і низьким – в другій половині, а нульовий біт кодується зворотною послідовністю – спочатку низька напруга, потім висока. Така схема гарантує зміну напруги в середині періоду бітів, що дозволяє приймачу синхронізуватися з передавачем. Недоліком манчестерського кодування є те, що воно вимагає подвійної пропускнуєї спроможності лінії по відношенню до прямого двійкового кодування, оскільки імпульси мають половинну ширину. Наприклад, для того, щоб відправляти дані із швидкістю 10 Мбіт/с, необхідно змінювати сигнал 20 мільйонів раз в секунду. Манчестерське кодування показано на рис. 15, б.

Різницеве манчестерське кодування, показане на рис. 15, в, є варіантом основного манчестерського кодування. В ньому біт 0 кодується зміною стану на початку інтервалу, а битий 1 – збереженням попереднього Рівня. В обох випадках в середині інтервалу обов'язково присутній перехід. Різницева схема вимагає складнішого устаткування, зате володіє доброю захищеністю від шуму. У всіх мережах Ethernet

використовується манчестерське кодування завдяки його простоті. Високий сигнал кодується напругою в $+0,85$ В, а низький сигнал - $-0,85$ В, внаслідок чого постійна складова напруги рівна 0 В. Разностное манчестерське кодування в Ethernet не використовується, але використовується в інших ЛВС (наприклад, стандарт 802.5, маркерне кільце).

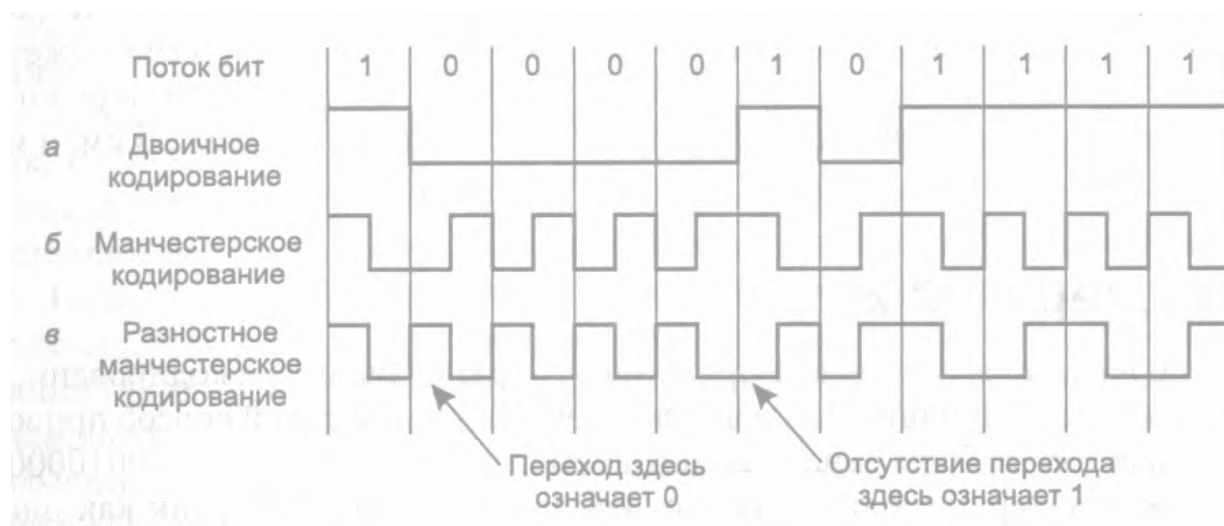


Рис. 15. Двійкове кодування (а); манчестерське кодування (б); різницеве манчестерське кодування (в)

12.4. Протокол підрівня управління доступом до середовища в Ethernet

Початкова структура кадру, запропонована свого часу DIX (DEC, Intel, Xerox), показана на рис. 16. Кожний кадр починається з поля Preamble (преамбула, заголовок) завдовжки 8 байт яке містить послідовність 10101010. Манчестерське кодування такої послідовності бітів дає в результаті меандр з частотою 10 МГц і

тривалістю 6,4 мкс, що дозволяє одержувачу синхронізувати свій годинник з годинником відправника. Далі до кінця кадру вони повинні зберігати синхронізований стан за рахунок манчестерського коду, що береже відмітки меж бітів.

Кадр містить дві адреси: одержувача і відправника. За стандартом дозволяються 2-байтові і 6-байтові адреси, проте параметри немодульованої передачі із швидкістю 10 Мбіт/с передбачають тільки 6-байтові адреси. Старший біт адреси одержувача містить 0 для звичайних адрес і 1 для групових одержувачів. Групові адреси дозволяють декільком станціям приймати інформацію від одного відправника. Кадр, що відправляється груповому адресату, може бути отриманий всіма станціями, що входять до цієї групи. Такий механізм називається груповою розсилкою. Якщо адреса складається тільки з одиниць, то кадр можуть прийняти абсолютно всі станції мережі. У такий спосіб здійснюється широкомовлення. Різниця між груповою розсилкою і широкомовленням дуже істотна, тому ще раз повторюваний: кадр, призначений для групової розсилки, посилається деякій групі станцій Ethernet; широкомовний же кадр одержують абсолютно всі станції мережі. Групова розсилка більш вибіркова, але вимагає деяких зусиль при управлінні групами. Широкомовлення – це більш груба технологія, але не вимагає ніякої настройки груп.

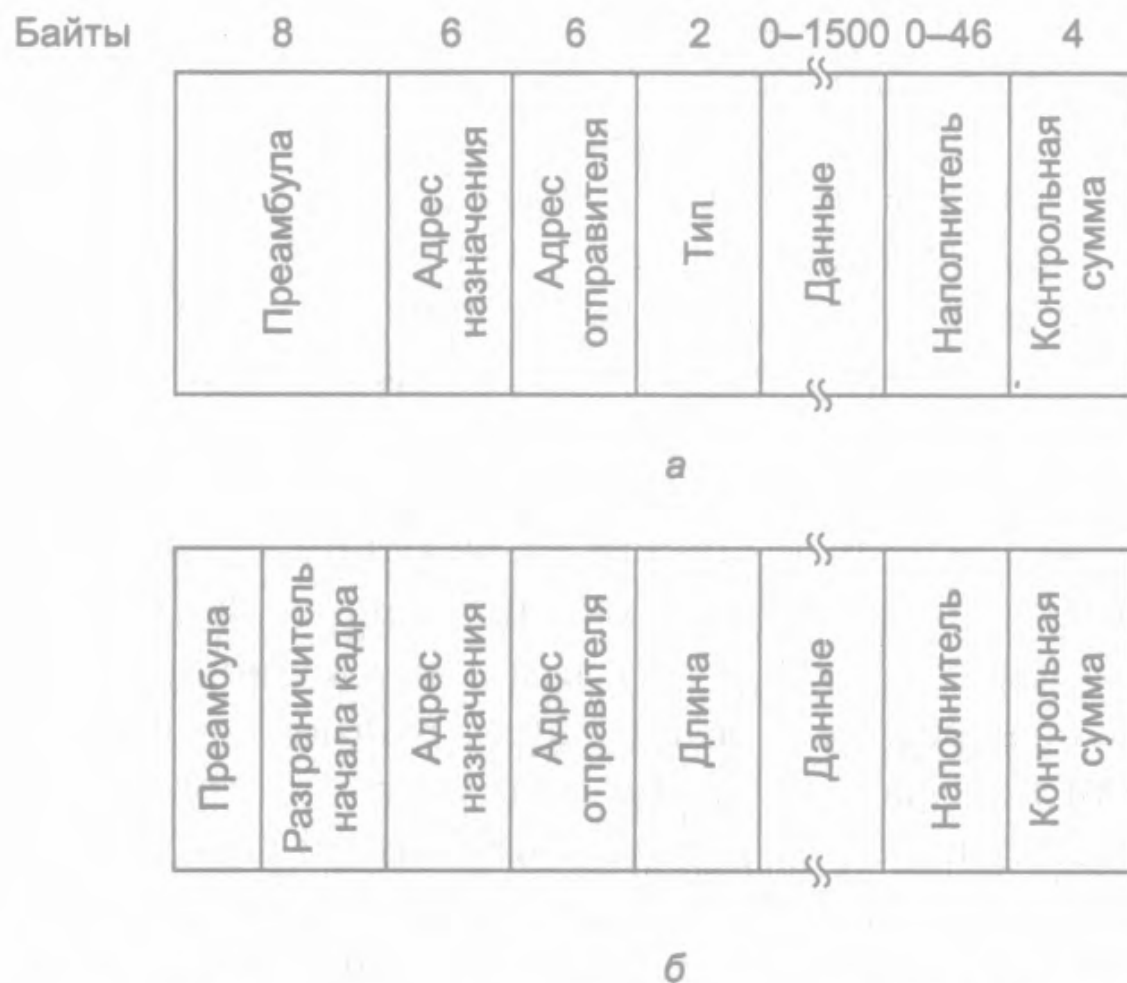


Рис. 16. Форматы кадров: DIX Ethernet (а); IEEE 802.3 (б)

Ще однією цікавою особливістю адресації є використання 46-го біта (сусіднього із старшим бітом), що дозволяє відрізнити локальні адреси від глобальних. Локальні адреси призначаються адміністратором кожної мережі і не мають сенсу за її межами. Глобальні адреси, навпаки, призначаються IEEE, і це гарантує, що одна і та ж глобальна адреса не використовується двома станціями. При $48 - 2 = 46$ доступних бітах може бути призначений близько $7 \cdot 10^{13}$ глобальних адрес. Ідея полягає в тому, що кожна станція може бути однозначно ідентифікований по її 48-бітовому номеру. Знайти по цьому номеру саму станцію – задача мережного рівня.

Потім слідує поле Туре, яке показує приймачу, що робити з кадром. Річ у тому, що одночасно на одній і тій же машині можуть працювати декілька протоколів мережного рівня, тому коли приходить кадр Ethernet, ядро повинне розуміти, якому протоколу його передати. Поле Туре визначає процес, який повинен узяти собі кадр.

Нарешті, за полем Туре слідує поле даних, розмір якого обмежений 1500 байтами. Таке обмеження було вибрано, загалом, довільно в ті часи, коли офіційно був закріплений стандарт DIX. При виборі посилалися на те, що приймачу-передавач потрібно досить багато оперативної пам'яті для того, щоб берегти весь кадр. А пам'ять в тому далекому 1978 році була ще дуже дорогою. Відповідно, збільшення верхньої межі розміру поля даних привело б до необхідності установки більшого об'єму пам'яті, а значить, до дорожчання всього приймача-передавач.

Тим часом, окрім верхньої межі розміру поля даних дуже важлива і нижня межа. Поле даних, що містить 0 байт, викликає певні проблеми. Річ у тому, що коли приймач-передавач знаходить зіткнення, він обрізує поточний кадр, а це означає, що окремі шматки кадрів постійно блукають по кабелю. Щоб було легшим відрізнити нормальні кадри від сміття, мережі Ethernet потрібен кадр розміром не менше 64 байт (від поля

адреси одержувача до поля контрольної суми включно). Якщо в кадрі міститься менше 46 байт даних, в нього вставляється спеціальне поле Pad, за допомогою якого розмір кадру доводиться до необхідного мінімуму.

Іншою (і навіть більш важливою) метою установки обмеження розміру кадру знизу є запобігання ситуації, коли станція встигає передати короткий кадр раніше, ніж його перший біт дійде до найдалшого кінця кабелю, де він може зіткнутися з іншим кадром. Ця ситуація показана на рис. 17. У момент часу 0 станція А на одному кінці мережі посилає кадр. Хай час проходження кадру по кабелю рівно t . За мить до того, як кадр досягне кінця кабелю (тобто у момент часу $t - \epsilon$), найдалша станція В починає передачу. Коли станція В помічає, що одержує велику потужність, ніж передає саму, вона розуміє, що відбулося зіткнення. Тоді вона припиняє передачу і видає 48-бітовий шумовий сигнал, застережливий решту станцій. Приблизно у момент часу $2t$ відправник помічає шумовий сигнал і також припиняє передачу. Потім він вичікує випадковий час і намагається відновити передачу.

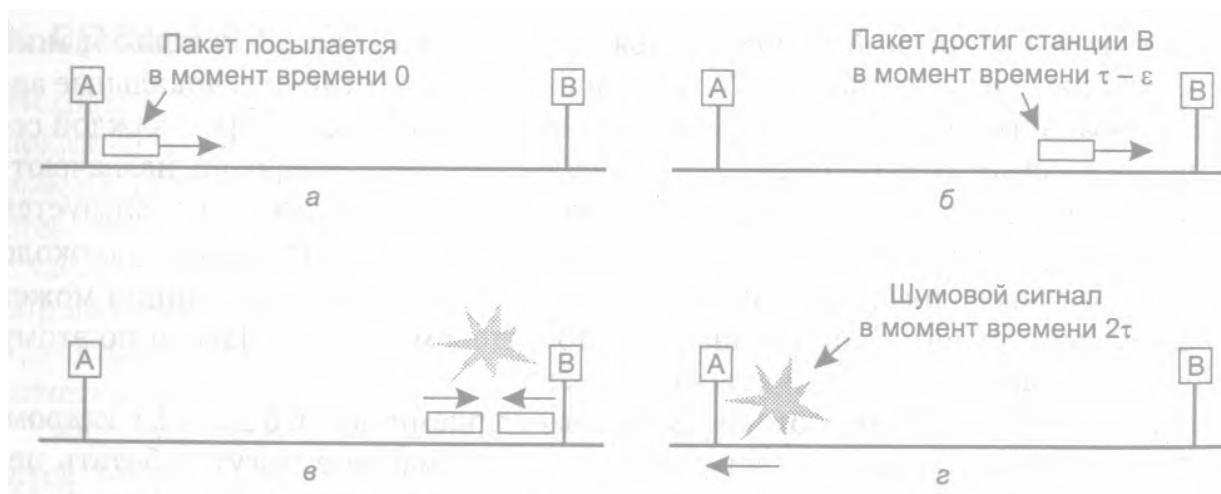


Рис. 4.17. Виявлення зіткнення може зайняти $2t$

Якщо розмір кадру буде дуже маленьким, відправник закінчить передачу перш, ніж отримає шумовий сигнал. В цьому випадку він не зможе зрозуміти, відбулося це зіткнення з його кадром або з якимсь іншим, і, отже, може припустити, що його кадр був успішно прийнятий. Для запобігання такої ситуації всі кадри повинні мати таку довжину, щоб час їх передачі було більше 2т. Для локальної мережі із швидкістю передачі 10 Мбіт/с при максимальній довжині кабелю в 2500 м і наявності чотирьох повторювачів (вимога специфікації 802.3) мінімальний час передачі одного кадру повинен складати у гіршому разі приблизно 50 мкс, включаючи час на проходження через повторювач, яке, зрозуміло, відмінне від нуля. Отже, довжина кадру повинна бути такою, щоб час передачі було принаймні не менше цього мінімуму. При швидкості 10 Мбіт/с на передачу одного біта витрачається 1000 нс, значить, мінімальний розмір кадру повинен бути рівний 500 біт. При цьому можна гарантувати, що система зможе знайти колізії в будь-якому місці кабелю. З міркувань більшої надійності це число було збільшено до 512 біт або 64 байт. Кадри меншого розміру за допомогою поля Pad штучно доповнюються до 64 байт.

У міру зростання швидкостей передачі даних в мережі мінімальний розмір кадру повинен збільшуватися, або повинна пропорційно зменшуватися максимальна довжина кабелю. Для 2500-метрової локальної мережі, що працює на швидкості 1 Гбіт/с, мінімальний розмір кадру повинен складати 6400 байт. Або ж можна використовувати кадр розміром 64 байт, але тоді треба скоротити максимальну відстань між станціями мережі до 250 м. У міру наближення до гігабітних швидкостей подібні обмеження стають все більш суворими.

Останнє поле кадру стандарту Ethernet містить контрольну суму. По суті справи, це 32-бітовий хеш-код даних. Якщо які-небудь біти прийняті неправильно (в результаті шуму в каналі), контрольна сума практично

напевно буде неправильною, і помилка, таким чином, буде помічена. Алгоритм обчислення контрольної суми заснований на циклічному надлишковому коді (CRC), який ми вже обговорювали.

Коли інститут IEEE приймав стандарт Ethernet, у формат кадру було внесено дві зміни, як показано на рис. 16, 6. По-перше, преамбула була зменшена до 7 байт, а останній байт був оголошений обмежувачем кадру (Start Frame) для сумісності із стандартами 802.4 і 802.5. По-друге, поле Турі було перетворено в Length. Звичайно, приймач при цьому втратив можливість визначення дії над кадром, що прийшов, але ця проблема була вирішена додаванням невеликого заголовка поля даних, призначеного саме для подібної інформації. Ми окремо обговоримо формат поля даних, коли розглядатимемо управління логічним з'єднанням.

На жаль, до часу публікації 802.3 по всьому світу розповсюдилося вже немало програмного забезпечення і устаткування, відповідного стандарту DIX Ethernet, тому зміна формату кадру була сприйнята виробниками і користувачами без ентузіазму. В 1997 році в IEEE зрозуміли, що боротися марно і безглуздо і оголосили обидва стандарти прийнятними. На щастя, всі поля Турі, що використалися до 1997 року, мали значення більше 1500. Відповідно, будь-які номери, менші або рівні 1500, можна було без сумнівів інтерпретувати як Length, а перевищуючі 1500 – як Турі. Тепер IEEE може говорити, що всі використовують запропонований їм стандарт, і при цьому всі користувачі і виробники можуть безсоромно продовжувати працювати точно так, як і раніше.

12.5. Алгоритм двійкової експоненціальної „відміни”

Розглянемо, як здійснюється рандомізація періоду очікування після зіткнення. Модель представлена на рис. 4.5. Після виникнення колізії час ділиться на дискретні інтервали, тривалість яких рівна максимальному часу кругового обігу сигналу (тобто його проходження по кабелю в прямому і зворотному напрямках), $2t$. Для

задоволення потреб Ethernet при максимальному розмірі мережі необхідно, щоб один інтервал складав 512 бітових інтервалів, або 51,2 мкс.

Після першого зіткнення кожна станція чекає або 0 або 1 інтервал, перш ніж спробувати передавати знову. Якщо дві станції зіткнуться і виберуть одне і те ж псевдовипадкове число, то вони зіткнуться знову. Після другого зіткнення кожна станція вибирає випадковим чином Про, 1, 2 або 3 інтервали з набору і чекає знову. При третьому зіткненні (ймовірність такої події після подвійного зіткнення рівна $1/4$) інтервали вибиратимуться в діапазоні від 0 до 2^3-1 .

В загальному випадку після g зіткнень випадковий номер вибирається в діапазоні від 0 до 2^i-1 , і ця кількість інтервалів станція пропускає. Проте після 10 зіткнень підряд інтервал рандомізації фіксується на відмітці 1023. Після 16 зіткнень підряд контроллер визнає свою поразку і повертає комп'ютеру помилку. Подальшим відновленням займаються більш високі рівні.

Цей алгоритм, званий двійковим експоненціальним алгоритмом відкоту, був вибраний для динамічного обліку кількості станцій, що намагаються здійснити передачу. Якщо вибрати інтервал рандомізації рівним 1023, то ймовірність повторного зіткнення дуже мала, проте середній час очікування складе сотні тактів, внаслідок чого середній час затримки буде дуже великий. З другого боку, якщо кожна станція вибиратиме час очікування всього з двох варіантів, 0 і 1, то у разі зіткнення сотні станцій вони продовжуватимуть стикатися знову і знову до тих пір, поки 99 з них не виберуть 1, а одна станція – 0. Такої події можна буде чекати протягом років. Експоненціально збільшуючи інтервал рандомізації у міру виникнення повторних зіткнень, алгоритм забезпечує невеликий час затримки при зіткненні невеликої кількості станцій і одночасно гарантує, що при зіткненні великого числа станцій конфлікт буде дозволений за розумний час.

Як впливає зведеного опису, в системі CSMA/CD немає підтвержень. Оскільки проста відсутність зіткнень ще не гарантує, що біти не були спотворені сплесками шуму в кабелі, для надійного зв'язку необхідно перевіряти контрольну суму і, якщо вона правильна, посилати відправнику кадр підтвердження. З погляду протоколу це буде ще один звичайний кадр, якому так само доведеться боротися за канал, як і інформаційному кадру. Проте нескладна модифікація алгоритму боротьби за канал дозволить прискорити пересилку підтвердження успішного прийому кадру (Tokoro and Tamaru, 1977). Все, що для цього вимагається, – зарезервувати перший часовий інтервал після успішної передачі кадру за що отримала цей кадр станцією. На жаль, стандарт не передбачає такої можливості.

12.6. Продуктивність мережі стандарту 802.3

Оцінимо продуктивність Ethernet в умовах великого постійного завантаження, тобто коли до станцій постійно готові до передачі. Строгий аналіз алгоритму двійкового експоненціального відкату досить складений. Натомість ми последmemo за міркуваннями Меткалфа (Metcalfe) і Боггса (Boggs) (1976) і припустимо, що ймовірність повторної передачі в кожному інтервалі часу постійна. Якщо кожна станція передає протягом одного інтервалу часу з ймовірністю p , то ймовірність того, що якій-небудь станції вдасться заволодіти каналом, рівна

$$A = kp(1 - p)^{k-1}. \quad (4.5)$$

Значення A буде максимальним, коли $p = 1/k$. При k , яке прямує до нескінченності, A прямуватиме до $1/e$. Ймовірність того, що період змагання за канал складатиметься рівно з j інтервалів, буде рівний s , отже, середнє число інтервалів боротьби за канал буде рівне

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

Оскільки тривалість кожного інтервалу часу рівна 2τ , середня тривалість періоду боротьби складатиме $w=2\tau/A$. При оптимальному значенні ймовірності p середня кількість інтервалів за період боротьби ніколи не перевершуватиме e , таким чином, середня тривалість періоду боротьби буде рівна $2\tau e \approx 5,4\tau$.

Якщо середній час передачі кадру складає P секунд, то ефективність каналу при його сильній завантаженості буде рівна

$$\text{Эффективность канала} = \frac{P}{P + 2\tau/A}. \quad (4.6)$$

В цій формулі ми бачимо, як максимальна довжина кабелю впливає на продуктивність, і стає очевидним недолік топології мережі, показаної на рис. 14, а. Чим довший кабель, тим довшим стає період боротьби за канал. З цих міркувань стає зрозуміло, чому стандарт Ethernet накладає обмеження на максимальну відстань між станціями.

Корисно переформулювати рівняння (4.6) в термінах довжини кадру K пропускної спроможності мережі B , довжини кабелю L і швидкості розповсюдження сигналу c для оптимального випадку: e інтервалів зіткнень на кадр. При $P = F/B$ рівняння (4.6) прийме вигляд

$$\text{Ефективність каналу} = \frac{1}{1 + 2BLE/cF} \quad (4.7)$$

Якщо другий доданок дільника великий, ефективність мережі буде низькою. Зокрема, збільшення пропускної спроможності або розмірів мережі (добуток BL) зменшить ефективність при заданому розмірі кадру. На жаль, основні дослідження в області мережного устаткування націлені саме на збільшення цього твору. Користувачі хочуть великої швидкості при великих відстанях (що забезпечують, наприклад, оптоволоконні регіональні мережі), отже, для даних додатків стандарт Ethernet буде не кращим рішенням.

На рис. 18 показана залежність ефективності каналу від числа готових станцій для $2\tau = 51,2$ мкс і швидкості передачі даних, рівної 10 Мбіт/с. Для розрахунків використовується рівняння (4.7). При 64-байтному часовому інтервал 64-байтні кадри виявляються неефективними, і це не дивно. З другої сторони, якщо використовувати кадри завдовжки 1024 байти, то при асимптотичному значенні e періоду змагання за канал, рівному 64-байтовому інтервал; тобто 174 байтам, ефективність каналу складе 85 %.

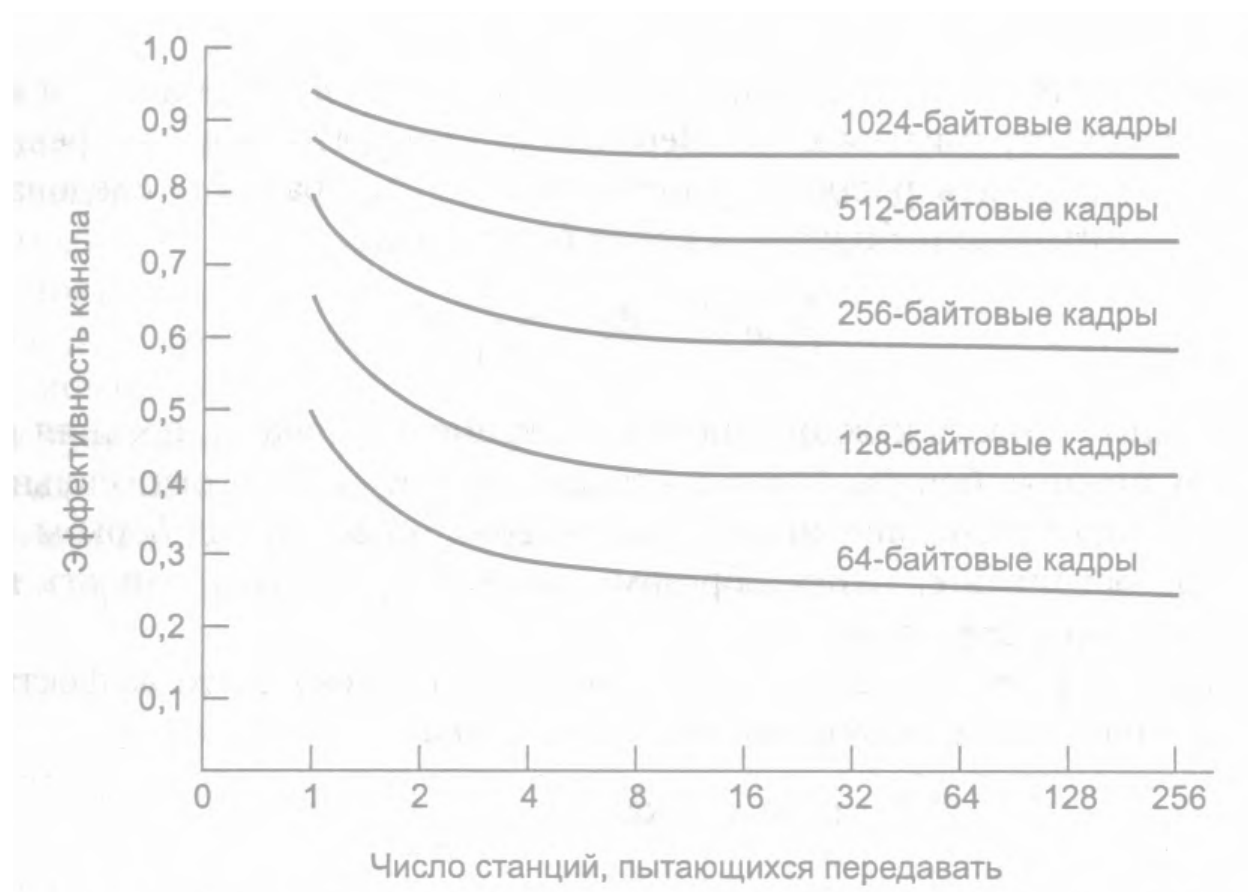


Рис. 18. Ефективність мереж стандарту 802.3 на швидкості 10 Мбіт/с з 512-бітовими інтервалами часу

Щоб визначити середню кількість станцій, готових до передачі в умовах сильного завантаження, можна скористатися наступною грубою моделлю. Кожний передаваний кадр займає канал на період змагання і на час передачі кадру, що складає в сумі $P+w$ секунд. Таким чином, за секунду $p <$ каналу передається $1/(P + w)$ кадрів.

Якщо кожна станція формує кадри із середньою швидкістю X кадрів в секунду, то при знаходженні системи в стані k сумарна вхідна швидкість k незаблокованих станцій складе kX кадрів на секунду. Оскільки в стані рівноваги вхідна швидкість повинна бути рівна вихідній, ми можемо прирівняти ці дві швидкості і вирішити рівняння відносно k . (Зверніть увагу: w є функцією від k).

Слід зазначити, що теоретичному аналізу продуктивності мереж Ethernet (і інших мереж) було присвячено багато робіт. Практично у всіх цих дослідженнях передбачається, що трафік підкоряється пуассонівському розподілу. Коли ж дослідники розглянули реальні потоки даних, то виявилось, що мережний трафік рідко розподілений по Пуассону, а частіше буває автомодельним. Це означає, що при збільшенні періоду усереднювання трафік не згладжується. Дисперсія середовищ його кількості пакетів в кожну хвилину години не менше дисперсії середньої кількості пакетів в кожну секунду хвилини. Следствием цього відкриття є те, що більшість моделей мережного трафіку не відповідає реальній роботі мереж і тому повинні сприйматися дуже критично.

12.7. Комутовані мережі Ethernet

При додаванні станцій до Ethernet трафік спочатку ростиме. Нарешті, локальна мережа насититься. Одним з рішень в даному випадку є збільшення швидкості передачі даних – наприклад, перехід з 10 Мбіт/с на 100 Мбіт/с. Проте частка мультимедійних даних в загальному потоці стає все помітнішою, і навіть 100-мегабітні і гігабітні версії Ethernet можуть перестати справлятися із своєю задачею.

На щастя, можливо не таке радикальне рішення, а саме, комутована локальна мережа Ethernet. Серцем системи є комутатор, що містить високошвидкісну плату, в слоти якій звичайно вставляються від 4 до 32

контроллерів ліній, в кожному з яких від одного до восьми роз'ємів. Частіше за все до роз'єму підключається вита пара 10Base-T, що з'єднує комутатор з єдиним хостом.

Коли станція хоче передати кадр Ethernet, вона посилає стандартний кадр в комутатор. Плата в комутаторі, отримавши кадр, перевіряє, чи не адресований цей кадр станції, приєднаної до тієї ж плати. Якщо так, то кадр пересилається їй. В іншому випадку кадр пересилається по об'єднувальної плати, до якої підключена станція-одержувач. Об'єднувальна плата звичайно працює на швидкості в декілька гігабіт в секунду з використанням власного протоколу.

Що відбудеться, якщо дві машини, приєднані до однієї і тієї ж карти комутатора, одночасно стануть передавати кадри? Результат залежить від конструкції карти. Одним з варіантів може бути об'єднання всіх портів карти разом з утворенням на карті невеликої локальної мережі. Зіткнення у такій мережі виявляються і обробляються так само, як і в будь-кому іншій мережі CSMA/CD – при допомозі повторних передач кадрів з використанням алгоритму двійкового експоненціального відкату. При використуванні такого типу карт в кожний момент часу можлива передача тільки однієї станції з підключених до карти, але всі карти можуть передавати або приймати дані паралельно. При такій схемі комутатора кожна карта утворює свій простір зіткнень, незалежний від інших. Наявність тільки однієї станції в просторі зіткнень виключає власне зіткнення і підвищує продуктивність.

Можливий також інший різновид карт – з буферизацією даних, що приходять на кожний вхід, в оперативній пам'яті карти. При цьому всі вхідні порти можуть передавати і приймати кадри одночасно в дуплексному режимі, що далеко не завжди вдається реалізувати в моноканалі із застосуванням CSMA/CD. Після прийому кадру карта може перевірити, кому він призначається. Якщо адресатом є якийсь з портів поточної

карти, то кадр зразу ж туди і передається. Якщо ж потрібно передати дані на порт іншої карти, то це робиться за допомогою об'єднувальної плати. При цьому кожний порт має окремий простір колізій, тому зіткнення не виникають. Загальна продуктивність системи може бути підвищена на порядок в порівнянні з 10Base5, оскільки в останній використовується єдиний простір зіткнень.

Оскільки комутатор чекає на кожному вхідному порту кадри Ethernet, можна використовувати деякі з цих портів як концентратори. На рис. 19 порт в правому верхньому кутку сполучено не з однією станцією, а з 12-портовим концентратором. Прибуваючи в концентратор, кадри змагаються звичайним способом, включаючи зіткнення і двійковий відкат. Вдалі кадри потрапляють в комутатор і піддаються там тій же процедурі, що і вся решта кадрів, тобто перенаправляються на потрібні вихідні лінії через високошвидкісну об'єднуючу плату. Концентратори дешевші за комутатори, проте їх швидке здешевлення означає тенденцію, що лише намічається, до застарівання. Проте, все ще існують діючі концентратори.

Тема 13. Безпроводові мережі (БМ)

13.1. Загальна характеристика і класифікація БМ

13.2. Стандарт БМ IEEE 802.11

13.2.1 Стек протоколів

13.2.2 Фізичний рівень

13.2.3 Протокол підрівня управління доступом до середовища

13.2.4 Структура кадру

13.2.5 Сервіси

13.3. Широкополосні БМ

13.3.1 Порівняння стандартів 802.11 і 802.16

13.3.2 Стек протоколів

13.3.3 Фізичний рівень

13.3.4 Протокол підрівня MAC

13.3.5 Структура кадру

13.4. Безпроводова технологія Bluetooth

13.4.1 Архітектура Bluetooth

13.4.2 Застосування Bluetooth

13.4.3 Набір протоколів

13.4.4 Рівень радіозв'язку

13.4.5 Рівень немодульованої передачі

13.4.6 Рівень L2CAP

13.4.7 Структура кадру

13.1. Загальна характеристика і класифікація БМ

Ідея цифрового безпроводового зв'язку не нова. Вже в 1901 році італійський фізик Гульєльмо Марконі (Guglielmo Marconi) продемонстрував телеграфний зв'язок між кораблем і берегом за допомогою азбуки Морзе, що складається з крапок і тире, що вельми схоже на двійковий код. Сьогоднішні цифрові радіосистеми володіють більш високою продуктивністю, проте в їх основі лежить та ж ідея.

В першому наближенні БМ можна розбити на наступні три категорії:

- ◆ взаємодіючі системи;
- ◆ безпроводові ЛОМ (LAN);
- ◆ безпроводові глобальні мережі (WAN).

Під взаємодіючими системами розуміється перш за все поєднання між собою компонентів комп'ютера з використанням радіохвиль малого радіусу дії. Майже будь-який комп'ютер складається з декількох частин: монітора, клавіатури, миші, принтера... Кожний з цих зовнішніх пристроїв, як відомо, під'єднується до системного блоку за допомогою кабелів. А знаєте, скільки проблем з підключенням цієї техніки виникає у новачків, не дивлячись на маркіровку роз'ємів і докладне керівництво по експлуатації? Недаремно ж більшість фірм, торгуючих комп'ютерами, пропонує послуги технічної служби, що полягають тільки в з'єднанні компонентів системи. Декілька компаній одна за одною прийшли до ідеї створення безпроводової призначеної

системи **Bluetooth**, для того, щоб позбавити компоненти комп'ютера від кабелів і роз'ємів. Окрім стандартних пристроїв, за допомогою Bluetooth можна підключати до комп'ютера цифрові камери, гарнітури, сканери і ін. Тобто тепер практично будь-які цифрові пристрої, розташовані недалеко від системного блоку, можна з'єднати з ним БМ. Ніяких дротів, ніяких роз'ємів, ніяких драйверів. Потрібно просто принести пристрій, включити його, і воно працюватиме. Для багатьох початківців користувачів така простота – великий плюс.

В найпростішому випадку взаємодія усередині системи підкоряється принципу «головний - підлеглий». Системний блок частіше за все виступає в ролі головного пристрою, а всі інші – в ролі підлеглих. В чому полягає це верховенство? Саме системний блок призначає адреси пристроїв, визначає моменти, в які вони можуть «віщати», обмежує час передачі, задає діапазони робочих частот і т.д.

Наступним кроком в розвитку цього напрямку стали **безпроводові ЛОМ** (локальні обчислювальні мережі). В них кожний комп'ютер обладнаний радіомодемом і антеною, з їх допомогою він може обмінюватися даними з іншими комп'ютерами. Іноді є загальна антена, розташована на стелі, і передача даних відбувається через неї, але якщо робітники станції мережі розташовані достатньо близько, то звичайно використовують однорангову конфігурацію. Беспроводні мережі все ширше використовуються в бізнесі і для домашніх цілей, де прокладати Ethernet немає ніякого значення, а також в старих будівлях, що орендуються під офіси, в кафетеріях, в офісних центрах, конференц-залах і інших місцях. Стандарт БМ має маркіровку **IEEE 802.11**, і саме він частіше всього реалізується і стає все більш популярним.

Третій тип БМ використовується в глобальних мережах. Прикладом може служити система стільниковому зв'язку, є насправді низькопродуктивною цифровою БМ. Виділяють вже цілих три покоління стільникового зв'язку. Перші стільникові мережі були аналоговими і призначалися тільки для передачі мови. Друге покоління

було вже цифровим, але нічого, окрім мови, передавати було як і раніше не можна. Нарешті, нинішнє, третє покоління – цифрове, причому з'явилася можливість передачі як голосу, так і інших даних. В деякому розумінні, стільникові мережі – це ті ж безпроводові ЛОМ, різниця лише в зоні обхвату і більш низкою швидкості передачі. Якщо звичайні БМ можуть працювати з швидкістю до 50 Мбіт/с на відстані десятків метрів, то стільникові системи передають дані на швидкості 1 Мбіт/с, але відстань від базової станції до комп'ютера або телефону обчислюється кілометрами, а не метрами.

Зараз розвиваються не тільки низько-, але і високопродуктивні глобальні БМ. Початкова установка така: необхідно організувати доступ в Інтернет з нормальною швидкістю, щоб при цьому не був задіяний телефон. Таку послугу іноді називають локальною багатовузловою системою розподілу.

Майже всі БМ в якомусь місці мають шлюз, що забезпечує зв'язок із звичайними комп'ютерними мережами, інакше просто неможливо було б організувати, припустимо, доступ в Інтернет.

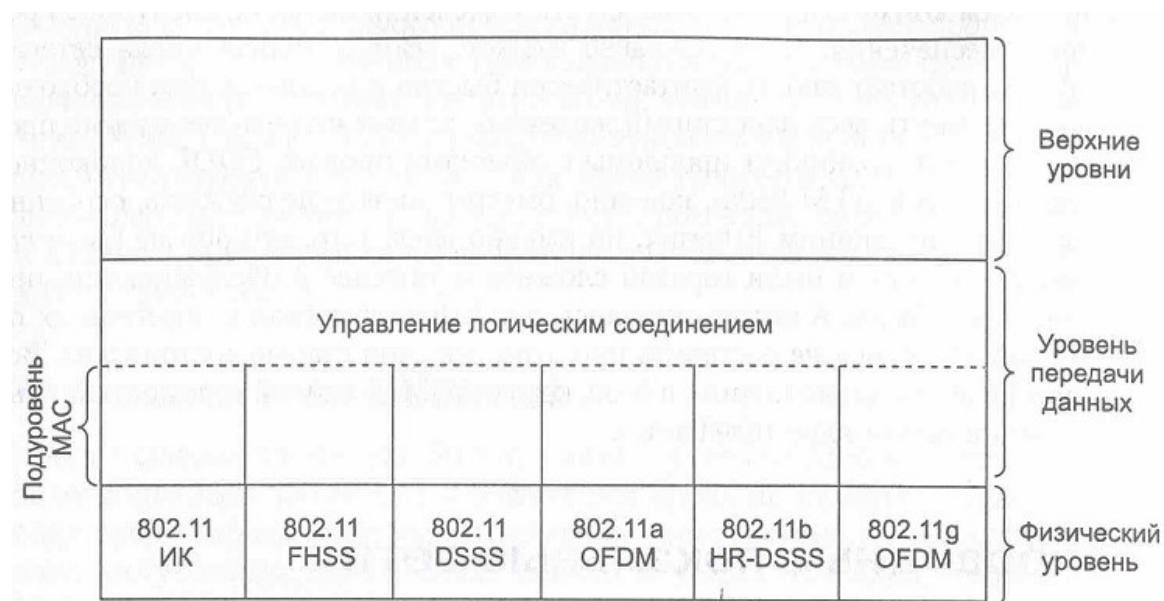
Федеральна комісія з електрозв'язку США (FCC) визначила такі категорії PCS (Personal Communication Services) та відповідні смуги частот:

- вузькосмугові PCS (діапазон 900-901, 930-931, 940-941 МГц) для високошвидкісних пейджерних систем, двонапрявленого передавання повідомлень, передавання мовленнєвих повідомлень;
- широкосмугові PCS (120, 1850-2200 МГц); стільниковий зв'язок - цифрове передавання мовлення та даних.
- неліцензовані PCS (40 МГц, від 1890 до 1930 МГц) - БМ та АТС організацій у найближчому радіусі дії - у межах одного будинку або групи будівель. Неліцензовані PCS забезпечують передавання даних зі швидкістю до 10 Мбіт/с.

13.2. Стандарт БМ IEEE 802.11

13.2.1 Стек протоколів

Всі протоколи, що використовуються сімейством стандартів 802.x, схожі по структурі. Частина стека протоколів зображена на мал. 4.22. Фізичний рівень практично відповідає фізичному рівню в моделі OSI, а ось рівень передачі даних у всіх протоколах 802.x розбитий на два або більш підрівня. Що стосується 802.11, то підрівень MAC (підрівень управління доступом до середовища) відповідає за розподіл каналу, тобто за те, яка станція передаватиме слідуноюю. Над MAC в ієрархії знаходиться підрівень LLC (управління логічним з'єднанням), задача якого полягає в тому, щоб зробити відмінності стандарт 802.x невидимими для мережного рівня.



Мал. 4.22. Частина стека протоколів 802.11

Стандарт 802.11 1997 року визначає три методи передачі, реалізовані на фізичному рівні. Метод інфрачервоної передачі сильно нагадує метод, що використовується в системах дистанційного керування побутовою технікою. В двох інших методах застосовується радіозв'язок невеликого радіусу дії (при цьому працюють методи FHSS і DSSS). Вони обидва використовують не підлягаючу ліцензуванню частина спектру (діапазон ISM 2,4 ГГц). В цій же частині спектру здійснюють передачу сигналу радіобрелки відкриття воріт гаражів, так що не дивуйтеся, якщо ваш ноутбук не зможе в якийсь момент поділити ефір з вашим же гаражем. Крім того, в цьому ж діапазоні працюють домашні радіотелефони і СВЧ-печі. Незалежно від методу швидкість роботи складає 1-2 Мбіт/с, і сигнал використовується відносно малопотужний, що дозволяє зменшити кількість

конфліктів між передавачами. З метою збільшення пропускної спроможності в 1999 році були розроблено два додаткові методи: OFDM і HR-DSSS. Вони працюють з швидкостями 54 Мбіт/с і 11 Мбіт/с відповідно. В 2001 році була представлена нова модифікація OFDM, що працює в іншому частотному діапазоні. Зараз ми вивчимо коротко всі ці методи. Вони відносяться до фізичного рівня.

13.2.2 Фізичний рівень

Всі п'ять методів передачі даних, що розглядаються далі дозволяють передати кадр підрівня MAC з однієї станції на іншу. Розрізняються вони технологіями і досяжними швидкостями, що використовуються.

При передачі в інфрачервоному діапазоні (зовні діапазону видимого світла) використовуються довжини хвиль 0,85 або 0,95 мкм. Можливі дві швидкості передачі: 1 і 2 Мбіт/с. При 1 Мбіт/с використовується схема кодування з угрупованням чотирьох біт в 16-бітове кодове слово, що містить 15 нулів і 1 одиницю. Це так званий **код Грея**. Одна з його властивостей полягає в тому, що невелика помилка в синхронізації може привести у гіршому разі до помилки в одному біті вихідної послідовності. При швидкості передачі 2 Мбіт/с вже 2 біти кодуються в 4-бітове кодове слово, також що має всього одну одиницю: 0001, 0010, 0100 або 1000. Сигнали інфрачервоного діапазону не проникають крізь стіни, тому стільники, розташовані в різних кімнатах, дуже добре ізольовані один від одного. Проте через досить низьку пропускну спроможність (а також тому що сонячне світло може спотворювати інфрачервоні сигнали) цей метод не дуже популярний.

В методі **FHSS** (Frequency Hopping Spread Spectrum – передача широкосмугових сигналів по методу частотних стрибків) використовуються 79 каналів шириною 1 МГц кожний. Діапазон, в якому працює цей метод, починається з 2,4 ГГц (це неліцензійований [ISM] діапазон). Для визначення послідовностей стрибків

частот використовується генератор псевдовипадкових чисел. Оскільки при цьому для всіх станцій використовується один і той же генератор, вони синхронізовані в часі і одночасно здійснюють однакові частотні скачки. Період часу, протягом якого станція **працює** на певній частоті, називається часом перебування. Це величина, що настраюється, але вона повинна бути не більше 400 мс. Рандомізація, здійснювана в методі FHSS, є простим способом розподілу некерованого ISM-діапазону. Крім того, постійна зміна частот – це непоганий (хоча, звичайно, недостатній) спосіб захисту інформації від несанкціонованого прослуховування, оскільки непроханий слухач, не знаючи послідовності частотних переходів і часу перебування, не зможе підслухувати передавані дані. При зв'язку на більш довгих дистанціях може виникати проблема багатопроменевого загасання, і FHSS може виявитися хорошою підмогою в боротьбі з нею. Цей метод також відносно слабо чутливий до інтерференції з радіосигналом, що робить його популярним при зв'язку між будівлями. Головний недолік FHSS – це низька пропускна спроможність.

Третій метод модуляції називається **DSSS** (Direct Sequence Spread Spect-*jj*Sim – передача широкосмугового сигналу по методу прямої послідовності). Швидкості передачі обмежені 1 або 2 Мбіт/с. DSSS трохи нагадує ту, що вже обговорювалася в розділі «Друге покоління мобільних телефонів: цифрова передача голосу» систему CDMA, проте має і деякі відмінності. Кожний біт передається у вигляді 11 елементарних сигналів, які називаються послідовністю **Баркера**. Для цього використовується модуляція з фазовим зсувом із швидкістю 1 Мбод (1 біт на бод при роботі на 1 Мбіт/с і 2 біти на бод при роботі на 2 Мбіт/с). Протягом декількох років комісія FCC вимагала, щоб все безпроводове устаткування в США працювало в неліцензійованих діапазонах, проте в травні 2002 року ця вимога була знята, оскільки з'явилися нові технології.

Перша високошвидкісна безпроводова ЛОМ, **802.11a**, використовувала метод **OFDM** (Orthogonal Frequency Division Multiplexing – ортогональне частотне ущільнення) для передачі сигналу з швидкістю до 54 Мбіт/с в розширеному неліцензійованому діапазоні 5 ГГц. Як і вважається при частотному ущільненні тут використовуються різні частоти. Всього їх 52, з них 48 частот призначено для даних, 4 – для синхронізації (майже як в ADSL). Одночасна передача сигналів на різних частотах дозволяє говорити про розширений спектр, хоча цей метод істотно відрізняється від CDMA і FHSS. Розділення сигналу на багато вузьких діапазонів має переваги перед передачею в одному широкому діапазоні – зокрема, більш низьку чутливість до вузькополосній інтерференції і можливість використання незалежних діапазонів. Система кодування досить складна. Вона заснована на модуляції з фазовим зсувом для швидкостей до 18 Мбіт/с і на QAM при більш високих швидкостях. При 54 Мбіт/с 216 біт даних кодуються 288-бітовими кодовими словами. Однією з переваг OFDM є сумісність з Європейською системою HiperLAN/2 (Doufexi і ін., 2002). Метод має хорошу спектральну ефективність в термінах співвідношення біт/герц і хороший імунітет проти багатопроменевого загасання.

Нарешті, ми підійшли до методу **HR-DSSS** (High Rate Direct Sequence Spread Spectrum – високошвидкісна передача широкосмугового сигналу по методу прямої послідовності). Це ще один широкосмуговий спосіб, який для досягнення швидкості 11 Мбіт/с кодує біти із швидкістю 11 мільйонів елементарних сигналів в секунду. Стандарт називається 802.11b, **але** він не є послідовником 802.11a. Насправді 802.11b був визнаний і потрапив на ринок навіть раніше, ніж 802.11a. Швидкості передачі даних, підтримувані цим стандартом, рівні 1, 2, 5,5 і 11 Мбіт/с. Дві низькі швидкості вимагають 1 Мбод при 1 і 2 бітах на бод відповідно. Використовується модуляція з фазовим зсувом (для сумісності з DSSS). Дві високі **швидкості вимагають кодування** із швидкістю 1,375 Мбод при 4 і 8 бітах на бод відповідно. Застосовується код Уолша – Адамара. Швидкість передачі може бути

динамічно змінений під час роботи для досягнення оптимальних результатів залежно від умов навантаження і зашумленості лінії. На практиці швидкість роботи стандарту 802.11b майже завжди рівна 11 Мбіт/с. Хоча 802.11b повільніше, ніж 802.11a, діапазон першого майже в 7 разів ширше, що дуже важливе в багатьох ситуаціях.

Поліпшена версія 802.11b називається **802.11g**. Цей стандарт був прийнятий IEEE в листопаді 2001 року після довгих обговорень того, чия ж патентована технологія застосовуватиметься. У результаті в 802.11g застосовується метод модуляції OFDM, узятий з 802.11a, проте робочий діапазон співпадає з 802.11b (вузький неліцензуючий діапазон 2,4 ГГц). Теоретично максимальна швидкість 802.11g рівна 54 Мбіт/с. Дотепер не дуже зрозуміло, чи може бути досягнутий така швидкість на практиці. Зате, поки суть та справа, комітет 802.11 може гордо заявити, що він розробив три високошвидкісні стандарти безпроводових ЛОМ: 802.11a, 802.11b і 802.11g (не кажучи вже про три низькошвидкісних безпроводових ЛОМ). Можна цілком обгрунтовано дивуватися з того, що ж в цьому хорошого. Ну, мабуть, три – це просто щасливе число для комітету 802.11.

13.2.3 Протокол підрівня управління доступом до середовища

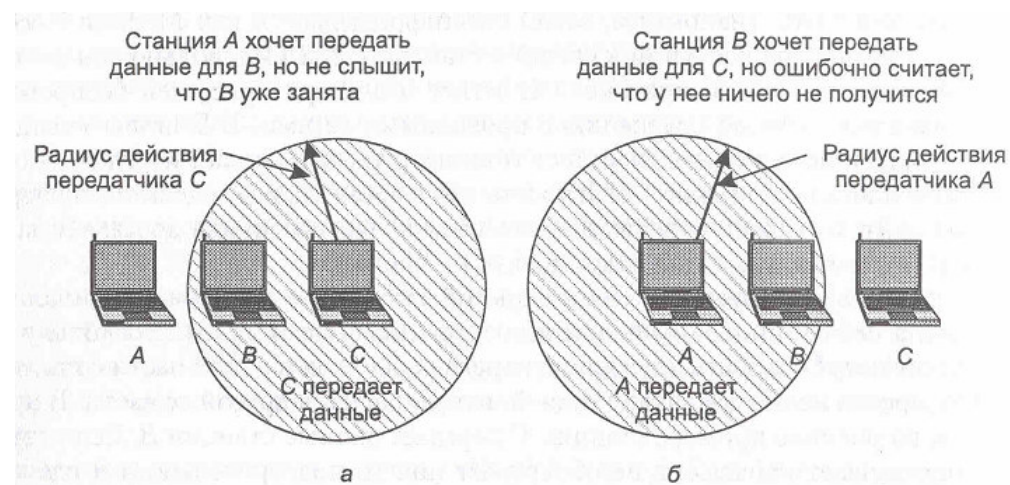
Протокол підрівня MAC (нагадаємо, MAC розшифровується як Medium Access Control – управління доступом до середовища) в стандарті 802.11 досить сильно відрізняється від аналогічного протоколу Ethernet завдяки властивій БМ складності в порівнянні з кабельними мережами. В Ethernet станція просто чекає, поки в каналі настане тиша, і тоді починає передачу. Якщо шумовий сплеск не приходить назад в перебіг часу, необхідного на пересилку 64 байт, то можна затверджувати, що кадр майже напевно доставлений коректно. В БМ такий фокус не проходить.

По-перше, існує проблема прихованої станції – ми вже згадували про неї раніше, а зараз приводимо ще і ілюстрацію (мал. 4.23, а). Оскільки не всі станції можуть чути один одного, передача, що йде в одній частині стільника, може не бути просто сприйнятий станцією, що знаходиться в іншій її частині. В приведеному на малюнку прикладі станція З передає дані станції В. Если станція А прослуховуватиме канал, вона не знайде нічого підозрілого і зробить помилковий висновок про те, що вона має право почати передачу станції В. Крім того, є і зворотна проблема, показана на мал. 4.23, би. Тут В хоче відправити дані для станції З і прослуховує канал. Почувши, що в ньому вже здійснюється якась передача, станція В робить знову-таки помилковий висновок про те, що передача для Із зараз неможлива. Тим часом станція А – джерело сигналу, який збентежив станцію В, – може насправді здійснювати передачу для станції D (на малюнку не показана). Ситуація усугубляє ще і тим, що більшість радіосистем є напівдуплексною, тобто не може одночасно і на одній і тій же частоті посилати сигнали і сприймати сплески шуму на лінії. У результаті 802.11 не може використовувати, як Ethernet, метод CSMA/CD.

Як боротися з цією проблемою? Стандарт 802.11 підтримує два режими роботи. Перший називається **DCF** (Distributed Coordination Function – розподілена координація) і не має ніяких засобів централізованого управління (в цьому значенні нагадуючи Ethernet). Другий режим, PCF (Point Coordination Function – зосереджена координація), має на увазі, що базова станція бере на себе функцію управління активністю всіх станцій даного стільника. Всі реалізації стандарту повинні підтримувати DCF, тоді як PCF є додатковою можливістю.

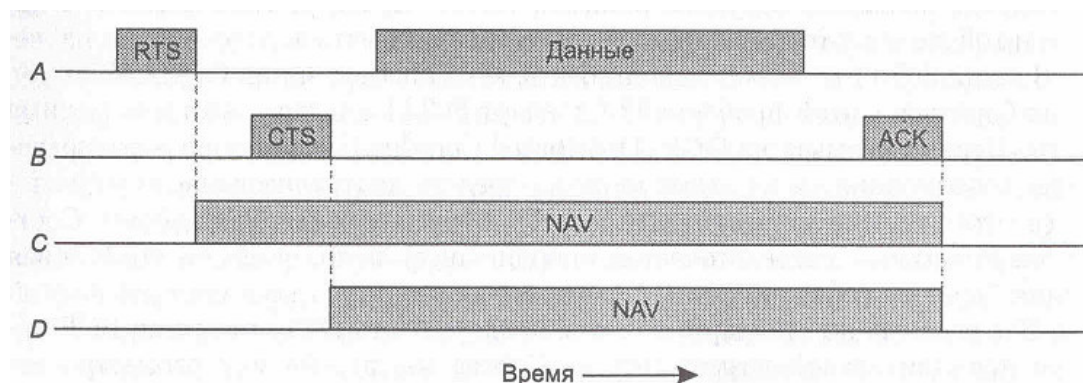
В режимі DCF 802.11 використовує протокол, званий CSMA/CA (CSMA with Collision Avoidance – CSMA із запобіганням колізій). Тут ведеться прослуховування як фізичного, так і віртуального каналу. Протокол

CSMA/CA може працювати в двох режимах. В першому режимі станція перед передачею прослуховує канал. Якщо він вільний, починається пересилка даних. Під час пересилки канал не прослуховується, і станція передає кадр цілком, причому він може бути зруйнований на стороні приймача через інтерференцію сигналів. Якщо канал зайнятий, відправник чекає його звільнення і потім починає передачу. Якщо виникає колізія, станції, що не поділили між собою канал, вичікують протягом випадкових інтервалів часу (використовується двійковий експоненціальний відкіт такий же, як в Ethernet) і потім знову намагаються відправити кадр.



Мал. 4.23. Проблема прихованої станції (а); проблема засвіченої станції (б)

Інший режим CSMA/CA заснований на протоколі MACAW і використовує контроль віртуального каналу, як показано на мал. 4.24. В даному прикладі станція A хоче передати дані станції B. Станція C знаходиться в зоні дії (тобто чує) A, а також, можливо, в зоні дії B, але це не має значення. Станція D входить в зону дії B, але не входить в зону дії A.



Мал. 4.24. Використання прослуховування віртуального каналу в протоколі CSMA/CA

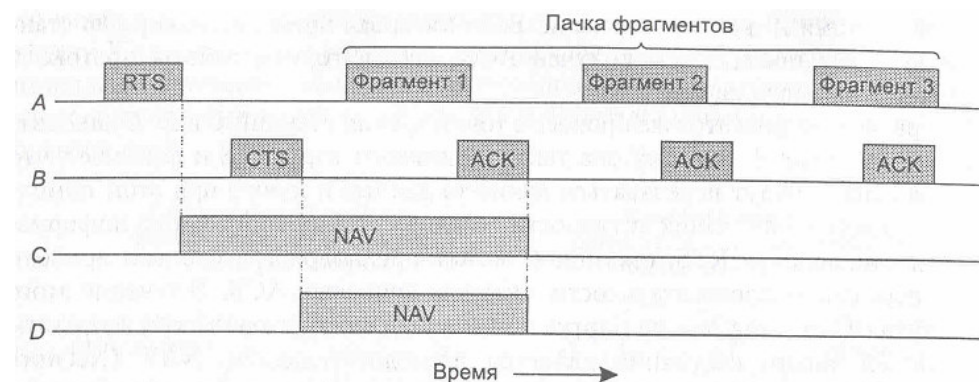
Протокол починає працювати тоді, коли *A* вирішує, що їй необхідно послати дані *B*. *A* посилає станції *B* кадр RTS, запрошуючи дозвіл на передачу. Якщо *B* може прийняти дані, вона посилає назад позитивне підтвердження, кадр CTS. Після прийому CTS *A* запускає таймер ACK і починає передачу даних. У разі коректного прийому *B* генерує кадр ACK, що повідомляє станції *A* про кінець передачі. Якщо інтервал часу таймера на станції *A* закінчується перш, ніж отриманий ACK, весь алгоритм роботи протоколу повторюється із самого початку.

Тепер розглянемо цей же процес з погляду станцій *C* і *D*. *C* знаходиться в зоні дії *A*, тому вона також приймає кадр RTS і розуміє, що скоро по каналу передаватимуться якісь дані і краще при цьому помовчати і почекати закінчення активності сусідніх станцій. Виходячи з інформації, що міститься в RTS, станція *C* може припустити, скільки часу займе передача послідовності, включаючи кінцевий ACK. Протягом цього проміжку *C* вважає, що її віртуальний канал зайнятий і вона може відпочивати. Індикацією такого стану є послідовність

NAV (Network Allocation Vector – вектор виділеної мережі), показана на мал. 4.24. Станція *D* не чує RTS, посланий *A*, зате чує CTS, посланий станцією *B*, і також виставляє NAV. Зверніть увагу: сигнали NAV не передаються, а є лише внутрішніми нагадуваннями станцій про те, що потрібно берегти мовчання протягом певного проміжку часу.

В протилежність кабельним каналам, безпроводові галасливі і ненадійні, якоюсь мірою через СВЧ-печі, що працюють в тому ж діапазоні. В результаті вірогідність коректної передачі кадру зменшується пропорційно збільшенню довжини кадру. Якщо вірогідність помилки в одному біті рівна p , то вірогідність того, що n -бітний кадр буде прийнятий коректно, рівна $(1 - p)^n$. Наприклад, для $p=10^{-4}$ вірогідність коректної передачі повного Ethernet-кадру завдовжки 12 144 біт складає менше 30 %. Якщо $p = 10^{-5}$, приблизно один кадр з 9 буде зіпсований. Навіть при $p= 10^{-6}$ більше 1 % кадрів буде зіпсовано, тобто за 1 секунду помилки в кадрах виникатимуть приблизно 12 разів. Довгі кадри взагалі мають дуже мало шансів дійти до одержувача непошкодженими, і їх потрібно посилати наново.

Для вирішення проблеми зашумлених каналів БМ застосовується розбиття кадрів на невеликі відрізки, кожний з яких містить власну контрольну суму. Фрагменти нумеруються і підтверджуються індивідуально з використанням протоколу з очікуванням (тобто відправник не може передати фрагмент з номером $d_0 + 1$, поки не отримає підтвердження про доставку фрагмента з номером d_0). Захопивши канал за допомогою діалогу, що складається з RTS і CTS, відправник може передати декілька кадрів підряд, як показано на мал. 4.25. Послідовність фрагментів називається **пачкою фрагментів**.



Мал. 4.25 Пачка фрагментів

Фрагментація підвищує продуктивність шляхом примусової повторної пересилки коротких відрізків кадрів, в яких відбулася помилка, а не кадрів цілком. Розмір фрагмента не закріплюється стандартом, а є параметром кожної комірки безпроводової мережі, що настраюється, і може оптимізуватися базовою станцією. Механізм виставлення NAV утримує станції від передачі тільки до приходу першого підтвердження про доставку. Але є і інший механізм (він описаний далі), що дозволяє одержувачу прийняти всю пачку фрагментів без інтерференції з сигналами сторонніх станцій.

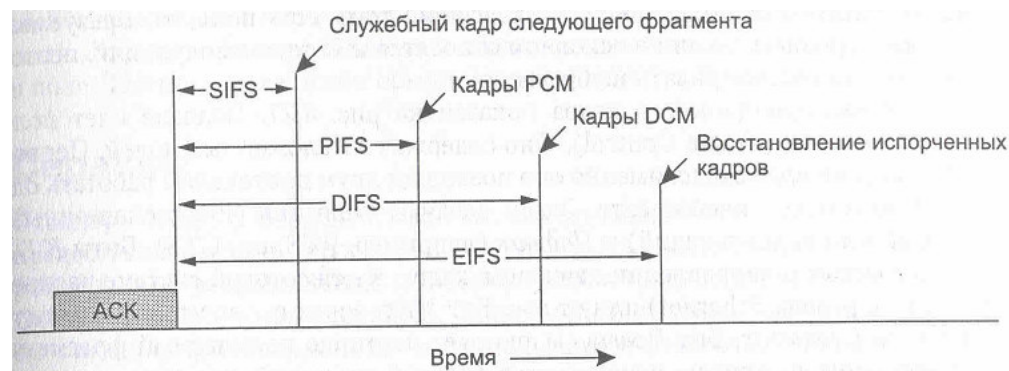
Отже, все описане раніше відноситься до режиму DCF (режим розподіленої координації) стандарту 802.11. В даному режимі відсутній централізований контроль, і станції самостійно борються за ефірний час приблизно так само, як в Ethernet. Але БМ можуть працювати і в іншому режимі, який називається PCF (режим зосередженої координації). Тут базова станція опитує всі підлеглі їй станції, виявляючи ті з них, які вимагають надати їм канал. Порядок «виступів» повністю і централізований координується базовою станцією, тому колізії

в режимі PCF виключені. Стандарт лише наказує здійснювати таку координацію, але не дає конкретні вказівки, що стосуються частоти, порядок опитування або наявність або відсутність яких-небудь пріоритетів у окремих станціях.

Механізм заснований на тому, що базова станція широкомовним способом періодично (10-100 разів в секунду) передає **сигнальний кадр**. В ньому містяться такі системні параметри, як послідовності зміни частот і періоди перебування на частотах (для FHSS), дані для синхронізації і т.д. Він також є запрошенням для нових станцій, які бажають увійти до списку опитуваних станцій. Потрапивши в цей список, станція одержує гарантовану частку пропускнуої спроможності (при певних параметрах швидкості), тобто їй гарантується якість обслуговування.

Акумулятори мають властивість розряджатися, тому в БМ економія електроенергії – це дуже животрепетне питання. Зокрема, базова станція може наказати станції йти спати (тобто перейти в режим зниженого споживання) до тих пір, поки її не розбудять (базова станція або користувач). Проте навіть в такому «сонному режимі» станція повинна мати нагоду зберігати в буфері кадри, що приходять, для подальшої їх обробки.

Режими PCF і DCF можуть співіснувати навіть усередині одного стільника мережі. Спочатку це може показатися нереальним: як це так – зосереджений і розподілений контроль одночасно? Проте стандарт 802.11 дійсно пропонує таку можливість. Це робиться шляхом дуже акуратного визначення міжкадрового інтервалу. Після відправки кадру необхідний якийсь час простою, перш ніж яка-небудь станція отримає дозвіл послати кадр. Всього визначено чотири інтервали, кожний з яких має власне призначення. Вони зображені на мал. 4.26.



Мал. 4.26. міжкадрові інтервали в стандарті 802.11

Найкоротший інтервал – це **SIFS** (Short InterFrame Interval – короткий міжкадровий інтервал). Він використовується для того, щоб одна із сторін, що ведуть діалог за допомогою управляючих кадрів, могла отримати шанс почати першою. Тут може бути CTS, посланий приймачем у відповідь на запит RTS; ACK, посланий їм же після закінчення прийому фрагмента або цілого кадру; чергова частина пакету фрагментів, послана відправником (тобто він не посилає RTS після кожного фрагмента).

Після інтервалу SIFS відповіді може завжди тільки одна станція. Якщо вона упускає свій шанс і час **PIFS** (PCF InterFrame Spacing – міжкадровий інтервал PCF) закінчується, то базова станція може послати сигнальний кадр або кадр опиту. Цей механізм дозволяє станції, що посилає кадр даних або послідовність фрагментів, закінчити свою передачу без якого-небудь втручання з боку сусідів, але дає і базовій станції можливість після закінчення передачі станцією захопити канал, не борючись за нього з іншими охочими.

Якщо базовій станції нічого сказати і інтервал **DIFS** (DCF InterFrame Spacing – міжкадровий інтервал DCF) закінчується, то будь-яка станція може спробувати захопити канал. Застосовуються при цьому звичайні правила боротьби, включаючи Двійковий експоненціальний відкіт у разі колізії.

Останній часовий інтервал називається **EIFS** (Extended InterFrame Spacing – розширений міжкадровий інтервал). Він використовується тільки тією станцією, яка тільки що отримала зіпсований або непізнаний кадр і хоче повідомити про цей факт. Чому найнижчий пріоритет відданий саме цій події? Річ у тому, що приймач може відразу не зміркувати, що відбувається, і йому потрібно почекати протягом якогось інтервалу, щоб не перервати своїм обуреним вигуком що йде в цей час діалог між станціями.

13.2.4 Структура кадру

Стандарт 802.11 визначає три класи кадрів, передавані по каналу: інформаційні, службові і керівники. Всі вони мають заголовки з безліччю полів, що використовуються підрівнем MAC. Крім того, є поля, що використовуються фізичним рівнем.

Формат інформаційного кадру показаний на мал. 4.27. Спочатку йде поле *Управління кадром* (Frame Control). Воно містить 11 вкладених полів. Перше з них – *Версія протоколу*, саме воно дозволяє двом протоколам працювати одночасно в одному осередку мережі. Потім слідує поля *Тип* (інформаційний, службовий або керівник) і *Підтип* (наприклад, RTS або CTS). Бити *До DS і Від DS* говорять про напрям руху *кадру*: до міжстільникової системи розподілу (наприклад, Ethernet) або від неї. Біт MF говорить про те, що далі слідує ще один фрагмент. Битий Повтор маркірує повторно посиляний фрагмент. *Бит* Управління живленням використовується базовою станцією для перемикання станції в режим зниженого споживання або виходу з

цього режиму. Біт Продовження говорить про те, що взагалі-то у *відправника* є ще кадри для пересилки. Біт W є індикатором використання шифрування в тілі кадру по алгоритму WEP (Wired Equivalent Protocol – протокол **забезпечення** конфіденційності). Нарешті, Про говорить приймачу **про те**, що кадри з цим бітом повинні оброблятися строго по порядку.



Мал. 4.27. Інформаційний кадр стандарту 802.11

Друге основне поле інформаційного кадру – це поле *Тривалість*. В ньому задається час, який буде витрачений на передачу кадру і підтвердження. Це поле можна знайти і в службових кадрах, і саме відповідно до нього станції виставляють ознаки NAV. Заголовок кадру містить також чотири адреси у форматі, відповідному стандарту IEEE 802. Зрозуміло, що потрібні адреси відправника і одержувача, але що ж міститься в двох тих, що залишилися? Річ у тому, що кадри можуть входити в осередок або покидати її через базову станцію. Дві адреси якраз і беруть адреси початкового і цільового осередків при передачі трафіку між осередками.

Поле *Номер* дозволяє нумерувати фрагменти. З 16 доступних біт 12 ідентифікують кадр, а 4 – фрагмент. Поле *Дані* містить передавану по каналу інформацію, його довжина може досягати 2312 байт. В кінці, як завжди, розташовано поле *Контрольна сума*.

Управляючі кадри мають формат, схожий з форматом інформаційних кадрів, за одним виключенням: в управляючому кадрі відсутні поля базових станцій, оскільки таким кадрам немає чого виходити за межі стільника. Службові кадри набагато коротше: в них міститься один або дві адреси, відсутні поля *Дані* і *Номер*. Ключовою тут є інформація, що міститься в полі *Підтип*. Значеннями звичайно є RTS, CTS або ACK.

13.2.5 Сервіси

Стандарт 802.11 затверджує, що все сумісні безпроводові ЛОМ повинні надавати дев'ять типів сервісів (послуг). Їх можна розділити на дві категорії: сервіси розподілу (до них відносяться п'ять з дев'яти) і станційні (відповідно, чотири сервіси). Сервіси розподілу пов'язані з управлінням станціями, що знаходяться в даному стільнику, і взаємодією із зовнішніми станціями. Станційні сервіси, навпаки, мають відношення до управління активністю усередині одного стільника.

П'ять сервісів розподілу надаються базовою станцією і мають справу з мобільністю станцій при їх вході в стільник або виході з неї. При цьому станції встановлюють або розривають взаємодію з базовою станцією. Нижче перераховані сервіси розподілу.

1. Асоціація. Цей сервіс використовується мобільними станціями для підключення до базових станцій (БС). Звичайно він застосовується зразу ж після входження в зону дії БС. Мобільна станція передає ідентифікаційну інформацію і повідомляє про свої можливості (підтримуваної швидкості передачі даних,

необхідності RCF-послуг, або опиту) і вимоги по управлінню електроживленням. Базова станція може прийняти або відкинути мобільну станцію. Якщо остання прийнята, вона повинна пройти ідентифікацію.

2. Дизасоціація. За ініціативою мобільної або базової станції може бути проведена дизасоціація, тобто розрив відносин. Це потрібне при виключенні станції або її відході із зони дії БС. Втім, базова станція також може бути ініціатором дизасоціації, якщо, наприклад, вона тимчасово вимикається для проведення технічного обслуговування.

3. Реасоціація. За допомогою цього сервісу станція може змінити БС. Очевидно, дана послуга використовується при переміщенні станції з одного стільника в інший. Якщо вона проходить коректно і без збоїв, то при переході ніякі дані не втрачаються. (Проте, як і в мережі Ethernet, в стандарті 802.11 всі послуги надаються лише із зобов'язанням додатку максимальних зусиль до їх виконання, але не з гарантією.)

4. Розподіл. За допомогою цієї послуги визначається маршрутизація кадрів, посланих базовій станції. Якщо адреса призначення є локальною з погляду БС, то кадри слідує просто напряму (передаються в ефірі). В осоружному випадку їх необхідно пересилати по дротяній мережі.

5. Інтеграція. Якщо кадру потрібно пройти через мережу, що не підкоряється стандарту 802.11 і використовуючу іншу схему адресації и/или формат кадру, то на допомогу приходить даний сервіс. Він реалізує трансляцію форматів. Чотири, що залишилися, сервіси – це внутрішні послуги стільника. Вони надаються після проходження *асоціації*, описаної вище. Нижче перераховані станційні сервіси:

1. Ідентифікація. Оскільки безпроводові комунікації мають на увазі дуже легке підключення до мережі і можливість прийому/відправки даних будь-якими станціями, що потрапили в зону дії БС, то виникає необхідність ідентифікації. Тільки після ідентифікації станції дозволяється обмін даними. Після ухвалення

мобільної станції в ряди поточних абонентів стільника базова станція посилає спеціальний кадр запиту, що дозволяє зрозуміти, чи знає станція привласнений їй секретний ключ (пароль). Підтвердження здійснюється шляхом шифрування кадру запиту і відсилання його назад базовій станції. Якщо шифрування виконано коректно, мобільна *i* станція одержує нормальні права доступу до мережі. Спочатку стандарт не вимагає, щоб базова станція відправляла свої ідентифікаційні дані мобільної станції, але робота над виправленням цього упущення вже ведеться.

2. Деідентифікація. Якщо станція, що працювала в мережі, покидає її, вона повинна провести деідентифікацію. Після виконання даного сервісу вона більше не зможе використовувати осередок.

3. Конфіденційність. Щоб зберегти передавані по мережі дані в таємниці від сторонніх «вух», їх необхідно шифрувати. Даний сервіс здійснює операції по кодуванню і декодуванню інформації. Застосовується алгоритм RC4, винайдений Рональдом Рівестом (Ronald Rivest) з МЛТ.

4. Доставка даних. Власне кажучи, саме цей сервіс є ключовим у всій роботі мережі. Адже мережа 802.11 існує для обміну даними. Оскільки стандарт 802.11 заснований на стандарті Ethernet, а в останньому доставка даних не є гарантованою на 100%, то для БМ це тим більше вірно. Знаходити і виправляти помилки доручено верхнім рівням.

У клітинки 802.11 є деякі параметри, які перевіряються і іноді випадках настраюються. Вони відносяться до шифрування даних, інтервалів тайм-аутів, швидкостей передачі даних, частот сигналів і т.д.

Безпроводні мережі на основі стандарту 802.11 все ширше застосовуються в установах, аеропортах, готелях, ресторанах, а також на виробничих територіях і в університетських кампусах по всьому світу. Швидке розповсюдження цих мереж вже практично неминуче.

13.3. Широкополосні БМ

В багатьох країнах телефонна система в якийсь момент перестала бути жорстко керованою, і з'явилася безліч фірм, що пропонують локальні послуги голосового зв'язку і інтернет-послуги.

Пропозицій дійсно багато. Проблема тільки в тому, що прокладка волоконно-оптичного кабелю, коаксіала або навіть витой пари п'ятої категорії до мільйонів абонентів обходиться дуже дорого. Що ж робити?

Відповідь одночасно і проста, і складна. Потрібні широкополосні БМ. Встановити одну велику антену на горі де-небудь поряд з населеним пунктом і розставити на дахах будинків абонентів приймальні антени більш простіше і дешевше, ніж рити траншеї і протягувати кабель. Таким чином, конкуруючі оператори зв'язку виявилися у край зацікавлені в розвитку багатомегабітних безпроводових систем зв'язку, що реалізують послуги голосової комунікації, доступу до Інтернету, відео за замовленням і т.д. Як було продемонстровано на мал. 2.27, дуже непогано із задачею справляється система LMDS. Проте ще до недавніх пір кожний оператор прагнув використовувати свою власну систему. Відсутність стандартів означала, що апаратне і програмне забезпечення не могли бути запущені в масове виробництво. Це, у свою чергу, приводило до установки невиправдано високих цін при низькій популярності.

Нарешті світлі голови, що працюють в даній галузі, зрозуміли, що саме стандартизація широкополосних БМ є головним каменем спотикання. За традицією, сформувати комітет для розробки стандарту було доручено IEEE. До комітету **802.16** увійшли представники найбільших фірм і наукових організацій. Робота була почата в липні 1999 року, а офіційний результат був представлений в квітні 2002 року. Назва стандарту така: «фірний

інтерфейс стаціонарних широкосмугових безпроводових систем доступу». Проте, більшість вважає за краще використовувати більш коротку назву: **безпроводові регіональні мережі**, або **безпроводові місцеві лінії**. Ми вважаємо, що всі ці назви рівноцінні і взаємозамінні.

Подібно деяким іншим стандартам з серії 802, стандарт 802.16 побудований з використанням ідей моделі OSI. Тут можна знайти і рівні, і підрівні, використовується схожа термінологія, сервісні примітиви і т.п. На жаль, як і OSI, стандарт 802.16 страждає громіздкістю.

13.3.1 Порівняння стандартів 802.11 і 802.16

Здавалося б, навіщо проголошувати новий стандарт? Ніж такі погані мережі 802.11, що їх не можна вже і на вулицю винести? Пояснень появи нового стандарту можна знайти дещо. По-перше, 802.11 і 802.16 вирішують абсолютно різні проблеми. Перш ніж говорити про які-небудь технічні подробиці, варто, папевно, сказати декілька слів в захист творців саме нового стандарту.

Мережі 802.11 і 802.16 схожі один на одного перш за все в тому, що і ті, і інші призначені для забезпечення безпроводового зв'язку з високою пропускнуою спроможністю. Проте далі починаються відмінності. По-перше, 802.16 надає послуги зв'язку для цілих будівель, а будівлі, як відомо, відрізняються у край малюю мобільністю. Вони не часто мігрують із стільника в стільник. Тим часом мережі 802.11 багато в чому орієнтовані на мобільність абонентів. В будівлі може бути розташовано декілька комп'ютерів, і цей варіант дещо складніше, ніж мобільна станція з єдиним ноутбуком. Власники будівель звичайно готові платити за хороший зв'язок більше, ніж власники ноутбуків, тому з'являється можливість установки якісних

радіоприймачів і передавачів. Зокрема, цей аспект впливає на те, що мережа 802.16 може використовувати повнодуплексний зв'язок, тоді як економія грошей користувачами мережі 802.11 не дає такої можливості.

Мережі 802.16 можуть охоплювати цілі райони міст, і відстані при цьому обчислюються кілометрами. Отже, одержуваний станціями сигнал може бути різній потужності залежно від їх віддаленості від передавача. Ці відхилення впливають на співвідношення сигнал/шум, що, у свою чергу, приводить до використання декількох схем модуляції. Цей вид телекомунікацій є відкритим, ефірний сигнал проходить над цілими містами, тому питання захисту інформації тут украй важливі.

В кожній комірці широкосмугової регіональної мережі може бути набагато більше користувачів, ніж в звичайному осередку 802.11, і при цьому кожному користувачу надається набагато більш висока пропускна спроможність, ніж користувачу безпроводової ЛОМ. Крім всього іншого, важко уявити собі, щоб начальство фірми зібрало в одній кімнаті офісної будівлі 50 співробітників, для того, щоб подивитися, що буде з мережею, якщо на кожному з 50 мобільних станцій завантажувати свій відеофільм. В середовищі користувачів 802.16 така ситуація може легко виникнути сама собою, тільки не в межах однієї кімнати, а в межах одного осередку регіональної мережі. неліцензуючої (ISM) смуги частот явно недостатньо для такого навантаження, тому мережі 802.16 працюють у високочастотному діапазоні 10-66 ГГц. На момент розробки стандарту це була єдина відповідна незайнята частина спектру.

Але ж міліметрові хвилі такого діапазону володіють зовсім іншими фізичними властивостями, ніж більш довгі хвилі ISM-діапазону. Значить, необхідно розробити спеціальний фізичний рівень для 802.16. Міліметрові хвилі, на жаль, дуже ефективно поглинаються водою (особливо дощем, снігом, градом, а іноді навіть туманом). Значить, потрібно якось це враховувати при обробці помилок. Даний тип хвиль є вузьконаправленим (хвилі,

вживані в стандарті 802.11, розповсюджуються по всіх напрямках), тому питання про багатопроменеве розповсюдження тут стає більше теоретичним, ніж практичним.

Ще одна проблема – якість обслуговування. Мережі 802.11 підтримують передачу інформації в реальному часі, але взагалі-то вони не призначені для телефонного зв'язку і великого мультимедійного трафіку. Стандарт 802.16, навпаки, орієнтований на підтримку подібних додатків, оскільки він призначений як для обивателів, так і для ділових людей.

Двома словами можна так змалювати відмінність між описуваними мережами: стандарт 802.11 – це мобільний аналог Ethernet, а 802.16 – безпроводовий, але стаціонарний аналог кабельного телебачення. Різниця виявилася такою великою, що стандарти вийшли зовсім не схожі. Це і зрозуміло: вони служать різним цілям.

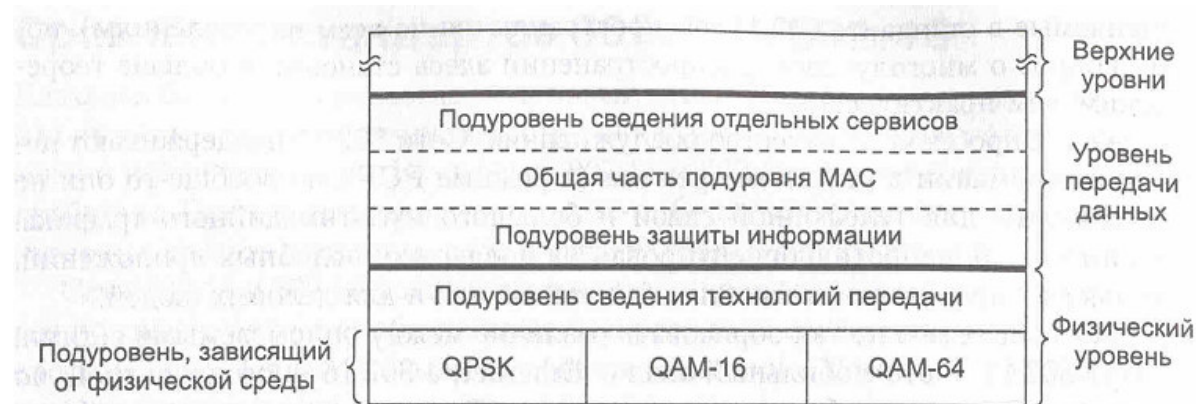
Можна спробувати провести якусь аналогію із стільниковою телефонною системою. Кажучи про мобільні телефони, ми маємо на увазі голосовий зв'язок, здійснюваний в досить вузькому частотному діапазоні, з невисокою потужністю і хвилями середньої довжини. Ніхто (поки що) не дивиться на екранах мобільних телефонів двогодинні фільми з високим дозволом. Навіть UMTS, схоже, не змінить ситуацію. Коротше кажучи, запити у користувачів безпроводових регіональних мереж набагато вище, ніж у власників мобільних апаратів. Отже, потрібна зовсім інша система. Питання про можливе використання стандарту 802.16 для мобільних додатків залишається відкритим. Він не має на увазі цього, але така можливість, у принципі, є. На сьогоднішній день ведеться безпроводове обслуговування виключно стаціонарних абонентів.

13.3.2 Стек протоколів

Набір протоколів, що використовується стандартом 802.16, показаний на мал. 4.28. Загальна структура подібна іншим стандартам серії 802, проте тут ми бачимо більше підрівнів. Нижній підрівень займається фізичною передачею даних. Використовується звичайна вузькополосна радіосистема із звичайними схемами модуляції сигналу. Над фізичним рівнем знаходиться підрівень зведення (з наголосом на другий склад), що приховує від рівня передачі даних відмінності технологій. Насправді, в стандарті 802.11 можна знайти щось подібне, просто комітет не потрудився дати цьому назву в стилі моделі OSI.

Хоча ми і не показали цього на малюнку, вже розробляються два нові протоколи фізичного рівня. Стандарт 802.16a підтримуватиме OFDM в діапазоні 2-11 ГГц. 802.16b зможе працювати в 5-гігагерцевому ISM-діапазоні. Обидві варіації на тему 802.16 є спробами наблизитися до 802.11.

Рівень передачі даних складається з трьох підрівнів. Нижній з них відноситься до захисту інформації, що дуже критично для мереж, в яких передача Даних здійснюється в ефірі, фізично ніяк не захищеному від прослуховування. В мережах 802.11 у прямому розумінні слова «стіни допомагають» приховати інформацію від несанкціонованого доступу. На цьому підрівні проводиться шифрація, декодування даних, а також управління ключами доступу.



Мал. 4.28. Стек протоколів 802.16

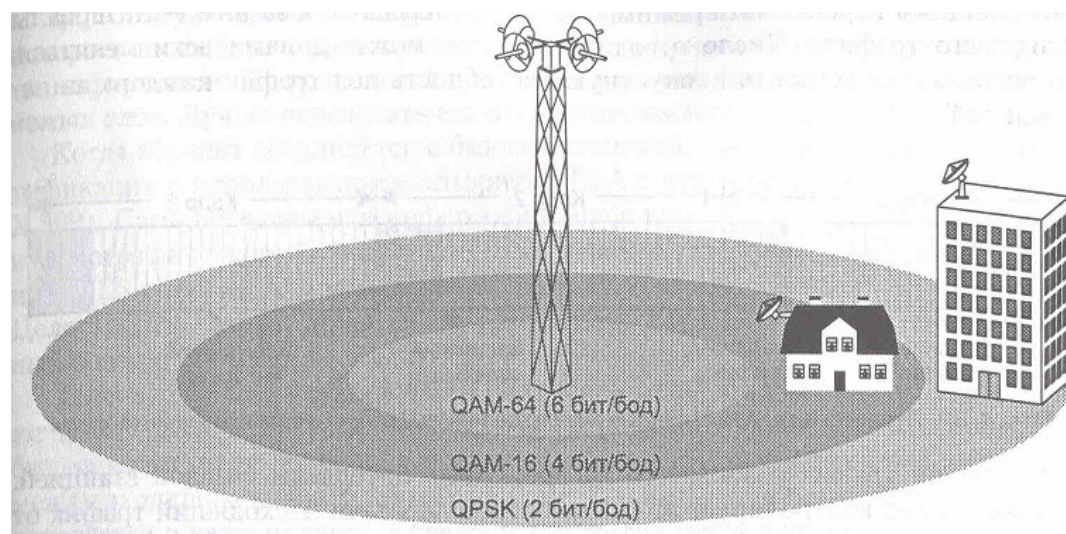
Потім слідує загальна частина підрівня MAC. Саме на цьому рівні ієрархії розташовуються основні протоколи – зокрема, протоколи управління каналом. Ідея полягає в тому, що базова станція контролюють всю систему. Вона дуже ефективно розподіляє черговість передачі вхідного трафіку абонентам, чималу роль грає і в управлінні витікаючим трафіком (від абонента до базової станції). Від всієї решти стандартів 802.x MAC-підрівень стандарту 802.16 відрізняється тим, що він повністю орієнтований на установку з'єднання. Таким чином можна гарантувати певну якість обслуговування при наданні послуг телефонного зв'язку і при передачі мультимедіа.

Підрівень зведення окремих сервісів грає роль підрівня логічного зв'язку в інших протоколах 802.x. Його функція полягає в організації інтерфейсу для мережного рівня. Складність тут полягає в тому, що стандарт 802.16, по ідеї розробників, повинен бути повністю сумісним як з дейтаграмними протоколами (наприклад, PPP, IP і Ethernet), так і з АТМ. Виникає проблема: пакетні протоколи – це протоколи без встановлення з'єднання, а

АТМ орієнтований на встановлення з'єднання. Це означає, що будь-яке з'єднання з використанням АТМ повинне відображатися на з'єднання 802.16. Це здійснюється без проблем. Але куди накажете відображати ІР-пакет, що прийшов? Рішенням цієї проблеми займається підрівень зведення сервісів.

13.3.3 Фізичний рівень

Як було сказано раніше, широкосмуговим БМ необхідний широкий частотний спектр, який можна знайти тільки в діапазоні від 10 до 66 ГГц. Міліметрові хвилі володіють однією цікавою властивістю, яка відсутня у більш довгих мікрохвиль: вони розповсюджуються не на всіх напрямках (як звук), а по прямих лініях (як світло). Отже, на базовій станції повинна бути встановлений безліч антен, що покривають різні сектори навколишньої території, як показано на мал. 4.29. В кожному секторі будуть свої користувачі. Сектори не залежать один від одного, чого не скажеш про стільниковий радіозв'язок, в якому сигнали розповсюджуються відразу по всіх напрямках.



Мал. 4.29. Оперативне середовище передачі даних мереж 802.16

Оскільки потужність сигналу передаваних міліметрових хвиль сильно зменшується із збільшенням відстані від передавача (тобто базової станції), то і співвідношення сигнал/шум також знижується. З цієї причини 802.16 використовує три різні схеми модуляції залежно від видалення абонентної станції. Якщо абонент розташований недалеко від БС, то застосовується QAM-64 з шістьма бітами на відлік. На середньому видаленні використовується QAM-16 і 4 би-та/бод. Нарешті, якщо абонент розташований далеко, то працює схема QPSK з двома бітами на відлік. Наприклад, при типовій смузі спектру 25 МГц QAM-64 дають швидкість 150 Мбіт/с, QAM-16 - 100 Мбіт/с, а QPSK - 50 Мбіт/с. Іншими словами, чим далі знаходиться абонент від базової станції, тим нижче швидкість передачі даних (те ж саме ми спостерігали в ADSL, див. мал. 2.23). Фазові діаграми всіх трьох методів були показані на мал. 2.21.

Перед розробниками мереж 802.16 стояла важка задача: необхідно було створити широкопasmову систему з урахуванням приведених раніше фізичних обмежень. Для цього було слід продумати найефективніший спосіб використання доступного спектру. Схеми роботи стандартів GSM і DAMPS були знехтувані відразу: і там, і там для вхідного і витікаючого трафіку використовуються хоча і різні, але еквівалентні по ширині смуги частот. Для голосового зв'язку це дійсно логічно, але при роботі в Інтернеті надання широкої смуги для витікаючого трафіку є недозвеною розкішшю. Стандарт 802.16 забезпечує гнучкість розподілу смуги пропускання. Застосовуються дві схеми модуляції: **FDD** (Frequency Division Duplexing – дуплексний зв'язок з частотним розділенням) і **TDD** (Time Division Duplexing – дуплексний зв'язок з тимчасовим розділенням). Останній метод показаний на мал. 4.30. Що тут відбувається? Базова станція періодично передає кадри, розділені на тимчасові інтервали. Перша частина тимчасових інтервалів відводиться під вхідний трафік. Потім слідує захисний інтервал (роздільник), що дозволяє станціям перемикаєти режими прийому і передачі, а за ним – інтервали витікаючого трафіку. Число тактів, що відводяться, може динамічно мінятися, що дозволяє підстроїти пропускну спроможність під трафік кожного з напрямів.



Мал. 4.30. Дуплексний зв'язок з тимчасовим розділенням: кадри і тимчасові інтервали

Вхідний трафік розбивається на тимчасові інтервали базовою станцією. Вона повністю контролює цей напрям передачі. Витікаючий трафік від абонентів управляється складнішим чином і залежить від необхідної якості обслуговування. Ми ще повернемося до розподілу тимчасових інтервалів, коли обговорюватимемо підрівень MAC.

Ще однією цікавою властивістю фізичного рівня є його здатність упаковувати декілька сусідніх кадрів MAC в одну фізичну передачу. Це дає можливість підвищити ефективність розподілу спектру шляхом зменшення числа різних преамбул і заголовків, таких улюблених фізичним рівнем.

Необхідно також відзначити, що для безпосереднього виправлення помилок на фізичному рівні використовується код Хеммінга. Майже всі мережні технології просто покладаються на контрольні суми і знаходять помилки з їх допомогою, запрошуючи повторну передачу зіпсованих фрагментів. Але при широкопasmовому безпроводового зв'язку на великих відстанях виникає стільки помилок, що їх обробкою доводиться займатися фізичному рівню, хоча на більш високих рівнях і застосовується метод контрольних сум. Основна задача корекції помилок на фізичному рівні полягає в тому, щоб примусити канал виглядати краще, ніж він є насправді (так само компакт-диски здаються такими надійними носіями тільки завдяки тому, що більше половини сумарного числа біт відводиться під виправлення помилок на фізичному рівні).

13.3.4 Протокол підрівня MAC

Отже, рівень передачі даних роздільний на три підрівні, як показано на мал. 2.28. Оскільки ми аж до восьмого розділу не торкатимемося принципів криптографії, то зараз немає значення пояснювати роботу підрівня захисту інформації. Достатньо сказати, що для заховання передаваних даних застосовується кодування,

причому кодуються тільки самі дані; а заголовки не кодуються. Це означає, що нехороший дядько може взнати, хто з ким розмовляє, але не може підслуховувати зміст розмови.

Коли абонент з'єднується з базовою станцією, виконується взаємна ідентифікація з використанням алгоритму RSA з відкритим ключем (сертифікат X.509). Сама передавана інформація шифрується за допомогою симетричного криптографічного ключа: або DES з ланцюжком цифрових блоків, або потрібний DES з двома ключами. Незабаром, можливо, буде доданий AES (Rijndael). Цілісність даних перевіряється алгоритмом SHA-1. Ну що, не дуже страшний абзац вийшов?

Тепер перейдемо до загальної частини підрівня MAC. Кадри MAC завжди займають ціле число тимчасових інтервалів фізичного рівня. Кожний кадр розбитий на частини, перші дві з яких містять карту розподілу інтервалів між вхідним і витікаючим трафіком. Там знаходиться інформація про те, що передається в кожному такті, а також про те, які такти вільні. Карта розподілу вхідного потоку містить також різноманітні системні параметри, які важливі для станцій, тільки що підключилися до ефіру.

Канал вхідного трафіку влаштований досить просто, оскільки є базова станція, яка визначає, що розмістити в кожній частині кадру. З витікаючим каналом всі декілька складніше, оскільки є конкуруючі між собою станції, охочі отримати доступ до нього. Його розподіл тісно пов'язаний з питанням якості обслуговування. Визначено чотири класи сервісів:

1. Сервіс з постійною бітовою швидкістю.
2. Сервіс реального часу із змінною бітовою швидкістю.
3. Сервіс, що працює не в реальному масштабі часу, із змінною бітовою швидкістю.
4. Сервіс із зобов'язанням додатку максимальних зусиль за поданням послуг.

Всі що надаються стандартом 802.16 сервіси орієнтовано на з'єднання, і кожне з'єднання дістає доступ до одного з приведених раніше класів сервісу. Це визначається при установці зв'язку. Таке рішення сильно відрізняється як від 802.11, так і від Ethernet, де були відсутні які-небудь натяки на встановлення з'єднання на підрівні MAC.

Сервіс з постійною бітовою швидкістю призначений для передачі нестислої мови, такий, яка передається по каналу T1. Тут вимагається передавати приречений об'єм даних в приречені тимчасові інтервали. Це реалізується шляхом призначення кожному з'єднанню такого типу своїх інтервалів. Після того, як канал виявляється розподіленим, доступ до тимчасових інтервалів здійснюється автоматично, і немає необхідності запрошувати кожний з них по окремоті.

Сервіс реального масштабу часу із змінною бітовою швидкістю застосовується при передачі стислих мультимедійних даних і інших програмних застосувань реального часу. Необхідна в кожний момент часу пропускна спроможність може мінятися. Та або інша смуга виділяється базовою станцією, яка опитує через певні проміжки часу абонента з метою виявлення необхідної на даний момент ширини каналу.

Сервіс, що працює не в реальному масштабі часу, із змінною бітовою швидкістю призначений для інтенсивного трафіку – наприклад, для передачі файлів великого об'єму. Тут базова станція теж опитує абонентів досить часто, але не в строго встановлені моменти часу. Абонент, що працює з постійною бітовою швидкістю, може встановити в одиницю один із спеціальних бітів свого кадру, тим самим пропонуючи базовій станції опитати його (це означає, що у абонента з'явилися дані, які потрібно передати з новою бітовою швидкістю).

Якщо станція не відповідає на k-опитувань підряд, базова станція включає її в широкомовну групу і припиняє персональні опити. Тепер якщо станції буде потрібно передати дані, то під час широкомовного опиту вона повинна відповісти базовій станції, запрошуючи тим самим сервіс. Таким чином, станції з малим трафіком не віднімають у базової станції цінний час на персональні опити.

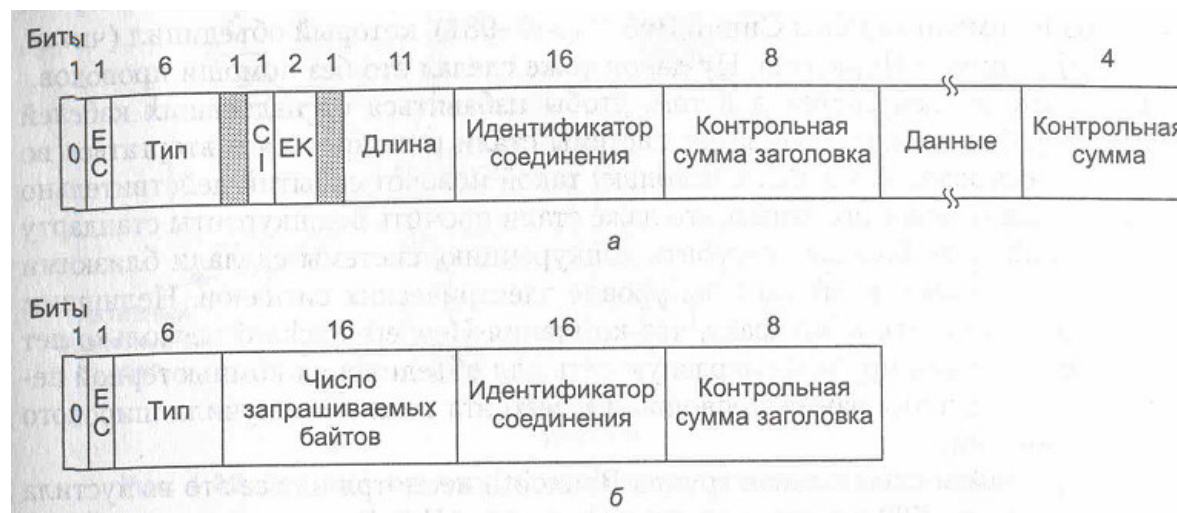
Нарешті, сервіс із зобов'язанням додатку максимальних зусиль використовується для всієї решти типів передачі. Ніяких опитів тут немає, а станції, охочі захопити канал, повинні змагатися з іншими станціями, яким потрібен той же клас сервісу. Запит пропускної спроможності здійснюється в тимчасових інтервалах, помічених в карті розподілу витікаючого потоку як доступні для конкуренції. Якщо запит пройшов вдало, це буде відзначено в наступній карті розподілу вхідного потоку. В осоружному випадку абоненти-невдахи повинні продовжувати боротьбу. Для мінімізації числа колізій використовується узятий з Ethernet алгоритм двійкового експоненціального відкоту.

Стандартом визначено дві форми розподілу пропускної спроможності: для станції і для з'єднання. В першому випадку абонентна станція збирає разом всі вимоги своїх абонентів (наприклад, комп'ютерів, що належать мешканцям будівлі) і здійснює колективний запит. Отримавши смугу, вона розподіляє її між користувачами на свій розсуд. В останньому випадку базова станція працює з кожним з'єднанням окремо.

13.3.5 Структура кадру

Всі кадри підрівня управління доступом до середовища (MAC) починаються з одного і того ж заголовка. За ним слідує (або не слідує) поле даних, і кінчається кадр також необов'язковим полем контрольної суми (CRC). Це показано на мал. 4.31. Поле даних відсутнє в службових кадрах, які призначені, наприклад, для

запиту тимчасових інтервалів. Контрольна сума (як не дивно) теж є необов'язковою завдяки тому, що виправлення помилок проводиться на фізичному рівні і ніколи не буває спроб повторно переслати кадри інформації, що передається в реальному масштабі часу. Так якщо все одно немає повторних передач, навіщо ж турбувати апаратуру обчисленням і перевіркою контрольних сум?



Мал. 4.31. Звичайний кадр (а); кадр запиту каналу (б)

Давайте стисло розглянемо поля заголовка (мал. 4.31, а). Біт ЄС говорить про те, чи шифрується поле даних. Поле Тип указує тип кадру (зокрема, повідомляє про те, чи пакується кадр і чи є фрагментація). Поле СІ указує на наявність або відсутність поля фінальної контрольної суми. Поле ЕНК повідомляє, який з ключів шифрування використовується (якщо він взагалі використовується). В полі Довжина міститься інформація про повну довжину кадру, включаючи заголовок. Ідентифікатор з'єднання повідомляє, якому із з'єднань належить

кадр. В кінці заголовка є поле Контрольна сума заголовка, значення якого обчислюється за допомогою полінома $x^8 + x^2 + x + 1$.

На мал. 4.31, би показаний інший тип кадру. Це кадр запиту каналу. Він починається з одиничного, а не нульового біта і в цілому нагадує заголовок звичайного кадру, за винятком другого і третього байтів, які складають 16-бітовий номер, говорячий про необхідну смугу для передачі відповідного числа байтів. В кадрі запиту каналу відсутнє поле даних, немає і контрольної суми всього кадру.

13.4. Безпроводова технологія Bluetooth

В 1994 році компанія Л. М. Эриксона (L. M. Ericsson) зацікавилася питанням безпроводовим зв'язком між мобільними телефонами і іншими пристроями (наприклад, PDA). Спільно з чотирма іншими відомими компаніями (IBM, Intel, Nokia і Toshiba) була сформована спеціальна група (тобто консорціум), яка зайнялася розвитком стандарту безпроводового зв'язку обчислювальних пристроїв і пристроїв зв'язку, а також створенням аксесуарів, що використовують недорогі малопотужні радіопристрої невеликого радіусу дії. Проект був названий Bluetooth («синій зуб») на честь великого короля вікінгів на ім'я Гаральд Синій Зуб II (940-981), який об'єднав (читай, завоював) Данію і Норвегію. Ну так, він теж зробив це без допомоги дротів.

Спочатку ідея полягала в тому, щоб позбутися обридливих кабелів між пристроями, проте потім системи стали розширятися і вторгтися у володіння безпроводових ЛОМ. Оскільки такий поворот подій дійсно робить стандарт більш корисним, його навіть стали готувати в конкуренти стандарту 802.11. Щоб ще більше усугубляти конкуренцію, системи зробили близькими не тільки на рівні ідей, але і на рівні електричних

сигналів. незайвим також буде відзначити і той факт, що компанія Hewlett-Packard кілька років тому представила миру інфрачервону мережу для об'єднання комп'ютерної периферії без використання дротів. Проте ця ідея не отримала широкого розповсюдження.

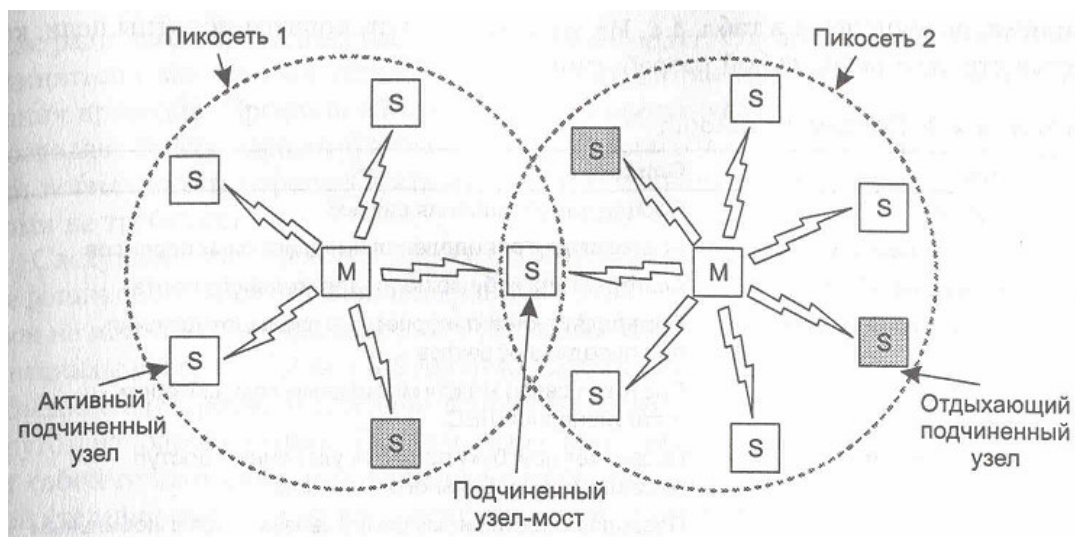
Безстрашна спеціальна група Bluetooth не дивлячись на все це випустила в липні 1999 року 1500-сторінкову специфікацію V1.0. Незабаром після цього група стандартизації IEEE узяла даний документ за основу стандарту 802.15 (персональні мережі) і почала шматувати його, підганяючи під свої потреби. Може спочатку показатися дивній ідея розробки стандарту того, що вже стандартизовано, причому дуже детально специфіковано, особливо якщо не видно ніяких несумісних систем, які треба було б суміщати. Проте досвід показує, що відкриті стандарти, створені такими нейтральними організаціями, як IEEE, часто сприяють популяризації і розвитку нових технологій. Необхідно зробити одне уточнення: специфікація Bluetooth охоплює цілу систему, від фізичного до прикладного рівня. Комітет IEEE 802.15 займається стандартизацією тільки фізичного рівня і рівня передачі даних; частина стека протоколів, що стосується інших рівнів, не входить в його компетенцію.

Не дивлячись на те, що в 2002 році IEEE затвердив перший стандарт персональних мереж, 802.15.1, спеціальна група Bluetooth як і раніше активно працює і займається поліпшеннями системи. Хоча на даний момент Bluetooth і стандарт IEEE не зовсім ідентичні, очікується, що скоро відбудеться їх об'єднання.

13.4.1 Архітектура Bluetooth

Почнемо вивчення системи Bluetooth з короткого огляду того, з чого вона полягає і для чого призначена. Основу Bluetooth складає **пікомережа** (piconet), що складається з одного головного вузла і декількох (до семи)

підлеглих вузлів, розташованих в радіусі 10 м. В одній і тій же кімнаті, якщо вона достатньо велика, можуть розташовуватися декілька пікомереж. Більш того, вони можуть навіть зв'язуватися один з одним за допомогою моста (спеціального вузла), як показано на мал. 4.32. Декількох з'єднаних разом пікомереж складають **розсіяну мережу (scatternet)**.



Мал. 4.32. Дві пікомережі можуть, з'єднавшись, сформувати розсіяну мережу

Крім семи активних підлеглих вузлів, один головний вузол може підтримувати до 255 так званих відпочиваючих вузлів. Це пристрої, які головний вузол перевів в режим зниженого енергоспоживання – за рахунок цього продовжується ресурс їх джерел живлення. В такому режимі вузол може тільки відповідати на запити активації або на сигнальні послідовності від головного вузла. Існують ще два проміжні режими енергоспоживання – припинений і аналізуючий, але ми їх зараз розглядати не будемо.

Таке рішення з головним і підлеглим вузлами виявилось дуже простим і дешевим в реалізації (вся мікросхема Bluetooth стоїть менш \$5). Оскільки цього і добивалися розробники, такий варіант і був прийнятий. Результатом цього є те, що підлеглі вузли вийшли дуже неговіркими – вони лише виконують те, що їм накаже головний вузол. В основі пікомереж лежить принцип централізованої системи з тимчасовим ущільненням. Головний вузол контролює тимчасові інтервали і розподіляє черговість передачі даних кожним з підлеглих вузлів. Зв'язок існує тільки між підлеглим і головним вузлами. Прямого зв'язку між підлеглими вузлами немає.

13.4.2 Застосування Bluetooth

Більшість мережних протоколів просто надає канали зв'язку між комунікаційними одиницями і залишає прикладне використання цих каналів на розсуд розробників. Наприклад, в стандарті 802.11 ніщо не мовиться про те, що користувачі повинні використовувати свої ноутбуки для читання електронної пошти, роботи в Інтернеті і т.п. В протилежність цьому специфікація Bluetooth V1.1 називає 13 конкретних підтримуваних додатків і для кожного з них надає свій набір протоколів. На жаль, Це приводить до сильного ускладнення системи, тому багато деталей в нашому описі ми вимушено опустити. Тринадцять додатків, звані профілями, **перераховано** в табл. 4.4. З цієї таблиці стають зрозумілі цілі, які ставили перед собою розробники системи.

Таблиця 4.4. Профілі Bluetooth

Таблица 4.4. Профили Bluetooth

Название	Описание
Общий доступ	Процедуры управления связью
Определение сервиса	Протокол для определения предлагаемых сервисов
Последовательный порт	Альтернатива кабелю последовательного порта
Общий объектный обмен	Определяет клиент-серверные взаимоотношения при передаче объектов
Доступ к ЛВС	Протокол связи между мобильным компьютером и стационарной ЛВС
Удаленный доступ	Позволяет ноутбуку получать удаленный доступ посредством мобильного телефона
Факс	Позволяет мобильному факсу связываться с мобильным телефоном
Беспроводная телефония	Связывает трубку с локальной базовой станцией
Intercom	Цифровые переносные рации
Гарнитура	Обеспечивает связь устройств hands-free с телефонами
Передача объектов	Обеспечивает обмен простыми объектами
Передача файлов	Предоставляет легкий способ пересылки файлов
Синхронизация	Позволяет PDA синхронизироваться с другим компьютером

Профіль групового доступу насправді не є застосуванням. Це швидше та основа, на якій будуються реальні застосування. Його головна задача полягає в забезпеченні установки і підтримки захищеної від несанкціонованого доступу зв'язку (створенні каналу) між головним і підлеглим вузлами. Також досить загальним є профіль визначення сервісу, що використовується для визначення того, які сервіси можуть бути

надані іншими пристроями. Вся апаратура системи Bluetooth повинна підтримувати два описаних раніше профілю. Всі інші є необов'язковими.

Профіль послідовного порту – це транспортний протокол, який використовується більшістю інших профілів. Він емулює послідовний канал і особливо корисний при роботі з додатками, яким потрібен цей канал.

Профіль загального об'єктного обміну визначає клієнт-серверні зв'язки, що виникають при обміні даними. Клієнти ініціюють операції, але підлегла станція може виступати або в ролі клієнта, або в ролі серверу. Як і профіль послідовного порту, це одна з цегли, з якої будуються інші профілі.

Наступна група, що складається з трьох профілів, має відношення до мереж. Профіль доступу до ЛОМ дозволяє пристрою Bluetooth під'єднатися до стаціонарної обчислювальної мережі. Цей профіль є найсправжнішим конкурентом стандарту 802.11. Профіль видаленого доступу був, власне кажучи, тим, ради чого спочатку був задуманий весь проект. Він дозволяє ноутбуку з'єднуватися з мобільним телефоном, що має вбудований модем, без використання дротів. Профіль «Факс» схожий на попередній з тією різницею, що він дозволяє безпроводовим факс-машинам посилати і одержувати факси за допомогою мобільного телефону. Знову ж таки, ніякі дроти для зв'язку між пристроями не потрібні.

Наступні три профілі відносяться до телефонії. Профіль безпроводової телефонії забезпечує зв'язок телефонної трубки з базою. Зараз домашній телефон не може використовуватися як мобільне, навіть якщо він не має зовсім ніяких дротів, проте в майбутньому, мабуть, ці два пристрої буде з'єднано. Профіль Intercom дозволяє двом телефонам з'єднуватися один з одним на зразок рацій. Нарешті, останній профіль цієї групи є додатком, що дозволяє пристроям hands-free тримати зв'язок з базою (телефоном). Це зручно, наприклад, при управлінні автомобілем.

Три, що залишилися, профілі призначено для організації обміну об'єктами (даними) між беспроводними пристроями. Об'єкти можуть бути електронними візитними картками, зображеннями або файлами з даними. Зокрема, профіль синхронізації призначений для завантаження даних в PDA або ноутбук, коли власник цих пристроїв, наприклад, виходить з будинку. Після повернення дані можна витягнути.

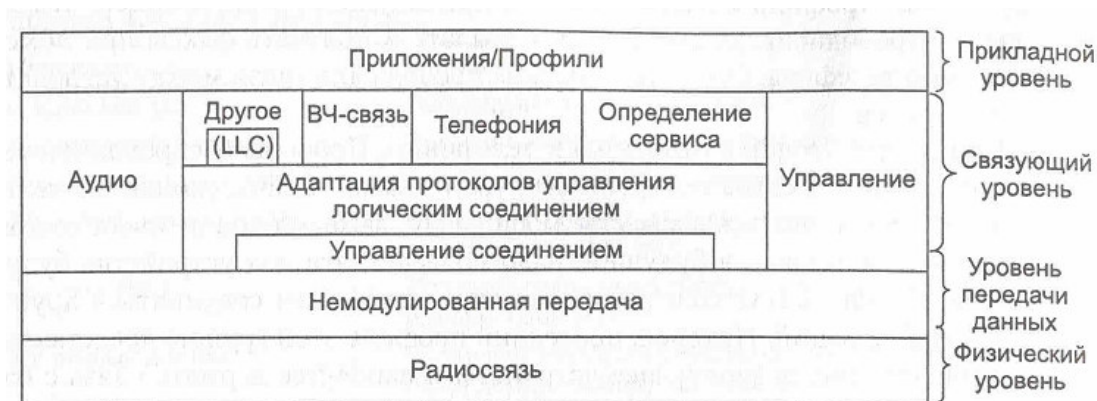
Невже дійсно необхідно було так детально описувати в стандарті всі додатки і надавати набори протоколів для кожного з них? Може бути, і ні, але було створено досить багато робочих груп, що займалися різними аспектами вживання системи. Кожна робоча група розробила свій профіль. Вважайте це демонстрацією закону Конвея у дії. (В квітні 1968 року в журналі *Datamation* була опублікована стаття Melvin Conway, в якій затверджувалося, що якщо доручити написання компілятора п програмістам, то вийде n-прохідний компілятор. В більш загальному вигляді ця думка звучить так: структура програмного забезпечення відображає структуру групи розробників.) Напевно, можна було обійтися не тринадцятьма, а двома наборами протоколів (один для передачі файлів і один для передачі даних в реальному масштабі часу).

13.4.3 Набір протоколів

Стандарт Bluetooth включає безліч протоколів, досить вільно розбитих на рівні. Структура стека протоколів не слідує ні моделі OSI, ні TCP/IP, ні 802, ні якій-небудь іншій відомій моделі. Проте IEEE працює над тим, щоб якось вписати Bluetooth в модель 802. Базова архітектура протоколів в модифікованому комітетом 802 вигляді представлена на мал. 4.33.

В самому низу знаходиться фізичний (радіотехнічний) рівень, який цілком відповідає представленням моделей OSI і 802 про те, яким повинен бути цей рівень. На ньому описуються радіозв'язок і вживані методи

модуляції. Багато що тут направлено на те, щоб зробити систему якомога дешевше і доступніше масовому покупцю.



Мал. 4.33. Архітектура протоколів Bluetooth: версія 802.15

Рівень немодульованої передачі чимось нагадує підрівень MAC, але включає і деякі елементи фізичного рівня. Тут описується те, як головний вузол управляє тимчасовими інтервалами і як ці інтервали групуються в кадри.

Далі слідує рівень, що містить групу зв'язаних між собою протоколів. Протокол управління з'єднанням встановлює логічні канали між пристроями, управляє режимами енергоспоживання, ідентифікацією, а також якістю послуг, що надаються. Підрівень адаптації протоколів управління логічними з'єднаннями (часто званий L2CAP) приховує від верхніх рівнів технічні деталі нижніх рівнів. Його можна вважати аналогом звичайного підрівня LLC з сімейства стандартів 802. Проте влаштований він по-іншому. аудіопротоколи і протоколи

управління, як впливає з їх назви, займаються відповідно передачею звуку і управлінням. Додатки можуть звертатися до них напряму, минувши протокол L2CAP.

Наступний рівень називається зв'язуючим, він містить безліч різноманітних протоколів. Для сумісності з мережами 802.x IEEE помістив сюди, наприклад, LLC. Втім, протоколи високочастотного (ВЧ) зв'язку, телефонії і визначення сервісів завжди належали Bluetooth. Протокол ВЧ-зв'язку емулює роботу стандартного послідовного порту ПК, до якого звичайно підключаються клавіатура, миша, модем і інші пристрої. Він дозволяє послідовникам цих традиційних пристроїв нетрадиційно обходитися без дротів. Протокол телефонії є протоколом, що працює в реальному масштабі часу. Він використовується трьома відповідними профілями, орієнтованими на передачу мови. В його задачі входять установка і розрив телефонного з'єднання. Нарешті, протокол визначення сервісів використовується для пошуку доступних в мережі сервісів.

На самому верхньому рівні знаходяться додатки і профілі. Вони працюють з протоколами нижніх рівнів, які забезпечують їх функціонування. Кожному додатку зіставлений свій набір протоколів. Специфічні пристрої типу гарнітур використовують тільки ті протоколи, які необхідні для їх роботи.

В наступних розділах ми розглянемо три нижні рівні стека протоколів Bluetooth, оскільки вони, хай грубо, але все-таки відповідають фізичному рівню і підрівню MAC.

13.4.4 Рівень радіозв'язку

Рівень радіозв'язку переносить інформацію біт за бітом від головного вузла до підлеглих і назад. В реальності це малопотужна прийомопередаюча система з радіусом дії порядку 10 м. Вона працює в неліцензійованому діапазоні 2,4 ГГц. Діапазон роздільний на 79 каналів по 1 МГц в кожному. Як метод

модуляції застосовується частотна маніпуляція з 1 бітом на герц, що дає сумарну швидкість 1 Мбіт/с. Проте велика частина спектру зайнята службовою інформацією. Для розподілу каналів застосовується розширений спектр із стрибкоподібною перебудовою частоти (1600 стрибків частоти в секунду, час перебування – 625 мкс). Всі вузли пікомереж перебудовують частоти одночасно; послідовність частот генерується головним вузлом.

Оскільки мережі 802.11 і Bluetooth працюють в одному і тому ж неліцензійованому діапазоні 2,4 ГГц на одних і тих же 79 каналах, то, природно, вони інтерферують один з одним. Проте Bluetooth розвивається набагато стрімкіше 802.11, і схоже, що саме Bluetooth ховатиме 802.11, а не навпаки. Але і 802.11, і 802.15 є стандартами IEEE, і звичайно, IEEE намагається знайти який-небудь вихід з цієї пікантної ситуації. Але це не така проста задача, як здається: річ у тому, що обидві системи використовують даний діапазон з тієї причини, що він не підлягає ліцензуванню. Стандарт 802.11a працює в іншому неліцензійованому діапазоні (5 ГГц), але він набагато вужче, завдяки фізичним властивостям радіохвиль. Отже 802.11a виявляється далеко не панацеєю від всіх випадків. Деякі компанії розв'язали проблему радикально: вони просто зрадили Bluetooth анафемі. Рішення цілком у дусі ринкових відносин: більш сильна (в політичному і економічному, а не технічному значенні) технологія вимагає від більш слабкої змінити свій стандарт так, щоб вона не заважала під ногами. Деякі думки із цього приводу можна також знайти у (Lansford і ін., 2001).

13.4.5 Рівень немодульованої передачі

Рівень немодульованої передачі – це найбільш близький до MAC-подуровню елемент ієрархії Bluetooth. Він трансформує простий потік біт в кадри і визначає деякі ключові формати. В найпростішому випадку головний вузол кожної пікомереж видає послідовності тимчасових інтервалів по 625 мкс, причому передача

даних з боку головного вузла починається в парних тактах, а із сторони підлеглих вузлів – в непарних. Це, по суті справи, традиційне тимчасове ущільнення, в якому головна сторона одержує одну половину тимчасових інтервалів, а підлеглі ділять між собою другу. Кадри можуть бути завдовжки 1, 3 або 5 тактів.

Той, що тактує із стрибкоподібною зміною частоти, відводить на заспокоєння системи 250-260 мкс при кожному стрибку. Час заспокоєння можна і зменшити, але ціна за це досить велика. В кадрі, що складається з одного такту, після заспокоєння системи залишається час на передачу 366 з 625 біт. З них 126 біт йде на код доступу і заголовки. Залишається 240 біт корисній інформації на кадр. Якщо сумістити п'ять тимчасових інтервалів в один кадр, знадобиться всього один період заспокоєння системи, тому з $5 \cdot 625 = 3125$ біт доступні 2781 біт на рівні немодульованої передачі. Виходить, що довгі кадри ефективно одноктактових.

Всі кадри передаються між головним і підлеглими вузлами по логічному каналу, званому з'єднанням. Існує два типи з'єднань. Перший називається **ACL** (Asynchronous Connectionless – асинхронний без встановлення зв'язку), він використовується для комутації пакетів даних, які можуть з'явитися в довільний момент часу. Такі дані з'являються з рівня L2CAP на передаючій стороні і доставляються на той же рівень на приймаючій стороні. Трафік ACL доставляється за принципом максимальних прикладених зусиль для забезпечення сервісу. Ніяких гарантій не дається. Кадри можуть втрачатися і пересилатися повторно. У підлеглому вузла може бути тільки одне ACL-з'єднання з своїм головним вузлом.

Другий вид з'єднання називається **SCO** (Synchronous Connection Oriented – синхронний зі встановленням зв'язку). Він призначений для передачі даних в реальному масштабі часу – це потрібне, наприклад, при телефонних розмовах. Такий тип каналу одержує фіксований часовий інтервал для передачі в кожному з напрямів. Через критичної до часу передачу природи SCO кадри, передані по даному типу каналу, ніколи не

пересилаються наново. Натомість може бути використаний пряма корекція помилок, що забезпечує більш надійне з'єднання. У підлеглого вузла може бути до трьох з'єднань типу SCO з головним вузлом, кожне з яких є аудіоканалом РСМ з пропускною спроможністю 64 000 бит/с.

13.4.6 Рівень L2CAP

Рівень L2CAP виконує три основні функції. По-перше, він приймає пакети розміром до 64 Кбайт з верхніх рівнів і розбиває їх на кадри для передачі по фізичному каналу. На протилежному кінці цей же рівень протоколів використовується для зворотної дії – об'єднання кадрів в пакети.

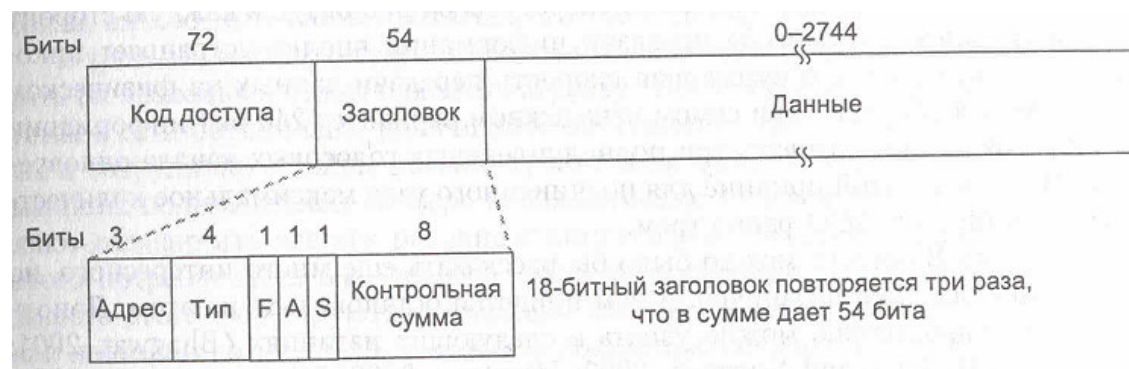
По-друге, L2CAP займається мультиплексуванням і демультіплексуванням безлічі джерел пакетів. Після збірки пакету він визначає, куди слід направити пакет (наприклад, на протоколу ВЧ-зв'язку або телефонії).

По-третє, L2CAP відповідає за якість обслуговування як під час передачі, так і під час очікування. Під час встановлення з'єднання він домовляється про максимально дозволена кількість передаваної корисної інформації, що дозволяє уникнути завалення даними пристрою, якому доводиться працювати з маленькими пакетами. Ця дія необхідна тому, не всі учасники мережі можуть працювати з 64-кілобайтними пакетами.

13.4.7 Структура кадру

Існує декілька форматів кадрів, найважливіший з яких показаний рис 4.34. На початку кадру вказується код доступу, який звичайно служить ідентифікатором головного вузла. Це дозволяє двом головним вузлам, які розташовані достатньо близько, щоб «чути» один одного, розрізняти, кому з них призначаються дані. Потім слідує 54-бітовий заголовок, в якому містяться поля, характерні для кадру підрівня MAC. Далі розташовано

поле даних, розмір якого обмежений 2744 бітами (для передачі з п'яти тактів). Якщо кадр має довжину, відповідну одному тактовому інтервалу, то формат залишається таким же, з тією різницею, що поле даних в цьому випадку складає 240 біт.



Мал. 4.34. Типовий інформаційний кадр Bluetooth

Розглянемо, з чого складається заголовок кадру. Поле *Адресу* ідентифікує один з восьми пристроїв, якому призначена інформація. Поле *Тип* визначає тип передаваного кадру (ACL, SCO, опит або порожній кадр), метод корекції помилок і кількість тимчасових інтервалів, з яких складається кадр. Біт *F* (Flow – потік) виставляється підлеглим вузлом і повідомляє про те, що його буфер заповнений. Це така примітивна форма управління потоком. Бітовий *A* (Acknowledgement – підтвердження) є підтвердженням (ACK), що відсилається у згоді з кадром. Біт *S* (Sequence – послідовність) використовується для нумерації кадрів, що дозволяє знаходити повторні передачі. Це протокол з очікуванням, тому 1 біта дійсно виявляється достаточ-Ю. Далі слідує 8-бітова контрольна сума заголовка. Весь 18-бітовий заголовок кадру повторюється тричі, що у результаті складає 54 біти, як показано на мал. 4.34. На приймаючій стороні нескладна схема аналізує всі три копії кожного біта. Якщо

вони співпадають, біт приймається таким, який він є. В іншому випадку все вирішує більшість. Як бачите, на передачу 10 біт тратиться в даному випадку 54 біти. Причина дуже проста: за все потрібно платити. За забезпечення передачі даних за допомогою дешевих малопотужних пристроїв (2,5 мВт) з невисокими обчислювальними здібностями доводиться платити великою надмірністю.

В кадрах ACL застосовуються різні формати поля даних. Найпростіший формат – в кадрах SCO: довжина поля даних завжди рівна 240 біт. Можливі три варіанти: 80, 160 або 240 біт корисної інформації. Біти поля даних, що при цьому залишилися, використовуються для виправлення помилок. Найнадійніша версія (80 біт корисної інформації) влаштована дуже просто: один і той же вміст повторюється три рази (що і складає 240 біт). Тобто метод тут застосовується той же, що і в заголовку кадру.

Оскільки підлеглі вузли можуть використовувати тільки непарні тимчасові інтервали, їм дістається 800 інтервалів в секунду. Стільки ж одержує і головний вузол. При 80 бітах корисних даних, що передаються в одному кадрі, місткість каналу підлеглого вузла рівна 64 000 бит/с. Цьому ж значенню рівна і місткість каналу головного вузла. Цього якраз вистачає для організації повнодуплексного РСМ-каналу голосового зв'язку (саме тому 1600 стрибків в секунду було вибрано як швидкість перебудови частот). Всі ці цифри говорять про те, що повнодуплексний канал із швидкістю 64 000 бит/с в кожную сторону при найнадійнішому способі передачі інформації цілком влаштовує пико-мережу, незважаючи на те, що сумарна швидкість передачі даних на фізичному рівні рівна 1 Мбіт/с. При самому ненадійному варіанті (240 біт інформації на кадр) можна організувати три повнодуплексні голосові канали одночасно. Саме з цієї причини для підлеглого вузла максимальну кількість з'єднань типу SCO рівно трьом.

Тема 14. Мережі Token Ring і 100VG-AnyLan

- 14.1. Загальні характеристики і топологічна структура.
- 14.2. Маркерний метод доступу.
- 14.3. Формати кадрів.
- 14.4. Фізичний рівень Token Ring.
- 14.5. Особливості мережі 100VG-Anylan

Л. [1, 3 6-8, 10, 12, 17,20]

14.1. Загальні характеристики і топологічна структура.

Загальна характеристика.

Локальна мережа Token Ring - це мережа кільцевої топології з ретрансляцією та маркерним методом доступу.

Технологія Token Ring була розроблена компанією ІВМ у 1984 році, а потім передана як проект стандарту в комітет ІЕЕЕ 802, який на її основі прийняв у 1985 році стандарт 802.5. Компанія ІВМ використовує технологію Token Ring у якості своєї основної мережної технології для побудови локальних мереж на основі комп'ютерів різних класів – мейнфреймів, міні-комп'ютерів і персональних комп'ютерів. В даний час саме

компанія IBM є основним законодавцем моди технології Token Ring, виробляючи близько 60% мережних адаптерів цієї технології.

Мережі Token Ring працюють із двома бітовими швидкостями – 4 і 16 Мбіт/с. Змішування станцій, що працюють на різних швидкостях, в одному кільці не допускається. Мережі Token Ring, що працюють зі швидкістю 16 Мбіт/с, мають деякі вдосконалення в алгоритмі доступу в порівнянні зі стандартом 4 Мбіт/с.

Влітку 1998 р. прийнято стандарт IEEE-802.5t мережі Token Ring зі швидкістю 100 Мбіт/с. Розробляють варіант і на 1000 Мбіт/с.

Порівняно з мережею Ethernet Token Ring посідає друге місце за використанням (наприклад, у 1993 р. у світі було випущено 8 млн. адаптерів Ethernet, 2 млн. Token Ring і 300 тис. Arcnet). Мережа Token Ring значно складніша, ніж Ethernet як технічно, так і алгоритмами та процедурами функціонування. Адаптери Token Ring у три-п'ять разів дорожчі, ніж адаптери Ethernet. Водночас Token Ring має і деякі переваги порівняно з Ethernet. Зокрема, вона ефективніше працює при великих навантаженнях (у цьому випадку Ethernet може використовувати до 30-40% від номінальної пропускної здатності, а Token Ring - 90%).

Мережі Token Ring, так само як і мережі Ethernet, характеризує поділюване середовище передачі даних, що у даному випадку складається з відрізків кабелю, що з'єднують усі станції мережі в кільце. Кільце розглядається як загальний поділюваний ресурс, і для доступу до нього потрібний не випадковий алгоритм, як у мережах Ethernet, а детермінований, заснований на передачі станціям права на використання кільця у визначеному порядку. Це право передається за допомогою кадру спеціального формату, який називається маркером чи токеном (token).

Технологія Token Ring є більш складною технологією ніж Ethernet. Вона володіє властивостями

відмовостійкості. У мережі Token Ring визначені процедури контролю роботи мережі, які використовують зворотний зв'язок кільцеподібної структури – посланий кадр завжди повертається в станцію-відправник. У деяких випадках виявлені помилки в роботі мережі усуваються автоматично, наприклад може бути відновлений загублений маркер. В інших випадках помилки тільки фіксуються, а їхнє усунення виконується вручну обслуговуючим персоналом.

Для контролю мережі одна зі станцій виконує роль так званого активного монітора. Активний монітор вибирається під час ініціалізації кільця як станція з максимальним значенням MAC-адреса. Якщо активний монітор виходить з ладу, процедура ініціалізації кільця повторюється і вибирається новий активний монітор. Щоб мережа могла знайти відмову активного монітора, останній у працездатному стані кожні 3 секунди генерує спеціальний кадр своєї присутності. Якщо цей кадр не з'являється в мережі більш 7 секунд, то інші станції мережі починають процедуру вибору нового активного монітора.

Топологічна структура

Топологічна структура Token Ring кільцева (див. рис. 8.1). Окремі станції приєднані через свої мережеві адаптери NIC (Network Interface Card). В адаптерній платі є кілька мікросхем, які виконують програмні функції керування передаванням даних у мережі. Комплект програм адаптерної плати називається агентом. Агент безпосередньо взаємодіє з протоколом сеансового рівня Netbios. Адаптерна плата приєднана до пристроїв багатостанційного доступу MAU (Multistation Access Unit) через спеціальний абонентський кабель (lobe cable). Пристрої MAU мають по кілька роз'єднувачів для приєднання станцій і по два для приєднання у кільце. Якщо роз'єднувачстанції порожній, то контакт у MAU замкнений і кільце замкнене. У випадку приєднання станції до

MAU роз'єднувач розмикається і станція “потрапляє” у кільце. MAU також сполучені між собою. Для передавання даних використовують чотирипроводову лінію (одне кільце резервне).

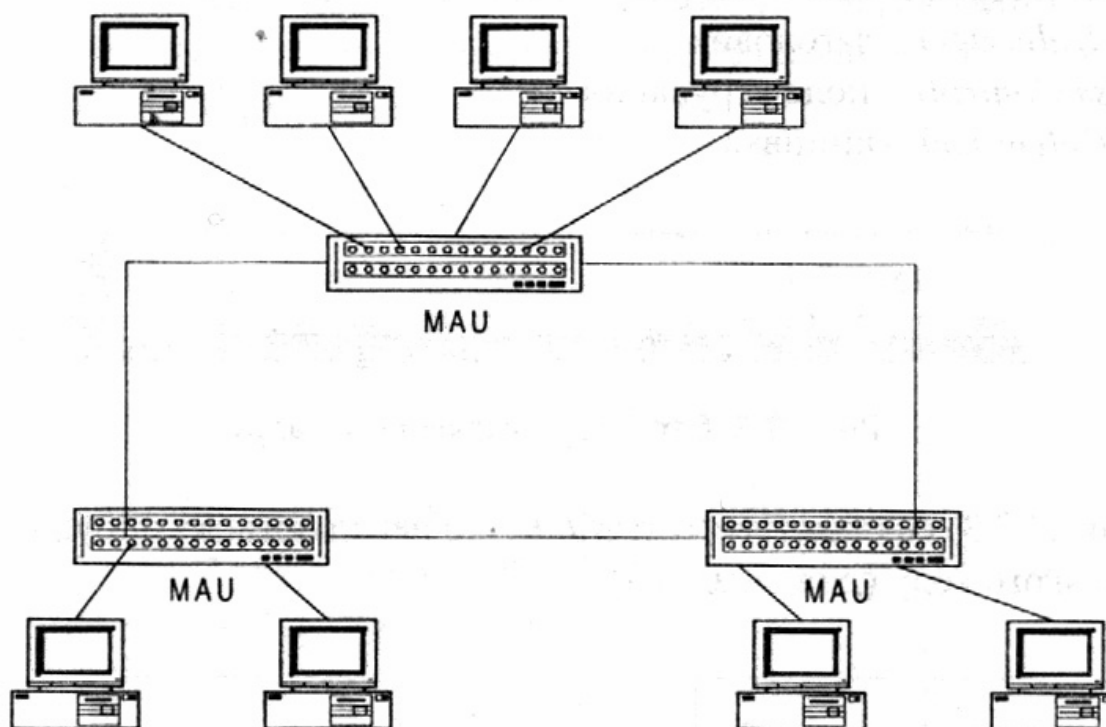


Рис. 8.1. Топологічна структура мережі

У мережі Token Ring реалізовано маркерний метод доступу для мереж з ретрансляцією. Маркер – трибайтовий кадр, що циркулює кільцем. Станція, яка одержала маркер, усуває його з мережі і передає свій інформаційний кадр, який робить повне коло мережею та повертається до станції, яка його передавала. Ця

станція усуває інформаційний кадр з мережі і передає маркер. Замість інформаційного LLC-кадру може передаватися службовий MAC-кадр.

14.2. Маркерний метод доступу.

(розглянуто на практичному занятті)

14.3. Формати кадрів.

В Token Ring існує три різних формати кадрів:

- маркер;
- кадр даних;
- послідовність, що перериває.

Маркер

Кадр маркера складається з трьох полів, кожне довжиною в один байт.

- **Початковий лімітатор** (Start Delimiter, SD) з'являється на початку маркера, а також на початку будь-якого кадру, що проходить по мережі. Поле являє собою наступну унікальну послідовність символів манчестерського коду: JK0JK000. Тому початковий лімітатор не можна сплутати ні з якою бітовою послідовністю всередині кадру.

- **Управління доступом** (Access Control) складається з чотирьох підполів: PPP, T, M і RRR, де PPP –

біти пріоритету, T – біт маркера, M – біт монітора, RRR – резервні біти пріоритету. Біт T, встановлений в 1, вказує на те, що даний кадр є маркером доступу. Біт монітора встановлюється в 1 активним монітором і в 0 будь-якою іншою станцією, що передає маркер чи кадр. Якщо активний монітор бачить маркер чи кадр, що містить біт монітора із значенням 1, то активний монітор знає, що цей кадр чи маркер вже один раз обійшов кільце і не був оброблений станціями. Якщо це кадр, то він видаляється з кільця. Якщо це маркер, то активний монітор передає його далі по кільцю. Використання полів пріоритетів буде розглянуто нижче.

- **Кінцевий лімітатор** (End Delimiter, ED) – останнє поле маркера. Так само як і поле початкового лімітатора, це поле містить унікальну послідовність манчестерських кодів JK1JK1, а також дві однобітові ознаки: I і E. Ознака I (Intermediate) показує, чи є кадр останнім у серії кадрів (I=0) чи проміжним (I=1). Ознака E (Error) – це ознака помилки. Вона встановлюється в 0 станцією-відправником, і будь-яка станція кільця, через яку проходить кадр, повинна встановити цю ознаку в 1, якщо вона знайде помилку по контрольній сумі чи іншу некоректність кадру.

Кадр даних і послідовність, що перериває

Кадр даних включає ті ж три поля, що і маркер, і має крім них ще кілька додаткових полів. Таким чином, кадр даних складається з наступних полів:

- *початковий лімітатор (Start Delimiter, SD);*
- *управління кадром (Frame Control, FC);*
- *адреса призначення (Destination Address, DA);*
- *дані (INFO);*

- *контрольна сума (Frame Check Sequence, FCS);*
- *кінцевий лімітатор (End Delimiter, ED);*
- *статус кадру (Frame Status, FS).*

Кадр даних може переносити або службові дані для управління кільцем (дані MAC-рівня), або дані користувачів (LLC-рівня). Стандарт Token Ring визначає 6 типів управлінських кадрів MAC-рівня. Поле FC визначає тип кадру (MAC чи LLC), і якщо він визначений як MAC, те поле також вказує, який із шести типів кадрів представлений даним кадром. Призначення цих шести типів кадрів описано нижче.

- Щоб впевнитися, що його адреса унікальна, станція, коли вперше приєднується до кільця, посилає кадр *Тест дублювання адреси (Duplicate Address Test, DAT)*.
- Щоб повідомити іншим станціям, що він працездатний, активний монітор періодично посилає в кільце кадр *Існує активний монітор (Active Monitor Present, AMP)*.
- Кадр *Існує резервний монітор (Standby Monitor Present, SMP)* відправляється будь-якою станцією, що не є активним монітором.
- Резервний монітор відправляє кадр *Маркер заявки (Claim Token, CT)*, коли підозрює, що активний монітор відмовив, потім резервні монітори домовляються між собою, який з них стане новим активним монітором.
- Станція відправляє кадр *Сигнал (Beacon, BCN)* у випадку виникнення серйозних мережних проблем, таких як обрив кабелю, виявлення станції, що передає кадри без чекання маркера, вихід станції з ладу. Визначаючи, яка станція відправляє кадр сигналу, діагностуюча програма (її існування і функції не визначаються стандартами Token Ring) може локалізувати проблему. Кожна станція періодично передає кадри

BCN доти, поки не прийме кадр BCN від свого попереднього (NAUN) сусіда. У результаті цього, в кільці тільки одна станція продовжує передавати кадри BCN – та, у якій є проблеми з попереднім сусідом. У мережі Token Ring кожна станція знає MAC-адрес свого попереднього сусіда, тому Beacon-процедура приводить до виявлення адреси некоректно працюючої станції.

- Кадр *Очищення (Purge, PRG)* використовується новим активним монітором для того, щоб перевести всі станції у вихідний стан і очистити кільце від усіх раніше посланих кадрів.

В стандарті 802.5 використовуються адреси тієї ж структури, що й у стандарті 802.3. Адреси призначення і джерела можуть мати довжину або 2, або 6 байт. Перший біт адреси призначення визначає групова чи індивідуальна адреса як для 2-байтових, так і для 6-байтових адрес. Другий біт у 6-байтових адресах говорить про те, чи призначена адреса є локальною чи глобальною. Адреса, що складається з всіх одиниць, є широкомовною.

Адреса джерела має той же розмір і формат, що й адреса призначення. Однак ознака групової адреси використовується в ньому особливим способом. Оскільки адреса джерела не може бути груповою, то наявність одиниці в цьому розряді говорить про те, що в кадрі є спеціальне *поле маршрутної інформації (Routing Information Field, RIF)*. Ця інформація потрібна при роботі мостів, що зв'язують кілька кілець Token Ring, у режимі маршрутизації від джерела.

Поле даних INFO кадру може містити дані одного з описаних керуючих кадрів рівня MAC чи користувальницькі дані, упаковані в кадр рівня LLC. Це поле, як уже відзначалося, не має визначеної стандартом максимальної довжини, хоча існують практичні обмеження на його розмір, засновані на тимчасових співвідношеннях між часом утримання маркера і часом передачі кадру.

Поле статусу FS має довжину 1 байт і містить 4 резервних біти і 2 підполя: біт розпізнавання адреси A і біт копіювання кадру C. Оскільки це поле не супроводжується сумою, що обчислюється CRC, то біти, що використовуються для надійності дублюються: поле статусу FS має вигляд ACxxACxx. Якщо біт розпізнавання адреси не встановлений під час одержання кадру, це означає, що станція призначення більше не є присутньою у мережі (можливо, внаслідок неполадок, а можливо, станція знаходиться в іншому кільці, пов'язаному з даним за допомогою моста). Якщо обидва біти розпізнавання адреси і копіювання кадру встановлені і біт виявлення помилки також установлений, то вихідна станція знає, що помилка сталася після того, як цей кадр був коректно отриманий.

Послідовність, що переривається, складається з двох байтів, що містять початковий і кінцевий лімітатори. Послідовність, що переривається, може з'явитися в будь-якому місці потоку бітів і сигналізує про те, що поточна передача кадру чи маркера скасовується.

Пріоритетний доступ до кільця

Кожен кадр даних чи маркер має пріоритет, що встановлюється бітами пріоритету (значення від 0 до 7, причому 7 – найвищий пріоритет). Станція може скористатися маркером, тільки якщо в неї є кадри для передачі з пріоритетом рівним чи більшим, ніж пріоритет маркера. Мережний адаптер станції з кадрами, у якого пріоритет нижчий, ніж пріоритет маркера, не може захопити маркер, але може помістити найбільший пріоритет передачі своїх кадрів, що очікують, у резервні біти маркера, але тільки в тому випадку, якщо записаний у резервних бітах пріоритет нижче ніж його власний. У результаті цього, в резервних бітах пріоритету

встановлюється найвищий пріоритет станції, що намагається одержати доступ до кільця, але не може цього зробити через високий пріоритет маркера.

Станція, що зуміла захопити маркер, передає свої кадри з пріоритетом маркера, а потім передає маркер наступному сусіду. При цьому вона переписує значення резервного пріоритету в поле пріоритету маркера, а резервний пріоритет обнуляється. Тому при наступному проході маркера по кільцю його захопить станція, що має найвищий пріоритет.

При ініціалізації кільця основний і резервний пріоритет маркера встановлюються в 0.

Хоча механізм пріоритетів є в наявності у технології Token Ring, але він починає працювати тільки в тому випадку, коли додаток чи прикладний протокол вирішують його використовувати. Інакше всі станції будуть мати рівні права доступу до кільця, що в основному і відбувається на практиці, тому що велика частина прикладних програм цим механізмом не користується. Це пов'язано з тим, що пріоритети кадрів підтримуються не у всіх технологіях, наприклад у мережах Ethernet вони відсутні, тому прикладна програма буде поводитися по-різному, в залежності від технології нижнього рівня, що є небажаним. В сучасних мережах пріоритетність обробки кадрів звичайно забезпечується комутаторами чи маршрутизаторами, котрі підтримують їх незалежно від протоколів каналного рівня, що використовуються.

14.4. Фізичний рівень Token Ring.

Стандарт Token Ring фірми IBM спочатку передбачав побудову зв'язків в мережі за допомогою концентраторів, званих MAU (Multistation Access Unit) або MSAU (Multi-Station Access Unit), тобто пристроями багатостанційного доступу (рис.8.2). Мережа Token Ring може включати до 260 вузлів.

Концентратор Token Ring може бути активним або пасивним. Пасивний концентратор просто з'єднує порти внутрішніми зв'язками так, щоб станції, що підключаються до цих портів, утворили кільце. Ні посилення сигналів, ні їх ресинхронізацію пасивний MSAU не виконує. Такий пристрій можна вважати простим кросовим блоком за одним винятком MSAU забезпечує обхід якого-небудь порту, коли приєднаний до цього порту комп'ютер вимикають. Така функція необхідна для забезпечення зв'язності кільця незалежно від стану підключених комп'ютерів. Звичайно обхід порту виконується за рахунок релейних схем, які харчуються постійним струмом від мережевого адаптера, а при вимкненні мережевого адаптера нормально замкнені контакти реле з'єднують вхід порту з його виходом.

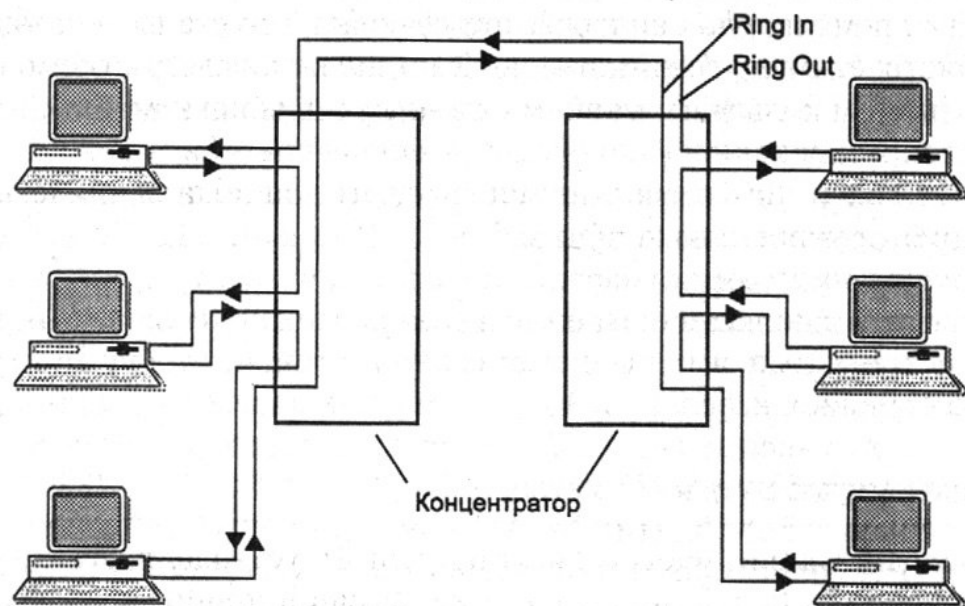


Рис. 8.2. Фізична структура мережі Token Ring

Активний концентратор виконує функції регенерації сигналів і тому іноді називається повторювачем, як в стандарті Ethernet.

Виникає питання якщо концентратор є пасивним пристроєм, то яким чином забезпечується якісна передача сигналів на великі відстані, які виникають при включенні в мережу декількох стільників комп'ютерів? Відповідь полягає в тому, що роль підсилювача сигналів в цьому випадку бере на себе кожний мережевий адаптер, а роль ресинхронізуючого блоку виконує мережевий адаптер активного монітора кільця. Кожний мережевий адаптер Token Ring має блок повторення, який уміє регенерувати і ресинхронізувати сигнали, однак останню функцію виконує в кільці тільки блок повторення активного монітора.

Блок ресинхронізації складається з 30-бітного буфера, який приймає манчестерські сигнали з декілька спотвореними за час обороту по кільцю інтервалами проходження. При максимальній кількості станцій в кільці (260) варіація затримки циркуляції біта по кільцю може досягати 3-бітових інтервалів. Активний монітор “вставляє” свій буфер в кільце і синхронізує бітові сигнали, видаючи їх на вихід з необхідною частотою.

У загальному випадку мережа Token Ring має комбіновану зоряно-кільцеву конфігурацію. Кінцеві вузли підключаються до MSAU по топології зірки, а самі MSAU об’єднуються через спеціальні порти Ring In (RI) і Ring Out (RO) для утворення магістрального фізичного кільця.

Всі станції в кільці повинні працювати на одній швидкості або 4 Мбіт/с, або 16 Мбіт/с. Кабелі, що з’єднують станцію з концентратором, називаються розгалужувальними (lobe cable), а кабелі, що з’єднують концентратори, магістральними (trunk cable).

Технологія Token Ring дозволяє використати для з’єднання кінцевих станцій і концентраторів різні типи кабелю: STP Type I, UTP Type 3, UTP Type 6, а також волоконно-оптичний кабель.

При використанні екранованої пари, що виється STP Type 1 з номенклатури кабельної системи IBM в кільце допускається об’єднувати до 260 станцій при довжині розгалужувальних кабелів до 100 метрів, а при використанні неекранованої пари, що виється максимальна кількість станцій скорочується до 72 при довжині розгалужувальних кабелів до 45 метрів.

Відстань між пасивними MSAU може досягати 100 м при використанні кабелю STP Type 1 і 45 м при використанні кабелю UTP Type 3. Між активними MSAU максимальна відстань збільшується відповідно до 730 м або 365 м в залежності від типу кабелю.

Максимальна довжина кільця Token Ring становить 4000 м. Обмеження на максимальну довжину кільця і кількість станцій в кільці в технології Token Ring не є такими жорсткими, як в технології Ethernet. Тут ці обмеження багато в чому пов'язані з часом обороту маркера по кільцю (але не тільки є і інші міркування, що диктують вибір обмежень). Так, якщо кільце складається з 260 станцій, то при часі утримання маркера в 10 мс маркер повернеться в активний монітор в гіршому випадку через 2,6 з, а цей час якраз складає тайм-аут контролю обороту маркера. У принципі, всі значення тайму-аутів в мережевих адаптерах вузлів мережі Token Ring можна налаштувати, тому можна побудувати мережу Token Ring з великою кількістю станцій і з більшою довжиною кільця.

Існує велика кількість апаратури для мереж Token Ring, яка поліпшує деякі стандартні характеристики цих мереж: максимальну довжину мережі, відстань між концентраторами, надійність (шляхом використання подвійних кілець).

Нещодавно компанія IBM запропонувала новий варіант технології Token Ring, названий High-Speed Token Ring, HSTR. Ця технологія підтримує бітові швидкості в 100 і 155 Мбіт/с, зберігаючи основні особливості технології Token Ring 16 Мбіт/с.

14.5. Особливості мережі 100VG-Anylan

Технологія 100VG-AnyLAN відрізняється від класичного Ethernet в значно більшій мірі, ніж Fast Ethernet, зокрема:

- Використовується інший метод доступу Demand Priority, який забезпечує більш справедливий розподіл

пропускної спроможності мережі в порівнянні з методом CSMA/CD. Крім того, цей метод підтримує пріоритетний доступ для синхронних прикладень

- Кадри передаються не всім станціям мережі, а тільки станції призначення.
- У мережі є виділений арбітр доступу – концентратор, і це помітно відрізняє дану технологію від інших, в яких застосовується розподілений між станціями мережі алгоритм доступу.
- Підтримуються кадри двох технологій – Ethernet і Token Ring (саме ця обставина додала словосполучення AnyLAN в назві технології).
- Дані передаються одночасно по 4 парах кабеля UTP категорії 3. По кожній парі дані передаються з швидкістю 25 Мбіт/с, що в сумі дає 100 Мбіт/с. На відміну від Fast Ethernet в мережах 100VG-AnyLAN немає колізій, тому вдалося використати для передачі всі чотири пари стандартного кабеля категорії 3. Для кодування даних застосовується код 5B/6B, який забезпечує спектр сигналу в діапазоні до 16 МГц (смуга пропускання UTP категорії 3) при швидкості передачі даних 25 Мбіт/с.

Метод доступу Demand Priority заснований на передачі концентратору функцій арбітра, який вирішує проблему доступу до середовища, що розділяється. Мережа 100VG-AnyLAN складається з центрального концентратора, званого також кореневим, і сполучених з ним кінцевих вузлів і інших концентраторів (рис. 7).

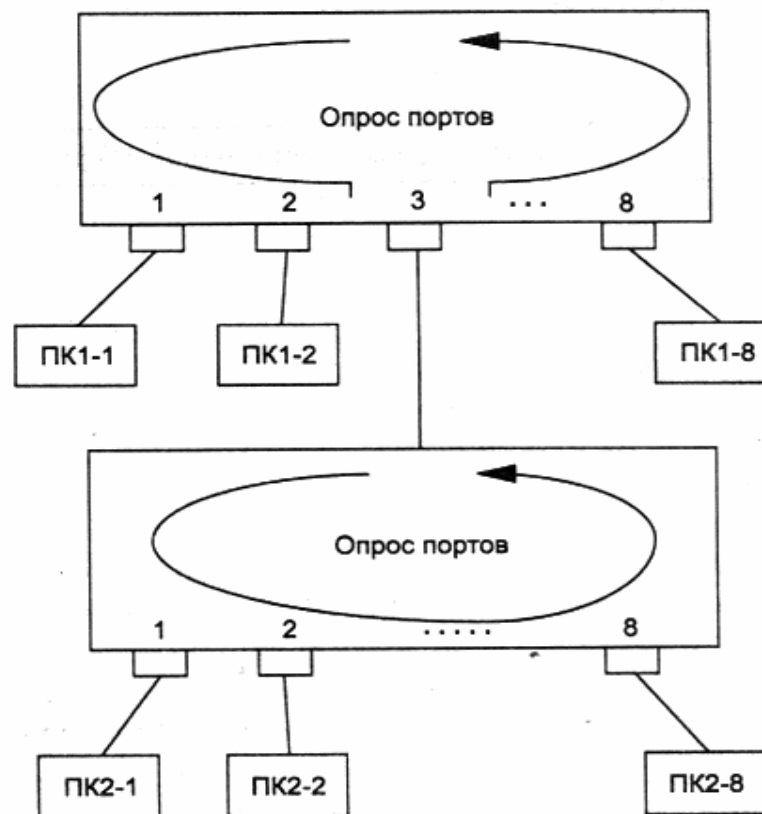


Рис.7 Мережа 100VG-AnyLAN

Допускаються три рівні каскадування. Кожний концентратор і мережевий адаптер 100VG-AnyLAN повинен бути налаштований або на роботу з кадрами Ethernet, або з кадрами Token Ring, причому одночасна циркуляція обох типів кадрів не допускається.

Концентратор циклічно виконує опитування портів. Станція, що бажає передати пакет, посилає

спеціальний низькочастотний сигнал концентратору, запитуючи дозволу на передачу кадру і вказуючи його пріоритет. У мережі IOOVG-AnyLAN використовуються два рівні пріоритетів – низький і високий. Низький рівень пріоритету відповідає звичайним даним (файлова служба, служба друку і т.п., а високий пріоритет відповідає даним, чутливим до тимчасових затримок (наприклад, мультимедіа). Пріоритети запитів мають статичну і динамічну складові, тобто станція з низьким рівнем пріоритету, що довго не має доступу до мережі, отримує високий пріоритет.

Якщо мережа є вільною, то концентратор дозволяє передачу пакету. Після аналізу адреси одержувача в прийнятому пакеті концентратор автоматично відправляє пакет станції призначення. Якщо мережа зайнята, концентратор ставить отриманий запит в чергу, яка обробляється відповідно до порядку надходження запитів і з урахуванням пріоритетів. Якщо до порту підключений інший концентратор, то опит припиняється до завершення опиту концентратором нижнього рівня. Станції, підключені до концентраторам різного рівня ієрархії, не мають переваг по доступу до середовища, що розділяється, оскільки рішення про надання доступу приймається після проведення опиту всіма концентраторами опиту всіх своїх портів.

Технологія IOOVG-AnyLAN підтримує декілька специфікацій фізичного рівня. Первинний варіант був розрахований на чотири неекрановані пари категорій, що виються 3,4,5. Пізніше з'явилися варіанти фізичного рівня, розраховані на дві неекрановані пари категорії, що виються 5, дві екрановані пари типу, що виються 1 або ж два оптичних багатомодових оптоволоконна.

Важливою особливістю технології IOOVG-AnyLAN є збереження форматів кадрів Ethernet і Token Ring. Прихильники IOOVG-AnyLAN затверджують, що цей підхід полегшить міжмережеву взаємодію через мости і маршрутизатори, а також забезпечить сумісність з існуючими коштами мережевого управління, зокрема з

аналізаторами протоколів.

Незважаючи на багато хороших технічних рішень, технологія IOOVG-AnyLAN не знайшла великої кількості прихильників і значно поступається за популярністю технологіями Fast Ethernet. Можливо, це сталося через те, що технічні можливості підтримки різних типів трафіка у технології ATM істотно ширше, ніж у IOOVG-AnyLAN. Тому при необхідності високоякісного обслуговування застосовують (або мають намір застосовувати) технологію ATM. А для мереж, в яких немає необхідності підтримувати високу якість обслуговування на рівні сегментів, що поділяються, більш звичною виявилася технологія Fast Ethernet. Відмітим що для підтримки дуже вимогливих до швидкості передачі даних додатків є технологія Gigabit Ethernet, яка, зберігаючи спадкоємність з Ethernet і Fast Ethernet, забезпечує швидкість передачі даних 1000 Мбіт/с.

Тема15. Мережа (технологія) FDDI

- 15.1. Основні характеристики технології
- 15.2. Особливості методу доступу
- 15.3. Фізичний рівень FDDI
- 15.4. Порівняння FDDI з Ethernet і TokenRing

[1, 3, 4, 7, 8, 10, 12, 15, 17, 20, 21]

15.1. Основні характеристики технології.

Технологія FDDI (Fiber Distributed Data Interface) – оптоволоконний інтерфейс розподілених даних – це перша технологія локальних мереж, в якій середою передачі даних є волоконно-оптичний кабель. Роботи по створенню технологій і пристроїв для використання волоконно-оптичних каналів в локальних мережах почалися в 80-і роки, незабаром після початку промислової експлуатації подібних каналів в територіальних мережах. Проблемна група X3T9.5 інституту ANSI розробила в період з 1986 по 1988 рр. початкові версії стандарту FDDI, який забезпечує передачу кадрів з швидкістю 100 Мбіт/з по подвійному волоконно-оптичному кільцю довжиною до 100 км.

Технологія FDDI багато в чому засновується на технології Token Ring, розвиваючи і вдосконалюючи її основні ідеї. Розробники технології FDDI ставили перед собою як найбільш пріоритетні наступні цілі:

- підвищити бітову швидкість передачі даних до 100 Мбіт/с;

- підвищити відмовостійкість мережі за рахунок стандартних процедур відновлення її після відмов різного роду – пошкодження кабеля, некоректної роботи вузла, концентратора, виникнення високого рівня перешкод на лінії і т.п.;
- максимально ефективно використати потенційну пропускну спроможність мережі як для асинхронного, так і для синхронного (чутливого до затримок) трафіків.

Мережа FDDI будується на основі двухоптоволоконних кілець, які утворюють основний і резервний шляхи передачі даних між вузлами мережі. Наявність двох кілець – це основний спосіб підвищення відмовостійкості в мережі FDDI, і вузли, які хочуть скористатися цим підвищеним потенціалом надійності, повинні бути підключені до обох кілець.

У нормальному режимі роботи мережі дані проходять через всі вузли і всі ділянки кабеля тільки первинного (Primary) кільця, цей режим названий режимом Thru – “крізним” або “транзитним”. Повторне кільце (Secondary) в цьому режимі не використовується.

У разі якого-небудь вигляду відмови, коли частина первинного кільця не може передавати дані (наприклад, обрив кабеля або відмова вузла), первинне кільце об’єднується з повторним (мал. 1), знову утворюючи єдине кільце. Цей режим роботи мережі називається Wrap, тобто “згортання” або “згортання” кільця. Операція згортання виробляється засобами концентраторів і/або мережевих адаптерів FDDI. Для спрощення цієї процедури дані по первинному кільцю завжди передаються в одному напрямі (на діаграмах цей напрям зображається проти годинникової стрілки), а по повторному – в зворотному (зображається за годинниковою стрілкою). Тому при утворенні загального кільця з двох кілець передавачі станцій як і раніше

залишаються підключеними до приймачів сусідніх станцій, що дозволяє правильно передавати і приймати інформацію сусідніми станціями.

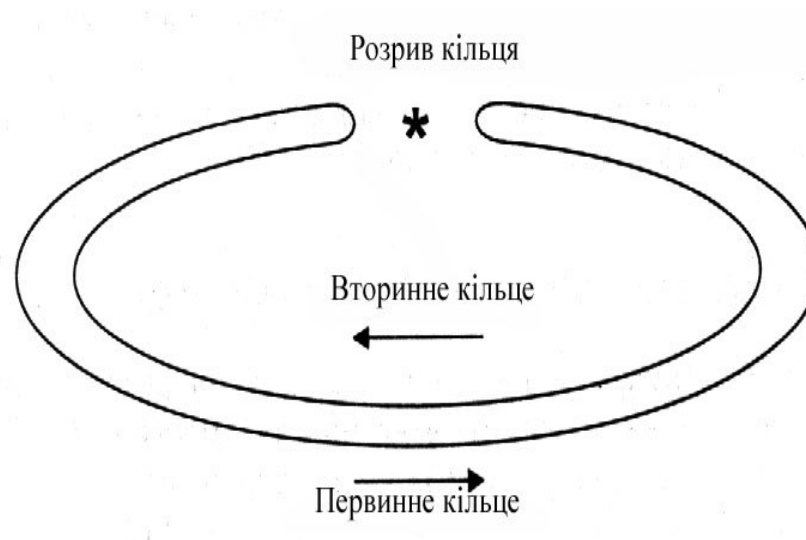


Рис.1 Реконфігурація кілець FDDI при відмові.

У стандартах FDDI багато уваги відводиться різним процедурам, які дозволяють визначити наявність відмови в мережі, а потім зробити необхідну реконфігурацію. Мережа TDDI може повністю відновлювати свою працездатність у разі одиничних відмов її елементів. При множинних відмовах мережа розпадається на декілька не пов'язаних мереж. Технологія FDDI доповнює механізми виявлення відмов технології Token Ring

механізмами реконфігурації шляху передачі даних в мережі, заснованими на наявності резервних зв'язків, що забезпечуються другим кільцем.

Кільця в мережах FDDI розглядаються як загальне середовище передачі даних, що розділяється, тому для неї визначений спеціальний метод доступу. Цей метод дуже близький до методу доступу мереж Token Ring і також називається методом маркерного (або токенного) кільця – token ring.

Відмінності методу доступу полягають в тому, що час утримання маркера в мережі FDDI не є постійною величиною, як в мережі Token Ring. Цей час залежить від завантаження кільця – при невеликому завантаженні воно збільшується, а при великих перевантаженнях може меншати до нуля. Ці зміни в методі доступу торкаються тільки асинхронного трафіка, який не критичний до невеликих затримок передачі кадрів. Для синхронного трафіка час утримання маркера як і раніше залишається фіксованою величиною. Механізм пріоритетів кадрів, аналогічний прийнятому в технології Token Ring, в технології FDDI відсутній. Розробники технології вирішили, що розподіл трафіка на 8 рівнів пріоритетів надмірно і досить розділити трафік на два класи – асинхронний і синхронний, останній з яких обслуговується завжди, навіть при перевантаженнях кільця.

У іншому пересилка кадрів між станціями кільця на рівні MAC повністю відповідає технології Token Ring. Станції FDDI застосовують алгоритм раннього звільнення маркера, як і мережі Token Ring з швидкістю 16 Мбіт/с.

Адреси рівня MAC мають стандартний для технологій IEEE 802 формат. Формат кадру FDDI близький до формату кадру Token Ring, основні відмінності полягають у відсутності полів пріоритетів. Ознаки розпізнавання адреси, копіювання кадру і помилки дозволяють зберегти процедури обробки кадрів, що є в мережах Token Ring станцією-відправником, проміжними станціями і станцією-одержувачем.

На мал. 2. приведена відповідність структури протоколів технології FDDI семирівневої моделі OSI. FDDI визначає протокол фізичного рівня і протокол підрівня доступу до середина (MAC) канального рівня. Як і у багатьох інших технологіях локальних мереж, в технології FDDI використовується протокол підрівня управління каналом даних LLC, визначений в стандарті IEEE 802.2. Таким чином, незважаючи на те що технологія FDDI була розроблена і стандартизована інститутом ANSI, а не комітетом IEEE, вона повністю вписується в структуру стандартів 802.



Рис.2 Структура протоколів технології FDDI

Відмінною особливістю технології FDDI є рівень управління станцією – Station Management (SMT). Саме рівень SMT виконує всі функції по управлінню і моніторингу всіх інших рівнів стека протоколів FDDI. У управлінні кільцем бере участь кожний вузол мережі FDDI. Тому всі вузли обмінюються спеціальними кадрами SMT для управління мережею.

Відмовостійкість мереж FDDI забезпечується протоколами і інших рівнів: за допомогою фізичного рівня усуваються відмови мережі по фізичних причинах, наприклад через обрив кабеля, а за допомогою рівня MAC – логічні відмови мережі, наприклад втрата потрібного внутрішнього шляху передачі маркера і кадрів даних між портами концентратора.

15.2. Особливості методу доступу

FDDI максимально відповідає Token Ring, однак вона має і відмінності, зумовлені потребою збільшити швидкість передавання.

У мережі FDDI використано схему кодування 4B5B, яка кодує 4-бітові комбінації даних у 5-бітові комбінації світлових імпульсів так, що для передавання даних з швидкістю 100 Мбіт/с реалізується швидкість передавання сигналів 125 Мбод.

На відміну від мережі Token Ring, у FDDI маркер передається відразу після передавання кадру станції, без очікування на повернення кадру кільцем. FDDI не використовує полів пріоритету та механізму резервування Token Ring. Натомість кожна станція класифікується, як асинхронна (що не ставити жорстких вимог до години доступу) і синхронна (яка ставити такі вимоги).

Структура маркера мережі FDDI показана на мал. 3.

Зміст полів SD, FC, ED, FS відповідає змісту однойменних полів для мережі Token Ring.

Преамбула	Початковий обмежувач	Контроль кадру	Кінцевий обмежувач	Статус кадру
8	1	1	1	
	SD	FC	ED	FS

Рис.3 Структура маркера FDDI

Для передачі синхронних кадрів станція завжди має право захопити маркер при його надходженні. При цьому час утримання маркера має зазделегідь задану фіксовану величину.

Якщо ж станції кільця FDDI треба передати асинхронний кадр (тип кадру визначається протоколами верхніх рівнів), то для з'ясування можливості захоплення маркера при його черговій появі станція повинна виміряти інтервал часу, який пройшов з моменту попереднього приходу маркера. Цей інтервал називається часом обороту маркера (Token Rotation Time, TRT). Інтервал TRT порівнюється з іншою величиною – максимально допустимим часом обороту маркера по кільцю T_{Org} . Якщо в технології Token Ring максимально допустимий час обороту маркера є фіксованою величиною (2,6 із з розрахунку 260 станцій в кільці), то в технології FDDI станції домовляються про величину T_{Org} під час ініціалізації кільця. Кожна станція може запропонувати своє значення T_{Org} , в результаті для кільця встановлюється мінімальне із запропонованих

станціями часів. Це дозволяє враховувати потреби додатків, працюючих на станціях. Звичайно синхронним додаткам (додаткам реального часу) треба частіше передавати дані в мережу невеликими порціями, а асинхронним додаткам краще отримувати доступ до мережі рідше, але великими порціями. Перевага віддається станціям, що передають синхронний трафік.

Таким чином, при черговому надходженні маркера для передачі асинхронного кадру порівнюється фактичний час обороту маркера TRT з максимально можливим T_Org . Якщо кільце не переобтяжене, то маркер приходить раніше, ніж закінчується інтервал T_Org , тобто $TRT < T_Org$. У цьому разі станція дозволяється захопити маркер і передати свій кадр (або кадри) в кільце. Час утримання маркера TRT рівно різниці $T_Org - TRT$, і протягом цього часу станція передає в кільце стільки асинхронних кадрів, скільки встигне.

Якщо ж кільце переобтяжене і маркер спізнився, то інтервал TRT буде більшим T_Org . У цьому випадку станція не має права захопити маркер для асинхронного кадру. Якщо всі станції в мережі хочуть передавати тільки асинхронні кадри, а маркер зробив оборот по кільцю дуже повільно, то всі станції пропускають маркер в режимі повторення, маркер швидко робить черговий оборот і на наступному циклі роботи станції вже мають право захопити маркер і передати свої кадри.

Метод доступу FDDI для асинхронного трафіка є адаптивним і добре регулює тимчасові перевантаження мережі.

15.3.Фізичний рівень FDDI.

У технології FDDI для передачі світлових сигналів по оптичних волокнах реалізоване логічне кодування 4В/5В в поєднанні з фізичним кодуванням NRZI. Ця схема приводить до передачі по лінії зв'язку сигналів з тактовою частотою 125 МГц.

Оскільки з 32 комбінацій 5-битних символів для кодування початкових 4-бітних символів потрібне тільки 16 комбінацій, то з 16, що залишилися вибрано декілька кодів, які використовуються як службові. До найбільш важливих службових символів відноситься символ Idle – простий, який постійно передається між портами протягом пауз між передачею кадрів даних. За рахунок цього станції і концентратори мережі FDDI мають постійну інформацію про стан фізичних з'єднань своїх портів. У разі відсутності потоку символів Idle фіксується відмова фізичного зв'язку і проводиться реконфігурація внутрішнього шляху концентратора або станції, якщо це можливе.

При первинному з'єднанні кабелем двох вузлів їх порти спочатку виконують процедуру встановлення фізичного з'єднання. У цій процедурі використовуються послідовності службових символів коду 4В/5В, за допомогою яких створюється деяка мова команд фізичного рівня. Ці команди дозволяють портам з'ясувати один у одного типи портів (А, В, М або S) і вирішити, чи коректно дане з'єднання (наприклад, з'єднання S-S є некоректним і ____). Якщо з'єднання коректне, то далі виконується тест якості каналу при передачі символів кодів 4В/5В, а потім перевіряється працездатність рівня MAC сполучених пристроїв шляхом передачі декількох кадрів MAC. Якщо всі тести пройшли успішно, то фізичне з'єднання вважається встановленим. Роботу по встановленню фізичного з'єднання контролює протокол управління станцією SMT.

Фізичний рівень розділений на два підрівня: незалежний від середовища підрівень PHY (Physical) і підрівень, що залежить від середовища PMD (Physical Media Dependent) (див. мал. 2).

Технологія FDDI на даний час підтримує два підрівня PMD: для волоконно-оптичного кабеля і для неекранованої витой пари категорії 5. Останній стандарт з'явився пізніше оптичного і носить назву TP-PMD.

Оптоволоконний підрівень PMD забезпечує необхідні кошти для передачі даних від однієї станції до іншої по оптичному волокну. Його специфікація визначає:

- використання як основного фізичного середовища багатомодового волоконно-оптичного кабеля 62,5/125 мкм;
- вимоги до потужності оптичних сигналів і максимальному загасанню між вузлами мережі. Для стандартного багатомодового кабеля ці вимоги приводять до граничної відстані між вузлами в 2 км, а для одномодового кабеля відстань збільшується до 10-40 км в залежності від якості кабеля;
- вимоги до оптичних обхідних перемикачів (optical bypass switches) і оптичного приймача-передавача;
- параметри оптичних роз'єм МІС (Media Interface Connector), їх маркіровку;
- використання для передачі світла з довжиною хвилі в 1300 нм;
- представлення сигналів в оптичних волокнах відповідно до методу NRZI.

Підрівень TP-PMD визначає можливість передачі даних між станціями по парі, що виється відповідно до методу фізичного кодування MLT-3, що використовує два рівні потенціалу: +V і -V для представлення даних в кабелі. Для отримання рівномірного по потужності спектра сигналу дані перед фізичним кодуванням проходять через скремблер. Максимальна відстань між вузлами у відповідності зі стандартом TP-PMD дорівнює 100 м.

Максимальна загальна довжина кільця FDDI становить 100 кілометрів, максимальне число станцій з подвійним підключенням в кільці – 500.

15.4. Порівняння FDDI з Ethernet і TokenRing.

У таблиці 1 представлені результати порівняння технології FDDI з технологіями Ethernet і Token Ring.

Таблиця 1 Характеристики технологій FDDI, Ethernet, Token Ring

Характеристика	FDDI	Ethernet	Token Ring
Бітова швидкість	100 Мбіт/с	10 Мбіт/с	16 Мбіт/с
Топологія	Подвійне кільце дерев	Шина/зірка	Зірка/кільце
Метод доступу	Частка від часу обороту маркера	CSMA/CD	Пріоритетна система резервування
Середовище передачі даних	«Оптоволокно, неекранована вита пара категорії 5	Товстий коаксіал, тонкий коаксіал, вита пара категорії 3, оптоволокно	Екранована і неекранована вита пара оптоволокно
Максимальна довжина мережі (без мостів)	200 км (100 км на кільце)	2500 м	4000м
Максимальна відстань між вузлами	2 км (не більше 11 дБ втрат між вузлами)	2500 м	100м
Максимальна кількість вузлів	500 (1000 з'єднань)	1024	260 для екранованої витої пари, 72 для неекранованої витої пари
Тактування і відновлення після відмов	Розподілена реалізація тактування і відновлення після відмов	Не визначені	Активний монітор

Тема 16. Об'єднання мереж протоколами мережевого рівня

16.1 Принципи об'єднання мереж протоколами мережного рівня.

16.2 Поняття internetworking.

16.3 Принципи маршрутизації.

16.4 Протоколи маршрутизації.

16.5 Функції маршрутизації.

16.6. Реалізація міжмережевої взаємодії засобами TCP/IP

16.7 Рівні між мережною взаємодією,

16.8 відповідність моделі ISO/OSI.

16.1. Принципи об'єднання мереж на основі протоколів мережевого рівня

У стандартній моделі взаємодії відкритих систем у функції мережевого рівня входить рішення наступних задач:

- передача пакетів між кінцевими вузлами в складових мережах;
- вибір маршруту передачі пакетів, якнайкращого по деякому критерію;
- узгодження різних протоколів канального рівня, що використовуються в окремих підмережах однієї складової мережі.

Протоколи мережевого рівня реалізуються, як правило, у вигляді програмних модулів і виконуються на кінцевих вузлах-комп'ютерах, званих хостами, а також на проміжних вузлах - маршрутизаторах, званих шлюзами. Функції маршрутизаторів можуть виконувати як спеціалізовані пристрої, так і універсальні комп'ютери з відповідним програмним забезпеченням.

Обмеження мостів і комутаторів

Створення складної, структурованої мережі, яка інтегрує різні базові технології, може здійснюватися і засобами канального рівня: для цього

можуть бути використані деякі типи мостів і комутаторів. Міст або комутатор розділяє мережу на сегменти, локалізуючи трафік усередині сегменту. Тим самим мережа розпадається на окремі підмережі, з яких можуть бути побудовані складові мережі досить крупних розмірів.

Проте побудова складних мереж тільки на основі повторювачів, мостів і комутаторів має істотні обмеження і недоліки.

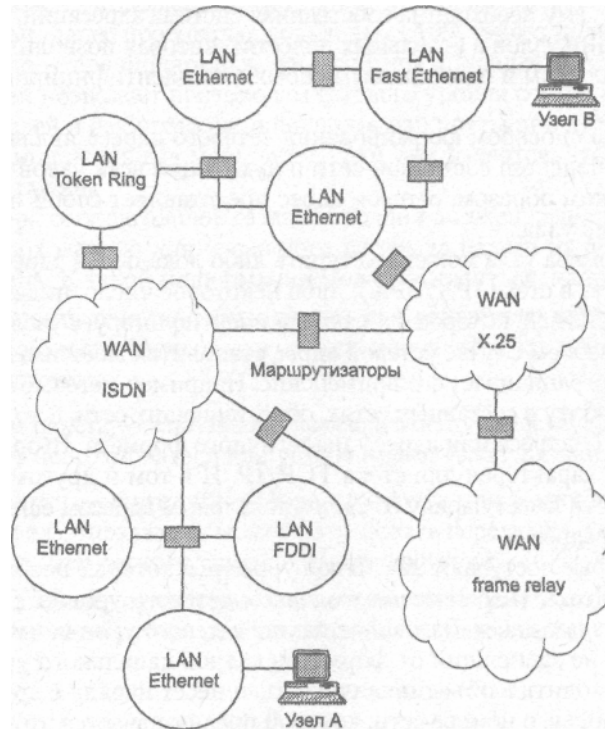
- По-перше, в топології мережі, повинні *бути відсутнім петлі*. Дійсно, міст/комутатор може вирішувати задачу доставки пакету адресату тільки тоді, коли між відправником і одержувачем існує єдиний шлях. В той же час наявність надмірних зв'язків, які і утворюють петлі, необхідна для кращого балансування навантаження, а також для підвищення надійності мережі за рахунок утворення резервних шляхів.
- По-друге, логічні сегменти мережі *слабо ізольовані* один від одного, а саме не захищені від так званих ширококомовних штормів. Якщо яка-небудь станція посилає ширококомовне повідомлення, то це повідомлення передається всім станціям всіх логічних сегментів мережі. Захист від ширококомовних штормів в мережах, побудованих на основі мостів і комутаторів, має кількісний, а не якісний характер: адміністратор просто обмежує кількість ширококомовних пакетів, яку дозволяється генерувати деякому вузлу в одиницю часу. Використовування ж механізму віртуальних мереж, реалізованого в багатьох комутаторах, хоча і дозволяє достатньо гнучко створювати ізольовані по трафіку групи станцій, але при цьому ізолює їх повністю, так що вузли однієї віртуальної мережі не можуть взаємодіяти з вузлами іншої віртуальної мережі.
- По-третє, складно розв'язується задача управління трафіком на основі даних, що містяться в пакеті. У таких мережах це можливо тільки за допомогою користувацьких фільтрів, для створення яких адміністратору доводиться мати справу з двійковим представленням пакетів.

- По-четверте, реалізація транспортної підсистеми тільки засобами фізичного і канального рівнів, до яких відносяться мости і комутатори, приводить до недостатньо гнучкої, однорівневої системи адресації: як адреса призначення використовується MAC-адреса, жорстко пов'язана з мережевим адаптером.
- Нарешті, можливістю трансляції протоколів канального рівня володіють далеко не всі типи мостів і комутаторів, до того ж ці можливості обмежені. Зокрема, повинні співпадати максимально допустимі розміри полів даних в кадрах, оскільки мостами і комутаторами не підтримується функція фрагментації кадрів.

Наявність серйозних обмежень у протоколів канального рівня показує, що побудова на основі засобів цього рівня великих неоднорідних мереж є вельми проблематичною.

16.2. Поняття *internetworking*

Мережа в загальному випадку розглядається як сукупність декількох мереж і називається складовою мережею або інтермережею (*internet work* або *internet*). Мережі, що входять в складову мережу, називаються підмережами (*subnet*) (мал. 5.1).



Мал. 5.1. Архітектура складової мережі

Підмережі з'єднуються між собою маршрутизаторами. Компонентами складової мережі можуть бути як локальні, так і глобальні мережі. Внутрішня структура кожної мережі на малюнку не показана, оскільки вона не має значення при розгляді мережевого протоколу. Всі вузли в межах однієї підмережі взаємодіють, використовуючи єдину для них технологію. Так, в складову мережу, показану на малюнку, входить декілька мереж різних технологій: локальні мережі Ethernet, Fast Ethernet, Token Ring, FDDI і глобальні мережі frame relay, X.25, ISDN. Кожна з цих технологій достатня для того, щоб організувати взаємодію всіх вузлів в своїй підмережі, але не здатна побудувати інформаційний зв'язок між довільно вибраними вузлами, що належать різним підмережам, наприклад між вузлом А і вузлом В на мал. 5.1. Отже, для організації взаємодії між будь-якою довільною парою вузлів цієї «великої» складової мережі потрібні додаткові засоби. Такі засоби і надає мережевий рівень.

Мережевий рівень виступає як координатор, організуючий роботу всіх підмереж, що лежать на шляху просування пакету по складовій мережі. Для переміщення даних в межах підмереж мережевий рівень звертається до використовуваних в цих підмережах технологій.

Хоча багато технологій локальних мереж (Ethernet, Token Ring, FDDI, Fast Ethernet і ін.) використовують одну і ту ж систему адресації вузлів на основі MAC-адрес, існує немало технологій (X.25, АТМ, frame relay), в яких застосовуються інші схеми адресації. Адреси, привласнені вузлам відповідно до технологій підмереж, називають локальними. Щоб мережевий рівень міг виконати свою задачу, йому необхідна власна система адресації, не залежна від способів адресації вузлів в окремих підмережах, яка дозволила б на мережевому рівні універсальним і однозначним способами ідентифікувати будь-який вузол складової мережі.

Природним способом формування мережевої адреси є унікальна нумерація всіх підмереж складової мережі і нумерація всіх вузлів в межах кожної підмережі. Таким чином, мережева адреса є парою: номер мережі (підмережі) і номер вузла.

Як номер вузла може виступати або локальна адреса цього вузла (така схема прийнята в стеку IPX/SPX), або деяке число, ніяк не пов'язане з локальною технологією, яке однозначно ідентифікує вузол в межах даної підмережі. У першому випадку мережева адреса стає залежною від локальних технологій, що обмежує його застосування. Наприклад, мережеві адреси IPX/SPX розраховані на роботу в складових мережах, в яких використовуються тільки MAC-адреси або адреси аналогічного формату. Другий підхід більш універсальний, він характерний для стека TCP/IP. І в тому і іншому випадку кожен вузол складової мережі має разом з своєю локальною адресою ще одну – універсальну мережеву адресу.

Дані, які поступають на мережевий рівень і які необхідно передати через складову мережу, забезпечуються заголовком мережевого рівня. Дані

разом із заголовком утворюють пакет. Заголовок пакету мережевого рівня має уніфікований формат, не залежний від форматів кадрів канального рівня тих мереж, які можуть входити в рб'єдіненну мережу, і несе разом з іншою службовою інформацією дані про номер мережі, якій призначається цей пакет. Мережевий рівень визначає маршрут і переміщає пакет між підмережами.

При передачі пакету з однієї підмережі в іншу пакет мережевого рівня, інкапсульований в прибулий канальний кадр першої підмережі, звільняється від заголовків цього кадру і оточується заголовками кадру канального рівня наступної підмережі. Інформацією, на основі якої робиться ця заміна, є _ службові поля пакету мережевого рівня. У полі адреси призначення нового кадру розташовується локальна адреса наступного маршрутизатора.

ПРИМІТКА Якщо в підмережі доставка даних здійснюється засобами канального і фізичного рівнів (як, наприклад, в стандартних локальних мережах), то пакети мережевого рівня вкладаються в кадри канального рівня. Якщо ж в якій-небудь підмережі для транспортування повідомлень використовується технологія, заснована на стеках з великим числом рівнів, то пакети мережевого рівня упаковуються в блоки передаваних даних найвищого рівня підмережі.

Якщо проводити аналогію між взаємодією різнорідних мереж і листуванням людей з різних країн, то мережева інформація – це загальноприйнятий індекс країни, доданий до адреси листу, написаному на одному з сотні мов земної кулі, наприклад на санскриті. І навіть якщо цей лист повинен пройти через безліч країн, поштові працівники яких не знають санскриту, зрозумілий їм індекс країни-адресата підкаже, через які проміжні країни краще передати лист, щоб воно найкоротшим шляхом потрапило до Індії. А вже там працівники місцевих поштових відділень зможуть прочитати точну адресу, указива-

Основним полем заголовка мережевого рівня є номер мережі-адресата. У розглянутих нами раніше протоколах локальних мереж такого поля в кадрах передбачено не було – передбачалося, що всі вузли належать одній мережі. Явна нумерація мереж дозволяє протоколам мережевого рівня скласти точну карту міжмережєвих зв'язків і вибирати раціональні маршрути при будь-якій їх топології, зокрема альтернативні маршрути, якщо вони є, що не уміють робити мости і комутатори.

Окрім номера мережі заголовок мережевого рівня повинен містити і іншу інформацію, необхідну для успішного переходу пакету з мережі одного типу в мережу іншого типу. До такої інформації може відноситися, наприклад:

- номер фрагмента пакету, необхідний для успішного проведення операцій збірки-розбирання фрагментів при з'єднанні мереж з різними максимальними розмірами пакетів;
- час життя пакету, вказуюче, як довго він подорожує по інтермережі, цей час може використовуватися для знищення пакетів, що «заблукали»;
- якість послуги – критерій вибору маршруту при міжмережєвих передачах - наприклад, вузол-відправник може зажадати передати пакет з максимальною надійністю, можливо, в збиток часу доставки.

Коли дві або більш мережі організують сумісну транспортну службу, то такий режим взаємодії звичайно називають міжмережєвою взаємодією (internetworking).

16.3. Принципи маршрутизації

Найважливішою задачею мережевого рівня є маршрутизація – передача пакетів між двома кінцевими вузлами в складовій мережі.

Розглянемо принципи маршрутизації на прикладі складової мережі, зображеної на мал. 5.2. У цій мережі 20 маршрутизаторів об'єднують 18 мереж в загальну мережу; S1, S2, ..., S20 – це номери мереж. Маршрутизатори

мають по декілька портів (принаймні, по два), до яких приєднуються мережі. Кожен порт маршрутизатора можна розглядати як окремий вузол мережі: він має власну мережеву адресу і власну локальну адресу в тій підмережі, яка до нього підключена. Наприклад, маршрутизатор під номером 1 має три порти, до яких підключені мережі S1, S2, S3. На малюнку мережеві адреси цих портів позначені як M1(1), M1(2) і M1(3). Порт M1(1) має локальну адресу в мережі з номером S1, порт M1(2) – в мережі S2, а порт M1(3) – в мережі S3. Таким чином, маршрутизатор можна розглядати як сукупність декількох вузлів, кожний з яких входить в свою мережу. Як єдиний пристрій маршрутизатор не має ні окремої мережевої адреси, ні якої-небудь локальної адреси.

ПРИМІТКА Якщо маршрутизатор має блок управління (наприклад, SNMP-управління), то цей блок має власні локальну і мережеву адреси, по яких до нього звертається центральна станція управління, що знаходиться десь в складовій мережі.

У складних складових мережах майже завжди існує декілька альтернативних маршрутів для передачі пакетів між двома кінцевими вузлами. Маршрути – це послідовність маршрутизаторів, які повинен пройти пакет від відправника до пункту призначення. Так, пакет, відправлений з вузла А у вузол В, може пройти через маршрутизатори 17,12, 5,4 і 1 або маршрутизатори 17,13,7, 6 і 3. Неважко знайти ще декілька маршрутів між вузлами А і В.

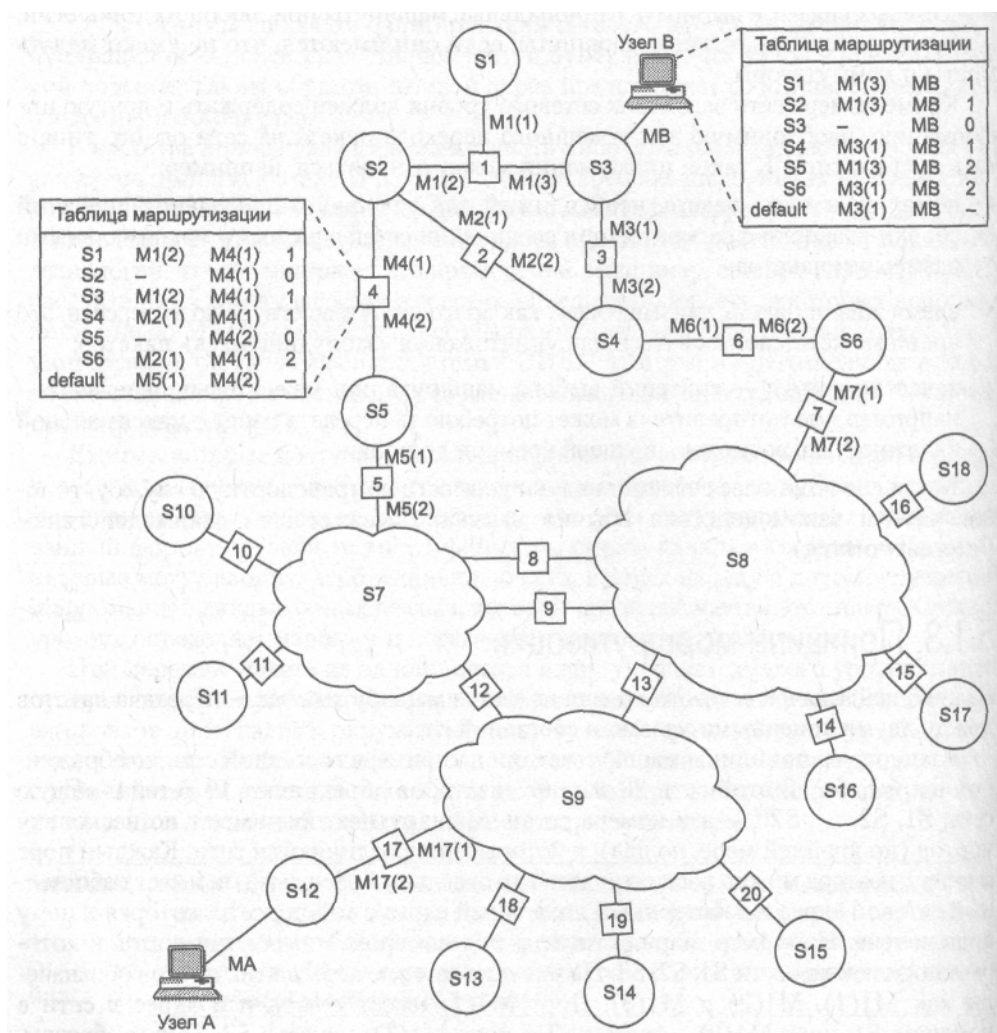


Рис. 5.2. Принципи маршрутизації в складовій мережі

Задачу вибору маршруту з декількох можливих вирішують маршрутизатори, а також кінцеві вузли. Маршрут вибирається на підставі інформації, що є у цих пристроїв, про поточну конфігурацію мережі, а також на підставі вказаного критерію вибору маршруту. Звичайно як критерій виступає затримка проходження маршруту окремим пакетом або середня пропускна спроможність.

Щоб за адресою мережі призначення можна було б вибрати раціональний маршрут подальшого проходження пакету, кожен кінцевий вузол і маршрутизатор аналізують спеціальну інформаційну структуру, яка називається таблицею маршрутизації. Використовуючи умовні позначення для мережевих адрес маршрутизаторів і номерів мереж в тому вигляді, як

вони приведені на мал. 5.2, подивимося, як могла б виглядати таблиця маршрутизації, наприклад, в маршрутизаторі 4 (табл. 5.1).

Таблиця 5.1. Таблиця маршрутизації маршрутизатора 4

Номер мережі	Мережева адреса наступного маршрутизатора	Мережева адреса вихідного порту	Відстань до мережі призначення
S1	M1(2)	M4(1)	1
S2	–	M4(1)	0 (приєднана)
S3	M1(2)	144(1)	1
S4	M2(1)	M4(1)	1
S5	–	M4(2)	0 (приєднана)
S6	M2(1)	M4(1)	2
Default	M5(1)	«4(?)»	–

ПРИМІТКА Таблиця 5.1 значно спрощена в порівнянні з реальними таблицями, наприклад, відсутні стовпці з масками, ознаками стану маршруту, часом, протягом якого дійсні записи даної таблиці (їх застосування буде розглянуте пізніше). Крім того, як вже було сказано, тут вказані адреси мереж умовного формату, не відповідні якому-небудь певному мережевому протоколу. Проте ця таблиця містить основні поля, що є в реальних таблицях при використуванні конкретних мережевих протоколів, таких як IP, IPX або X.25.

У першому стовпці таблиці перераховуються номери мереж, що входять в інтермережу. У кожному рядку таблиці слідом за номером мережі

указується мережева адреса наступного маршрутизатора (більш точно, мережева адреса відповідного порту наступного маршрутизатора), на який треба направити пакет, щоб той пересувався у напрямку до мережі з даним номером по раціональному маршруту.

Коли на маршрутизатор поступає новий пакет, номер мережі призначення, витягнутий з кадру, що поступив, послідовно порівнюється з номерами мереж з кожного рядка таблиці. Рядок з номером мережі, що співпав, вказує, на який найближчий маршрутизатор слід направити пакет. Наприклад, якщо на який-небудь порт маршрутизатора 4 поступає пакет, адресований в мережу S6, то з таблиці маршрутизації виходить, що адреса наступного маршрутизатора – M2(1), тобто черговим етапом руху даного пакету буде рух до порту 1 маршрутизатора 2.

Оскільки пакет може бути адресований в будь-яку мережу складової мережі, може показатися, що кожна таблиця маршрутизації повинна мати записи про всі мережі, що входять в складову мережу. Але при такому підході у разі крупної мережі об'єм таблиць маршрутизації може виявитися дуже великим, що вплине на час її перегляду, зажадає багато місця для зберігання і т.п. Тому на практиці число записів в таблиці маршрутизації прагнуть зменшити за рахунок використання спеціального запису – *«маршрутизатор за умовчанням» (default)*. Дійсно, якщо взяти до уваги топологію складової мережі, то в таблицях маршрутизаторів, що знаходяться на периферії складової мережі, достатньо записати номери мереж, безпосередньо приєднаних до даного маршрутизатора[^] або розташованих поблизу, на тупикових маршрутах. Про всю ж решту мереж можна зробити в таблиці єдиний запис, вказуючий на маршрутизатор, через який пролягає шлях до всіх цих мереж. Такий маршрутизатор називається маршрутизатором за умовчанням, а замість номера мережі у відповідному рядку поміщається особливий запис, наприклад default. У нашому прикладі таким маршрутизатором за умовчанням для мережі S5 є маршрутизатор 5,

точніший його порт M5(1). Це означає, що шлях з мережі S5 майже до всіх мереж великої складової мережі пролягає через цей порт маршрутизатора.

Перш ніж передати пакет наступному маршрутизатору, поточний маршрутизатор повинен визначити, на який з декількох власних портів він повинен помістити даний пакет. Для цього служить третій стовпець таблиці маршрутизації. Ще раз підкреслимо, що кожен порт ідентифікується власною мережевою адресою.

Деякі реалізації мережевих протоколів допускають наявність в таблиці маршрутизації відразу декількох рядків, відповідних одній і тій же адресі мережі призначення. В цьому випадку при виборі маршруту береться до уваги стовпець «Відстань до мережі призначення». При цьому під відстанню розуміється будь-яка метрика, використовувана відповідно до заданого в мережевому пакеті критерію (часто званим класом сервісу). Відстань може вимірюватися хопами, часом проходження пакету по лініях зв'язку, якою-небудь характеристикою надійності ліній зв'язку на даному маршруті або іншою величиною, що відображає якість даного маршруту по відношенню до заданого критерію. Якщо маршрутизатор підтримує декілька класів сервісу пакетів, то таблиця маршрутів складається і застосовується окремо для кожного виду сервісу (критерію вибору маршруту).

У табл. 5.1 відстань між мережами вимірювалася хопами. Відстань для мереж, безпосередньо підключених до портів маршрутизатора, тут приймається рівною 0, проте в деяких реалізаціях відлік відстаней починається з 1.

Наявність декількох маршрутів до одного вузла роблять можливим передачу трафіку до цього вузла паралельно по декількох каналах зв'язку, це підвищує пропускну спроможність і надійність мережі.

Задачу маршрутизації вирішують не тільки проміжні вузли-маршрутизатори, але і кінцеві вузли – комп'ютери. Засоби мережевого рівня, встановлені на кінцевому вузлі, при обробці пакету повинні, перш за все,

визначити, чи прямує він в іншу мережу або адресований якому-небудь вузлу даної мережі. Якщо номер мережі призначення співпадає з номером даної мережі, то для даного пакету не вимагається вирішувати задачу маршрутизації. Якщо ж номери мереж відправлення і призначення не співпадають, то маршрутизація потрібна. Таблиці маршрутизації кінцевих вузлів повністю аналогічні таблицям маршрутизації, що зберігаються на маршрутизаторах.

Звернемося знову до мережі, зображеної на мал. 5.2. Таблиця маршрутизації для кінцевого вузла В могла б виглядати таким чином (табл. 5.2). Тут MB – мережева адреса порту комп'ютера В. На підставі цієї таблиці кінцевий вузол У вибирає, на який з двох S3 маршрутизаторів, що є в локальній мережі, слід посилати той або інший пакет.

Таблиця 5.2. Таблиця маршрутизації кінцевого вузла В

Номер мережі призначення	Мережева адреса наступного маршрутизатора	Мережева адреса вихідного порту	Відстань до мережі призначення
S1	M1(3)	MB	1
S2	M1(3)	MB	1
S3	–	MB	0
S4	M3(1)	MB	1
S5	M1(3)	MB	2
S6	M3(1)	MB	2
Default	M3(1)	MB	–

Кінцеві вузли в ще більшому ступені, ніж маршрутизатори, користуються прийомом маршрутизації за умовчанням. Хоча вони також в

загальному випадку мають в своєму розпорядженні таблицю маршрутизації, її об'єм звичайно незначний, що пояснюється периферійним розташуванням всіх кінцевих вузлів. Кінцевий вузол часто взагалі працює без таблиці маршрутизації, маючи тільки відомості про адресу маршрутизатора за умовчанням. За наявності одного маршрутизатора в локальній мережі цей варіант – єдино можливий для всіх кінцевих вузлів. Але навіть за наявності декількох маршрутизаторів в локальній мережі, коли перед кінцевим вузлом стоїть проблема їх вибору, завдання маршруту за умовчанням часто використовується в комп'ютерах для скорочення об'єму їх таблиці маршрутизації.

Нижче поміщена таблиця маршрутизації іншого кінцевого вузла складової мережі – вузла А (табл. 5.3). Компактний вид таблиці маршрутизації відображає той факт, що всі пакети, що направляються з вузла А, або не виходять за межі мережі S12, або неодмінно проходять через порт 1 маршрутизатора 17. Цей маршрутизатор і визначений в таблиці маршрутизації як маршрутизатор за умовчанням.

Таблиця 5.3. Таблиця маршрутизації кінцевого вузла А

Номер мережі	Мережева адреса	
Мережева адреса наступного маршрутизатора	Відстань до мережі призначення вихідного порту	призначення
S12		МА
0 Default	M17(!)	МА
–		

Ще однією відмінністю роботи маршрутизатора і кінцевого вузла при виборі маршруту є спосіб побудови таблиці маршрутизації. Якщо маршрутизатори звичайно автоматично створюють таблиці маршрутизації,

обмінюючись службовою інформацією, то для кінцевих вузлів таблиці маршрутизації часто створюються уручну адміністраторами і зберігаються у вигляді постійних файлів на дисках.

16.4. Протоколи маршрутизації

Задача маршрутизації розв'язується на основі аналізу таблиць маршрутизації, розміщених у всіх маршрутизаторах і кінцевих вузлах мережі. Яким же чином проходить формування цих таблиць? Якими засобами забезпечується адекватність інформації, що міститься в них, структурі мережі, що постійно змінюється? Основна робота із створення таблиць маршрутизації виконується автоматично, але і можливість уручну скоректувати або доповнити таблицю теж, як правило, передбачається.

Для автоматичної побудови таблиць маршрутизації маршрутизатори обмінюються інформацією про топологію складової мережі відповідно до спеціального службового протоколу. Протоколи цього типу називаються протоколами маршрутизації (або маршрутизуючими протоколами). Протоколи маршрутизації (наприклад, RIP, OSPF, NLSP) слід відрізнити від власне мережевих протоколів (наприклад, IP, IPX). І ті і інші виконують функції мережевого рівня моделі OSI – беруть участь в доставці пакетів адресату через різнорідну складову мережу. Але тоді як перші збирають і передають по мережі чисто службову інформацію, другі призначені для передачі призначених для користувача даних, як це роблять протоколи канального рівня. Протоколи маршрутизації використовують мережеві протоколи як транспортний засіб. При обміні маршрутною інформацією пакети протоколу маршрутизації поміщаються в полі даних пакетів мережевого рівня або навіть транспортного рівня, тому з погляду вкладеності пакетів протоколи маршрутизації формально слід було б віднести до вищого рівня, ніж мережевий.

У тому, що маршрутизатори для ухвалення рішення про просування пакету звертаються до адресних таблиць, можна побачити їх деяка схожість з мостами і комутаторами. Проте природа використовуваних ними адресних таблиць сильно розрізняється. Замість MAC-адрес в таблицях маршрутизації вказуються номери мереж, які з'єднуються в інтермережу. Іншою відмінністю таблиць маршрутизації від адресних таблиць мостів є спосіб їх створення. Тоді як міст будує таблицю, пасивно спостерігаючи за проходжаними через нього інформаційними кадрами, посланими кінцевими вузлами мережі один одному, маршрутизатори за своєю ініціативою обмінюються спеціальними службовими пакетами, повідомляючи сусідів про відомі їм мережі в інтермережі, маршрутизаторах і про зв'язки цих мереж з маршрутизаторами. Звичайно враховується не тільки топологія зв'язків, але і їх пропускна спроможність і стан. Це дозволяє маршрутизаторам швидше адаптуватися до змін конфігурації мережі, а також правильно передавати пакети в мережах з довільною топологією, що допускає наявність замкнутих контурів.

За допомогою протоколів маршрутизації маршрутизатори складають карту зв'язків мережі того або іншого ступеня подробности. На підставі цієї інформації для кожного номера мережі ухвалюється рішення про те, якому наступному маршрутизатору треба передавати пакети, що направляються в цю мережу, щоб маршрут виявився раціональним. Результати цих рішень заносяться в таблицю маршрутизації. При зміні конфігурації мережі деякі записи в таблиці стають недійсними. У таких випадках пакети, відправлені по помилкових маршрутах, можуть зациклюватися і втрачатися. Від того, наскільки швидко протокол маршрутизації приводить у відповідність вміст таблиці реальному стану мережі, залежить якість роботи всієї мережі.

Протоколи маршрутизації можуть бути побудовані на основі різних алгоритмів, відмінних способами побудови таблиць маршрутизації,

способами вибору якнайкращого маршруту і іншими особливостями своєї роботи.

У всіх описаних вище прикладах при виборі раціонального маршруту визначався тільки наступний (найближчий) маршрутизатор, а не вся послідовність маршрутизаторів від початкового до кінцевого вузла. Відповідно до цього підходу маршрутизація виконується по розподіленій схемі – кожен маршрутизатор відповідальний за вибір тільки одного кроку маршруту, а остаточний маршрут складається в результаті роботи всіх маршрутизаторів, через які проходить даний пакет. Такі алгоритми маршрутизації називаються однокроковими.

Існує і прямо протилежний, багатокроковий підхід – *маршрутизація від джерела (Source Routing)*. Відповідно до нього вузол-джерело задає в пакеті, що відправляється в мережу, повний маршрут його проходження через всі проміжні маршрутизатори. При використуванні багатокрокової маршрутизації немає необхідності будувати і аналізувати таблиці маршрутизації. Це прискорює проходження пакету по мережі, розвантажує маршрутизатори, але при цьому велике навантаження лягає на кінцеві вузли. Ця схема в обчислювальних мережах застосовується сьогодні набагато рідше, ніж схема розподіленої однокрокової маршрутизації. Проте в новій версії протоколу IP разом з класичною однокроковою маршрутизацією буде дозволена і маршрутизація від джерела.

Однокрокові алгоритми залежно від способу формування таблиць маршрутизації діляться на три класи:

- алгоритми фіксованої (або статичної) маршрутизації;
- алгоритми простої маршрутизації;
- алгоритми адаптивної (або динамічної) маршрутизації.

У алгоритмах *фіксованої маршрутизації* всі записи в таблиці маршрутизації є статичними. Адміністратор мережі сам вирішує, на які маршрутизатори треба передавати пакети з тими або іншими адресами, і

уручну (наприклад, за допомогою утиліти route ОС Unix або Windows NT) заносить відповідні записи в таблицю маршрутизації. Таблиця, як правило, створюється в процесі завантаження, надалі вона використовується без змін до тих пір, поки її вміст не буде відредаговано уручну. Такі виправлення можуть знадобитися, наприклад, якщо в мережі відмовляє який-небудь маршрутизатор і його функції покладаються на інший маршрутизатор. Розрізняють одномаршрутні таблиці, в яких для кожного адресата заданий один шлях, і багатомаршрутні таблиці, що визначають декілька альтернативних шляхів для кожного адресата. У багатомаршрутних таблицях повинне бути задане правило вибору одного з маршрутів. Частіше всього один шлях є основним, а інші – резервними. Зрозуміло, що алгоритм фіксованої маршрутизації з його ручним способом формування таблиць маршрутизації прийнятний тільки в невеликих мережах з простою топологією. Проте цей алгоритм може бути ефективно використаний і для роботи на магістралях крупних мереж, оскільки сама магістраль може мати просту структуру з очевидними якнайкращими шляхами проходження пакетів в підмережі, приєднані до магістралі.

У алгоритмах *простої маршрутизації* таблиця маршрутизації або зовсім не використовується, або будується без участі протоколів маршрутизації. Виділяють три типи простої маршрутизації:

- *випадкова маршрутизація*, коли прибулий пакет посилається в першому випадковому напрямі, що потрапив, окрім початкового;
- *лавинна маршрутизація*, коли пакет ширококомовно посилається по всіх можливих напрямках, окрім початкового (аналогічно обробці мостами кадрів з невідомою адресою);
- *маршрутизація по попередньому досвіду*, коли вибір маршруту здійснюється по таблиці, але таблиця будується за принципом моста шляхом аналізу адресних полів пакетів, що з'являються на вхідних портах.

Найпоширенішими є алгоритми *адаптивної* (або *динамічної*) *маршрутизації*. Ці алгоритми забезпечують автоматичне оновлення таблиць маршрутизації після зміни конфігурації мережі. Протоколи, побудовані на основі адаптивних алгоритмів, дозволяють всім маршрутизаторам збирати інформацію про топологію зв'язків в мережі, оперативно відпрацьовувати всі зміни конфігурації зв'язків. У таблицях маршрутизації при адаптивній маршрутизації звичайно є інформація про інтервал часу, протягом якого даний маршрут залишатиметься дійсним. Цей час називають часом *життя маршруту* (*Time To Live, TTL*).

Адаптивні алгоритми звичайно мають розподілений характер, який виражається у тому, що в мережі відсутні які-небудь виділені маршрутизатори, які збирали б і узагальнювали топологічну інформацію: ця робота розподілена між всіма маршрутизаторами.

ПРИМІТКА Останнім часом намітилася тенденція використовувати так звані сервери маршрутів. Сервер маршрутів збирає маршрутну інформацію, а потім роздає її по запитах маршрутизаторам, які звільняються в цьому випадку від функції створення таблиць маршрутизації, або створюють тільки частини цих таблиць. З'явилися спеціальні протоколи взаємодії маршрутизаторів з серверами маршрутів, наприклад *Next Hop Resolution Protocol (NHRP)*.

Адаптивні алгоритми маршрутизації повинні відповідати декільком важливим вимогам. По-перше, вони повинні забезпечувати, якщо не оптимальність, то хоча б раціональність маршруту. По-друге, алгоритми повинні бути достатньо простими, щоб при їх реалізації не витрачалися дуже багато мережеві ресурси, зокрема вони не повинні вимагати дуже великого об'єму обчислень або породжувати інтенсивний службовий трафік. І нарешті, алгоритми маршрутизації повинні володіти властивістю збіжності, тобто завжди приводити до однозначного результату за прийнятний час.

Адаптивні протоколи обміну маршрутною інформацією, вживані в даний час в обчислювальних мережах, в свою чергу діляться на дві групи, кожна з яких пов'язана з одним з наступних типів алгоритмів:

- дистанційно-векторні алгоритми (Distance Vector Algorithms, DVA);
- алгоритми стану зв'язків (Link State Algorithms, LSA).

У алгоритмах *дистанційно-векторного типу* кожен маршрутизатор періодично і ширококомовно розсилає по мережі вектор, компонентами якого є відстані від даного маршрутизатора до всіх відомих йому мереж. Під відстанню звичайно розуміється число хопів. Можлива і інша метрика, що враховує не тільки число проміжних маршрутизаторів, але і час проходження пакетів по мережі між сусідніми маршрутизаторами. При отриманні вектора від сусіда маршрутизатор нарощує відстані до вказаних у векторі мереж на відстань до даного сусіда. Одержавши вектор від сусіднього маршрутизатора, кожний маршрутизатор додає до нього інформацію про відомих йому інших мережах, про яких він взнав безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектора по мережі. Врешті-решт, кожен маршрутизатор дізнається інформацію про всі мережі, що є в інтермережі, і про відстань до них через сусідні маршрутизатори.

Дистанційно-векторні алгоритми добре працюють тільки в невеликих мережах. У великих мережах вони засмічують лінії зв'язку інтенсивним ширококомовним трафіком, до того ж зміни конфігурації можуть відпрацьовуватися по цьому алгоритму не завжди коректно, оскільки маршрутизатори не мають точного уявлення про топологію зв'язків в мережі, а мають в своєму розпорядженні тільки узагальнену інформацію – вектор дистанцій, до того ж одержаної через посередників. Робота маршрутизатора відповідно до дистанційно-векторного протоколу нагадує роботу моста, оскільки точної топологічної картини мережі такий маршрутизатор не має.

Найпоширенішим протоколом, заснованим на дистанційно-векторному алгоритмі, є протокол RIP, який поширений в двох версіях – RIP IP, працюючий з протоколом IP, і RIP IPX, працюючий з протоколом IPX.

Алгоритми стану зв'язків забезпечують кожен маршрутизатор інформацією, достатньою для побудови точного графа зв'язків мережі. Всі маршрутизатори працюють на підставі однакових графів, що робить процес маршрутизації стійкішим до змін конфігурації. «Широкомовна» розсилка (тобто передача пакету всім безпосереднім сусідам маршрутизатора) використовується тут тільки при змінах стану зв'язків, що відбувається в надійних мережах не так часто. Вершинами графа є як маршрутизатори, так і об'єднані ними мережі. Поширювана по мережі інформація складається з опису зв'язків різних типів: маршрутизатор–маршрутизатор, маршрутизатор–мережа.

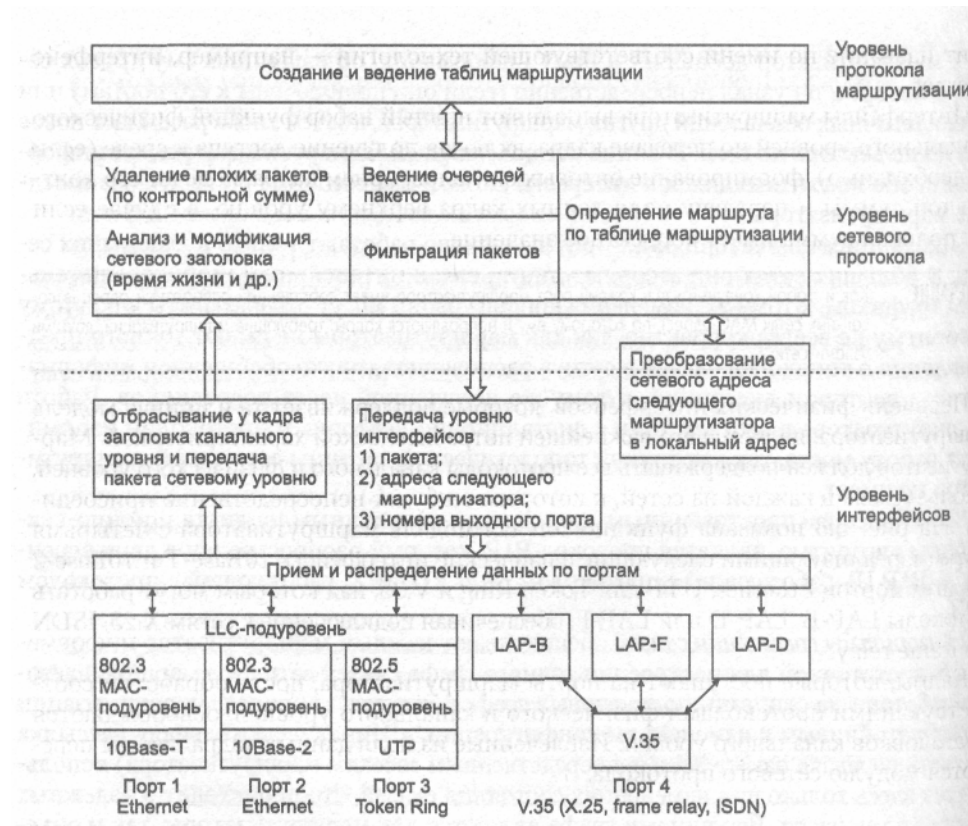
Щоб зрозуміти, в якому стані знаходяться лінії зв'язку, підключені до його портів, маршрутизатор періодично обмінюється короткими пакетами HELLO з своїми найближчими сусідами. Цей службовий трафік також засмічує мережу, але не в такому ступені як, наприклад, RIP-пакети, оскільки пакети HELLO мають набагато менший об'єм.

Протоколами, заснованими на алгоритмі стану зв'язків, є протоколи IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP і недавно реалізований протокол NLSP стека Novell.

16.5. Функції маршрутизатора

Основна функція маршрутизатора – читання заголовків пакетів мережевих протоколів, що приймаються і буферизованих по кожному порту (наприклад, IPX, IP, AppleTalk або DECnet), і ухвалення рішення про подальший маршрут проходження пакету за його мережевою адресою, що включає, як правило, номер мережі і номер вузла.

Функції маршрутизатора можуть бути розбиті на 3 групи відповідно до рівнів моделі OSI (мал. 5.3).



Мал. 5.3. Функціональна модель маршрутизатора

Рівень інтерфейсів

На нижньому рівні маршрутизатор, як і будь-який пристрій, підключений до мережі, забезпечує фізичний інтерфейс з середовищем передачі, включаючи узгодження рівнів електричних сигналів, лінійне і логічне кодування, оснащення певним типом роз'єму. У різних моделях маршрутизаторів часто передбачаються різні набори фізичних інтерфейсів, що є комбінацією портів для під'єднання локальних і глобальних мереж. З кожним інтерфейсом для підключення локальної мережі нерозривно зв'язаний певний протокол канального рівня – наприклад, Ethernet, Token Ring, FDDI. Інтерфейси для приєднання до глобальних мереж найчастіше визначають тільки деякий стандарт фізичного рівня, над яким в маршрутизаторі можуть працювати різні протоколи канального рівня.

Наприклад, глобальний порт може підтримувати інтерфейс V.35, над яким можуть працювати протоколи канального рівня: LAP-B (використовуваний в мережах X.25), LAP-F (використовуваний в мережах frame relay), LAP-D (використовуваний в мережах ISDN). Різниця між інтерфейсами локальних і глобальних мереж пояснюється тим, що технології локальних мереж працюють за власними стандартами фізичного рівня, які не можуть, як правило, використовуватися в інших технологіях, тому інтерфейс для локальної мережі є поєднанням фізичного і канального рівнів і носить назву на ім'я відповідної технології – наприклад, інтерфейс Ethernet.

Інтерфейси маршрутизатора виконують повний набір функцій фізичного і канального рівнів по передачі кадру, включаючи отримання доступу до середовища (якщо це необхідно), формування бітових сигналів, прийом кадру, підрахунок його контрольної суми і передачу поля даних кадру верхньому рівню, у випадку якщо контрольна сума має коректне значення.

ПРИМІТКА Кожі і будь-який кінцевий вузол, кожен порт маршрутизатора має власну апаратну адресу (у локальних мережах MAC-адреса), по якому йому і прямують кадри, що вимагають маршрутизації, іншими вузлами сети.

Перелік фізичних інтерфейсів, які підтримує та або інша модель маршрутизатора, є його найважливішою споживацькою характеристикою. Маршрутизатор повинен підтримувати всі протоколи канального і фізичного рівнів, використовувані в кожній з мереж, до яких він буде безпосередньо приєднаний. На мал. 5.3 показана функціональна модель маршрутизатора з чотирма портами, що реалізують наступні фізичні інтерфейси: 10Base-T і 10Base-2 для двох портів Ethernet, UTP для Token Ring і V.35, над яким можуть працювати протоколи LAP-B, LAP-D або LAP-F, забезпечуючи підключення до мереж X.25, ISDN або frame relay.

Кадри, які поступають на порти маршрутизатора, після обробки відповідними протоколами фізичного і канального рівнів, звільняються від заголовків канального рівня. Витягнуті з поля даних кадру пакети передаються модулю мережевого протоколу.

Рівень мережевого протоколу

Мережевий протокол в свою чергу витягує з пакету заголовки мережевого рівня і аналізує зміст його полів. Перш за все перевіряється контрольна сума, і якщо пакет прийшов пошкодженим, то він відкидається. Виконується перевірка, чи не перевищив час, який провів пакет в мережі (час життя пакету), допустимої величини. Якщо перевищило – то пакет також відкидається. На цьому етапі вносяться коректування у зміст деяких полів, наприклад, нарощується час життя пакету, перераховується контрольна сума.

На мережевому рівні виконується одна з найважливіших функцій маршрутизатора – фільтрація трафіку. Маршрутизатор, володіючи вищим інтелектом, ніж мости і комутатори, дозволяє задавати і може відпрацьовувати значно складніші правила фільтрації. Пакет мережевого рівня, що знаходиться в полі даних кадру, для мостів/комутаторів представляється неструктурованою двійковою послідовністю. Маршрутизатори ж, програмне забезпечення яких містить модуль мережевого протоколу, здатні виробляти розбір і аналіз окремих полів пакету. Вони оснащуються розвиненими засобами призначеного для користувача інтерфейсу, які дозволяють адміністратору без особливих зусиль задавати складні правила фільтрації. Вони, наприклад, можуть заборонити проходження в корпоративну мережу всіх пакетів, окрім пакетів, що поступають з підмереж цього ж підприємства. Фільтрація в даному випадку виробляється за мережевими адресами, і всі пакети, адреси яких не входять в дозволений діапазон, відкидаються. Марш-

рутизатори, як правило, також можуть аналізувати структуру повідомлень транспортного рівня, тому фільтри можуть не пропускати в

мережу повідомлення певних прикладних служб, наприклад служби telnet, аналізуючи поле типу протоколу в транспортному повідомленні.

У випадку якщо інтенсивність надходження пакетів вища інтенсивності, з якою вони обробляються, пакети можуть утворити чергу. Програмне забезпечення маршрутизатора може реалізувати різні дисципліни обслуговування черг пакетів: у порядку надходження за принципом «перший прийшов – першим обслужений» (First Input First Output, FIFO), випадкове раннє виявлення, коли обслуговування йде за правилом FIFO, але при досягненні завдовжки черги деякого порогового значення знов поступаючі пакети відкидаються (Random Early Detection, RED), а також різні варіанти пріоритетного обслуговування.

До мережевого рівня відноситься основна функція маршрутизатора – визначення маршруту пакету. По номеру мережі, витягнутому із заголовка пакету, модуль мережевого протоколу знаходить в таблиці маршрутизації рядок, що містить мережеву адресу наступного маршрутизатора, і номер порту, на який потрібно передати даний пакет, щоб він рухався в правильному напрямі. Якщо в таблиці відсутній запис про мережу призначення пакету і до того ж немає запису про маршрутизатор за умовчанням, то даний пакет відкидається.

Перш ніж передати мережеву адресу наступного маршрутизатора на канальний рівень, необхідно перетворити його на локальну адресу тієї технології, яка використовується в мережі, що містить наступний маршрутизатор. Для цього мережевий протокол звертається до протоколу дозволу адрес. Протоколи цього типу встановлюють відповідність між мережевими і локальними адресами або на підставі наперед складених таблиць, або шляхом розсилки ширококомовних запитів, Таблиця відповідності локальних адрес мережевим адресам будується окремо для кожного мережевого інтерфейсу. Протоколи дозволу адрес займають проміжне положення між мережевим і канальним рівнями.

З мережевого рівня пакет, локальна адреса наступного маршрутизатора і номер порту маршрутизатора передаються вниз, каналному рівню. На підставі вказаного номера порту здійснюється комутація з одним з інтерфейсів маршрутизатора, засобами якого виконується упаковка пакету в кадр відповідного формату. У полі адреси призначення заголовка кадру поміщається локальна адреса наступного маршрутизатора. Готовий кадр відправляється в мережу.

Рівень протоколів маршрутизації

Мережеві протоколи активно використовують в своїй роботі таблицю маршрутизації, але ні її побудовою, ні підтримкою її вмісту не займаються. Ці функції виконують протоколи маршрутизації. На підставі цих протоколів маршрутизатори обмінюються інформацією про топологію мережі, а потім аналізують одержані відомості, визначаючи якнайкращі по тих або інших критеріях маршрути. Результати аналізу і складають вміст таблиць маршрутизації.

Крім перерахованих вище функцій, на маршрутизатори можуть бути покладені і інші обов'язки, наприклад операції, пов'язані з фрагментацією. Детальніше робота маршрутизаторів буде описана при розгляді конкретних протоколів мережевого рівня.

16.6. Реалізація міжмережевої взаємодії засобами TCP/IP

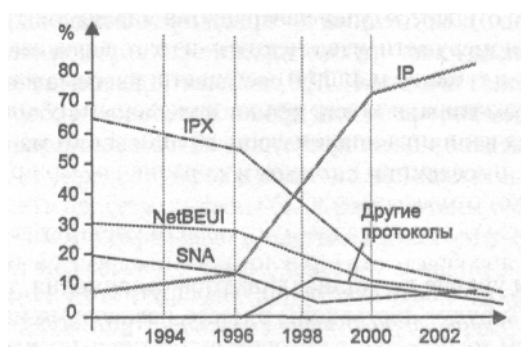
В даний час стек TCP/IP є найпопулярнішим засобом організації складових мереж. На мал. 5.4 показана частка, яку складає той або інший стек протоколів в загальносвітовій інсталяційній мережевій базі. До 1996 року безперечним лідером був стек IPX/SPX компанії Novell, але потім картина різко змінилася – стек TCP/IP по темпах зростання числа установок набагато став випереджати інші стеки, а з 1998 року вийшов в лідери і в абсолютному виразі. Саме тому подальше вивчення функцій мережевого рівня проводитиметься на прикладі стека TCP/IP.

	Прикладний рівень
	Основний (транспортний) рівень
	Рівень міжмережевої взаємодії
	Рівень мережевих інтерфейсів

Мал. 5.5. Багаторівнева архітектура стека TCP/IP

Рівень міжмережевої взаємодії

Стрижнем всієї архітектури є рівень міжмережевої взаємодії, який реалізує концепцію передачі пакетів в режимі без встановлення з'єднань, тобто дейтаграмним способом. Саме цей рівень забезпечує можливість переміщення пакетів по мережі, використовуючи той маршрут, який в даний момент є найраціональнішим. Цей рівень також називають рівнем internet, указуючи тим самим на основну його функцію – передачу даних через складову мережу.



Мал. 5.4. Стек TCP/IP стає основним засобом побудови складових мереж

16.7 Рівні між мережної взаємодії

У стеку TCP/IP визначені 4 рівні (мал. 5.5). Кожний з цих рівнів несе на собі деяке навантаження за рішенням основної задачі – організації надійної і продуктивної роботи складової мережі, частини якої побудовані на основі різних мережевих технологій.

Основним протоколом мережевого рівня (в термінах моделі OSI) в стеку є протокол IP (Internet Protocol). Цей протокол спочатку проектувався як протокол передачі пакетів в складових мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює в мережах з складною топологією, раціонально використовуючи наявність в них підсистем і економно витрачаючи пропускну спроможність низько-швидкісних ліній зв'язку. Оскільки протокол IP є дейтаграмним протоколом, він не гарантує доставку пакетів до вузла призначення, але старається це зробити.

До рівня міжмережевої взаємодії відносяться і всі протоколи, пов'язані з складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол міжмережевих управляючих повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі і вузлом-джерелом пакету. За допомогою спеціальних пакетів ICMP повідомляє про неможливість доставки пакету, про перевищення часу життя або тривалості збірки пакету з фрагментів, про аномальні величини параметрів, про зміну маршруту пересилки і типу обслуговування, про стан системи і т.п.

Основний рівень

Оскільки на мережевому рівні не встановлюються з'єднання, то немає ніяких гарантій, що всі пакети будуть доставлені в місце призначення цілими і неушкодженими або придуть в тому ж порядку, в якому вони були відправлені. Цю задачу -обеспеченіє надійного інформаційного зв'язку між

двома кінцевими вузлами -решаєт *основний рівень* стека TCP/IP, званий також *транспортним*.

На цьому рівні функціонують протокол управління передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача UDP (User Datagram Protocol). Протокол TCP забезпечує надійну передачу повідомлень між видаленими прикладними процесами за рахунок утворення логічних з'єднань. Цей протокол дозволяє рівноранговим об'єктам на комп'ютері-відправнику і комп'ютері-одержувачі підтримувати обмін даними в дуплексному режимі. TCP дозволяє без помилок доставити сформований на одному з комп'ютерів потік байт в будь-який інший комп'ютер, що входить в складову мережу. TCP ділить потік байт на частини – *сегменти* і передає їх нижче лежачому рівню міжмережевої взаємодії. Після того, як ці сегменти будуть доставлені засобами рівня міжмережевої взаємодії в пункт призначення, протокол TCP знову збере їх в безперервний потік байт.

Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і головний протокол рівня міжмережевої взаємодії IP, і виконує тільки функції зв'язуючої ланки (мультиплексора) між мережевим протоколом і численними службами прикладного рівня або призначеними для користувача процесами.

Прикладний рівень

Прикладний рівень об'єднує всі служби, що надаються системою призначеним для користувача додаткам. За довгі роки використання в мережах різних країн і організацій стек TCP/IP накопичив велику кількість протоколів і служб при-

кладного рівня. Прикладний рівень реалізується програмними системами, побудованими в архітектурі клієнт-сервер, що базуються на протоколах нижніх рівнів. На відміну від протоколів решти трьох рівнів, протоколи прикладного рівня займаються деталями конкретного додатку і не

«цікавляться» способами передачі даних по мережі. Цей рівень постійно розширяється за рахунок приєднання до старих, пройшли багаторічну експлуатацію мережевих служб типа Telnet, FTP, TFTP, DNS, SNMP порівняльно нових служб таких, наприклад, як протокол передачі гіпертекстової інформації HTTP.

Рівень мережевих інтерфейсів

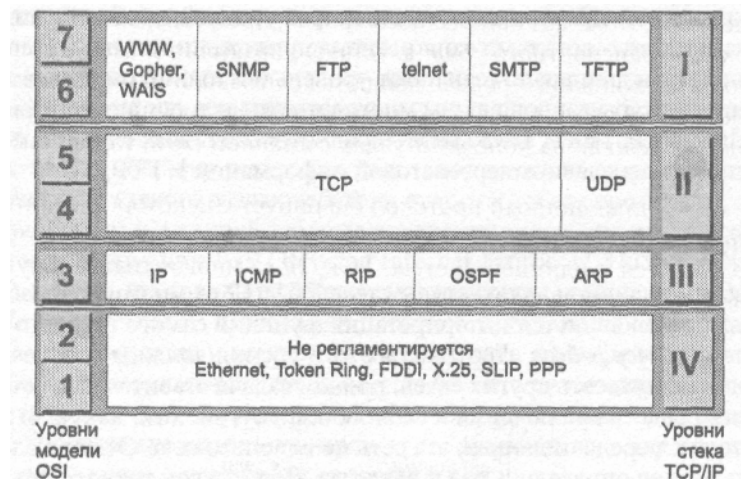
Ідеологічною відмінністю архітектури стека TCP/IP від багаторівневої організації інших стеків є інтерпретація функцій самого нижнього рівня – рівня мережевих інтерфейсів. Протоколи цього рівня повинні забезпечувати інтеграцію в складову мережу інших мереж, причому задача ставиться так: мережа TCP/IP повинна мати засоби включення в себе будь-якої іншої мережі, яку б внутрішню технологію передачі даних ця мережа не використовувала. Звідси витікає, що цей рівень не можна визначити раз і назавжди. Для кожної технології, що включається в складову мережу підмережі, повинні бути розроблені власні інтерфейсні засоби. До таких інтерфейсних засобів відносяться протоколи інкапсуляції IP-пакетів рівня міжмережевої взаємодії в кадри локальних технологій. Наприклад, документ RFC 1042 визначає способи інкапсуляції IP-пакетів в кадри технологій IEEE 802. Для цих цілей повинен використовуватися заголовок LLC/ SNAP, причому в полі Турі заголовка SNAP повинен бути вказаний код 0x0800. Тільки для протоколу Ethernet в RFC 1042 зроблене виключення – крім заголовка LLC/ SNAP дозволяється використовувати кадр Ethernet DIX, що не має заголовка LLC, зате що має поле Турі. У мережах Ethernet переважним є інкапсуляція IP-пакету в кадр Ethernet DIX.

Рівень мережевих інтерфейсів в протоколах TCP/IP не регламентується, але він підтримує всі популярні стандарти фізичного і каналного рівнів: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, IOOVG-AnyLAN, для глобальних мереж – протоколи з'єднань «крапка-крапка» SLIP і PPP, протоколи територіальних

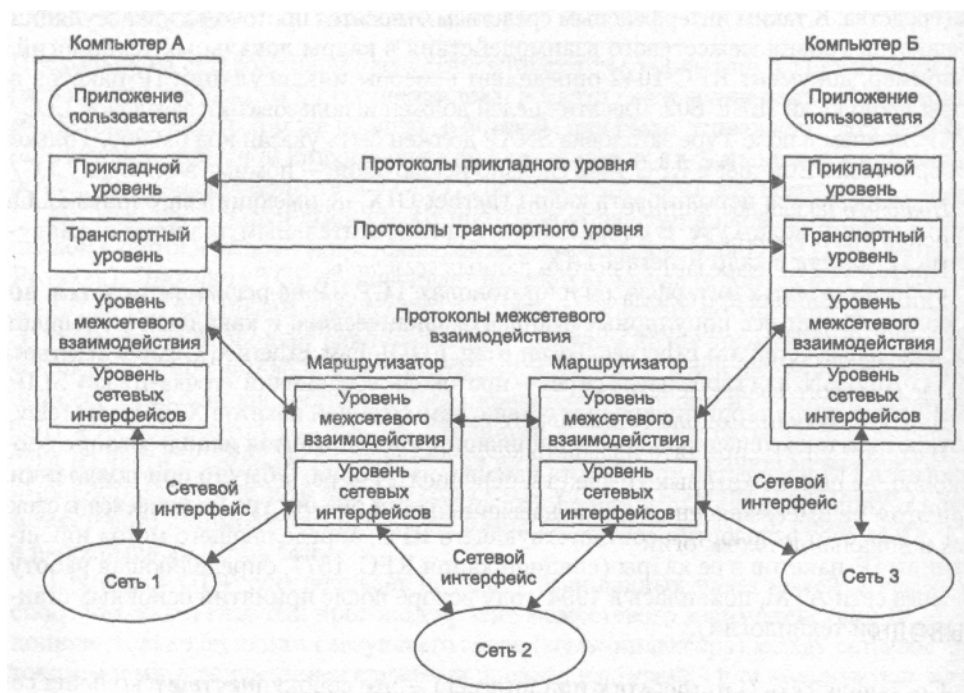
мереж з комутацією пакетів X.25, frame relay. Розроблена також спеціальна специфікація, що визначає використання технології АТМ як транспорт каналного рівня. Звичайно при появі нової технології локальних або глобальних мереж вона швидко включається в стек TCP/IP за рахунок розробки відповідного RFC, визначаючого метод інкапсуляції IP-пакетів в її кадри (специфікація RFC 1577, що визначає роботу IP через мережі АТМ, з'явилася в 1994 році незабаром після ухвалення основних стандартів цієї технології).

16.8 Відповідність рівнів стека TCP/IP семирівневої моделі ISO/OSI

Оскільки стек TCP/IP був розроблений до появи моделі взаємодії відкритих систем ISO/OSI, то, хоча він також має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделі OSI достатньо умовна (мал. 5.6). Розглядаючи багаторівневу архітектуру TCP/IP, можна виділити в ній, подібно архітектурі OSI, рівні, функції яких залежать від конкретної технічної реалізації мережі, і рівні, функції яких орієнтованні на роботу з додатками (мал. 5.7).



Мал. 5.6. Відповідність рівнів стека TCP/IP семирівневої моделі OSI



Мал. 5.7. Сетезавісиміє і сетенезавісиміє рівні стека TCP/IP

Протоколи прикладного рівня стека TCP/IP працюють на комп'ютерах, що виконують додатки користувачів. Навіть повна зміна мережевого устаткування в загальному випадку не повинна впливати на роботу додатків, якщо вони дістають доступ до мережевих можливостей через протоколи прикладного рівня.

Протоколи транспортного рівня вже більш залежать від мережі, оскільки вони реалізують інтерфейс до рівнів, безпосередньо організуючих передачу даних по мережі. Проте, подібно протоколам прикладного рівня, програмні модулі, що реалізують протоколи транспортного рівня, встановлюються тільки на кінцевих вузлах. Протоколи двох нижніх рівнів є сетезавісимими, а отже, програмні модулі протоколів міжмережевого рівня і рівня мережевих інтерфейсів встановлюються як на кінцевих вузлах складової мережі, так і на маршрутизаторах.

Кожен комунікаційний протокол оперує з деякою одиницею передаваних даних. Назви цих одиниць іноді закріплюються стандартом, а

частіше просто визначаються традицією. У стеку TCP/IP за багато років його існування утворилася стала термінологія в цій області (мал. 5.8).



Мал. 5.8. Назва одиниць даних, використовувані в TCP/IP

Потоком називають дані, що поступають від додатків на вхід протоколів транспортного рівня TCP і UDP.

Протокол TCP нарізує з потоку даних *сегменти*.

Одиницю даних протоколу UDP часто називають *дейтаграммою* (або датаграм-мою). Дейтаграмма – це загальна назва для одиниць даних, якими оперують протоколи без встановлення з’єднань. До таких протоколів відноситься і протокол міжмережевої взаємодії IP.

Дейтаграмму протоколу IP називають також *пакетом*.

У стеку TCP/IP прийнято називати *кадрами (фреймами)* одиниці даних протоколів, на основі яких IP-пакети переносяться через підмережі складової мережі. При цьому не має значення, яка назва використовується для цієї одиниці даних в локальній технології.

Складова мережа (internetwork або internet) – це сукупність декількох мереж, званих також підмережами (subnet), які з’єднуються між собою маршрутизаторами. Організація сумісної транспортної служби в складовій мережі називається міжмережевою взаємодією (internetworking).

У функції мережевого рівня входить: передача пакетів між кінцевими вузлами в складових мережах, вибір маршруту, узгодження локальних технологій окремих підмереж.

Маршрут – це послідовність маршрутизаторів, які повинен пройти пакет від відправника до пункту призначення. Задачу вибору маршруту з декількох можливих вирішують маршрутизатори і кінцеві вузли на основі таблиць маршрутизації. Записи в таблицю можуть заноситися уручну адміністратором і автоматично протоколами маршрутизації.

Протоколи маршрутизації (наприклад, RIP або OSPF) слід відрізнити від власне мережевих протоколів (наприклад, IP або IPX). Тоді як перші збирають і передають по мережі чисто службову інформацію про можливі маршрути, другі призначені для передачі призначених для користувача даних.

Мережеві протоколи і протоколи маршрутизації реалізуються у вигляді програмних модулів на кінцевих вузлах-комп'ютерах і на проміжних вузлах-маршрутизаторах.

Маршрутизатор є складним багатофункціональним пристроєм, в задачі якого входить: побудова таблиці маршрутизації, визначення на її основі маршруту, буферизація, фрагментація і фільтрація поступаючих пакетів, підтримка мережевих інтерфейсів. Функції маршрутизаторів можуть виконувати як спеціалізовані пристрої, так і універсальні комп'ютери з відповідним програмним забезпеченням.

Для алгоритмів маршрутизації характерні однокроковий і багатокроковий підходи. Однокрокові алгоритми діляться на алгоритми фіксованої, простої і адаптивної маршрутизації. Адаптивні протоколи маршрутизації є найпоширенішими і в свою чергу можуть бути засновані на дистанційно-векторних алгоритмах і алгоритмах стану зв'язків.

Найбільше поширення для побудови складових мереж останнім часом набув стек TCP/IP. Стек TCP/IP має 4 рівні: прикладний, основний, рівень міжмережевої взаємодії і рівень мережевих інтерфейсів. Відповідність рівнів стека TCP/IP рівням моделі OSI достатньо умовна.

Прикладний рівень об'єднує всі служби, що надаються системою призначеним для користувача додаткам: традиційні мережеві служби типу telnet, FTP, TFTP, DNS, SNMP, а також порівняльно нові, такі, наприклад, як протокол передачі гіпертекстової інформації HTTP.

На основному рівні стека TCP/IP, званому також транспортним, функціонують протоколи TCP і UDP. Протокол управління передачею TCP вирішує задачу забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами. Дейтаграммний протокол UDP використовується як економічний засіб зв'язку рівня міжмережевої взаємодії з прикладним рівнем.

Рівень міжмережевої взаємодії реалізує концепцію комутації пакетів в режимі без встановлення з'єднань. Основними протоколами цього рівня є дейтаграммний протокол IP і протоколи маршрутизації (RIP, OSPF, BGP і ін.). Допоміжну роль виконують протокол міжмережевих управляючих повідомлень ICMP, протокол групового управління IGMP і протокол дозволу адрес ARP.

Тема 17. Адресація у IP-мережах

17.1. Типи адрес стеку TCP/IP.

17.2. Класи IP адрес

17.3. Особливості IP адреси

17.1. Типи адрес стеку TCP/IP.

В стеку TCP/IP використовують 3 типи адрес:

1 Апаратні

2 IP адреси або мережеві

3 Символьні доменні імена

Під локальним адресом розуміють такий тип адрес, який використовує засоби базової технології для доставки даних в мережах. В різних малих мережах допускаються різні мережеві технології і різні стеки протоколів, тому при створенні стека TCP/IP враховують різні типи локальних адрес. Якщо під мережею інтранет є локальна мережа, то лок-й адрес = MAC адресу. MAC адрес призначається мережним адаптерам і інтерфейсам маршрутизаторів. MAC адреси призначені виробниками є унікальні так як керуються централізовано. Для всіх функціональних технологій локальних мереж MAC адрес має 6 байт. Однак протокол IP має може працювати і над протоколами вищого рівня виконання: IPX, X 25. В цих випадках локальними адресами для протоколів IP будуть адреси IPX і X 25. деякі комп-ри в локальних мережах можуть мати декілька локальних адрес. Деякі мережеві пристрої взагалі без локального адреса: глобальні порти маршрутизаторів, модемні порти тощо.

IP адреса представляє собою основний тип адрес, на базі якої мережений рівень передає пакети між мережами. Ці адреси складаються з 4 байт. IP адрес призначається амін-ом мережі під час конфігурування комп-ів і

маршрутизаторів. Ір адрес складається з 2-ох частин: № мержі та № вузла. № мережі призначається організацією ІнтерНІС, № вузла призначається довільним чином. Маршрутизатор вказують в кілька мереж одночасно, тому кожен порт маршрутизатора має свій власний ІР адрес. Таким чином маршрутизатор вказує не на конкретний комп-р, маршрутизатор... а на одне мережеве з'єднання.

Доменні імена будуються в ІР мережах по ієрархічній ознаці. Складові повного символного мені в ІР мережах розділяються «.» і перераховуються в наступному порядку : просте імя і вузла, імя групи вузлів, імя вищої групи і так до імені домена самого вищого рівня. Приклад: ua, ru, com, de... між доменним імям і ІР адресом вузла немає ніякого алгоритмічного відношення тому тре використовувати додаткові таблиці або служби, щоб вузол в мережі визначався як по доменній адресі так і по ІР. В ТСПІР використовують служби DNS, які встановлюють цю відповідність на основі створеної амін-ми мереженої таблиці відповідності.

17.2. Класи ІР адрес

ІР адреса має 4 байти і записується у вигляді 4 чисел в 10-й формі і розділяються «.» Насправді стек ТСПІР працює з 2-ми представленнями цих чисел. Значення цих біт також визначають до якого класу відносяться той чи інший ІР адрес.

Якщо в 2-й системі самий старший біт = 0, то мережа --- класу А, № мережі=1 байту, решта № вузла. Мережі класу А мають № від 1...126. № 0 не використовують, а 127 для спец-них цілей. Мереж класу А небагато, але кількість вузлів може досягати 2^{24} .

Якщо перші байти = 10 то мережа класу В. по 16 біт під номер. Таких мереж 16384, в кожній по 65536 вузлів. Якщо адрес = 110, то мережа класу С. тоді № мережі=24 бітам, № вузла – 8 біт. Мережі цього класу максимально поширені, № вузла – 256.

Якщо 1110 то мережа класу D, такі адреси є груповими адресами(multicast). Якщо в адресі призначення вказано адрес класу D, то такий пакет мають отримати всі вузли, що мають даний адрес.

Якщо 11110, то мережа відноситься до класу E. адреси цього класу зареєстровані для використання у майбутньому.

- 0 A: 1.0.0.0 – 126.0.0.0 --- 2^{24} хостів
- 10 B: 128.0.0.0 – 191.255.0.0 --- 2^{16} хостів
- 110 C: 192.0.0.0 – 223.255.255.0 --- 2^8 хостів
- 1110 D: 224.0.0.0 – 239.255.255.255 --- 0 хостів
- 11110 E: 240.0.0.0 – 247.255.255.255

17.3. Особливості IP адреси

Якщо IP складається лише з 0000 то вона асоціюється з вузлом який відправив пакет. Якщо в полі мережі стоять 0000 то вважається, що вузол призначення знаходиться в тій же мережі що і відправник. Коли всі 2-ві розряди IP адреси складаються з 1-ць, то цей пакет відправляється всім хто знаходиться з ним в мережі. Це називається лімітед бродкаст. Якщо в полі № одержувача тільки 1-ці, то цей пакет розсилається всім вузлам визначеної мережі. При адресації необхідно враховувати всі обмеження які вносять особові IP адреси. Якщо 1-й байт = 127 то така адреса використ-ся для тестування програм та процесів в середині машини. При відправленні на адреси які складаються з 1, пакет піде на всі компютери в мережі, якщо на IP то тільки в даному вузлі. Існує форма групової IP організації – мультикаст. Ці групи дозволяють передавати пакети які входять в певну групу з номером який вказано в полі адрес. Вузли самостійно ідентифікують до якої групи належать, один вузол може належати до декількох груп. Члени групи мультикаст можуть знаходитись в одній групі. Для таких груп розроблений спец протокол IGMP. Він працює за принципом: вузол повідомляє про ініціативу створення нової групи і маршрутизатор розсилає інформацію про

створення нової групи в мережах підключених до цих портів. Вузли які хочуть приєднатись до щойно створеної групи повідомляють по це своїм локальним маршрутизаторам а ті передають дану інф-ю хосту ініціатору. Основне призначення мультикаст це відправлення за схемою 1 : N . такий протокол дозволяє економно передавати інформацію одночасно багатьом вузлам. Щоб маршрутизатори могли розпізнавати інформацію по групах, мультикаст використовує протокол MOSPF.

Існують спец адреси для локального використання класів IP адресації:

Клас А : 10.0.0.0

В : 172.16.0.0 до 172.31.0.0

С : 192.168.0.0 по 192.168.255.0

Використання масок

З метою встановлення гнучкого з'єднання номеру мережі і вузла використовують мережева маска. Маска це число яке дублюється і містить 1 там де це відноситься до мережі. Оскільки номер мережі це неперервна послідовність розрядів то і маска повинна включати неперервну послідовність одиниць.

Поділ по класам:

А FF.0.0.0

В FF.FF.0.0

С FF.FF.FF.0

Приклад: 185.23.44.206 коли вона доповнена маскою 255.255.255.0 то мережа стане класу С а не В.

Механізм масок широко представлений в IP адресації. За допомогою масок можна адмініструвати мережу, а також об'єднувати у одну мережу за допомогою префіксів.

Порядок розподілу IP адрес

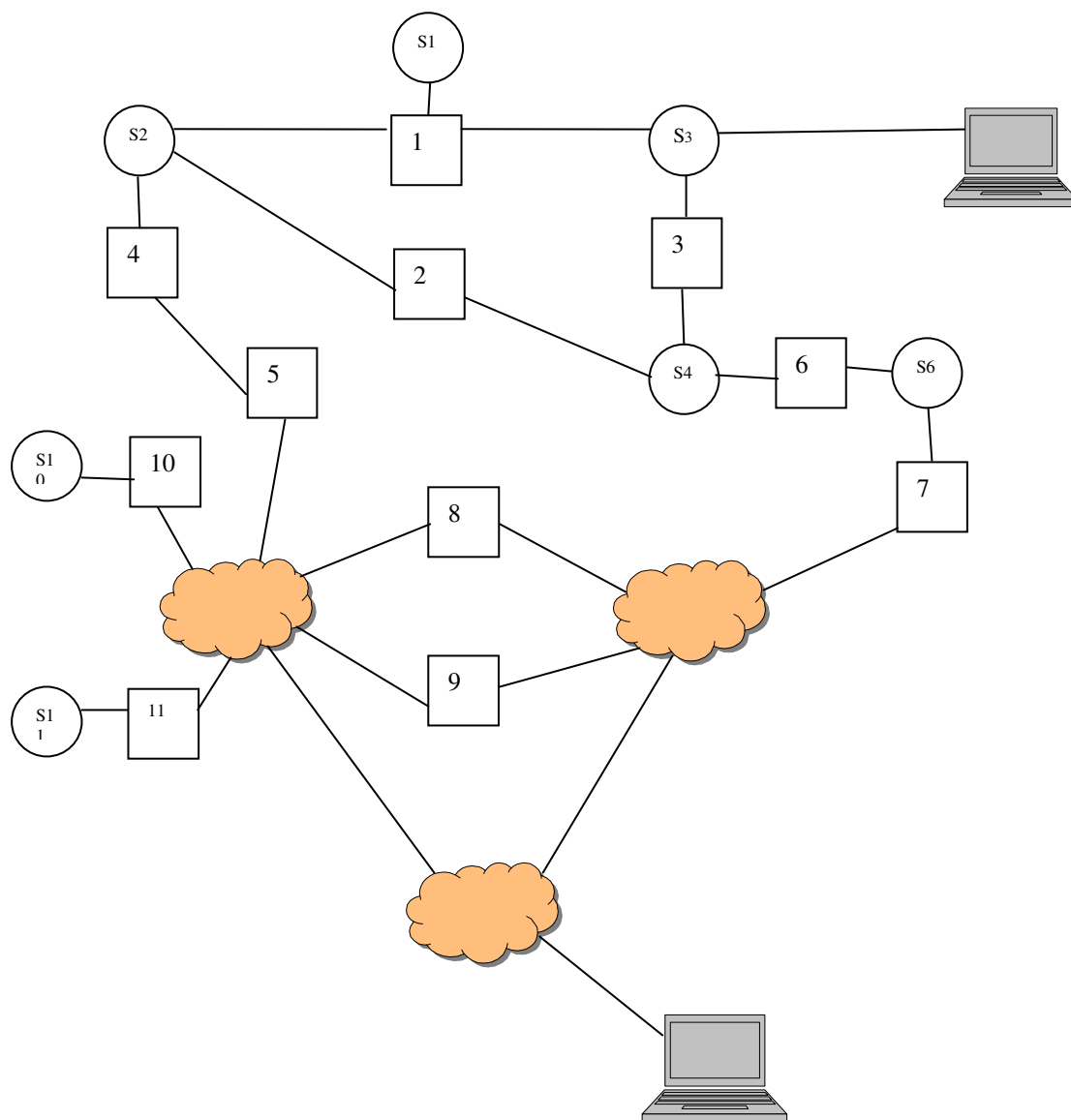
Номери мереж коли вони є частиною мережі є централізовані. Неефективне використання існуючих IP призвело до їх дефіциту. Якщо потрібно сполучити 2 мережі, то використовують з'єднання point to point, і для виродженої мережі яка утворена каналом зв'язку двох портів необхідно виділяти окремий № мережі. Для вирішення проблеми дефіциту розроблено IP V6 який використовує 16 байтні адреси.

В CIDR відсутній розподіл адрес на класи. Це дозволяє адресувати стільки адрес скільки потрібно. Ще один протокол NAT реалізує переадресацію із внутрішніх у зовнішні адреси.

Тема 18. Протоколи маршрутизації в IP-мережах.

Принципи маршрутизації

Важливим завданням мереженого рівня є маршрутизація – пересилання пакетів між кінцевими вузлами у мережі

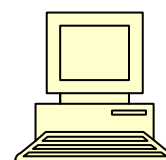
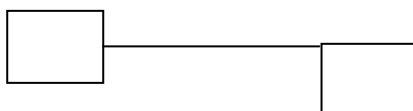


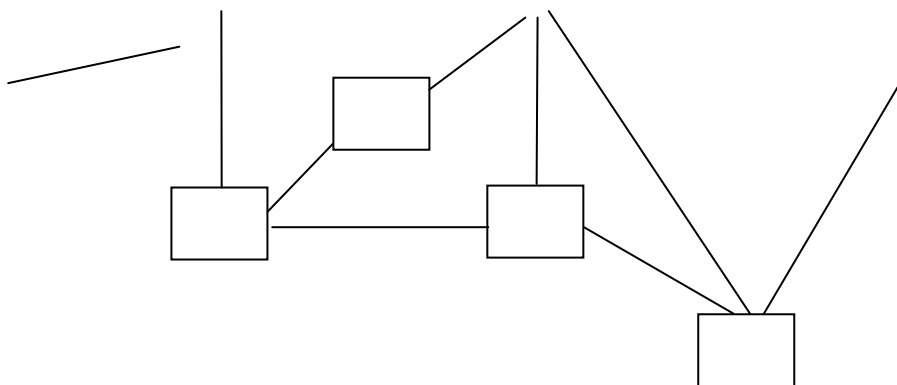
Адреса мережі до	Куди	Кількість	Через	що
------------------	------	-----------	-------	----

якої пересилають	пересилають	переходів	проходить
192.168.1.0 192.168.2.0	192.168.5.4	2 1	192.168.5.5
192.168.10.0	192.168.7.10	1	192.168.7.5

Протоколи маршрутизації

Задачею вибору маршруту з деяких можливих вирішують як маршрутизатори так і кінцеві вузли, якщо вони підключені до двох або більше вузлів. Маршрут обирається на основі мережі та на основі критерію вибору маршруту, такий критерій може бути на основі затримок проходження маршруту або на основі пропускнуої здатності каналів усього маршруту. Також може бути простий критерій на основі кількості пропускнух маршрутів. Маршрутизатори мають таблицю маршрутизації на основі якої вибирають маршрут. В таблиці маршрутизації маршрути перераховані зверху вниз і по першому маршруту який задовольняє пункт призначення пакет відправляється.





4. Протоколи маршрутизації

Задача маршрутизації виконується на основі аналізу табл. маршрутизації розташованих як на маршрутизаторах так і на вузлах. Основна робота по створенню табл. маршрутизації виконується автомат-но, але дозволяє ручне корегування чи доповнення таблиць. Для автомат-ї побудови таблиці маршрутизації (ТМ) використовують спец. службові протоколи які називаються протоколи маршрутизації(ПМ). ПМ наприклад RIP, OSPF, NLSP необхідно відрізнити від протоколів мережі IP і IPX не дивлячись на те , що ті і ті виконують функції мереженого рівня OSI. Але протоколи збирають і передають по мережі лише службову інформацію, в той час коли МП призначені для короткочасних даних. ПМ використовують мережеві протоколи як транспортні засоби. при обміні маршрутизованою інформацією пакети протоколу поміщається в поле даних транспортного рівня або мереженого. А тому з точки зору вкладеності пакетів їх можна відносити до більш високих рівнів системи OSI. Для прийняття рішення маршрутизатором про рух пакетів, маршрутизатори звертаються до адресних таблиць подібно з адресними таблицями мостів та комутаторів. Але замість MAC адресів в ТМ вказується № мережі.

Мости будують таблицю пасивно, тобто спостерігаючи за рухом кадрів на портах в той час як маршрутизатори обмінюються спец службовими пакетами, повідомляючи сусідні маршрутизатори про всі мережі з якими вони мають зв'язок.

ПМ можуть бути побудовані на основі різних алгоритмів які відрізняються способами побудови таблиць маршрутизації, вибору маршруту та інше. В прикладі наведеному вище вибирається тільки найближчий маршрутизатор у відповідності такий алгоритм називається одно кроковим. Крім одно крокових існують також алгоритми «від джерела» (Source routing). Одно крокові алгоритми в залежності від способу формування діляться на 3 групи:

- 1) З фіксованою або статичною маршрутизацією;
- 2) Простої маршрутизації;
- 3) Адаптивної або динамічної маршрутизації;

В алг-х фіксованої маршрутизації всі записи в ТМ є статичними. Таблиця як правило створюється в процесі завантаження системи з можливістю її редагувати вручну.

Розрізняють 1_но і багато маршрутні таблиці. В багато маршрутних таблицях задається правило вибору маршрутів. Найчастіше перший шлях є основним всі решта резервними. В класі алг-мів простої маршрутизації таблиці маршрутизації взагалі немає.

Виділяють 3 типи простої маршрутизації:

- 1) Випадкова (коли прибувший пакет відправляється в перший ліпшим напрямом крім обратного)
- 2) Лавинна маршрутизація – пакет відправляється в усіх напрямках крім того з якого він прийшов.

- 3) За попереднім досвідом – коли вибір маршруту здійснюється по таблиці, а таблиця будується по принципу моста. Шляхом аналізу адресних полів пакету які з'являються на вхідних портах.

Адаптивна маршрутизація або динамічна, є найбільш поширений алгоритм. Дозволяє автоматично змінювати таблиці маршрутизації після змін конфігурації мережі. Такі протоколи дозволяють збирати інформацію про топологію зв'язків в мережі для всіх маршрутизаторів, оперативно обробляючи всі зміни в конфігурації зв'язків.

Динамічна маршрутизація ділиться на два типи:

- 1) Дистанційно-векторні алгоритми;
- 2) Алгоритми стану зв'язків;

В алгоритмах дистанційно-векторного типу кожен маршрутизатор періодично розсилає пакет із ширококомовними пакетами по мережі, вектор компонентами якого є віддалі від даного маршрутизатора до всіх відомих мереж. Під віддалю розуміють число НОР-ів, але можлива і інша метрика, яка буде враховувати час проходження пакетів по мережі між сусідніми маршрутизаторами. При отриманні нового вектора наш маршрутизатор доповнює свою таблицю і збільшує вектор на відповідне число. Дистанційно векторні алгоритми добре працюють на невеликих мережах так як вони інтенсивно обмінюються ширококомовним трафіком, але деколи в них трапляється кільце.

Прикладами є RIP IP, RIP IPX.

Тема 19. Основні характеристики маршрутизаторів і модульного концентраторів.

Алгоритм стану зв'язків, динамічна маршрутизація.

Забезпечують кожен маршрутизатор інформацією достатньою для побудови точного графу зв'язків мережі.

Всі маршрутизатори працюють на основі однакових графів, що робить процес маршрутизації більш стійкішим до змін конфігурації. Широкомовна розсилка використовується лише при зміні зв'язків. Вершинами графа є як маршрутизатори так і об'єднані ними мережі. Інформація, що розповсюджується по мережі складається з опису зв'язків різних типів: Маршрутизатор- Маршрутизатор, Маршрутизатор-Мережа. Щоб зрозуміти в якому стані, лінія зв'язку підключена до портів маршрутизатора він періодично обмінюється портовими пактами HELLO із своїми сусідами. Цей службовий трафік засмічує мережу але не так як RIP пакети, так як пакети HELLO мають малий розмір.

Приклади: IS-IS, Steka OSI, OSPF, NLSP, Stekanovel.

П

Пр

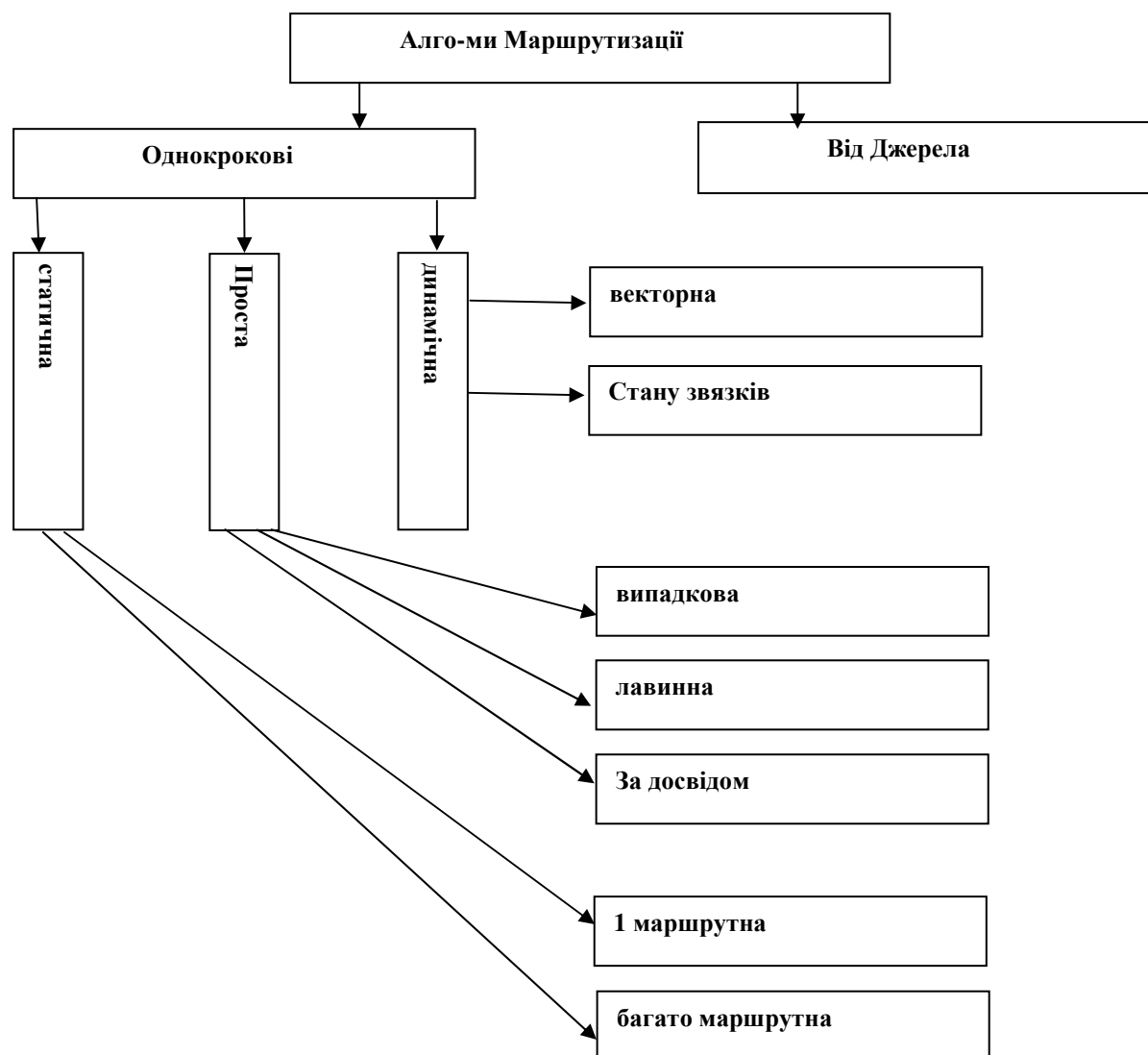
С

Т IP, IPX, Net level (RIP, OSPF, NCSP)

М

К

Ф



Функції маршрутизаторів

Основна функція маршрутизатора це читання заголовків пакетів мережених протоколів IP, IPX, Tencet, Apple talk, що приймаються на кожному порту і прийняття рішень про маршрут пакета НП основі його мережевого адреса який включає як правило № мережі та № вузла. Ф-ї маршрутизатора розбивають на 3 групи у відповідності до моделі OSI:

Рівень інтерфейсів ;

Рівень мереженого протоколу;

Рівень протоколів маршрутизації;

На нижньому рівні маршрутизатори як будь-які пристрої, що підключені до мережі, забезпечує фіз-й інтерфейс для взаємодії з середовищем передачі включає узгодження рівнів

Електричних сигналів лінійне та логічне кодування. Також маршрутизатор оснащений відповідним типом роз'ємну. В різних моделях маршрутизаторів часто передбачаються різні набори фіз. Інтерфейсів, що представляють собою комбінацію портів для підєднання до глобальних та локальних мереж. З кожним інтерфейсом для під єднання лок. мережі зв'язаний відповідний протокол каналного рівня.

В свою чергу інтерфейси для під єднання до глобальних мереж частіше всього визначають тільки деякий стандарт фіз. Рівня над яким можуть різні протоколи каналного рівня. Так наприклад глобальний порт може працювати інтерфейс V.35 над яким можуть працювати наступні маршрутизатори LAP B(X 25) , LAP F(Frame Relay), LAP D(ISDN). Інтерфейсом маршрутизатора використовують повний набір функцій фіз. I кан-го рівня по передачі кадру, включаючи отримання доступу до середовища, форм-ня бітових сигналів, прийом кадру, підрахунок його контрольної суми, передача поля кадру вищому рівню. Маршрутизатор

повинен підтримувати всі протоколи каналного та фізичного рівня які використовуються в кожній з мереж до яких він приєднаний.

Кадри які поступають на порти маршрутизатора після обробки відповідними протоколами каналного та фізичного рівня, та позбавляються від заголовків каналного рівня. Отримані з поля даних кадру пакети передаються модулю мереженого протоколу.

Рівень мереженого протоколу

Мережевий протокол в свою чергу протокол в свою чергу вилучає з пакету заголовки мереженого рівня і аналізує зміст його полів. Перш за все перевіряється контрольна сума, якщо пакет прийшов пошкодженим, то він відкидається. Потім перевіряється поле часу життя пакету, якщо час життя пакета перевищує задане значення, цей пакет відкидається. На цьому етапі також вноситься корекція у деякі поля пакету, наприклад збільшується на 1 час життя пакету.

Також на мереженому рівні викорис-ся функція фільтрації трафіку. Маршрутизатор маючи більш високий інтелект ніж мости та комутатори може обробляти більш складніші правила фільтрації. Так пакет мережевого рівня, що знаходяться, що знаходиться в полі даних кадру для моста і компаратора представляються не структурною двійковою послідовністю, а маршрутизатори здатні робити аналіз деяких полів пакету. Маршрутизатори як правило можуть аналізувати структуру пов-нь транспортного рівня, тому фільтри можуть не пускати в мережу пов-ня визначених прикладних служб. Якщо в маршрутизаторі інтенсивність поступання пакетів більша ніж його здатність обробити то пакети можуть створювати чергу. Тип черги залежить від програмного забезпечення маршрутизатора.

Типи черг

- 1) FIFO

- 2) Випадкове попереднє виявлення. Обслуговування іде по правилу FIFO але при дуже великій черзі знову поступаючи пакети відкидаються.
- 3) Різні варіанти пріоритетного обслуговування

Перед тим як подати мереж-й адрес наступного комп-ра на каналний рівень, необхідно перетворити його в локальний адрес тої технології яка використовується в мережі, до якої підєднаний наступний маршрутизатор. Для цього мережений протокол звертається до протоколу узгодження адрес. Протоколи цього типу встановлюють відпов-сть між мережами і лок-ми адресами або на основі попередньо заданих таблиць, та шляхом розсилання широкомовних запитів. Такі таблиці будуються окремо для кожного інтерф-су. Протоколи узгодження адрес займають проміжне положення між мереженими і каналними рівнями.

З мереж-го рівня передається каналному на основі номера порта, здійснюється комутація з відповідним інтер-сом маршрутизатора, засобами якого відбувається упаковка пакету в кадр певного формату. В поле адреси заголовка поміщається локальний адрес наступного маршрутизатора. Готовий кадр відправляється в мережу.

Рівень протоколів маршрутизації.

Мережеві протоколи активно використовують таблицю маршрутизації, але не займаються її підтримкою вмісту. Ці функції виконують протоколи маршрутизації. На основі цих протоколів маршрутизатори обмежуються інф-ю про топологію мережі та аналізують отримані повідомлення, визначаючи найкращий маршрут по тим чи іншим критеріям. Результат аналізу поміщається в табл-ю маршрутизації. Крім перерахованих фун-й, маршрутизатори можуть виконувати операції зв'язані з фрагментацією пакетів.

Тема 20. Глобальні зв'язки на основі цифрових виділених ліній.

20.1. Технологія PDH.

20.2. Технологія SONET/SDN.

20.3. Застосування цифрових первинних мереж.

[1, 3-5, 7,10, 12, 13, 20]

20.1. Технологія PDH

Цифрові виділені лінії утворюються шляхом постійної комутації в первинних мережах, побудованих на базі комутаційної апаратури, яка працює на принципах поділу каналу в часі – TDM. Існують два покоління технологій цифрових первинних мереж – технологія плезіохронної («плезіо» означає «майже», тобто майже синхронної) цифрової ієрархії (Plesiochronic Digital Hierarchy, PDH) і більш пізня технологія – синхронна цифрова ієрархія (Synchronous Digital Hierarchy, SDH). В США технології SDH відповідає стандарт SONET.

Цифрова апаратура мультиплексування і комутації була розроблена наприкінці 60-х років компанією AT&T для вирішення проблеми зв'язку великих комутаторів телефонних мереж між собою. Канали з частотним ущільненням, які застосовуються для цього на ділянках АТС-АТС, вичерпали свої можливості по організації високошвидкісного багатоканального зв'язку по одному кабелю. У технології FDM для одночасної передачі даних 12 чи 60 абонентських каналів використовувалася вита пара, а для підвищення швидкості зв'язку приходилося прокладати кабелі з великою кількістю пар проводів чи більш дорогі коаксіальні кабелі. Крім того, метод частотного ущільнення високо чуттєвий до різного роду перешкод, що завжди присутні в територіальних кабелях, та й високочастотна несуча мови сама створює перешкоди в прийомній апаратурі, будучи погано відфільтрована.

Для рішення цієї задачі була розроблена апаратура T1, яка дозволяла в цифровому вигляді мультиплексувати, передавати і комутувати (на постійній основі) дані 24 абонентів. Так як абоненти як і раніше користувалися звичайними телефонними апаратами, то передача голосу йшла в аналоговій формі, то мультиплексори T1 самі здійснювали оцифрування голосу з частотою 8000 Гц і кодували голос з допомогою імпульсно-кодової модуляції (Pulse Code Modulation, PCM). У результаті кожен абонентський канал утворював цифровий потік даних 64 Кбіт/с. Для з'єднання магістральних АТС канали T1 являли собою занадто слабкі засоби мультиплексування, тому в технології була реалізована ідея створення каналів з ієрархією швидкостей. Чотири канали типу T1 поєднуються в канал наступного рівня цифрової ієрархії – T2, що передає дані зі швидкістю 6,312 Мбіт/с, а сім каналів T2 утворюють при об'єднанні канал T3, який передає дані зі швидкістю 44,736 Мбіт/с. Апаратура T1, T2 і T3 може взаємодіяти між собою, утворюючи ієрархічну мережу з магістральними і периферійними каналами трьох рівнів швидкостей.

Із середини 70-х років виділені канали, побудовані на апаратурі T1, стали здаватися телефонними компаніями в оренду на комерційних умовах, переставши бути внутрішньою технологією цих компаній. Мережі T1, а також більш швидкісні мережі T2 і T3 дозволяють передавати не тільки голос, але і будь-які дані, представлені в цифровій формі, – комп'ютерні дані, телевізійне зображення, факси і т.п.

Технологія цифрової ієрархії була пізніше стандартизована ССІТТ. При цьому в неї були внесені деякі зміни, що призвело до несумісності американської і міжнародної версій цифрових мереж. Американська версія поширена сьогодні крім США також у Канаді і Японії (з деякими розбіжностями), а в Європі застосовується міжнародний стандарт. Аналогом каналів T в міжнародному стандарті є канали типу E1, E2 і E3 з іншими швидкостями – відповідно 2,048 Мбіт/с, 8,488 Мбіт/с і 34,368 Мбіт/с.

Американський варіант технології також був стандартизований ANSI.

Незважаючи на розбіжності американської і міжнародної версій технології цифрової ієрархії, для позначення ієрархії швидкостей прийнято використовувати ті самі позначення – DS_n (Digital Signal n). У табл. 15.1 приводяться значення для всіх введених стандартами рівнів швидкостей обох технологій.

Таблиця 15.1. Ієрархія цифрових швидкостей

Позначення швидкості	Америка			СІТТ (Європа)		
	Кількість голосових каналів	Кількість каналів попереднього рівня	Швидкість, Мбіт/с	Кількість голосових каналів	Кількість каналів попереднього рівня	Швидкість, Мбіт/с
DS-0	1	1	64 Кбіт/с	1	1	64 Кбіт/с
DS-1	24	24	1,544	30	30	2,048
DS-2	96	4	6,312	120	4	8,488
DS-3	672	7	44,736	480	4	34,368
DS-4	4032	6	274,176	1920	4	139,264

На практиці в основному використовуються канали T1/E1 і T3/E3. Мультиплексор T1 забезпечує передачу даних 24-х абонентів зі швидкістю 1,544 Мбіт/с в кадрі, що має досить простий формат. У цьому кадрі послідовно передається по одному байті кожного абонента, а після 24-х байт вставляється один біт синхронізації. Спочатку пристрої T1 (які дали ім'я також і всій технології, що працює на швидкості 1,544 Мбіт/с) працювали тільки на внутрішніх тактових генераторах, і кожен кадр за допомогою бітів синхронізації міг передаватися асинхронно. Апаратура T1, а також більш швидкісна апаратура T2 і T3 за довгі роки існування з нею відбулися значні зміни. Сьогодні мультиплексори і комутатори первинної мережі працюють

на централізованій тактовій частоті, яка розподіляється з однієї точки всієї мережі. Однак принцип формування кадру залишився, тому біти синхронізації в кадрі як і раніше присутні. Сумарна швидкість користувацьких каналів складає $24 \times 64 = 1,536$ Мбіт/с, а ще 8 Кбіт/с додають біти синхронізації.

В апаратурі T1 призначення восьмого біта кожного байта в кадрі різне і залежить від типу переданих даних і покоління апаратури.

При передачі голосу в мережах T1 усі 24 каналу є абонентськими, тому керуюча і контрольна інформація передається восьмим (найменш значущим) бітом вимірів голосу. У ранніх версіях мереж T1 службовим був 8-й біт кожного байта кадру, тому реальна швидкість передачі користувацьких даних складала 56 Кбіт/с (як правило восьмий біт приділявся під такі службові дані, як номер викликуваного телефонного абонента, сигнал зайнятості лінії, сигнал зняття трубки і т.п.). Потім технологія була поліпшена і для службових цілей стали використовувати тільки кожен шостий кадр. Таким чином, у п'ятьох кадрах із шести користувацькі дані представлені всіма вісьма бітами, а в шостому – тільки сімома.

При передачі комп'ютерних даних канал T1 надає для користувацьких даних тільки 23 канали, а 24-й канал приділяється для службових цілей, в основному – для відновлення спотворених кадрів. Для одночасної передачі як голосових, так і комп'ютерних даних використовуються всі 24 канали, причому комп'ютерні дані передаються зі швидкістю 56 Кбіт/с. Техніка використання восьмого біта для службових цілей одержала назву «крадіжки біта» (bit robbing).

При мультиплексуванні 4-х каналів T1 в один канал T2 між кадрами DS-1 до тепер використовується один біт синхронізації, а кадри DS-2 (які складаються з 4-х послідовних кадрів DS-1) розділяються 12 службовими бітами, що призначені не тільки для поділу кадрів, але і для їхньої синхронізації. Відповідно, кадри DS-3 складаються з 7 кадрів DS-2,

розділених службовими бітами.

Міжнародна версія цієї технології описана в стандартах G.700-G.706. Вона більш логічна, тому що не використовує схему «крадіжки біта». Крім того, вона заснована на постійному коефіцієнті кратності швидкості 4 при переході до наступного рівня ієрархії. Замість восьмого біта в каналі E1 на службові цілі приділяються 2 байти з 32. Для голосових каналів чи каналів даних залишається 30 каналів зі швидкістю передачі 64 Кбіт/с кожний.

Користувач може орендувати кілька каналів 64 Кбіт/с (56 Кбіт/с) у каналі T1/E1. Такий канал називається «дробним» (fractional) каналом T1/E1. У цьому випадку користувачу приділяється трохи тайм-слотів роботи мультиплексора.

Фізичний рівень технології PDH підтримує різні види кабелів: виту пару, коаксіальний кабель і волоконно-оптичний кабель. Основним варіантом абонентського доступу до каналів T1/E1 є кабель із двох витих пар з розйомами RJ-48. Дві пари потрібні для організації дуплексного режиму передачі даних зі швидкістю 1,544/2,048 Мбіт/с. Для представлення сигналів використовується: у каналах T1 біполярний потенційний код B8ZS, у каналах E1 – біполярний потенційний код HDB3. Для посилення сигналу на лініях T1 через кожні 1800 м (одна миля) встановлюються регенератори й апаратура контролю лінії.

Коаксіальний кабель завдяки своїй широкій смузі пропускання підтримує канал T2/E2 чи 4 канали T1/E1. Для роботи каналів T3/E3, як правило, використовується або коаксіальний кабель, або волоконно-оптичний кабель, або канали СВЧ.

Фізичний рівень міжнародного варіанта технології визначається стандартом G.703, назвою якого позначається тип інтерфейсу маршрутизатора чи моста, що підключається до каналу E1. Американський варіант інтерфейсу називається T1.

Необхідно відмітити що як американський, так і міжнародний варіанти

технології PDH володіють декількома недоліками.

Одним з основних недоліків є складність операцій мультиплексування і демультиплексування користувацьких даних. Сам термін «плезіо-хронний», що використовується для цієї технології, говорить про причину такого явища – відсутності повної синхронності потоків даних при об'єднанні низькошвидкісних каналів у більш високошвидкісні. Споконвічно асинхронний підхід до передачі кадрів породив вставку біта чи декількох біт синхронізації між кадрами. У результаті для витягнення користувацьких даних з об'єданого каналу необхідно повністю мультиплексувати кадри цього об'єданого каналу.

Іншим істотним недоліком технології PDH є відсутність вбудованих процедур контролю і керування мережею. Службові біти дають мало інформації про стан каналу, не дозволяють його конфігурувати і т.п. Немає в технології і процедур підтримки відказостійкості, які дуже корисні для первинних мереж, на основі яких будуються відповідальні міжміські і міжнародні мережі. У сучасних мережах керуванню приділяється велика увага, причому вважається, що керуючі процедури бажано вбудовувати до основного протоколу передачі даних мережі.

Третій недолік полягає в занадто низьких по сучасних поняттях швидкостях ієрархії PDH. Волоконно-оптичні кабелі дозволяють передавати дані зі швидкостями в декілька гігабіт в секунду по одному волокну, що забезпечує консолідацію в одному кабелі десятків тисяч користувацьких каналів, але цю властивість технологія PDH не реалізовує – її ієрархія швидкостей закінчується рівнем 139 Мбіт/с.

Усі названі вище недоліки усунуті в новій технології первинних цифрових мереж, що одержала назву синхронної цифрової ієрархії – Synchronous Digital Hierarchy, SDH.

20.2. Технологія SONET/SDH.

Технологія синхронної цифрової ієрархії (Synchronous Digital Hierarchy, SDH) спочатку була розроблена компанією Bellcore за назвою «Синхронні оптичні мережі» – Synchronous Optical NETs, SONET. Перший варіант стандарту з'явився в 1984 році. Потім ця технологія була стандартизована комітетом T1 ANSI. Міжнародна стандартизація технології проходила під егідою Європейського інституту телекомунікаційних стандартів (ETSI) і ССІТТ разом з ANSI і провідними телекомунікаційними компаніями Америки, Європи і Японії. Основною метою розробників міжнародного стандарту було створення такої технології, що дозволяла б передавати трафік всіх існуючих цифрових каналів (як американських T1 – T3, так і європейських E1 – E3) у рамках високошвидкісної магістральної мережі на волоконно-оптичних кабелях і забезпечила б ієрархію швидкостей, яка продовжила ієрархію технології PDH, до швидкості в декілька гігабіт в секунду.

У результаті тривалої роботи вдалося розробити міжнародний стандарт Synchronous Digital Hierarchy, SDH (специфікації G.707-G.709), а також доробити стандарти SONET таким чином, що апаратура і стеки SDH і SONET стали сумісними і можуть мультиплексувати вхідні потоки практично будь-якого стандарту PDH – як американського, так і європейського. У термінології і початковій швидкості технології SDH і SONET залишилися розбіжності, але це не заважає сумісності апаратурі різних виробників, а технологія SONET/ SDH фактично стала вважатися єдиною технологією. У Росії застосовуються стандарти й адаптована термінологія SDH.

Ієрархія швидкостей при обміні даними між апаратурою SONET/SDH, що підтримує технологія SONET/SDH, представлена в табл. 15.2.

Таблиця 15.2. Швидкості технології SONET/SDH

SDN	SONET	Швидкість
-----	-------	-----------

–	S15-1, OC-1	51,840 Мбіт/с
STM-1	STS-3, OC-3	155,520 Мбіт/с
STM-3	STS-9, OC-9	466,560 Мбіт/с
STM-4	STS-12, OC-12	622,080 Мбіт/с
STM-6	STS-18, OC-18	933,120 Мбіт/с
STM-8	STS-24, OC-24	1,244 Гбіт/с
STM-12	STS-36, OC-36	1,866 Гбіт/с
STM-16	STS-48, OC-48	2,488 Гбіт/с

У стандарті SDH всі рівні швидкостей (і, відповідно, формати кадрів для цих рівнів) мають загальну назву: STM-n – Synchronous Transport Module level n. У технології SONET існують два позначення для рівнів швидкостей: STS-n – Synchronous Transport Signal level n, вживане при передачі даних електричним сигналом, і OC-n – Optical Carrier level n, вживане при передачі даних світловим променем по волоконно-оптичному кабелі. Формати кадрів STS і OC ідентичні.

Як видно з таблиці 15.2, стандарт SONET починається зі швидкості 51,84 Мбіт/с, а стандарт SDH – зі швидкості 155,52 Мбіт/с, рівної потроєної початкової швидкості SONET. Міжнародний стандарт визначив початкову швидкість ієрархії в 155,52 Мбіт/с, щоб зберігалася гнучкість і спадковість технології SDH з технологією PDH – у цьому випадку канал SDH може передавати дані рівня DS-4, швидкість яких дорівнює 139,264 Мбіт/с. Будь-яка швидкість технології SONET/ SDH кратна швидкості STS-1. Деяка надмірність швидкості 155,52 Мбіт/с для передачі даних рівня DS-4 пояснюється великими накладними витратами на службові заголовки кадрів SONET/SDH. Кадри даних технологій SONET і SDH, які називаються також циклами, по форматах співпадають, відповідно починаючи з загального рівня STS-3/STM-1. Ці кадри мають дуже велику надмірність, тому що передають велику кількість службової інформації, що потрібна для:

- забезпечення гнучкої схеми мультиплексування потоків даних різних швидкостей, що дозволяють вставляти (add) і витягати (drop) користувацьку інформацію будь-якого рівня швидкості, не демультимплексуючи весь потік;
- забезпечення відмовостійкості мережі;
- підтримки операцій контролю і керування на рівні протоколу мережі;
- синхронізації кадрів у випадку невеликого відхилення частот двох мереж, що сполучаються.

Стек протоколів і основні структурні елементи мережі SONET/SDH показані на рис.15.1.

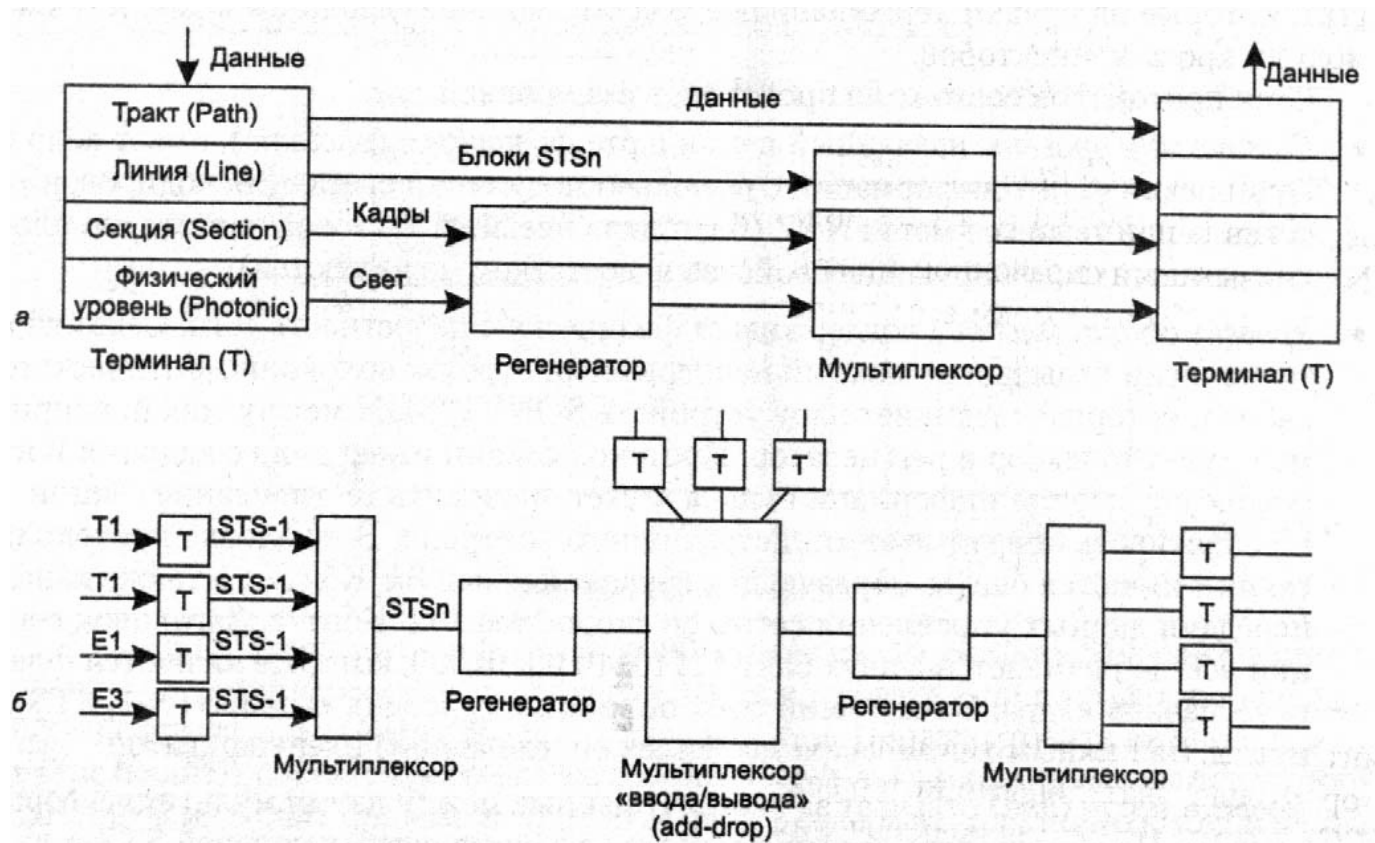


Рис.15.1. Стек протоколів і структура мережі SONET/SDH.

Нижче перераховані пристрої, що можуть входити в мережу технології SONET/SDH.

- Термінальні пристрої (Terminal, T), які називаються також сервісними адаптерами (Service Adapter, SA), приймають користувацькі дані від

низькошвидкісних каналів технології PDH (типу T1/E1 чи T3/E3) і перетворюють їх у кадри STS-n. (Далі аббревіатура STS-n використовується як загальне позначення для кадрів SONET/SDH.)

- Мультиплексори (Multiplexers) приймають дані від термінальних пристроїв і мультиплексують потоки кадрів різних швидкостей STS-n у кадри більш високої ієрархії STS-m.

- Мультиплексори “вводу-виводу” (Add-Drop Multiplexers) можуть приймати і передавати транзитом потік визначеної швидкості STS-n, вставляючи чи видаляючи «на ходу», без повного демультимплексування, користувачькі дані, прийняті з низькошвидкісних входів.

- Цифрові кросс-конектори (Digital Cross-Connect, DCC), які називаються також апаратурою оперативного переключення (АОП), призначені для мультиплексування і постійної комутації високошвидкісних потоків STS-n різного рівня між собою (на рис.15.1 не показані). Кросс-конектор являє собою різновид мультиплексора, основне призначення якого – комутація високошвидкісних потоків даних, можливо, різної швидкості. Кросс-конектори утворюють магістраль мережі SONET/SDH.

- Регенератори сигналів, що використовуються для відновлення потужності і форми сигналів, що пройшли значну відстань по кабелі. На практиці іноді складно провести чітку грань між описаними пристроями, тому що багато виробників випускають багатофункціональні пристрої, що включають термінальні модулі, модулі “вводу-виводу”, а також модулі кросс-конекторів.

Стек протоколів

Стек протоколів складається із протоколів 4-х рівнів.

1. Фізичний рівень, який називається у стандарті фотонним (photonic), має справу з кодуванням бітів інформації за допомогою модуляції світла. Для кодування сигналу застосовується метод NRZ (завдяки

зовнішній тактовій частоті його погані самосинхронізуючі властивості недоліком не являються).

2. Рівень секції (section) підтримує фізичну цілісність мережі. Секцією в технології називаються кожен безупинний відрізок волоконно-оптичного кабелю, що з'єднує пари пристроїв SONET/SDH між собою, наприклад мультиплексор і регенератор. Протокол секції має справу з кадрами і на основі службової інформації кадру може проводити тестування секції і підтримувати операції адміністративного контролю. У заголовку протоколу секції є байти, що утворюють звуковий канал 64 Кбіт/с, а також канал передачі даних керування мережею зі швидкістю 192 Кбіт/с. Заголовок секції завжди починається з двох байт 11110110 00101000, які є прапорами початку кадру. Наступний байт визначає рівень кадру: STS-1, STS-2 і т.д. За кожним типом кадру закріплений визначений ідентифікатор.
3. Рівень лінії (Line) відповідає за передачу даних між двома мультиплексорами мережі. Протокол цього рівня працює з кадрами різних рівнів STS-n для виконання різних операцій мультиплексування і демультиплексування, а також вставки і видалення користувацьких даних. Таким чином, лінією називається потік кадрів одного рівня між двома мультиплексорами. Протокол лінії також відповідальний за проведення операцій реконфігурації лінії у випадку відмови якого-небудь її елемента – оптичного волокна, порту чи сусіднього мультиплексора.
4. Рівень тракту (path–шлях) відповідає за доставку даних між двома кінцевими користувачами мережі. Тракт (шлях) – це складене віртуальне з'єднання між користувачами. Протокол тракту повинен прийняти дані, що надходять у користувацькому форматі, наприклад форматі T1, і перетворити їх у синхронні кадри STS-n/STM-m.

Формат кадру STS-1 представлений на рис.15.2. Кадри технології SONET/SDH прийнято представляти у вигляді матриці, яка складається із n рядків і m стовпців. Таке представлення добре відображає структуру кадру зі свого роду підкадрами, які називаються віртуальними контейнерами (Virtual Container, VC – термін SDH) чи віртуальними притоками (Virtual Tributaries, VT – термін SONET). Віртуальні контейнери – це підкадри, що переносять потоки даних, швидкості яких нижчі, ніж початкова швидкість технології SONET/SDH у 51,84 Мбіт/с (наприклад, потік даних T1 зі швидкістю 1,544 Мбіт/с).



Рис.15.2. Формат кадру STS-1.

Кадр STS-1 складається з 9 рядків і 90 стовпців, тобто з 810 байт даних. Між пристроями мережі кадр передається послідовно по байтах – спочатку перший рядок зліва направо, потім другий і т.д. Перші 3 байти кожного рядка являють собою службові заголовки. Перші 3 рядки являють собою заголовок з 9 байт протоколу рівня секції і містять дані, необхідні для контролю і реконфігурації секції. Інші 6 рядків складають заголовок протоколу лінії, що використовується для реконфігурації, контролю і керування лінією. Пристрої

мережі SONET/SDH, що працюють з кадрами, мають достатній буфер для розміщення в ньому всіх байт кадру, які протікають синхронно через пристрій, тому пристрій для аналізу інформації на якийсь час має повний доступ до всіх частин кадру. Таким чином, розміщення службової інформації в несуміжних байтах не представляє складності для обробки кадру.

Ще один стовпець являє собою заголовок протоколу шляху. Він використовується для вказівки місця розташування віртуальних контейнерів усередині кадру, якщо кадр переносить низькошвидкісні дані користувачьких каналів типу T1/E1. Місце розташування віртуальних контейнерів задається не жорстко, а за допомогою системи покажчиків (pointers).

Концепція покажчиків є ключовою у технології SONET/SDH. Покажчик покликаний забезпечити синхронну передачу байт кадрів з асинхронним характером користувачьких даних.

У технології SONET/SDH існує гнучка, але досить складна схема використання поля даних кадрів STS-n. Складність цієї схеми в тому, що потрібно «вкласти» у кадр найбільш раціональним способом мозаїку з віртуальних контейнерів різного рівня. Тому в технології SONET/SDH стандартизовано шість типів віртуальних контейнерів, які добре сполучаються один з одним при створенні кадру STS-n. Існує ряд правил, по яких контейнери кожного виду можуть утворювати групи контейнерів, а також входити до складу контейнерів більш високого рівня.

Відмовостійкість мережі SONET/SDH вбудована в її основні протоколи. Цей механізм називається автоматичним захисним переключенням – Automatic Protection Switching, APS. Існують два способи його роботи. У першому способі захист здійснюється за схемою 1:1. Для кожного робочого волокна (і обслуговуючого його порту) призначається резервне волокно. В другому способі, який називається 1:n, для захисту n волокон призначається тільки одне захисне волокно.

У схемі захисту 1:1 дані передаються як по робочому, так і по резервному волокну. При виявленні помилок приймаючий мультиплексор повідомляє передавальному, яке волокно повинне бути робочим. Звичайно при захисті 1:1 використовується схема двох кілець, схожа на подвійні кільця FDDI (рис. 15.3), але тільки з одночасною передачею даних у протилежних напрямках. При обриві кабелю між двома мультиплексорами відбувається згортання кілець, і, як і в мережах FDDI, із двох кілець утворюється одне робоче.

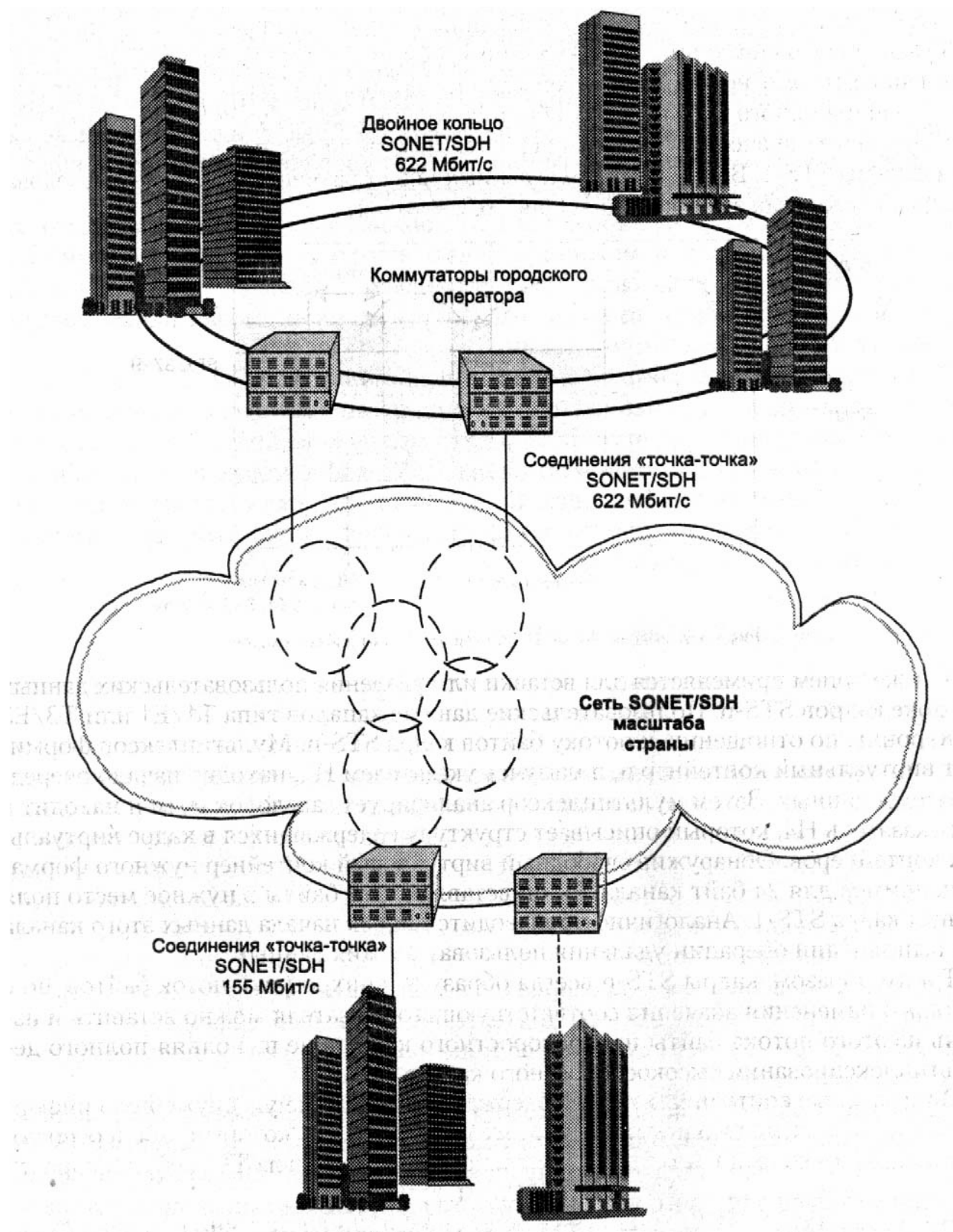


Рис.15.3. Використання подвійних кілець для забезпечення відмовостійкості мережі SONET/SDN.

Застосування схеми резервування 1:1 не обов'язково вимагає кільцевого з'єднання мультиплексорів, можна застосовувати цю схему і при радіальному підключенні пристроїв, але кільцеві структури вирішують проблеми відказостійкості ефективніше – якщо в мережі немає кілець, радіальна схема не зможе нічого зробити при обриві кабелю між пристроями.

Процедури: керування, конфігурування й адміністрування мережі SONET/SDH також вбудовані в протоколи. Службова інформація протоколу дозволяє централізовано і дистанційно конфігурувати шляхи між кінцевими користувачами мережі, змінювати режим комутації потоків у кросс-конекторах, а також збирати докладну статистику про роботу мережі. Існують могутні системи керування мережами SDH, що дозволяють прокладати нові канали простим переміщенням миші за графічною схемою мережі.

20.3. Застосування цифрових первинних мереж.

Мережі SDH і мережі плезіохронної цифрової ієрархії дуже широко використовуються для побудови як публічних, так і корпоративних мереж. Особливо популярні їхні послуги в США, де більшість великих корпоративних мереж побудовано на базі виділених цифрових каналів. Ці канали безпосередньо з'єднують маршрутизатори, розташовувані на границі локальних мереж відділень корпорації.

При оренді виділеного каналу мережний інтегратор завжди впевнений, що між локальними мережами існує канал цілком визначеної пропускної здатності. Це позитивна риса оренди виділених каналів. Однак при відносно невеликій кількості поєднаних локальних мереж пропускна здатність виділених каналів ніколи не використовується на 100%, і це недолік монопольного володіння каналом - підприємство завжди платить не за реальну пропускну здатність. У зв'язку з цією обставиною останнім часом все більшу популярність здобуває служба мереж frame relay, у яких канали

розділяють кілька підприємств.

На основі первинної мережі SDH можна будувати мережі з комутацією пакетів, наприклад frame чи ATM, чи ж мережі з комутацією каналів, наприклад ISDN. Технологія ATM полегшила цю задачу, прийнявши стандарти SDH як основні стандарти фізичного рівня. Тому при існуванні інфраструктури SDH для створення мережі ATM досить з'єднати ATM-комутатори SDH-каналами – жорстко сконфігурованими в мережі .

Телефонні комутатори також можуть використовувати технологію цифрової ієрархії, тому побудова телефонної мережі за допомогою каналів PDH чи SONET/SDH не вимагає багато зусиль. На рис.15.4. показаний приклад співіснування двох мереж – комп'ютерної і телефонної – на основі виділених каналів однієї і тієї ж первинної цифрової мережі.

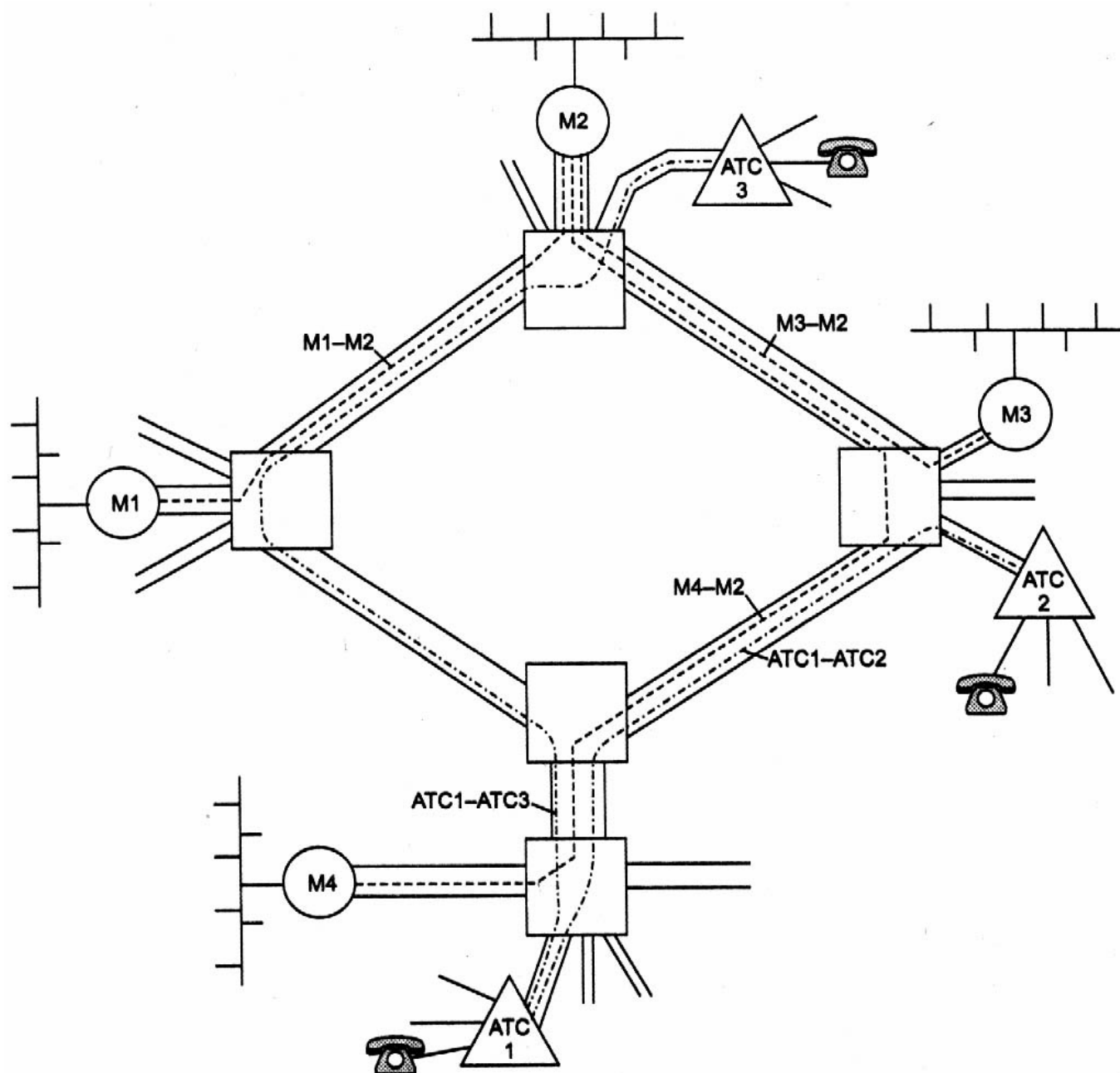


Рис.15.4. Використання цифрової первинної мережі для організації двох накладених мереж – обчислювальної і телефонної.

Технологія SONET/SDH досить економно вирішує задачу мультиплексування і комутації потоків різної швидкості. Тому вона на сьогодні, незважаючи на неможливість динамічного перерозподілу пропускної здатності між абонентськими каналами, є найбільш розповсюдженою технологією створення первинних мереж. Технологія ATM,

хоча і дозволяє динамічно перерозподіляти пропускну здатність каналів, але є значно складнішою, і з вищим рівнем накладних витрат.

Прикладом російських мереж SDH можуть служити мережі «Макомнет», «Метроком» і «Раском», побудовані спільними підприємствами за участю американської компанії Andrew Corporation.

Початок створення мережі «Макомнет» відноситься до 1991 року, коли було створено спільне підприємство, засновниками якого виступили Московський метрополітен і компанія Andrew Corporation.

Транспортним середовищем мережі стали одномодові 32-, 16- і 8-жильні волоконно-оптичні кабелі фірми Pirelli, прокладені в тунелях метрополітену. У метро було покладено більш 350 км кабелю. Постійно розширюючись, сьогодні кабельна система «Макомнет» з урахуванням з'єднань «останньої милі» має довжину вже більш 1000 кілометрів.

Початково в мережі «Макомнет» використовувалося устаткування SDH тільки 1 рівня (155 Мбіт/с) – мультиплексори TN-1X фірми Northern Telecom (Nortel), що володіють функціями комутації 63 каналів E1 по 2 Мбіт/с кожний. З даних мультиплексорів були організовані дві кільцеві топології «Східна» і «Західна» (вони розділили кільцеву лінію метрополітену на два півкільця) і кілька відрізків «точка-точка», що простягнулися до ряду клієнтів, що абонували порівняно великі ємності мережі. Ці кільця утворили магістраль мережі, від якої відгалужувалися зв'язки з абонентами.

Зростаючі день в день потреби замовників змушували створювати нові топології і переконфігурувати старі. Протягом двох років у мережі «Макомнет» задача збільшення пропускну здатності вирішилася за рахунок прокладки нових кабелів і установки нового обладнання, що дозволило потроїти кількість топологій по кільцевій лінії. Число вузлів комутації зросло до сімдесятьох. Але настав момент, коли гостро постало питання про кількість резервних оптичних волокон на деяких ділянках мережі, і з врахуванням прогнозів на розвиток було прийняте рішення про побудову

нового, 4-го рівня SDH (622 Мбіт/с).

Підготовчі роботи по переконфігуруванню і введенню діючих потоків у мережу нового рівня відбувалися без припинення роботи мережі в цілому. В якості устаткування 4 рівня (622 Мбіт/с) були встановлені мультиплексори TN-4X фірми Nortel. Разом з новим устаткуванням була придбана принципово нова високоінтелектуальна система управління (Network Resource Manager). Ця система є надбудовою над системами керування устаткування 1 і 4 рівнів. Вона володіє не тільки усіма функціями контролю устаткування, властивими кожній із систем, але і поруч додаткових можливостей: автоматичної прокладки каналу по мережі, коли оператору потрібно вказати початкову і кінцеву точки; функціями інвентаризації каналів, що забезпечують їхній швидкий пошук у системі, і інших.

Введення всього шести вузлів TN-4X значно збільшив транспортну ємність мережі, а волокна, що вивільнилися, уможливили її подальше нарощування. Спочатку клієнтами «Макомнет» стали телекомунікаційні компанії, які використовують канали «Макомнет» для будівництва власних мереж. Однак згодом коло клієнтів значно розширилося: банки, різні комерційні і державні структури. Устаткування компанії розташоване на території багатьох міських, а також основних міжнародних і міжміських телефонних станцій.

Тема 21. Глобальні мережі з комутацією пакетів

21.1. Комутація пакетів з використанням віртуальних каналів

21.2. Мережі X.25.

21.3. Мережі Frame Relay.

21. Мережі АТМ.

□

21.1. Комутація пакетів з використанням віртуальних каналів.

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

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

Зміст створення віртуального каналу полягає в тому, що маршрутизація пакетів між комутаторами мережі на основі таблиць маршрутизації відбувається тільки один раз – при створенні віртуального каналу (мається на увазі створення віртуального каналу, що комутується, оскільки створення постійного віртуального каналу здійснюється вручну і не вимагає передачі

пакетів по мережі). Після створення віртуального каналу передача пакетів комутаторами відбувається на основі так званих номерів чи ідентифікаторів віртуальних каналів (Virtual Channel Identifier, VCI). Кожному віртуальному каналу присвоюється значення VCI на етапі створення віртуального каналу, причому це значення має не глобальний характер, як адреса абонента, а локальний – кожен комутатор самостійно нумерує новий віртуальний канал. Крім нумерації віртуального каналу, кожен комутатор при створенні цього каналу автоматично настроює так звані таблиці комутації портів – ці таблиці описують, на який порт потрібно передати пакет, що прийшов, якщо він має визначений номер VCI. Так що після прокладки віртуального каналу через мережу комутатори більше не використовують для пакетів цього з'єднання таблицю маршрутизації, а передають пакети на основі номерів VCI невеликої розрядності. Самі таблиці комутації портів також включають звичайно менше записів, чим таблиці маршрутизації, тому що зберігають дані тільки про діючі на даний момент з'єднання, що проходять через даний порт.

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

Режим PVC є особливістю технології маршрутизації пакетів у глобальних мережах, у мережах TCP/IP такого режиму роботи немає. Робота в режимі PVC є найбільш ефективною за критерієм продуктивності мережі. Половину роботи з маршрутизації пакетів адміністратор мережі уже виконав, тому комутатори швидко займаються передаванням кадрів на основі готових

таблиць комутації портів. Постійний віртуальний канал подібний виділеному каналу в тому, що не потрібно встановлювати з'єднання чи роз'єднання. Обмін пакетами по PVC може відбуватися в будь-який момент часу. Відмінність PVC у мережах X.25 від виділеної лінії типу 64 Кбіт/с полягає в тому, що користувач не має ніяких гарантій щодо дійсної пропускної здатності PVC. Використання PVC звичайно набагато дешевше, ніж оренда виділеної лінії, тому що користувач поділяє пропускну здатність мережі з іншими користувачами.

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

Принцип маршрутизації пакетів на основі віртуальних каналів пояснюється на рис.13.1. При встановленні з'єднання між кінцевими вузлами використовується спеціальний тип пакета – запит на встановлення з'єднання (звичай називається Call Request), що містить багаторозрядну (у прикладі семирозрядну) адресу вузла призначення.

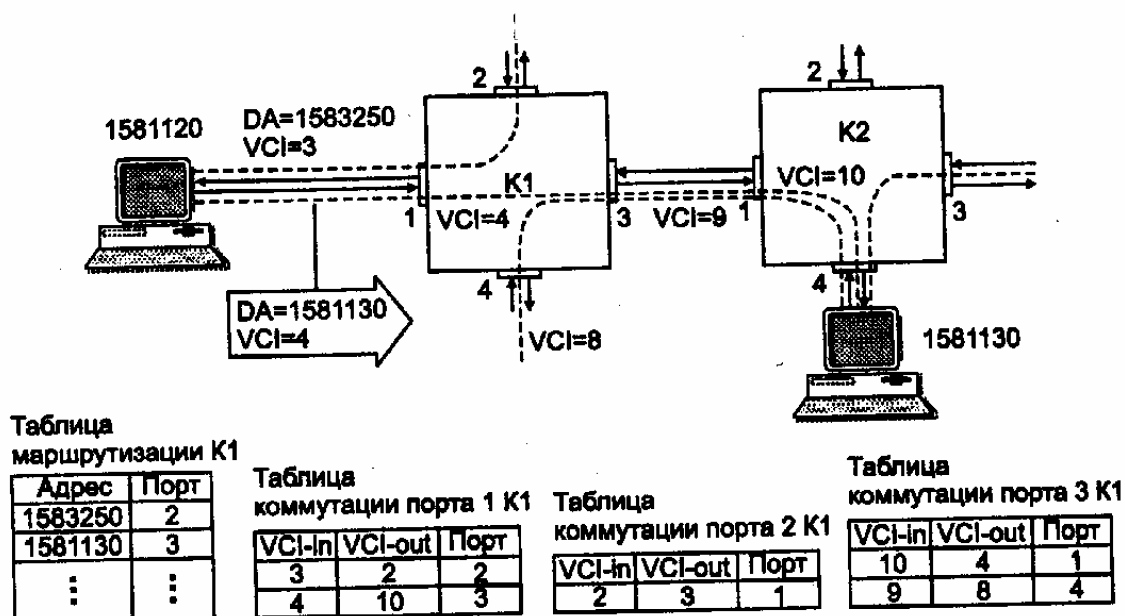


Рис. 13.1. Комутація в мережах з віртуальними з'єднаннями

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

Далі пакет типу Call Request з адресою призначення 1581130, номером VCI 4 і адресою джерела 1581120 відправляється в порт 1 комутатора K1 мережі. Адреса призначення використовується для маршрутизації пакета на основі таблиць маршрутизації, аналогічних таблицям маршрутизації протоколу IP, але з більш простою структурою кожного запису. Запис складається з адреси призначення і номера порту, на який потрібно переслати пакет. Адреса наступного комутатора не потрібна, тому що всі зв'язки між комутаторами є зв'язками типу «крапка-крапка», множинних з'єднань між портами немає. Стандарти глобальних мереж звичайно не описують який-небудь протокол обміну маршрутною інформацією, подібний RIP чи OSPF, що дозволяє комутаторам мережі автоматично будувати таблиці маршрутизації. Тому в таких мережах адміністратор звичайно вручну складає подібну таблицю, вказуючи для забезпечення відказостійкості основний і резервний шляхи для кожної адреси призначення. Виключенням є мережі ATM, для яких розроблений протокол маршрутизації PNNI, заснований на алгоритмі стану зв'язків.

У приведеному прикладі відповідно до таблиці маршрутизації виявилось необхідним передати пакет Call Request з порту 1 на порт 3.

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

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

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

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

Власне кажучи, технологія віртуальних каналів дозволяє реалізувати два режими просування пакетів – стандартний режим маршрутизації пакета на підставі адреси призначення і режим комутації пакетів на підставі номера віртуального каналу. Ці режими застосовуються поетапно, причому перший етап складається в маршрутизації всього одного пакета – запиту на встановлення з'єднання.

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

короткочасних потоків IP-пакетів, тому вона стала досить популярною, хоча і не придбала статус стандарту.

21.2. Мережі X.25

Призначення і структура мереж X.25

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

Стандарт X.25 «Інтерфейс між кінцевим устаткуванням даних і апаратурою передачі даних для терміналів, що працюють у пакетному режимі в мережах передачі даних загального користування» був розроблений комітетом ССІТТ у 1974 році і переглядався кілька разів. Стандарт щонайкраще підходить для передачі трафіка низької інтенсивності, характерного для терміналів, і в меншому ступені відповідає більш високим вимогам трафіка локальних мереж. Як видно з назви, стандарт не описує внутрішній пристрій мережі X.25, а тільки визначає користувальницький інтерфейс із мережею. Взаємодія двох мереж X.25 визначає стандарт X.75.

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

- Наявність у структурі мережі спеціального пристрою – PAD (Packet Assembler Disassembler), призначеного для виконання операції збирання декількох низькошвидкісних потоків байтів від алфавітно-цифрових

терміналів у пакети, які передаються по мережі і направляються комп'ютерах для обробки. Ці пристрої мають також російськомовну назву “Зборщик-разборщик пакетов”, СРП.

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

- Орієнтація на однорідні стеки транспортних протоколів у всіх вузлах мережі – мережний рівень розрахований на роботу тільки з одним протоколом каналного рівня і не може подібно протоколу IP поєднувати різнорідні мережі. Мережа X.25 складається з комутаторів (Switches, S), які називаються також центрами комутації пакетів (ЦКП), розташованих у різних географічних точках і з'єднаних високошвидкісними виділеними каналами (рис.13.2). Виділені канали можуть бути як цифровими, так і аналоговими.

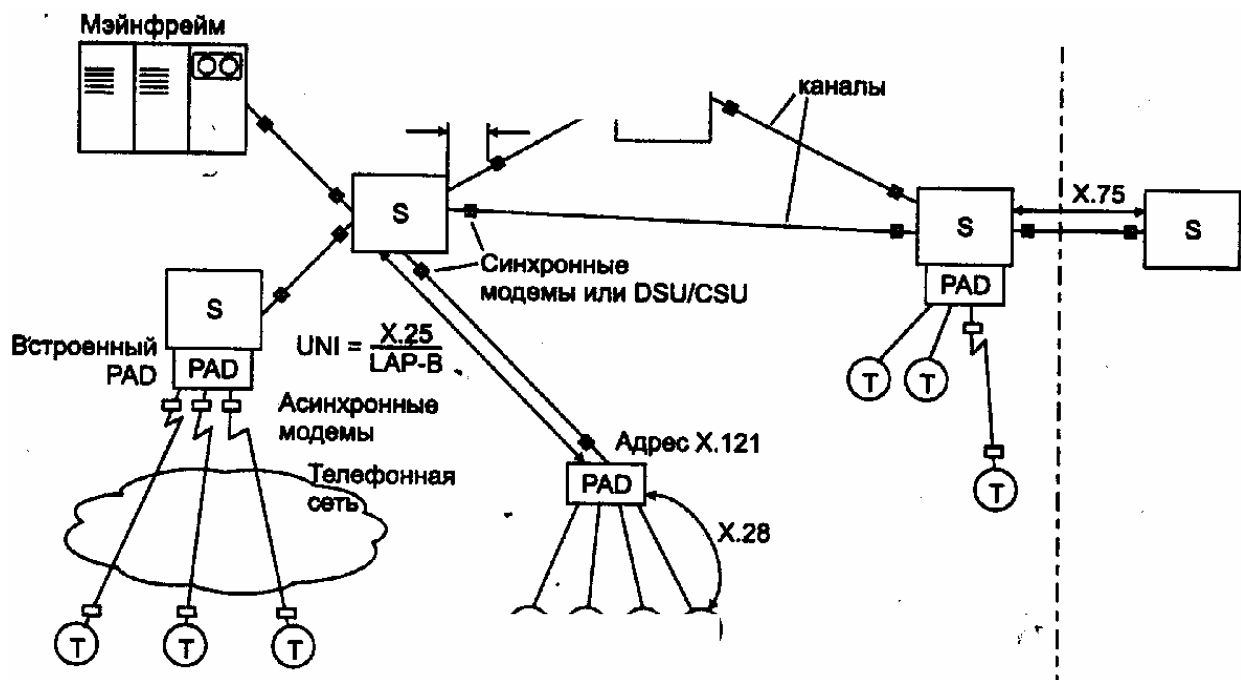


Рис.13.2. Структура мережі X.25

Асинхронні старт-стопні термінали підключаються до мережі через пристрої PAD. Вони можуть бути вбудованими чи віддаленими. Вбудований

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

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

- збирання символів, отриманих від асинхронних терміналів, у пакети;
- розбивання полів даних у пакетах і вивід даних на асинхронні термінали;
- керування процедурами встановлення з'єднання і роз'єднання по мережі X.25 з потрібним комп'ютером;
- передача символів, що включають старт-стопні сигнали і біти перевірки на парність, за вимогою асинхронного терміналу;
- просування пакетів при наявності відповідних умов, таких як заповнення пакета, закінчення часу очікування й ін.

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

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

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

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

Комп'ютери і локальні мережі звичайно підключаються до мережі X.25 безпосередньо через адаптер X.25 чи маршрутизатор, який підтримує на своїх інтерфейсах протоколи X.25. Для керування пристроями PAD у мережі існує протокол X.29, за допомогою якого вузол мережі може керувати і конфігурувати PAD віддалено по мережі. При необхідності передачі даних комп'ютери, які підключені до мережі X.25 безпосередньо, послугами PAD

не користаються, а самостійно встановлюють віртуальні канали в мережі і передають по них дані в пакетах X.25.

Адресація в мережах X.25

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

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

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

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

По стандарті ISO 7498 для нумерації мереж X.25 до адреси у форматі X.121 додається тільки один байт префікса, який несе код 36 (використання в адресі тільки кодів десяткових цифр) чи 37 (використання довільних

двійкових комбінацій). Цей код дозволяє універсальним комутаторам, наприклад комутаторам мережі ISDN, що підтримує також і комутацію пакетів X.25, автоматично розпізнавати тип адреси і правильно виконувати маршрутизацію запиту на встановлення з'єднання.

Стек протоколів мережі X.25

Стандарти мереж X.25 описують 3 рівні протоколів (рис.13.3).

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

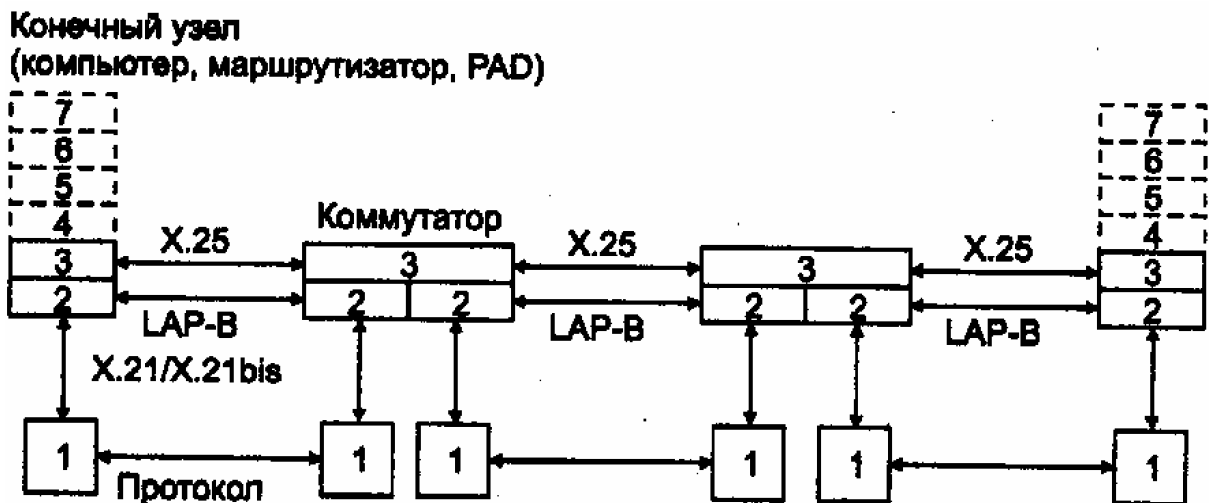


Рис. 13.3. Стек протоколів мережі X.25

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

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

На каналному рівні зазвичай використовується протокол LAR-B. Цей протокол забезпечує збалансований режим роботи, тобто обидва вузли, що беруть участь у з'єднанні, рівноправні. По протоколі LAR-B встановлюється з'єднання між користувальницьким устаткуванням DTE (комп'ютером, IP- чи IPX-маршрутизатором) і комутатором мережі. Хоча стандарт це і не обумовлює, але за протоколом LAR-B можливо також встановлення з'єднання на каналному рівні всередині мережі між безпосередньо зв'язаними комутаторами. Протокол LAR-B майже у всіх відносинах ідентичний протоколу LLC2, крім адресації. Кадр LAR-B містить одне однобайтове адресне поле (а не два – DSAP і SSAP), у якому вказується не адреса служби верхнього рівня, а напрямок передачі кадру – 0x01 для направлення команд від DTE до DCE (у мережу) чи відповідей від DCE до DTE (з мережі) і 0x03 для направлення відповідей від DTE до DCE чи команд від DCE до DTE. Підтримується як нормальний режим (з максимальним вікном у 8 кадрів і однобайтовим полем керування), так і розширений режим (з максимальним вікном у 128 кадрів і двобайтовим полем керування).

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

Після встановлення з'єднання на каналному рівні кінцевий вузол повинен встановити віртуальне з'єднання з іншим кінцевим вузлом мережі.

Для цього він у кадрах LAP-B посилає пакет Call Request протоколу X.25.
 Формат пакета Call Request показаний на рис. 13.4.

Q	D	Modulo	LGN
LCN			
Type = 0x0B			
Длина DA		Длина SA	
Адрес назначения (DA)			

Адрес источника (SA)			

Длина поля услуг (FL)			
Услуги (Facilities)			

Пользовательские данные (User Data)			

Рис.13.4. Формат пакета Call Request

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

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

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

- постійний віртуальний канал;
- віртуальний канал, що комутується тільки для вхідних повідомлень (симплексний);
- віртуальний канал, що комутується, тільки для вихідних повідомлень (симплексний);
- дуплексний віртуальний канал, що комутується.

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

Поле *Номер логічного каналу* (Logical Channel Number, LCN) містить номер віртуального каналу), який призначений вузлом-джерелом (для віртуальних каналів, що комутуються,) чи адміністратором мережі (для постійних віртуальних каналів). Максимальна кількість віртуальних каналів, що проходять через один порт, дорівнює 256.

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

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

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

Поля *Довжина поля послуг* (Facilities length) і *Послуги* (Facilities) потрібні для узгодження додаткових послуг, що надає мережа абоненту. Наприклад, послуга «Ідентифікатор користувача мережі» дозволяє задати ідентифікатор користувача (відмінний від його мережної адреси), на підставі якого можуть оплачуватися рахунки за користування мережею. Користувач за допомогою послуги «Узгодження параметрів керування потоком» може попросити мережу використовувати нестандартні значення параметрів

протоколу – розміра вікна, максимального розміру поля даних пакета і т.п. Протокол X.25 допускає наступні максимальні значення довжини поля даних: 16,32, 64, 128, 256, 512 і 1024 байт. Найкращою є довжина 128 байт.

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

21.3. Мережі Frame Relay

Призначення і загальна характеристика

Мережі frame relay – порівняно нові мережі, що набагато краще підходять для передачі пульсуючого трафіка локальних мереж у порівнянні з мережами X.25, правда, ця перевага виявляється тільки тоді, коли канали зв'язку наближаються по якості до каналів локальних мереж, а для глобальних каналів така якість зазвичай досяжна тільки при використанні волоконо-оптичних кабелів.

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

Особливістю технології frame relay є гарантована підтримка основних показників якості транспортного обслуговування локальних мереж – середньої швидкості передачі даних по віртуальному каналі при допустимих пульсаціях трафіка. Крім технології frame relay гарантії якості обслуговування на сьогодні може надати тільки технологія АТМ, у той час як

інші технології надають необхідну якість обслуговування тільки в режимі «з максимальними зусиллями» (best effort), тобто без гарантій.

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

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

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

Консорціум Frame Relay Forum розробив специфікацію, яка відповідає вимогам базового протоколу frame relay, розробленого TISI і ССІТТ. Однак консорціум розширив базовий протокол, включивши додаткові можливості по керуванню мережею з боку користувача, що дуже важливо при використанні мереж frame relay у складних корпоративних мережах. Ці доповнення до frame relay називають узагальнено Local Management Interface (LMI) – локальний інтерфейс керування.

Стандарти ІТУ-Т звичайно відрізняються високим рівнем складності і наявністю багатьох можливостей, що досить важко втілити на практиці. Специфікації Frame Relay Forum спрощують деякі аспекти стандартів ІТУ-Т чи відкидають деякі можливості. Так, технологія frame switching не знайшла свого відображення в специфікаціях FRF, а процедури створення віртуальних каналів, що комутуються, з'явилися в специфікаціях FRF пізніше, ніж у стандартах ІТУ-Т, і виявилися більш простими.

Стандарти frame relay, як ІТУ-Т/ANSI, так і Frame Relay Forum, визначають два типи віртуальних каналів – постійні (PVC) і що комутуються (SVC). Це відповідає потребам користувачів, тому що для з'єднань, по яких трафік передається майже завжди, більше підходять постійні канали, а для з'єднань, що потрібні тільки кілька годин на місяць, більше підходять канали, що комутуються.

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

Стек протоколів frame relay

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

Крім того, протокол каналного рівня LAR-F у мережах frame relay має два режими роботи – основний (core) і керуючий (control). В основному режимі, що фактично практикується в сьгоднішніх мережах frame relay,

кадри передаються без перетворення і контролю, як і в комутаторах локальних мереж. За рахунок цього мережі frame relay мають дуже високу продуктивність, тому що кадри в комутаторах не піддаються перетворенню, а мережа не передає квитанції підтвердження між комутаторами на кожен користувальницький кадр, як це відбувається в мережі X.25. Пульсації трафіка передаються мережею frame relay досить швидко і без великих затримок.

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

Структура стека (рис.13.5) добре відбиває походження технології frame relay у надрах технології ISDN, тому що мережі frame relay запозичають багато чого зі стека протоколів ISDN, особливо в процедурах установа виртуального каналу, що комутується.

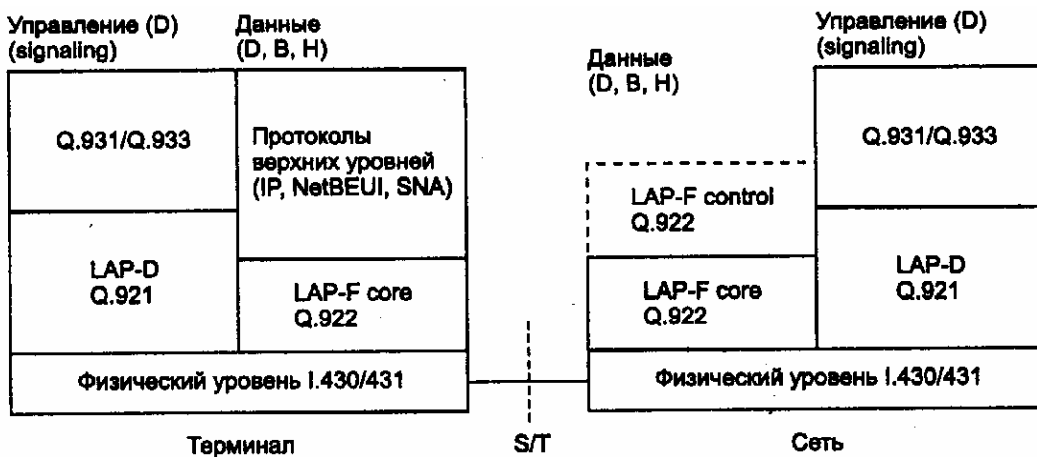


Рис. 13.5. Стек протоколів frame relay

Основу технології складає протокол LAP-F core, який є дуже спрощеною версією протоколу LAP-D. Протокол LAP-F (стандарт Q.922 ITU-T) працює на будь-яких каналах мережі ISDN, а також на каналах типу T1/E1. Термінальне устаткування посилає в мережу кадри LAP-F у будь-який

момент часу, вважаючи що віртуальний канал у мережі комутаторів уже прокладений. При використанні PVC устаткуванню frame relay потрібно підтримувати тільки протокол LAR-F core.

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

Для установки віртуальних каналів, що комутуються, стандарт ІТУ-Т пропонує канал D користувальницького інтерфейсу. На ньому як і раніше працює знайомий протокол LAR-D, що використовується для надійної передачі кадрів у мережах ISDN. Поверх цього протоколу працює протокол Q.931 чи протокол Q.933 (який є спрощенням і модифікацією протоколу Q.931 ISDN), що встановлює віртуальне з'єднання на основі адрес кінцевих абонентів (у стандарті E.164 чи ISO 7498), а також номери віртуального з'єднання, що у технології frame relay називається Data Link Connection Identifier – DLCI.

Після того віртуальний канал, що комутується як, у мережі frame relay установлений за допомогою протоколів LAR-D і Q.931/933, кадри можуть транслюватися по протоколі LAR-F, що комутує їх за допомогою таблиць комутації портів, у яких використовуються локальні значення DLCI. Протокол LAR-F core виконує не усі функції канального рівня в порівнянні з протоколом LAR-D, тому ІТУ-Т зображує його на пів рівня нижче, ніж протокол LAR-D, залишаючи місце для функцій надійної передачі пакетів протоколу LAR-F control.

Через те, що технологія frame relay закінчується на канальному рівні, вона добре погодиться з ідеєю інкапсуляції пакетів єдиного мережного протоколу, наприклад IP, у кадри канального рівня будь-яких мереж, що складають інтермережу. Процедури взаємодії протоколів мережного рівня з технологією frame relay стандартизовані, наприклад, прийнята специфікація

RFC 1490, яка визначає методи інкапсуляції в трафік frame relay трафіка мережних протоколів і протоколів канального рівня локальних мереж і SNA.

Іншою особливістю технології frame relay є відмова від корекції виявлених у кадрах спотворень. Протокол frame relay має на увазі, що кінцеві вузли будуть виявляти і коректувати помилки за рахунок роботи протоколів транспортного чи більш високих рівнів. Це вимагає деякого ступеня інтелектуальності від кінцевого устаткування, що по більшій частині справедливо для сучасних локальних мереж. У цьому відношенні технологія frame relay близька до технологій локальних мереж, таких як Ethernet, Token Ring і FDDI, які також тільки відкидають спотворенні кадри, але самі не займаються їхньою повторною передачею. Структура кадру протоколу LAR-F наведена на рис. 13.6.

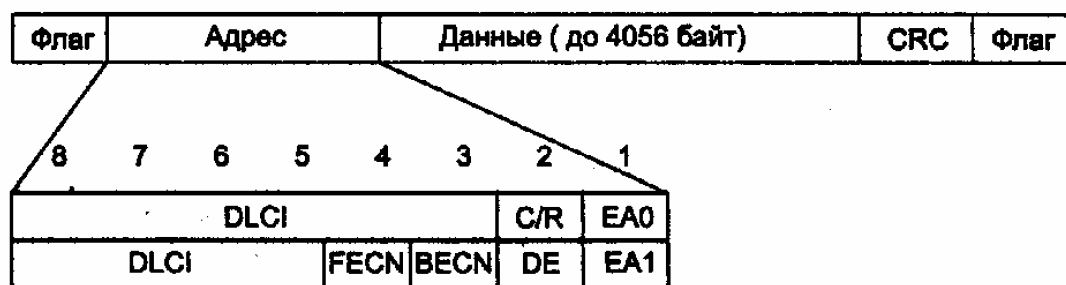


Рис.13.6. Формат кадру IAP-F

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

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

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

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

- 0 – використовується для віртуального каналу локального керування (LMI);
- 1-15 – зарезервовані для подальшого застосування;
- 16-991 – використовуються абонентами для нумерації PVC і SVC;
- 992-1007 – використовуються мережною транспортною службою для внутрімережних з'єднань;
- 1008-1022 – зарезервовані для подальшого застосування;
- 1023 – використовуються для керування каналним рівнем.

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

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

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

21.4. Технологія АТМ

Технологія *асинхронного режиму передачі* (Asynchronous Transfer Mode, АТМ) розроблена як єдиний універсальний транспорт для нового покоління мереж з інтеграцією послуг, які називаються широкополосними мережами ISDN (Broadband-ISDN, B-ISDN).

Технологія АТМ поєднує в собі підходи двох технологій – комутації пакетів і комутації каналів. Від першої вона взяла на озброєння передачу даних у вигляді адресуємих пакетів, а від другої – використання пакетів

невеликого фіксованого розміру, у результаті чого затримки в мережі стають більш передбачуваними. За допомогою технології віртуальних каналів, попереднього замовлення параметрів якості обслуговування каналу і пріоритетного обслуговування віртуальних каналів з різною якістю обслуговування вдається домогтися передачі в одній мережі різних типів трафіка без дискримінації. Хоча мережі ISDN також розроблялися для передачі різних видів трафіка в рамках однієї мережі, голосовий трафік явно був для розробників більш пріоритетним. Технологія ATM із самого початку розроблялася як технологія, здатна обслуговувати усі види трафіка відповідно до їхніх вимог.

Служби верхніх рівнів мережі B-ISDN повинні бути приблизно такими ж, що й у мережі ISDN – це передача факсів, поширення телевізійного зображення, голосова пошта, електронна пошта, різні інтерактивні служби, наприклад проведення відеоконференцій. Високі швидкості технології ATM створюють набагато більше можливостей для служб верхнього рівня, що не могли бути реалізовані мережами ISDN – наприклад, для передачі кольорового телевізійного зображення необхідна смуга пропускання в районі 30 Мбіт/с. Технологія ISDN таку швидкість підтримати не може, а для ATM вона не складає великих проблем.

Розробку стандартів ATM здійснює група організацій за назвою ATM Forum під егідою спеціального комітету IEEE, а також комітети ITU-T і ANSI. ATM – це дуже складна технологія, яка вимагає стандартизації у всіх аспектах, тому, хоча основне ядро стандартів було прийнято в 1993 році, робота зі стандартизації активно продовжується.

Основні принципи технології ATM

Мережа ATM має класичну структуру великої територіальної мережі – кінцеві станції з'єднуються індивідуальними каналами з комутаторами нижнього рівня, які у свою чергу з'єднуються з комутаторами більш високих

рівнів. Комутатори АТМ користаються 20-байтними адресами кінцевих вузлів для маршрутизації трафіка на основі технології віртуальних каналів. Для приватних мереж АТМ визначений протокол маршрутизації PNNI (Private NNI), за допомогою якого комутатори можуть будувати таблиці маршрутизації автоматично. У публічних мережах АТМ таблиці маршрутизації можуть будуватися адміністраторами вручну, як і в мережах X.25, чи можуть підтримуватися протоколом PNNI.

Комутація пакетів відбувається на основі ідентифікатора віртуального каналу (Virtual Channel Identifier, VCI), який призначається з'єднанню при його встановленні і знищується при розриві з'єднання. Адреса кінцевого вузла АТМ, на основі якого прокладається віртуальний канал, має ієрархічну структуру, подібну до номера в телефонній мережі, і використовує префікси, що відповідають кодам країн, міст, мережам постачальників послуг і т.п., що спрощує маршрутизацію запитів встановлення з'єднання, як і при використанні агрегованих IP-адрес відповідно до технології CIDR.

Віртуальні з'єднання можуть бути постійними (Pennant Virtual Circuit, PVC) і такими що комутуються (Switched Virtual Circuit, SVC). Для прискорення комутації у великих мережах використовується поняття віртуального шляху – Virtual Path, що поєднує віртуальні канали, які мають у мережі АТМ загальний маршрут між вихідним і кінцевим вузлами чи загальну частину маршруту між деякими двома комутаторами мережі. Ідентифікатор віртуального шляху (Virtual Path Identifier, VPI) є старшою частиною локальної адреси і являє собою загальний префікс для деякої кількості різних віртуальних каналів. Таким чином, ідея агрегування адрес у технології АТМ застосована на двох рівнях – на рівні адрес кінцевих вузлів (працює на стадії встановлення віртуального каналу) і на рівні номерів віртуальних каналів (працює при передачі даних по наявному віртуальному каналі).

З'єднання кінцевої станції АТМ із комутатором нижнього рівня

визначаються стандартом UNI (User Network Interface). Специфікація UNI визначає структуру пакета, адресацію станцій, обмін керуючою інформацією, рівні протоколу АТМ, способи встановлення віртуального каналу і способи керування трафіком. В даний час прийнята версія UNI 4.0, але найбільш розповсюдженою версією є версія UNI 3.1.

Стандарт АТМ не вводить свої специфікації на реалізацію фізичного рівня. Тут він ґрунтується на технології SDH/SONET, приймаючи її ієрархію швидкостей. Відповідно до цього початкова швидкість доступу користувача мережі – це швидкість OC-3 155 Мбіт/с. Організація АТМ Forum визначила для АТМ не всі ієрархії швидкостей SDH, а тільки швидкості OC-3 і OC-12 (622 Мбіт/с). На швидкості 155 Мбіт/с можна використовувати не тільки волоконо-оптичний кабель, але і неекрановану виту пару категорії 5. На швидкості 622 Мбіт/с допустимо тільки волоконо-оптичний кабель, причому як SMF, так і MMF.

Є і інші фізичні інтерфейси до мереж АТМ, відмінні від SDH/SONET. До них відносяться інтерфейси T1/E1 і T3/E3, розповсюджені в глобальних мережах, і інтерфейси локальних мереж – інтерфейс із кодуванням 4B/5B зі швидкістю 100 Мбіт/с (FDDI) і інтерфейс зі швидкістю 25 Мбіт/с, запропонований компанією IBM і затверджений АТМ Forum. Крім того, для швидкості 155,52 Мбіт/с визначений так званий «cell-based» фізичний рівень, тобто рівень, заснований на ячейках, а не на кадрах SDH/SONET. Цей варіант фізичного рівня не використовує кадри SDH/SONET, а відправляє по каналі зв'язку безпосередньо ячейці формату АТМ, що скорочує накладні витрати на службові дані, але трохи ускладнює задачу синхронізації приймача з передавачем на рівні ячейок.

Усі перераховані вище характеристики технології АТМ не свідчать про те, що це деяка «особлива» технологія, а скоріше представляють її як типову технологію глобальних мереж, засновану на технології віртуальних каналів. Особливості ж технології АТМ лежать в області якісного обслуговування

різнорідного трафіка і підрозуміваються прагненням вирішити задачу сполучення в тих самих каналах зв'язку й у тому самому комунікаційному устаткуванні комп'ютерного і мультимедійного трафіка таким чином, щоб кожен тип трафіка одержав необхідний рівень обслуговування і не розглядався як «другорядний».

Трафік обчислювальних мереж має яскраво виражений асинхронний і пульсуючий характер. Комп'ютер посилає пакети в мережу у випадкові моменти часу, у міру виникнення в цьому необхідності. При цьому інтенсивність посилення пакетів у мережу і їхній розмір можуть змінюватися в широких межах – наприклад, коефіцієнт пульсацій трафіка (відношення максимальної миттєвої інтенсивності трафіка до його середньої інтенсивності) протоколів без встановлення з'єднань може доходити до 200, а протоколів із встановленням з'єднань – до 20. Чутливість комп'ютерного трафіка до втрат даних висока, тому що без втрачених даних обійтися не можна і їх необхідно відновити за рахунок повторної передачі.

Мультимедійний трафік, який передає, наприклад, голос чи зображення, характеризується низьким коефіцієнтом пульсацій, високою чутливістю до затримок передачі даних (віддзеркалюваних на якості відтвореного безупинного сигналу) і низькою чутливістю до втрат даних. Складність сполучення комп'ютерного і мультимедійного трафіка з діаметрально протилежними характеристиками добре видно на рис.13.6.

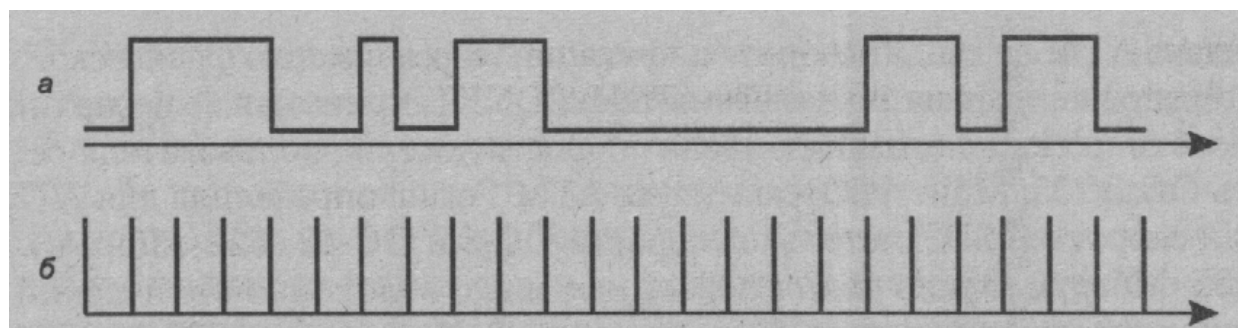


Рис. 13.6. Два типи трафіка: а -комп'ютерний; б -мультимедійний

На можливості сполучення цих двох видів трафіка великий вплив робить розмір комп'ютерних пакетів. Якщо розмір пакета може мінятися в широкому діапазоні (наприклад, від 29 до 4500 байт, як у технології FDDI), то навіть при доданні голосовим пакетам вищого пріоритету обслуговування в комутаторах час очікування комп'ютерного пакета може виявитися неприпустимо високим. Наприклад, пакет у 4500 байт буде передаватися у вихідний порт на швидкості 2 Мбіт/с (максимальна швидкість роботи порту комутатора frame relay) 18 мс. При сполученні трафіка за цей час необхідно через цей же порт передати 144 виміри голосу. Переривати передачу пакета в мережах небажано, тому що при розподіленому характері мережі накладні витрати на оповіщення сусіднього комутатора про переривання пакета, а потім – про поновлення передачі пакета з перерваного місця виявляються занадто великими.

Підхід, реалізований у технології АТМ, складається в передачі будь-якого виду трафіка – комп'ютерного, телефонного чи відео – пакетами фіксованої і дуже маленької довжини в 53 байта. Пакети АТМ називають осередками – cell. Поле даних осередка займає 48 байт, а заголовок – 5 байт.

Щоб пакети містили адреси вузла призначення й у той же час відсоток службової інформації не перевищував розмір поля даних пакета, у технології АТМ застосований стандартний для глобальних обчислювальних мереж прийом – передача осередків відповідно до технології віртуальних каналів з довжиною номера віртуального каналу в 24 біт, що цілком достатньо для обслуговування великої кількості віртуальних з'єднань кожним портом комутатора глобальної (може бути всесвітньої) мережі АТМ.

Розмір осередку АТМ є результатом компромісу між телефоністами і комп'ютерщиками – перші наполягали на розмірі поля даних у 32 байта, а в другі в 64 байта.

Чим менший пакет, тим легше імітувати послуги каналів з постійною бітовою швидкістю, яка характерна для телефонних мереж. Ясно, що при

відмовленні від жорстко синхронізованих тимчасових слотів для кожного каналу ідеальної синхронності домогтися буде неможливо, однак чим менший розмір пакета, тим легше цього досягти.

Для пакета, що складає з 53 байт, при швидкості в 155 Мбіт/с час передачі кадру на вихідний порт складає менш 3 мкс. Так що ця затримка не дуже істотна для трафіка, пакети якого повинні передаватися кожні 125 мкс. Однак на вибір розміру осередку більший вплив зробила не величина очікування передачі осередку, а затримка пакетизації. Затримка пакетизації – це час, протягом якого перший вимір голосу чекає моменту остаточного формування пакета і відправлення його по мережі. При розмірі поля даних у 48 байт один осередок АТМ звичайно переносить 48 вимірів голосу, які виробляються з інтервалом у 125 мкс. Тому перший вимір повинен чекати приблизно 6 мс, перш ніж осередок буде відправлено по мережі. Саме з цієї причини телефоністи були за зменшення розміру осередку, тому що 6 мс – це затримка, близька до межі, за яким починаються порушення якості передачі голосу. При виборі розміру осередку в 32 байта затримка пакетизації склала б 4 мс, що гарантувало б більш якісну передачу голосу. А прагнення комп'ютерних фахівців збільшити поле даних до 64 байт цілком зрозуміло – при цьому підвищується корисна швидкість передачі даних. Надмірність службових даних при використанні 48-байтного поля даних складає 10 %, а при використанні 32-байтного поля даних вона відразу підвищується до 16%.

Вибір для передачі даних будь-якого типу невеликого осередку фіксованого розміру ще не вирішує задачу сполучення різнорідного трафіка в одній мережі, а тільки створює передумови для її рішення. Для повного рішення цієї задачі технологія АТМ залучає і розвиває ідеї замовлення пропускної здатності і якості обслуговування, реалізовані в технології frame relay. Але якщо мережа frame relay споконвічно була призначена для передачі тільки пульсуючого комп'ютерного трафіка (у зв'язку з цим для мереж frame relay так важко дається стандартизація передачі голосу), то розробники

технології АТМ проаналізували всілякі зразки трафіка, створювані різними додатками, і виділили 4 основних класи трафіка, для яких розробили різні механізми резервування і підтримки необхідної якості обслуговування.

Клас трафіка (названий також класом послуг – *service class*) якісно характеризує необхідні послуги по передачі даних через мережу АТМ. Якщо додаток указує мережі, що потрібна, наприклад, передача голосового трафіка, то з цього стає ясно, що особливо важливими для користувача будуть такі показники якості обслуговування, як затримки і варіації затримок осередків, що істотно впливають на якість переданої інформації – голосу чи зображення, а втрата окремого осередку з декількома вимірами не так вже важлива, тому що, наприклад, пристрій що відтворює голос може апроксимувати відсутні виміри і якість постраждає не дуже. Вимоги до синхронності переданих даних дуже важливі для багатьох додатків – не тільки голосу, але і відеозображення, і наявність цих вимог стало першим критерієм для розподілу трафіка на класи.

Іншим важливим параметром трафіка, що істотно впливає на спосіб його передачі через мережу, є величина його пульсацій. Розробники технології АТМ вирішили виділити два різних типи трафіка у відношенні цього параметра – трафік з постійною бітовою швидкістю (*Constant Bit Rate, CBR*) і трафік з перемінною бітовою швидкістю (*Variable Bit Rate, VBR*).

До різних класів були віднесені трафіки, які породженні додатками, що використовують для обміну повідомленнями протоколи з встановленням з'єднань і без встановлення з'єднань. У першому випадку дані передаються самим додатком досить надійно, як це звичайно роблять протоколи з встановленням з'єднання, тому від мережі АТМ високої надійності передачі не вимагається. А в другому випадку додаток працює без встановлення з'єднання і відновленням загублених і перекручених даних не займається, що висуває підвищені вимоги до надійності передачі осередків мережею АТМ.

У результаті було визначено п'ять класів трафіка, що відрізняються

наступними якісними характеристиками:

- наявністю чи відсутністю пульсації трафіка, тобто трафіки CBR чи VBR;
- вимогою до синхронізації даних між передавальною і приймаючою сторонами;
- типом протоколу, що передає свої дані через мережу АТМ, – із встановленням з'єднання чи без встановлення з'єднання (тільки для випадку передачі комп'ютерних даних).

Основні характеристики класів трафіка АТМ приведені в табл. 6.4.

Таблиця 6.4. Класи графіка АТМ

Клас графіка	Характеристика
А	<p>Постійна бітова швидкість – Constant Bit Rate, CBR.</p> <p>Вимагаються тимчасові співвідношення між переданими і даними, що приймаються.</p> <p>З встановленням з'єднання.</p> <p>Приклади: голосовий трафік, трафік телевізійного зображення</p>
В	<p>Перемінна бітова швидкість – Variable Bit Rate, VBR.</p> <p>Вимагаються тимчасові співвідношення між переданими і прийнятими даними.</p> <p>З встановленням з'єднання.</p> <p>Приклади: компресований голос, компресоване відеозображення</p>
С	<p>Перемінна бітова швидкість – Variable Bit Rate, VBR.</p> <p>Не вимагаються тимчасові співвідношення між переданими і прийнятими даними.</p> <p>З встановленням з'єднання.</p> <p>Приклади: трафік комп'ютерних мереж, у яких кінцеві вузли</p>

	працюють по протоколах із встановленням з'єднань: frame relay, X.25, LLC2, TCP
D	<p>Перемінна бітова швидкість – Variable Bit Rate, VBR.</p> <p>Не вимагаються тимчасові співвідношення між переданими і прийнятими даними.</p> <p>Без встановлення з'єднання.</p> <p>Приклади: трафік комп'ютерних мереж, у яких кінцеві вузли працюють по протоколах без встановлення з'єднань (IP, Ethernet DNS, SNMP)</p>
X	Тип трафіка і його параметри визначаються користувачем

Протокол АТМ

Протокол АТМ займає в стеці протоколів АТМ приблизно те ж місце, що протокол IP у стеці TCP/IP чи протокол LAP-F у стеці протоколів технології frame relay. Протокол АТМ займається передачею осередків через комутатори при встановленому і набудованому віртуальному з'єднанні, тобто на підставі готових таблиць комутації портів. Протокол АТМ виконує комутацію по номері віртуального з'єднання, що у технології АТМ розбитий на дві частини – ідентифікатор віртуального шляху (Virtual Path Identifier, VPI) і ідентифікатор віртуального каналу (Virtual Channel Identifier, VCI). Крім цієї основної задачі протокол АТМ виконує ряд функцій по контролі за дотриманням трафік-контракта з боку користувача мережі, маркіруванню осередків-порушників, відкиданню осередків-порушників при перевантаженні мережі, а також керуванню потоком осередків для підвищення продуктивності мережі (природно, при дотриманні умов трафік-контракта для усіх віртуальних з'єднань).

Протокол АТМ працює з осередками наступного формату, представленого на рис. 13.7.

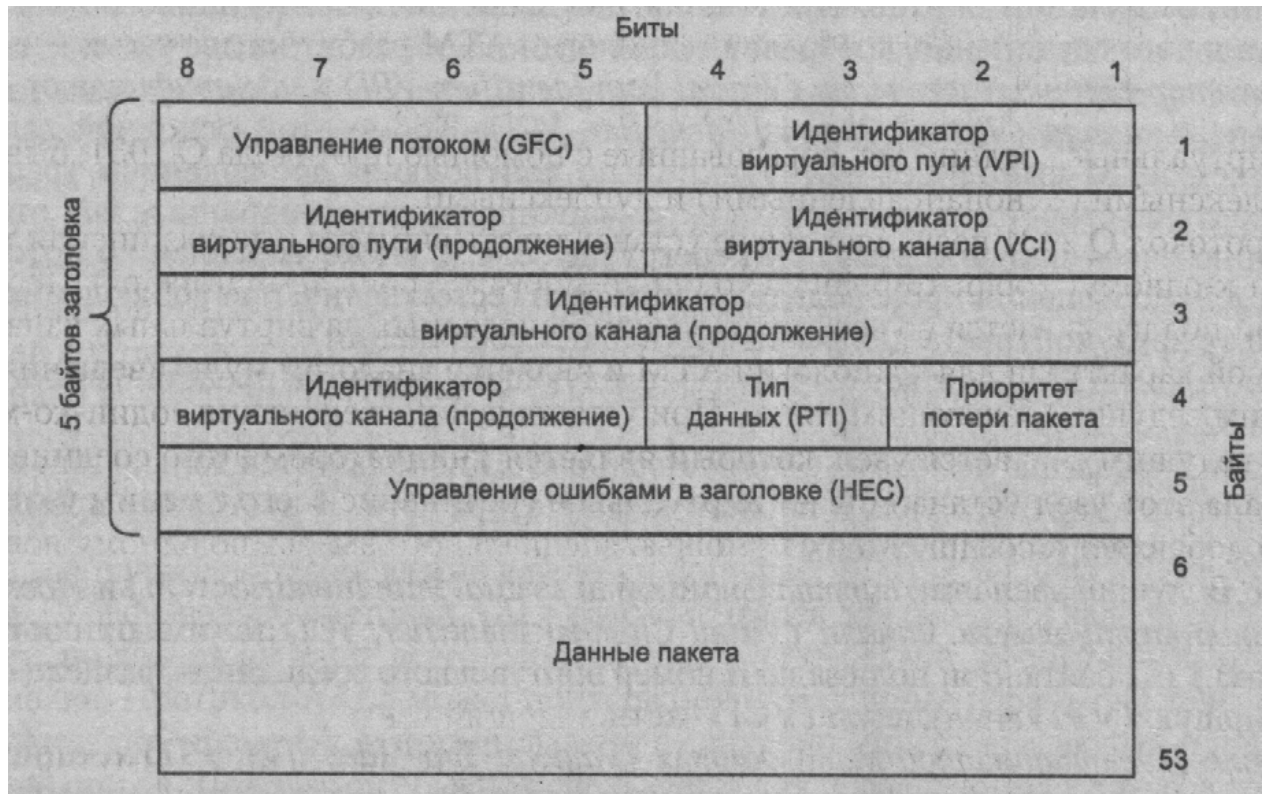


Рис. 13.7. Формат ячейки АТМ.

Поле *Керування потоком* (Generic Flow Control) використовується тільки при взаємодії кінцевого вузла і першого комутатора мережі. В даний час його точні функції не визначені.

Поля *Ідентифікатор віртуального шляху* (Virtual Path Identifier, VPI) і *Ідентифікатор віртуального каналу* (Virtual Channel Identifier, VCI) займають відповідно 1 і 2 байти. Ці поля задають номер віртуального з'єднання, розділений на старшу (VPI) і молодшу (VCI) частини.

Поле *Ідентифікатор типу даних* (Payload Type Identifier, PTI) складається з 3-х біт і задає тип даних, що переносяться осередком, – користувальницькі чи керуючі (наприклад, керуючі встановленням віртуального з'єднання). Крім того, один біт цього поля використовується для вказівки перевантаження в мережі – він називається Explicit Congestion Forward Identifier, EFCI – і відіграє ту ж роль, що біт FECN у технології frame relay, тобто передає інформацію про перевантаження по напрямку потоку

даних.

Поле *Пріоритет утрати кадру* (CeULoss Priority, CLP) відіграє в даній технології ту ж роль, що і поле DE у технології frame relay – у ньому комутатори АТМ відзначають осередки, які порушують угоди про параметри якості обслуговування, щоб видалити їх при перевантаженнях мережі. Таким чином, осередки з CLP=0 є для мережі високопріоритетними, а осередки з CLP=1 – низькопріоритетними.

Поле *Керування помилками в заголовку* (Header Error Control, HEC) містить контрольну суму, обчислену для заголовка осередку. Контрольна сума обчислюється за допомогою технології коригувальних кодів Хеммінга, тому вона дозволяє не тільки виявляти помилки, але і виправляти всі одиночні помилки, а також деякі подвійні. Поле HEC забезпечує не тільки виявлення і виправлення помилок у заголовку, але і знаходження границі початку кадру в потоці байтів кадрів SDH, що є кращим фізичним рівнем технології АТМ, чи ж у потоці біт фізичного рівня, заснованого на осередках.

Тема 22: Протокол TCP

6.1 На теперішній час стек TCP/ IP є самим популярним засобом організації складних мереж. До 96 року лідером був IPX/ SPX компанії NOVEL. Але пізніше картина різко змінилася і TCP/ IP вийшов в лідери. Крім вище згаданих протоколів використ-ся NETBIOS, стек протоколів SNA та APPLE TALK.

В стеку TCP/ IP виділено 4 рівня. Кожен з них несе на собі відповідне навантаження по вирішенні основної задачі – організація надійної і продуктивної роботи складної мережі. Під мережі якої побудовані на основі різних мережених технологій. Основою архітектури мереж на основі стеку TCP/ IP є рівень між мер-ї взаємодії(III) який реалізує концепцію передачі пакетів в режимі без встановлення роз'ємів. Тобто дейтаграмним способом. Саме цей рівень забезпечує перміщення пакетів по мережі використовуючи той маршрут який є найкращим. Цей рівень також називають рівнем Internet.

6.2 Основним протоколом мереж-го рівня є IP, цей протокол проектувався як протокол передачі даних в складних мережах. IP економно використовує пропускну здатність низькоскоросних ліній зв'язку. Так як IP є дейтаграмним, він не гарантує доставку пакету до вузла, але намагається це зробити. До рівня міжмережевої взаємодії відносяться також всі протоколи маршрутизації: RIP, OSP, EGRP, а також протокол міжмережєвих керуючих повідомлень ICMP. Цей протокол призначений для обміну інф-ю про помилки між марш-ми мережі а також вузлами. З допомогою SMP пакетів реалізуються наступні повідомлення:

Неможливість доставки пакету;

Перевищення часу життя або довгий час зборки пакету з фрагментів;

Аномальні величини параметра;

Зміна маршруту пересилки;

Тип обслуговування;

Стан системи;

6.3 Основний рівень. Оскільки на мереж-му рівні не встановлюється зеднання то нема гарантії, що всі пакети доставляться в місце призначення цілі і не ушкоджені, або придуть в тому порядку в якому їх відправляли. Цю задачу забезпечує основний рівень стеку TCP/ IP яий наз-ся трансп-м. На цьому рівні функціонує протокол керув-ння передачею TCPІ – протокол дейтаграм UTP. Протокол TCP забезп-є надійну передачу даних між віддаленими прикладними процесами за рахунок встановлення логічних зв'язків. Цей протокол забезпечує передачу даних у дуплексному режимі. TCP дозволяє без помилок доставити потік байтів з одного комп-ра на інший, при цьому він розділяє їх на сегменти і передає IP протоколу. Після того як пакети будуть доставлені TCP збирає їх у неперервний потік байтів.

Протокол UTP забез-є передачу прикладних пакетів дейтаграмним способом подібно до рівня міжмер-ї взаємодії і викор-є тільки функ-ї зв'язної ланки мультиплексора між мереженим протоколом і службами прикладного рівня.

6.4 Прикладний рівень. Забезпечує всі служби які надаються системою корист-ким прог-мам. За довгий переод формування стек TCPMP накопичив велику кількість протоколів і служб прикладного рівня. Прикладний рівень побудований програмами системи які реалізовані на основі арх.-ри клієнт\сервер на відміну від протоколів іншиз 3 рівнів, протоколи прокладного рівня займаються деталями конкретної програми і не вникають в особливості передчі даних по мережі. Цей рівень постійно росте за рахунок приєднання до старих прикладних протоколів які пройшли багаторічну експлуатацію мереженою службою DNS, SNP, HTTP.

6.5 Рівень мережевих інтерфейсів. Відмінністю архітектури стека TCPMP від багаторівневої організації інших стеків є інтеграція функ-й самого нижнього рівня (мережевих інтерфейсів). Протоколи цього рівня повинні забезпечувати інтеграцію в складних мережах інших мереж. Причому задача

ставиться наступним чином: мережа TCP/IP повинна мати засоби включення в себе іншої мережі, яку би іншу технологію ця мережа не використовувала. Тому для кожної технології яка вкл-на в складну мережу повинні бути розроблені власні інтерфейсні засоби. До них належать протоколи інкапсуляції IP пакетів рівня між мер-ї взаємодії в кадр локальної технології. Наприклад документ RFC 1042 визначає способи інкапс-ї IP пакетів в кадри технології IEEE 802. Для цієї мети повинен викликатися заголовок LLC SNAP. Причому в полі TYPE заголовку SNAP повинен вказуватися код 07.08.00. рівень мережевих інтерф-ів протоколу TCP/IP не регламентується. Але він підтримує всі стандарти фізичного і канального рівнів, як для локал-ї так і глоб-ї мереж.

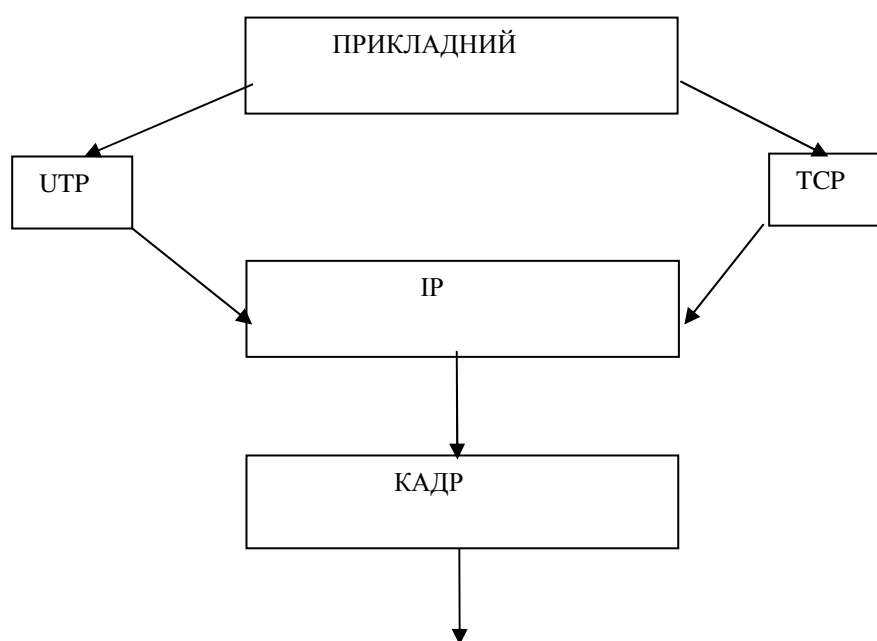
Розглядаючи багаторівневу TCP/IP можна замітити її схожість з OSI. Протоколи прикладного рівня стеку TCP/IP працюють на комп'ютерах які виключають прикладні програми користувачів. Навіть повна заміна мереженого обладнання не впливатиме на роботу програм. Протоколи транспортного рівня вже більше залежать від мережі так як, вони реалізують інтерфейс до рівнів безпосередньо організовують передачу даних. Однак програмні модулі що реалізують протоколи транспортного рівня встановлюють лише на кінці вузлах. Протоколи двох нижніх рівнів є повністю залежні від мережі, а тому прог. Модулі міжмережевого рівня і рівня інтерфейсів встановлюються на всіх вузлах складної мережі і маршрутизаторах.

Потоком називають дані які поступають від ПП на вхід протоколів TCP і UDP . TCP нарізає з потоку даних сегмент, а UDP робить з потоку дейтаграми. Дейтаграми це загальна назва для одиниць даних якими оперують протоколи без встановлення зв'язків. До таких протоколів відносять міжмережеві IP. Дейтаграму IP називають пакет. Стек у TCP/IP прийнято називати кадрами – одиниці даних які передаються за допомогою різних мережевих протоколів.

TCP/IP

OSMISO

№		відповідність	
1	FTP, SMTP, POP3, HTTP, SNMP, SIP	Прикладний, представницький	
2	TCP, UDP	Сеансовий, транспортний	
3	IP, ICMP, RIP, BGP, OSPF	мережевий	
4	FDDI, ARC NET, ATM	канальний транспортний	



МЕРЕЖА

Тема 23. Протоколи прикладного рівня стеку TCP/IP

- 23.1. Протоколи прикладного рівня
- 23.2. Протокол TELNET
- 23.3. Протокол FTP
- 23.4. Протокол SMTP
- 23.5. r-команди
- 23.6. NFS
- 23.7. Протокол SNMP
- 23.8. X-Window
- 23.9. Взаємозалежність протоколів сімейства TCP/IP

23.1. Протоколи прикладного рівня

Чому існують два транспортні протоколи TCP і UDP, а не один з їх? Річ у тому, що вони надають різні послуги прикладним процесам. Більшість прикладних програм користується тільки однією з них. Ви, як програміст, вибираєте той протокол, який найкращим чином відповідає вашим потребам. Якщо вам потрібна надійна доставка, то кращим може бути TCP. Якщо вам потрібна доставка датаграмм, то краще може бути UDP. Якщо вам потрібна ефективна доставка по довгому і ненадійному каналу передачі даних, то краще може підійти протокол TCP. Якщо потрібна ефективність на швидких мережах з короткими з'єднаннями, то кращим може бути протокол UDP. Якщо ваші потреби не потрапляють ні в одну з цих категорій, то вибір транспортного протоколу не ясний. Проте прикладні програми можуть усувати недоліки вибраного протоколу. наприклад, якщо ви вибрали UDP, а вам необхідна надійність, то прикладна програма повинна забезпечити надійність. Якщо ви вибрали TCP, а вам потрібне передавати записи, то прикладна програма повинна вставляти маркери в потік байтів так, щоб можна було розрізнити записи.

Які ж прикладні програми доступні в мережах з TCP/IP?

Загальна їх кількість велика і продовжує постійно збільшуватися. Деякі додатки існують з самого початку розвитку internet. Наприклад, TELNET і FTP. Інші з'явилися недавно: X-Window, SNMP.

Протоколи прикладного рівня орієнтовані на конкретні прикладні задачі. Вони визначають як процедури по організації взаємодії певного типу між прикладними процесами, так і форму уявлення інформації при такій взаємодії. У цьому розділі ми коротко опишемо деякі з прикладних протоколів.

23.2. Протокол TELNET

Протокол TELNET дозволяє обслуговуючій машині розглядати все видалені термінали як стандартні "мережеві віртуальні термінали" рядкового типу, працюючі в коді ASCII, а також забезпечує можливість узгодження складніших функцій (наприклад, локальний або видалений луна-контроль, сторінковий режим, висота і ширина екрану і т.д.) TELNET працює на базі протоколу TCP. А прикладному рівні над TELNET знаходиться або програма підтримки реального терміналу (на стороні користувача), або прикладний процес в машині, що обмірковує, до якого здійснюється доступ з терміналу.

Робота з TELNET схожа на набір телефонного номера. Користувач набирає на клавіатурі щось подібне до

```
telnet delta
```

і одержує на екрані запрошення на вхід в машину delta.

Протокол TELNET існує вже давно. Він добре випробуваний і широко поширений. Створено безліч реалізацій для самих різних операційних систем. Цілком допустимо, щоб процес-клієнт працював, скажімо, під управлінням ОС VAX/VMS, а процес-сервер під ОС UNIX System V.

23.3. Протокол FTP

Протокол FTP (File Transfer Protocol - протокол передачі файлів) поширений також широко як TELNET. Він є одним із старих протоколів сімейства TCP/IP. Також як TELNET він користується транспортними послугами TCP. Існує безліч реалізацій для різних операційних систем, які добре взаємодіють між собою. Користувач FTP може викликати декілька команд, які дозволяють йому подивитися каталог видаленої машини, перейти з одного каталога в інший, а також скопіювати один або декілька файлів.

23.4. Протокол SMTP

Протокол SMTP (Simple Mail Transfer Protocol - простий протокол передачі пошти) підтримує передачу повідомлень (електронної пошти) між довільними вузлами мережі internet. Маючи механізми проміжного зберігання пошти і механізми підвищення надійності доставки, протокол SMTP допускає використання різних транспортних служб. Він може працювати навіть в мережах, що не використовують протоколи сімейства TCP/IP. Протокол SMTP забезпечує як групування повідомлень на адресу одного одержувача, так і розмноження декількох копій повідомлення для передачі на різні адреси. Пекло модулем SMTP мається в своєму розпорядженні поштова служба конкретних обчислювальних систем.

23.5. r-команди

Існує ціла серія "r-команд" (від remote - видалений), які вперше з'явилися в ОС UNIX. Вони є аналогами звичних команд UNIX, але призначені для роботи з видаленими машинами. априклад, команда rcp є аналогом команди cp і призначена для копіювання файлів між машинами. Для передачі файлу на вузол delta достатньо ввести

```
rcp file.c delta:
```


Для виконання команди "cc file.c" на машині delta можна використовувати команду rsh:

```
rsh delta cc file.c
```

Для організації входу у видалену систему призначена команда rlogin:

```
rlogin delta
```

Команди r-серії використовуються головним чином в системах, що працюють під управлінням ОС UNIX. Існують також реалізації для MS-DOS. Команди позбавляють користувача від необхідності набирати паролі при вході у видалену систему і істотно полегшують роботу.

23.6. NFS

Мережева файлова система NFS (Network File System) вперше була розроблена компанією Sun Microsystems Inc. NFS використовує транспортні послуги UDP і дозволяє вмонтовувати в єдине ціле файлові системи кількох машин з ОС UNIX. Бездисккові робочі станції дістають доступ до дискам файл-серверу так, як-будто це їх локальні диски.

NFS значно збільшує навантаження на мережу. Якщо в мережі використовуються повільні лінії зв'язку, то від NFS мало толку. Проте, якщо пропускна здатність мережі дозволяє NFS нормально працювати, то користувачі одержують великі переваги. Оскільки сервер і клієнт NFS реалізуються у ядрі ОС, всі звичні мережеві програми дістають можливість працювати з видаленими файлами, розташованими на підвмонтованих NFS-дисках, точно також як з локальними файлами.

23.7. Протокол SNMP

Протокол SNMP (Simple Network Management Protocol - простий протокол управління мережею) працює на базі UDP і призначений для використання мережевими управляючими станціями. Він дозволяє управляючим станціям збирати інформацію про положення справ в мережі internet. Протокол визначає формат даних, їх обробка і інтерпретація залишаються на розсуд управляючих станцій або менеджера мережі.

23.8. X-Window

Система X-Window використовує протокол X-Window, який працює на базі TCP, для багатовіконного відображення графіки і тексту на растрових дисплеях робочих станцій. X-Window - це набагато більше, ніж просте утиліти для малювання вікон; це ціла філософія людино-машинного взаємодії.

23.9. Взаємозалежність протоколів сімейства TCP/IP

На малюнку представлена схема взаємозв'язків між протоколами сімейства TCP/IP.

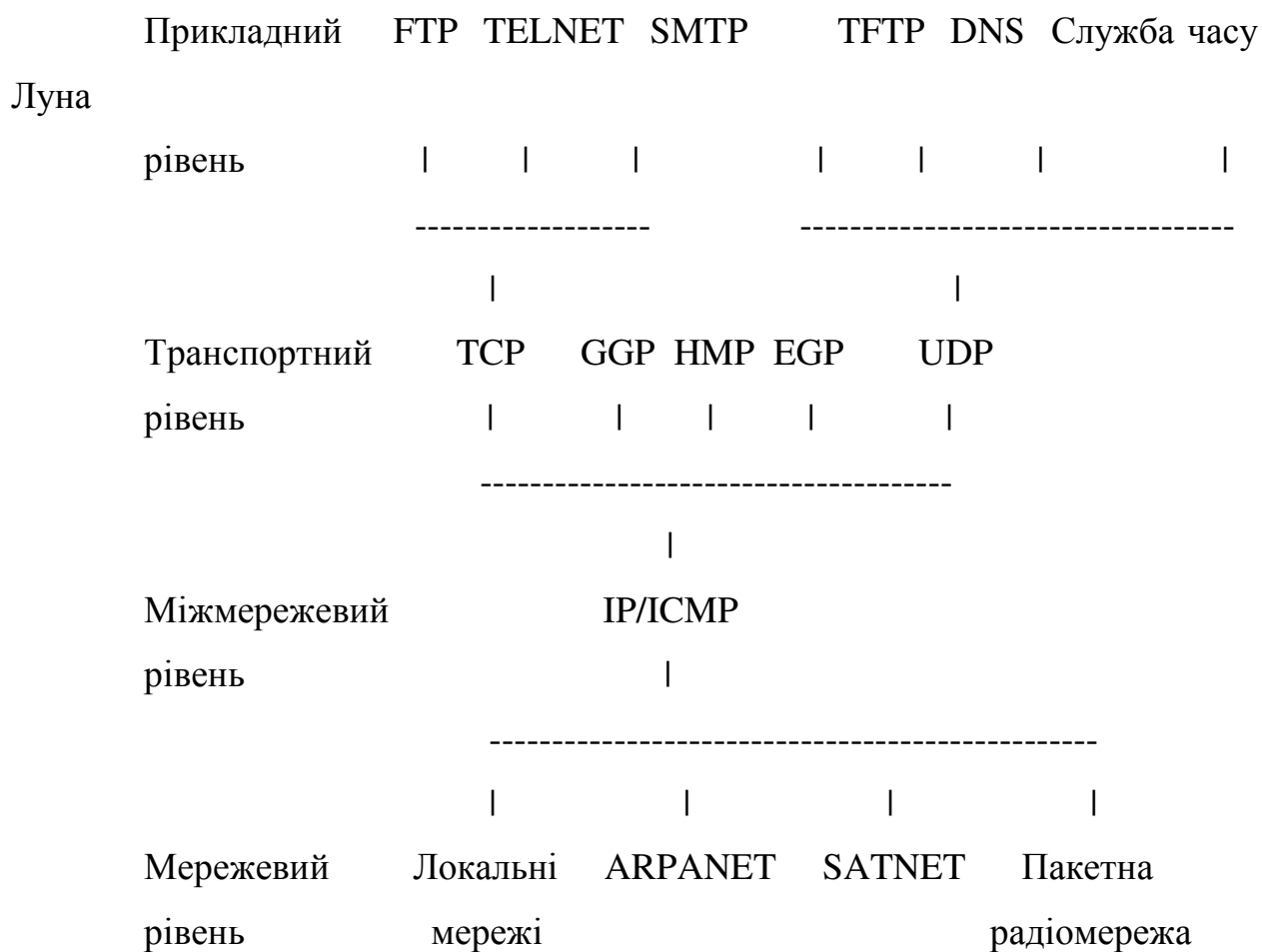


Рис.13. Структура взаємозв'язків протоколів сімейства TCP/IP