МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Б.Ю. Жураковський, І.О. Зенів

КОМП'ЮТЕРНІ МЕРЕЖІ
ЧАСТИНА 1
НАВЧАЛЬНИЙ ПОСІБНИК

*Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів,
які навчаються за спеціальністю 121 «Інженерія програмного забезпечення»
та 126 «Інформаційні системи та технології»
спеціалізацією «Інженерія програмного забезпечення інформаційно управляючих
систем» та «Інформаційне забезпечення робототехнічних систем»*

Київ
КПІ ім. Ігоря Сікорського
2020

УДК 004.7(075.8)

Рецензенти

1) *Толюпа С.В.,* д.т.н., професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету ім. Тараса Шевченко
2) *Отрох С.І.,* д.т.н., доцент, професор кафедри автоматизації проектування енергетичних процесів та систем НТУУ “Київський політехнічний інститут ім. Ігоря Сікорського”

Відповідальний редактор *Батрак Є.В., канд. техн. наук, доц.*

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 10 від 18.06.2020 р.) за поданням Вченої ради Факультету інформатики та обчислювальної техніки (протокол № 10 від 18.05.2020 р.)

Електронне мережне навчальне видання

Жураковський Богдан Юрійович, доктор техн. наук, проф.
Зенів Ірина Онуфріївна, кандидат техн. наук, доц.

КОМП’ЮТЕРНІ МЕРЕЖІ
ЧАСТИНА 1
НАВЧАЛЬНИЙ ПОСІБНИК

КОМП’ЮТЕРНІ МЕРЕЖІ Частина 1 НАВЧАЛЬНИЙ ПОСІБНИК [Електронний ресурс]: навч. посіб. для студ. спеціальності 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології», спеціалізації «Інженерія програмного забезпечення інформаційно управляючих систем» та «Інформаційне забезпечення робототехнічних систем»/ Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 8,6 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с.

Посібник призначений для опанування теоретичних та практичних навичок, які необхідні майбутнім фахівцям для вивчення дисципліни «Комп’ютерні мережі». Обсяг та перелік тем запропонованого посібника повністю покриває потреби 121 та 126 спеціальностей. Для кожної теми наведено перелік питань для самоконтролю, задачі для роботи в аудиторії різного рівня складності та вказано питання, що будуть включені в модульну контрольну роботу. Посібник призначений для студентів спеціальностей 121 «Інженерія програмного забезпечення» та 126 «Інформаційні системи та технології» всіх форм навчання.

ЗМІСТ

Вступ

Розвиток сучасних інформаційних технологій супроводжується збільшенням ролі телекомунікаційних систем різного призначення та комп'ютерних мереж. Це пояснюється необхідністю більш швидкої передачі інформації, в тому числі й управлінської, для якої важливе значення мають час та оперативність її доставки до користувачів. Більш вагомим стає використання засобів електронного обміну документів – електронної пошти, програмного забезпечення браузерів тощо – за допомогою яких набагато збільшується ефективність роботи фахівців різних рівнів управління сучасними підприємствами та установами.

Особливе місце в цих завданнях займають сучасні технології комп'ютерних мереж, серед яких слід виділити локальні та глобальні мережі. Це пояснюється необхідністю використання корпоративної інформації, що міститься в корпоративних базах даних, які можуть розташовуватися як в окремих підрозділах підприємства, так й за його межами. Отже сучасні технології оброблення документів різного призначення повинні базуватися на засобах телекомунікаційного зв'язку й стандартів комп'ютерних мереж, які виступають як транспортні системи передачі даних.

Для підвищення ефективності функціонування мереж підприємства повинні використовуватися засоби їх поширення у випадку збільшення кількості робочих станцій та користувачів. Це призводить до необхідності більш детальнішого вивчення та використання спеціальних пристроїв та відповідних стандартів для об'єднання окремих локальних мереж в єдину. До них належать концентратори, мости, шлюзи, комутатори, які дозволяють збільшувати ефективність окремих мереж за рахунок поєднання мереж із різними стандартами та протоколами. Вибір певного стека протоколів забезпечує визначення можливостей роботи мережі згідно із обраним стандартом та дозволяє вирішувати питання оцінки ефективності розгортання мережі із заданим рівнем масштабованості та розподіленості даних. За такими умовами виникає необхідність обґрунтування вибору системного мережного

забезпечення в умовах клієнт-серверної технології доступу та оброблення запитів користувачів.

Таким чином, комп’ютерні мережі та телекомунікаційні системи стають підґрунтям для підвищення ефективності інструментальної складової та інтелектуалізації процесів прийняття рішень в сучасних умовах високотехнологічного виробництва.

Розділ 1. ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ КОМП'ЮТЕНИХ МЕРЕЖ

1.1.Основні поняття

З кожним роком підсилюється тенденція зближення комп'ютерних і телекомунікаційних мереж різних видів. Намагаються створити універсальну, так звану *мультисервісну мережу,* здатну надавати послуги як комп'ютерних, так і телекомунікаційних мереж.

До телекомунікаційних мереж відносяться телефонні мережі, радіомережі й телевізійні мережі. Головне, що поєднує їх з комп'ютерними мережами, – те, що як ресурс, який надається клієнтам, виступає інформація. Однак ці мережі, як правило, представляють інформацію у різному вигляді. Так, споконвічно комп'ютерні мережі розроблялися для передачі алфавітно-цифрової інформації, що часто називають просто даними, у результаті в комп'ютерних мереж є й інша назва – *мережі передачі даних,* у той час як телефонні мережі й радіомережі були створені для передачі тільки голосової інформації, а телевізійні мережі передають і голос, і зображення.

Незважаючи на це, *конвергенція телекомунікаційних* і *комп'ютерних мереж* йде за декількома напрямками.

Еволюційні процеси в галузі зв'язку можна спостерігати як у вдосконаленні рівнів технологічного розвитку, так і в зміні термінології.

Так, загальноприйнятий термін «*електрозв'язок*» поступово трансформувався в міжнародний термін «*телекомунікації*». Сучасні мережі зв'язку є, мабуть, найскладнішими штучними системами, які вдалося створити сучасній цивілізації.

Вивчення таких систем вимагає комплексних знань у багатьох сферах інтелектуальної діяльності людини.

Комунікація (Communication) - поняття, що означає сполучення, зв'язок, а також засоби сполучення і зв'язку.

Телекомунікації (теле - у перекладі з давньогрецької означає далеко) - сукупність засобів, що забезпечують можливість організації зв'язку на значній відстані [1].

Загальне поняття «телекомунікації» базується на уявленні про засоби, які дозволяють організувати зв'язок між двома і більше віддаленими пунктами.

Секція телекомунікацій Міжнародного союзу електрозв'язку (*Telecommunications Standardization Sector of International Telecommunications Union, ITU-T*) у Рекомендаціях серії I (I.110, I.112) визначає термін «*телекомунікації*» (Telecommunications) **–** як ***сукупність засобів*** телекомунікацій, які забезпечують перенесення інформації, подану у необхідній формі, на значну відстань за допомогою поширення сигналів в одному з середовищ (міді, оптичному волокні, ефірі) або сукупності середовищ.

Засобами, визначеними загальним поняттям **«засоби телекомунікацій»,** є лінії зв'язку, пристрої з'єднання середовищ, системи передачі, комунікаційні пристрої мережі, обладнання сигналізації, синхронізації та ін.

Телекомунікаційна мережа *(Telecommunication Network, TN)* – це системоутворююча сукупність засобів телекомунікацій, що надає територіально віддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (електричними, оптичними або радіо) [2].

Телекомунікаційна мережа (мережа зв'язку) є *базовим зв'язуючими компонентами* будь-якої *територіально-розподіленої системи.* Поняття *система* характеризує складність об'єкта (численність і неоднорідність елементів, зв'язків між ними), а поняття *розподілена* – його мережну структуру.

Транспортування **(Transfer)** інформації в мережевій термінології означає *перенесення інформації,* перетвореної в сигнал від джерела до одержувача.

Його слід відрізняти від терміна **«передача» (Transmission),** під яким розуміється *процес поширення сигналу* у фізичному середовищі між двома суміжними пунктами мережі.

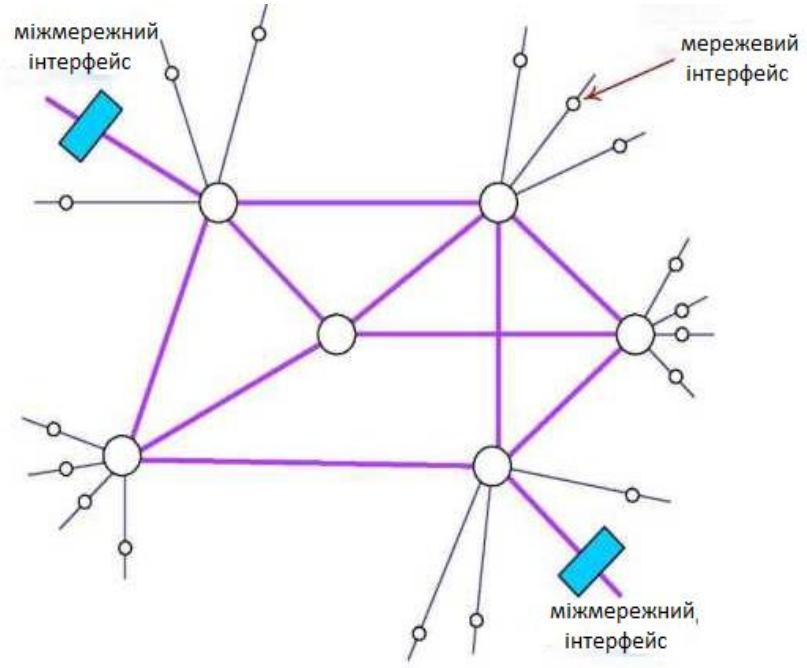


Рис.1.1. Телекомунікаційна мережа

Територіально віддаленими об'єктами у мережі зв'язку можуть виступати як термінальні пристрої користувачів так і кінцеві системи мережі,так і окремі мережі.

Обслуговування користувачів з боку телекомунікаційної мережі здійснюється шляхом надання ***послуг*** і ***додатків.***

Послуга (Service) - це те, що пропонується мережею користувачеві з метою задоволення його комунікаційних потреб.

Телекомунікаційні послуги (Telecommunication Service) – результат функціонування телекомунікаційної мережі, при якому задовольняється запит на доставку (транспортування) даних або на встановлення зв'язку.

Додаток (Application) є подібний до поняття послуги, але, на відміну від останньої, надається користувачеві як кінцевий продукт, який може багаторазово ним використовуватися. Наприклад, придбання спеціального пакета програм для реалізації послуг мультимедіа з їхньою інсталяцією на смартфоні є прикладом додатків [3].

Службою мережі (Service network) називається організаційно-технічний комплекс, який забезпечує надання мережею конкретного виду послуг.

Платформою надання послуг називається сукупність об'єднаних ресурсів

мережі, що беруть участь у виробництві і наданні послуг.

Оператор мережі (network operator) – юридична особа (державна структура або приватна компанія), що є власником мережі, забезпечує її експлуатацію і потрібний рівень показників її працездатності.

Провайдер послуг (service provider), або **постачальник послуг** – юридична особа, яка формує платформу надання послуг, вт. ч. шляхом оренди мережевих ресурсів (наприклад, виділених каналів зв'язку) у операторів мережі.

Поняттям ***«технологія»*** (Technology) у сфері телекомунікацій позначають спосіб реалізації режиму перенесення інформації в мережі, який забезпечує користувачів певним гарантованим рівнем якості обслуговування.

Спосіб реалізації перенесення даних (інформації) в просторі, що забезпечує певний гарантований рівень якості обслуговування в мережі називається **телекомунікаційною технологією (Telecommunication technology).**

1.2. Режими перенесення інформації

Термін ***«режим перенесення»*** (Transfer Mode) узагальнено розуміють як сукупність методів мультиплексування, передавання та комутації, за допомогою яких у телекомунікаційній мережі уможливлюється транспортування інформації від джерела до одержувача.

Режим перенесення інформації в мережі можна організувати *синхронним* способом або *асинхронним*

Синхронний режим перенесення **(Synchronous Transfer Mode)** ґрунтується на принципі синхронного часового мультиплексування та часового розділення каналів у процесі передавання інформації від одного вузла комутації до іншого. При цьому всі ланки тракту передавання інформації з кінця в кінець працюють синхронно. Таку синхронізацію забезпечують спеціальні синхронні технології, основані на використанні генераторів тактових сигналів, які працюють від єдиного еталонного джерела в мережі [4].

Для асинхронного режиму перенесення **(Asynchronous Transfer Mode)** достатньо забезпечити синхронне передавання інформації лише між суміжними об'єктами (передавачем і приймачем вузлів, безпосередньо з'єднаних лінією зв'язку). У транзитному вузлі інформаційні блоки зберігаються деякий час у пристрої запам'ятовування,а потім передаються в наступний вузол мережі. При цьому швидкості у вхідному та вихідному каналах вузла можуть відрізнятися. Таким чином, при асинхронному режимі інформація переміщується мережею естафетним способом.

1.3. Інформаційна мережа

Поняття **«інформаційна мережа» (Information Network, IN)** передбачає розгляд телекомунікаційної мережі в сукупності зі взаємодіючими за допомогою неї об'єктами. У такому розумінні інформаційна мережа – це «навантажена» телекомунікаційна мережа.

У загальному випадку **під інформаційною мережею** будемо розуміти сукупність територіально розосереджених кінцевих систем і об'єднуючої їх телекомунікаційної мережі, що забезпечує доступ прикладних процесів будь-якої з цих систем до всіх ресурсів інформаційної мережі і їхнє спільне використання.

Поняття «інформаційна мережа», на відміну від поняття «телекомунікаційна мережа», є більш узагальненим і відображає множину ***інформаційних процесів,*** які протікають в мережі [6]. Ці процеси виникають у результаті взаємодії кінцевих систем, під'єднаних до телекомунікаційної мережі. Інформаційні мережі призначені для надання користувачам послуг, пов'язаних з обміном інформацією, її споживанням, а також обробкою, зберіганням і накопиченням.

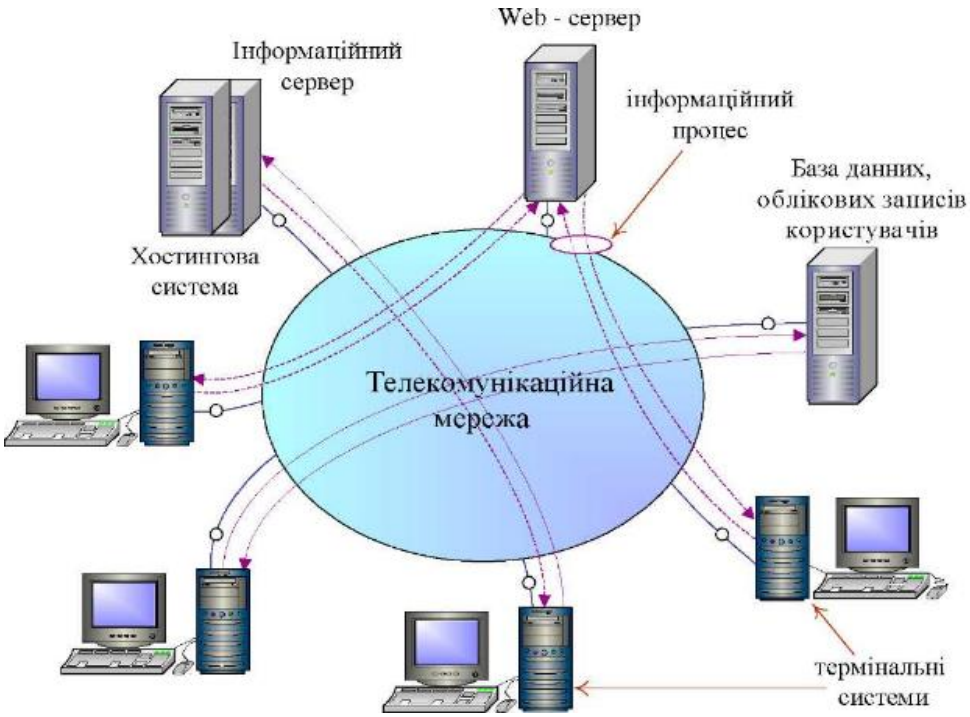


Рис.1.2. Інформаційна мережа

Споживач інформації, що одержав доступ до інформаційної мережі, стає її **користувачем (User).** Користувачами можуть бути як фізичні, такі юридичні особи (фірми, організації, підприємства).

Телекомунікаційна мережа, якій і належить, у складі інформаційної мережі виконує функції *транспортувальної системи.*

Інформаційна мережа (Information Network) – системоутворювальна сукупність територіально розосереджених кінцевих систем, об'єднаних телекомунікаційною мережею, за допомогою якої забезпечується взаємодія прикладних процесів, що активізуються в кінцевих системах, і колективний доступ до їх інформаційних і обчислювальних ресурсів.

Базовим компонентом, ядром інформаційної мережі, є *телекомунікаційна мережа.*

Інформаційні технології (Information Technologies) – методи і способи накопичення, обробки, зберігання, відображення, пошуку і забезпечення цілісності інформації.

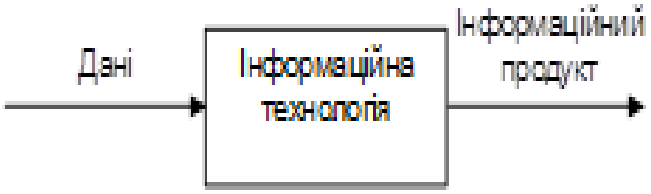


Рис.1.3. Інформаційна технологія

Метою інформаційної технології є виробництво інформації для її аналізу та прийняття рішення для виконання певної дії.

Користувач отримує інформацію з мережі у вигляді **контенту (content)** – *деякого обсягу, що забезпечує сприйняття його смислового змісту. У цьому контексті інформаційні послуги ще називають контент-послугами.*

Під **контентом (content)** *розуміють дані, призначені для зберігання з метою подальшої можливості перетворення в будь-яку необхідну форму.*

Інформаційна послуга (Information Service) – *це задоволення інформаційного запиту користувача, сформованого в результаті цілеспрямованого пошуку інформації в розподіленій системі інформаційних ресурсів, шляхом доставки засобами телекомунікацій затребуваної копії контенту.*

Конвергенція на рівні мереж, технологій і послуг інформаційної та телекомунікаційної сфер породила нове концептуальне поняття «*інфокомунікацій*».

1.4. Інфокомунікаційна мережа

Інфокомунікації – *порівняно новий термін, що означає нерозривний зв'язок інформаційних і телекомунікаційних елементів інформаційного обміну, які розвиваються в процесі конвергенції,тобто взаємного проникнення.*

Інфокомунікації - *це об'єднання телекомунікацій з інформаційними, комп'ютерними технологіями та радіотехнологіями.*

Інфокомунікації (Infocommunication) — це сукупність засобів обробки, накопичення, зберігання інформації та перенесення її в просторі, імплементованих в єдину мережну структуру, за допомогою якої забезпечується доступність інформаційних ресурсів та інформаційний обмін.

Інфокомунікаційна мережа (Infocommunication Network) — це сукупність територіально розосереджених інформаційних, обчислювальних ресурсів, програмних комплексів управління, що розміщуються в кінцевих системах мережі та термінальних системах користувачів, взаємодія між якими забезпечується за допомогою телекомунікацій і які спільно утворюють єдину мультисервісну платформу

Інфокомунікаційна послуга (Infocommunication Service) — це мультипослуга, що забезпечує задоволення телекомунікаційних або інформаційних, або тих та інших одночасно потреб споживача з наданням йому можливості керувати процесом реалізації цієї послуги.

Під ***інфокомунікаційними службами*** розуміються всі існуючі системи передачі й обробки інформації: телефонія, телеграфія, передача даних, телебачення, а також служби: телеметрія, телекерування, теленаведення, телеконтроль, телеосвіта, телемагазин, телебіржа, телеаукціон, телереклама, дистанційна аварійна сигналізація тощо.

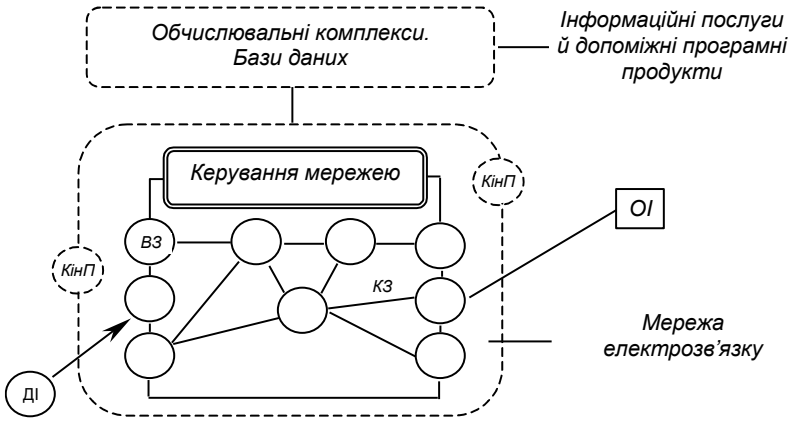


Рис. 1.4. Схема інфокомунікаційної мережі:
КінП – кінцевий пункт; *КЗ* – канал зв'язку; *ВЗ* – вузол зв'язку; *ДІ* – джерело інформації; *ОІ* – одержувач інформації

Інформацію, як і речовину та енергію, можна збирати і зберігати, обробляти і змінювати [2]. Але, крім того, інформація може створюватися і зникати, тиражуватися, бути правдивою і помилковою. Є в неї також ще одна особливість – вона не витрачається при використанні.

Інформація як відображення деякого об’єкта чи суб’єкта матеріальної системи може існувати незалежно від того, буде вона колись відновлена, чи ні. Цінність інформації та її споживча вартість залежать від споживача і творця інформації – людини чи процесу обробки в ЕОМ. Людина (чи процес обробки в ЕОМ), що створює інформацію, використовує її дуже обмежено. Інформація ж має високу цінність тоді, коли її творець стає джерелом інформації і передає її за допомогою засобів зв’язку, тобто споживча вартість інформації створюється в процесі зв’язку. Щоб одержати економічний або будь-який інший ефект (політичний, соціальний), необхідно передати інформацію будь-кому чи будь-чому за допомогою засобів зв’язку.

Отже, роль зв’язку в процесі інформатизації дуже велика, оскільки вона пронизує інформаційний процес від об’єкта спостереження і формування початкової інформації (сприйняття) через її обробку (квантування, кодування, модуляцію), передачу й обробку в приймачі доставки інформації до одержувача в обробленому вигляді.

Інфокомунікаційну мережу можна уявити як велику систему, до якої входять користувачі, засоби різних видів зв’язку, обладнання для надання послуг і системи керування.

1.5. Глобальна Інформаційна Інфраструктура

Глобальна Інформаційна Інфраструктура (Global Information Infrastructure, GII) надає користувачам набір комунікаційних послуг, які забезпечують множину застосувань, що охоплює усі види інформації та надає можливість її отримання в будь-якому місці, в будь-який час, за прийнятною ціною і з прийнятною якістю.

На Урядовій конференції країн "Великої сімки" (G7), що провадилась Комісією з Європейської Економічної Співдружності (ЄЕС), було прийнято основні принципи, на яких має базуватися розвиток GII, у числі яких:

- *прийнятність;*
- *елемент культури;*
- *керованість;*
- *мінімалізм;*
- *мобільність;*
- *номадізм;*
- *ефективність;*
- *портативність;*
- *взаємодія (інтероперабельність);*
- *якість;*
- *надійність;*
- *сумісність;*
- *ефективність (маштабованість);*
- *практичність;*
- *захист даних (безпека).*

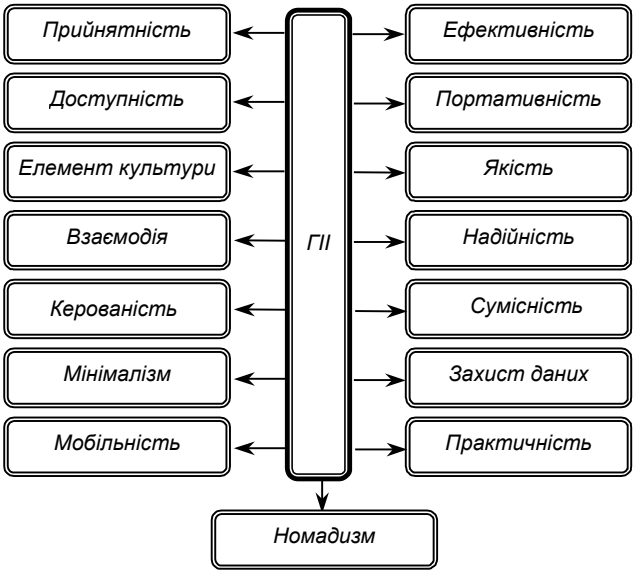


Рис. 1.5. Мінімальний набір принципів при створенні ГІІ

Прийнятність – економічна ефективність використання ресурсів

підприємствами, організаціями і споживачами у визначений період часу;

Доступність – ступінь доступності до визначеного ресурсу чи групи ресурсів;

Елемент культури – спеціальні характеристики мов і загальноприйнятих правил їх вживання (особливо писемною формою), що властиві визначеним суспільствам і географічним регіонам;

Керованість – можливість для кожного підприємства, організації і визначеного споживача контролювати розміщення й використання своїх ресурсів;

Мінімалізм – методологія або підхід, який забезпечує приєднання з мінімальною кількістю вимог;

Ефективність – ступінь виконання системою чи підсистемою своїх функцій, характеризується часом доступу, пропускною спроможністю, кількістю операцій за секунду, швидкістю відеоінформації;

Портативність – ступінь легкості, з якою програмне забезпечення і дані можуть бути передані з однієї системи в іншу;

Мобільність **–** можливості доступу до послуг із різних місць і під час руху. При цьому визначення й локалізація джерела надходження запитів мають забезпечуватися мережею;

Номадизм **–** можливості переміщення з одного місця в інше, зберігаючи при цьому доступ до послуг незалежно від доступності чи не доступності цих послуг у місцевому середовищі, ***тобто безперервність доступу в просторі й часі;***

Надійність – імовірність того, що продукт або система будуть функціонувати належним чином протягом визначеного проміжку часу;

Сумісність – здатність працювати з різними за швидкістю, ємністю і ціною прикладними платформами і середовищами;

Інтероперабельність (interoperability) — здатність систем мережі обмінюватися інформацією та спільно її використовувати;

Якість — забезпечення рівня якості, який очікує користувач;

Масштабованість — властивість сервісів та систем ефективно виконувати свої функції при широкому діапазоні параметрів, що визначають технічні та ресурсні характеристики підтримуючого середовища;

Практичність – ступінь легкості використання продукту чи системи.

Безпека — захист ресурсів (апаратних, програмних, інформаційних) від випадкових або навмисних дій, що призводять до несанкціонованого доступу до ресурсів і порушення конфіденційності їх використання, модифікації та руйнуванню ресурсів, а також розкриття інформації.

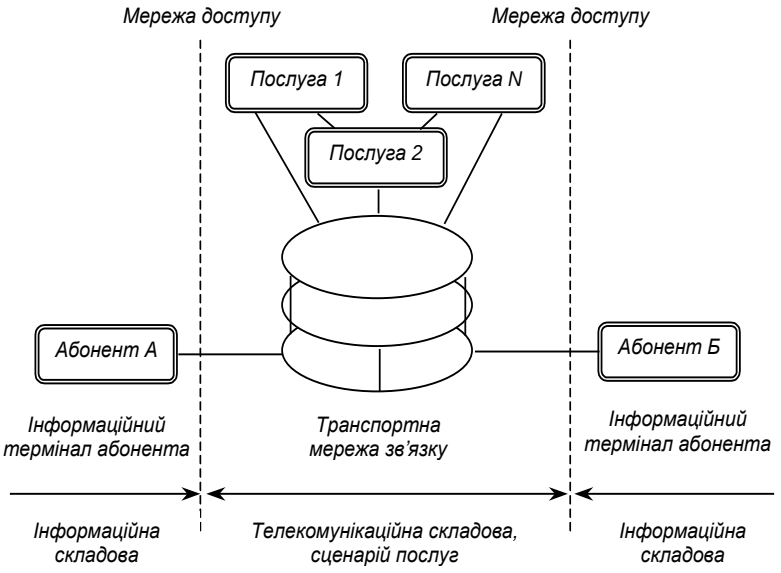


Рис.1.6. Глобальна Інформаційна Інфраструктура

Таким чином, *GII* можна вважати сукупністю термінального обладнання, за допомогою якого користувач має доступ до різних (1,2,...,N послуг і мереж доступу, транспортних та інших засобів, в т.ч. інформаційних ресурсів. Основою є сучасна *інфокомунікаційна* мережа.

Усі мережі зв'язку належать до класу об'єктів, які називають складними системами.

Складні системи за своїм складом є *гетерогеннимu,* тобто характеризуються величезною кількістю неоднорідних елементів і зв'язків між ними.

Під *системним описом* розуміють багаторівневий опис об'єкта у вигляді *моделей,* кожна з яких відображає об'єкт в певному аспекті його розгляду (рівня абстрагування).

Модель – це формалізований опис об'єкта, що дозволяє досліджувати його основні елементи, не відволікаючись на несуттєві, з точки зору поставленої мети,

деталі. Рівні абстрагування зазвичай розташовуються в ієрархічному порядку (під порядкування за старшинством).

Мережам зв'язку властиво мати всі ознаки складних систем і підпорядковуватися відповідним їм закономірностям. Зазначимо деякі з них:

- **Ієрархічність**
- **Комунікаційність**
- **Емержентність**

Ієрархічність – розташування частин та елементів цілого в порядку від вищого до нижчого. Дотримуючись цієї закономірності, ми можемо розчленовувати мережу на окремі підмережі (сегменти) нижчого порядку. *Наприклад, глобальна мережа може бути представлена сукупністю територіальних мереж різного масштабу: континентальних, регіональних, міських, локальних та ін.*

Комунікаційність - закономірність, що вказує на велику кількість зв'язків (комунікацій) системи: зовнішніх – з середовищем і внутрішніх – з підсистемами та елементами. Це означає, що будь-яку мережу зв'язку можна розглядати як підмережу (підсистему) або елемент системи більш високого порядку (наприклад, як елемент Глобальної Інформаційної Інфраструктури) і в той же час вона може розглядатися як самостійна система, що включає підсистеми (сегменти) більш низького порядку.

Емержентність - закономірність, яка полягає у вияві системою інтегрованої якості - цілісності, невластивої окремим її елементам. Так, наприклад, у мережі ми можемо виділити такі функційно важливі й відносно незалежні підсистеми, як мережа доступу, транспортна мережа, система керування мережею та ін. Жодну із зазначених систем неможна ототожнити з мережею зв'язку в цілому, і тільки їх взаємозв'язок відображає це поняття. З іншого боку, розглядаючи та вивчаючи структури окремих підсистем, ми поглиблюємо своє уявлення про систему.

Процес побудови ряду окремих структур системи має назву «структуризація». Структуризація складної системи ототожнюється з

архітектурою.

Отже, **архітектура** – це багаторівневий опис системи, отриманий шляхом структуризації.

Поняття архітектури характеризує цілісне уявлення про побудову мережі і, отже, відбиває її *емержентність*.

Архітектурою *називається системний опис мережі, що відображає всю множину її елементів, зв'язків між ними і правил взаємодії.*

1.6.Протокольна модель

Протокольна модель — опис правил взаємодії систем у мережі на рівні взаємодії об'єктів і логічних модулів, необхідних для реалізації процесів передавання й оброблення інформації взаємодіючими системами [7].

У цій моделі всі правила (протоколи) взаємодії групуються за їх функційним призначенням в окремі групи — *протокольні блоки***.** Ці блоки розміщуються в ієрархічному порядку, і кожний з них є множиною протоколів взаємодії об'єктів певного рівня систем.

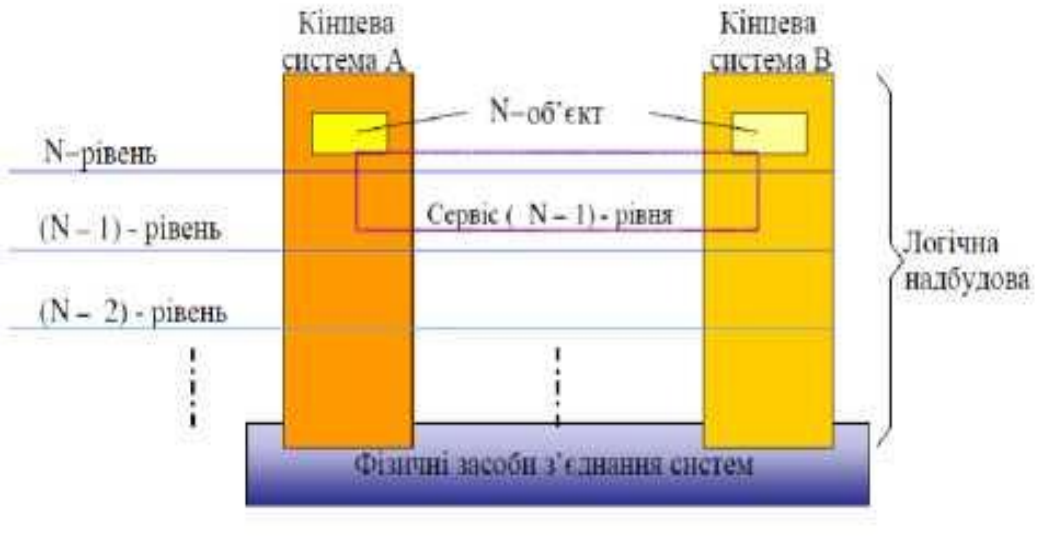


Рис.1.5. Принцип побудови протокольної моделі

Усі правила взаємодії об'єктів у протокольній моделі визначають стандарти для конкретної мережі і класифікуються як протоколи (стандарти взаємодії

об'єктів одного рівня з іншим) та інтерфейси (стандарти взаємодії об'єктів сусідніх рівнів). Будь-який об'єкт N рівня активізуючись видає інформацію двох типів:

1) інформацію, яка призначена для N-об'єкту (дані користувача) і не пов'язана з операціями підтримання зв'язку N-рівня;

2) інформацію керування, яка призначена для об'єкта (N-1) - рівня, за допомогою якої здійснюється координація процедур "з'єднання" об'єктів N-рівня.

Контрольні питання до розділу

1. Дайте визначення поняттю «*Комунікація*»?
2. Дайте визначення поняттю «*Телекомунікації*»?
3. Дайте визначення поняттю *«Телекомунікаційна мережа»?*
4. Дайте визначення поняттю *«Транспортування інформації*»?
5. Дайте визначення поняттю «Передача» (Transmission)?
6. Дайте визначення поняттю *«Послуга» (Service)?*
7. Дайте визначення поняттю *«Телекомунікаційні послуги» (Telecommunication Service)?*
8. Дайте визначення поняттю *«Додаток (Application)» ?*
9. Що розуміють під службою мережі (*Service network*)?
10. Що розуміють під платформою надання послуг?
11. Дайте визначення поняттю «*Оператор мережі*»?
12. Дайте визначення поняттю «*Провайдер послуг*»?
13. Що розуміють під поняттям *«технологія» (Technology)?*
14. Що розуміють під телекомунікаційною технологією (*Telecommunication technology*)?
15. Поясніть поняття терміну *«режим перенесення» (Transfer Mode)?*
16. Поясніть поняття с*инхронного режиму перенесення* (*Synchronous Transfer Mode*)?
17. Поясніть поняття *асинхронного режиму перенесення* (*Asynchronous Transfer Mode*)?
18. Поясніть поняття «*інформаційна мережа*»?
19. Поясніть поняття «*інформаційні технології*»?
20. Дайте визначення поняттю контенту (content)?
21. Що таке «*інформаційна послуга*» ?
22. Поясніть поняття і*нфокомунікації (Infocommunication)?*
23. Поясніть поняття «*інфокомунікаційна мережа»?*
24. Поясніть поняття «*інфокомунікаційна послуга»?*
25. В чому полягають принципи на яких має базуватися розвиток Глобальної Інформаційної Інфраструктури (Global Information Infrastructure, GII)?
26. Дайте визначення поняттю «*мобільність» (mobility)?*
27. Дайте визначення поняттю «*номадизм» (nomodicity)?

28. Дайте визначення поняттю «*інтероперабельність» (interoperability)?*
29. Дайте визначення поняттю «*якість»(quality)?*
30. Дайте визначення поняттю «*масштабованість» (scalability)?*
31. Дайте визначення поняттю «*безпека» (security)?*
32. Дайте визначення терміну «м*одель»?*
33. Які ознаки складних систем властиво мати мережам зв'язку?
34. Поясніть поняття «ієрархічність»?
35. Поясніть поняття «комунікаційність»?
36. Поясніть поняття «емержентність»?
37. Дайте визначення терміну «а*рхітектура»?*
38. Що собою представляє протокольна модель?

Список рекомендованої літератури

1. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
2. Компьютерные сети. 4-е изд./ *И. Таненбаум*. – СПб.: Питер, 2003. – 992 с.
3. *Стеклов В.К., Беркман Л.Н.* Телекомунікаційні мережі. –К.: Техніка, 2001.– 392 с.
4. *Кривуца В.Г., Беркман Л. Н., Лапінський В.В.* Основи інфокомунікацій: навч. посібник для загальноосвіт. навч. закладів - К.: ДУІКТ, 2011.- 276 с.
6. *А.П. Бондарчук, Г.С. Срочинська, М.Г. Твердохліб* Основи інфокомунікаційних технологій (Навчальний посібник).К.: ДУТ, 2015.—76 с
7. *Стрихалюк Б. М.* Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. – Львів: Львівська політехніка, 2017. – 121 с.

Розділ 2. ЕТАЛОННА МОДЕЛЬ OSI

2.1. Основні поняття

Відкритою системою називається будь-яка система (мережа, програмний продукт, апаратний засіб), яка може взаємодіяти з аналогічною іншою системою та побудована відповідно до *відкритих специфікацій.*

Під терміном «*специфікація*» розуміють формалізований опис апаратного або програмного компонента мережі, способу його функціонування, взаємодії з іншими компонентами та особливих характеристик.

Переваги при дотриманні відкритих стандартів:

1. можливість побудови мереж з апаратних і програмних засобів різних виробників;

2. безпроблемну заміну одних компонентів мережі іншими, більш досконалими, що дозволяє забезпечити розвиток мережі з мінімальними витратами;

3. вільне сполучення однієї мережі з іншою.

Організації у сфері стандартизації:

- окремі великі фірми-виробники (наприклад, *IBM, Sun* і т.п.);
- спеціальні комітети та об'єднання, засновані декількома компаніями (наприклад, *ATM Forum* з кількісним складом колективних учасників близько 100, *Fast Ethernet Alliance* з розробки стандартів 100Мбіт *Ethernet* та ін.);
- національні інститути та центри, які є організаціями країн і великих регіонів:
- ***Інститут національних стандартів США*** (*American National Standards Institute, ANSI*),
- ***Інститут стандартів телекомунікацій Європейського Союзу*** (*European Telecommunications Standards Institute, ETSI*),
- ***Інститут інженерів з електротехніки та електроніки США*** (*Institute of Electrical and Electronics Engineers, IEEE*),

- ***Комітет з телекомунікаційних технологій Японії*** (*Telecommunication Technology Commity, TTC*);
- ***міжнародні організації***, такі як:
    - Міжнародна організація стандартизації (*International Organization for Standardization, ISO*),
    - Міжнародний союз електрозв'язку (*International Telecommunication Union, ITU*) з такими секціями: *ITU-R* - секція радіомовлення, *ITU-T* - секція телекомунікацій, *ITU-D* – секція розвитку;
    - всесвітні організації, очолені міжнародними групами. Це організації, які займаються інтернет - стандартизацією, серед яких основним є науково-адміністративне співтовариство Інтернету (Internet Society, *ISOC*) зі складом понад 100000 осіб.

2.2. Рівні еталонної моделі OSI

Еталонна модель OSI є визначальним документом для розробки відкритих стандартів з організації з'єднань систем і мереж зв'язку.

Розробники еталонної моделі за основу взяли такі принципи:

- кількість протокольних рівнів не повинна бути занадто великою, щоб розробка мережі та її реалізація не ускладнювалися, водночас ця кількість немає бути занадто малою, щоб не перевантажувати логічні модулі кожного рівня;

- рівні повинні чітко відрізнятися логічними модулями й функціями (об'єктами), які на них виконуються;

- функції та протоколи одного рівня можуть змінюватися, якщо це не порушує інші рівні;

- кількість інформації, яка передається через інтерфейси між рівнями, повинна бути мінімальною;

- допускається подальше структурування рівнів на підрівні, якщо виникає необхідність локального зосередження на функціях у межах одного рівня.

Таблиця 2.1. *Рівні еталонної моделі OSI*

№ Рівня	Українська назва рівня	Англійська назва рівня	Позначення рівня
7	Прикладний	Application	A
6	Представлення	Presentation	P
5	Сеансовий	Session	S
4	Транспортний	Transport	T
3	Мережевий	Network	N
2	Канальний	DataLink	DL
1	Фізичний	Physical Link	PL

Фізичний рівень (Physical Layer) (рівень1) визначає електротехнічні, механічні, процедурні і функціональні характеристики встановлення, підтримки і роз'єднання фізичного каналу між кінцевими системами [3].

Електричні характеристики описують рівні напруги (або струму) і тимчасові характеристики сигналів, що подають 0 або 1.

Функціональні характеристики відображають функції, виконувані фізичним інтерфейсом. У більшості протоколів фізичного рівня ці функції класифікуються як функції керування, синхронізації, передачі даних і заземлення.

Механічні характеристики описують інтерфейсні рознімання і проводи. Звичайно всі проводи для передачі даних, сигналізації і керування збираються в один кабель.

Процедурні характеристики відображають дії, які мають здійснювати з'єднувачі, і послідовність дій при передаванні даних через інтерфейс.

Призначення і функції:

- встановлення, підтримка і роз'єднання фізичних з'єднань з заданими механічними, електричними, процедурними та функціональними характеристиками;
- прозора передача потока бітів між об'єктами другого рівня;

- ретрансляція потока біт у випадку з’єднання декількох каналів;

- синхронна (або асинхронна) передача фізичних блоків даних (одного або декількох біт);

- управління рівнем;

- оповіщення об’єктів другого рівня про несправності фізичного рівня;

- визначення параметрів якості послуг, що надаються.

Послуги служби фізичного рівня:

- фізичні з’єднання;
- фізичні блоки даних;
- кінцеві точки фізичного рівня;
- ідентифікація фізичного каналу;
- упорядкування бітів потоку;
- повідомлення про відмови;
- контроль параметрів якості обслуговування.

Специфікації фізичного рівня:

EIA-RS-232-C, ITU-T V.24/V.28 – механічні/електричні характеристики не збалансованого послідовного інтерфейсу;

EIA-RS-422/449, ITU-T V.10 - механічні, електричні і оптичні характеристики збалансованого послідовного інтерфейсу;

IEEE 802.3 CSMA/CD (Ethernet). Метод доступу і специфікації фізичного рівня;

IEEE 802.5 Token Ring. Метод доступу до кільця з передачею маркера і специфікації фізичного рівня;

I.430 – Основний інтерфейс «користувач – мережа» N-ISDN. Специфікація рівня 1;

I.431 – Інтерфейс «користувач - мережа» на первинній швидкості. Специфікація рівня 1;

SDH – Synchronous Digital Hierarchy (синхронна цифрова ієрархія);

PDH – Plesiochronous Digital Hierarchy (плезіохронна цифрова ієрархія);

FR – Frame Relay (фізичний рівень). Метод ретрансляції кадрів, визначений стандартами ITU-T, ANSI и Frame Relay Forum;

DSL – Digital Subscriber Line (цифрова абонентська лінія).

Фізичний рівень також описує процедури передачі сигналів у канал й одержання їх з каналу. Він призначений для переносу потоку двійкових сигналів (послідовності біт), у вигляді, придатному для передачі по конкретному використовуваному фізичному середовищу. Фізичним середовищем передачі можуть виступати: канал тональної частоти, сполучна проводова лінія, радіоканал або щось інше.

Фізичний рівень виконує три основні функції:

1. *встановлення й роз'єднання з'єднань;*

2. перетворення сигналів;

3. реалізація інтерфейсу.

Типовий профіль протоколів при використанні модему, що підтримує тільки функції фізичного рівня.

При цьому вважається, що комп'ютер (*DTE*) з'єднується з модемом (*DCE*) за допомогою інтерфейсу RS-232, а модем використає протокол модуляції *V.21*.

Канальний рівень (Data Link Layer) (рівень2) відповідає за якісну передачу даних між двома пунктами, пов'язаними фізичним каналом з урахуванням особливостей середовища-передавача.

Здійснює "прозору і безпомилкову" передачу. При цьому фізичні середовища передачі можуть відрізнятися (мідь, оптичне волокно, ефір). Несумісними можуть виявитися й вимоги до формату подання даних у кожному каналі, що називається лінійним кодуванням. У цій ситуації канальний рівень бере на себе функції адаптації даних до типу фізичного каналу зв'язку, надаючи вищим рівням «прозоре з'єднання».

Також канальний рівень здійснює виявлення та виправлення помилок, тобто «безпомилкову передачу»

Призначення і функції:

- формування з переданої послідовності біт блоків даних певного розміру для їхнього подальшого розміщення в інформаційному полі кадрів, які й передаються по каналі;

- кодування вмісту кадру завадостійким кодом (як правило, з виявленням помилок) з метою підвищення вірогідності передачі даних;
- відновлення вихідної послідовності даних на прийомній стороні;
- забезпечення кодонезалежної передачі даних з метою реалізації для користувача (або прикладних процесів) можливості довільного вибору коду подання даних;
- управління потоком даних на рівні каналу, тобто темпу їхньої видачі в DTE одержувача;
- усунення наслідків втрат, перекручувань або дублювання переданих у каналі кадрів.

Протоколи канального рівня:

- ***HDLC*** – *High-Level Data Link Control* (процедура управління ланкою даних верхнього рівня для послідовни з'єднань);
- ***IEEE 802.2*** – Управління логічною ланкою (LLC), забезпечує управління доступом до середовища передачі (MAC);
- ***Ethernet (IEEE 802.3)*** – локальна мережа на основі протоколу CSMA/CD;
- ***Token Ring (IEEE 802.5)*** – кільцева локальна обчислювальна мережа з передачею маркера, розроблена фірмою IBM і працююча зі швидкістю 4 Мбіт/с;
- ***X.25*** (функції рівня ланки даних) – інтерфейс між кінцевим обладнанням даних (DTE) і апаратурою закінчення каналу даних (DCE) для кінцевих пристроїв, які працюють в пакетному режимі і підключені до мереж даних загального користування.
- ***Frame relay*** (ретрансляція кадрів) – високошвидкісна технологія передачі кадрів, включаюча поділ даних передаючим пристроєм на кадри змінної довжини (кожний кадр має заголовок з ідентифікатором логичного з'єднання), передачу кадрів цифровим пристроєм з використанням власного віртуального каналу й збірку блока даних на приймальному кінці);
- ***PPP*** (*Point-to-Point Protocol*) – протокол передачі від точки до точки, протокол двохточкового з'єднання (набір протоколів кадрування та аутентифікації, є частиною сервиса віддаленого доступу RAS (Remote

Access Service) системи Windows; зв’язує конфігураційні параметри багаточисельних рівней моделі OSI).

Можливий профіль протоколів для модему, що підтримує функції фізичного й канального рівнів.

Вважається, що комп'ютер з'єднується з модемом за допомогою інтерфейсу *RS-232*, і вже модем реалізує протокол модуляції *V.34* й апаратну корекцію помилок згідно стандарту *V.42*.

Мережевий рівень Network Layer (рівень3) – це комплексний рівень, який забезпечує можливість з'єднання і вибір маршруту між двома кінцевими системами.

Основною функцією мережевого рівня є ***маршрутизація.*** Вона полягає в прийнятті рішення, через які конкретно проміжні пункти повинен пройти маршрут передавання даних, які направляються з однієї кінцевої системи в іншу, та як має виконуватися ***комутація*** (яка відповідає конкретному маршруту) між входами та виходами мережевих пристроїв, розташованих у проміжних пунктах мережі. Мережний рівень забезпечує прокладку віртуальних каналів між взаємодіючими системами через комутаційну підмережу.

Віртуальный канал – це таке функціонування компонентів мережі, що створює взаємодіючим об’єктам ілюзію прокладки між ними (тільки між ними) потрібного тракту. На цьому рівні також забезпечується керування потоками блоків даними, що передаються і які називаються пакетами [2–4].

Алгоритм маршрутизації - протокол мережного рівня, що керує пакетами під час їхнього руху в підмережі до необхідного місця призначення. Моменти часу, коли приймаються рішення про вибір маршруту, залежать від того, чи використовує мережа дейтаграмну передачу, чи віртуальні з’єднання.

У мережі з віртуальними з’єднаннями маршрут вибирається при встановленні кожного віртуального з’єднання.

Алгоритм маршрутизації застосовується для вибору мережі для даного віртуального з’єднання.

Всі пакети віртуального з’єднання послідовно використовують цей шлях аж до моменту, коли дане віртуальне з’єднання закінчує своє існування або коли для даного з’єднання з будь-яких причин вибирається інший маршрут.

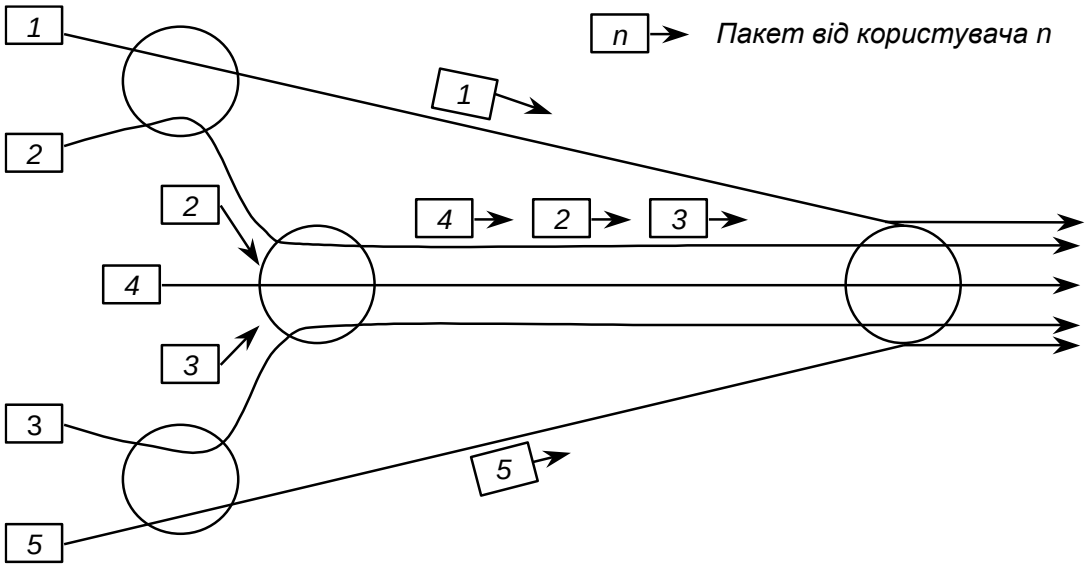


Рис. 2.1. Маршрутизація в ланцюзі з віртуальними каналами

Причини складності маршрутизації

Складність маршрутизації обумовлена рядом причин.

По-перше, вона потребує координації роботи усіх вузлів підмережі, а не тільки однієї пари модулів, як, наприклад, у протоколах канального і транспортного рівнів.

По-друге, система маршрутизації має бути нечутливою (інваріантною) до виходів із ладу ліній або вузлів шляху перенаправлення трафіка і відновлення бази даних, що використовуються системою.

По-третє, для досягнення найкращих характеристик алгоритм маршрутизації може змінити маршрути, коли деяка область мережі перевантажена [5].

Двома головними функціями, що виконує алгоритм маршрутизації, є *вибір маршрутів для різних пар відправник–адресат* і *забезпечення правильної доставки повідомлень адресатам після вибору маршрутів.*

Друга функція здійснюється використанням різних протоколів і структур даних (маршрутних таблиць).

Алгоритм маршрутизації істотно впливає на дві основні характеристики – *пропускну спроможність* (кількість обслуговувань) і *середню затримку пакета* (якість обслуговування).

Маршрутизація взаємозв'язана з керуванням потоками при визначенні характеристик за допомогою механізму зворотного зв'язку.

Відносно малий трафік, що надходить у підмережу від зовнішніх джерел, повністю приймається мережею, у даному випадку пропускна спроможність – навантаження, що надходить.

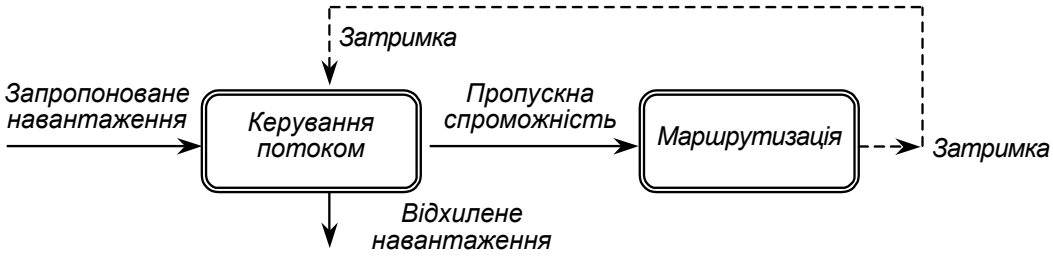


Рис. 2.2. Взаємозв'язок між маршрутизацією і керуванням потоком

Якщо навантаження надмірно велике, частина його буде відхилятися алгоритмом керування потоками, тобто *пропускна спроможність – це навантаження, що надходить, за вилученням відхиленого навантаження.*

Трафік, прийнятий мережею, матиме середню затримку пакетів, яка залежить від маршрутів, вибраних алгоритмом маршрутизації. Проте на пропускну спроможність істотний вплив має також алгоритм маршрутизації, тому що алгоритм керування потоками звичайно діє на основі підтримки балансу між пропускною спроможністю і середньою затримкою. Наприклад, навантаження, що надходить, не приймається, як тільки затримка стає занадто великою. Тому, якщо алгоритму маршрутизації вдається більш успішно підтримувати малу затримку, то алгоритм керування потоками дозволяє приймати в мережу більше трафіка. Хоча точний баланс між затримкою і пропускною спроможністю встановлюється алгоритмом керування потоками, ефективна маршрутизація в умовах великого запропонованого трафіка дає кращу залежність *затримка – пропускна здатність,* за якою діє алгоритм

керування потоками.

Існує декілька способів класифікації алгоритмів маршрутизації [1]. Один із них полягає в розподілі всіх алгоритмів на централізовані і розподілені. У *централізованих* алгоритмах вибір усіх маршрутів здійснюється в центральному вузлі, а в *розподілених* – у вузлах мережі. При цьому вузли обмінюються інформацією у разі потреби.

Транспортний рівень Transport Layer (рівень 4) забезпечує послуги з транспортування даних між двома взаємодіючими абонентами.

Функцією транспортного рівня є надійне транспортування даних через мережу. Транспортний рівень здійснює формування блоків даних та їх нумерацію та утворення неперервного потоку даних із блоків даних.

Щоб реалізувати різні типи передач даних, які можуть знадобитися як на транспортному рівні, так і в роботі різних мереж, транспортний протокол *OSI* передбачає п’ять класів з’єднань. Вони позначаються номерами 0, 1, 2, 3 і 4 [6].

Клас 0 за рекомендацією ITU прийнятний для транспортних послуг в терміналах телетекс. Це найпростіше транспортне з’єднання, для якого визначено мінімум функцій. Вважається, що його мережне з’єднання забезпечує ймовірність помилок не вищу від заданої, а також частоту відмов, яка не перевищує допустиму. Для цього класу транспортного протоколу слід тільки встановити просте транспортне з’єднання між користувачами, а у фазі передачі даних при потребі забезпечити можливість сегментування повідомлень. Він не передбачає відновлення при збоях і не дає змоги об’єднати кілька транспортних з’єднань в одному мережному з’єднанні. У разі виникнення збоїв мережний рівень сигналізує про це, і сигнали передаються на вищестоящі рівні для вжиття відповідних заходів.

Клас 1 теж простий, але має можливості відновлення при збоях. Збої можуть статися через роз’єднання або пошкодження в мережі, через прийом блоку даних невпізнаного транспортного з’єднання і т.д.

Класи 2, 3 і 4 складніші, вони мають більші функціональні можливості щодо задоволення конкретних вимог до послуг, подолання труднощів або збоїв, які можуть виникнути, якщо знизиться надійність мережних з’єднань.

Прикладами таких можливостей можуть служити об'єднання декількох транспортних з'єднань в одному мережному з'єднанні, розподіл одного транспортного з'єднання кількома мережними з'єднаннями і відновлення при збоях, про які сигналізує мережа.

Вибір класу визначається якістю обслуговування, що запитує користувач транспортної послуги, а також нижчестоящим мережним з'єднанням (або з'єднаннями), що надає необхідні послуги. Стандарт транспортного протоколу (ТП) визначає три типи мережних з'єднань, які можуть використовуватися в сполученні з різними класами.

Тип А – це мережне з'єднання з прийнятною ймовірністю помилок і інтенсивністю збоїв, про які надходять сигнали в транспортний протокол, тобто основне з'єднання передбачається високоякісним: пакети не губляться і не порушується їх послідовність, отже немає потреби передбачати на транспортному рівні послуги відновлення після збоїв, інформування про втрату даних, відновлення послідовності тощо. Це – тип мережного з'єднання, за яким працює клас 0. Прикладом застосування може служити мережа з послугами віртуальних каналів на мережному рівні.

Особливістю мережних з'єднань ***типу В*** є прийнятна ймовірність помилок, але неприйнятна інтенсивність надходження сигналів про пошкодження. За таких умов транспортний протокол має передбачати відновлення з'єднання після збоїв. До цієї категорії належить клас 1.

Мережним з'єднанням ***типу С*** характерна частота збоїв, неприйнятна для користувача транспортної послуги. *Транспортний протокол* для цього типу має передбачати можливість виявлення мережних збоїв і відновлення з'єднання, виявлення і виправлення порушень послідовності, дублювання, посилку даних за неправильною адресою, тощо. За цих умов мережна послуга може бути відносно низької якості, але протокол має відокремити користувача транспортних послуг від труднощів, пов'язаних з цим. Прикладами таких мереж є деякі види локальних мереж, дейтаграмні мережі з пакетами, що можуть надходити з порушенням послідовності, міські мережі з мобільними вузлами, пакетні радіомережі з завмираннями [7].

Протокол класу 4 розрахований на роботу зі з'єднаннями типу *C*, **протокол класу 2** – на роботу з мережними з'єднаннями типу *A*.

Протокол класу 2, який передбачає надійне мережне з'єднання, не потребує передачі у фазі з'єднання блоку даних для підтвердження на відміну від протоколу класу 4.

Клас 2 дає можливість об'єднання, чого клас 0 не передбачає.

Протокол класу 3 розрахований на роботу зі з'єднаннями типу *B*, на об'єднання класу 2 та процедури відновлення після збоїв.

Таблиця 2.2. *Вимоги до основних функцій класів транспортного протоколу OSI*

Клас	**Тип мережного з'єднання**	**Вимоги**
0	*A*	Встановлення зв'язку
1	*B*	Усунення збоїв
2	*A*	Об'єднання
3	*B*	Усунення збоїв і об'єднання
4	*C*	Виявлення збоїв та їх усунення

Таким чином, на транспортному рівні зв'язку виконуються *з'єднання, передача інформації і роз'єднання.*

Транспортні послуги поділяються на дві групи – *послуги для керування з'єднанням* і *для передачі даних.*

У свою чергу, послуги з керування з'єднанням складаються з послуг, необхідних для надання з'єднання від початку до кінця, і для завершення зв'язку або роз'єднання.

Передача даних може бути як *нормальною*, так і *терміновою*. Передбачено також вибір передачі без з'єднання, що дозволяє передавати поодинокі блоки даних.

Сеансовий рівень Session Layer (рівень5) встановлює, управляє і завершує сеанси взаємодії між прикладними завданнями. Сеанси складаються з діалогу між об'єктами.

Сеансовий рівень синхронізує діалог між об'єктами рівня представлення і управляє обміном інформації між ними.

Сеансовий рівень забезпечує виконання функцій *керування сеансом зв'язку (сесією)*, орієнтованим на наскрізну передачу повідомлень, таких, наприклад, як встановлення й завершення сесії; *керування черговістю й режимом передачі даних (симплекс, напівдуплекс, дуплекс); синхронізація; керування активністю сесії; складання звітів про надзвичайні ситуації.* Разом із транспортним рівнем сеансів рівень формує протоколи, орієнтовані на встановлення з'єднання й протоколи, які забезпечують для вищих рівнів надійний сервіс без встановлення з'єднання.

Послуги сеансової служби:

- управління взаємодією;
- дуплексна взаємодія;
- напівдуплексна взаємодія;
- сімплексна взаємодія;
- синхронізація сеансового з’єднання;
- оповіщення про особові стани;
- обмін звичайними даними;
- обмін срочними даними.

Рівень представлення (Presentation layer) (рівень 6) здійснює інтерпретацію і перетворення даних, які передаються у мережі до типу, що сприймається процесами прикладного рівня та зворотне перетворення; забезпечує подання даних в узгоджених форматах і синтаксис і, трансляцію й інтерпретацію програм з різних мов, шифрування й стиснення даних.

На рівні представлення реалізуються наступні функції:

- запрос встановлення сеансу;
- узгодження синтаксису;
- перетворення синтаксису;
- передача даних;
- запрос завершення сеансу.

Рівень представлення використовує три версії синтаксису даних:

- синтаксис, який використовується прикладним об’єктом–відправником;
- синтаксис, який використовується прикладним об’єктом–отримувачем;
- синтаксис передачі, який використовується об’єктами представницького рівня.

Прикладний рівень (Application Layer) (рівень7) забезпечує послугами прикладні процеси, здійснює керування терміналами й прикладними процесами в кінцевих системах мережі, які є джерелами та споживачами інформації.

Цей рівень надає сервіси безпосередньо для прикладних програмам користувачів, ідентифікує і встановлює наявність прикладних процесів, а також встановлює і погоджує процедури усунення помилок і управління цілісністю інформації [1,2].

Протоколи взаємодії об'єктів сьомого рівня отримали назву прикладних.

Стандарти прикладного рівня визначають:

- *концептуальну схему рівня*, що містить модель сервісу, наданого процесам, і операції, які при цьому слід виконувати;
- *предметну область*, тобто засоби для забезпечення взаємодії прикладних процесів;
- *функції та мови* для задоволення запитів прикладних процесів.

Згідно з цим на прикладному рівні виконуються такі операції:

- відкриття портів для прикладних процесів і встановлення асоціації з іншими процесами;
- закриття портів і ліквідація асоціації;
- запит на передачу блоків даних;
- надання кожному з процесів черги на передачу,
- здійснення передачі блоків даних;
- синхронізація передачі інформації;
- керування надзвичайними ситуаціями.

Таблиця 2.3. *Функції рівнів моделі взаємодії відкритих систем*

Рівень	**Функції**
7. Прикладний	Інтерфейс із прикладними процесами
6. Представницький	Узгодження подання й інтерпретація переданих даних
5. Сеансовий	Підтримка діалогу між вилученими процесами; забезпечення з'єднання й роз'єднання цих процесів; реалізація обміну даними між ними
4. Транспортний	Забезпечення наскрізного обміну даними між системами
3. Мережний	Маршрутизація; сегментування й об'єднання блоків даних; керування потоками даних; комутація
2. Канальний	Управління каналом передачі даних; формування кадрів; управління доступом до середовища передачі; передача даних по каналу; виявлення помилок у каналі і їхня корекція
1. Фізичний	Фізичний інтерфейс із каналом передачі даних; бітові протоколи модуляції й лінійного кодування

2.3. Протоколи рівнів моделі OSI

Таблиця 2.4. *Протоколи рівнів моделі OSI*

<table>
<tr><th colspan="2">Рівні моделі OSI</th><th>Протоколи</th><th>Реалізація</th><th>Залежність від технології</th></tr>
<tr><td>7</td><td>Прикладний</td><td rowspan="2">Протоколи верхнього рівня</td><td rowspan="5">Програмна</td><td rowspan="2">Мережно-незалежні протоколи</td></tr>
<tr><td>6</td><td>Представницький</td></tr>
<tr><td>5</td><td>Сеансовий</td><td rowspan="3">Протоколи середнього рівня</td><td></td></tr>
<tr><td>4</td><td>Транспортний</td><td></td></tr>
<tr><td>3</td><td>Мережний</td><td rowspan="3">Мережно-залежні протоколи</td></tr>
<tr><td>2</td><td>Канальний</td><td rowspan="2">Протоколи нижнього рівня</td><td rowspan="2">Апаратна</td></tr>
<tr><td>1</td><td>Фізичний</td></tr>
</table>

Три нижніх рівні фізичний, канальний і мережний є мереже-залежними. Протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі та з використаним комунікаційним устаткуванням.

Три верхні рівні *сеансовий*, *представлення* і *прикладний* вирішують задачі надання прикладних сервісів на підставі існуючої транспортної підсистеми.

Вони орієнтовані на застосування і мало залежать від технічних особливостей побудови мережі. На протоколи цих рівнів не впливають жодні зміни в топології мережі, заміна устаткування або перехід на іншу мережну технологію.

Транспортний рівень є проміжним, він приховує всі деталі функціонування протоколів нижніх рівнів від протоколів верхніх рівнів. Це дозволяє розробляти застосування, що не залежать від технічних засобів передавання повідомлень, які безпосередньо займаються транспортуванням.

Розрізняють протоколи нижнього, середнього і верхнього рівнів, а також стеки протоколів з апаратною та програмною реалізацією.

2.4. Системний опис мережевої архітектури

Рис. 2.3. Системний опис мережевої архітектури

Сукупність таких моделей будемо називати ***системним описом мережевої архітектури.***

- ***Топологічна модель*** **-** визначає розташування пунктів мережі та ліній зв'язку.
- ***Фізична модель*** **-** відображає фізичні пристрої та програмні засоби, в котрих реалізовано функціональні елементи мережі, фізичні середовища передавання сигналів.
- ***Організаційна модель*** **-** визначає тип, призначення, статус елементів мережі залежно від виконуваних ними функцій;
- ***Логічна модель*** **-** описує роботу мережі на рівні взаємодії мережевих функцій та правил встановлення зв'язку між кінцевими системами, взаємодіючими через телекомунікаційну мережу.

2.4.1. Топологічна модель

Топологією називається структура взаємозв'язків пунктів і з'єднуючих їх ліній

Розрізняють ***топології фізичних зв'язків і топології логічних зв'язків***.

Топологія фізичних зв'язків (Фізична топологія) – це граф, вершинами якого є вузли мережі, а ребрами – фізичні зв’язки між ними (лінії зв’язку).
Топологія фізичних зв'язків відображає схему з'єднань елементів мережі.

Логічна топологія відображає розподіл інформаційних потоків між вузлами

Фізична і логічна топологія мережі можуть неспівпадати між собою.

Фактично логічна топологія визначає алгоритм, згідно із яким мережеві вузли будуть здійснювати доступ до середовище передачі даних

Для дослідження топологічних особливостей мережі її зручно зобразити у вигляді графа.

Граф є моделлю топологічної структури мережі.

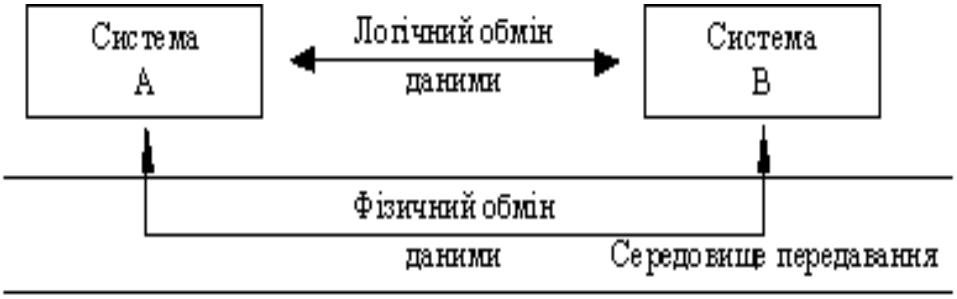


Рис. 2.4. Модель топологічної структури мережі

Топологія - це конфігурація фізичних зв'язків між вузлами мережі. Характеристики мережі залежать від типу встановлюваної топології. Зокрема, вибір тієї чи іншої топології впливає:

- на склад необхідного мережевого обладнання;
- на можливості мережевого обладнання;
- на можливості розширення мережі;
- на спосіб управління мережею.

На практиці використовуються шість базових топологій:

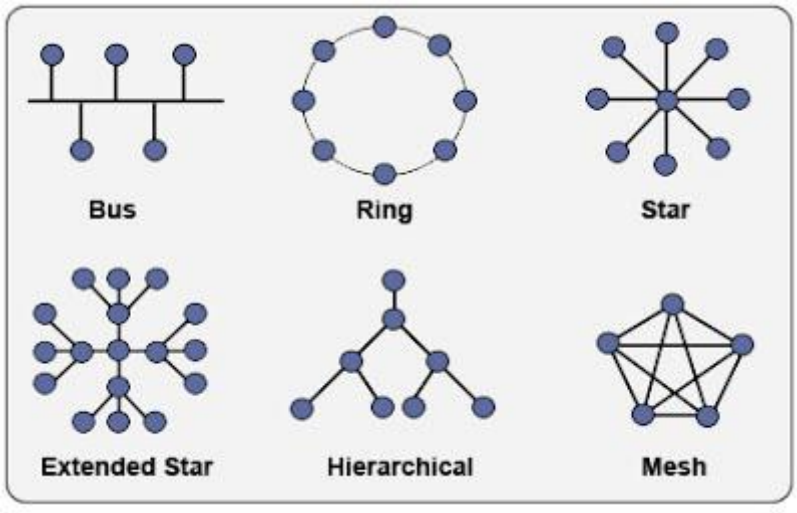


Рис. 2.5. Різновиди топологій мереж

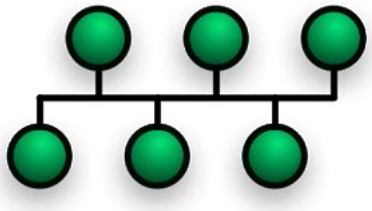
- Зіркоподібна;
- Кільцева;
- Шинна;

- Змішан;
- Деревоподібна;
- Повнозв’язна.

Затримка мережі - це час передачі інформаціфйних повідомлень між абонентами, тобто час між видачею повідомлення з абонента-джерела і його прийомом абонентом-одержувачем (адресатом).

Перепускна здатність - це максимальне число бітів абонентських повідомлень, що можуть передаватися через мережу в одиницю часу.

Топологія шина (bus)



Спільна **шина** є вельми розповсюдженою топологією для локальних мереж. У цьому випадку вузли підключаються до одного коаксіального кабелю. Передана інформація може поширюватися в обидва боки. Канал закінчується з двох сторін пасивними термінаторами, що поглинають передані сигнали, оскільки за своєю природою передача в такій мережі є широкомовною.

Вузли підключаються до шини безпосередньо до з’єднувачів кабельних секцій або за допомогою спеціальної урізки, що просто проколює коаксіальний кабель до контакту з центральним провідником.

Переваги:

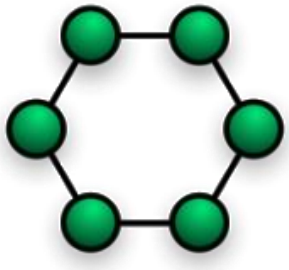
- Налаштування є гранично простий для будь-якого просунутого користувача.
- Система досить просто встановлюється і при цьому обумовлює мінімум фінансових витрат, якщо всі робочі станції розташовуються на невеликій відстані між собою.

- Якщо ламається або ж починає давати збій якась конкретна станція в мережі, всі інші продовжують працювати в колишньому режимі без будь-яких проблем.

Недоліки:

- Якщо виникає неполадка в якому-небудь місці, моментально виходить з ладу повністю вся мережа.
- Досить складно знайти які-небудь неполадки в разі їх виникнення.
- Досить низька продуктивність в порівнянні з іншими технологіями. Це обумовлюється тим, що топологія мережі «шина» передбачає одночасну передачу даних тільки з одного комп'ютера, а якщо ж кількість робочих станцій збільшується, паралельно знижується продуктивність мережі.
- Погана масштабованість. Щоб додати нові робочі станції, потрібно повністю замінити ділянки вже використовується "шини".

Топологія кільце (ring)



У мережі з кільцевою топологією вузли підключаються до повторювачів сигналів, зв’язаних у односпрямоване кільце, чи до двох повторювачів, зв’язаних у два різноспрямованих кільця.

У мережах з кільцевою конфігурацією дані передаються по колу від одного комп'ютера до іншого — як правило, в одному напрямку. Якщо комп'ютер розпізнає дані як «свої», то він копіює їх собі у внутрішній буфер.

У мережі з кільцевою топологією необхідно вживати спеціальних заходів, щоб у разі виходу з ладу чи відключення якоїсь станції не перервався канал зв'язку між іншими станціями.

Підключення нових абонентів в «кільце» звичайно зовсім безболісно,

хоча й вимагає обов’язкової зупинки роботи всієї мережі на час підключення. Як і у випадку топології «шина», максимальна кількість абонентів у кільці може бути досить велика (до тисячі й більше). Кільцева топологія звичайно є самою стійкою до перевантажень, вона забезпечує впевнену роботу із самими великими потоками переданої по мережі інформації, тому що в ній, як правило, немає конфліктів (на відміну від шини), а також відсутній центральний абонент (на відміну від зірки).

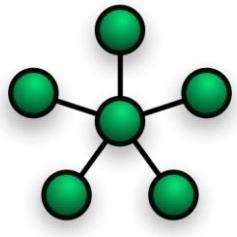
Переваги:

- Комп'ютери досить просто об'єднуються в мережу.
- Практично немає ніякої необхідності в тому, щоб використовувати додаткове устаткування.
- Можна домогтися стабільної роботи без якого-небудь помітного падіння швидкості транслювання даних при серйозній завантаженні мережі.
- Будь-яка робоча станція повинна активно використовуватися в процедурі передачі даних, і якщо зламається хоча б один комп'ютер, або ж у певному місці обірветься кабель, вся система повністю перестане функціонувати.
- Якщо буде підключатися нова робоча станція, мережа потрібно на певний час вимкнути, так як потрібно розмикання кільця в процесі установки нового обладнання.
- Система відрізняється досить складною конфігурацією і налаштуваннями.
- При виникненні тих чи інших несправностей навіть фахівцям досить складно знайти, у чому саме полягає проблема.

Недоліки:

- низька надійність мережі, оскільки відмова будь-якого вузла тягне за собою відмову всієї системи;
- для підключення нового клієнта необхідно відключити роботу мережі;
- при великій кількості клієнтів швидкість роботи в мережі сповільнюється, так як вся інформація проходить через кожнй вузол.

Топологія зірка (star)



У мережі із зіркоподібною топологією кожен абонент, що посилає і (чи) приймає інформацію, приєднаний одним чи двома виділеними каналами зв’язку до єдиного центрального вузла, через який проходить весь мережевий трафік.

Кожен вузол підключається окремим кабелем до загального пристрою, який має назву концентратор та розташовується в центрі мережі.

У функції концентратора входить спрямування переданої комп'ютером інформації одному чи всім іншим комп'ютерам мережі. Крім того, концентратор може відігравати роль інтелектуального фільтра інформації, що надходить від вузлів у мережу, і за необхідності блокувати заборонені адміністратором передачі.

Переваги:

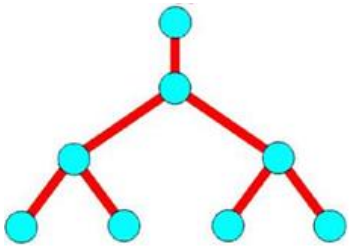
- Якщо ламається якась конкретна станція (або ж пошкоджується її кабель), на роботі, в цілому всієї мережі це ніяк не позначається, тобто все інше обладнання продовжує стабільно працювати.
- Прекрасна масштабованість. Для того щоб підключити нову робочу станцію, потрібно просто прокласти окремий кабель від комутатора.
- Досить просто можна знайти, і після цього усунути несправності або ж які-небудь обриви в мережі.
- Гранично висока продуктивність, особливо якщо порівнювати з аналогічними варіантами топології.
- Ідеальна простота настройки і адміністрування усього обладнання.
- В мережу без праці можна вбудувати додаткові пристрої.
- Якщо ламається центральний комутатор, вся мережа перестає працювати.

- Щоб використовувати мережеве обладнання, потрібно виділити також додаткові витрати, так як потрібне придбання окремого пристрою, до якого будуть підключатися всі комп'ютери, підключені до мережі.
- Кількість робочих станцій обмежується кількістю портів у використовуваному центральному комутаторі.

Недоліки:

- відмова центрального вузла призводить до відмови працездатності мережі;
- вартість реалізації, в якій має бути центральний вузол та більша ніж у шинній топології кількість кабелю;
- обмежена кількість з’єднань з центральним вузлом, яка залежить від кількості роз’ємів.

Топологія дерево (tree, hierarhical)



Деревоподібні мережі будуються на базі техніки кабельного телебачення, тобто з використанням таких засобів зв’язку, як кінцеві частотні ретранслятори, розщеплювачі-об’єднувачі, двонапрямлені посилювачі, відгалужувачі, радіочастотні модеми, фільтри тощо.

Надійність деревоподібної мережі забезпечується структурним резервуванням її зв’язкових пристроїв, час напрацювання на відмову яких може складати до 400 тис. год.

Окремий вид деревоподібної топології – топологія «точка-точка».

Переваги:

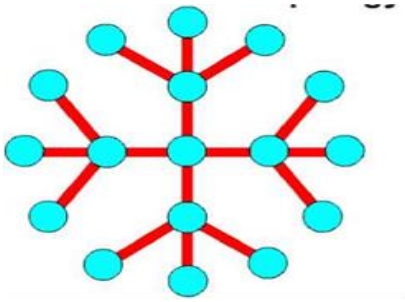
- відносно велика протяжність (до 50 км) та можливість паралельної передачі мови, даних та зображень, що забезпечується за рахунок частотного ущільнення каналів (у описаних вище мережах використовується часове ущільнення каналів)

Недоліки:

- можливості щодо нарощування деревоподібних мереж досить таки обмежені через високу вартість їх встановлення та складність їх аналогових компонентів, що вимагають ще й постійного налагоджування.

Розширена зіркоподібна топологія

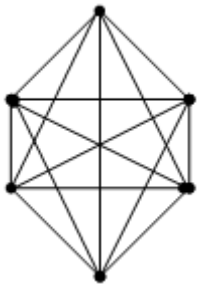
Топологія ***розширена зірка*** (*Extended Star*) це топологія при якій до одного центрального вузла приєднуються інші вузли, причому до кожного з них може бути під'єднана зіркоподібна топологія.



Повнозв’язна топологія

Повнозв'язна топологія - топологія комп'ютерної мережі, в якій кожна робоча станція підключена до всіх інших. Цей варіант є громіздким і неефективним, незважаючи на свою логічну простоту. Для кожної пари повинна бути виділена незалежна лінія, кожен комп'ютер повинен мати стільки комунікаційних портів скільки комп'ютерів в мережі. Найчастіше ця топологія використовується в багатомашинних комплексах або глобальних мережах при

малій кількості робочих станцій.



Переваги:

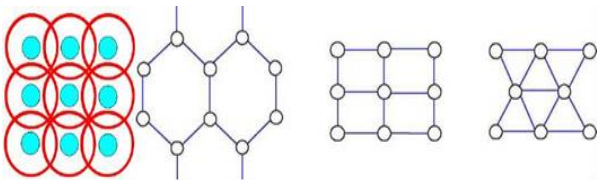
- розрив кабелю не відбивається на працездатності мережі.

Недоліки:

- надто великі витрати кабелю;
- громіздка та неефективна мережа.

Комірчаста (стільникова) топологія

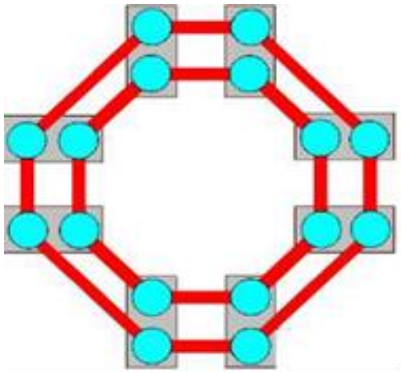
Решітка - це топологія, у якій вузли утворюють регулярну багатовимірну решітку. При цьому кожне ребро решітки паралельно її осі і з'єднує два суміжних вузла вздовж цієї осі. Одновимірна решітка - це ланцюг, що з'єднує два зовнішніх вузла (що мають лише одного сусіда) через деякий кількість внутрішніх (у яких по два сусіди - ліворуч і праворуч). При з'єднанні обох зовнішніх вузлів виходить топологія "кільце". Дво- і тривимірні решітки використовуються в архітектурі суперкомп'ютерів.



Кожен пункт сегмента має безпосередній зв'язок і з невеликою кількістю пунктів, найближчих за відстанню**.**

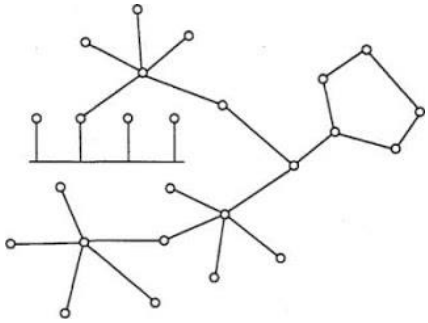
Топологія подвійне кільце

Топологія *подвійне кільце* (*Dual Ring Apology*) – це мережева топологія, в якій утворюється подвійні з'єднання між парами вузлів, при яких інформаційний потік направляється в двох протилежних напрямках



Змішана топологія (mesh)

Включає в себе декілька топологій, але зазвичай це "розширена зірка" або "дерево зірок".



Мережа зі змішаною топологією є, як правило, неповнозв’язаною мережею вузлів комутації повідомлень (пакетів), до яких приєднуються кінцеві системи. Усі канали зв’язку є виділеними двоточковими. Такого роду зв’язки найбільш часто використовуються у великомасштабній та регіональній обчислювальній мережах, але іноді вони застосовуються й у локальних обчислювальних мережах. Змішану мережу можна розглядати як зіркоподібну мережу, у якої центральний вузол має розподілену архітектуру.

У вузлах комутації змішаної мережі звичайно реалізується статична (фіксованими шляхами) чи динамічна (адаптивна) маршрутизація повідомлень.У результаті для того ж числа кінцевих систем вартість змішаної

мережі вища ніж вартість будь-якої іншої мережі.

Надійність змішаної мережі забезпечується таким з'єднанням вузлів комутації каналами зв'язку, щоби між будь-якою парою кінцевих систем були наявні щонайменше два шляхи передачі повідомлень. Уведення надлишкових каналів між вузлами комутації, тобто збільшення зв'язності мережі, - стандартний спосіб підвищення надійності.

2.4.2. Фізична модель

Під **фізичною структурою мережі** будемо розуміти склад її активного та пасивного обладнання та топологію його розміщення в просторі.

Активне мережеве обладнання кінцеве і комунікаційне обладнання, функціонування якого забезпечується за рахунок споживання електроенергії від зовнішніх джерел живлення. Активне мережеве обладнання виконує комплекси тих функцій мережі, які реалізуються в апаратурі.

Пасивне обладнання мережі, на відміну від активного, немає потреби в джерелах електроживлення й містить у собі кабельну систему, телекомунікаційні роз'єми, комутаційн панелі, комутаційні шнури, монтажне обладнання тощо.

Під ***апаратурою (Equipment)*** розуміють активне обладнання, в якому функції можуть бути реалізовані як у вигляді апаратного забезпечення, так і у вигляді програмного забезпечення.

Елементами моделі апаратурної реалізації є такі:

- ***Апаратне забезпечення*** (*Hardware*) - обладнання, в якому одна або декілька функцій реалізовано фізично.
- ***Програмне забезпечення*** (*Software*) – один або декілька програмних модулів, які представляють собою реалізацію одного або декількох об'єктів.
- ***Фізичний інтерфейс*** *(Phisical interface*) – фізичне середовище (проводи) для передачі сигналів між різною апаратурою.

Сукупність різних пристроїв, потенційн призначених для використання в мережевих середовищах, називається **парком апаратури активного обладнання мережі.**

Активне обладнання мережі

Активне обладнання мереж зв'язку складається з пристроїв, які використовуються для організації мережевих пунктів, а також інтерфейсних пристроїв, які забезпечують спряження апаратури з лініями зв'язку.

У технічній літературі набули вжитку такі позначення класів апаратури: ***DTE, DCE і DTE/DCE.*** Охарактеризуймо кожен з них більш детально.

Усі пристрої в мережі, які функціонують як джерела та приймачі даних на фізичному рівні моделі OSI/ISO,визначаються як клас DTE (Data Terminal Equipment) – кінцева апаратура даних (КАД). ***У термінології електрозв'язку дана апаратура називається ще «кінцевим обладнання даних» (КОД).***

Разом і з функцією формування даних, у реалізації якої в основному бере участь програмне забезпечення, в DTE здійснюється також функція керування потоком даних для узгодження роботи джерелай приймача. Ця функція, як правило, виконується апаратно.

Відмінною особливістю обладнання класу DTE є те, що воно не належить до складу устаткування ліній зв'язку.

Для забезпечення обміну даними між пристроями DTE через канали зовнішніх телекомунікацій необхідно використовувати фізичні інтерфейсні пристрої, які здійснюють обробку даних з урахуванням вимог передачі каналом певного стандарту. Ці пристрої забезпечують не тільки протокол фізичного рівня, а й фізичні засоби приєднання до середовища передачі, а тому вважаються устаткуванням лінії зв'язку.

Обладнання, що забезпечує сполучення DTE з каналами зв'язку, визначається як клас DCE (Data Communication Equipment) – апаратура передачі даних (АПД). Пристрої DCE працюють на фізичному рівні, відповідаючи за передачу й прийом сигналів потрібної форми та потужності в середовищі передачі, й не можуть розглядатися в якості джерел і приймачів даних.

Визначаючи чіткіше, варто зауважити, що мережеве обладнання важко розподілити за конкретними класами DTE та DCE. Наприклад, мережевий адаптер можна вважати як складовою комп'ютера (DTE), так і частиною каналу

зв'язку (DCE).

У кожному сегменті інформаційної мережі DTE набуває функцій будь-якого джерела даних, поданих у форматі кадру канального рівня. Отже, це може бути й мережевий адаптер, і вихідний порт комутатора, й вихідний порт маршрутизатора. Хоча кадр даних спочатку продукується мережевим адаптером комп'ютера, а через комутатор або маршрутизатор відбувається його трансляція, для сегменту мережі, під'єднаного до вихідного порта комутатора або маршрутизатора, цей кадр є новим. Отже, ***вихідний порт*** і комутатора, і маршрутизатора стає джерелом кадрів і може розглядатися як вихід пристрою DTE.

Зважаючи на сказане вище так і комунікаційні пристрої, як мости, комутатори і маршрутизатори розглядають у межах змішаного класу – класу DTE/DCE, де розрізняють відповідні ***типи портів:*** DTE або DCE. Для цих портів принципами функціонування є такі: для порту DTE сигнал даних передавача є вихідним, а сигнал даних приймача - вхідним; для порту DCE – відповідно навпаки.

Клас DTE/DCE – змішаний клас (комунікаційні пристрої-мости, комутатори і маршрутизатори)

Пасивне обладнання мережі

Пасивне обладнання використовується для побудови комп’ютерних кабельних систем мережі. Кабельна система – це складний технічний об'єкт, який будується відповідно жорстким вимогам загальноприйнятих стандартів. До нього належать лінійно-кабельні споруди ліній зв'язку, регенераційне обладнання, тощо. Створення й правильна експлуатація такого об'єкта вимагають відповідного рівня кваліфікації проектувальників, монтажників і обслуговуючого персоналу.

Обладнання кабельних систем для мереж підприємств є набором компонентів і аксесуарів структурованих кабельних систем (СКС) і складається з кабелів, роз'ємів телекомунікаційних та інформаційних розеток, монтажного обладнання, настінних коробів для прокладки кабелів горизонтальної розводки,

закладних для прокладання кабелів вертикальної розводки та ін.

Організаційна структура мережі зв'язку визначає ***рольове призначення*** й ***статус*** мережевих елементів та утворених ними структурних компонентів залежно від поставленого завдання та займаного місця в мережі. Рольове призначення характеризує, умовно кажучи, «права та обов'язки» елементів або виділених структурних фрагментів мережі під час реалізації покладених на них функціональних завдань, а статус – рівень їх значимості відповідно до ієрархічної приналежності.

Організаційну структуру мережі можна порівняти, наприклад, із моделлю адміністративного устрою підприємства. Така модель узагальнено складається з адміністрації та виробничих підрозділів різного призначення. У межах цієї структури визначено посади й функції співробітників, які беруть участь у виробничому процесі, ієрархію адміністративного управління та принципи структуризації підприємства (наявність робочих груп, відділів, філій та ін.). Крім того важливими чинниками є виробничі завдання, які вирішуються кожним підрозділом, а також його масштаб.

Елементи моделі організаційної структури

Пункти та лінії зв'язку передусім розглядаються як елементи моделі організаційної структури мережі.

Елементами організаційної структури мережі є: пункти та зв'язуючі системи передавання (напрямні системи).

Однак особлива увага зосереджується не на їх розміщенні в просторі, а їх рольове призначення та статус, яких вони набувають в рамках моделі організаційної структури мережі.

Пункти мережі поділяються на кінцеві і вузлові**.**

Кінцеві пункти (КП) (End points) – це пункти, в яких розміщено термінальне обладнання користувачів і кінцеві системи мережі (сервери, на яких зосереджено інформаційні ресурси й застосування, у тому числі

застосування системи керування мережею).

Пункти, призначені для розміщення термінального обладнання користувачів, яке забезпечує доступ в мережу, функціонують у ролі абонентських пунктів (АП). Пункти, у яких зосереджено інформаційні ресурси, називаються інформаційними центрами (ІЦ), а пункти системи керування відповідно – центрами керування (ЦК).

У кінцевих пунктах телекомунікаційна мережа представлена пристроєм мережевого закінчення (Network Termination Unit, NTU), або просто мережевим закінченням (Network Termination, NT),яке в організаційній структурі набуває статусу ***точки присутності телекомунікаційної мережі.*** Прикладом цього є звичайна телефонна розетка, інформаційна розетка з телекомунікаційним роз'ємом для під'єднання комп'ютера.

Вузловий пункт (Node Points) – це пункт мережі, в якому сходяться дві і більше ліній зв'язку.

У вузловому пункті зазвичай розміщується комунікаційне (мережеве) обладнання, за допомогою якого можуть виконуватися такі функції, як ***концентрація, розподілення, мультиплексування, комутація*** та ***маршрутизація.***

Концентрація (Concentration) передбачає поєднання декількох невеликих за потужністю вхідних інформаційних потоків з метою отримання більш потужного вихідного потоку. Функція може бути реалізована в спеціалізованому пристрої на основі ущільнення (асинхронне мультиплексування). Слід зауважити, що в концентраторі для локальних мереж, який має назву «хаб», ця функціявиконується досить умовно. Повідомлення, яке надходить на один з входів хаба, передається одночасно на всі виходи.

Розподілення (Distribution) – відгалуження від концентрованого вхідного інформаційного потоку малих за потужністю вихідних потоків і розподіл їх між виходами. Функція реалізується в пристроях, які називаються

відгалужувані.

Мультиплексування (Multiplexing) забезпечує можливість передачі декількох потоків інформації однією лінією, що здійснюється закріпленням за кожним із них фіксованої частини ресурсу лінії (смуги пропускання або часу зайняття). Фіксований розподіл ресурсу лінії залишається незмінним навіть у періоди відсутності інформації. Зворотна функція **- *демультиплексування.*** Реалізація в комунікаційних пристроях (мультиплексорах) функції мультиплексування завжди поєднується з демультиплексуванням.

Комутація (Switching) є процесом встановлення зв'язку між входами та виходами комутаційного пристрою на основі аналізу адресної інформації повідомлень і використання інформації відповідних таблиць комутації. Комутація може бути оперативною (на час передачі одного повідомлення) та довготривалою, яка здійснюється шляхом кросування ліній, які сходяться у вузловому пункті.

Маршрутизація (Routing) – це поєднання процедур пошуку зв'язних шляхів (маршрутів) між вузлами мережі з метою формування таблиць маршрутизації та встановлення зв'язку між входами та виходами пристрою на основі адресної інформації повідомлень та з урахуванням вибору найкращого (за обраним критерієм) маршруту проходження повідомлення мережею.

У комунікаційному пристрої може бути реалізована одна з перераховани хфункцій, саме тоді цей пристрі й відповідно називається або концентратором, або мультиплексором, або комутатором, або маршрутизатором та ін. Можливим є також суміщення декількох функцій в одному пристрої як, наприклад, у маршрутизуючому комутаторі, АТС.

Рольове призначення вузлових пунктів в моделі організаційної структури

Вузловий пункт відносно кінцевих пунктів, які він обслуговує, незалежно від статусу, може виступати в ролі: ***опорного вузла, транзитного вузла*** або

опорно-транзитного вузла.

Якщо вузловий пункт забезпечує проходження трафіку тільки між КП конкретної групи, то відносно цих КП він виступає в ролі **опорного вузла.**

Якщо через вузловий пункт проходить трафік від деякої групи КП до будь-яких інших КП мережі, то він виступає в ролі **транзитноговузла.**

Якщо вузловий пункт забезпечує проходження трафіку як внутрішнього, так і зовнішнього обміну деякого конкретного числа КП мережі, то відносно цих КП він виступає у ролі **опорно-транзитного вузла.**

У практиці побудови та експлуатації телекомунікаційних та інформаційних мереж давно склалася й використовується термінологія, яка досить чітко відбиває рольове призначення вузлових пунктів.

Вузловий пункт, у якому забезпечується доступ користувачів до служб мережі з метою отримання телекомунікаційних та інформаційних послуг, називають ***сервісним вузлом (Service Node, SN).*** Це може бути вузол рівня доступу, розподілу або ядра.

Вузловий пункт, де забезпечується з'єднання сегментів телекомунікаційної мережі, наприклад, мережі доступу та транспортної мережі, називається ***вузлом доступу (Access Node, AN).***

Вузловий пункт, у якому забезпечується підключення сервіс-провайдера національного рівня в глобальну інформаційну мережу Інтернет, називається ***точкою мережевого доступу (Network Access Point, NAP).*** Це вузловий пункт рівня ядра. Через NAP зорганізується спілкування клієнтів одного національного провайдера з клієнтами інших національних провайдерів.

Сервіс-провайдер національного рівня, як правило, має в декількох регіонах вузлові пункти, які називаються ***точками присутності (Points of Presents, POP).*** До POP під'єднуються провайдери регіонального рівня, які, у свою чергу, розміщують у різних місцях регіону свої точки присутності для підключення провайдерів нижчого рівня або корпоративних клієнтів. Такі вузлові пункти мають статус рівня розподілу. Точки присутності провайдерів,

де забезпечується підключення індивідуальних клієнтів, мають статус рівня доступу.

Порядок співвідношення між елементами (їх статус) в моделі організаційної структури визначається рівнями їхієрархії.

Найнижчий рівень займають абонентські пункти. Статус вузлових пунктів визначається відповідно ***рівнем доступу, розподілу та ядра.***

Абонентські пункти зазвичай поєднуються до вузлових ***пунктів рівня доступу.*** Таким чином для них реалізується право ***доступу в мережу*** (до її ресурсів).

Призначення та статус вузлових пунктів ***рівня розподілу (Aggregation)*** визначається забезпеченням інформаційного обміну між абонентськими пункти, під'єднаними до різних вузлових пунктів рівня доступу. Залежно від способу структуризації мережі, рівень розподілу матимеде кілька підрівнів. Вузлові пункти всіх підрівнів розподілу виконують функцію ***концентрації трафіку*** у висхідних напрямах і функцію ***розподілу –*** у низхідних.

У вузлових пунктах ***рівня ядра*** інформаційні потоки досягають максимальної концентрації та перерозподіляються між усіма іншими пунктами мережі. ***Вузлові пункти рівня ядра*** мають найвищий статус, оскільки вони забезпечують зв'язність мережі в цілому за рахунок об'єднання вузлових пунктів рівня розподілу.

Точка підключення кінцевих систем (інформаційних центрів мережі) може бути організована у вузловому пункті будь-якого рівня. Це визначається масштабом контингенту користувачів, які мають загальну потребу у зверненні до інформаційного ресурсу. Чим вище сягає рівень підключення ресурсу, тим ширшою є його доступність. Теж відноситься і до пунктів розміщення обладнання системи керування мережею – центрів керування (ЦК). Чим вищим є рівень підключення, тим ширшою зона моніторингу технічного стану елементів мережі.

Лінії зв'язку в моделі організаційної структури також отримують

відповідний статус.

Лінії, які з'єднують абонентські пункти з відповідним вузловим пунктом рівня доступу, мають найнижчий статус і називаються ***абонентськими лініями.***

Лінії, які з'єднують вузлові пункти між собою, називаються ***магістральними.*** Чим вищим є рівень ієрархії з'єднуваних магістралями вузлових пунктів, тим вищим-статус самих магістралей, і, відповідно, вимоги до їх пропускної здатності, надійності.

На логічному рівні мережу зв'язку описують такими моделями:

- Функційна модель;
- Протокольна модель;
- Модель програмного забезпечення.

2.4.3. Функційна модель

Функційна модель – це абстрактний опис мережі зв'язку, що не залежить від принципів її фізичної реалізації.

Функційна модель відображає взаємозв'язок функцій, які виконуються в мережі, які в даному випадку розглядаються як елементи моделі.

Функція – це певний логічний елемент, що виконує конкретне завдання в мережі.

Функції реалізуються в наступних варіантах:

- У вигляді апаратних засобів;
- У вигляді програмного продукту.

Поняття «функція», що використовується в телекомунікаціях, традиційно передбачало реалізацію в апаратному забезпеченні. Однак, завдяки потужному розвитку індустрії програмного забезпечення, виникла можливість реалізації функцій програмним способом. ***Функції, реалізовані у вигляді програмних***

продуктів, прийнято називати об'єктами. Хоча, строго кажучи, обидва поняття є синонімами, надалі все-таки будемо дотримуватися цього умовного розмежування, підкреслюючи таким чином, що в мережі реалізовано програмно, а що апаратно.

Об'єкт – це функції, реалізовані у вигляді програмних продуктів.

Застосовання (Application) – це програми користувачів прикладного рівня, які підтримує мережа.

Розрізняють такі основні типи функцій мережі зв'язку:

- **Прикладні функції** - об'єкти застосовань користувачів;
- **Функції обробки та зберігання даних** - об'єкти, що забезпечують виклик об'єктів застостосовань, їх взаємодію, а також витяг необхідних даних або розміщення їх у базу даних;
- **Функції керування послугами** - об'єкти, що дозволяють формувати послуги, необхідні користувачами, управляти ресурсами мережі, пов'язаними з їх наданням, і взаємодією користувачів з цими послугами;
- **Комунікаційні функції** – транспортні функції, функції керування передачею потоків даних, функції керування телекомунікаційними послугами;
- **Функції керування мережею** - об'єкти, які здійснюють керування роботою мережі в цілому (моніторинг дієздатності елементів мережі, збір статистики про проходження сигналів, вирішення аварійних і неординарних ситуацій та ін.).

Порядок і правила взаємодії між функціями та об'єктами мережі формують ***зв'язки*** між елементами у функціональній моделі. Повна специфікація такої взаємодії називається **логічним інтерфейсом.**

Логічний інтерфейс є поняттям, що охоплює як набір правил поведінки взаємодіючих елементів, так і формат подання інформації, якою вони обмінюються.

Логічний інтерфейс між об'єктами одного типу називається **протоколом.**

Логічний інтерфейс між комунікаційними функціями отримав назву **еталонної точки телекомунікаційної мережі.**

2.4.4. Протокольна модель

Протокольна модель опису є роботу мережі зв'язку на рівні правил взаємодії (протоколів) об'єктів (функцій) та ***функціональних модулів, розосереджених*** на різних кінцевих системах.

Типовим прикладом протокольної моделі є Еталонна модель взаємодії відкритих систем (Open System Interconnection, OSI)

Модель програмного забезпечення

Сучасне мережеве програмне забезпечення є структурованим. Основні функції й уся архітектура зв'язку (протокольні моделі) по суті реалізуються в програмному забезпеченні мережі.

Аналіз програмної структури дозволяє розглянути ієрархію мережевого програмного забезпечення. Елементами цієї структури є програмні модулі, в яких реалізовано об'єкти та логічні модулі мережі.

Ієрархія програмного забезпечення (ПЗ) може бути подана таким чином:

Прикладне ПЗ;

- **Проміжне ПЗ;**
- **Базове ПЗ.**

У прикладному ПЗ реалізовано об'єкти застосовань. Розрізняють два типи застосовань, які впливають на структуру організації ПЗ – локальнообмежені і розподільчі.

Локально обмежене застосовання інсталюється, викликається, керується й виконується в межах однієї кінцевої системи та не вимагає залучення комунікаційних функцій. Прикладом може бути редагування документа при підготовці тексту на комп'ютері користувача (терміналі користувача).

Розподільче застосовання складається з кількох компонентів, які можуть виконуватися в різних кінцевих системах а, отже, вимагають організації

взаємодії цих кінцевих систем. Наприклад, спільне редагування тексту значної за обсягом публікації користувачами, які знаходяться на віддалі.

Компоненти розподільчого застосування можуть неодноразово використовуватися іншими застосуваннями. У цьому випадку вони стають об'єктами проміжного ПЗ і підтримують послуги, пов'язані з інтелектуальними можливостями мережі.

Проміжне ПЗ реалізує в мережі функції керування послугами та функції адміністративного керування мережею. Об'єкти обох груп ПЗ аналогічно до компонентів розподільчих застосовань взаємодіють за допомогою комунікаційних функцій мережі

Базове ПЗ призначено для забезпечення об'єктів прикладного ПЗ та проміжного ПЗ виконанням спільних дій з іншими об'єктами за допомогою взаємодії середовища з комунікаційними функціями мережі й логічними інтерфейсами користувачів. Організація цього середовища здійснюється уніфікованими програмними комплексами, які називаються мережевими операційними системами. Від того, які концепції керування ресурсами покладено в основу мережевої ОС, залежить ефективність роботи не тільки об'єктів прикладного та проміжного ПЗ, але й мережі в цілому. Стандартами мережевих ОС де–факто на сьогодні стали системи UNIX і мережеві версії Windows. Логічні компоненти комунікаційних функцій, реалізованих програмно, які забезпечують підтримання зв'язку між віддаленими об'єктами, також розглядають як функції базового ПЗ.

До базового ПЗ належать також об'єкти обробки та зберігання даних, реалізовані в таких програмних комплексах, як СКБД (системи керування базами даних), базове ПЗ сервера обробки транзакцій та ін.

Тип взаємодії між об'єктами визначається типом об'єктного інтерфейсу, який є подібним до протоколу та функціональної еталонної точки.

Розрізняють такі типи об'єктних інтерфейсів (програмних інтерфейсів):

- **Прикладний протокол (Application Protocol, AP) –** логічний інтерфейс

між прикладними об'єктами;

- **Інтерфейс прикладних програм (Application Program Interface, API) –** логічний інтерфейс між прикладними об'єктами та об'єктами проміжного ПЗ, які підтримують прикладні об'єкти;
- **Протокол проміжного ПЗ (Managing Protocol, MP) –** логічний інтерфейс між об'єктами проміжного ПЗ;
- **Інтерфейс базових програм (Base Program Interface, BPI) –** логічний інтерфейс між об'єктами проміжного та базового програмного забезпечення, які підтримують об'єкти проміжного ПЗ;
- **інтерфейс "людина-комп'ютер" (User – Computer Interface, UCI) –** логічний інтерфейс між користувачем і, головним чином, об'єктами базового ПЗ, проте він може включати в себе також логічний інтерфейс з об'єктами проміжного ПЗ і навіть об'єктами застосовань.

Мережеве програмне забезпечення є ресурсом, яке бере участь в організації платформ надання послуг, а з цього випливає, що композиційним принципам об'єднання програмних модулів, які принципам побудови функціональної моделі мережі, притаманна така ж специфіка динамізму, які принципам побудови функціональної моделі мережі.

2.5. Основні характеристики сучасних комп'ютерних мереж

Якість роботи мережі характеризують такі властивості: продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість.

До основних характеристик ***продуктивності*** мережі відносяться:

• ***час реакції*** - характеристика, яка визначається як час між виникненням запиту до якого-небудь мережевого сервісу і отриманням відповіді на нього;

• ***пропускна здатність*** - характеристика, яка відображає об'єм даних, переданих мережею в одиницю часу;

• ***затримка передачі*** - інтервал між моментом надходження пакету на вхід якого-небудь мережевого пристрою і моментом його появи на виході цього пристрою.

Для ***оцінки надійності*** мереж використовуються різні характеристики, в тому числі:

- ***коефіцієнт готовності,*** що означає частку часу, протягом якого система може бути використана;
- ***безпеку,*** тобто здатність системи захистити дані від несанкціонованого доступу;
- ***відмовостійкість*** - здатність системи працювати в умовах відмови деяких її елементів.

Розширюваність означає можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків, сервісів), нарощування довжини сегментів мережі і заміни існуючої апаратури більш потужною.

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

Прозорість - властивість мережі приховувати від користувача деталі свого внутрішнього устрою, спрощуючи тим самим його роботу в мережі.

Керованість мережі має на увазі можливість централізовано контролювати стан основних елементів мережі, виявляти і вирішувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності і планувати розвиток мережі.

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

Контрольні питання до розділу

1. Які основні функції ралізує фізичний рівень моделі OSI?

a. *синхронізація по кодовим комбінаціям;*
b. *реалізація інтерфейсу з середовищем передачі;*
c. *ідентифікація приймальної або передаючої інформації;*
d. *встановлення й роз'єднання з'єднань;*
e. *перетворення сигналів.*

2. Які основні функції ралізує канальний рівень моделі OSI?
   a. *побудова віртуальних каналів;*
   b. *розбивка потоку інформації на кадри;*
   c. *ідентифікація приймальної або передаючої інформації;*
   d. *реалізація інтерфейсу з середовищем передач;*
   e. *перетворення інформації.*
3. Які основні функції ралізує мережний рівень моделі OSI?
   a. *побудова віртуальних каналів;*
   b. *комутація;*
   c. *ідентифікація приймальної або передаючої інформації;*
   d. *реалізація інтерфейсу з середовищем передач;*
   e. *маршрутизація.*
4. Які основні функції ралізує транспортний рівень моделі OSI?
   a. *корегування помилок в кодовій комбінації;*
   b. *контроль якості обслуговування;*
   c. *ідентифікація приймальної або передаючої інформації;*
   d. *встановлення з'єднання;*
   e. *маршрутизація.*
5. Які основні функції ралізує представницький рівень моделі OSI?
   a. *перетворення синтаксису;*
   b. *перетворення інформації;*
   c. *сеанс передачі інформації;*
   d. *перетворення формату;*
   e. *запрос встановлення сеансу.*
6. Які основні функції ралізує сеансовий рівень моделі OSI?
   a. *керування сеансом зв'язку;*
   b. *контроль якості обслуговування;*
   c. *сеанс передачі інформації;*
   d. *діалог між двома комунікаційними пристроями;*
   e. *маршрутизація.*
7. Які основні функції ралізує прикладний рівень моделі OSI?
   a. *керування надзвичайними ситуаціями;*
   b. *контроль якості обслуговування;*
   c. *сеанс передачі інформації;*
   d. синхронізація передачі інформації;
   e. *надання кожному з процесів черги на передачу.*
8. Які принципи взяли за основу при розробці еталонної моделі OSI?
9. Наведіть послуги служби фізичного рівня.
10. Які мережні протоколи відносяться до протоколів канального рівня?
11. Наведіть визначення віртуального каналу.
12. Скільки класів з'єднань передбачає транспортний рівень моделі OSI?

13. Скільки типів мережних з’єднань використовується на транспортному рівні?
14. Наведіть послуги сеансової служби.
15. Що визначають стандарти прикладного рівня?
16. Які протоколи моделі OSI є мережно-незалежними, а які мережно-залежні?
17. Системний опис мережевої архітектури є сукупністю наступних моделей:
    a. *технологічна модель побудови;*
    b. *логічна модель побудови;*
    c. *інформаційна модель побудови;*
    d. *топологічна модель побудови;*
    e. *фізична модель побудови;*
    f. *організаційна модель побудови.*
18. Що собою представляє топологічна модель системним описом мережевої архітектури?
19. Що собою представляє фізична модель системного опису мережевої архітектури?
20. Що собою представляє організаційна модель системного опису мережевої архітектури?
21. Що собою представляє логічна модель системного опису мережевої архітектури?
22. Чим відрізняється між собою логічна та фізична топології?
23. Які існують різновиди топологій мереж?
24. Особливості, переваги та недоліки топології «шина»?
25. Особливості, переваги та недоліки топології «кільце»?
26. Особливості, переваги та недоліки топології «зірка»?
27. Особливості, переваги та недоліки топології «дерево»?
28. Особливості, переваги та недоліки повнозв'язної топології?
29. Особливості, переваги та недоліки змішаної топології?
30. Яка організація розробила OSI модель?
    a. *ANSI;*
    b. *ISO;*
    c. *IEEE;*
    d. *EIA.*
31. Оберіть необхідне: «Шинна топологія» -
    a. *це топологія при якій до одного центрального вузла приєднуються інші вузли, при чому кожен з них використовує свою окрему лінію зв'язку;*
    b. *при якій всі вузли під'єднанні до одного середовища передавання даних (лінії зв'язку) і інформація від кожного вузла одночасно передається всім іншим вузлам;*
    c. *топологія при якій до одного центрального вузла приєднуються інші вузли, причому до кожного з них може бути під'єднана зіркоподібна топологія;*
    d. *кожен вузол зв'язаний з одним вузлом вищої ієрархії і одним чи декількома вузлами нижчої ієрархії;*
    e. *мережева топологія, в якій кожен вузол має точно два з'єднання з іншими вузлами.*

f. *кожен пункт сегмента має безпосередній зв'язок і з невеликою кількістю пунктів, найближчих за відстанню.*

32. Оберіть необхідне: «Деревоподібна топологія» -
    a. *це топологія при якій до одного центрального вузла приєднуються інші вузли, при чому кожен з них використовує свою окрему лінію зв'язку;*
    b. *при якій всі вузли під'єднанні до одного середовища передавання даних (лінії зв'язку) і інформація від кожного вузла одночасно передається всім іншим вузлам;*
    c. *топологія при якій до одного центрального вузла приєднуються інші вузли, причому до кожного з них може бути під'єднана зіркоподібна топологія;*
    d. *кожен вузол зв'язаний з одним вузлом вищої ієрархії і одним чи декількома вузлами нижчої ієрархії;*
    e. *мережева топологія, в якій кожен вузол має точно два з'єднання з іншими вузлами.*
    f. *кожен пункт сегмента має безпосередній зв'язок і з невеликою кількістю пунктів, найближчих за відстанню.*

33. Оберіть необхідне: «Кільцева топологія» -
    a. *це топологія при якій до одного центрального вузла приєднуються інші вузли, при чому кожен з них використовує свою окрему лінію зв'язку;*
    b. *при якій всі вузли під'єднанні до одного середовища передавання даних (лінії зв'язку) і інформація від кожного вузла одночасно передається всім іншим вузлам;*
    c. *топологія при якій до одного центрального вузла приєднуються інші вузли, причому до кожного з них може бути під'єднана зіркоподібна топологія;*
    d. *кожен вузол зв'язаний з одним вузлом вищої ієрархії і одним чи декількома вузлами нижчої ієрархії;*
    e. *мережева топологія, в якій кожен вузол має точно два з'єднання з іншими вузлами.*
    f. *мережева топологія, в якій утворюється подвійні з'єднання між парами вузлів, при яких інформаційний потік направляється в двох протилежних напрямках;*
    g. *топологія забезпечує з'єднання вузлів за принципом «кожен з кожним»;*
    h. *кожен пункт сегмента має безпосередній зв'язок і з невеликою кількістю пунктів, найближчих за відстанню.*

34. Що собою представляє активне мережеве обладнання.
35. Що собою представляє пасивне обладнання мережі.
36. Які елементи відносяться до елементів організаційної структури?
37. Що собою представляють такі елементи організаційної структури як кінцеві пункти (КП)?
38. Що собою представляють такі елементи організаційної структури як вузлові пункти (КП)?
39. Поясніть значення такого поняття як *концентрація?*
40. Поясніть значення такого поняття як *розподілення?*

41. Поясніть значення такого поняття як *мультиплексування?*
42. Поясніть значення такого поняття як *комутація?*
43. Поясніть значення такого поняття як *маршрутизація?*
44. Наведіть рольове призначення вузлових пунктів?
45. Оберіть визначення, яке відповідає поняттю: «Сервіс-провайдер має вузлові пункти, які називаються»:
    a. *сервісним вузлом (Service Node, SN);*
    b. *вузлом доступу (Access Node, AN);*
    c. *точкою мережевого доступу (Network Access Point, NAP);*
    d. *точками присутності (Points of Presents, POP).*
46. Оберіть визначення, яке відповідає поняттю: «Вузловий пункт, у якому забезпечується підключення сервіс-провайдерів називається»:
    a. *сервісним вузлом (Service Node, SN);*
    b. *точками присутності (Points of Presents, POP).*
    c. *вузлом доступу (Access Node, AN);*
    d. *точкою мережевого доступу (Network Access Point, NAP).*
47. Що собою представляє модель програмного забезпечення?
48. Які типи об'єктних інтерфейсів (програмних інтерфейсів) використовуються в моделі програмного забезпечення?
49. Які основні характеристики сучасних комп'ютерних мереж?
50. Які характеристики відносяться до характеристик *продуктивності* мережі?
51. Які характеристики відносяться до характеристик *надійності* мережі?

Список рекомендованої літератури

1. *Якубайтис Э.А.* Открытые информационные сети. – М.: Радио и связь, 1991. – 208 с.
2. *Шварц М.* Сети связи: протоколы, моделирование и анализ. Ч.1. – М.: Наука, 1992. – 336 с.
3. *Шварц М.* Сети связи: протоколы, моделирование и анализ. Ч. 2. –М.: Наука, 1992. – 272 с.
4. *Блэк Ю.* Сети ЭВМ: протоколы, стандарты, интерфейсы. – М.: Мир, 1990. – 506 с.
5. *Кривуца В.Г., Беркман Л. Н., Лапінський В.В.* Основи інфокомунікацій: навч. посібник для загальноосвіт. навч. закладів - К.: ДУІКТ, 2011.- 276 с.
6. *Кривуца В.Г., Барковський В.В., Беркман Л.Н*. Математичне моделювання телекомунікаційних систем. К.: ДП «ДВІА Зв'язок», 2007. – 270с.
7. *О.М. Ткаченко, Д.О. Нацик* Оптимізація параметрів систем управління телекомунікаційними мережами // Вісник Державного університету інформаційно Т 3, Випуск 3-4, 2005, - с. 71-73

Розділ 3. ЛІНІЇ ЗВ'ЯЗКУ

3.1. Типи ліній зв'язку

Лінія зв'язку складається в загальному випадку з фізичного середовища, по якому передаються електричні інформаційні сигнали, апаратури передачі даних і проміжної апаратури [1]. Синонімом терміна *лінія зв'язк* (*line*) є термін *канал зв'язку* (*channel*).

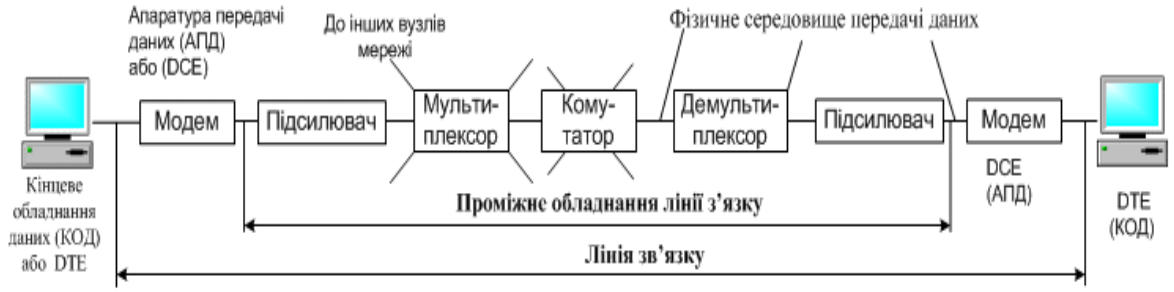
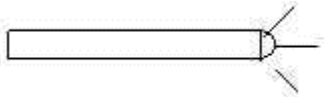


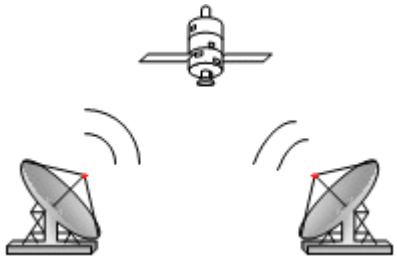
Рис. 3.1. Лінія зв'язку

Фізичне середовище передачі даних (*medium*) може являти собою кабель, тобто набір проводів, ізоляційних і захисних оболонок і сполучних рознімань, а також земну атмосферу чи космічний простір, через які поширюються електромагнітні хвилі.

проводові (повітряні)



кабельні (мідні і волоконно-оптичні)



радіоканали наземного і супутникового зв'язку

***Проводові* (*повітряні*)** лінії зв'язку являють собою провід без якої-небудь ізоляції чи опльоток, які екранують, прокладений між стовпами і висячій в повітрі. По таких лініях зв'язку традиційно передаються телефонні чи телеграфні сигнали, але при відсутності інших можливостей ці лінії використовуються і для передачі комп'ютерних даних. Швидкісні якості і перешкодозахищеність не краща. Сьогодні повітряні лінії зв'язку швидко витісняються кабельними.

Кабельні лінії являють собою досить складну конструкцію. Кабель складається з провідників, укладених у кілька шарів ізоляції: електричної, електромагнітної, механічної, а також, можливо, кліматичної [1].

Кабель може бути оснащений роз'ємами, що дозволяють швидко виконувати приєднання до нього різного устаткування.

У комп'ютерних мережах застосовуються три основних типи кабелю:

- *кабелі на основі кручених пар мідних проводів;*
- *коаксіальні кабелі з мідною жилою;*
- *волоконно-оптичні кабелі.*

Кручена пара існує в *екранованому варіанті* (*Shielded Twistedpair, STP та Foiled Twisted Pair, FTP*), коли мідні провод обертається в ізоляційний екран, і *неекранованому* (*Unshielded Twistedpair, UTP)*, коли ізоляційна обгортка відсутня.

Розрізняють декілька типів кручених пар (рис. 3.2):

- **UTP** (Unshielded Twisted Pair) – незахищена кручена пара;
- **FTP** (Foiled Twisted Pair) – фольгована кручена пара;
- **STP** (Shielded Twisted Pair) – екранована кручена пара.

Кручена пара UTP – це вісім мідних дротів, скручені попарно в спільній ізоляції. Вона є найпоширенішою та найдешевшою крученою парою, проте в разі її експлуатації виникають проблеми з електромагнітною сумісністю. У FTP

та STP кабелях пари дротів мають спільний екран для захисту від електромагнітного випромінювання (ЕМВ). У STP, окрім того, кожна пара дротів має окремий екран. Кручені пари STP та FTP мають ширший частотний діапазон передавання, менше електромагнітне випромінювання порівняно з UTP, однак вони дорожчі та складніші у прокладанні і монтажі [2].

Зкручування проводів знижує вплив зовнішніх перешкод на корисні сигнали, що передаються по кабелю.

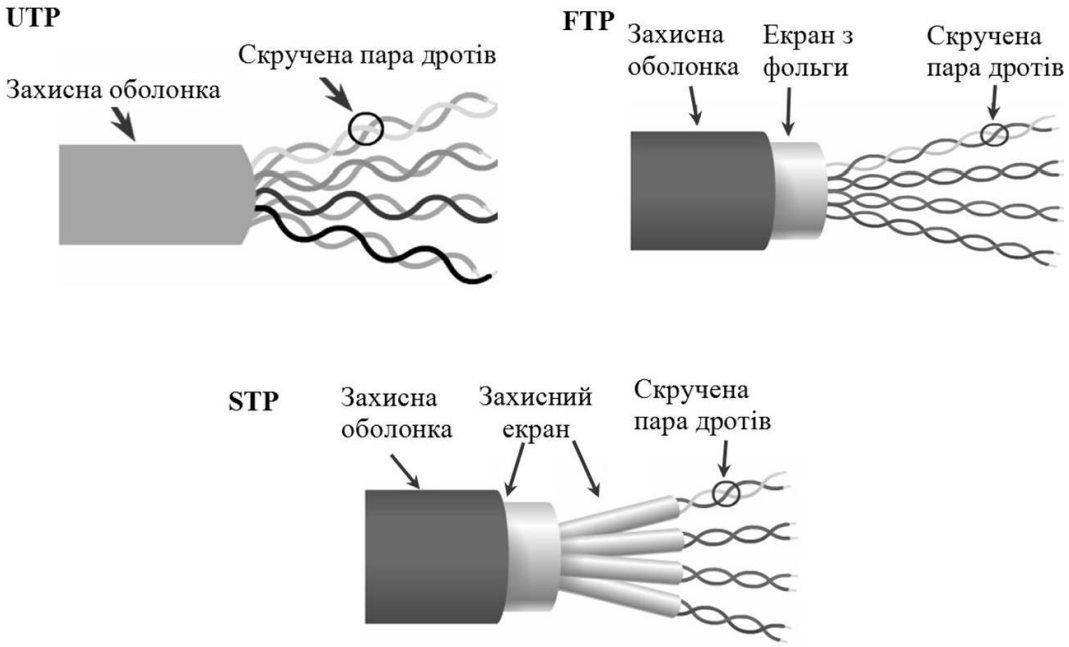
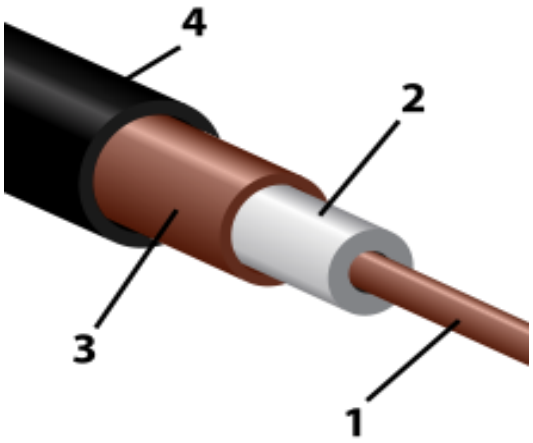


Рис. 3.2. Різновиди крученої пари

Коаксіальний кабель (coaxial) має несиметричну конструкцію і складається з внутрішньої мідної жили й оплетки, відділеної від жили шаром ізоляції. Існує кілька типів коаксіального кабелю, що відрізняються характеристиками й областями застосування — для локальних мереж, для глобальних мереж, для кабельного телебачення і т.п.



1- Центальна жила; 3 - Металева оплітка;

2- Внутрішня ізоляція; 4 – Зовнішя оболонка.

Рис. 3.3. Будова коаксіального кабеля

Коаксіальний кабель донедавна був дуже популярний, що пов'язане з його високою перешкодозахищеністю (завдяки металевої обплетенню), більше широкими, чим у випадку крученої пари, смугами пропущення (понад 1ГГц), а також більшими припустимими відстанями передачі (до кілометра). До нього важче механічно підключитися для несанкціонованого прослуховування мережі, він дає також помітно менше електромагнітних випромінювань зовні. Однак монтаж і ремонт коаксіального кабелю істотно складніше, ніж кручений пари, а вартість його вище (він дорожче приблизно в 1,5 – 3 рази). Складніше й установка рознімань на кінцях кабелю. Зараз його застосовують рідше, ніж кручену пару. Стандарт EIA/TIA-568 містить у собі тільки один тип коаксіального кабелю, застосовуваний у мережі Ethernet.

Волоконно-оптичний кабель (*optical fiber*) складається з тонких (5-60 мікрон) волокон, по яких поширюються світлові сигнали. Це найбільш якісний тип кабелю — він забезпечує передачу даних з дуже високою швидкістю (до 10 Гбіт/з і вище) і до того ж краще інших типів передавальної середовища забезпечує захист даних від зовнішніх перешкод.

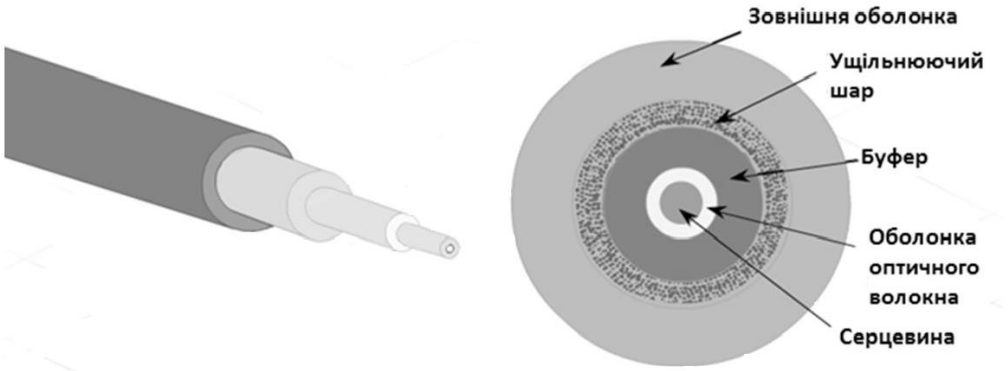


Рис. 3.4. Будова волоконно-оптичного кабелю

У центрі розташована серцевина – світлопередаюче середовище, що виготовлене з прозорого матеріалу. Навколо серцевини розміщена оболонка, що має менший коефіцієнт заломлення, завдяки чому промінь світла відбивається в серцевину ВОК. Це запобігає розсіюван ню світла при проходженні його по кабелю. Оболонку ВОК виготовляють з плавною або ступінчастою зміною коефіцієнта заломлення. Ступінчасті кабелі дешевші та простіші. У них більше послаблюється сигнал. У градієнтних кабелях значно менші послаблення сигналу, що дає змогу збільшити швидкість і відстань передавання. Оболонка має зовнішнє захисне покриття (буфер, ущільнюючий шар та зовнішня оболон ка) для захисту кабелю та надання йому механічної стійкості. Буфер використовують для захисту серцевини та оболонки ВОК від пошкоджень. Ущільнюючий шар оточує буфер та захищає ВОК від розтягування при його монтажі та експлуатації. У якості матеріалу ущільнюючого шару можуть використовувати кевларові волокна. Зовнішня оболонка призначена для захисту ВОК від зношування, розчинників та інших агре- сивних речовин. Склад зовнішньої оболонки залежить від середовища де, можливе застосування кабелю [2].

Радіоканали наземного і супутникового зв'язку утворяться за допомогою передавача і приймача радіохвиль. Існує велика кількість різних типів радіоканалів, що відрізняються як використовуваним частотним діапазоном,

так і дальністю каналу. Діапазони коротких, середніх і довгих хвиль (КХ, СХ і ДХ), називані також діапазонами амплітудної модуляції (Amplitude Modulation, АМ) по типі використовуваного в них методу модуляції сигналу, забезпечують далекий зв'язок, але при невисокій швидкості передачі даних. Більш швидкісними є канали, що працюють на діапазонах ультракоротких хвиль (УКВ), для яких характерна частотна модуляція (Frequency Modulation, FM), а також діапазонах надвисоких частот (НВЧ чи microwaves). У діапазоні НВЧ (понад 4 Ггц) сигнали вже не відбиваються іоносферою Землі і для стійкого зв'язку потрібно наявність прямої видимості між передавачем і приймачем. Тому такі частоти використовують або супутникові канали, або радіорелейні канали, де ця умова виконується.У комп'ютерних мережах сьогодні застосовуються практично всі описані типи фізичних середовищ передачі даних, але найбільш перспективними є волоконно-оптичні. На них сьогодні будуються як магістралі великих територіальних мереж, так і високошвидкісні лінії зв'язку локальних мереж. Популярним середовищем є також кручена пари, що характеризується відмінним співвідношенням якості до вартості, а також простотою монтажу. За допомогою кручений пари звичайно підключають кінцевих абонентів мереж на відстанях до 100 метрів від концентратора. Супутникові канали і радіозв'язок використовуються найчастіше в тих випадках, коли кабельні зв'язки застосувати не можна — наприклад, при проходженні каналу через малонаселену чи місцевість же для зв'язку з мобільним користувачем мережі, таким як шофер вантажівки, лікар, що робить обхід, і т.п.

Кожен вузол оснащується антеною, яка одночасно є передавачем і приймачем електромагнітних хвиль. Електромагнітні хвилі поширюються в атмосфері або вакуумі зі швидкістю 3×10^8 м/с у всіх напрямках або ж у межах певного сектора. Направленість або ненаправленість розповсюдження залежить від типу антени. Наприклад, параболічна антена, є направленою. Інший тип антен – ізотропна антена, що являє собою вертикальний дріт довжиною у чверть хвилі випромінювання. Ізотропні антени є не- направленими, вони широко використовують в переносних портативних пристроях. Оскільки при

ненаправленому розповсюдженні електромагнітні хвилі заповнюють весь простір (в межах певного радіусу, що визначається загасанням потужності сигналу), то цей простір може служити середовищем передавання [2].

Діапазони електромагнітного спектру і відповідні їм бездротові системи передавання інформації поділяються на чотири групи.

1. Діапазон до 300 ГГц має загальну назву – **радіочастотний діапазон (Radio Frequency, RF)**.

Союз ITU розділив його на кілька піддіапазонів:

- **ELF** (Extremely Low Frequency) – діапазон наднизьких частот (0,3 КГц – 3 КГц);
- **VLF** (Very Low Frequency) – діапазон дуже низьких частот (3 КГц – 30 КГц);
- **LF** (Low Frequency) – діапазон низьких частот (30 КГц – 300 КГц);
- **MF** (Medium Frequency) – діапазон середніх частот (300 КГц – 3 МГц);
- **HF** (High Frequency) – діапазон високих частот (3 МГц – 30 МГц);
- **VHF** (Very High Frequency) – діапазон дуже високих частот (30 МГц – 300 МГц);
- **UHF** (Ultra High Frequency) – діапазон ультрависоких частот (300 МГц – 3 ГГц);
- **SHF** (Super High Frequency) – діапазон надвисоких частот (3 ГГц – 30 ГГц);
- **EHF** (Extra High Frequency) – діапазон вкрай високих частот (30 ГГц - 300 ГГц);

Низькошвидкісні системи AM- та FM-діапазонів, призначені для передавання даних з швидкостями від декількох десятків до сотень кілобіт за секунду. Прикладом можуть служити радіомодеми, які з'єднують два сегменти локальної мережі на швидкостях 2400, 9600 або 19200 Кбіт/с.

Окремі ділянки радіочастотного діапазону виділені для використання пристроями, що не вимагають ліцензії наглядових органів: бездротовими LAN, бездротовими телефонами і периферійними комп'ютерними

пристроями. Ці пристрої працюють в діа- пазонах частот 900 МГц, 2,4 ГГц і 5 ГГц. Вказані діапазони частот також називають **ISM-діапазонами** (Industrial, Scientific, Medical – промисловість, наука і медицина). На їх використання не накладено суттєвих обмежень.

Діапазон 900 МГц є найбільш «населеним», оскільки низькочастотна техніка є найпоширенішою. До числа технологій, які використовують смуги частот 2,4 ГГц відносять сучасні технології **бездротових LAN (Wireless LAN, WLAN)**, наприклад, технології IEEE 802.11 і Bluetooth. Сьогодні активно освоюється діапазон 5 ГГц, який дозволяє забезпечувати більш високі швидкості передавання даних.

2. Декілька діапазонів надвисоких частот (НВЧ) радіочастотного діапазону від 300 МГц до 300 ГГц мають спільну назву – **мікрохвильовий діапазон (microwave)**.

Мікрохвильові системи охоплюють найширший клас систем, що об'єднує радіорелейні лінії зв'язку, супутникові канали, бездротові локальні мережі (WLAN) та системи фіксованого бездротового доступу, звані також **системами бездротових абонентських закінчень (Wireless Local Loop, WLL)**.

3. Вище мікрохвильових діапазонів розташовується **інфрачервоний діапазон (Infrared, IR)**.

Інфрачервоний (ІЧ) діапазон також широко використовують для бездротового передавання інформації. Оскільки, інфрачервоне випромінювання не може проникати через стіни, то системи на базі інфрачервоних хвиль служать для побудови невеликих сегментів локальних мереж в межах одного приміщення.

Для обміну інформацією між пристроями за допомогою інфрачервоного випромінювання використовують спеціалізований комунікаційний порт IrDA (Infrared Direct Access). Підключення по інфрачервоному каналу може бути тільки двоточковим.

Інфрачервоне випромінювання використовують пристроями дистанційного керування, бездротовими мишами і клавіатурами. Воно

забезпечує зв’язок в межах малої віддалі і в межах прямої видимості. При цьому ІЧ-сигнали можуть відбиватися від поверхні об’єктів, що збільшує радіус дії. Для забезпечення більшої дальності зв’язку потрібні більш низькі частоти електромагнітного випромінювання.

4. В останні роки **видиме світло (Visible Light)** теж застосовують для передавання інформації (за допомогою лазерів). Системи видимого світла використовують як високошвидкісну альтернативу мікрохвильовим двоточковим каналам для організації доступу на невеликих відстанях [2].

У комп'ютерних мережах сьогодні застосовуються практично всі описані типи фізичних середовищ передачі даних, але найбільш перспективними є *волоконно-оптичні*. На них сьогодні будуються як магістралі великих територіальних мереж, так і високошвидкісні лінії зв'язку локальних мереж.

Популярним середовищем є також с*кручена пара*, що характеризується відмінним співвідношенням якості до вартості, а також простотою монтажу. За допомогою крученої пари звичайно підключають кінцевих абонентів мереж на відстанях до 100 метрів від концентратора.

Супутникові канали і радіозв'язок використовуються найчастіше в тих випадках, коли кабельні зв'язки застосувати не можна — наприклад, при проходженні каналу через малонаселену чи місцевість же для зв'язку з мобільним користувачем мережі, таким як шофер вантажівки, лікар, що робить обхід, і т.п.

3.2. Канали передачі даних мереж

Канал передачі даних **(КПД)** — канал зв’язку, оснащений спеціальною апаратурою для передачі дискретних сигналів.

До складу апаратури передачі даних (АПД) входять: автоматичні викличні пристрої, пристрої захисту від помилок і пристрої перетворення сигналів. В якості кінцевого устаткування даних (КУД) виступають сервери, абонентські системи (АС) та вузли комутації (ВК).

Рис. 3.5. Канал передачі даних

Апаратура передачі даних (АПД чи *DCE— Data Circuit terminating Equipment*) безпосередньо зв'язує комп'ютери чи локальні мережі користувача з лінією зв'язку і є, таким чином, прикордонним устаткуванням. Традиційно апаратуру передачі даних включають до складу лінії зв'язку. Прикладами DCE є модеми, термінальні адаптери мереж ISDN, оптичні модеми, пристрої підключення до цифрових каналів. Звичайно DCE працює на фізичному рівні, відповідаючи за передачу і прийом сигналу потрібної форми і потужності у фізичне середовище [3].

Апаратура користувача лінії зв'язку, що виробляє дані для передачі по лінії зв'язку і, що підключається безпосередньо до апаратури передачі даних, узагальнено зветься закінчене устаткування даних (КУД чи DTE — Data Terminal Equipment). Прикладом DTE можуть служити чи комп'ютери маршрутизатори локальних мереж. Цю апаратуру не включають до складу лінії зв'язку.

Поділ устаткування на класи DCE і DTE у локальних мережах є досить умовним. Наприклад, адаптер локальної мережі можна вважати як приналежністю комп'ютера, тобто DTE, так і складовою частиною каналу зв'язку, тобто DCE.

Проміжна апаратура звичайно використовується на лініях зв'язку великої довжини. Проміжна апаратура вирішує дві основні задачі:

- поліпшення якості сигналу;
- утворення постійного складеного каналу зв'язку між двома абонентами мережі.

У локальних мережах проміжна апаратура може зовсім не використовуватися, якщо довжина фізичного середовища — чи кабелів

радіоефіру — дозволяє одному мережному адаптеру приймати сигнали безпосередньо від іншого мережного адаптера, без проміжного посилення. У противному випадку застосовуються пристрої типу повторювачів і концентраторів.

У глобальних мережах необхідно забезпечити якісну передачу сигналів на відстані в сотні і тисячі кілометрів. Тому без підсилювачів сигналів, установлених через визначені відстані, побудувати територіальну лінію зв'язку неможливо. У глобальній мережі необхідна також і проміжна апаратура іншого роду — мультиплексори, демультиплексори і комутатори. Ця апаратура вирішує другу зазначену задачу, тобто створює між двома абонентами мережі складений канал з відрізків фізичного середовища, що не комутуються - кабелів з підсилювачами. Мультиплексори, демультиплексори і комутатори утворюють складений канал на довгостроковій основі, наприклад на місяць чи рік, причому абонент не може впливати на процес комутації цього каналу — ці пристрої керуються по окремих входах, абоненту недоступним (на малюнку не показані). Наявність проміжної комутаційної апаратури рятує творців глобальної мережі від необхідності прокладати окрему кабельну лінію для кожної пари вузлів мережі, що з'єднуються. Замість цього між мультиплексорами і комутаторами використовується високошвидкісне фізичне середовище, наприклад волоконно-оптичний чи коаксіальний кабель, по якому передаються одночасно дані від великого числа порівняно низько швидкісних абонентських ліній [3]. А коли потрібно утворити постійне з'єднання між якими-небудь двома кінцевими вузлами мережі, що знаходяться, наприклад, у різних містах, те мультиплексові, комутатори і демультиплексори набудовуються оператором каналу відповідним чином. Високошвидкісний канал звичайно називають ущільненим каналом.

Проміжна апаратура каналу зв'язку прозора для користувача, він її не замічає і не враховує у своїй роботі. Для нього важливі тільки якість отриманого каналу, що впливає на швидкість передачі дискретних даних. У дійсності ж проміжна апаратура утворить складну мережу, що називають первинною мережею, тому що сама по собі вона ніяких високорівневих служб

(наприклад, файлової чи передачі голосу) не підтримує, а тільки є основою для побудови комп'ютерних, телефонних чи інших мереж.

В залежності від типу проміжної апаратури всі лінії зв'язку поділяються на аналогові і цифрові. В *аналогових лініях* проміжна апаратура призначена для посилення аналогових сигналів, тобто сигналів, що мають безупинний діапазон значень. Такі лінії зв'язку традиційно застосовувалися в телефонних мережах для зв'язку АТС між собою. Для створення високошвидкісних каналів, що мультиплексують трохи низько швидкісних аналогових абонентських каналів, при аналоговому підході звичайно використовується техніка частотного мультиплексування (Frequency Division Multiplexing, FDM).

У *цифрових лініях* зв'язку сигнали, що передаються мають кінцеве число станів. Як правило, елементарний сигнал, тобто сигнал, переданий за один такт роботи передавальної апаратури, має 2 чи 3 стани, що передаються в лініях зв'язку імпульсами прямокутної форми. За допомогою таких сигналів передаються як комп'ютерні дані, так і оцифрована мова і зображення. У цифрових каналах зв'язку використовується проміжна апаратура, що поліпшує форму імпульсів і забезпечує їх ресинхронізацію, тобто відновлює період їхнього проходження. Проміжна апаратура утворення високошвидкісних цифрових каналів (мультиплексові, демультиплексори, комутатори) працює за принципом тимчасового мультиплексуования каналів (Time Division Multiplexing, TDM), коли кожному низько швидкісному каналу виділяється визначена частка часу (тайм-слот чи квант) високошвидкісного каналу [3].

Апаратура передачі дискретних комп'ютерних даних по аналогових і цифрових лініях зв'язку істотно відрізняється, тому що в першому випадку лінія зв'язку призначена для передачі сигналів довільної форми і не пред'являє ніяких вимог до способу представлення одиниць і нулів апаратурою передачі даних, а в другому — усі параметри переданих лінією імпульсів стандартизовані. Іншими словами, на цифрових лініях зв'язку протокол фізичного рівня визначений, а на аналогових лініях — немає.

За можливістю ***зміни напрямку передачі*** інформації розрізняють канали:

- ***симплексні,*** що забезпечують передачу інформації тільки в одному напрямку;
- ***напівдуплексні***, що дають можливість передавати почергово інформацію у двох напрямках;
- ***дуплексні***, що передають інформацію одночасно в обох напрямках.

Залежно ***від способу передачі даних*** розрізняють канали зв'язку:

- ***з послідовною передачею сигналів*** - розряди кожного символу передаються послідовно по одним і тим самим лініям зв'язку
- ***з паралельною передачею сигналів*** - всі розряди кожного символу передаються одночасно по окремим лініям зв'язку.

Часто фізичне з'єднання між передавачем і приймачем утворюється послідовним з'єднанням кількох каналів зв'язку в єдиний ***складений канал зв'язку***.

Залежно від режиму використання складеного каналу зв'язку розрізняють:

- ***некомутовані (орендовані) канали*** - складений канал, який створюється й існує протягом певного інтервалу часу незалежно від того, передається інформація чи ні.
- ***комутовані канали*** - створюється тільки на час передачі повідомлень, а поза цим — окремі канали зв'язку, з яких він складається, можуть використовуватися за іншим призначенням.

3.3. Характеристики ліній зв'язку

Типи характеристик і способи їхнього визначення

До основних характеристик ліній зв'язку відносяться [4]:

- амплітудно-частотна характеристика;
- смуга пропущення;
- загасання;
- першкодостійкість;
- перехресні наведення на ближньому кінці лінії;

- пропускна здатність;
- вірогідність передачі даних;
- питома вартість.

У першу чергу розроблювача обчислювальної мережі цікавлять пропускна здатність і вірогідність передачі даних, оскільки ці характеристики прямо впливають на продуктивність і надійність створюваної мережі. Пропускна здатність і вірогідність — це характеристики як лінії зв'язку, так і способу передачі даних. Тому якщо спосіб передачі (протокол) уже визначений, те відомі і ці характеристики. Наприклад, пропускна здатність цифрової лінії завжди відома, тому що на ній визначений протокол фізичного рівня, що задає бітову швидкість передачі даних — 64 Кбіт/с, 2 Мбіт/с и т. п. Однак не можна говорити про пропускну здатність лінії зв'язку, до того як для неї визначений протокол фізичного рівня. Саме в таких випадках, коли тільки має бути визначити, який з безлічі існуючих протоколів можна використовувати на даній лінії, дуже важливими є інші характеристики лінії, такі як смуга пропущення, перехресні наведення, перешкодостійкість і інші характеристики. Для визначення характеристик лінії зв'язку часто використовують аналіз її реакцій на деякі еталонні впливи. Такий підхід дозволяє досить просто й однотипно визначати характеристики ліній зв'язку будь-якої природи, не прибігаючи до складних теоретичних досліджень. Найчастіше як еталонні сигнали для дослідження реакцій ліній зв'язку використовуються синусоїдальні сигнали різних частот. Це зв'язано з тим, що сигнали цього типу часто зустрічаються в техніку і з їх допомогою можна представити будь-як функцію часу — як безупинний процес коливань звуку, так і прямокутні імпульси, які генеруються комп'ютером.

Спектральний аналіз сигналів на лініях зв'язку

З теорії гармонійного аналізу відомо, що будь-який періодичний процес можна представити у виді суми синусоїдальних коливань різних частот і різних амплітуд (рис. 3.6).

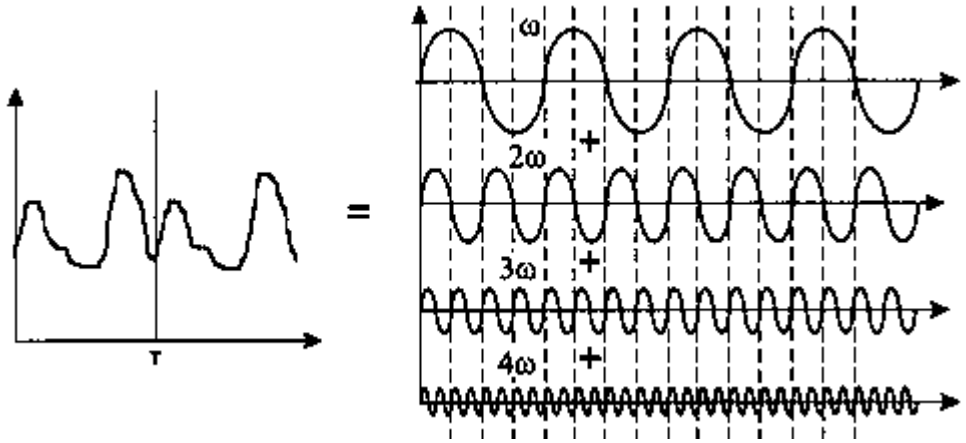


Рис. 3.6 Подання періодичного сигналу сумою синусоїд

Кожна складова синусоїда називається також гармонікою, а набір усіх гармонік називають спектральним розкладанням вихідного сигналу. Неперіодичні сигнали можна представити у вигляді інтеграла синусоїдальних сигналів з безупинним спектром частот.

Неперіодичні сигнали можна представити у виді інтеграла синусоїдальних сигналів з безупинним спектром частот. Неперіодичні сигнали можна подавати у вигляді інтегралу синусоїдальних сигналів з неперервним спектром частот. Наприклад, спектральних поділ ідеального імпульсу (одиничної потужності і нульової тривалості) має складові всього спектру частот, від мінус нескінченності до плюс нескінченності (рис.3.7).

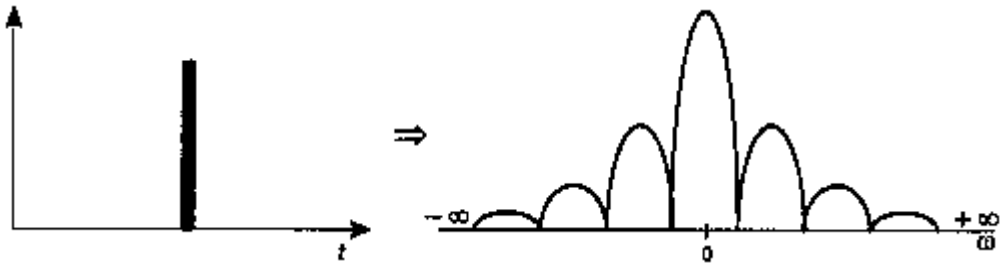


Рис. 3.7. Спектральний розподіл ідеального імпульсу

Техніка перебування спектра будь-якого вихідного сигналу добре відома. Для деяких сигналів, що добре описуються аналітично (наприклад, для послідовності прямокутних імпульсів однакової тривалості й амплітуди), спектр легко обчислюється на підставі формул Фур'є. Для сигналів довільної

форми, що зустрічаються на практиці, спектр можна знайти за допомогою спеціальних приладів — спектральних аналізаторів, які вимірюють спектр реального сигналу і відображають амплітуди складових гармонік на екрані чи роздруковують їх на принтері [4].

Перекручування передавальним каналом синусоїди якої-небудь частоти приводить у кінцевому рахунку до перекручування переданого сигналу будь-якої форми, особливо якщо синусоїди різних частот спотворюються неоднаково. Якщо це аналоговий сигнал, що передає мову, то змінюється тембр голосу за рахунок перекручування обертонів — бічних частот. При передачі імпульсних сигналів, характерних для комп'ютерних мереж, спотворюються низькочастотні і високочастотні гармоніки, у результаті фронти імпульсів утрачають свою прямокутну форму (рис. 3.8). Внаслідок цього на прийомному кінці лінії сигнали можуть погано розпізнаватися.

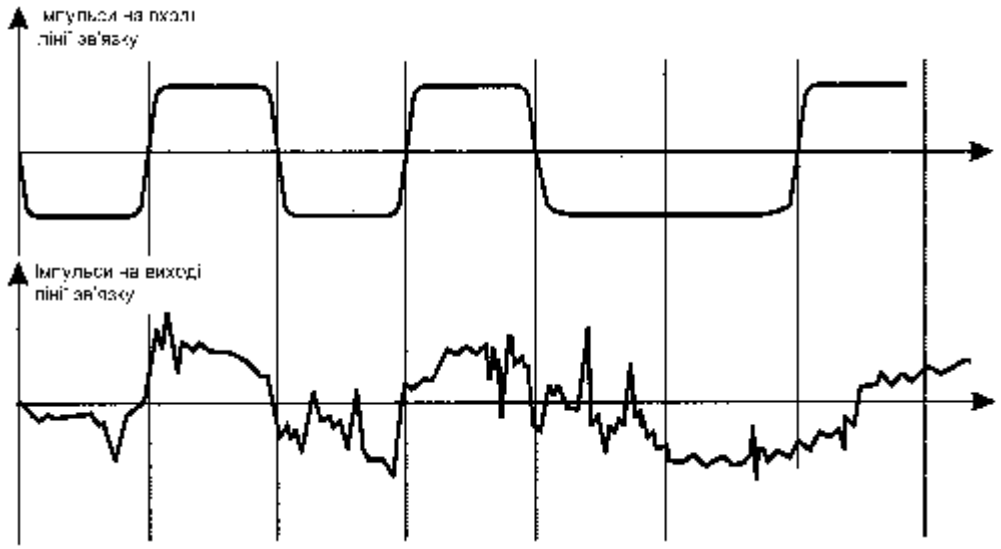


Рис. 3.8. Спотворення імпульсу в лінії зв'язку

Лінія зв'язку спотворює передані сигнали через те, що її фізичні параметри відрізняються від ідеальних. Так, наприклад, мідні проводи завжди являють собою деяку розподілену по довжині комбінацію активного опору, ємнісного й індуктивного навантаження (рис. 3.9).

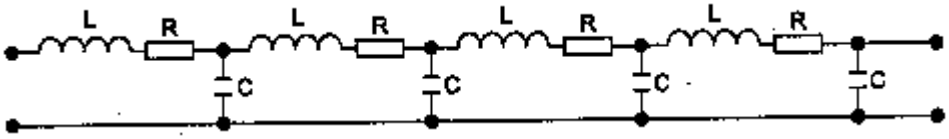


Рис. 3.9 Комбінація активного опору, ємнісного й індуктивного навантаження

У результаті для синусоїд різних частот лінія буде володіти різним повним опором, а виходить, і передаватися вони будуть по-різному. Волоконно-оптичний кабель також має відхилення, що заважають ідеальному поширенню світла. Якщо лінія зв'язку включає проміжну апаратуру, то вона також може вносити додаткові перекручування, тому що неможливо створити пристрої, які б однаково добре передавали весь спектр синусоїд, від нуля до нескінченності.

Крім перекручувань сигналів, внесених внутрішніми фізичними параметрами лінії зв'язку, існують і зовнішні перешкоди, що вносять свій внесок у перекручування форми сигналів на виході лінії. Ці перешкоди створюють різні електричні двигуни, електронні пристрої, атмосферні явища і т.д. Незважаючи на захисні міри, що починаються розроблювачами кабелів і посиленно-комутуючої апаратури, цілком компенсувати вплив зовнішніх перешкод не вдається. Тому сигнали на виході лінії зв'язку звичайно мають складну форму(як це подано рис. 3.8), по якій іноді важко зрозуміти, яка дискретна інформація була подана на вхід лінії.

Амплітудно-частотна характеристика, смуга пропущення і загасання

Ступінь перекручування синусоїдальних сигналів лініями зв'язку оцінюється за допомогою таких характеристик, як амплітудно-частотна характеристика, смуга пропущення і загасання на визначеній частоті [5].

Амплітудно-частотна характеристика (рис. 3.10) показує, як загасає амплітуда синусоїди на виході лінії зв'язку в порівнянні з амплітудою на її вході для всіх можливих частот переданого сигналу. Замість амплітуди в цій

характеристиці часто використовують також такий параметр сигналу, як його потужність.

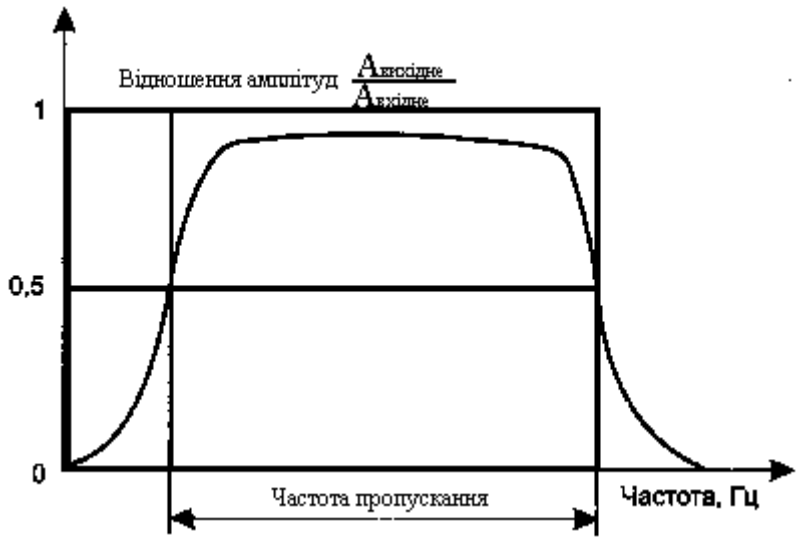


Рис. 3.10 Амплітудно-частотна характеристика

Знання амплітудно-частотної характеристики реальної лінії дозволяє визначити форму вихідного сигналу практично для будь-якого вхідного сигналу. Для цього необхідно знайти спектр вхідного сигналу, перетворити амплітуду складаючих її гармонік відповідно до амплітудно-частотної характеристик, а потім знайти форму вихідного сигналу, склавши перетворені гармоніки. Незважаючи на повноту інформації, наданої амплітудно-частотної характеристикою про лінії зв'язку, її використання ускладнюється тою обставиною, що одержати її дуже важко. Адже для цього потрібно провести тестування лінії еталонними синусоїдами по всьому діапазоні частот від нуля до деякого максимального значення, що може зустрітися у вхідних сигналах.

Змінювати частоту вхідних синусоїд потрібно з невеликим кроком, а кількість експериментів повинна бути дуже великою. Тому на практиці замість амплітудно-частотної характеристики застосовуються інші, спрощені характеристики — смуга пропущення і загасання. Смуга пропущення (bandwidth) — це безупинний діапазон частот, для якого відношення амплітуди вихідного сигналу до вхідного перевищує деяку заздалегідь задану межу, звичайно це - 0,5.

Тобто смуга пропущення визначає діапазон частот синусоїдального сигналу, при яких цей сигнал передається по лінії зв'язку без значних перекручувань. Знання смуги пропущення дозволяє одержати з деяким ступенем наближення той же результат, що і знання амплітудно-частотної характеристики. Як ми побачимо нижче, ширина смуги пропущення найбільшою мірою впливає на максимально можливу швидкість передачі інформації з лінії зв'язку. Саме цей факт знайшов відображення в англійському еквіваленті розглянутого терміна (width — ширина). Загасання (attenuation) визначається як відносне зменшення амплітуди чи потужності сигналу при передачі по лінії сигналу визначеної частоти. Таким чином, загасання являє собою одну точку з амплітудно-частотної характеристики лінії. Часто при експлуатації лінії заздалегідь відома основна частота переданого сигналу, тобто та частота, гармоніка якої має найбільшу амплітуду і потужність. Тому досить знати загасання на цій частоті, щоб приблизно оцінити перекручування переданих по лінії сигналів. Більш точні оцінки можливі при відомому загасанні на декількох частот, що відповідають декільком основним гармонікам сигналу, який передається. Загасання А виміряється в децибелах (д., decibel — d) і обраховується за формулою [4]:

$$\boldsymbol{A} = 10\ log_{10}\ \boldsymbol{P}_{вих}/\boldsymbol{P}_{вх},$$

де $\boldsymbol{P}_{вих}$ — потужність сигналу на виході з лінії,

$\mathbf{P}_{вх}$ — потужність сигналу на вході лінії.

Тому що потужність вихідного сигналу кабелю без проміжних підсилювачів завжди менше, ніж потужність вхідного сигналу, загасання кабелю завжди є негативною величиною. Наприклад, кабель на кручений парі категорії 5 характеризується загасанням не нижче -23,6 дБ для частоти 100 МГц при довжині кабелю 100 м. Частота 100 МГц обрана тому, що кабель цієї категорії призначений для високошвидкісної передачі даних, сигнали яких мають значимі гармоніки з частотою приблизно 100 Мгц. Кабель категорії 3 призначений для низько швидкісною передачі даних, тому для нього

визначається загасання на частоті 10 МГц (не нижче -11,5 дБ). Часто оперують з абсолютними значеннями загасання, без указівки знака. Абсолютний рівень потужності, наприклад рівень потужності передавача, також виміряється в децибелах. При цьому як базове значення потужності сигналу, щодо якого виміряється поточна потужність, приймає значення в 1мвт. Таким чином, рівень потужності ***p*** обчислюється по наступній формулі [5]:

$$\boldsymbol{P} = 10\ log_{10}\boldsymbol{P}/1\text{мвт}\ [\text{дБм}],$$

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

Таким чином, амплітудно-частотна характеристика, смуга пропущення і загасання є універсальними характеристиками, і їхнє знання дозволяє зробити висновок про те, як через лінію зв'язку будуть передаватися сигнали будь-якої форми. Смуга пропущення залежить від типу лінії і її довжини. На рис. 3.11 показані смуги пропускання ліній зв'язку різних типів, а також ті частотні діапазони, що найбільш часто використовуються в техніці зв'язку.

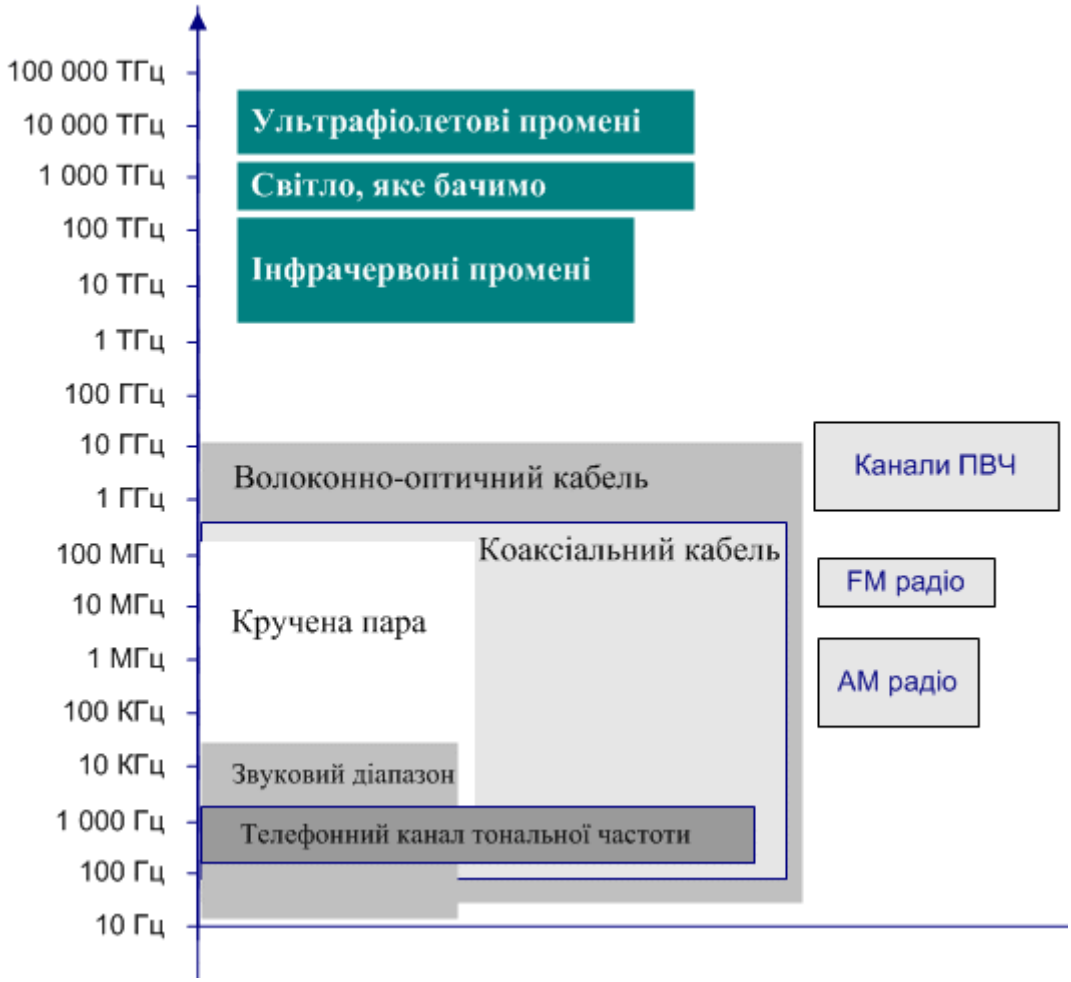


Рис. 3.11 Смуги пропускання ліній зв'язку та популярні частотні діапазони

Пропускна здатність лінії

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

Пропускна здатність лінії зв'язку залежить не тільки від її характеристик, таких як амплітудно-частотна характеристика, але і від спектра сигналів, що передаються [4]. Якщо значимі гармоніки сигналу (тобто ті гармоніки, амплітуди яких вносять основний вклад у результуючий сигнал) попадають у смугу пропускання лінії, то такий сигнал буде добре передаватися даною лінією зв'язку і приймач зможе правильно розпізнати інформацію, відправлену по лінії передавачем (рис.3.12, а). Якщо ж значимі гармоніки виходять за границі смуги пропущення лінії зв'язку, то сигнал буде значно спотворюватися, приймач буде

помилятися при розпізнаванні інформації, а інформація не зможе передаватися з заданою пропускною здатністю (рис. 3.12, б) [5].

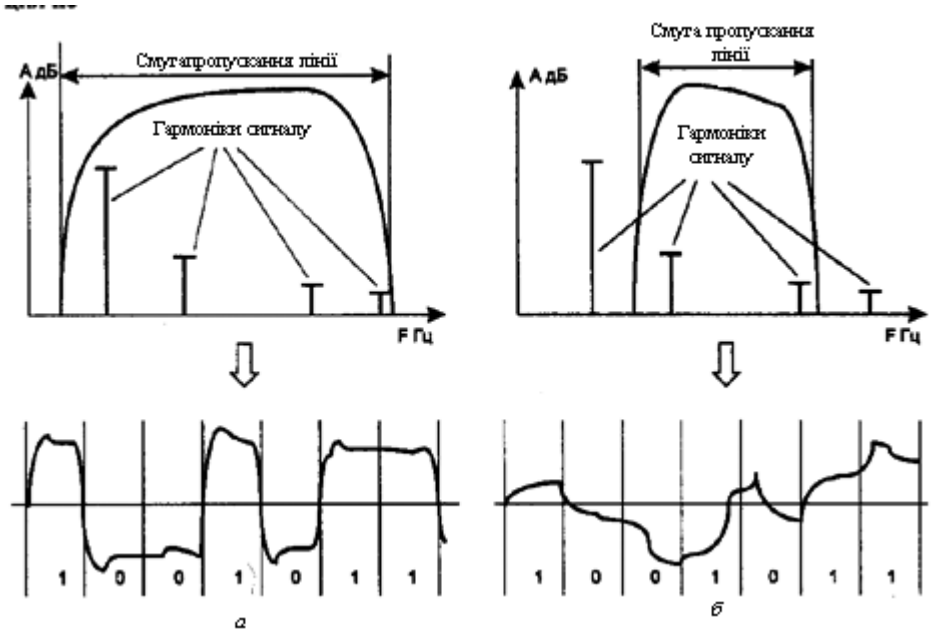


Рис. 3.12 Співвідношення між смугою пропускання лінії зв'язку і спектром сигналу

Вибір способу представлення дискретної інформації у вигляді сигналів, що подаються на лінію зв'язку, називається фізичним чи лінійним кодуванням. Від обраного 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 — ні. Наприклад, скручена пари категорії 3 може передавати дані з пропускною здатністю 10 Мбіт/с при способі кодування стандарту фізичного рівня l0Base-T і 33 Мбіт/с при способі кодування стандарту 100Base-T4. У прикладі, приведеному на рис. 3.12, прийнятий наступний спосіб кодування — логічна 1 представлена на лінії позитивним потенціалом, а логічний 0 — негативним.

Теорія інформації говорить, що будь-яка помітна і непередбачена зміна прийнятого сигналу несе в собі інформацію. Відповідно до цього прийом синусоїди, у якої амплітуда, фаза і частота залишаються незмінними, інформації не несе, тому що зміна сигналу хоча і відбувається, але є добре

передбачуваною. Аналогічно, не несуть у собі інформації імпульси на тактовій шині комп'ютера, тому що їхні зміни також постійні в часі. А от імпульси на шині даних пророчити заздалегідь не можна, тому вони переносять інформацію між окремими блоками чи пристроями.

Більшість способів кодування використовують зміну якого-небудь параметра періодичного сигналу — частоти, амплітуди і фази синусоїди чиж знак потенціалу послідовності імпульсів. Періодичний сигнал, параметри якого змінюються, називають *несучим сигналом* чи *несучою частотою*, якщо в якості такого сигналу використовується синусоїда [6].

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

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

Пропускна здатність лінії в бітах у секунду в загальному випадку не збігається з числом бод. Вона може бути як вище, так і нижче числа бод, і це співвідношення залежить від способу кодування. Якщо сигнал має більш двох помітних станів, то пропускна здатність у бітах у секунду буде вище, ніж число бод. Наприклад, якщо інформаційними параметрами є фаза й амплітуда синусоїди, причому розрізняються 4 стани фази в 0, 90,180 і 270 градусів і два значення амплітуди сигналу, то інформаційний сигнал може мати 8 помітних станів. У цьому випадку модем, що працює зі швидкістю 2400 бод (з тактовою частотою 2400 Гц) передає інформацію зі швидкістю 7200 біт/с, тому що при одній зміні сигналу передається 3 битка інформації.

При використанні сигналів із двома помітними станами може спостерігатися зворотна картина. Це часто відбувається тому, що для надійного розпізнавання приймачем користувальницької інформації кожен біт у 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 два рази нижче, ніж число бод, передане по лінії.

На пропускну здатність лінії впливає не тільки фізичне, але і логічне кодування. *Логічне кодування* виконується до фізичного кодування і має на увазі заміну біт вихідної інформації новою послідовністю біт, що несе ту ж інформацію, але яке ще володіє, крім цього, додатковими властивостями, наприклад можливістю для прийомної сторони виявляти помилки в прийнятих даних [6]. Супровід кожного байта вихідної інформації одним бітом парності — це приклад способу логічного кодування, який часто застосовується при передачі даних за допомогою модемів. Іншим прикладом логічного кодування може служити шифрування даних, що забезпечує їх конфіденційність при передачі через суспільні канали зв'язку. При логічному кодуванні найчастіше початкова послідовність біт заміняється більш довгою послідовністю, тому пропускна здатність каналу стосовно корисної інформації при цьому зменшується.

Зв'язок між пропускною здатністю лінії і її смугою пропущення

Чим вище частота несучого періодичного сигналу, тим більше інформації в одиницю часу передається по лінії і тем вище пропускна здатність лінії при фіксованому способі фізичного кодування. Однак, з іншого боку, зі збільшенням частоти періодичного несучого сигналу збільшується і ширина спектру цього сигналу, тобто різниця між максимальною і мінімальною частотами того набору синусоїд, що у сумі дадуть обрану для фізичного кодування послідовність сигналів. Лінія передає цей спектр синусоїд з тими спотвореннями, що визначаються її смугою пропущення. Чим більше невідповідність між смугою пропущення лінії і шириною спектра інформаційних сигналів, які передаються, тим більше сигнали спотворюються і тем імовірніше помилки в розпізнаванні інформації приймаючою стороною, а

значить, швидкість передачі інформації насправді виявляється менше, ніж можна було припустити [4].

Зв'язок між смугою пропущення лінії і її *максимально можливою пропускною здатністю*, не залежить від прийнятого способу фізичного кодування, встановив Клод Шеннон [5]:

$$\boldsymbol{C} = F\ log_2\,(1 + \boldsymbol{P_c}/\boldsymbol{P_ш}),$$

Де $\boldsymbol{C}$ — максимальна пропускна здатність лінії в бітах за секунду, $\boldsymbol{F}$ — ширина смуги пропущення лінії в герцах, $\boldsymbol{P_c}$ — потужність сигналу, $\boldsymbol{P_ш}$ — потужність шуму.

З цього співвідношення видно, що хоча теоретичної межі пропускної здатності лінії з фіксованою смугою пропущення не існує, на практиці така межа існує. Дійсно, підвищити пропускну здатність лінії можна за рахунок збільшення потужності передавача чи зменшення потужності шуму (перешкод) на лінії зв'язку. Обидві ці складові піддаються зміні з важкими зусиллями. Підвищення потужності передавача веде до значного збільшення його габаритів і вартості. Зниження рівня шуму вимагає застосування спеціальних кабелів з гарними захисними екранами, що дуже дорого, а також зниження шуму в передавачі і проміжній апаратурі, чого досягти дуже не просто. До того ж вплив потужностей корисного сигналу і шуму на пропускну здатність обмежено логарифмічною залежністю, що росте далеко не так швидко, як прямо-пропорційно. Так, при досить типовому вихідному відношенні потужності сигналу до потужності шуму в 100 разів підвищення потужності передавача в 2 рази дасть тільки 15% збільшення пропускної здатності лінії [5].

Близьким по суті до формули Шеннона є наступне співвідношення, отримане Найквістом, що також визначає максимально можливу пропускну здатність лінії зв'язку, але без обліку шуму на лінії:

$\boldsymbol{C} = 2\boldsymbol{F}log_2\boldsymbol{M}$, де $\boldsymbol{M}$ — кількість помітних станів інформаційного параметра.

Якщо сигнал має 2 стани, то пропускна здатність дорівнює подвоєному значенню ширини смуги пропущення лінії зв'язку (рис. 4.10 а). Якщо ж передавач використовує більш ніж 2 стійкі стани сигналу для кодування даних, то пропускна здатність лінії підвищується, тому що за один такт роботи передавач передає декілька біт вихідних даних, наприклад 2 біти при наявності чотирьох помітних станів сигналу (рис. 3.13).

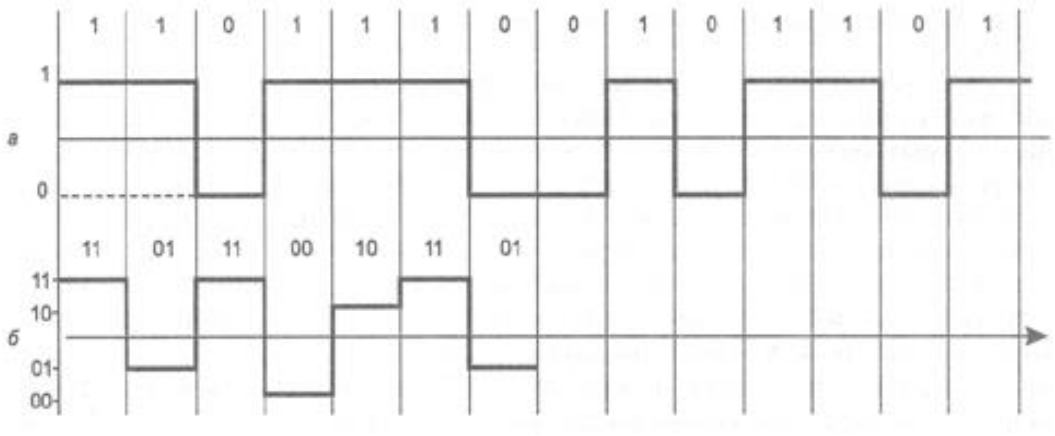


Рис. 3.13. Підвищення швидкості передачі за рахунок додаткових станів сигналу

Хоча формула Найквиста явно не враховує наявність шуму, побічно його вплив відбивається у виборі кількості станів інформаційного сигналу. Для підвищення пропускної здатності каналу хотілося б збільшити цю кількість до значних величин, але на практиці ми не можемо цього зробити через шум на лінії. Наприклад, для наведеного на рис. 3.13 прикладу, можна збільшити пропускну здатність лінії ще в два рази, використавши для кодування даних не 4, а 16 рівнів. Однак якщо амплітуда шуму часто перевищує різницю між сусідніми 16 рівнями, то приймач не зможе стійко розпізнавати дані, що пердаються. Тому кількість можливих станів сигналу фактично обмежується співвідношенням потужності сигналу і шуму, а формула Найквиста визначає граничну швидкість передачі даних у тому випадку, коли кількість станів вже обрано з урахуванням можливостей стійкого розпізнавання приймачем. Приведені співвідношення дають граничне значення пропускної здатності лінії,

а ступінь наближення до цієї межі залежить від конкретних методів фізичного кодування, які будуть розглянуті нижче.

Перешкодостійкість і вірогідність

Перешкодостійкість лінії визначає її здатність зменшувати рівень перешкод, які створюються в зовнішньому середовищі, на внутрішніх провідниках. Перешкодостійкість лінії залежить від типу фізичного середовища, яке використовується, а також від екрануючих і придушуючиш перешкоди засобів самої лінії. Найменше перешкодостійкими є радіолінії, гарною стійкістю володіють кабельні — волоконно-оптичні, вони малочутливі до зовнішнього електромагнітного випромінювання. Звичайно для зменшення перешкод, що з'являються через зовнішні електромагнітні поля, провідники екранують і скручують [6].

***Перехресні наведення на ближньому кінці* (*Near End Cross Talk — NEXT*)** визначають перешкодостійстійкість кабелю до внутрішніх джерел перешкод, коли електромагнітне поле сигналу, переданого 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 *NEXT*, виражений у децибелах, дорівнює

$$10 \log P_{вих}/P_{нав},$$

де $P_{вих}$ — потужність вихідного сигналу, $P_{нав}$ — потужність наведеного сигналу. Чим менше значення *NEXT*, тим краще кабель. Так, для кручений пари категорії 5 показник *NEXT* повинен бути менше - 27дб на частоті 100 Мгц.

Показник *NEXT* звичайно використовується до кабелю, що складає з декількох кручених пар, тому що в цьому випадку взаємні наведення однієї пари на іншу можуть досягати значних величин. Для одинарного коаксіального кабелю (тобто складає 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 друг для друга.

У зв'язку з тим, що в деяких нових технологіях використовується передача даних одночасно по декількох кручених парах, останнім часом став застосовуватися показник *PovserSUM*, що є модифікацією показника *NEXT*. Цей показник відбиває сумарну потужність перехресних наведень від усіх передавальних пар у кабелі.

Вірогідність передачі даних характеризує імовірність перекручування для кожного переданого 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, для кодів що самокоректуються чи протоколів з повторною передачею перекручених кадрів) складає, як правило, 10^{-6}-10^{-10}, в оптично-волоконних лініях зв'язку — 10^{-9}. Значення вірогідності передачі даних, наприклад, у 10^{4}говорить про те, що в середньому з 10 000 біт спотворюється значення одного біта. Перекручування біт відбуваються як через наявність перешкод на лінії, так і через перекручування форми сигналу обмеженою смугою пропущення лінії. Тому для підвищення вірогідності переданих даних потрібно підвищувати ступінь перешкодозахищеності лінії, знижувати рівень перехресних наведень у кабелі, а також використовувати більш широкополосні лінії зв'язку [6].

3.4. Стандарти кабелів

Кабель — це досить складний виріб, який складаються з провідників, шарів екрана й ізоляції. У деяких випадках до складу кабелю входять з'єднувачі, за допомогою яких кабелі приєднуються до устаткування. Крім цього, для забезпечення швидкої перекомутації кабелів і устаткування використовуються різні електромеханічні пристрої, які називаються кросовими секціями, кросовими коробками чи шафами. У комп'ютерних мережах застосовуються кабелі, що задовольняють визначеним стандартам, які

дозволяють будувати кабельну систему мережі з кабелів і сполучаючих пристроїв різних виробників. Сьогодні найбільш вживаними стандартами у світовій практиці є наступні.

- Американський стандарт EIA/TIA-568A, який був розроблений спільними зусиллями декількох організацій: ANSI, EIA/TIA і лабораторією Underwriters Labs (UL). Стандарт EIA/TIA-568 розроблений на основі попередньої версії стандарту EIA/TIA-568 і доповнень до цього стандарту TSB-36 і TSB-40A).
- Міжнародний стандарт ISO/IEC 11801.
- Європейський стандарт EN50173.

Ці стандарти близькі між собою і по багатьом позиціям, які пред'являються до кабелів. Однак є і розходження між цими стандартами, наприклад, у міжнародний стандарт 11801 і європейський EN50173 увійшли деякі типи кабелів, що відсутні в стандарті EIA/TAI-568A.

До появи стандарту EIA/TIA велику роль грав американський стандарт *системи категорій кабелів* Underwriters Labs, розроблений разом з компанією Anixter. Пізніше цей стандарт ввійшов у стандарт EIA/TIA-568.

Крім цих відкритих стандартів, багато компаній у свій час розробили свої фірмові стандарти, з яких і досі має практичне значення тільки один — стандарт компанії IBM.

При стандартизації кабелів прийнято протокольно-незалежний підхід. Це означає, що в стандарті обмовляються електричні, оптичні і механічні характеристики, яким повинен задовольняти той чи інший тип кабелю чи виробу для сполучення — роз'єм, кросова панель і т.п. Однак для якого протоколу призначений даний кабель, стандарт не визначає. Тому не можна придбати кабель для протоколу Ethernet чи FDDI, потрібно просто знати, які типи стандартних кабелів підтримують протоколи Ethernet і FDDI.

У ранніх версіях стандартів визначалися тільки характеристики кабелів, без з'єднувачів. В останніх версіях стандартів з'явилися вимоги до елементів сполучення (документи TSB-36 і TSB-40A, що ввійшли потім у стандарт 568A),

а також до ліній (каналів), що представляють типову зборку елементів кабельної системи, що складає зі шнура від робочої станції до розетки, самої розетки, основного кабелю (довжиною до 90 м для кручений пари), точки переходу (наприклад, ще однієї чи розетки твердого кросового з'єднання) і шнура до активного устаткування, наприклад концентратора чи комутатора.

Зупинимося тільки на основних вимогах до самих кабелів, не розглядаючи характеристик елементів сполучення і зібраних ліній. У стандартах кабелів розглядається досить багато характеристик, з яких найбільш важливі перераховані нижче (перші дві з них уже були досить детально розглянуті) [7].

- *Загасання* (*Attenuation*). Загасання виміряється в децибелах на метр для визначеного частоти чи діапазону частот сигналу.
- *Перехресні наведення на ближньому кінці* (*Near End Cross Talk, NEXT*). Виміряються в децибелах для визначеної частоти сигналу.
- *Імпеданс* (хвильовий опір) — це повний (активний і реактивний) опір в електричному ланцюзі. Імпеданс виміряється в Омах і є сталою величиною для кабельних систем (наприклад, для коаксіальних кабелів, які використовуються у стандартах Ethernet, імпеданс кабелю повинний складати 50 Ом). Для неекранованої кручений пари, яка найбільш часто використовується значення імпедансу — 100 і 120 Ом. В області високих частот (100-200 МГц) імпеданс залежить від частоти.
- *Активний опір* — це опір постійного струму в електричному ланцюзі. На відміну від імпедансу активний опір не залежить від частоти і зростає зі збільшенням довжини кабелю.
- *Ємність* — це властивість металевих провідників накопичувати енергію. Два електричних провідники в кабелі, розділені діелектриком, являють собою конденсатор, здатний накопичувати заряд. Ємність є небажаною величиною, тому варто прагнути до того, щоб вона була якнайменше (іноді застосовують термін “паразитна ємність”). Високе значення ємності в кабелі приводить до перекручування сигналу й обмежує смугу пропущення лінії.

- *Рівень зовнішнього електромагнітного випромінювання чи електричний шум*. Електричний шум — це небажана перемінна напруга в провіднику. Електричний шум буває двох типів: *фоновий* і *імпульсний*. Електричний шум можна також розділити на низько-, середньо- і високочастотний. Джерелами фонового електричного шуму в діапазоні до 150кГц є лінії електропередачі, телефони і лампи денного світла; у діапазоні від 150 кГц до 20 МГц — комп'ютери, принтери, ксерокси; у діапазоні від 20МГц до 1ГГц — телевізійні і радіопередавачі, мікрохвильові печі. Основними джерелами імпульсного електричного шуму є мотори, перемикачі і зварювальні агрегати. Електричний шум виміряється в мілівольтах.
- *Діаметр чи площа перетину провідника*. Для мідних провідників досить вживаною є американська система AWG (American Wire Gauge), що вводить деякі умовні типи провідників, наприклад 22AWG, 24AWG, 26AWG. Чим більше номер типу провідника, тим менше його діаметр. В обчислювальних мережах найбільш поширеними є типи провідників, приведені вище як приклади. У європейських і міжнародних стандартах діаметр провідника вказується в міліметрах.

Приведений перелік характеристик далеко не повний, причому в ньому представлені тільки електромагнітні характеристики і його потрібно доповнити механічними і конструктивними характеристиками, що визначають тип ізоляції, конструкцію з'єднання і т.п. Крім універсальних характеристик, таких, наприклад, як загасання, що застосовуються для всіх типів кабелів, існують характеристики, що застосовуються тільки до визначеного типу кабелю. Наприклад, параметр крок скрутки проводів використовується тільки для характеристики крученої пари, а параметр NEXT застосуємо тільки до багатопарних кабелів на основі скручений пари.

Основна увага в сучасних стандартах приділяється кабелям на основі скрученої пари і волоконно-оптичним кабелям.

Кабелі на основі неекранованої скручений пари

Мідний неекранований кабель UTP в залежності від електричних і механічних характеристик розділяється на 5 категорій (Category 1 — Category 5). Кабелі категорій 1 і 2 були визначені в стандарті EIA/TIA-568, але в стандарт 568A вже не ввійшли, як застарілі [7].

Кабелі *категорії 1* застосовуються там, де вимоги до швидкості передачі мінімальні. Звичайно це кабель для цифрової й аналогової передачі голосу і малої швидкості (до 20 Кбіт/с) передачі даних. До 1983 року це був основний тип кабелю для телефонного зв'язку.

Кабелі *категорії 2* були вперше застосовані фірмою IBM при побудові власної кабельної системи. Головна вимога до кабелів цієї категорії — здатність передавати сигнали зі спектром до 1 Мгц.

Кабелі *категорії 3* були стандартизовані в 1991 році, коли був розроблений *Стандарт телекомунікаційних кабельних систем для комерційних будинків* (EIA-568), на основі якого потім був створений діючий стандарт EIA-568A, Стандарт EIA-568 визначив електричні характеристики кабелів категорії 3 для частот у діапазоні до 16МГц, що підтримують, таким чином, високошвидкісні мережеві додатки. Кабель категорії 3 призначений як для передачі даних, так і для передачі голосу. Крок скрутки проводів дорівнює приблизно 3 витки на 1 фут (30,5 см). Кабелі категорії 3 зараз складають основу багатьох кабельних систем будинків, у яких вони використовуються для передачі і голосу, і даних.

Кабелі *категорії 4* являють собою трохи поліпшений варіант кабелів категорії 3. Кабелі категорії 4 зобов'язані витримувати тести на частоті передачі сигналу 20МГц і забезпечувати підвищену перешкодостійкість і низькі втрати сигналу. Кабелі категорії 4 добре підходять для застосування в системах зі збільшеними відстанями (до 135 метрів) і в мережах Token Ring із пропускною здатністю 16Мбіт/с. На практиці використовуються рідко.

Кабелі *категорії 5* були спеціально розроблені для підтримки високошвидкісних протоколів. Тому їх характеристики визначаються в діапазоні д. 100Мгц. Більшість нових високошвидкісних стандартів

орієнтуються на використання кручений пари 5 категорії. На цьому кабелі працюють протоколи зі швидкістю передачі даних 100Мбіт/с - FDDI (з фізичним стандартом TP-PMD), Fast Ethernet, 100VG-AnyLAN, а також більш швидкісні протоколи — ATM на швидкості 155Мбіт/с, і Gigabit Ethernet на швидкості 1000Мбіт/с (варіант Gigabit Ethernet на кручений парі категорії 5 став стандартом у червні 1999 р.). Кабель категорії 5 прийшов на заміну кабелю категорії 3, і сьогодні всі нові кабельні системи великих будинків будуються саме на цьому типі кабелю (у сполученні з волоконно-оптичним).

Найбільш важливі електромагнітні характеристики кабелю категорії 5 мають наступні значення:

- повний хвильовий опір у діапазоні частот до 100Мгц дорівнює 100 Ом (стандарт ISO 11801 допускає також кабель із хвильовим опором 120 Ом);
- величина перехресних наведень NEXT у залежності від частоти сигналу повинна приймати значення не менш 74 дБ на частоті 150кГц і не менш 32дБ на частоті 100 Мгц;
- загасання має граничні значення від 0,8дБ (на частоті 64 кГц) до 22дБ (на частоті 100МГц);
- активний опір не повинний перевищувати 9,4 Ом на 100 м;
- ємність кабелю не повинна перевищувати 5,6 нф на 100 м.

Всі кабелі UTP незалежно від їхньої категорії випускаються в 4-парному виконанні. Кожна з чотирьох пар кабелю має визначений колір і крок скрутки. Звичайно дві пари призначені для передачі даних, а дві - для передачі голосу.

Для з'єднання кабелів з устаткуванням використовуються вилки і розетки RJ-45, що представляють 8-контактні роз'єми, схожі на звичайні телефонні роз'єми RJ-11.

Особливе місце займають *кабелі категорій 6 і 7*, що почали випускатися порівняно недавно. Для кабелю категорії 6 характеристики визначаються до частоти 200 Мгц, а для кабелів категорії 7 - до 600 Мгц. Кабелі категорії 7

обов'язково екрануються, причому як кожна пара, так і весь кабель у цілому. Кабель категорії 6 може бути як екранованим, так і неекранованим. Основне призначення цих кабелів — підтримка високошвидкісних протоколів на відрізках кабелю більшої довжини, чим кабель UTP категорії 5. Деякі фахівці сумніваються в необхідності застосування кабелів категорії 7, тому що вартість кабельної системи при їхньому використанні виходить порівнянною по вартості мережі з використанням волоконно-оптичних кабелів, а характеристики кабелів на основі оптичних волокон вище.

Кабелі на основі екранованої скручений пари

Екранована скручена пари STP добре захищає сигнали від зовнішніх перешкод, а також менше випромінює електромагнітних коливань зовні, що захищає, у свою чергу, користувачів мереж від шкідливого для здоров'я випромінювання. Наявність екрана, що заземлюється, здорожує кабель і ускладнює його прокладку, тому що вимагає виконання якісного заземлення. Екранований кабель застосовується тільки для передачі даних, а голос по ньому не передають [6].

Основним стандартом, що визначає параметри екранованої скручений пари, є стандарт IBM. У цьому стандарті кабелі поділяються не на категорії, а на типи: *Type 1, Type 2, ... , Type 9.*

Основним типом екранованого кабелю є кабель *Type 1* стандарту IBM. Він складається з 2-х пар скручених проводів, екранованих провідною оплеткою, яка заземлюється. Електричні параметри кабелю *Type 1* приблизно відповідають параметрам кабелю UTP категорії 5. Однак хвильовий опір кабелю *Type 1* дорівнює 150 Ом (UTP категорії 5 має хвильовий опір 100 Ом), тому простого "поліпшення" кабельної проводки мережі шляхом заміни неекранованої пари UTP на STP *Type 1* неможливо. Трансівери, розраховані на роботу з кабелем, що має хвильовий опір 100 Ом, будуть погано працювати на хвильовому опорі 150 Ом. Тому при використанні STP Type 1 необхідні відповідні трансивери. Такі трансивери існують в мережних адаптерах

Token Ring, тому що ці мережі розроблялися для роботи на екранованій кручений парі. Деякі інші стандарти також підтримують кабель STP Type 1 — наприклад, l00VG-AnyLAN, а також Fast Ethernet (хоча основним типом кабелю для Fast Ethernet є UTP категорії 5). У випадку якщо технологія може використовувати UTP і STP, потрібно переконатися, на який тип кабелю розраховані трансивери. Сьогодні кабель STP Type 1 включений у стандарти EIA/TIA-568A, ISO 11801 і EN50173, тобто придбав міжнародний статус.

Екрановані скручені пари використовуються також у кабелі IBM Type 2, що представляє кабель Type 1 з додатковими 2 парами неекранованого проводу для передачі голосу.

Для приєднання екранованих кабелів до устаткування використовуються роз'єми конструкції IBM.

Не всі типи кабелів стандарту IBM відносяться до екранованих кабелів — деякі визначають характеристики неекранованого телефонного кабелю (Type 3) і оптично-волоконного кабеля (Type 5).

Коаксіальні кабелі

Існує велика кількість типів коаксіальних кабелів, які використовуються у мережах різного типу — телефонних, телевізійних і комп'ютерних. Нижче приводяться основні типи і характеристики цих кабелів.

- **RG-8** і **RG-11** — "товстий" коаксіальний кабель, розроблений для мереж Ethernet l0Base-5. Має хвильовий опір 50 Ом і зовнішній діаметр 0,5 дюйма (близько 12 мм). Цей кабель має досить товстий внутрішній провідник діаметром 2,17 мм, що забезпечує гарні механічні й електричні характеристики (загасання на частоті 10Мгц — не гірше 18 дБ/км). Зате цей кабель складно монтувати — він погано гнеться.
- **RG-58/U, RG-58 A/U** і **RG-58 C/U** — різновиди "тонкого" коаксіального кабелю для мереж Ethernet l)Base-2. Кабель RG-58/U має суцільний

внутрішній провідник, а кабель RG-58 A/U — багатожильний. Кабель RG-58 C/U проходить "військове приймання". Усі ці різновиди кабелю мають хвильовий опір 50 Ом, але мають гірші механічні й електричні характеристики в порівнянні з "товстим" коаксіальним кабелем. Тонкий внутрішній провідник 0,89мм не так міцний, зате має набагато більшу гнучкість, зручний при монтажних роботах. Загасання в цьому типі кабелю вище, ніж у "товстому" коаксіальному кабелі, що приводить до необхідності зменшувати довжину кабелю для одержання однакового загасання в сегменті. Для з'єднання кабелів з устаткуванням використовується роз'єм типу BNC.

- **RG-59** — телевізійний кабель із хвильовим опором 75 Ом. Широко застосовується в кабельному телебаченні.
- **RG-62** — кабель із хвильовим опором 93 Ом, використовувався в мережах ArcNet, устаткування яких сьогодні практично не випускається. Коаксіальні кабелі з хвильовим опором 50 Ом (тобто "тонкий" і "товстий") описані в стандарті EIA/TIA-568. Новий стандарт EIA/TIA-568A коаксіальні кабелі не описує, як морально застаріли.

Волоконно-оптичні кабелі

Волоконно-оптичні кабелі складаються з центрального провідника світла (серцевини) — скляного волокна, оточеного іншим шаром скла — оболонкою, що володіє меншим показником переломлення, чим серцевина. Поширюючи по серцевині, промені світла не виходять за її межі, відбиваючись від покриваючого шару оболонки. У залежності від розподілу показника переломлення і від величини діаметра сердечника розрізняють [8]:

- багатомодові волокно зі східчастою зміною показника переломлення (рис.4.11 а);
- багатомодові волокно з плавною зміною показника переломлення (рис.4.11 б);
- одномодове волокно (рис.4.11 в) .

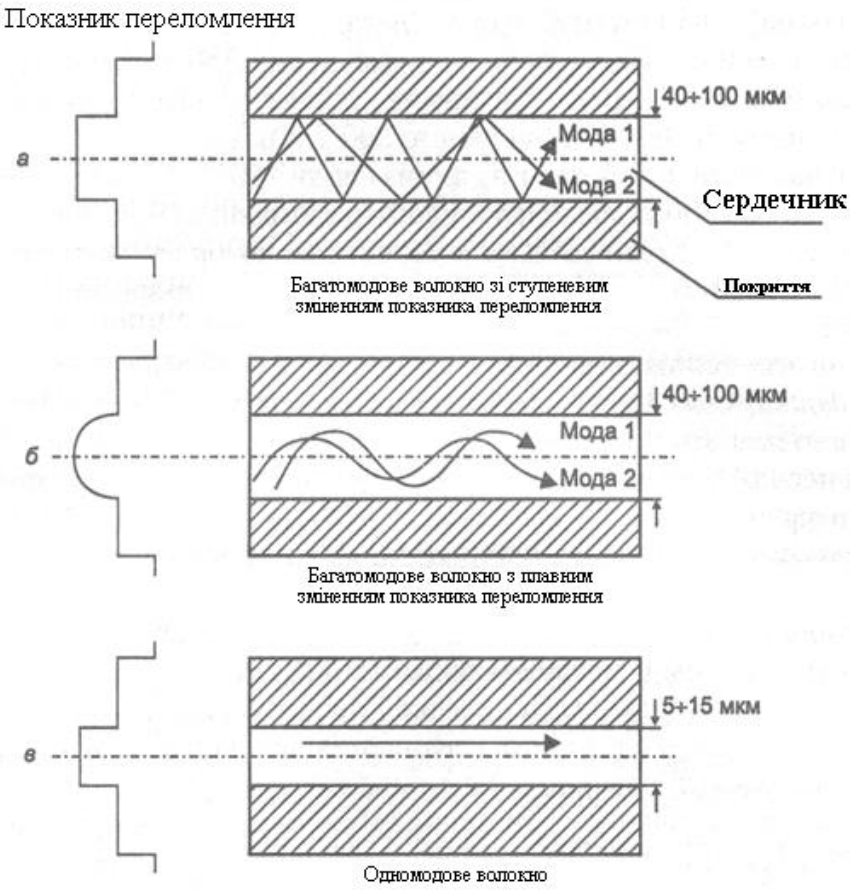


Рис. 3.14 Волоконно-оптичні кабелі

Одномодовий кабель

Поняття "мода" описує режим поширення світлових променів у внутрішньому сердечнику кабелю.

В одномодовому кабелі (*Single Mode Fiber, SMF*) використовується центральний провідник дуже малого діаметра, порівняно з довжиною хвилі світла — від 5 до 10 мкм. При цьому практично всі промені світла поширюються уздовж оптичної осі світловода, не відбиваючи від зовнішнього провідника. Смуга пропускання одномодового кабелю дуже широка — до сотень гігагерць на кілометр.

Недоліки

Виготовлення тонких якісних волокон для одномодового кабелю представляє складний технологічний процес, що робить одномодовий кабель досить дорогим.

Крім того, у волокно такого маленького діаметра досить складно направити пучок світла, не втративши при цьому значну частину його енергії.

Багатомодовий кабель

У багатомодових кабелях (*Multi Mode Fiber, MMF*) використовуються більш широкі внутрішні сердечники, що легше виготовити технологічно.

У стандартах визначені два найбільш вживаних багатомодових кабелі: 62,5/125 мкм і 50/125 мкм, де 62,5 мкм чи 50 мкм — це діаметр центрального провідника, а 125 мкм — діаметр зовнішнього провідника.

У багатомодових кабелях у внутрішньому провіднику одночасно існує кілька світлових променів, що відбиваються від зовнішнього провідника під різними кутами. Кут відображення променя називається *модою променя*. У багатомодових кабелях із плавною зміною коефіцієнта переломлення режим поширення кожної моди має більш складний характер.

Багатомодові кабелі мають більш вузьку смугу пропускання — від 500 до 800 Мгц/км. Звуження смуги відбувається через втрати світлової енергії при відображеннях, а також через інтерференцію променів різних мод [8].

Як джерела випромінювання світла у волоконно-оптичних кабелях застосовуються:

- світлодіоди;
- напівпровідникові лазери.

Для одномодових кабелів застосовуються тільки напівпровідникові лазери, тому що при такому малому діаметрі оптичного волокна світловий потік, який створюється світлодіом, неможливо без великих втрат направити у волокно.

Для багатомодових кабелів використовуються більш дешеві світлодні випромінювачі.

Для передачі інформації застосовується світло з довжиною хвилі 1550 нм (1,55 мкм), 1300 нм (1,3 мкм) і 850 нм (0,85 мкм).

Світлодіоди можуть випромінювати світло з довжиною хвилі 850 нм і 1300 нм. Випромінювачі з довжиною хвилі 850 нм істотно дешевше, ніж

випромінювачі з довжиною хвилі 1300 нм, але смуга пропускання кабелю для хвиль 850 нм уже, наприклад 200 Мгц/км замість 500 Мгц/км.

Лазерні випромінювачі працюють на довжинах хвиль 1300 і 1550 нм.

Швидкодія сучасних лазерів дозволяє модулювати світловий потік з частотами 10 Ггц і вище.

Лазерні випромінювачі створюють когерентний потік світла, за рахунок чого втрати в оптичних волокнах стають менше, ніж при використанні некогерентного потоку світлодіодів.

Безкабельні канали зв'язку

Крім кабельних каналів у комп'ютерних мережах іноді використовуються також безкабельні канали.

Їх головна перевага полягає в тому, що не потрібно ніякої прокладки проводів (не треба робити отворів в стінах, закріплювати кабель у трубах і жолобах, прокладати його під фальшполами, над підвісними стелями або у вентиляційних шахтах, шукати і усувати пошкодження). До того ж комп'ютери мережі можна легко переміщувати в межах кімнати або будівлі, так як вони ні до чого не прив'язані.

Радіоканал використовує передачу інформації по радіохвилях, тому теоретично він може забезпечити зв'язок на багато десятків, сотні і навіть тисячі кілометрів.

Швидкість передачі досягає десятків мегабіт в секунду (тут багато що залежить від обраної довжини хвилі і способу кодування).

Особливість радіоканалу полягає в тому, що сигнал вільно випромінюється в ефір, він не замкнутий в кабель, тому виникають проблеми сумісності з іншими джерелами радіохвиль (станціями радіо- і телерадіовіщання, радарами, радіолюбительськими і професійними передавачами і т.д.).

В радіоканалі використовується передача у вузькому діапазоні частот і модуляція інформаціонним сигналом сигналу несучої частоти.

Головним недоліком радіоканалу є :

- *його поганий захист від прослуховування, так як радіохвилі поширюються неконтрольовано.*
- *слабка перешкодозахищеність.*

Для локальних бездротових мереж (WLAN - Wireless LAN) в даний час застосовуються підключення по радіоканалу на невеликих відстанях (зазвичай до 100 метрів) і в межах прямої видимості.

Найчастіше використовуються два частотні діапазони - 2,4 ГГц і 5 ГГц.

Швидкість передачі - до 54 Мбіт/с (в 2009-му році затвердили стандарт 802.11n, який дозволяв досягати швидкість 150Мбіт/с при одній антені і навіть більше при більшій кількості антен). Поширений варіант зі швидкістю 11 Мбіт/с.

Мережі WLAN дозволяють встановлювати бездротові мережні з'єднання на обмеженій території (зазвичай всередині офісного або університетського будинку або в таких громадських місцях, як аеропорти).

Вони можуть використовуватися в тимчасових офісах або в інших місцях, де прокладка кабелів нездійсненна, а також в якості доповнення до наявної провідної локальної мережі, покликаного забезпечити користувачам можливість працювати, переміщаючись по будинку.

Популярна технологія *Wi-Fi (Wireless Fidelity)* дозволяє організувати зв'язок між комп'ютерами числом від 2 до 15 за допомогою концентратора (званого точкою доступу, *Access Point, AP*), або декількох концентраторів, якщо комп'ютерів від 10 до 50.

Крім того, ця технологія дає можливість зв'язати дві локальні мережі на відстані до 25 кілометрів за допомогою потужних бездротових мостів. Для прикладу на рис. показано об'єднання комп'ютерів за допомогою однієї точки доступу.

Важливо, що багато мобільні комп'ютери (ноутбуки) уже мають вбудований контроллер *Wi-Fi*, що істотно спрощує їх підключення до бездротової мережі.

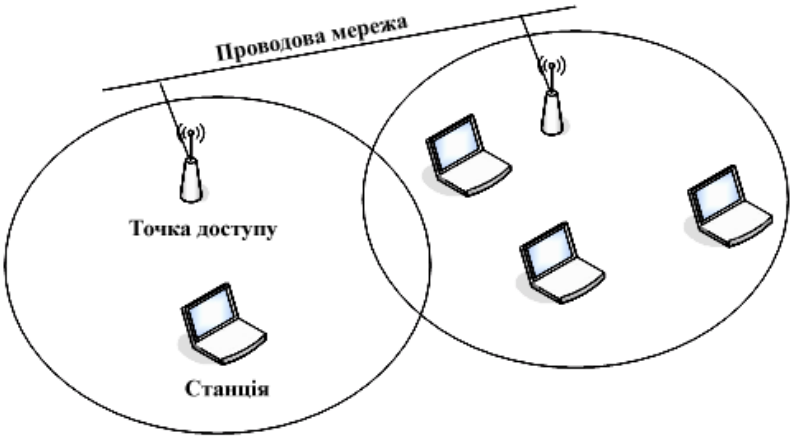


Рис. 3.15. Об'єднання комп'ютерів за допомогою однієї точки доступу

Радіоканал широко застосовується в глобальних мережах як для наземної, так і для супутникового зв'язку.

У цьому застосуванні у радіоканаланет конкурентів, так як радіохвилі можуть дійти до будь-якої точки земної кулі.

Інфрачервоний канал також не вимагає сполучних проводів, так як використовує для зв'язку інфрачервоне випромінювання (подібно пульту дистанційного керування домашнього телевізора).

Головна його перевага в порівнянні з радіоканалом - нечутливість до електромагнітних завад, що дозволяє застосовувати його, наприклад, в виробничих умовах, де завжди багато перешкод від силового обладнання. Правда, в даному випадку потрібно досить висока потужність передачі, щоб не впливали ніякі інші джерела теплового (інфрачервоного) випромінювання.

Погано працює інфрачервоний зв'язок і в умовах сильної запиленості повітря. Швидкості передачі інформації по інфрачервоному каналу зазвичай не перевищують 5-10 Мбіт/с, але при використанні інфрачервоних лазерів може бути досягнута швидкість більше 100 Мбіт/с.

Секретність переданої інформації, як і в випадку радіоканалу, не досягається, також потрібні порівняно дорогі приймачі і передавачі. Все це призводить до того, що застосовують інфрачервоні канали в локальних мережах досить рідко. В основному вони використовуються для зв'язку комп'ютерів з периферією (*інтерфейс IrDA*).

Інфрачервоні канали діляться на дві групи:

• *Канали прямої видимості, в яких зв'язок здійснюється на променях, що йдуть безпосередньо від передавача до приймача. При цьому зв'язок можливий тільки при відсутності перешкод між комп'ютерами мережі. Зате протяжність каналу прямої видимості може досягати декількох кілометрів.*

• *Канали на розсіяному випромінюванні, які працюють на сигналах, відбитих від стін, стелі, підлоги та інших перешкод.*

Перешкоди в даному випадку не перешкода, але зв'язок може здійснюватися тільки в межах одного приміщення.

Якщо говорити про можливі топології, то найприродніше всі бездротові канали зв'язку підходять для топології типу шина, в якій інформація передається одночасно всім абонентам.

Але при використанні вузьконаправленої передачі і/або частотного поділу по каналах можна реалізувати будь-які топології (кільце, зірка, комбіновані топології) як на радіоканалі, так і на інфрачервоному каналі.

Контрольні питання до розділу

1. Мідний неекранований кабель UTP в залежності від електричних і механічних характеристик розділяється на 5 категорій. Кабелі *категорії 2* застосовуються:
    a. *при передачі сигналів зі спектром до 1 Мгц;*
    b. *де вимоги до швидкості передачі мінімальні;*
    c. *для передачі даних та передачі голосу для частот у діапазоні до 16МГц;*
    d. *для передачі даних при частоті передачі сигналу 20МГц і забезпечують підвищену перешкодостійкість і низькі втрати сигналу;*
    e. *для передачі даних в діапазоні до 100Мгц.*
2. Характеризує достовірність переданих даних при впливі на сигнал адитивного білого гауссовского шуму, за умови, що послідовність символів відновлена ідеальним демодулятором. Визначається мінімальним співвідношенням сигнал / шум, який необхідний для передачі даних через канал з ймовірністю помилки, що не перевищує задану. Це -
    a. *Енергетична ефективність;*
    b. *Спектральна ефективність;*

c. *Лінійність підсилювачів;*
d. *Стійкість до впливів каналу передачі;*
e. *Складність реалізації.*

3. Канали, що дають можливість передавати почергово інформацію у двох напрямках:
   a. *симплексні;*
   b. *комплексні;*
   c. *напівдуплекні;*
   d. *дуплексні;*
   e. *складені.*
4. Для посилення сигналів з деякими видами модуляції можуть бути використані нелінійні підсилювачі, що дозволяє істотно знизити енергоспоживання передавача, при цьому рівень позасмугового випромінювання не перевищує допустимих меж. Це –
   a. *Енергетична ефективність;*
   b. *Спектральна ефективність;*
   c. *Стійкість до впливів каналу передачі;*
   d. *Лінійність підсилювачів;*
   e. *Складність реалізації.*
5. До основних характеристик ліній зв'язку відносяться:
   a. *амплітудно-частотна характеристика;*
   b. *смуга пропускання;*
   c. *загасання;*
   d. *перешкодостійкість;*
   e. *перехресні наведення на дальному кінці лінії;*
   f. *пропускна здатність;*
   g. *вірогідність передачі даних.*
6. Мідний неекранований кабель UTP в залежності від електричних і механічних характеристик розділяється на 5 категорій. Кабелі *категорії 1* застосовуються:
   а) при передачі сигналів зі спектром до 1 Мгц;
   б) де вимоги до швидкості передачі мінімальні;
   в) для передачі даних та передачі голосу для частот у діапазоні до 16МГц;
   г) для передачі даних при частоті передачі сигналу 20МГц і забезпечують підвищену перешкодостійкість і низькі втрати сигналу;
   д) для передачі даних в діапазоні до 100Мгц.
7. Мідний неекранований кабель UTP в залежності від електричних і механічних характеристик розділяється на 5 категорій. Кабелі *категорії 2* застосовуються:
   a. *при передачі сигналів зі спектром до 1 Мгц;*
   b. *де вимоги до швидкості передачі мінімальні;*
   c. *для передачі даних та передачі голосу для частот у діапазоні до 16МГц;*

d. *для передачі даних при частоті передачі сигналу 20МГц і забезпечують підвищену перешкодостійкість і низькі втрати сигналу;*
e. *для передачі даних в діапазоні до 100Мгц.*

8. Мідний неекранований кабель UTP в залежності від електричних і механічних характеристик розділяється на 5 категорій. Кабелі *категорії 3* застосовуються:
   a. *при передачі сигналів зі спектром до 1 Мгц;*
   b. *де вимоги до швидкості передачі мінімальні;*
   c. *для передачі даних та передачі голосу для частот у діапазоні до 16МГц;*
   d. *для передачі даних при частоті передачі сигналу 20МГц і забезпечують підвищену перешкодостійкість і низькі втрати сигналу;*
   e. *для передачі даних в діапазоні до 100Мгц.*
9. Що собою представляють кабельні лінії?
10. Що собою представляє скручена пара?
11. Які різновиди скручених пар існують?
12. Що собою представляє коаксіальний кабель?
13. Що собою представляє волоконно-оптичний кабель?
14. Що собою представляють радіоканали наземного і супутникового зв'язку?
15. На скільки груп поділяються діапазони електромагнітного спектру і відповідні їм бездротові системи передавання інформації?
16. Що собою представляє канал передачі даних?
17. Яка апаратура входить до складу апаратури передачі даних?
18. Що собою представляє спектральний аналіз сигналів на лініях зв'язку?
19. Що собою представляє амплітудно-частотна характеристика каналу?
20. Що собою представляє пропускна здатність лінії?
21. Що собою представляє загасання каналу?
22. Який існує зв'язок між пропускною здатністю лінії і її смугою пропущення?
23. Що собою представляє перешкодостійкість лінії ?
24. Що собою представляє перехресні наведення на ближньому кінці (Near End Cross Talk — NEXT)?
25. Що собою представляє вірогідність передачі даних ?
26. Які стандарти існують для кабелів?
27. Які найбільш важливі характеристики розглядаються у стандартах кабелів?
28. Наведіть особливості кабелів на основі неекранованої скручений пари ?
29. Наведіть особливості кабелів на основі екранованої скручений пари ?
30. Наведіть особливості коаксіального кабеля. «Товстий» та «тонкий» коаксіальний кабель ?
31. Наведіть особливості волоконно-оптичного кабеля?
32. Одномодовий волоконно-оптичний кабель. Переваги та недоліки?
33. Багатомодовий волоконно-оптичний кабель. Переваги та недоліки?

34. З якою довжиною хвилі застосовується світло для передачі інформації в одномодовому та багатомодовому кабелях?

35. Наведіть переваги та недоліки радіоканалу?

36. Які особливості використання інфрачервоних каналів?

37. Канали, що забезпечують передачу інформації тільки в одному напрямку:

a. *дуплексні;*
b. *симплексні;*
c. *напівдуплексні;*
d. *комплексні.*

38. Розрізняють наступні волоконно-оптичні кабелі:

a. *багатомодове волокно зі східчастою зміною показника переломлення;*
b. *багатомодове волокно зі східчастою зміною показника загасання;*
c. *багатомодове волокно з плавною зміною показника переломлення;*
d. *багатомодове волокно з плавною зміною показника загасання;*
e. *одномодове волокно з плавною зміною показника загасання;*
f. *одномодове волокно зі східчастою зміною показника переломлення.*

Список рекомендованої літератури

1. *Баскаков С. И.* Радиотехнические цепи и сигналы : учебник / С. И. Баскаков. – М. : Высшая школа, 1983. – 536 с.
2. *А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В.* Пасічник Комп'ютерні мережі [навчальний посібник] – Львів, «Магнолія 2006», 2013. – 256 с.
3. *Беркман Л.Н., Жураковський Б.Ю., Твердохліб М.Г.* Типові сигнали та завади в електрозв'язку [Навчальний посібник]. - К.: ДУТ, 2015.- 92с.
4. *Стеклов В.К., Беркман Л.Н.* Телекомунікаційні мережі. – К.: Техніка, 2001.– 392 с.
5. Теория передачи сигналов: учебник для вузов / *А. Г. Зюко, Д. Д. Кловский, М. В. Назаров, Л. М. Финк.* – М. : Радио и связь, 1986. – 304 с.
6. *Bohdan Zhurakovskiy, Nataliia Tsopa* Assessment Technique and Selection of Interconnecting Line of Information Networks 2019. // 3rd International Conference on Advanced Information and Communications Technologies (AICT) IEEE, 2019/7/2, - p. 71-75
7. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
8. *Однорог П. М., Михайленко Є. В., Котенко М. О. Омецінська О. Б.* Під редакцією Катка В. Б. Пасивні оптичні мережі доступу (xPON). – К.:ДУІКТ, 2006. – 65 с.

Розділ 4. БАЗОВІ ПРИНЦИПИ ПОБУДОВИ ТА КОМПОНЕНТИ КОМП'ЮТЕРНИХ МЕРЕЖ

4.1. Абонентські, адміністративні та асоціативні системи

Абонентські системи призначені для опрацювання прикладних процесів користувачів, і діляться на сім рівнів.

Прикладні процеси керування мережею	Прикладні процеси користувачів
7'	7
6'	6
5'	5
4'	4
3'	3
2'	2
1'	1
Фізичні засоби з'єднання	

Рис. 4.1. Структура абонентської і адміністративної систем.

Паралельно в системі реалізується ієрархія протоколів, що підтримують прикладні процеси керування мережею. Ці протоколи можуть бути тими ж, що й в ієрархії, що підтримує прикладні процеси користувачів, але можуть і відрізняться від них. Всі рівні в системі зв'язані з процесом керування системою.

Необхідно по можливості розвантажити центральну електронну машину абонентської системи від виконання функцій області взаємодії і дати їй можливість ефективно виконувати прикладні процеси. З цією метою абонентську систему поділяють на дві частини: термінальне устаткування і станцію.

Термінальне устаткування є основною частиною системи, що виконує прикладні процеси і, можливо, протоколи верхніх рівнів. *Станція* є допоміжною частиною системи, що реалізує протоколи нижніх або всіх рівнів.

У залежності від числа реалізованих протоколів, станцію називають канальною, транспортною або абонентською. Канальна станція виконує протоколи рівнів 1 - 2; транспортна - протоколи 1 - 4. Абонентська станція реалізує сім рівнів області взаємодії відкритих систем [1].

Станція і термінальне устаткування з'єднуються каналом або шиною. У обох випадках це з'єднання повинно бути подано спеціальним фізичним (1) і канальним (2) протоколами. Перший з них визначає характеристики каналу, а другий описує процедури керування каналом і передачу через них блоків даних. Спеціальні протоколи (1' і 2') не є стандартами ISO. Вони залежать від конкретних обраних каналів, методом зв'язку термінального устаткування зі станціями [1].

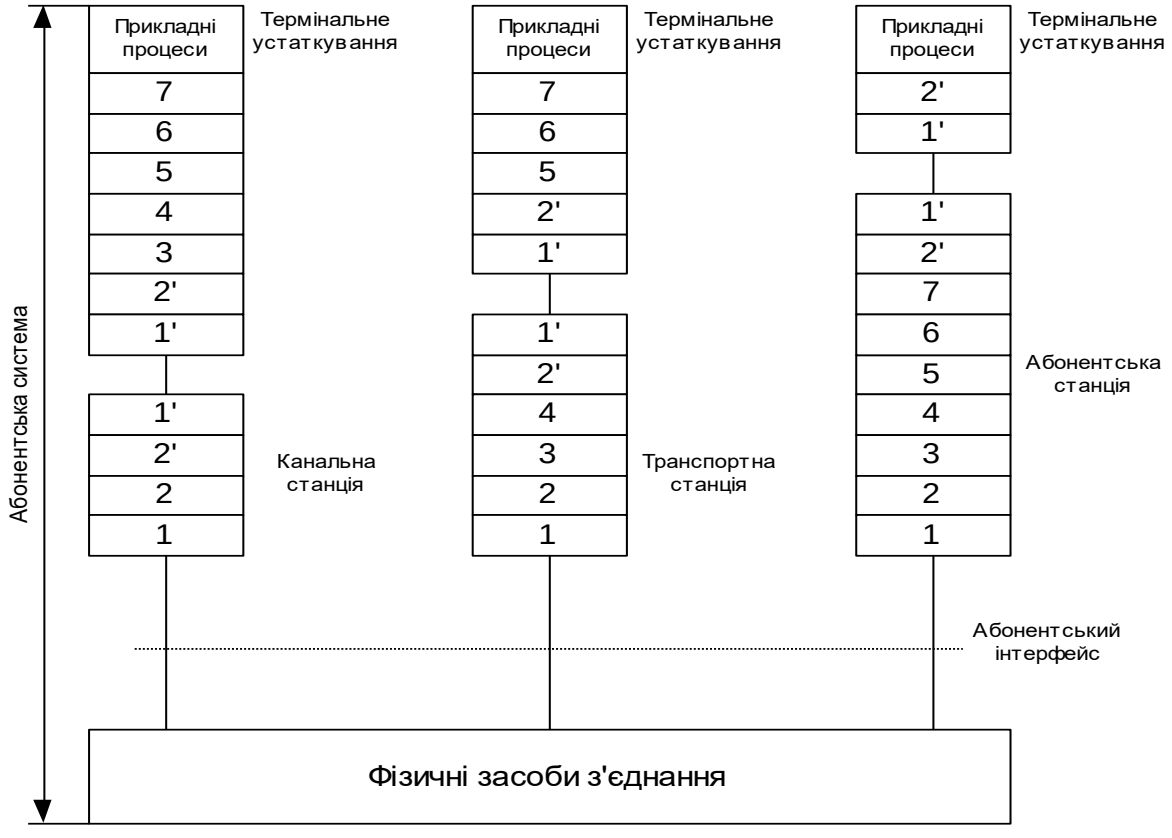


Рис. 4.2. Станції і абоненти.

*Канальна станція*_є найбільш проста, тому що реалізує лише протоколи рівнів (1,2) області взаємодії. Але ця простота вимагає серйозного завантаження абонента, котрий повинен виконувати функції, описувані протоколами інших п'яти рівнів.

Привабливою є *абонентська станція,* що цілком розвантажує термінальне устаткування від виконання задач, що забезпечують взаємодію в мережі прикладних процесів. Однак у складному термінальному устаткуванні часто працюють кілька комплексів прикладних процесів. Обмін інформацією між ними відбувається через сеансовий рівень. Тому в тих випадках, коли рівень 5 знаходиться в станції, робота термінального устаткування виявляється залежної від надійності,завадостійкісті і пропускної здатності каналу і станції, що не завжди прийнятно.

Тому на практиці найчастіше використовується транспортна станція. Вона виконує усі функції, зв'язані з передачею інформації між комплексами термінального устаткування через усю комунікаційну підмережу. Що стосується термінального устаткування, то воно забезпечує роботу прикладних процесів, що підтримуються прикладним, представницьким і сеансовими протоколами.

Абонентські системи є основними компонентами інформаційної мережі. Ці системи будуються на основі великих і малих ЕОМ, виготовлених великим числом виробників різних країн. Тому для кожного типу комутаційної підмережі розробляється абонентський інтерфейс, що визначає параметри і процедури взаємодії всіх абонентських систем з комунікаційної підмережею.

Адміністративні системи мають ту ж структуру, що і абонентські. Тут замість прикладних процесів користувачів працюють прикладні процеси керування мережею чи її частиною.

Асоціативна система на відміну від абонентської й адміністративної не здійснює обробку інформації для нестатків користувачів і керування мережею. Вона призначена для з'єднання в єдине ціле частин інформаційних мереж і забезпечення взаємодії цих мереж одина з одною [1].

У залежності від характеристик поєднуваних частин мереж виділяють чотири типи асоціативних систем.

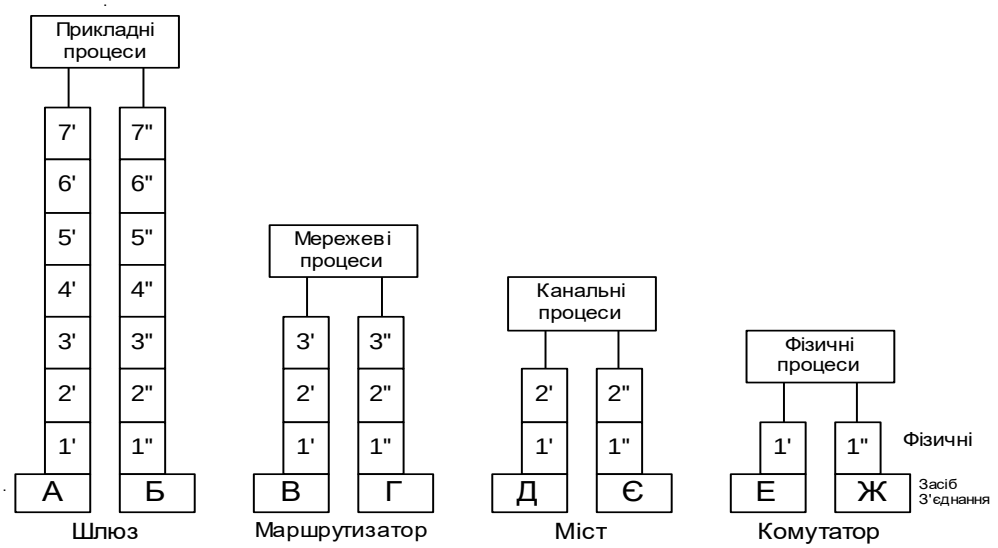


Рис. 4.3. Типи асоціативних систем.

Найбільш складної з них є ***шлюз.*** Він забезпечує взаємодію двох чи більш інформаційних мереж з різними наборами протоколів семи рівнів. На малюнку показані два набори: 1' - 7' і 1" - 7", зв'язані спеціальними прикладними процесами. Ці процеси перетворять один семирівневий табель протоколів в інший, забезпечуючи необхідну взаємодію.

Шлюзи найчастіше використовуються в тих випадках, коли потрібно об'єднати інформаційні мережі, створені за різними стандартами. Коли ж проектується група мереж у відповідності зі стандартами ISO, доцільний інший підхід. У цьому випадку в мережах, що з'єднуються, протоколи рівнів 4 - 7 робляться однаковими. Це дозволяє для з'єднання мереж використовувати не шлюзи, а більш прості асоціативні системи - машрутизатори і мости.

Задачею ***маршрутизатора*** є забезпечення взаємодії комунікаційних підмереж. Вони характеризуються лише трьома рівнями протоколів.

Тому логічна структура маршрутизатора має вид, показаний на малюнку. Як випливає з малюнка, маршрутизатор "не знає" протоколів рівнів 4 - 7 і є прозорим для них. У його задачу входить перетворення протоколів трьох нижніх рівнів. Іноді в інформаційних мережах маршрутизатори зв'язують частини комунікаційної підмережі, у яких використовуються однакові протоколи рівнів 1 - 3. У цих випадках у маршрутизаторах, що називаються вузлами комутації пакетів, перетворення протоколів не виконується. Тут

мережні процеси здійснюють лише комутацію і маршрутизацію інформації. У з'єднувальних вузлами підмережах повинна бути здійснена загальна адресація абонентських систем [1].

Мости призначені для з'єднання частин мереж, різних типів каналів передачі даних, наприклад циклічного кільця з моноканалом. Будь-який канал визначається протоколами рівнів 1 - 2, тому логічна структура моста має дворівневу структуру. Канальні процеси тут перетворять протоколи обох рівнів. При використанні методів, що з'єднуються у підмережах повинні бути погоджені структура, адрес і розмір кадрів [2].

Найбільш просту структуру має комутатор. Це зв'язано з тим, що він з'єднує один з одним тільки канали передачі даних, утворюючи необхідну фізичну базу тракту передачі інформації між абонентськими системами. У тому випадку, коли до комутатора підходить більше двох каналів він виконує функції, зв'язані з комутацією інформації. Комутація здійснюється прозорим способом, тобто без якої-небудь обробки цієї інформації. При будь-якому числі каналів, що з'єднуються, комутатор забезпечує посилення переданих сигналів і коректує крутість їхніх фронтів. Комутатор не має буферів, тому він прозорий для інформації. Комутатор вимагає, щоб швидкості передачі даних по сусідніх каналах були однакові. Фізичні процеси, виконувані комутатором, реалізуються апаратно.

Таким чином, асоціативні системи реалізують апаратно-мережні, канальні і фізичні процеси. Задачею їх є виконання функцій, у тому числі перетворення, необхідних для з'єднання частин чи мереж цілих мереж.

4.2. Комплекс базових профілів

Комплекс базових профілів охоплює два рівні області взаємодії відкритих систем: канальний і фізичний. Ці стандарти прийняті Міжнародною організацією стандартів ISO.

Комплекс включає два загальних стандарти ISO 8802/1, ISO 8802/2 і чотири спеціальних ISO 8802/3 - 8802/6. Вони визначають базу чотирьох типів

інформаційних мереж із селекцією інформації.

Канальний рівень розділений на дві частини. Операції, виконувані на підрівні 2Б, зв'язані зі створенням логічного зв'язку між абонентськими системами мережі. Підрівень 2А забезпечує доступ до фізичних портів мережі, а також, об'єднуючись із фізичним рівнем, створює основу для опису чотирьох типів базових профілів.

Стандарт ISO ***8802/2*** визначає на підрівні 2Б функції керування логічним каналом. Він не залежить від типу використовуваних фізичних засобів з'єднання, тому є загальним для чотирьох базових профілів. Обумовлені стандартом функції охоплюють опис переданих по мережі блоків інформації, іменованих кадрами.

Розглянутий стандарт забезпечує виконання двох видів сервісу. Перший із них не орієнтований на встановлення з'єднання, тому інформація передається і приймається без попередження партнера. Другий вид сервісу забезпечує попереднє створення з'єднання, по якому потім передаються кадри.

Структура стандартів 802.

Стандарт 8802/3 визначає моноканал із випадковим доступом. Моноканал може бути фізичним, тобто може використовувати фізичні засоби з'єднання (наприклад, кабель, скручену пару проводів) цілком.

Моноканал може бути і приватним, коли він використовує лише виділену йому смугу частот у фізичних засобах з'єднання.

Сутність методу випадкового доступу в моноканал у стандарті 8802/3 полягає в наступному. Абонентська система, що бажає взаємодіяти з одним або

декількома партнерами, прослухує моноканал, очікуючи; коли по ньому закінчиться передача сигналів іншій системою. При звільненні моноканала абонентська система починає передачу інформації. При цьому система може почути, що одночасно початку передачу ще одна система (у каналі відбулося сутичку кадрів). Тільки з'явиться сутички всі системи передачу припиняють. Після довільного (для кожної системи) інтервалу часу передача починається знову. При повторних сутичках система після кожної спроби подвоює час чекання [1].

Метод випадкового доступу, дуже простий, надійний, але ефективний тільки при відносно невеликому трафіку. Якщо ж частота передачі пакетів через моноканал стає великий, то швидко зростає число сутичок і ефективність каналу падає.

Стандарт 8804/4 описує функціонування моноканала з повноваженнями. Цей моноканал, як і моноканал із випадковим доступом, може бути фізичним або частотним. З погляду передачі інформації вхідні в моноканал абонентські системи утворять логічну каблучку. Кожній системі привласнюється адреса і їй відомі адреси попередньої (у логічній каблучці) і наступних систем.

Тут у моноканалі немає сутички кадрів, тому що кожна система передає інформацію, тільки отримавши на цей дозвіл, називаний повноваженням. Закінчивши передачу, система передає повноваження наступної по логічній каблучці системі. Володіти повноваженням система може тільки обмежений час. Моноканал із передачею повноважень є досить складним. Але моноканальна мережа забезпечує роботу в режимі реального часу, тому що вихід із ладу складного устаткування може привести до розриву логічної каблучки і блоки даних у потрібний час не потраплять до адресата. Додавання в мережу або видалення з неї абонентської системи вимагає переадресації систем у логічній каблучці.

Стандарт 8802/5 визначає циклічне кільце, створене на основі кільцевого каналу, у який включаються абонентські системи. Метод доступу в циклічне кільце заснований на передачі по ньому повноваження, що дозволяє черговій системі передачу інформації. Для керування повноваженнями одна з

абонентські систем стає активним монітором, що відповідає за виявлення і виправлення помилок у каблучці.

Стандарт 8802/6 описує мережа, що призначена для великого міста. Ця комунікаційна підмережа призначена для передачі не тільки даних, але і промови і відео зображень. Підмережа є складним моноканалом із двома рівнобіжними загальними каналами. Тому її називають "Подвійна шина".

Цей комплекс визначає не тільки характеристики чотирьох комунікаційних підмереж, але й описує єдину схему підключення в підмережі абонентської системи.

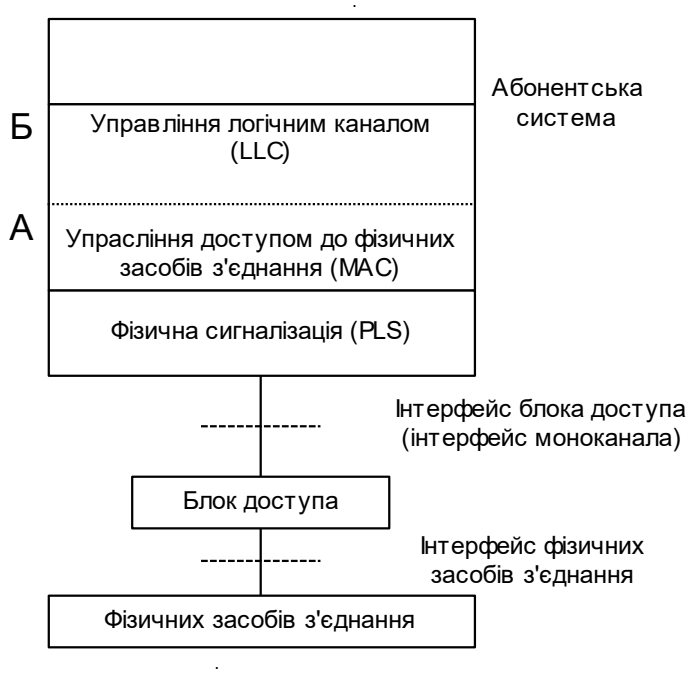


Рис. 4.4 Схема підключення абонентської системи.

У ній комунікаційна підмережа ділиться на дві частини: фізичні засоби з'єднання і блоки доступу. Заради стандартизації для блока доступу визначаються два інтерфейси. Один із них описує підключення блока до фізичних засобів з'єднання, а іншій - до абонентської системи. У любому з чотирьох розглянутих функціональних профілів визначаються тільки два рівні: канальний (2) і фізичний (1). Тому профілі є базовими і служать опорою, на основі якої можуть, будуються різні (і навіть не сумісні) інформаційні мережі.

4.3. Апаратура локальних мереж

Апаратура локальних мереж забезпечує реальний зв'язок між абонентами. Вибір апаратури має найважливіше значення на етапі проектування мережі, так як вартість апаратури становить найбільш суттєву частину від вартості мережі в цілому, а заміна апаратури пов'язана не тільки з додатковими витратами, але часто і з трудомісткими роботами. До апаратурі локальних мереж відносяться [3]:

- *кабелі для передачі інформації;*
- *роз'єми для приєднання кабелів;*
- *термінатори;*
- *мережеві адаптери;*
- *репітери;*
- *трансівери;*
- *концентратори;*
- *мости;*
- *маршрутизатори;*
- *шлюзи.*

Термінатори

Треба враховувати, що через особливості поширення електричних сигналів по довгих лініях зв'язку необхідно передбачати включення на кінцях шини спеціальних узгоджувальних пристроїв, ***термінаторів***.

Рис. 4.5. Підключення термінаторів

Без включення термінаторів сигнал відбивається від кінця лінії і спотворюється так, що зв'язок по мережі стає неможливою.

У разі розриву або пошкодження кабелю порушується узгодження лінії зв'язку, і припиняється обмін навіть між тими комп'ютерами, які залишилися з'єднаними між собою. Коротке замикання в будь-якій точці кабелю шини виводить з ладу всю мережу.

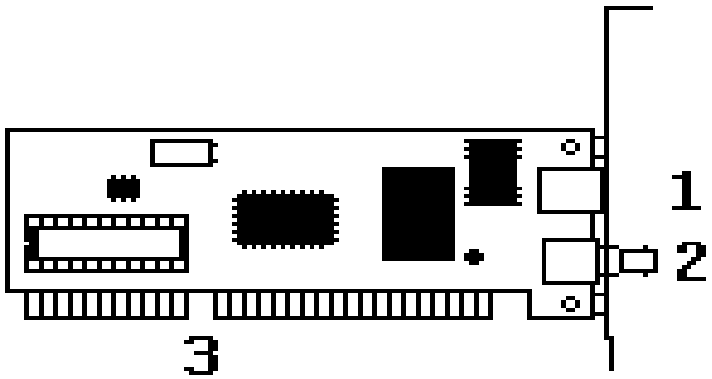
Мережеві адаптери

Мережеві адаптери (вони ж контролери, карти, плати, інтерфейси, *NIC - Network Interface Card*) - це основна частина апаратури локальної мережі.

Призначення мережевого адаптера - сполучення комп'ютера (або іншого абонента) з мережею, тобто забезпечення обміну інформацією між комп'ютером і каналом зв'язку відповідно до прийнятих правил обміну. Саме вони реалізують функції двох нижніх рівнів моделі OSI [4].

Як правило, мережеві адаптери виконуються у вигляді плати, що вставляється в слоти розширення системної магістралі (шини) комп'ютера (найчастіше *PCI, ISA або PC-Card*).

Плата мережного адаптера зазвичай має також один або кілька зовнішніх роз'ємів для підключення до неї кабелю мережі.



1 – роз'єм крученої пари;
2 – роз'єм коаксіального кабелю;
3 – роз'єм слоту ISA.

Рис. 4.6. Мережний адаптер

Наприклад, мережеві адаптери *Ethernet* можуть випускатися з наступними наборами роз'ємів:

• *TPO* - роз'єм *RJ-45* (для кабелю на кручених парах по стандарту *10BASE-T*).

• *TPC* - роз'єми *RJ-45* (для кабелю на кручених парах *10BASE-T*) і *BNC* (для коаксіального кабелю *10BASE2*).

• *TP* - роз'єм *RJ-45 (10BASE-T)* і трансіверний роз'єм *AUI*.

• *Combo* - роз'єми *RJ-45 (10BASE-T), BNC (10BASE2), AUI*.

• *Coax* - роз'єми *BNC, AUI*.

• *FL* - роз'єм ST (для оптоволоконного кабелю *10BASE-FL*).

Функції мережевого адаптера діляться на *магістральні і мережеві*. До *магістральних* відносяться ті функції, які здійснюють взаємодію адаптера з магістраллю (системною шиною) комп'ютера (тобто впізнання своєї магістральної адреси, пересилання даних в комп'ютер і з комп'ютера, вироблення сигналу переривання процесора і т.д.). *Мережеві функції* забезпечують спілкування адаптера з мережею.

Пристрої підключення

- ***Ретранслятори (повторювачі) і концентратори*** працюють на першому рівні набору протоколів TCP/IP.
- ***Мости*** працюють на перших двох рівнях.
- ***Маршрутизатори*** працюють на перших трьох рівнях.
- Існують два типа комутаторів: перший тип — ускладнений міст та другий — ускладнений маршрутизатор
- ***Шлюзи*** працюють на усіх рівнях моделі ISO.

Трансівери або приймачі *(від англійського* ***TRANsmitter + reCEIVER)*** служать для передачі інформації між адаптером та кабелем мережі або між двома сегментами (частинами) мережі.

Трансівери підсилюють сигнали, перетворюють їх рівні або перетворять сигнали в іншу форму (наприклад, з електричної в світлову і назад). Трансіверами також часто називають вбудовані в адаптер приймачі.

Повторювач (Repeater) працює на фізичному рівні моделі ISO/OSI.

Повторювач виконує відновлення электричних сигналів для передачі їх в інші сегменти з збереженням побітового синхронізму в усіх об’єднаних мережах

За допомогою повторювача можливо з’єднувати тільки сегменти, в яких використовується однакова технологія передачі. Сегменти *Ethernet*, з’єднані повторювачами, створюють єдине розділене середовище передачі або домен колізій, тобто в усіх сегментах вести передачу може тільки один пристрій. Мета такої ретрансляції сигналів складається виключно в збільшенні довжини мережі.

Концентратори (хаби, hub), як випливає з їх назви, служать для об'єднання в мережу декількох сегментів.

Концентратори (або репітерні концентратори) представляють собою кілька зібраних в єдиному конструктиві репитерів, вони виконують ті ж функції, що і репітери.

Перевага подібних концентраторів в порівнянні з окремими репітерами в тому, що всі точки підключення зібрані в одному місці, це спрощує реконфігурацію мережі, контроль і пошук несправностей. До того ж все репітери в даному випадку живляться від єдиного якісного джерела живлення.

Концентратори іноді втручаються в обмін, допомагаючи усувати деякі явні помилки обміну. У будь-якому випадку вони працюють на першому рівні моделі OSI, так як мають справу тільки з фізичними сигналами, з бітами пакету і не аналізують вміст пакету, розглядаючи пакет як єдине ціле. На першому ж рівні працюють і трансівери, і репітери.

З'єднання вузлів між собою здійснюється через центральний пристрій – *концентратор*.

Концентратор - фактично багатовхідний ретранслятор. Він зазвичай використовується, щоб створити з'єднання між станціями в фізичній зоряній топології.

Концентратор **(*Hub*)** є пристроєм 1-го рівня та здійснює функції повторювача на всіх відрізках кручених пар між концентратором і вузлом, за винятком того порту, з якого надходить сигнал. Кожен порт має приймач (R) і передавач (T). Крім того, концентратор сам виявляє колізію і посилає jam-послідовність на всі свої виходи. Типова ємність концентратора - від 8 до 72 портів [3].

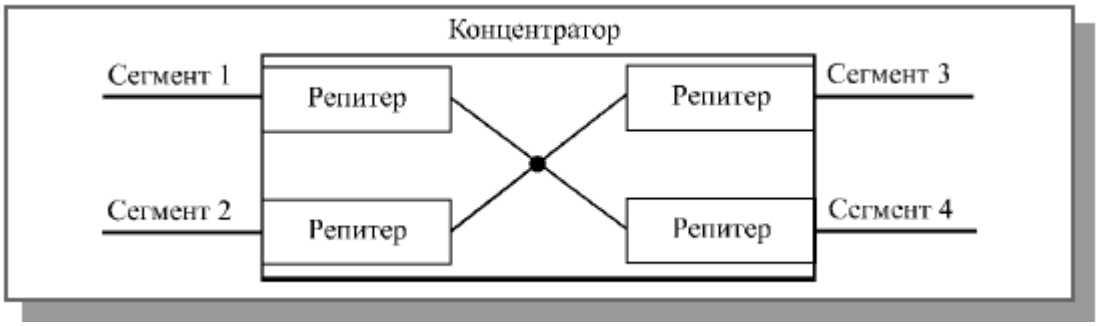


Рис. 4.7. Концентратор

Концентратори можна з'єднувати один з одним за допомогою тих же портів, які використовуються для підключення вузлів. Стандарт дозволяє з'єднувати концентратори тільки в деревоподібні структури, будь-які петлі між портами концентратора заборонені.

Для надійного розпізнавання колізії між двома будь-якими вузлами повинно бути не більше 4 концентраторів, при цьому максимальна довжина між концентраторами повинна бути не більше 100 метрів, а діаметр всієї мережі - не більше 500 метрів.

Рис. 4.8. Мережа на основі концентраторів

Мережа, побудована на основі концентраторів, розглядається як одна єдина локальна мережа. Ця мережа представляється логічною топологією типу "шина" (якщо станція передає пакет, він буде отриманий кожної іншою станцією без переадресації). Побудова локальних мереж великої ємності тільки за допомогою концентраторів призводить до зростання числа колізій і зниження пропускної здатності мережі. Тому концентратори використовуються для побудови невеликих фрагментів мереж, які потім об'єднуються за допомогою мостів і комутаторів.

Міст (Bridge) є пристроєм 2-го рівня, він також з'єднує два сегменти мережі, але, на відміну від повторювача, забезпечений певною логікою [4].

Порт моста записує всі кадри, що надходять від вузлів одного сегмента, в буферну пам'ять даних. Як пристрій фізичного рівня, він відновлює сигнал, який отримує. Як пристрій рівня ланки передачі даних, міст може перевірити фізичну адресу (джерело і пункт призначення), що містяться в пакеті.

Мости - найбільш прості пристрої, що служать для об'єднання мереж з різними стандартами обміну, наприклад, *Ethernet і Arcnet,* або декількох сегментів (частин) однієї і тієї ж мережі, наприклад, *Ethernet.*

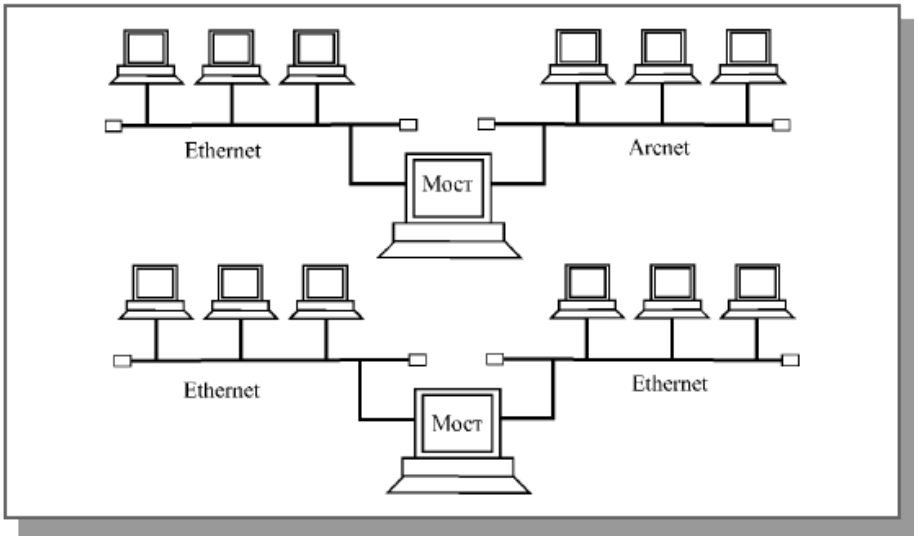


Рис. 4.9. Побудова мережі за допомогою мостів

Міст, подібно ретранслятору, не має ніякого фізичної адреси. Він діє тільки як фільтр, але не як вихідний передавач до кінцевого пункту призначення. У початковому стані, коли склад мережі невідомий, міст ретранслює буферізовані кадри, що надходять з одного порту, на інший порт за алгоритмом CSMA / CD.

Мости "прозорі" і розпізнавані; вони можуть бути легко встановлені між двома сегментами локальної мережі (принцип "*plug and play*" - "включай і працюй" 1).

Таблиця моста спочатку порожня, але як тільки міст отримує і передає вперед пакет, він створює в своїй таблиці вхід з вихідною адресою і інтерфейсом прибуття [5]. З тих пір міст знає, від кого надходить кожен пакет, до якого пункту призначення, від якого інтерфейсу.

Міст також робить запис інформації про пункт призначення, використовуючи інформацію, що міститься в пакеті.

Міст зберігає таблицю відповідності між MAC-адресами пристроїв і номерами своїх портів, к яким підключені сегменти з даними пристроями.

Таблиця оновлюється при надходженні кожного кадру у відповідності із значенням MAC-адреси джерела. Записи з таблиці удаляються по тайм-ауту.

При надходженні наступного кадру міст:

2. Перевіряє коректність кадру (деякі кадри відкидаються)
3. Аналізує адресу отримувача:

- Якщо MAC-адреса отримувача знаходиться в тому ж сегменті, із якого прийшов кадр, мост завершує обробку кадра;
- Якщо MAC-адреса отримувача знаходиться в іншому сегменті, мост передає кадр в сегмент, к якому підключений отримувач;
- Якщо міст не може визначити сегмент отримувача (або використан групова адреса), він передає кадр в усі сегменти, крім того, з якого він був отриманий.

Таким чином, міст ефективно ізолює локальні трафіки сегментів.

Комутуючі концентратори (*Switched Hubs*) або комутатори (*Switches*) в першому наближенні можуть розглядатися як багатопортові простіші та дуже швидкі мости.

Комутатор рівня два - міст з багатьма інтерфейсами, який дозволяє краще (швидше) розподіляти інформацію. Міст з декількома інтерфейсами може підключити кілька сегментів *LAN* разом. Міст з багатьма інтерфейсами може розподілити інформацію кожної станції до кожної станції на одному і тому ж сегменті. Використовуємо термін "**міст**" для комутатора рівня 2.

Комутатор рівня три - маршрутизатор. Комутатор рівня три може отримати, обробити і послати пакет набагато швидше, ніж традиційний маршрутизатор, навіть при тому, що функціональні можливості у них одні й ті ж. Використовуємо термін "**маршрутизатор**" для комутатора рівня три.

Комутатор (Switch) використовує топологію типу "зірка", є пристроєм 2-го рівня і функціонально являє собою багатопортовий міст, до кожного порту якого може бути підключений окремий хост, концентратор, сервер або маршрутизатор

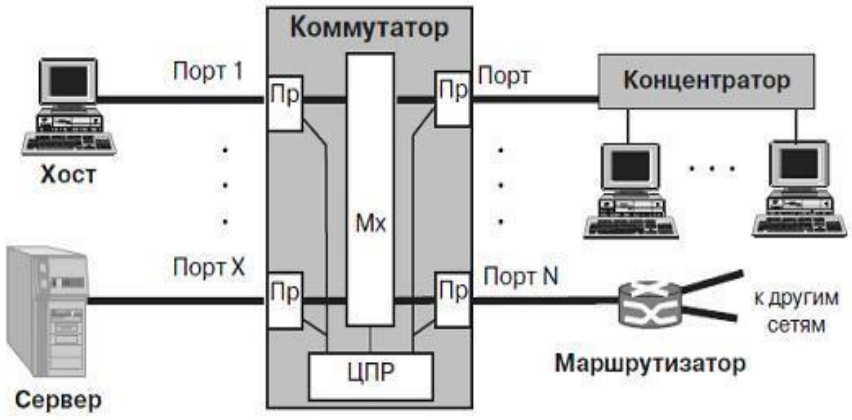


Рис. 4.10. Структура комутатора

Кожен порт комутатора оснащений процесором обробки пакетів (Пр.), який може працювати як в *напівдуплексному*, так і в *дуплексному режимі.*

При підключенні до порта комутатора окремого вузла (комп'ютера або маршрутизатора) порт комутатора встановлюється в двобічний режим, а в вузол ставиться мережева карта з придушенням колізій. За рахунок цього вузол і комутатор мають можливість одночасної передачі і прийому пакетів.

При підключенні до порта комутатора концентратора порт комутатора встановлюється в напівдуплексний режим.

Для комутації кадрів між портами використовується комутаційна матриця (МХ).

Аналогічно мосту кожен порт веде адресну таблицю MAC-адрес, підключених до нього пристроїв і повідомляє про неї центральний процесор (ЦПР).

Після прийому початкових біт кадру вхідний процесор аналізує адресу призначення і починає з'єднуватися через комутаційну матрицю, не чекаючи приходу біт кадру, що залишилися. Для цього він звертається до ЦПР з заявкою на встановлення шляху в комутаційної матриці

ЦПР має адресну таблицю і може здійснити запит з'єднання, якщо порт призначення вільний, тобто не поєднаний з іншим портом.

Якщо ж порт зайнятий, то ЦПР в з'єднанні відмовляє, і кадр продовжує буферізуватися процесором вхідного порту до звільнення вихідного порту

Після того як необхідний шлях в комутаційної матриці встановлено, по ньому направляються кадри в вихідний порт, де вони повторно буферизуються на випадок різній швидкості комутованих портів.

Процесор вихідного порту за значенням контрольної суми (FCS) опціонально може перевірити цілісність прийнятого кадру і починає передавати по сегменту прийнятий кадр.

Через наявність безлічі портів комутатор має істотно більш високою продуктивністю за рахунок паралельної обробки кадрів.

Маршрутизатор - пристрій з трьома рівнями, він працює на фізичному рівні, канальному рівні ланки (рівні ланки передачі даних) і мережевому рівні.

Як пристрій фізичного рівня, він відновлює сигнал, який він отримує.

Як пристрій рівня ланки передачі даних, маршрутизатор перевіряє фізичні адреси (джерело і пункт призначення), що містяться в пакеті.

Як пристрій мережевого рівня, маршрутизатор перевіряє адреси мережевого рівня (адреси в рівні IP).

Маршрутизатор може:

- *з'єднувати локальні мережі;*
- *з'єднувати разом мережі загального призначення;*
- *підключити локальні мережі до мереж загального призначення*

Маршрутизатор - пристрій мережевого обміну, він з'єднує разом незалежні мережі, щоб формувати мережу Internet.

Є три головні відмінності між маршрутизатором з ретранслятором або мостом:

1. Маршрутизатор має фізичний і логічний (IP) адреса для кожного з його інтерфейсів

2. Маршрутизатор діє тільки на тих пакетах, в яких адреса одержувача відповідає адресі інтерфейсу, куди пакет прибуває. Це вірно для односпрямованої, групової або широкомовної адреси

3. Маршрутизатор змінює фізичну адресу пакета (і джерело, і пункт призначення), коли він передає пакет вперед

Маршрутизатори діють на мережі подібно станціям. Але на відміну від більшості станцій, які включаються тільки в одну мережу, маршрутизатори адресуються і підключені до двох або більше мереж [6].

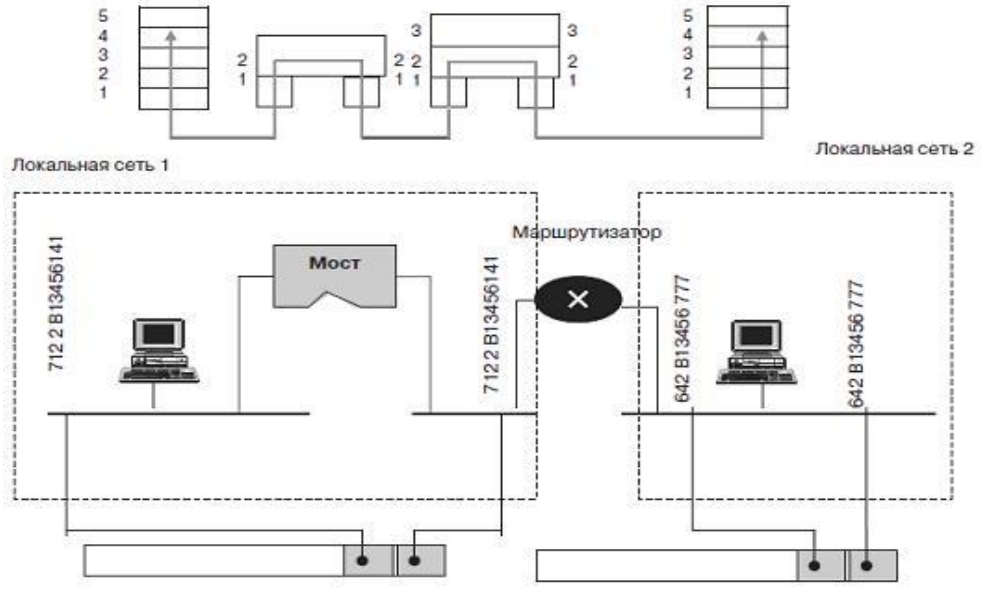


Рис. 4.11. Використання маршрутизатора при підключенні двох локальних мереж

Шлюз – пристрій для об’єднання мереж, які використовують різні стеки протоколів або окремі протоколи. Шлюз може працювати на всіх рівнях моделі ISO/OSI. Шлюзи використовуються для зв’язку систем, які використовують різні структури і формати даних, кодування, мають різну архітектуру.

Шлюз витягує дані пакетів, які надходять із мережі джерела, пропускаючи їх снизу на гору через повний стек протоколів вихідної мережі, заново упаковує данні, пропускаючи їх зверху до низу через стек протоколів мережі призначення.

В залежності від задачі шлюз може використовувати усі рівні моделі OSI, а може обмежитися декількома або одним (наприклад, прикладним).

4.4. Мережі загального та обмеженого користування

В умовах ринкової економіки суб'єктами підприємницької діяльності у

галузі телекомунікації виступають мережеві оператори та сервіс-провайдери (постачальники послуг). Вони забезпечують побудову ***мереж зв'язку загального користування,*** так званих ***публічних мереж (Public Network).*** Ці мережі призначені постачати послуги зв'язку широкому колу користувачів різних категорій [6].

Приватні мережі складають групу так званих ***мереж обмеженого користування.***

Мережі обмеженого користування, приватні мережі, PrivateNetworks *— це мережі, призначені для надання послуг обмеженому колу користувачів. Такі мережі можуть взаємодіяти між собою з використанням мереж загального користування.*

Всі ресурси мережі використовуються тільки співробітниками підприємства, яке володіє мережею. Це приватна, або ***закрита мережа,*** тобто призначена для конфіденційного (службового) зв'язку.

Мережі загального користування поділяються на:

- ***Мережі операторів***
- ***Мережі провайдерів***

Мережі операторів

Оператором мережі (Network Operator) називається компанія, яка є власником телекомунікаційної інфраструктури та бере на себе всі витрати щодо забезпечення її працездатності з заданим рівнем якості обслуговування. Її ще називають ***мережевим оператором,*** або просто ***оператором.***

Кінцевим продуктом діяльності мережевого оператора є надання послуг з транспортування інформації його мережею. Ці послуги називаються **телекомунікаційними послугами (Telecommunication Services)** та надаються як кінцевим користувачам мережі, так і іншим мережевим операторам, забезпечуючи їх транзитною можливістю з передачі трафіку через свої мережі.

У зв'язку з цим мережі операторів прийнято називати

телекомунікаційними мережами. Їх основним завданням є забезпечення можливості віддалено розташованих об'єктів обмінюватися інформаційними повідомленнями.

Створюючи мережу загального користування, оператор зобов'язаний забезпечити в будь-якому місці мережі, до якого під'єднано кінцеві пристрої, ***стандартний інтерфейс*** (точку з'єднання).

Розрізняють операторів фіксованого та мобільного (стільникового) зв'язку.

Оператори фіксованого зв'язку (Fixed Communication Operators) – організовують стаціонарні мережі, в яких комунікаційне обладнання та пристрої користувачів розміщуються в стаціонарних пунктах мережі.

Оператори мобільного зв'язку (Mobile Communication Operators) – створюють мережеве покриття території, розміщуючи свої базові станції за стільниковою схемою в стаціонарних або рухомих пунктах, забезпечуючи тим самим можливість вільного переміщення в зоні покриття.

Серед основних тенденцій розвитку ринку стільникового зв'язку найприкметнішою є поява так званих **віртуальних операторів (Virtual operators)**. Це компанії, які не мають власних мережевих ресурсів, займаються в основному маркетинговою діяльністю й у вигляді пакетів популярних послуг на основі гнучкої тарифної сітки реалізують їх клієнтам під своєю торговою маркою. Реалізацію ж послуг виконує мережевий оператор, з яким віртуальний оператор вступає у договірні відносини з частковою участю в прибутку від продажу послуг. Оператор, якому належить мережеве обладнання, при цьому повністю зосереджує свою діяльність на підтримці високого рівня його працездатності.

У період лібералізації ринків основні інтереси всіх операторів зосереджуються на пошуку нових ринкових форм комплексних рішень щодо розширення послуг, які надаються користувачам. Для операторів фіксованих мереж таким рішенням є надання мобільного доступу своїм абонентам. Операторові мобільного зв'язку фіксована мережа дозволяє стати

постачальником повного набору послуг. Доступність комбінації мобільного та фіксованого доступу, надання широкосмугового доступу, а також послуг передачі даних забезпечують ідеальні умови виживання операторів зв'язку в умовах високої конкуренції на ринку телекомунікацій.

Мережі провайдерів

Провайдер послуг – це суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мережі надання в користування каналів електрозв'язку. (Згідно *закону України «Про телекомунікації»)*

Провайдер послуг Інтернету (Internet Service Provider, ISP), Інтернет – провайдер — це суб'єкт господарювання, що надає послуги доступу до мережі Інтернет та інші пов'язані з Інтернетом послуги.

Мережі обмеженого користування, Private Networks, Приватні мережі – це телекомунікаційні мережі ресурси яких використовуються тільки співробітниками суб'єкту господарювання, який володіє мережею.

Під терміном «приватна мережа» розуміють також ***закриту мережу,*** призначену для конфіденційного (службового) зв'язку.

Приватна мережа – це комунікаційне середовище, у якому доступ контрольований через дозвіл сполучення між респондентами тільки в середині визначеної спільноти за інтересами і побудований на певних формах спільного використання основного комунікаційного середовища, де це основне комунікаційне середовище забезпечує послуги мережі на невиключній основі.

Мережі обмеженого користування поділяються на:

- Мере жі підприємств та установ
- Мережі спеціального призначення

Мережі підприємств та установ

Мережами підприємств (Enterprise Networks), або приватними

мережами (Private Networks), називають мережі, які належать установам і компаніям, інтереси бізнесу яких виходять за межі ринку телекомунікацій.

Відмінною особливістю приватних мереж є те, що всі ресурси мережі використовуються виключно співробітниками підприємства, яке є власником мережі. Крім того під терміном «приватна» мережа розуміють також ***закриту мережу,*** призначену для конфіденційного зв'язку. У цьому розумінні поняття «приватна мережа» частіше вживається відносно мереж великих корпорацій, що мають філії в різних містах, країнах і навіть континентах. Мережі підприємств меншого масштабу завжди сприймаються як приватні [6].

Поєднання комп'ютерів в мережу дозволяє підприємству оптимізувати його інформаційну інфраструктуру (роботу програм, баз даних, тощо), що в результат і підвищує ефективність бізнес-процесу в цілому.

Залежно від масштабу виробничого підрозділу, в межах якого діє мережа, розрізняють ***мережі робочих груп, мережі відділів, мережі кампусів (будівлі)*** і ***корпоративні мережі.***

Мережі робочих груп зазвичай характеризуються малою кількістю робочих місць (до10) та використовуються невеликими групами співробітників підприємства, які виконують спільне виробниче завдання. Метою створення мережі в даному випадку є поділ дорогого периферійного обладнання та даних, спільне використання застосувань, а також надання універсальних засобів комунікацій як для внутрішнього, так і зовнішнього зв'язку (рис.4.12).

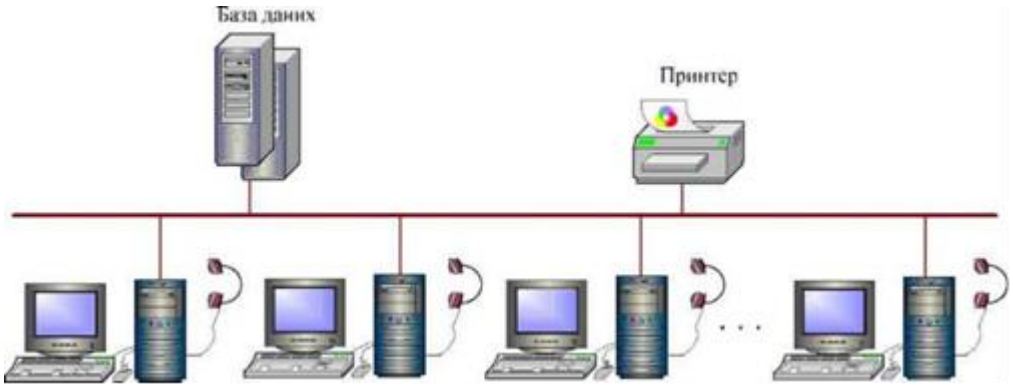


Рис.4.12 Мережа робочої групи

Мережі відділів можуть об'єднувати від 30 до 100 робочих місць і призначені для забезпечення спільної роботи співробітників одного відділу. Ці співробітники зазвичай вирішують ряд взаємопов'язаних завдань, наприклад, займаються планово-фінансовою діяльністю підприємства, ведуть облік матеріально-технічних цінностей та ін. Завдяки мережі забезпечується робота в режимі розподілу лазерних принтерів, модемів, інформаційних ресурсів відділу та мережевих застосувань.

Комп'ютерно-телефонна інтеграція зумовила появу нових ознак, властивих сучасним мережам відділів. Робочі місця співробітників поповнилися спеціалізованими телефонними апаратами, під'єднаними до послідовних портів персональних комп'ютерів (ПК). Крім того з'явилася можливість емуляції телефонного апарата за допомогою плат розширення в стандарті ***програмного інтерфейсу телефонного застосування*** (Telephony Application Programming Interface, **TAPI).**

Факс як необхідний елемент ділового життя будь-якого офісу або відділу завдяки новим стандартам також інтегрувався в телефонно-комп'ютерну систему.

У зв'язку з переходом на високошвидкісні технології стало можливим під'єднання до мережі широкосмугового мультимедійного обладнання, яке забезпечує організацію відеоконференцзв'язку (рис.4.13).

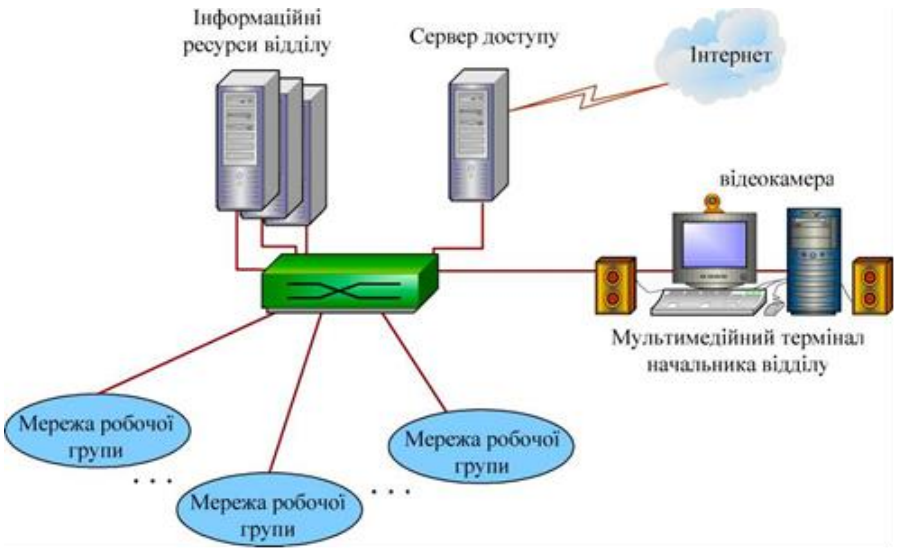


Рис. 4.13 Мережа відділу

Мережі нового типу засновують як на базі УАТС, так і на базі технологій IP-мереж, що забезпечує можливість створення гібридних застосувань, наприклад, таких, як уніфікований обмін повідомленнями [6].

Мережа будівлі або кампусу об'єднує мережі різних відділів великого підприємства. Мережі відділів можуть розташовуватися як у межах одного багатоповерхового будинку,так і в декількох будинках, розміщених неподалік один від одного, які утворюють кампус (невелике містечко) (рис.4.14).

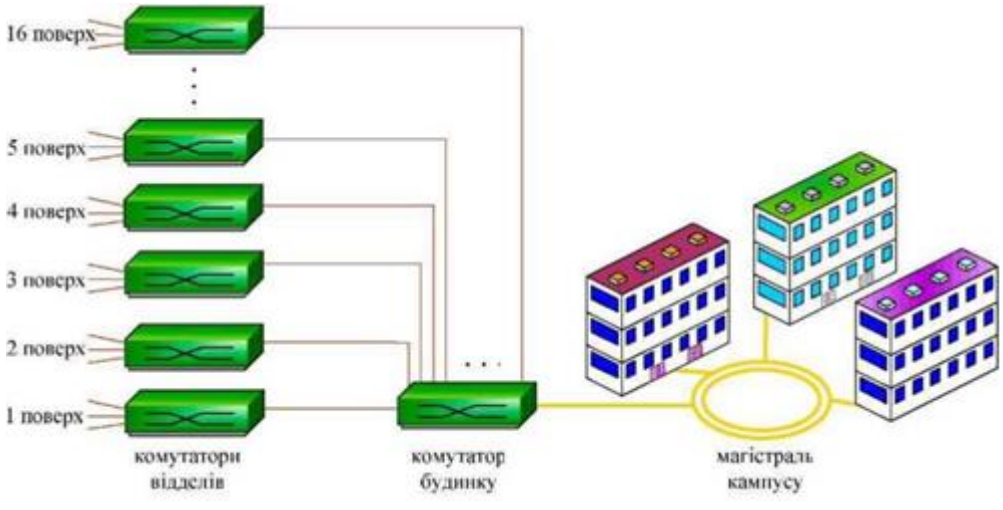


Рис. 4.14 Мережа кампусу

Мережі кампусів налічують близько декількох сотень комп'ютерів. Вони

використовують спеціальні служби мережевої взаємодії, що забезпечує доступ до загальних баз даних підприємства, факс-серверів, високошвидкісних модемів та ін. Завдяки цьому співробітники одних відділів отримують доступ до мереж та ресурсів інших відділів.

Кампусна мережа може складатися з різних типів комп'ютерів, неоднорідного апаратного й програмного забезпечення, різних мережевих технологій, що є прикладом ***гетерогенного*** мережевого середовища. Усе це створює проблему, пов'язану зі складністю керування кампусними мережами, а також вимагає високої кваліфікації мережевих адміністраторів.

Корпоративні мережі, як правило, належать великим компаніям, які складаються з головної штаб-квартири (центрального офісу), а також віддалених філій в інших містах, країнах і навіть на різних континентах. Кількість користувачів і комп'ютерів у такій мережі досягає декількох тисяч [2].

Підрозділи корпорації можуть мати різний масштаб: від малого з одним або кількома працівниками компанії до філії масштабу кампусу, а тому об'єднання мереж корпоративних підрозділів є можливим лише з використанням ***зовнішніх телекомунікацій*** які, не належать даному підприємству (рис. 4.15).

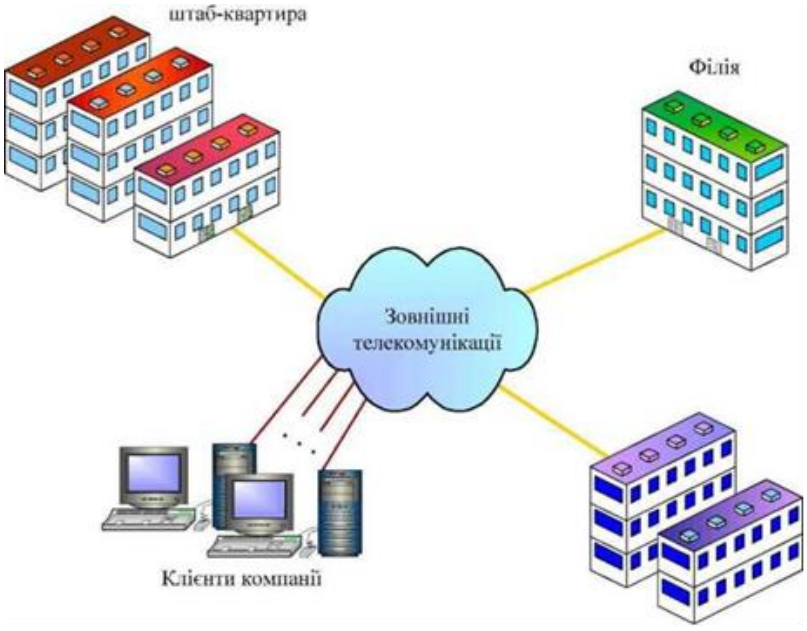


Рис. 4.15 Корпоративна мережа

Корпоративна мережа може обслуговувати не лише підрозділи однієї великої компанії, але й певну групу користувачів, до якої крім працівники в компанії входять бізнес-партнери та основні клієнти компанії. У будь-якому випадку санкціонований доступ до корпоративної мережі має лише ***обмежений контингент*** користувачів, група конкретних осіб.

Корпоративні мережі включають усю комунікаційну інфраструктуру, що забезпечує взаємодію між користувачами: різні типи термінальних пристроїв, кабельні системи в місцях розташування офісів, глобальні комунікації на базі ресурсів мережевих операторів і функціональні елементи керування мережею.

Оскільки об'єкти нерухомості, в яких інсталюються мережі, поділяються на виробничі будівлі та житловий сектор, розрізняють ***мережі офісного типу, не офісного типу,*** а також ***мережі малих офісів*** і ***домашні мережі*** (так званий сектор SOHO).

Мережі офісного типу монтують на об'єктах, споруджених з урахуванням специфічних виробничих умов (промислові підприємства, бізнес-центри, банки, органи державного управління). У переважній більшості такі підприємства мають у своєму розпорядженні розвинену комунікаційну інфраструктуру на основі спеціально виділених для цього кабелі в зв'язку та відповідного комунікаційного устаткування. Відмінною особливістю мереж офісного типу є те, що кабельна розводка для них будується практично завжди у формі структурованих кабельних систем (СКС). Різні аспекти реалізації таких систем, які є технічними об'єктами, добре опрацьовано та закріплено відомими національними й міжнародними стандартами.

Мережі не офісного типу характеризуються слабкострумовою кабельною розводкою, великою кількістю працюючих в системі застосовань (телефонії, охоронної сигналізації, відеоспостереження та ін.) у поєднанні з ефірним і кабельним телебаченням.

Типовими об'єктами не офісного призначення є житловий сектор (квартири, котеджі, мікрорайони в межах міста або сучасні селища в заміської зоні), а також лікарні та готелі в секторі громадських будівель.

Сектор малих офісів (Small Office/Home Office, **SOHO)** містить у собі категорію об'єктів не офісного типу, таких, як мережі малих фірм і домашні мережі. Прикметною особливістю цього сектору є мала кількість працівників або тих співробітників підприємства, які працюють вдома та взаємодіють з центральним офісом. Організація такої взаємодії є самостійним колом задач, об'єднаних загальним поняттям «віддалений доступ».

Мережі спеціального призначення

Мережі зв'язку спеціального призначення утворюють групу мереж обмеженого користування.

Мережі зв'язку спеціального призначення використовуються для забезпечення потреб державного управління, оборони, безпеки й охорони правопорядку в країні, для забезпечення виробничої діяльності організацій і управління технологічними процесами і т.д.

Основне призначення телекомунікаційної мережі, як вже зазначалося – це реалізація транспортної функції, тобто перенесення інформації, поданої у формі сигналу з кінця в кінець між інтерфейсами мережі.

Мережева активність при транспортуванні інформації різними ділянками телекомунікаційної мережі визначається інтенсивністю створеного в них мережевого трафику. Принцип розподілу інтенсивності трафику на різних ділянках телекомунікаційної мережі може бути основою декомпозиції транспортної функції. Така декомпозиція передбачає виділення трьох типів сегментів, які вирішують відносно самостійні функціональні підзавдання, а саме: ***транспортні мережі, мережі доступу і розподільчі мережі.***

Транспортна мережа (Transport Network, Transmission Media) – це сегмент з високим ступенем концентрації трафику, за допомогою якого здійснюється інформаційний обмін між сегментами з більш повільним трафиком і в якому транспортне середовище для передавання будь-якого типу інформації забезпечується використанням єдиних технологічних принципів і встановлених стандартів з надання ширини смуги пропускання [7].

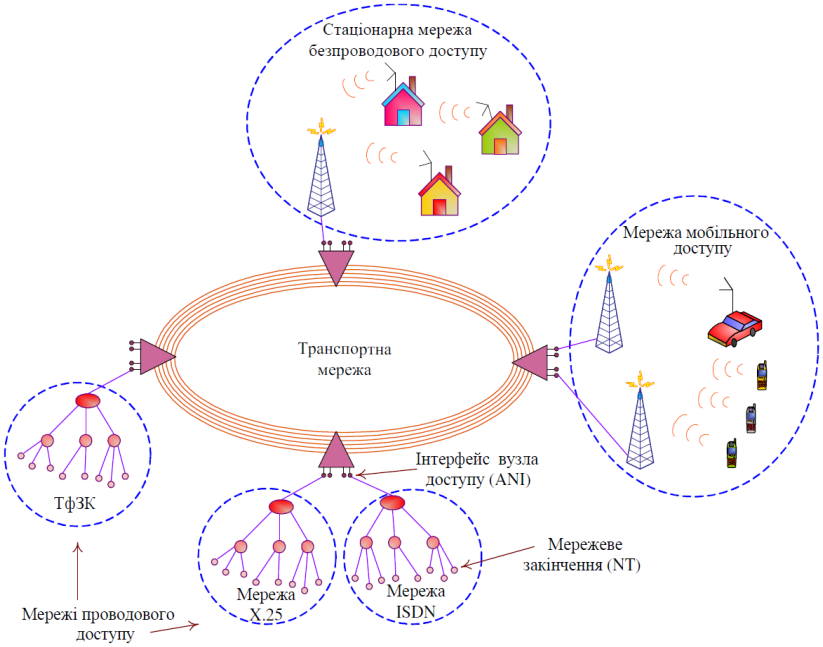


Рис.4.16 Транспортна мережа та мережа доступу

Мережею доступу (Access Network) називається сегмент телекомунікаційної мережі, в якому формуються інформаційні потоки, спрямовані в транспортну мережу.

Хоча мережі доступу та транспортна мережа спільно вирішують завдання реалізації транспортної функції з перенесення інформації з кінця в кінець, телекомунікаційні технології, які використовуються в них, істотно відрізняються [8].

З'єднання мереж доступу з транспортною мережею здійснюється у вузлах доступу до транспортної мережі.

Мережі доступу узагальнено поділяються на:

- Мережі проводового доступу;
- Стаціонарні мережі безпроводового доступу;
- Мережі мобільного доступу.

Мережа доступу з боку користувача має пристрій **мережевого закінчення** (Network Termination Unit, NTU), якій ще називається просто **мережевим закінченням** (Network Termination, **NT),** а на іншому кінці – **інтерфейс вузла доступу** (Access Node Interface, **ANI)** до транспортної мережі.

Ділянка мережі між мережевим закінченням NT, до якого під'єднано термінальний пристрій користувача, й **інтерфейсом сервісного вузла** (Service Node Interface, **SNI),** де абоненту надається необхідна послуга, визначається терміном **«мережа абонентського доступу»** [8]**.** Наприклад, ділянка між абонентською розеткою, куди підключається термінал користувача, і лінійним блоком місцевої телефонної станції.

Мережі доступу, у загальному випадку, мають багаторівневу архітектуру, що включає вузли рівнів доступу, розподілу і ядра.

Опорні вузли мереж абонентського доступу формують рівень доступу.

Вузли рівня розподілу забезпечують агрегацію інформаційних потоків, що надходять від опорних вузлів абонентського доступу, і магістралями направляють агреговані потоки у вузли доступу до транспортної мережі.

У вузлі доступу до транспортної мережі відбувається концентрація всіх інформаційних потоків від приєднаних вузлів рівня розподілу. Вузол доступу до транспортної мережі, таким чином, переміщується на рівень ядра в мережі доступу.

Якщо територіальна протяжність є значною, мережа доступу може розглядатися як самостійний сегмент MAN.

Розподільчою мережею (Distribution Network) називають сегмент телекомунікаційної мережі, за допомогою якого концентрований потік, який надходить з транспортної мережі, перерозподіляється та надходить до споживачів.

На практиці функції мережі доступу та розподільчої мережі часто поєднуються в одному сегменті.

Класичним прикладом власне розподільчої мережі є тільки мережа оператора кабельного телебачення [6]

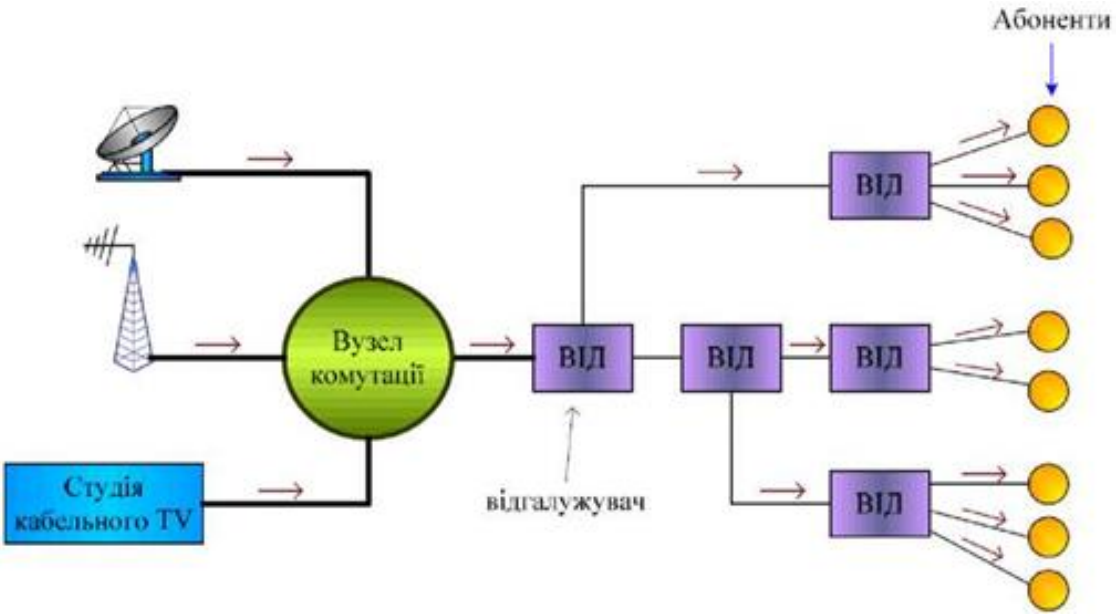


Рис. 4.17 Розподільча мережа

Контрольні питання до розділу

1. Скільки рівнів 7 – ми рівневої моделі реалізує транспортна станція:
   a. *2;*
   b. *3;*
   c. *4;*
   d. *6.*
2. Що представляє собою «*абонентська станція*».
3. Скільки рівнів 7 – ми рівневої моделі реалізує абонентська станція:
   a. *2;*
   b. *5;*
   c. *4;*
   d. *7.*
4. Який пристрій забезпечує взаємодію двох чи більше каналів передачі даних:
   a. *маршрутизатор;*
   b. *міст;*
   c. *концентратор;*
   d. *шлюз;*
   e. *комутатор.*
5. Комплекс базових профілів складається з:
   a. *моноканалу з випадковим доступом;*
   b. *моноканалу з невипадковим доступом;*
   c. *моноканалу без повноважень;*
   d. *моноканалу з повноваженнями;*

e. циклічного кільця; е). подвійної шини.

6. Скільки рівнів 7 – ми рівневої моделі реалізує канальна станція:

a. 2;b. 5;c. 4; d. 7.

7. Що собою представляє асоціативна система?

8. Які пристрої відносяться до асоціативних систем?

9. Скільки рівнів моделі ISO реалізує шлюз?

10. Скільки рівнів моделі ISO реалізує маршрутизатор?

11. Скільки рівнів моделі ISO реалізує міст?

12. Скільки рівнів моделі ISO реалізує комутатор?

13. На які підрівні поділяється канальний рівень в межах комплекса базових профілів.

14. Стандарт 8802/3 визначає:

a. моноканал з випадковим доступом;
b. моноканал з невипадковим доступом;
c. моноканал без повноважень;
d. моноканал з повноваженнями;
e. циклічне кільце;
f. подвійна шина.

15. Стандарт 8802/4 визначає:

a. моноканал з випадковим доступом;
b. моноканал з невипадковим доступом;
c. моноканал без повноважень;
d. моноканал з повноваженнями;
e. циклічне кільце;
f. подвійна шина.

16. Стандарт 8802/5 визначає:

a. моноканал з випадковим доступом;
b. моноканал з невипадковим доступом;
c. моноканал без повноважень;
d. моноканал з повноваженнями;
e. циклічне кільце;
f. *подвійна шина.*

17. Стандарт 8802/6 визначає:

a. моноканал з випадковим доступом;
b. моноканал з невипадковим доступом;
c. моноканал без повноважень;
d. моноканал з повноваженнями;
e. циклічне кільце;
f. подвійна шина.

18. Які пристрої відносяться до апаратурі локальних мереж?

19. Що собою представляють термінатори?

20. Що собою представляють мережеві адаптери?

21. Що собою представляють ретранслятори?

22. Що собою представляють концентратори?

23. Які пристрої працюють з MAC-адресами пристроїв?

24. Які функції виконує маршрутизатор?

25. Які існують відмінності між маршрутизатором з ретранслятором?
26. Що собою представляють мережі загального та обмеженого користування?
27. Чим відрізняються мережі операторів від мереж провайдерів?
28. В чому полягає відмінність операторів фіксованого та мобільного зв'язку?
29. Дайте визначення терміну «провайдер послуг» ?
30. Що собою представляють мережі обмеженого користування?
31. Що собою представляють мережі підприємств?
32. Чим відрізняються мережі робочих груп від мереж відділів?
33. Що собою представляє мережа будівлі або кампуса?
34. Що собою представляє корпоративна мережа?
35. Чим відрізняються мережі офісного типу та мережі сектору малих офісів?
36. Що собою представляє транспортна мережа?
37. Що собою представляє мережа доступу?
38. Що собою представляє розподільча мережа?
39. Який пристрій дозволяє відновити рівень сигналу і передати його з одного ін терфейсу в інший не змінюючи ні адреси, ні даних?
    a. *маршрутизатор;*
    b. *комутатор;*
    c. *повторювач;*
    d. *трансивер;*

Список рекомендованої літератури

1. *Якубайтис Э.А.* Открытые информационные сети. – М.: Радио и связь, 1991. – 208 с.
2. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
3. *Новиков Ю. В., Кондратенко С. В.* Основы локальных сетей. Курс лекций. [Електронний ресурс] – М.: Интернет-университет информационных технологий, 2005. – ISBN 5-9556-0032-9. Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/57/57/info.
4. *Шварц М.* Сети связи: протоколы, моделирование и анализ. Ч.1. – М.: Наука, 1992. – 336 с.
5. *Шварц М.* Сети связи: протоколы, моделирование и анализ. Ч. 2. –М.: Наука, 1992. – 272 с.
6. *Стрихалюк Б. М.* Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. – Львів: Львівська політехніка, 2017. – 121 с.
7. *Уэнделл Одом* Компьютерные сети. Первый шаг // Computer Networking First-step. – М.: «Вильямс», 2005. – 432 с.
8. *Жураковський Б.Ю., Срочинська Г.С., Довженко Н.М.* Кінцеві пристрої абонентського доступу. [Навчальний посібник]. – К.: ДУТ, 2015. – 65 с.

Розділ 5. КОДУВАННЯ І МОДУЛЯЦІЯ СИГНАЛІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

5.1. Види сигналів

Наше життя неможливо уявити без постійного обміну інформацією. Люди обмінюються інформацією в усній, писемній та інших формах. Засоби масової інформації щоденно доносять до нас потоки різноманітних відомостей. Протягом багатьох століть люди винаходили умовні знаки та способи для передачі інформації. У загальному розумінні та найширшому значенні слова *інформація* – це сукупність відомостей про навколишній світ. Інформація може зберігатися та передаватися від одного об'єкта до іншого.

Для того, щоб інформацію можна було зберігати, обробляти, передавати і використовувати, вона повинна бути представлена у вигляді повідомлення.

Повідомлення – це форма представлення (вираження) інформації, зручна для передавання на відстань. Повідомлення можуть мати найрізноманітнішу форму: *оптичну* (текст або послідовність числових символів на паперовому носії, фотографія, телевізійне зображення тощо), *звукову* (музика, мова) і т. д.

Для передавання різноманітних повідомлень на відстані використовують фізичні процеси, здатні долати з деякою швидкістю відстані між джерелом та одержувачем [1].

Такими процесами можуть бути звукові або електромагнітні хвилі, електричний струм.

Фізичний процес, що відображає повідомлення, називається ***сигналом.***

Відображення повідомлення забезпечується зміною якої-небудь фізичної величини, що характеризує процес. Ця величина є інформаційним параметром сигналу.

Розрізняють чотири види сигналів:

- *неперервний неперервного часу,*

- *неперервний дискретного часу,*
- *дискретний неперервного часу,*
- *дискретний дискретного часу.*

Неперервні сигнали неперервного часу називають скорочено *неперервними (аналоговими)* сигналами.

Вони можуть змінюватися в довільні моменти, приймаючи будь-які значення з неперервної множини можливих значень.

Рис. 5.1. Неперервні сигнали неперервного часу

Неперервні сигнали дискретного часу можуть приймати довільні значення, але змінюються тільки в певні, наперед задані (дискретні) моменти

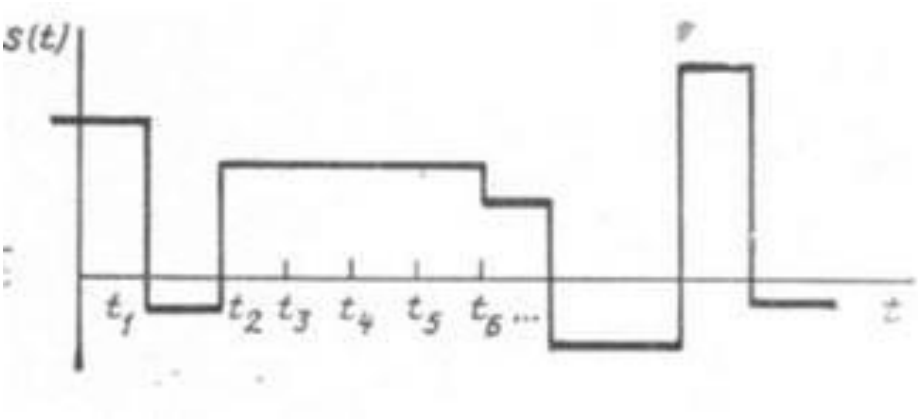


Рис. 5.2. Неперервні сигнали дискретного часу

Дискретні сигнали неперервного часу відрізняються від попередніх тим, що вони можуть змінюватися в довільні моменти, але їх величини приймають тільки конкретні дозволені (дискретні) значення (рівні).

Дискретні сигнали дискретного часу, скорочено *дискретні*, в дискретні моменти можуть приймати тільки конкретні дозволені (дискретні) значення (рівні).

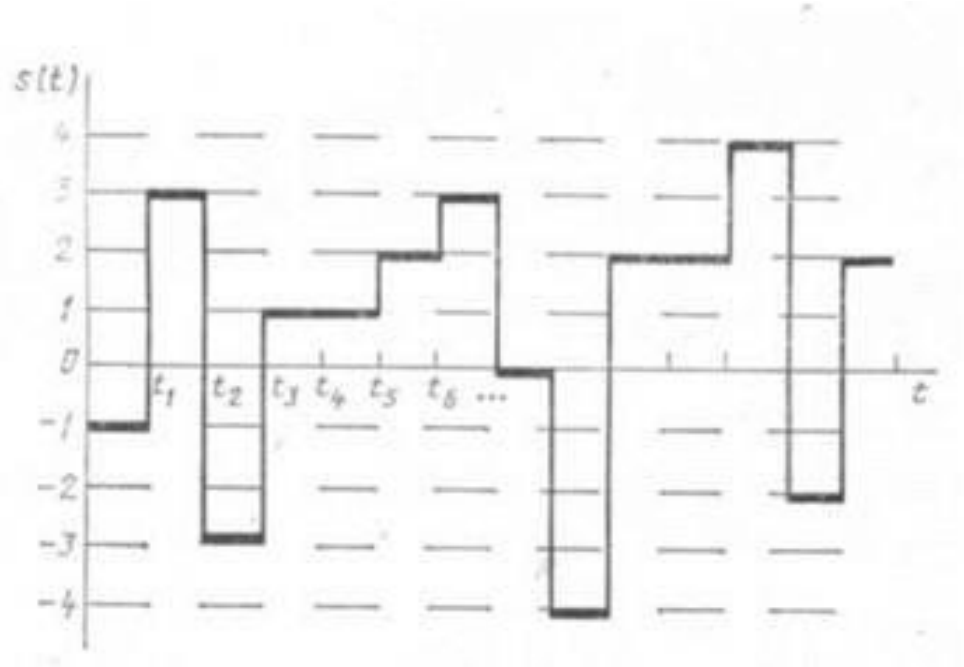


Рис. 5.3. Дискретні сигнали дискретного часу

Сигнали двох останніх видів називають ще *квантованими за рівнем*. Передавати за допомогою системи електрозв'язку дискретні сигнали, немає необхідності. Достатньо позначити цифрами всі дозволені рівні і передати дискретні сигнали, відповідні цим цифрам.

Сформовані таким чином дискретні сигнали називають *цифровими*, а операцію встановлення відповідності між цифрами і значеннями дискретних сигналів — *кодуванням*.

Іноді в окремий клас виділяють *імпульсні сигнали*, які відмінні від нуля лише протягом кінцевого (порівняльно невеликого) інтервалу часу. Імпульсні сигнали на інтервалі свого існування можуть бути неперервними (наприклад, імпульси дзвонової форми) або дискретними (прямокутні).

Приведемо ще одну класифікацію сигналів. Всі сигнали (як неперервні, так і дискретні) можуть бути підрозділені на періодичні і неперіодичні.

Періодичним називається сигнал, значення якого повторюються через певні рівні проміжки часу, що називаються періодом повторення сигналу, або просто *періодом*. Для неперіодичного сигналу ця умова не виконується.

Найпростішим періодичним неперервним сигналом є гармонічне коливання.

$$s(t) = S\cos(\omega + \varphi)$$

де S, ω, φ - амплітуда, кутова частота і початкова фаза коливання.

Однак іноді в мережах використовується і інший шлях - *модуляція інформаційними імпульсами* високочастотного аналогового сигналу (синусоїдального).

Таке аналогове кодування дозволяє при переході на широкосмугову передачу істотно збільшити пропускну здатність каналу зв'язку (в цьому випадку по мережі можна передавати кілька біт одночасно).

До того ж, при проходженні по каналу зв'язку аналогового сигналу (синусоїдального), не спотворюється форма сигналу, а тільки зменшується його амплітуда, а в разі цифрового сигналу форма сигналу спотворюється [2].

Амплітудна модуляція (АМ, AM - Amplitude Modulation), при якій логічній одиниці відповідає наявність сигналу (або сигнал більшої амплітуди), а логічному нулю - відсутність сигналу (або сигнал меншої амплітуди). Частота сигналу при цьому залишається незмінною.

Недолік амплітудної модуляції полягає в тому, що АМ-сигнал сильно схильний до дії перешкод і шумів, а також висуває підвищені вимоги до загасання сигналу в каналі зв'язку.

Переваги - простота апаратурної реалізації і вузький частотний спектр.

Частотна модуляція (ЧМ, FM - Frequency Modulation), при якій логічній одиниці відповідає сигнал більш високої частоти, а логічному нулю - сигнал більш низької частоти (або навпаки). Амплітуда сигналу при частотної модуляції залишається постійною, що є великою перевагою в порівнянні з амплітудною модуляцією.

Фазова модуляція (ФМ, PM - Phase Modulation), при якій зміні логічного нуля на логічну одиницю і навпаки відповідає різка зміна фази синусоїдального сигналу однієї частоти і амплітуди. Важливо, що амплітуда модульованого сигналу залишається постійною, як і в випадку частотної модуляції [2].

Найчастіше аналогова модуляція використовується при передачі інформації по каналу з вузькою смугою пропускання, наприклад, по телефонних лініях в

глобальних мережах. Крім того, аналогова модуляція застосовується в радіоканалах, що дозволяє забезпечувати зв'язок між багатьма користувачами одночасно. У локальних кабельних мережах аналогова модуляція практично не використовується через високої складності і вартості як кодуючого, так і декодуючого обладнання.

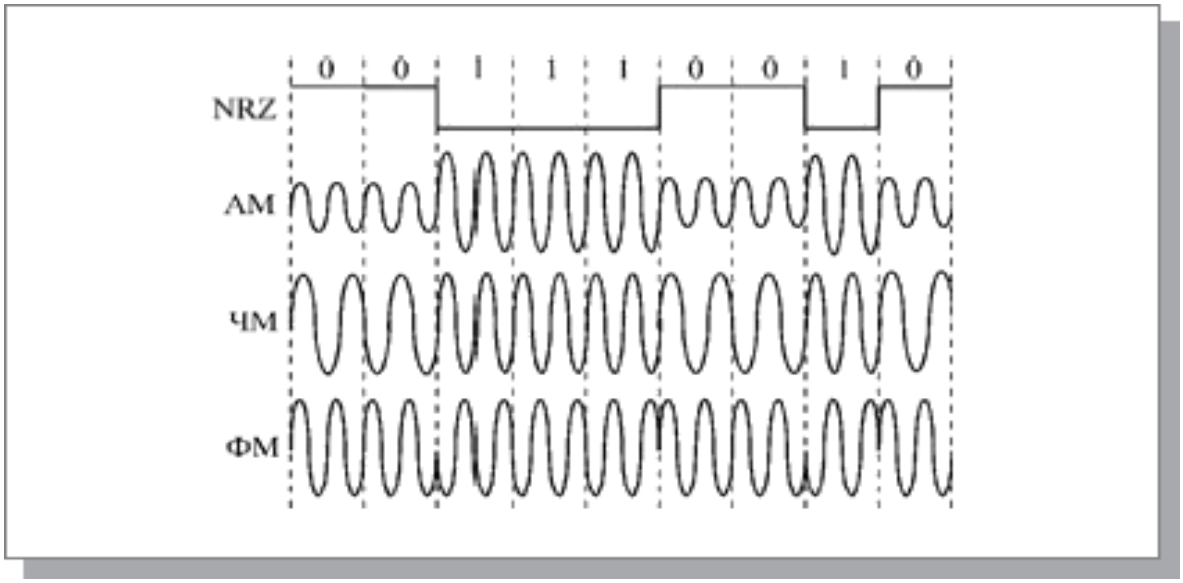


Рис. 5.4. Форми сигналів при двійковому коді для різних видів дискретної модуляції

5.2. Класифікація методів модуляції

Аналогова модуляція

- Амплітудна модуляція (*АМ*);
- Амплітудна модуляція з однією бічною смугою (*SSB – односмугова АМ);*
- Балансная амплітудна модуляція (*БАМ*) - *АМ* з придушенням несучої;
- Квадратурна модуляція *(QAM);*
- Кутова модуляція;
- Частотна модуляція *(ЧМ);*
- Лінійна частотна модуляція *(ЛЧМ);*
- Фазова модуляція *(ФМ);*
- Сигнально-кодова модуляція *(СКМ),* в англомовному варіанті *Signal* ;
- Code Modulation *(SCM).*

Цифрова модуляція (маніпуляція)

Імпульсна модуляція.

- Імпульсно-кодова модуляція (*ІКМ або PCM - Pulse Code Modulation);*
- Диференціальна імпульсно-кодова модуляція *(ДІКМ або DPCM - Differential PCM);*
- Адаптивна диференціальна імпульсно-кодова модуляція *(АДІКМ або ADPCM - Adaptive DPCM);*
- Широтно-імпульсна модуляція *(ШІМ);*
- Амплітудно-імпульсна модуляція *(АІМ);*
- Частотно-імпульсна модуляція *(ЧІМ);*
- Фазово-імпульсна модуляція *(ФІМ);*
- Дельта-модуляція (*ДМ або Δ модуляція*);
- Сігма-дельта модуляція (*Σ-Δ*).

Імпульсну модуляцію в залежності від вибору змінюваного параметра модулюємої імпульсної послідовності прийнято ділити на наступні види:

- ***амплітудно-імпульсну (АІМ),*** коли за законом переданого повідомлення змінюється амплітуда імпульсів вихідної послідовності (рис.в);
- ***широтно-імпульсну (ШІМ),*** при зміні згідно із законом переданого повідомлення тривалості (ширини) імпульсів вихідної послідовності (рис. г);
- ***фазоімпульсную (ФІМ),*** або часоімпульсную (ВІМ), якщо згідно із законом переданого повідомлення змінюється тимчасове положення імпульсів (рис. д);
- ***частотно-імпульсну модуляцію (ЧІМ)***, при зміні згідно із законом переданого повідомлення частоти проходження імпульсів піднесучих змінюються (рис. е);

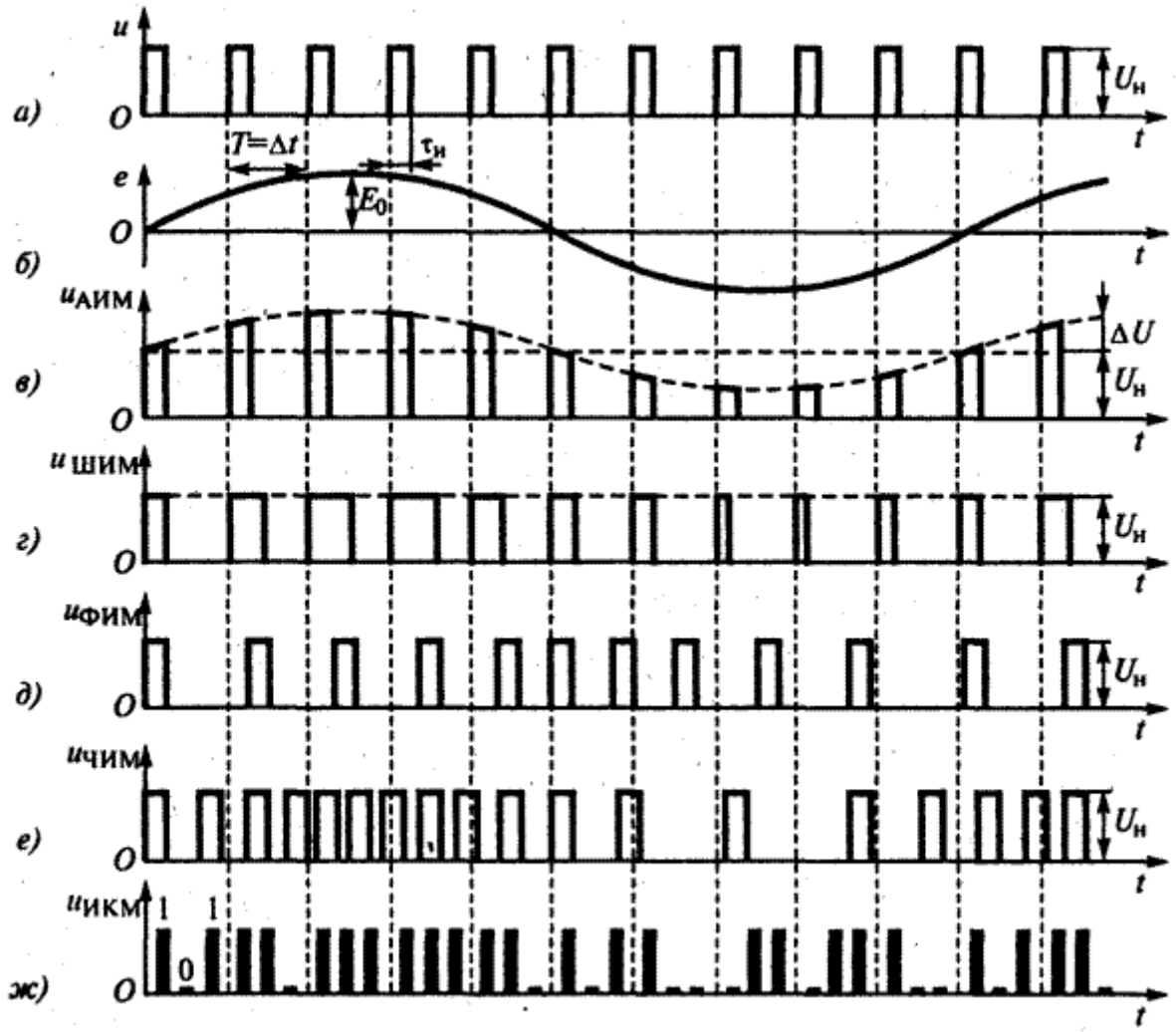


Рис. 5.5. Типи імпульсної модуляції

Імпульсно-кодова модуляція (ІКМ) - вид дискретної (цифрової) модуляції (цифровий маніпуляції), при якій передається аналоговий первинний сигнал перетворюється в цифровий код - послідовність імпульсів (1 «одиниць») і пауз (0- «нулів»), мають однакову тривалість, застосовується найбільш широко в сучасній радіоелектроніці і системах зв'язку. Цей вид імпульсної модуляції представлений на рис. ж.

Широтно-імпульсна модуляція (ШІМ — *pulse-width modulation, PWM*), або модуляція за тривалістю імпульсів (*pulse-duration modulation, PDM*) — процес керування шириною (тривалістю) високочастотних *імпульсів* за законом, який задає низькочастотний сигнал. В електроніці це може бути керування середнім значенням вихідної напруги шляхом зміни тривалості замкнутого стану

електронного (електромеханічного) ключа, наприклад, у схемі ключового стабілізатора напруги [4].

Адаптивна диференціальна імпульсно-кодова модуляція (АДІКМ) (*Adaptive differential pulse-code modulation, ADPCM)* - різновид диференціальної імпульсно-кодової модуляції, алгоритм якої має на увазі зміна кроку квантування, що дозволяє знизити необхідну смугу пропускання для заданого відношення сигнал/шум. Зазвичай адаптація ґрунтується на адаптивному коефіцієнті масштабування.

Сігма-де́льта модуля́ція — спосіб модуляції, що забезпечує оцифровку сигналу з заданими характеристиками в робочій смузі частот.

Сигма-дельта модуляція призначена для аналого-цифрового і цифро-аналогового перетворень звукових сигналів (ЗС). На відміну від імпульсно-кодової модуляції (ІКМ) вона дозволяє використовувати при цих операціях досить грубі перетворювачі з числом розрядів аж до одного, забезпечуючи при цьому відношення сигнал шум (SNR) до 120 … 140 дБ, що необхідно для професійного запису звуку. Технологія виробництва АЦП і ЦАП на основі сигма-дельта модуляції значно простіша і дешевша, тому такі перетворювачі широко використовуються в сучасних звукових картах, оптичному звукозапису, цифрових магнітофонах, в вимірювальній та іншій техніці.

На відміну від ІКМ АЦП і ЦАП на основі сигма-дельта модуляції працюють на частоті дискретизації в 4 і більше разів вище стандартного значення, відповідного вимогам теореми В. П. Котельникова. У них використовуються грубі квантувачі з числом розрядів q від 1 до 6 з частотно-залежним негативним зворотним зв'язком. В останні роки ця модуляція повністю «витіснила» з побутової і навіть професійної аудіотехніки імпульсно-кодову модуляцію.

Дельта модуляція

Фактично, дельта-модуляція є різновидом імпульсно-кодової модуляції (ІКМ), в якій число рівнів квантування дорівнює двом. При ДМ по каналу зв'язку передається не абсолютне значення сигналу, а різниця між вихідним аналоговим сигналом і апроксимується напругою (сигнал помилки). У порівнянні з конкуруючими методами, ІКМ і АДІКМ, дельта-модуляція характеризується

меншою складністю технічної реалізації, більш високими показниками перешкодозахищеності і гнучкістю зміни швидкості передачі.

Перевага дельта-модуляції в порівнянні, наприклад, з ІКМ, яка також генерує бінарний сигнал, полягає не стільки в реалізованої точності при заданій частоті дискретизації, скільки в простоті реалізації.

Основний недолік ДМ полягає в тому, що при швидких змінах сигналу дельта-кодер не встигає відстежувати зміни його рівня, внаслідок чого виникає так звана "перевантаження по крутизні". Існує велика кількість різновидів ДМ, в яких використовуються різні способи усунення цього виду спотворень. Більшість з них засновані на використанні миттєвого або інерційного компандування аналогового сигналу, або адаптивної зміни сходинки аппроксимуючої напруги відповідно до крутизни вхідного сигналу.

Основні характеристики:

- ***Енергетична ефективність.***
- ***Спектральна ефективність.***
- ***Стійкість до впливів каналу передачі.***
- ***Лінійність підсилювачів.***
- ***Складність реалізації.***

Енергетична ефективність *(потенційна завадостійкість)* характеризує достовірність переданих даних при впливі на сигнал адитивного білого гауссовского шуму, за умови, що послідовність символів відновлена ідеальним демодулятором.

Визначається мінімальним співвідношенням сигнал / шум (*Eb/N0*), який необхідний для передачі даних через канал з ймовірністю помилки, що не перевищує задану.

Енергетична ефективність визначає мінімальну потужність передавача, необхідну для достовірної роботи.

Характеристикою методу модуляції є крива енергетичної ефективності - залежність ймовірності помилки ідеального демодулятора від співвідношення сигнал / шум (*Eb/N0*).

Спектральна ефективність - співвідношення швидкості передачі даних до використаної смуги частот пропускання радіоканалу.

Приклади:

- AMPS: 0,83
- NMT: 0,46
- GSM: 1,35

Стійкість до впливів каналу передачі характеризує достовірність переданих даних при впливі на сигнал специфічних викривлень: завмирання внаслідок багатопроменевого поширення, обмеження смуги, зосереджені по частоті або часу завади, ефект Доплера та ін.

Лінійність підсилювачів. Для посилення сигналів з деякими видами модуляції можуть бути використані нелінійні підсилювачі, що дозволяє істотно знизити енергоспоживання передавача, при цьому рівень позасмугового випромінювання не перевищує допустимих меж. Даний фактор важливий для систем рухомого зв'язку.

Складність реалізації - визначається обчислювальним ресурсом, необхідним для реалізації алгоритму демодуляції, і вимогами до характеристик аналогової частини.

5.3. Модуляція при передачі даних

Використання цифрових методів пересилання інформації збільшує *імовірність* коректної доставки. Якщо для аналогової передачі потребується *відношення* сигнал/шум" на рівні 40-60 дБ, то при цифровій передачі достатньо 10-12 дБ.

Вибір типу модуляції залежить від задачі, яка ставиться і від характеристик каналу (смуги пропускання, загасання сигналу і т.д.).

Частотна модуляція менш чутлива до амплітудних флуктуацій сигналу. Загасання сигналу може варіюватися в часі із-за зміни в транспортному середовищі, що доволі типово для комутуємих телефонних мереж. В будь-якому випадку на передаючій стороні необхідний модулятор, а на приймальній -

демодулятор. Так як обмін зазвичай двонаправлений, ці пристрої об'єднуються в одному приборі, який називається **модемом** [5].

Таблиця 5.1. *Види модуляції в модемах*

FSK (Frequency Shift Keying)	ступеневе перемикання частоти синусоїдального сигналу від *f1* до *f2* при незмінній амплітуді; частоті *f1* ставиться у відповідність логічний нуль, а *f2* - логічна одиниця
BPSK(Binary Phase-Shift Keying)	стрибкоподібне перемикання фази синусоїдального сигналу на π при незмінній амплітуді; при цьому фазі 0 ставиться у відповідність логічний нуль, а π - логічна одиниця
DPSK (Differential Phase Shift Keying)	метод, при якому змінюється фаза несучої частоти при постійній амплітуді і частот. Різновид *PSK*, при якій кодується лише зміна сигналу
QAM (Quadrature Amplitude Modulation)	комбінація амплітудної і фазової модуляції, дозволяє зробити кодування 8 біт на бод
QPSK (Quadrature Phase-Shift Keying)	квадратурна фазова модуляція. Використовує 4 фіксованих значення фази 0, π/2, π і 3π/2, потребує в два рази більш вузьку смугу, чим *PSK*, і по цій причині дуже популярна
TCM (Trellis mathd Modulation)	метод передбачає використання надлишковості, кожний бод несе додатковий біт, який дозволяє більш точно відновити інформаційну бітову послідовність. При кодуванні сигналу використовується метод *QAM*. Метод реалізований в сучасних високошвидкісних модемах і дозволяє знизити вимоги до відношення "*сигнал*/*шум*" на 4-5 дБ

Квадратурно-амплітуднаі модуляція - КАМ (QAM – Quadrature Amplitude Modulation) може розглядатися як розширена багаторівнева *ФМ*, в якій два вихідних сигнала генеруються незалежно. Таким чином, тут має *місце* два повністю незалежних квадратурних канала, які включають процеси кодування і детектування в основній смузі.

Сигнально – точковий *простір* для системи з *16-КАМ* і чотирма рівнями в кожному квадратурному каналі. Точки представляють складений сигнал, а штрихи на вісях відмічають рівні амплітуди в кожному квадратурному каналі [6].

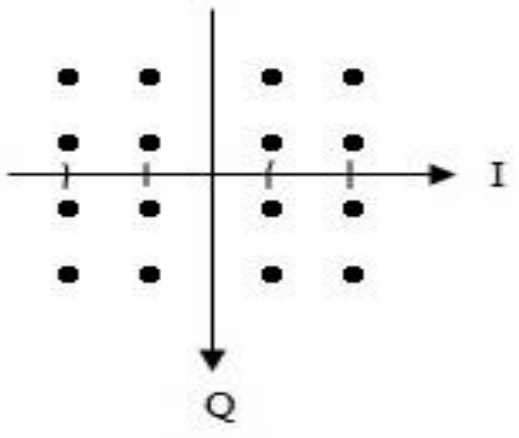


Рис. 5.6. Квадратурно–амплітудна модуляція

На відміну від *ФМ* сигналів сигнали *КАМ*, не вміщують постійної огинаючої. Наявність постійної огинаючої в *ФМ* пояснюється підтриманням відношення рівнів в квадратурних каналах. В *КАМ* такі обмеження не вводяться тому, що в кожному каналі рівні незалежні. Звідти витікає, що *КАМ* не може використовувати підсилювачі, які можуть мати насищення в межах можливих потужностей.

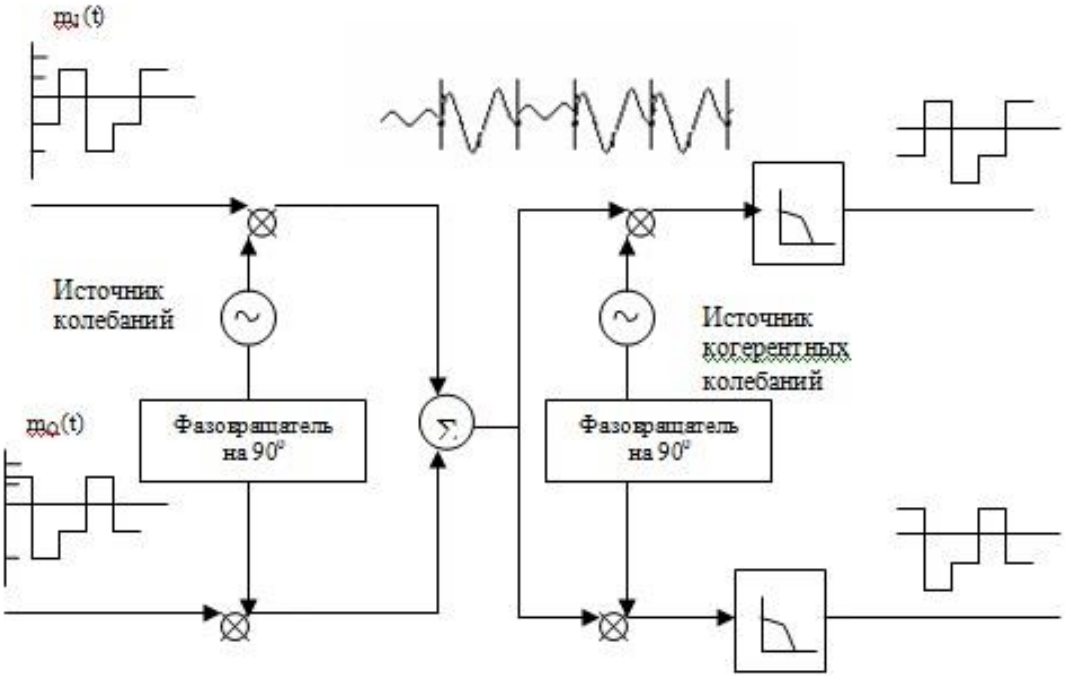


Рис. 5.7. Основна схема модулятор – демодулятора 16-КАМ

Спектр системи з *КАМ* визначається спектром вихідних сигналів, які надходять в квадратурні канали. Оскільки ці сигналі в своїй основі має ту ж структуру, що й вихідні ФМ сигнали, спектр *16-КАМ і 64-ФМ* співпадають при равному числі сигнальних точок на фазовій діаграмі.

Хоча спектри *ФМ і КАМ* співпадають, характеристики помилок цих систем сильно відрізняються. При достатньо великій кількості сигнальних точок системи *КАМ* мають, як правило, кращі характеристики, чим системи з ФМ. Основна причина полягає в тому, що відстань між сигнальними точками на діаграмі для системи з *КАМ* більше, ніж для відповідної системи з *ФМ*. На рис. приведено порівняння систем *16-ФМ і 16-КАМ*, що працюють на однаковій пікової потужності, по відстані між точками [7].

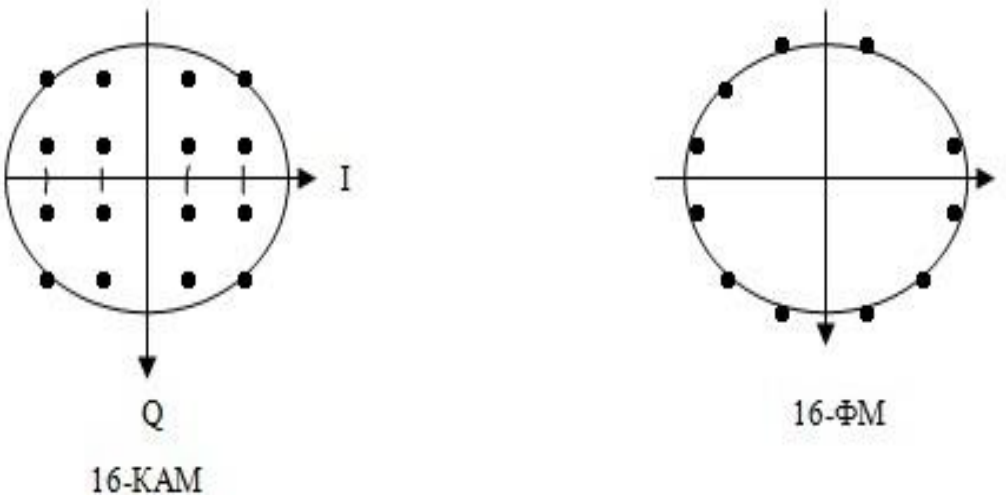


Рис. 5.8. Сигнально-точковий простір модуляції для 16-КАМ

В даний час для передачі користуються системами *256- КАМ*.

Надійне функціонування високоплотних форматів модуляції, таких як *256-КАМ* вимагає суворої лінійності підсилювачів, для можливості обробки широкого діапазону амплітуд сигналів.

Амплітудно фазову модуляція з придушенням несучої (Carrierless Amplitude and Phase Modulation - CAP) являє собою форму *КАМ* (іноді її називають амплітудно-фазова модуляція без несучої).

При цьому виді модуляції встановлюються фільтри на *синфазний канал (канал I)* і *квадратурний канал (канал Q)* для придушення несучої частоти.

Рис. 5.9. Амплітудно фазова модуляція з придушенням несучої

Фільтри створюються на базі цифрових сигнальних процесорів *(DSP).*

Фільтр синфазного каналу перетворює дані каналу *I* в косінусоїдального коливання, тоді як фільтр квадратурного каналу перетворює дані каналу *Q* в синусоїдальні коливання. Перетворення фільтрів такого типу зазвичай прив'язана до частоті несучої, так що на приймальному кінці можна відновити несучу.

Після складання синфазного і квадратурного сигналу *ХЕ* "синфазного і квадратурного сигналу", результуючий сигнал перетвориться в аналоговий за допомогою цифро-аналогового перетворювача ХЕ "цифро-аналогового перетворювача" *(ЦАП).*

5.4. Кодування інформації в локальних мережах

Інформація в кабельних локальних мережах передається в закодованому вигляді, тобто кожному біту інформації, що передається відповідає свій набір рівнів електричних сигналів в мережному кабелі.

Правильний вибір коду дозволяє підвищити *достовірність* передачі інформації, збільшити *швидкість передачі* або знизити вимоги до вибору кабелю.

Наприклад, при різних кодах максимальна швидкість передачі по одному і тому ж кабелю може відрізнятися в два рази. Від обраного коду напряму залежить також складність мережної апаратури (вузли кодування і декодування коду). Код

повинен в ідеалі забезпечити добру синхронізацію прийому, низький рівень помилок, роботу з будь-якою довжиною передаваємих інформаційних послідовностей [7].

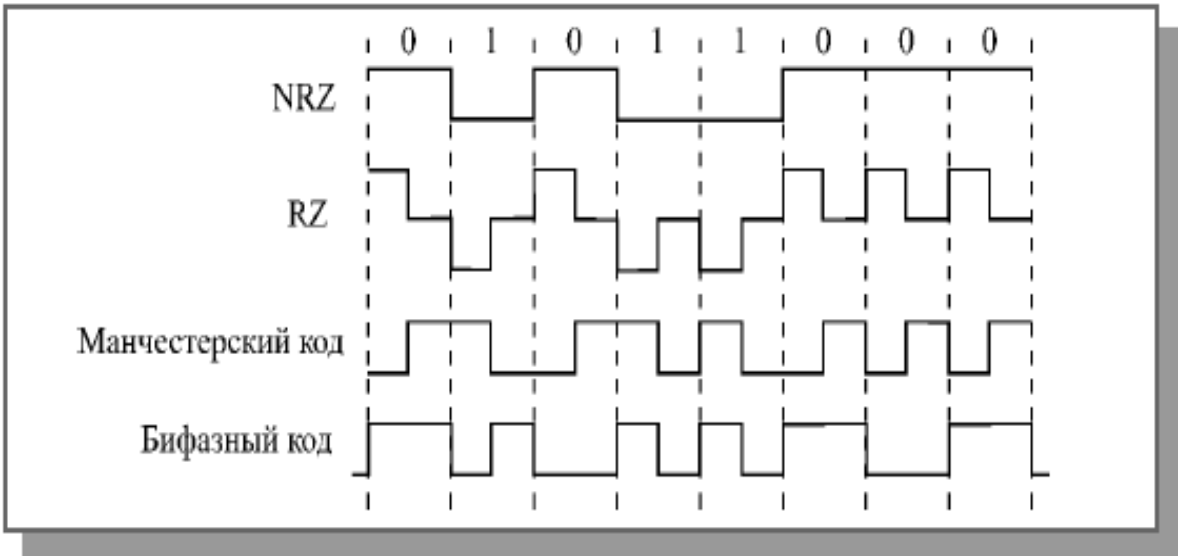


Рис. 5.10. Найбільш розповсюджені коди передачі інформації

Код *NRZ* (*Non Return to Zero – без повернення до нуля*) – це простійший код, представляє собою звичайний *цифровий сигнал*. Логічному нулю відповідає високий рівень напруги в кабелі, логичній одиниці – низький рівень напруги (або навпаки, що не принципово). Рівні можуть бути різної полярності або ж однієї полярності. На протязі бітового інтервалу (*bit time*, *BT*), тобто часу передачі одного біту ніяких змін рівня сигналу в кабелі не відбувається.

До переваг коду *NRZ* відноситься його доволі проста реалізація (вихідний сигнал не потрібно ні спеціально кодувати на передаючому кінці, ні декодувати на приймальному кінці), а також мінімальна серед інших кодів пропускна спроможність лінії зв’язку, необхідна при даній швидкості передачі.

Найбільш часта зміна сигналу в мережі буде при неперервному чередуванні одиниць і нулів, тобто при послідовності 1010101010..., тому при швидкості передачі, що дорівнює 10 Мбіт/с (протяжність одного біту дорівнює 100 нс) частота зміни сигналу і відповідно вимагаєма пропускна спроможність лінії складає 1 / 200нс = 5 МГц

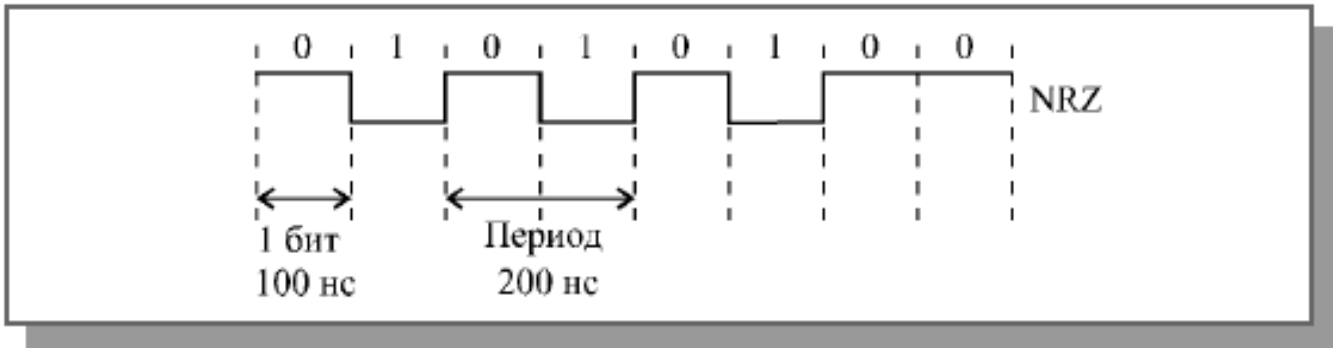


Рис. 5.11. Швидкість передачі і необхідна пропускна спроможність при коді NRZ

Самий великий недолік коду *NRZ* – це можливість втрати синхронізації приймачем під час прийому надто *довгих блоків*(пакетів) інформації. Приймач може прив'язувати момент початку тільки до першого (стартового) біту пакета, а на протязі прийому пакета він повинен користуватися тільки внутрішнім тактовим генератором (внутрішніми годинниками). Наприклад, якщо передається послідовність нулів або послідовність одиниць, то приймач може визначити, де проходять кордони бітових інтервалів, тільки по внутрішнім годинникам. І якщо годинники приймача розходяться з годинниками передавача, то часовий здвиг до кінця прийму пакета може перевищувати протяжність одного або навіть декількох біт. В результаті відбудеться втрата переданих даних.

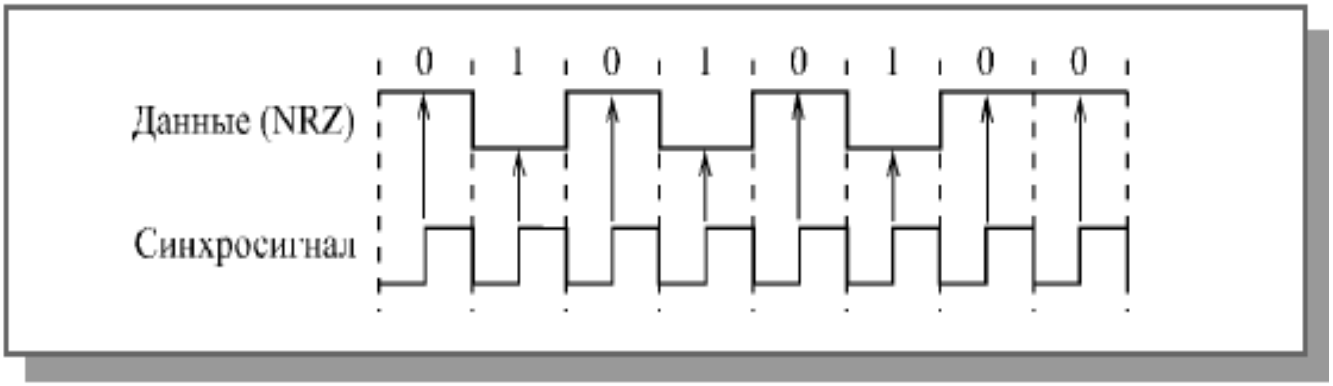


Рис. 5.12. Передача в коді NRZ с синхросигналом

Для того, щоб не було втрати синхронізації, можливо було б ввести іншу лінію зв'язку для сінхросигналу. Але при цьому необхідна кількість кабелю, число

приймачів та передавачів збільшується в два рази. При великій довжині мережі і значна кількість абонентів це невигідно [3].

В зв’язку з цим код *NRZ* використовується тільки для передачі короткими пакетами (звичайно до 1 Кбіта).

Ще одним недоліком коду *NRZ* є те, що він може забезпечити обмін повідомлень тільки фіксованої, заздалегідь обговореної довжини. Приймач, по тій інформації, що приймається не може визначити, чи йде ще передача чи вже закінчилася. Для синхронізації початку прийому пакету використовується стартовий службовий біт, чий рівень відрізняється від пасивного стану лінії зв’яку. Закінчується прийом після відліку приймача задано кількості біт послідовності.

Рис. 5.13. Визначення закінчення послідовності при коді NRZ

Найбільш відоме застосування коду *NRZ* – це стандарт RS232-C, послідовний порт персонального комп’ютера. Передача інформації в ньому ведеться байтами (8 біт), супроводжується стартовим і стоповим бітами.

Три інших коду (RZ, *манчестерський код*, біфазний код) принципово відрізняється від *NRZ* тим, що приймач може надійно приймати послідовності будь-якої довжини. Такі коди називаються *самосинхронізуючими*. Можливо вважати, що *самосинхронізуючі коди* несуть в собі *синхросигнал*.

Код RZ (*Return to Zero – з поверненням до нуля*) – цей трьохрівневий код отримав таку назву тому, що після значащого рівня сигналу в першій половині

бітового інтервалу відбувається повернення до "нульового", середнього рівня (наприклад, до нульового потенціалу). Перехід до нього відбувається в середині кожного бітового інтервалу. Логічному нулю, таким чином, відповідає позитивний імпульс, логічній одиниці – негативний (або навпаки) в першій половині бітового інтервалу.

В центрі бітового інтервалу завжди є перехід сигналу, відповідно, з цього коду приймач легко може виділити сінхроімпульс (строб). Можлива часова прив'язка не тільки до початку пакета, як у випадку коду *NRZ*, але й до кожного окремого біту, тому втрати синхронізації не відбудеться при будь-якій довжині пакету [4].

Манчестерський код (*або код Манчестер-II*) отримав найбільше розповсюдження в локальних мережах. Він також відноситься до *самосинхронізуючих кодів*, але на відміну від RZ має не три, а всього два рівня, що сприяє його кращій завадозахищеності та спрощенню приймаючих і передаючих вузлів.

Логічному нулю відповідає позитивний перехід в центрі бітового інтервалу (тобто є перша половина бітового інтервалу – низький рівень, інша половина – високий), а логічній одиниці відповідає негативний перехід в центрі бітового інтервалу (або навпаки).

Як і в RZ, обов'язкова наявність переходу в центрі біта дозволяє приймачу *манчестерського коду* легко виділити з сигналу, що надходить, синхросигнал і передавати інформацію великими послідовностями без втрат через розсинхронізацію.

Допустиме розходження годинників приймача і передавача може досягати 25%.

Подібно коду RZ, при використанні *манчестерського коду* потребується пропускна спроможність лінії в два рази вище, чим при застосуванні коду *NRZ*. Наприклад, для швидкості передачі 10 Мбіт/с необхідна смуга пропускання 10 МГц [7].

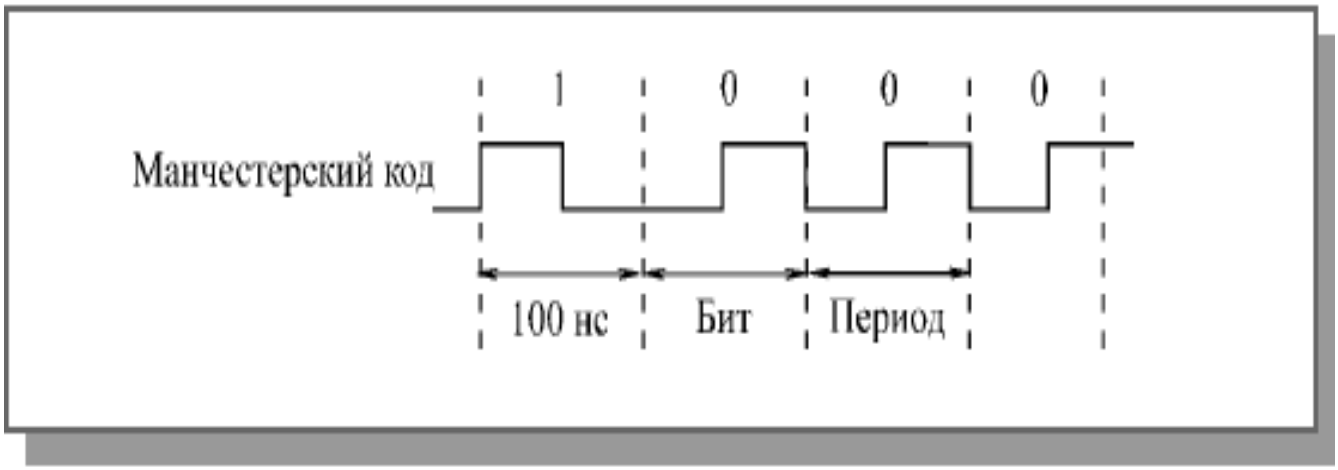


Рис. 5.14. Швидкість передачі і пропускна спроможність при манчестерському коді

Як і при коді RZ, в даному випадку приймач легко може визначити не тільки початок послідовності біт, що передається, але і її кінець.

Якщо на протязі бітового інтервалу немає переходу сигналу, то прийом закінчується.

В манчестерському коді можливо передавати послідовності біт змінної довжини.

Процес визначення часу передачі називають *контролем несучої*, хоча в явному вигляді несуча частоти в даному випадку не присутня.

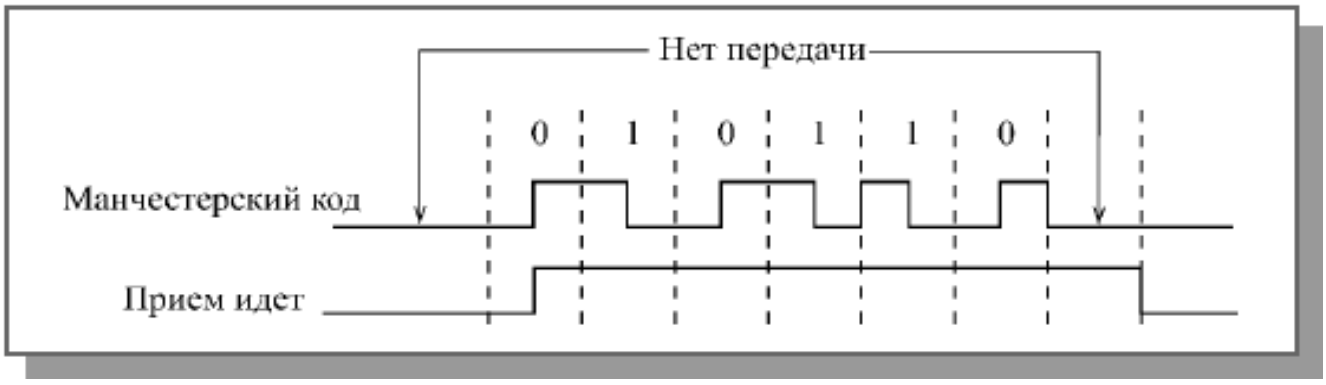


Рис. 5.15. Визначення початку і кінця прийому при манчестерському коді

Основна перевага *манчестерського коду* – постійна складова в сигналі (половину часу сигнал має високий рівень, іншу половину – низький).

Постійна складова дорівнює середньому значенню між двома рівнями сигналу.

Якщо ж один з рівнів сигналу в манчестерському коді нульовий (як, наприклад, в мережі *Ethernet*), то величина постійної складової впродовж передачі буде дорівнювати приблизно половині амплітуди сигналу.

Це дозволяє легко фіксувати зіткнення пакетів в мережі (конфлікт, колізію) по відхиленню величини постійної складової за встановлені межі.

Біфазний код відрізняється від класичного *манчестерського коду* тим, що він не залежить від зміни місць двох дротів кабелю. Особливо це зручно у випадку, коли для зв'язку використовується кручена пара, дроти якої легко переплутати.

Саме цей код використовується в одній з самих відомих мереж *Token-Ring* компанії *IBM*

Принцип даного коду простий: на початку кожного бітового інтервалу сигнал змінює рівень на протилежний попередньому, а в середині одиничних (і тільки одиничних) бітових інтервалів рівень змінюється ще раз. Таким чином, на початку бітового інтервалу завжди є перехід, який використовується для самосинхронізації.

Як й у випадку класичного *манчестерського коду*, в частотному спектрі при цьому присутні дві частоти. При швидкості 10 Мбіт/с це частоти 10 МГц (при послідовності одних одиниць: 11111111...) і 5 МГц (при послідовності одних нулів: 00000000...).

Інші коди

Усі розроблені в останні часи коди призведені знайти компроміс між полосою пропускання кабелю, що потребується при заданій швидкості передачі і можливістю самосинхронізації. Розробники намагаються зберегти самосинхронізацію, але не ціною двократного збільшення полоси пропускання, як в *RZ, манчестерському і біфазному кодах.*

Частіше всього для цього в потік бітів, що передаються, добавляють біти синхронізації. Наприклад, один біт синхронізації на 4, 5 або 6 інформаційних бітів

або два біта синхронізації на 8 інформаційних бітів. В дійсності усе дещо складніше: *кодування* не зводиться до простої вставки в дані, що передаються додаткових бітів.

Групи інформаційних бітів перетворюються в групи з кількістю бітів на один чи два більше. Приймач виконує зворотнє перетворення, відновлює вихідні інформаційні біти. Доволі просто відбувається в цьому випадку й визначення несучої частоти (детектування передачі).

В мережі *FDDI* (швидкість передачі 100 Мбіт/с) використовується код 4B/5B, який 4 інформаційних біта перетворює в 5 бітів, що передаються.

При цьому синхронізація приймача відбувається один раз на 4 біта, а не в кожному біті, як у випадку *манчестерського коду*. Але при цьому необхідна смуга пропускання збільшується у порівнянні з кодом *NRZ* не в два рази, а тільки в 1,25 рази (тобто складає не 100 МГц, а всього лише 62,5 МГц).

По тому ж принципу будуються й інші коди, такі як, 5B/6B, який використовується в стандартній мережі *100VG-AnyLAN*, або 8B/10B, що використовується в мережі Gigabit Ethernet [8].

Іноді вже *закодована інформація* піддається додатковому кодування, що дозволяє спростити синхронізацію на приймальному кінці. Найбільшого поширення для цього отримали:

- *2-рівневий код NRZI*, який застосовується в оптоволоконних мережах (*FDDI і 100BASE-FX*);
- *3-рівневий код MLT-3*, який використовується в мережах на кручених парах (*TPDDI і 100BASE-TX*).

Обидва ці коди не є самосинхронізуючими.

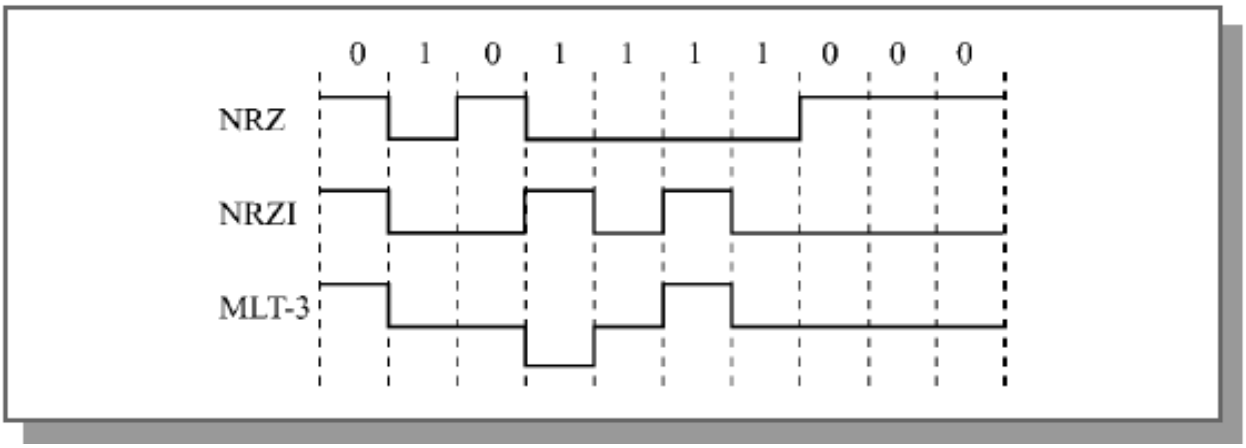


Рис. 5.16. Несамосінхронізуючі коди

Код NRZI (без повернення до нуля з інверсією одиниць - Non-Return to Zero, Invert to one) передбачає, що рівень сигналу змінюється на протилежний на початку одиничного бітового інтервалу і не змінюється при передачі нульового бітового інтервалу

При послідовності одиниць на кордонах бітових інтервалів є переходи, при послідовності нулів - переходів немає.

У цьому сенсі код *NRZI* краще синхронізується, ніж *NRZ* (там немає переходів ні при послідовності нулів, ні при послідовності одиниць).

Код MLT-3 (Multi-Level Transition-3) передбачає, що при передачі нульового бітового інтервалу рівень сигналу не змінюється, а при передачі одиниці - змінюється на наступний рівень по такому ланцюжку: + U, 0, -U, 0, + U, 0, -U і т.д.

Таким чином, максимальна частота зміни рівнів виходить вчетверо менше швидкості передачі бітів (при послідовності суцільних одиниць). Необхідна смуга пропускання виявляється менше, ніж при коді *NRZ* [8].

Всі коди передбачають безпосередню передачу в мережу цифрових дво- або триповерхових прямокутних імпульсів.

Ефективність і якість передачі двійкових сигналів

Основні показники, які характеризують ефективність і якість передачі двійкових сигналів по цифровим трактам [4]:

1. Швидкість модуляції – визначає максимальне число одиничних елементів, які можливо передати протягом однієї секунди:

$$B = \frac{1}{\tau}$$

де B - швидкість модуляції, Бод; τ – протяжність одного елемента, с.

2. Коефіцієнт використання пропускної спроможності цифрового тракта:

$$K_{вик} = \frac{B_{max}}{B_c}$$

де B_{max} – максимальна швидкість модуляції цифрового сигналу; B_c- швидкість модуляції лінійного сигналу в цифровому тракті. Номінальна швидкість модуляції B_0, виходячи з крайових спотворень на вході цифрового тракта, повинна бути не менша B_{max} (зазвичай $Bo = 0{,}5$).

3. Коефіцієнт помилок, який визначає відношення числа прийнятих з помилкою елементів (знаків, блоків) до числа усіх переданих елементів. Величина цього коефіцієнта, яка вихначає вірність передачі, в сучасних системах передачі даних досягає значень $10^{-6}…10^{-12}$.

4. Коефіцієнт розмноження помилок, який визначається для поодиноких помилок виразом:

$$\lambda = \frac{P_{дв}}{P_c}$$

де $P_{дв}$ - ймовірність помилки для двійкового сигналу; P_c - ймовірність для лінійного цифрового сигналу.

5. Коефіцієнт крайових спотворень, який хаактеризує розходження між значущим моментом в переданому та прийнятому сигналах:

$$\delta_o = \frac{\Delta\tau}{\tau_o}$$

де $\Delta\tau$ – помилка між значущим моментом в двійкому сигналі і моментом його передачі в цифровому тракті;

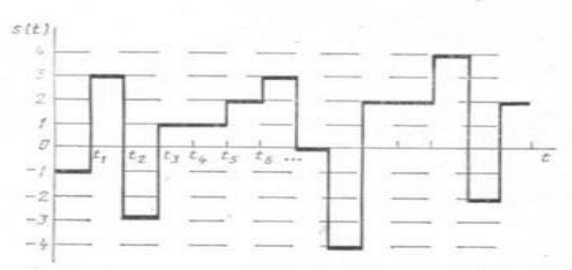
$$\tau_o = \frac{1}{B_o}$$

Контрольні питання до розділу

1. Модуляція, при якій логічній одиниці відповідає сигнал більш високої частоти, а логічному нулю - сигнал більш низької частоти (або навпаки):
    a. *Амплітудна модуляція (АМ);*
    b. *Частотна модуляція (ЧМ);*
    c. *Фазова модуляція (ФМ);*
    d. *Квадратурна модуляція (QAM);*
    e. *Імпульсно-кодова модуляція (ІКМ).*
2. Різновид імпульсно-кодової модуляції (ІКМ), в якій число рівнів квантування дорівнює двом. При цьому по каналу зв'язку передається не абсолютне значення сигналу, а різниця між вихідним аналоговим сигналом і апроксимується напругою (сигнал помилки):
    a. *Диференціальна імпульсно-кодова модуляція (ДІКМ);*
    b. *Імпульсно-кодова модуляція (ІКМ);*
    c. *Адаптивна диференціальна імпульсно-кодова модуляція (АДІКМ);*
    d. *Сігма-дельта модуляція (Σ-Δ);*
    e. *Квадратурна амплітудна модуляція (QAM);*
    f. *Дельта-модуляція (ДМ).*
3. Код, що має не три, а всього два рівня, що сприяє його кращій завадозахищеності та спрощенню приймаючих і передаючих вузлів. Логічному нулю відповідає позитивний перехід в центрі бітового інтервалу (тобто є перша половина бітового інтервалу – низький рівень, інша половина – високий), а логічній одиниці відповідає негативний перехід в центрі бітового інтервалу (або навпаки).
    a. *код NRZ;*
    b. *код RZ;*
    c. *Манчестерський код;*
    d. *Біфазний код;*
    e. *5B/6B.*
4. Спосіб модуляції, що забезпечує оцифровку сигналу з заданими характеристиками в робочій смузі частот. Призначена для аналого-цифрового і цифро-аналогового перетворень звукових сигналів (ЗС):

a. *Диференціальна імпульсно-кодова модуляція (ДІКМ);*
b. *Сігма-дельта модуляція (Σ-Δ);*
c. *Адаптивна диференціальна імпульсно-кодова модуляція (АДІКМ);*
d. *Дельта-модуляція (ДМ);*
e. *Квадратурна модуляція (QAM);*
f. *Імпульсно-кодова модуляція (ІКМ).*

5. Код, де на початку кожного бітового інтервалу сигнал змінює рівень на протилежний попередньому, а в середині одиничних (і тільки одиничних) бітових інтервалів рівень змінюється ще раз. Таким чином, на початку бітового інтервалу завжди є перехід, який використовується для самосинхронізації:
   a. *код NRZ;*
   b. *код RZ;*
   c. *Манчестерський код;*
   d. *Біфазний код;*
   e. *5B/6B.*
6. Який тип сигналу зображений на рисунку:



   a. *неперервний неперервного часу,*
   b. *неперервний дискретного часу,*
   c. *дискретний неперервного часу,*
   d. *дискретний дискретного часу.*
7. Простійший код, представляє собою звичайний цифровий сигнал. Логічному нулю відповідає високий рівень напруги в кабелі, логичній одиниці – низький рівень напруги. Рівні можуть бути різної полярності або ж однієї полярності. На протязі бітового інтервалу, тобто часу передачі одного біту ніяких змін рівня сигналу в кабелі не відбувається.
   a. *код NRZ;*
   b. *код RZ;*
   c. *Манчестерський код;*
   d. *Біфазний код;*
   e. *5B/6B.*
8. Модуляція, при якій зміні логічного нуля на логічну одиницю і навпаки відповідає різка зміна фази синусоїдального сигналу однієї частоти і амплітуди:
   a. *Амплітудна модуляція (АМ, AM - Amplitude Modulation),*
   b. *Частотна модуляція (ЧМ, FM - Frequency Modulation),*
   c. *Фазова модуляція (ФМ, PM - Phase Modulation),*
   d. *Квадратурна модуляція (QAM),*

e. *Імпульсно-кодова модуляція (ІКМ або PCM - Pulse Code Modulation).*

9. Модуляція, при якій логічній одиниці відповідає наявність сигналу (або сигнал більшої амплітуди), а логічному нулю - відсутність сигналу (або сигнал меншої амплітуди):

a. *Амплітудна модуляція (АМ);*
b. *Частотна модуляція (ЧМ);*
c. *Фазова модуляція (ФМ);*
d. *Квадратурна модуляція (QAM);*
e. *Імпульсно-кодова модуляція (ІКМ).*

10.Вид дискретної модуляції, при якій передається аналоговий первинний сигнал, що перетворюється в цифровий код - послідовність імпульсів (1 «одиниць») і пауз (0-«нулів»), мають однакову тривалість, застосовується найбільш широко в сучасній радіоелектроніці і системах зв'язку:

a. *Диференціальна імпульсно-кодова модуляція (ДІКМ або DPCM - Differential PCM)*
b. *Адаптивна диференціальна імпульсно-кодова модуляція (АДІКМ або ADPCM - Adaptive DPCM)*
c. *Квадратурна модуляція (QAM),*
d. *Імпульсно-кодова модуляція (ІКМ або PCM - Pulse Code Modulation).*
e. *Дельта-модуляція (ДМ або Δ модуляція)*

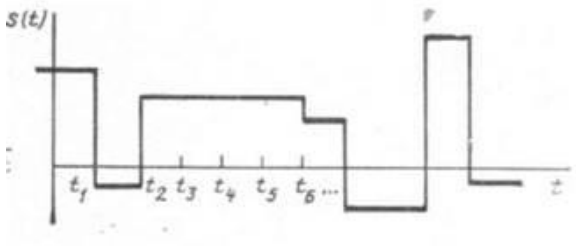
11. Різновид модуляції, алгоритм якої має на увазі зміну кроку квантування, що дозволяє знизити необхідну смугу пропускання для заданого відношення сигнал / шум:

a. *Диференціальна імпульсно-кодова модуляція (ДІКМ або DPCM - Differential PCM);*
b. *Адаптивна диференціальна імпульсно-кодова модуляція (АДІКМ або ADPCM - Adaptive DPCM);*
c. *Сігма-дельта модуляція (Σ-Δ);*
d. *Квадратурна модуляція (QAM);*
e. *Імпульсно-кодова модуляція (ІКМ або PCM - Pulse Code Modulation);*
f. *Дельта-модуляція (ДМ або Δ модуляція)*.

12. Трьохрівневий код, де після значащого рівня сигналу в першій половині бітового інтервалу відбувається повернення до "нульового", середнього рівня (наприклад, до нульового потенціалу). Перехід до нього відбувається в середині кожного бітового інтервалу. Логічному нулю, таким чином, відповідає позитивний імпульс, логічній одиниці – негативний (або навпаки) в першій половині бітового інтервалу:

a. *код NRZ;*
b. *код RZ;*
c. *Манчестерський код;*
d. *Біфазний код;*
e. *5B/6B.*

13. Який тип сигналу зображений на рисунку.



a. *неперервний неперервного часу,*
b. *неперервний дискретного часу,*
c. *дискретний неперервного часу,*
d. *дискретний дискретного часу.*

14. Модуляція, при якій логічній одиниці відповідає сигнал більш високої частоти, а логічному нулю - сигнал більш низької частоти (або навпаки):

a. *Амплітудна модуляція (АМ);*
b. *Частотна модуляція (ЧМ);*
c. *Фазова модуляція (ФМ);*
d. *Квадратурна модуляція (QAM);*
e. *Імпульсно-кодова модуляція (ІКМ).*

15. Який тип сигналу зображений на рисунку.

a. *неперервний неперервного часу,*
b. *неперервний дискретного часу,*
c. *дискретний неперервного часу,*
d. *дискретний дискретного часу.*

16. В чому відмінність між амплітудно-імпульсною (АІМ) та широтно-імпульсною (ШІМ) модуляціями?

17. Що собою представляє фазоімпульсна модуляція?

18. Що собою представляє частотно-імпульсна модуляція?

19. Що собою представляє імпульсно-кодова модуляція?

20. Що собою представляє адаптивна диференціальна імпульсно-кодова модуляція?

21. Що собою представляє сігма-де́льта модуляція?

22. Що собою представляє де́льта модуляція. Переваги та недоліки?

23. Співвідношення швидкості передачі даних до використаної смуги частот пропускання каналу:

a. *енергетична ефективність;*
b. *спектральна ефективність;*
c. *стійкість до впливів каналу передачі;*
d. *лінійність підсилювачі;*
e. *складність реалізації.*

24. Характеризує достовірність переданих даних при впливі на сигнал адитивного білого гауссовского шуму, за умови, що послідовність символів відновлена ідеальним демодулятором:

a. енергетична ефективність;
b. спектральна ефективність;
c. стійкість до впливів каналу передачі;
d. лінійність підсилювачі;
e. *складність реалізації.*

25. Характеризує достовірність переданих даних при впливі на сигнал специфічних викривлень: завмирання внаслідок багатопроменевого поширення, обмеження смуги, зосереджені по частоті або часу завади:

а) енергетична ефективність;
б) спектральна ефективність;
в) стійкість до впливів каналу передачі;
г) лінійність підсилювачі;
д) складність реалізації.

26. Визначається обчислювальним ресурсом, необхідним для реалізації алгоритму демодуляції, і вимогами до характеристик аналогової частини:

a. енергетична ефективність;
b. спектральна ефективність;
c. стійкість до впливів каналу передачі;
d. лінійність підсилювачі;
e. складність реалізації.

27. У якому методі кодування використовують три рівні потенціалу?

a. AMI;
b. NRZ;
c. манчестерське кодування;
d. *код 2B1Q*;
e. біфазний код.

28. Що описує параметр NEXT (Near End Crosstalk) в сертифікації кабелів скруче ної пари дротів?

a. співвідношення сигналу на кінці лінії і сигналу на її початку;
b. рівень перехресних завад на сусідніх дротах у разі однонапрямленого переда вання;
c. характеризує завади в сусідніх дротах у разі передавання даних парою дротів у різних напрямах;
d. відношення амплітуди переданого сигналу до амплітуди відбитого.

29. Що собою представляє квадратурно-амплітудна модуляція?

30. У якому діапазоні електромагнітного спектру працює супутниковий зв’язок?

a. ультрафіолетовий діапазон;
b. інфрачервоний діапазон;
c. діапазон видимого світла;
d. мікрохвильовий діапазон.

31. Що собою представляє амплітудно-фазова модуляція з придушенням несучої (CAP)?

32. Що собою представляє BPSK(Binary Phase-Shift Keying)?

33. Що собою представляє квадратурна фазова модуляція QPSK?

34. Яким чином працює код без повернення до нуля з інверсією одиниць NRZI?

35. Яким чином працює код MLT-3?

36. Яким чином працює біфазний код?

Список рекомендованої літератури

1. Телекомунікаційні та інформаційні мережі: Підручник для вищіх навчальних закладів. / *П.П.Воробієнко, Л.А.Нікітюк, П.І.Резніченко.* – К.: САММІТ-КНИГА, 2010. - 708 с.
2. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
3. *Новиков Ю. В., Кондратенко С. В.* Основы локальных сетей. Курс лекций. [Електронний ресурс] – М.: Интернет-университет информационных технологий, 2005. – ISBN 5-9556-0032-9. Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/57/57/info.
4. *Беркман Л.Н., Жураковський Б.Ю., Макаренко А.О.* Теорія передачі даних в інфокомунікаціях. [Навчальний посібник]. - К.: ДУТ, 2015.- 160с.
5. *Б.Ю Жураковський, Г.С Срочинська, Н.М Довженко* Кінцеві пристрої абонентського доступу [Навчальний посібник]. - К.: ДУТ, 2015 – 65 с.
6. *Ирвин Дж.* Передача данных в сетях: инженерный подход / Дж. Ирвин, Д. Харль. – СПб.: БХВ-Петербург, 2003. – 448 с.
7. Теория передачи сигналов: учебник для вузов / *А. Г. Зюко, Д. Д. Кловский, М. В. Назаров, Л. М. Финк.* – М. : Радио и связь, 1986. – 304 с.
8. *Дружинін В.А., Степанов М.М., Жураковський Б. Ю.* Обгрунтування доцільності практичного використання лінійно-частотно модульованих сигналів із внутріімпульсною фазовою маніпуляцією та різними модуляційними характеристиками в системах радіозв'язку. // Системи управління, навігації та зв'язку, №3 (2018р).- Полтава, 2018. – с. 33-35.

Розділ 6. СПОСОБИ КОМУТАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

6.1. Загальні положення

Для передачі дискретних повідомлень (ПДП) через мережу можуть бути встановлені з'єднання двох видів – *довгострокові* й *оперативні*. Відповідно до цього розрізняють два види мереж ПДП – з *довгостроковою* й *оперативною* комутацією.

Довгостроковою або ***кросовою*** комутацією називається такий спосіб комутації, при якому між двома точками мережі встановлюється пряме постійне з'єднання цілодобово чи з великим інтервалом часу. Канали, що беруть участь в організації таких з'єднань, називаються *виділеними*.

Після закінчення чергового сеансу зв'язку з'єднання не руйнується і перед початком сеансу не встановлюється заново. Іншими словами, між двома користувачами обмін підтримується постійно по тому самому каналу. Кросові з'єднання реалізуються за допомогою спеціальних розподільних пристроїв.

Застосування кросової комутації доцільне тільки в тих випадках, коли вимоги користувачів винятково високі, і вони не можуть бути задоволені застосуванням оперативної комутації. При цьому варто враховувати, що із зростанням кількості абонентських пунктів кількість необхідних ліній і оснащеність вузлів збільшуються дуже швидко, тому мережа з кросовою комутацією є самою неекономічною.

В основному в мережах ПДП застосовується ***оперативна*** комутація, при якій між двома точками мережі організовується тимчасове з'єднання. Розрізняють чотири види оперативної комутації: каналів (КК), повідомлень (Кп), пакетів (КП) і гібридну (ГК).

Важливим завданням архітектури відкритих мереж є ***комутація інформації***, тобто прокладення в мережах трактів, необхідних для доставлення послідовностей блоків даних абонентським системам-адресатам.

У деяких мережах від джерела до одержувача передаються блоки даних – *пакети*. Цей процес називається комутацією пакетів. Джерелами й одержувачами можуть бути термінали користувачів, комп'ютери, принтери чи будь-які інші пристрої передачі й обробки даних.

У мережах іншого типу застосовується *техніка комутації каналів* (у широко розповсюджених і звичних нам телефонних мережах). У таких мережах, якими звичайно передається мова і дані, між будь-якою парою чи групою користувачів, що намагаються зв'язатися один з одним, встановлюється окремий шлях передачі. Він утримується стільки часу, скільки вимагає передача.

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

Найтиповіші види навантаження створюють: передача даних в інтерактивному режимі, коли між терміналами чи між терміналами і комп'ютерами передаються короткі пачки повідомлень, що містять 400 – 1000 знаків; передача файлів, у цьому випадку між комп'ютерами або між нагромаджувачами масивів даних передається до мільйона знаків (чи байтів), і все зростаюча цифрова передача мови.

Передача мови і сьогодні залишається найрозповсюдженішим видом зв'язку в усьому світі. Вона характеризується невеликими капіталовкладеннями на устаткування. Телефонні мережі, створені для передачі мови, охоплюють усі регіони земної кулі. Прогнози показують, що мова буде залишатися і надалі джерелом найбільшого навантаження засобів зв'язку в усьому світі.

Телефонний зв'язок у реальному часі завжди здійснюється з комутацією каналів, хоча велика увага приділяється і можливостям передачі мови в реальному часі у формі пакетів. Дослідження цього виду мовного зв'язку тривають. У різних частинах світу були створені також мережі передачі даних з комутацією каналів.

У деяких випадках, наприклад у керуванні виробничими процесами, потрібно, щоб затримка доставки адресатові кожного блока, що передається, не перевищувала визначеного максимуму. Але найчастіше ця вимога відсутня, і

блоки даних можуть у розумних межах проходити з випадковим запізненням. Природно, що в цьому випадку устаткування і програмне забезпечення комутації інформації значно простіші [1].

Комутація є необхідним елементом зв'язку вузлів між собою, що дозволяє скоротити кількість необхідних ліній зв'язку й підвищити завантаження каналів зв'язку. Практично неможливо надати кожній парі вузлів виділену лінію зв'язку, тому в мережах завжди застосовується той або інший спосіб комутації абонентів, що використовує існуючі лінії зв'язку для передачі даних різних вузлів.

Мережею, що комутується, називається мережа, у якій зв'язок між вузлами встановлюється тільки по запиту.

Абоненти з'єднуються з комутаторами виділеними (індивідуальними) лініями зв'язку. Лінії зв'язку, що з'єднують комутатори, використовуються абонентами спільно.

Комутація може здійснюватися у двох режимах: динамічно й статично. У першому випадку комутація виконується на час сеансу зв'язку (звичайно від секунд до годин) з ініціативи одного з вузлів, а по закінченні сеансу зв'язок розривається. У другому випадку комутація виконується обслуговуючим персоналом мережі на значно більше тривалий період часу (кілька місяців або років) і не може бути змінена з ініціативи користувачів. Такі канали називаються **виділеними** (*dedicated*) або **орендованими** (*leased*).

Дві групи способів комутації: **комутація каналів** (*circuit switching*) і **комутація із проміжним зберіганням** (*store-and-forward*). Друга група складається із двох способів: **комутації повідомлень** (*message switching*) і **комутації пакетів** (*packet switching*).

При **комутації каналів** між вузлами, яким необхідно встановити зв'язок один з одним, забезпечується організація безперервного складеного каналу, що складається з послідовно з'єднаних окремих каналів між вузлами. Окремі канали з'єднуються між собою комутуючим устаткуванням (комутаторами). Перед передачею даних необхідно виконати процедуру встановлення з'єднання, у процесі якої створюється складений канал.

Під **комутацією повідомлень** розуміється передача єдиного блоку даних між вузлами мережі з тимчасовий буферизацією цього блоку кожним із транзитних вузлів. Повідомленням може бути текстовий файл, файл із графічним зображенням, електронний лист - повідомлення має довільний розмір, обумовлений виняткова його змістом, а не тими або іншими технологічними міркуваннями.

При **комутації пакетів** всі передані користувачем дані розбиваються передавальним вузлом на невеликі (до декількох кілобайт) частини – **пакети** (packet). Кожний пакет оснащується заголовком, у якому вказується, як мінімум, адреса вузла-одержувача й номер пакета. Передача пакетів по мережі відбувається незалежно друг від друга. Комутатори такої мережі мають внутрішню буферну пам'ять для тимчасового зберігання пакетів, що дозволяє згладжувати пульсації трафіка на лініях зв'язку між комутаторами. Пакети іноді називають **дейтаграмами (***datagram***)**, а режим індивідуальної комутації пакетів – **дейтаграмним** режимом.

Серед безлічі можливих підходів до вирішення завдання комутації абонентів у мережах виділяють два основних:

- ***комутація каналів (circuit switching);***
- ***комутація пакетів (packet switching).***

6.2. Комутація каналів

При комутації каналів комутаційна мережа утворює між кінцевими вузлами безперервний складовою фізичний канал з послідовно з'єднаних комутаторами проміжних канальних ділянок. Умовою того, що кілька фізичних каналів при послідовному з'єднанні утворюють єдиний фізичний канал, є рівність швидкостей передачі даних у кожному зі складових фізичних каналів. Рівність швидкостей означає, що комутатори такої мережі не повинні буферизувати передані дані.

У мережі з комутацією каналів перед передачею даних завжди необхідно виконати процедуру встановлення з'єднання, у процесі якої і створюється складений канал. І тільки після цього можна починати передавати дані.

Переваги комутації каналів

- *Постійна і відома швидкість передачі даних за встановленим між кінцевими вузлами каналу*
- *Низький і постійний рівень затримки передачі даних через мережу*
- *Не потребує ресурсів мережі для обробки повідомлень*

Недоліки комутації каналів

- *Відмова мережі в обслуговуванні запиту на встановлення з'єднання.*
- *Нераціональне використання пропускної здатності фізичних каналів.*
- *Обов'язкова затримка перед передачею даних через фази встановлення з'єднання.*
- *Неможливі зміни смуги пропускання каналу*
- *Неможлива інтеграція в одній мережі видів служб з різними швидкостями передачі*

6.3. Комутація пакетів

Ця техніка комутації була спеціально розроблена для ефективної передачі комп'ютерного трафіку.

Комутація каналів не дозволяє досягти високої загальної пропускної здатності мережі. Типові мережеві додатки генерують трафік дуже нерівномірно, з високим рівнем пульсації швидкості передачі даних.

При комутації пакетів всі передані користувачем повідомлення розбиваються у вихідному вузлі на порівняно невеликі частини, що називаються пакетами.

Мережа з *комутацією пакетів* уповільнює процес взаємодії конкретної пари абонентів, але підвищує пропускну здатність мережі в цілому.

Затримки в джерелі передачі:

- час на передачу заголовків;
- затримки, викликані інтервалами між передачею кожного наступного пакета.

Затримки в кожному комутаторі:

- час буферизації пакета;
- час комутації, яке складається з:

- часу очікування пакета в черзі (змінна величина);
- часу переміщення пакета у вихідний порт.

Переваги комутації пакетів

- Висока загальна пропускна здатність мережі при передачі пульсуючого трафіку.
- Можливість динамічно перерозподіляти пропускну здатність фізичних каналів зв'язку між абонентами відповідно до реальних потреб їхнього трафіку.

Недоліки комутації пакетів

- *Невизначеність швидкості передачі даних між абонентами мережі,* обумовлена тим, що затримки в чергах буферів комутаторів мережі залежать від загального завантаження мережі
- *Змінна величина затримки пакетів даних,* яка може бути досить тривалою у моменти миттєвих перевантажень мережі
- *Можливі втрати даних через переповнення буферів*
- *Висока складність протоколів канального і мережного рівнів*

6.4. Комутація повідомлень

Комутація повідомлень за своїми принципами близька до комутації пакетів.

Під *комутацією повідомлень* розуміється передача єдиного блоку даних між транзитними комп'ютерами мережі з тимчасовою буферизацією цього блоку на диску кожного комп'ютера.

Повідомлення на відміну від пакета має довільну довжину, яка визначається не технологічними міркуваннями, а змістом інформації, що становить повідомлення.

На ранній стадії розвитку мереж із комутацією повідомлень повідомлення комутувалися в центрах комутації (ЦК) з використанням системи ручного переприйому. Поява в 40-х рр. реперфораторів дала змогу здійснити напівавтоматичний переприйом. На даний час такі системи застосовуються у телеграфних мережах загального користування. Наприкінці

50-х і початку 60-х рр. почалося впровадження повністю автоматизованих систем комутації повідомлень. На перших етапах автоматизації операції переприйому виконувались електромеханічними пристроями, потім стали використовувати електронні пристрої. Починаючи із середини 60-х рр., ЦКп створюють в основному на базі систем з програмним керуванням. Основним елементом ЦКп у цей період стає обчислювальна машина. Швидке технічне переозброєння ЦКп з появою ЕОМ визначилося тим, що обчислювальна машина зі швидкодією в декілька сот тисяч операцій у секунду може бути використана як керуюча система в ЦКп, до якої приєднано декілька сот і навіть тисяч каналів ПДП [2].

Застосування принципу переприйому дозволяє реалізувати динамічний метод розподілу ресурсів, у тому числі і зв'язаних, між множиною користувачів. Тепер обсяг устаткування, на відміну від мереж із комутацією каналів (КК), не повинен визначатися з розрахунку обслуговування максимального навантаження. Повідомлення, що надійшли в години найбільшого навантаження (ГНН) і не передані користувачеві, розміщаються в нагромаджувачах ЦКп і передаються в період часу, коли навантаження спадає. Разом з тим, мережа з Кп має дуже істотний недолік, обумовлений саме принципом переприйому: час затримки в мережах із Кп є величиною змінною і носить випадковий характер. На тривалість затримки впливають такі основні фактори: пропускна спроможність каналів, швидкодія ЦКп (характеристики детерміновані) і інтенсивність потоку повідомлень, що надходить у мережу (величина випадкова). Другий недолік мережі з КП – неможливість організації діалогу між користувачами через відсутність прямого з'єднання між абонентськими пунктами [3].

Зазначені недоліки принципу передачі з проміжним нагромадженням відсутні в мережах із комутацією пакетів.

6.5. Порівняння комутації каналів і пакетів

Комутація каналів:

- Гарантована пропускна здатність (смуга) для взаємодіючих абонентів
- Мережа може відмовити абоненту у встановленні з'єднання
- Трафік реального часу передається без затримок
- Адреса використовується тільки на етапі встановлення з'єднання

Комутація пакетів:

- Пропускна здатність мережі для абонентів невідома, затримки передачі носять випадковий характер
- Мережа завжди готова прийняти дані від абонента
- Ресурси мережі використовуються ефективно при передачі пульсуючого трафіка
- Адреса передається з кожним пакетом.

У табл. 6.1 наведено для порівняння основні характеристики мереж з різними способами комутації.

Таблиця 6.1. *Характеристика мереж з різними способами комутації*

Характеристика	Спосіб комутації		
	КК	Кп	КП
Наявність електричного з'єднання	Тимчасове	Відсутнє	Відсутнє
Накопичення повідомлень	Відсутнє	У зовнішньому запам'ятовуючому пристрої	Невеликі частини повідомлень у запам'ятовуючому пристрої
Можливість діалогу	Можливий	Неможливий	Неможливий
Організація тракту	На інтервал тривалості одного з'єднання	Для кожного повідомлення лише ЦКп	Для кожного пакету чи на час сеансу
Процес виникнення затримки	Основна затримка при встановленні з'єднань	Основна затримка при передаванні	Дуже малі затримки при встановленні з'єднань і передаванні
Режим роботи мережі	З відмовленнями	З очікуванням	З очікуванням і відмовленнями
Режим перевантаження	З відмовленнями	Зростають затримки на доставлення	Затримки на доставлення значно менші, ніж у мережах Кп. Ймовірність відмовлень на

			порядок менша за ймовірність у випадку КК
Режим захисту повідомлень	Виконується користувачем	Основні функції реалізуються у мережі	Основні функції реалізуються у мережі
Можливість перетворень швидкостей, кодів і форматів	Неможливі	Можливі	Можливі
Обсяг навантажень, при яких досягається економічність	Малий	Великий	Великий

6.6. Постійна і динамічна комутація

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

- мережі з *динамічною комутацією*;
- мережі з *постійною комутацією*.

У мережах з *динамічною* комутацією:

- дозволяється встановлювати з'єднання з ініціативи користувача мережі;
- комутація виконується тільки на час сеансу зв'язку, а потім (за ініціативою одного з користувачів) розривається;
- в загальному випадку користувач мережі може з'єднатися з будь-яким іншим користувачем мережі;
- час з'єднання між парою користувачів при динамічній комутації складає від декількох секунд до декількох годин і завершується після виконання певної роботи - передачі файлу, перегляду сторінки тексту або зображення і т.п.

Мережа, що працює в режимі ***постійної комутації***:

- дозволяє парі користувачів замовити з'єднання на тривалий період часу;
- з'єднання встановлюється не користувачами, а персоналом, який обслуговує мережу;
- період, на який встановлюється постійна комутація, складає зазвичай декілька місяців;

- режим *постійної* (*permanent*) комутації в мережах з комутацією каналів часто називається сервісом *виділених* (*dedicated*) або *орендованих* (*leased*) каналів;
- в тому випадку, коли постійне з'єднання через мережу комутаторів встановлюється за допомогою автоматичних процедур, ініційованих обслуговуючим персоналом, його часто називають *полупостійним (semi-permanent)* з'єднанням, на відміну від режиму ручного конфігурування кожного комутатора.

6.7. Змішана комутація

При змішаній комутації використовуються рівні і процеси, застосовувані як у комутації каналів, так і в комутації пакетів. Існуючі канали віддають у першу чергу для створення трактів, що з'єднують абонентські системи. Вільні канали не простоюють і використовуються для комутації пакетів. Природно, що в даному випадку в підмережі встановлюються комбіновані вузли. Вони виконують як роль комутаторів каналів, так і комутаторів пакетів.

Змішана комутація починає широко використовуватися для одночасної передачі по одних і тих самих групах каналів і даних, і мови.

На цей час одним з найважливіших науково-технічних напрямків у галузі інфокомунікацій є створення конвергентних (об'єднаних або інтегральних) цифрових мереж зв'язку. Конвергентна мережа має об'єднати існуючі мережі передачі інформації, у першу чергу телефонні, локальні і мережі передавання даних, а також включити у свій склад і мережі передавання зображень.

Необхідність побудови конвергентної мережі визначається потребою підвищення ефективності використання мережних ресурсів, забезпечення доступу користувачів до широкого набору послуг у рамках однієї мережі. Досвід експлуатації окремих мереж передачі інформації, дослідження вимог користувачів до інформаційних послуг показують, що засоби комп'ютерних мереж як складова частина інфраструктури для суспільства можуть стати ефективними тільки за умови конвергенції всіх засобів різноманітних мереж у вигляді єдиної системи [4].

6.8. Інтегральна комутація

Як і змішана, інтегральна комутація призначена для забезпечення передачі інформації з заданим і випадковим часом доставки блоків даних. Проте інтегральна комутація відрізняється від змішаної тим, що тут комутація каналів і комутація пакетів здійснюються одночасно в кожному фізичному каналі.

Для забезпечення інтегральної комутації в кожному такому каналі прокладається група віртуальних каналів. Будь-який з них працює так, що створюється враження ніби пара взаємодіючих абонентських систем, яка використовує віртуальний канал, передає блоки даних за призначеним для них фізичним каналом.

Інтегральна комутація інформації здійснюється різними способами. Один з них називається *асинхронним часовим мультиплексуванням* (АЧМ). Суть цього способу ілюструється рис. 6.1, відповідно до якого для кожного фізичного каналу мережі час поділяється на повторювані цикли. По каналу передаються розмежники, кожен з яких повідомляє про початок чергового циклу. Після цього в кожному циклі виділяються n інтервалів часу, необхідних для створення n віртуальних каналів [5].

На базі тимчасових інтервалів створюються віртуальні канали. Так, інтервали “Канал 1” у послідовності циклів утворюють віртуальний канал 1, наданий парі абонентських систем. Аналогічно з інтервалів i, де $i = 2,\ldots, n$, утвориться віртуальний канал i.

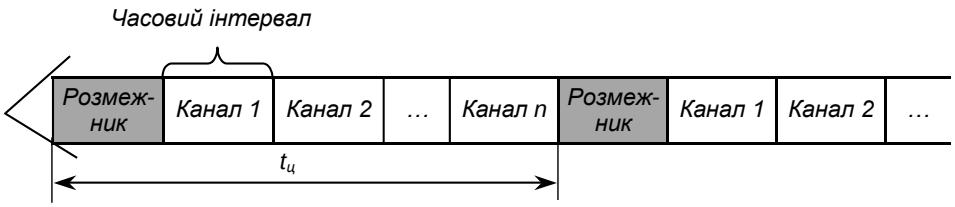


Рис. 6.1. Структура циклу асинхронного мультиплексування ($t_ц$ – тривалість циклу)

Розглянемо приклад, показаний на рис. 6.2 і в табл. 6.2. У мережі є чотири магістральних канали *a*,*b*,*c*,*d*, що зв'язують чотири вузли (маршрутизатора). У цих каналах час розподілений на цикли, кожний з яких містить до чотирьох часових інтервалів.

Таблиця 6.2. *Організація віртуальних каналів*

Номер каналу	Взаємодіючі абонентські системи	Віртуальні канали
1	*А–Е*	a_1
2	*В–К*	a_2
3	*Д–М*	c_1+d_1
4	*І–Т*	d_2+b_1

Нехай потрібно організувати одночасно взаємодію чотирьох пар абонентських систем, показаних у табл. 6.2. Ця взаємодія має забезпечити роботу в режимі комутації каналів (у прозорому режимі).

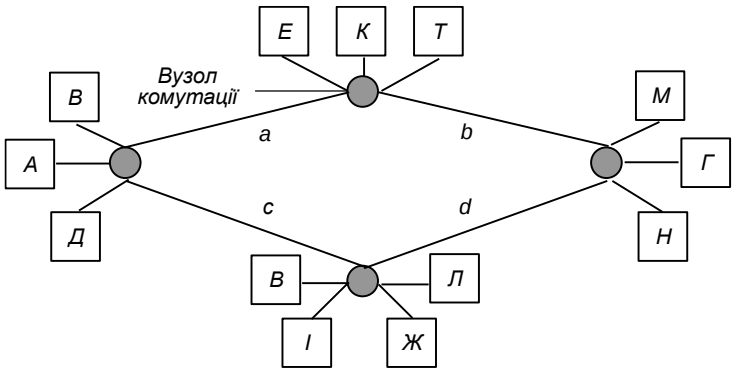


Рис. 6.2. Схема організації віртуальних каналів

З цією метою в порядку надходження замовлень для системи *А–Е* у фізичному каналі *a* у кожному циклі до закінчення сеансу взаємодії виділяється перший віртуальний канал (перший часовий інтервал), позначений a_1. Таким способом система *А–І* одержує через кожні $t_ц$ (див. рис. 6.1) часовий інтервал

для передачі блоків даних. У результаті відбувається передача інформації зі швидкістю $p/t_ц$ блоків за секунду, де p – число блоків.

Аналогічно для систем *В–К* у тому ж каналі дається другий віртуальний канал a_2. Для системи *Д–М* виділяється послідовність, що складається з каналів c_1, d_1. Система *І–Т* одержує послідовність каналів d_2, b_1.

Між системами, розташованими в мережі (рис. 4.3), можливі й інші тракти взаємодії. Так, системи *А–І* можуть взаємодіяти не тільки через фізичний канал a, але також через послідовність фізичних каналів c, d, b. Системи *Д–М* можуть бути зв'язані через фізичні канали a і b [5].

По фізичних каналах, що з'єднують абонентські системи з вузлами комутації, також можуть передаватися повторювані цикли, показані на рис. 6.2. Тоді кілька прикладних процесів однієї системи можуть одночасно взаємодіяти з групою процесів інших абонентських систем.

Після того, як часові інтервали розподілені за запитами на комутацію каналів, здійснюється друга частина керування комутацією інформації. Часові інтервали, що залишилися, використовуються для передачі в послідовності черги блоків даних, що направляються будь-якими абонентськими системами. Інакше кажучи, у ці часові інтервали здійснюється комутація пакетів. Так, у стані, показаному в табл. 6.2, для комутації пакетів використовуються вільні ділянки. Природно, що картина запитів на комутацію каналів увесь час змінюється. Відповідно до цього змінюється і список часових інтервалів, що залишаються для комутації пакетів.

Отже, при інтегральній комутації уже фактично немає в класичному розумінні ні комутації каналів, ні комутації пакетів. Тут обидва види комутації злилися в один спосіб передавання інформації з гарантією або без гарантії часу доставки блоків даних.

Важливо відзначити, що попередні способи комутації інформації оперували зі значним (не менше трьох) числом каналів у комунікаційній підмережі. Що ж стосується інтегральної комутації, то вона може здійснюватися і при наявності в підмережі тільки одного фізичного каналу, наприклад моноканалу. На базі інтегральної комутації дається можливість

передавати будь-які види інформації: дані, графіку, факсиміле, мову і навіть телебачення

6.9. Швидка комутація каналів

З метою підвищення ефективності використання мережних ресурсів для служб зі швидкістю передачі, що змінюється, і високою пачковістю трафіка була запропонована концепція швидкої комутації каналів (FCS – Fast Circuit Switching). Ресурси в мережі зі швидкою комутацією каналів використовуються тільки тоді, коли передається інформація.

Підвищення ефективності використання цифрових трактів зв'язку можливе за рахунок статистичного ущільнення [6], якщо при обслуговуванні телефонного навантаження на пучок цифрових каналів 64 кбіт/с надходить потік заявок на встановлення з'єднання не на весь термін сеансу зв'язку, а тільки на термін передачі фрагмента мови. У разі ідеальної роботи системи сигналізації з однією і тією ж імовірністю відмовлення обслуговувати ефективність використання цифрового тракту може бути підвищена в 1,8–2 рази.

Об'єднання ідей швидкої і багатошвидкісної комутації каналів приводить до концепції багатошвидкісної швидкої комутації каналів (MRFCS – Multirate Fast Circuit Switching). За цим принципом можна сконструювати пристрій, який забезпечить можливість виділення каналів з різними швидкостями передачі інформації. Це дало б змогу збільшити гнучкість мережі та підвищити ефективність використання мережних ресурсів. Основним недоліком такого режиму переносу інформації є складність реалізації системи керування, що дозволяла б встановлювати і роз'єднувати наскрізні з'єднання абонент–абонент за дуже короткий інтервал часу. Проте через високі вимоги до системи сигналізації ШКК не була обрана для транспортування інформації в майбутній широкосмуговій мережі.

У системах передавання з багатошвидкісною комутацією каналів використовується той же метод часового поділу (TDM–Time Division Multiplexing), що і в системах зі звичайною комутацією каналів. Проте в одному з'єднанні може

використовуватися n ($n > 1$) основних цифрових каналів. Таким чином, кожне з'єднання може бути кратним швидкості основного каналу. Це рішення прийняте до використання в цифровій мережі інтегрального обслуговування (ISDN) для відеотелефонії. Відеокодеки, розроблені для ISDN згідно з Рекомендацією H.261, можуть працювати зі швидкістю $n \times 64$ кбіт/с при $n < 30$. Системи комутації, що забезпечують багатошвидкісну комутацію каналів, складніші порівняно з системами зі звичайною комутацією каналів, тому що всі канали окремих ланок, що утворюють з'єднання, повинні бути синхронними. Насправді, якщо кожен канал комутується індивідуально, то канали можуть бути обрані не коригованими за синхронізацією, а інформація з одного каналу може надходити в термінальний пристрій з меншими часовими затримками, ніж інформація з іншого каналу, що абсолютно неприпустимо, тому що кінцевий пристрій розглядає ці канали як єдине ціле [7].

Іншою складною проблемою для систем із багатошвидкісною комутацією каналів є вибір базової (основної) швидкості. Так, для деяких служб (наприклад, для телеметрії) потрібна дуже низька швидкість передачі (близько 1 кбіт/с). Для інших служб, наприклад для телебачення високої чіткості (ТБВЧ), може знадобитися швидкість близько 140 Мбіт/с. Якщо за основну швидкість вибрати мінімальну швидкість (1 кбіт/с), то для формування каналу ТБВЧ буде потрібно 140 тисяч цифрових каналів зі швидкістю 1 кбіт/с. Керування і забезпечення синфазності для всіх цих каналів з метою встановлення одного з'єднання стає практично завданням, яке неможливо виконати. Якщо для зменшення складності за основний цифровий канал вибирається канал зі значно більшою швидкістю, то ширина смуги, що залишається невикористаною, стає дуже великою. Так, у разі вибору за основний цифровий канал зі швидкістю 2 Мбіт/с (у цьому випадку для формування з'єднання в мережах ТБВЧ потрібно тільки 70 основних цифрових каналів), спроба передачі мови (64 кбіт/с) і тим більше даних телеметрії призводить до дуже низької ефективності використання пропускної спроможності. Дана технічна проблема може вирішуватися й інакше – використанням у комутаторі каналів кількох основних швидкостей шляхом

поділу основного часу кадру на кілька часових інтервалів різної довжини.

Слід також зазначити, що телебачення і високошвидкісна передача даних не можуть здійснюватися одночасно при багатошвидкісній комутації каналів навіть у каналах зі швидкістю 140 Мбіт/с, незважаючи на те, що сумарна швидкість цих двох служб складає всього 35 Мбіт/с. Крім того, при багатошвидкісній комутації дуже низька ефективність використання каналів у разі обслуговування джерел зі швидкістю передачі, що змінюється.

Обрана швидкість каналу повинна бути рівною або перевищувати пікову швидкість передачі джерела під час усього сеансу зв'язку (сесії), хоча середня швидкість передачі може бути дуже низькою.

Низькі гнучкість і ефективність обслуговування джерел з високими коефіцієнтами пачковості стали причиною того, що концепція багатошвидкісної комутації не була рекомендована ITU для широкосмугової ISDN (B-ISDN).

6.10. Швидка комутація пакетів і асинхронний режим переносу

Основною ідеєю швидкої комутації пакетів (ШКП) є пакетна комутація з мінімумом функцій, виконуваних вузлами комутації на рівні ланки з метою підвищення часової прозорості мережі.

Найменування асинхронного режиму переносу інформації – ATM (Asynchronous Transfer Mode) рекомендоване ITU. Крім абревіатури ATM у науковій і технічній літературі використовуються терміни "асинхронний режим доставки" й "асинхронний режим переносу" [8].

Іноді зустрічаються й інші терміни: ATD (Asynchronous Transfer Division – асинхронний режим часового ущільнення), FPS (Fast Packet Switching –швидка комутація пакетів).

Оскільки термін ATM рекомендований ITU, то в науковій і технічній літературі він зустрічається найчастіше.

При виборі фіксованої чи змінної довжини пакета для ATM враховуються такі основні фактори:

- ефективність використання пропускної спроможності цифрових трактів зв’язку;
- досягнення високої продуктивності комутаційного устаткування, точніше досягнення компромісу між швидкістю комутації і складністю реалізації комутаційних пристроїв;
- тривалість затримки пакета.

У загальному випадку ефективність використання пропускної спроможності цифрових трактів зв’язку із застосуванням пакетів змінної довжини дещо вища, ніж із застосуванням пакетів постійної довжини. Однак ця перевага не є визначальною. Варіант із пакетами постійної довжини кращий як за швидкістю роботи комутаційного устаткування, так і за обсягом буферного простору.

Експерти ITU зробили висновок про доцільність використання пакетів фіксованої довжини. Щоб підкреслити, що йдеться саме про прийняту фіксовану довжину, термін “пакет” змінили на “чарунка” (cell).

Після прийняття рішення про використання пакетів постійної довжини необхідно було вибрати їх розмір. На вибір довжини чарунки вплинули такі основні фактори: ефективність використання пропускної спроможності цифрових трактів; затримки при заповненні пакета інформацією користувача (під час пакетування), в черзі, на депакетуванні, а також коливання цих затримок (джиттер); умови реалізації [ ].

Європейські вчені виступали за розмір чарунки 32 октети (32 × 8 двійкових розрядів) з метою усунення ехопригнічувачів при передачі мови, а вчені США і Японії запропонували чарунку розміром 64 октети для досягнення ефективнішого використання цифрових трактів. Був досягнутий компроміс, і довжина чарунки прийнята 53 октети.

Таблиця 6.3. *Перева ги та недоліки способів комутації*

Спосіб комутації	**Переваги**	**Недоліки**
Комутація каналів (КК)	1) не потребує ресурсів мережі для обробки повідомлень; 2) *затримка доставки повідомлень мінімальна* (вона дорівнює часу встановлення з'єднання *твз*).	1) неможливо зміни смуги пропускання каналу; 2) неможлива інтеграція в одній мережі видів служб з різними швидкостями передачі; 3) низьке використання смуги пропускання каналу
Коммутація пакетів (КП)	1) динамічна зміна швидкості передачі; 2) високе використання ресурсів мережі при пачечному трафіку.	1) затримка для пакетів з мовною інформацією може бути недопустимо великою; 2) висока складність протоколів канального і мережного рівнів; 3) велика залежність затримки повідомлень від навантаження, що поступає.
Швидка комутація каналів (ШКК)	1) можливість передачі пакетів даних в паузах мовного сигналу; 2) покращене використання смуги каналу при трафіку пачечного типу (Кп >1); 3) затримка доставки пакетів мала.	1) при перевантаженнях швидко ростуть втрати; 2) при перевантаженнях частина мовних відрізків втрачається; 3) після передачі кожного пакета (в паузах мовного обміну) необхідно відновлювати з'єднання між користувачами за час tвз ≤ 140 мс, щоб затримка «з кінця в кінець» не перевищувала 240 мс.
Швидка комутація пакетів (ШКП)	1) динамічна зміна швидкості передачі (смуги пропускання каналу); 2) мала ймовірність помилки; 3) простота протоколів ланки даних і мережевого рівнів в вузлах мережі; 4) мала величина затримки; 5) добре використання ресурсів мережі при пачечному трафіку; 6) гнучкість в умовах перевантаження.	1) втрата швидкості передачі із-за необхідності включення адреси в кожний пакет; 2) ускладнення комутаційних полів комутаторів.

6.11. Дейтаграмна передача та віртуальні з’єднання

У мережах з комутацією пакетів сьогодні застосовується два класи механізмів передачі пакетів:

- дейтаграмна передача;
- віртуальні канали.

Прикладами мереж, що реалізують дейтаграммний механізм передачі, є мережі Ethernet, IP і IPX. За допомогою віртуальних каналів передають дані мережі X.25, FRAME RELAY і ATM. Спочатку ми розглянемо базові принципи дейтаграмному підходу.

Дейтаграммний спосіб передачі даних заснований на тому, що всі передані пакети обробляються незалежно один від одного, пакет за пакетом. Належність пакета до певного потоку між двома кінцевими вузлами і двома додатками, що працюють на цих вузлах, ніяк не враховується.

Вибір наступного вузла - наприклад, комутатора Ethernet або маршрутизатора IP / IPX - відбувається тільки на основі адреси вузла призначення, що міститься в заголовку пакета. Рішення про те, якому вузлу передати пакет, що прийшов, приймається на основі таблиці, яка містить набір адрес призначення та адресну інформацію, однозначно визначальну наступний (транзитний або кінцевий) вузол. Такі таблиці мають різні назви - наприклад, для мереж Ethernet вони зазвичай називаються таблиці просування (forwarding table), а для мережевих протоколів, таких як IP і IPX, - таблицями маршрутизації (routing table). Далі для простоти будемо користуватися терміном "таблиця маршрутизації" в якості узагальненої назви такого роду таблиць, використовуваних для дейтаграмному передачі на підставі тільки адреси призначення кінцевого вузла.

У таблиці маршрутизації для одного і того ж адреси призначення може мати декілька записів, що вказують, відповідно, на різні адреси наступного маршрутизатора. Такий підхід використовується для підвищення продуктивності і надійності мережі. Деяка "розмитість" шляхів проходження пакетів з одним і тим же адресою призначення через мережу є прямим наслідком принципу незалежної обробки кожного пакета, властивого

дейтаграмним протоколів. Пакети, наступні по одному і тому ж адресою призначення, можуть добиратися до нього різними шляхами і внаслідок зміни стану мережі, наприклад відмови проміжних маршрутизаторів.

Така особливість дейтаграмному механізму як розмитість шляхів прямування трафіку через мережу також у деяких випадках є недоліком. Наприклад, якщо пакетів певної сесії між двома кінцевими вузлами мережі необхідно забезпечити задану якість обслуговування. Сучасні методи підтримки QoS працюють ефективніше, коли трафік, якому потрібно забезпечити гарантії обслуговування, завжди проходить через одні й ті ж проміжні вузли.

Механізм віртуальних каналів (virtual circuit або virtual channel) створює у мережі стійкі шляху проходження трафіку через мережу зкомутацією пакетів. Цей механізм враховує існування в мережі потоків даних.

Якщо метою є прокладка для всіх пакетів потоку єдиного шляху через мережу, то необхідним (але не завжди єдиним) ознакою такого потоку повинна бути наявність для всіх його пакетів спільних точок входу і виходу з мережі. Саме для передачі таких потоків в мережі створюються віртуальні канали. Між двома кінцевими вузлами може бути прокладено кілька віртуальних каналів, як повністю збігаються щодо шляху прямування через транзитні вузли, так і відмінних.

Мережа тільки забезпечує можливість передачі трафіку вздовж віртуального каналу, а які саме потоки будуть передаватися по цих каналах, вирішують самі кінцеві вузли. Вузол може використовувати один і той же віртуальний канал для передачі всіх потоків, які мають спільні з даними віртуальним каналом кінцеві точки, або ж тільки частини з них. Наприклад, для потоку реального часу можна використовувати один віртуальний канал, а для трафіку електронної пошти - інший. В останньому випадку різні віртуальні канали будуть висувати різні вимоги до якості обслуговування, і задовольнити їх буде простіше, ніж у тому випадку, коли по одному віртуальному каналу передається трафік з різними вимогами до параметрів QoS.

Важливою особливістю мереж з віртуальними каналами є використання локальних адрес пакетів при ухваленні рішення про передачу. Замість досить довгого адреси вузла призначення (його довжина повинна дозволяти унікально ідентифікувати всі вузли і підмережі в мережі, наприклад технологія ATM оперує адресами довжиною в 20 байт) застосовується локальна, тобто змінюється від вузла до вузла, мітка, якої позначаються всі пакети, що переміщуються по певному віртуальному каналу. Ця позначка в різних технологіях називається по-різному: в технології X.25 - номер логічного каналу (Logical Channel number, LCN), в технології frame relay - ідентифікатор з'єднання рівня каналу даних (Data Link Connection Identifier, DLCI), в технології ATM - ідентифікатор віртуального каналу (Virual Channel Identifier, VCI). Однак призначення її скрізь однаково - проміжний вузол, званий в цих технологіях комутатором, читає значення мітки із заголовка пакету, що прийшов і переглядає свою таблицю комутації, в якій вказується, на який вихідний порт потрібно передати пакет. Таблиця комутації містить записи тільки про що проходять через даний комутатор віртуальних каналах, а не про всі наявні в мережі вузлах (або підмережах, якщо застосовується ієрархічний спосіб адресації). Зазвичай у великій мережі кількість прокладених через вузол віртуальних каналів істотно меншою за кількість вузлів і підмереж, тому за розмірами таблиця комутації набагато менше таблиці маршрутизації, а, отже, перегляд займає набагато менше часу і не вимагає від комутатора великої обчислювальної потужності.

Ідентифікатор віртуального каналу (саме таку назву мітки буде використовуватися далі) також набагато коротше адреси кінцевого вузла (з тієї ж причини), тому і надмірність заголовка пакету, який тепер не містить довгого адреси, а переносить по мережі тільки ідентифікатор, істотно менше.

Контрольні питання до розділу

1. Переваги комутації каналів:

a. *низький і постійний рівень затримки передачі даних через мережу*
b. *постійна і відома швидкість передачі даних за встановленим між кінцевими вузлами каналу;*
c. *можливість динамічно перерозподіляти пропускну здатність фізичних каналів зв'язку між абонентами відповідно до реальних потреб їхнього трафіку*

2. Переваги комутації пакетів:
   a. *низький і постійний рівень затримки передачі даних через мережу*
   b. *постійна і відома швидкість передачі даних за встановленим між кінцевими вузлами каналу;*
   c. *можливість динамічно перерозподіляти пропускну здатність фізичних каналів зв'язку між абонентами відповідно до реальних потреб їхнього трафіку;*
   d. *висока загальна пропускна здатність мережі при передачі пульсуючого трафіка;*
   e. *адреса використовується тільки на етапі встановлення з'єднання*
   f. *ж) адреса передається з кожним пакетом*
3. У мережах з динамічною комутацією:
   a. *дозволяється встановлювати з'єднання з ініціативи користувача мережі;*
   b. *з'єднання встановлюється не користувачами, а персоналом, який обслуговує мережу;*
   c. *в загальному випадку користувач мережі може з'єднатися з будь-яким іншим користувачем мережі;*
   d. *дозволяє парі користувачів замовити з'єднання на тривалий період часу;*
   e. *час з'єднання між парою користувачів при динамічній комутації складає від декількох секунд до декількох годин і завершується після виконання певної роботи - передачі файлу, перегляду сторінки тексту або зображення і т.п.*
4. У мережах з постійною комутацією:
   a. *дозволяється встановлювати з'єднання з ініціативи користувача мережі;*
   b. *з'єднання встановлюється не користувачами, а персоналом, який обслуговує мережу;*
   c. *комутація виконується тільки на час сеансу зв'язку, а потім (за ініціативою одного з користувачів) розривається;*
   d. *дозволяє парі користувачів замовити з'єднання на тривалий період часу;*
   e. *час з'єднання між парою користувачів при динамічній комутації складає від декількох секунд до декількох годин і завершується після виконання певної роботи - передачі файлу, перегляду сторінки тексту або зображення і т.п.*

5. Комутація каналів. Особливості, переваги та недоліки.
6. Комутація пакетів. Особливості, переваги та недоліки.
7. Які затримки в джерелі передачі виникають в мережі при комутації пакетів?
8. Які затримки в кожному комутаторі виникають в мережі при комутації пакетів?
9. Комутація повідомлень. Особливості, переваги та недоліки.
10. Які існують відмінності пр порівняння комутації каналів і пакетів?
11. Які особливості мереж з *динамічною* комутацією?
12. Які особливості мереж з *постійною* комутацією?
13. Швидка комутація каналів. Переваги та недоліки.
14. Швидка комутація пакетів. Переваги та недоліки.
15. Назвіть особливості дейтаграмної передачі в мережах з комутацією пакетів?
16. Назвіть особливості побудови віртуальних каналів в мережах з комутацією пакетів?

Список рекомендованої літератури

1. *Бертсекас Д., Галлагер Р.* Сети передачи данных. – М.: Мир, 1989. – 544 с.
2. *Назаров А. Н., Симонов М. В.* АТМ: Технология высокоскоростных сетей М.: Эко-Тредз, 1998. – 234 с.
3. *Кривуца В.Г., Беркман Л.Н., Стеклов В.К.* Сучасні цифрові системи комутації – [Підручник]. К. : Техніка, 2010. – 389 с.
4. *Кривуца В.Г., Беркман Л. Н., Лапінський В.В.* Основи інфокомунікацій: навч. посібник для загальноосвіт. навч. закладів - К.: ДУІКТ, 2011.- 276 с.
5. *Гольдштейн А.Б., Гольдштейн Б.С.* Softswitch. – СПб.: БХВ - Санкт-Петербург, 2006.-368 с.
6. *Кеннеди Кларк, Кевин Гамильтон* Принципы коммутации в локальных сетях Cisco. – М.: Вильямс, 2003.
7. *Стеклов В.К., Беркман Л.Н.* Нові інформаційні технології: транспортні мережі телекомунікацій. – К.: Техніка, 2004. – 488 с.
8. *Блэк Ю.* Сети ЭВМ: протоколы стандарты, интерфейсы / Перев. с англ. – М.: Мир, 1990.

Розділ 7. МАРШРУТИЗАЦІЯ В МЕРЕЖАХ

7.1. Огляд процесу маршрутизації

У загальнодоступному значенні слова маршрутизація означає пересування інформації від джерела до пункту призначення через об'єднану мережу.

При цьому, як правило, на шляху зустрічається принаймні один вузол. Маршрутизація часто протиставляється об'єднання мереж за допомогою моста, яке, в популярному розумінні цього способу, виконує точно такі ж функції.

Основна відмінність між ними полягає в тому, що об'єднання з допомогою моста має місце на Рівні 2 еталонної моделі OSI, в той час як маршрутизація зустрічається на Рівні 3.

Цією різницею пояснюється те, що маршрутизація і об'єднання за мостовою схемою використовують різну інформацію в процесі її переміщення від джерела до місця призначення.

Маршрутизація включає в себе два основних компоненти:

- визначення оптимальних трактів маршрутизації;
- транспортування інформаційних груп (зазвичай званих пакетами) через об'єднану мережу.

Останній з цих двох компонентів часто називається ***комутацією***.

Комутація відносно проста. З іншого боку, визначення маршруту може бути дуже складним процесом.

Визначення маршруту може базуватися на різних показниках (величинах, результуючих з алгоритмічних обчислень по окремої змінної - наприклад, довжина маршруту) або комбінаціях показників.

Програмні реалізації алгоритмів маршрутизації вираховують показники маршруту для визначення оптимальних маршрутів до пункту призначення.

Для полегшення процесу визначення маршруту, алгоритми маршрутизації ініціалізують і підтримують таблиці маршрутизації, в яких міститься маршрутна інформація.

Маршрутна інформація змінюється в залежності від використовуваного алгоритму маршрутизації.

Алгоритми маршрутизації заповнюють маршрутні таблиці безліччю інформації. Асоціації "Пункт призначення / наступне пересилання" повідомляють роутеру, що певний пункт призначення може бути оптимально досягнутим шляхом відправлення пакета в певний роутер, що представляє "наступне пересилання" на шляху до кінцевого пункту призначення [1].

При прийомі коли надходить пакет, роутер перевіряє адресу пункту призначення і намагається асоціювати цю адресу з наступним пересиланням.

To reach network:	Send to:
27	Node A
57	Node B
17	Node C
24	Node A
52	Node A
16	Node B
26	Node A
.	.
.	.
.	.

Рис. 7.1. Приклад маршрутної таблиці "місце призначення / наступне пересилання"

У маршрутних таблицях може міститися також і інша інформація. "Показники" забезпечують інформацію про бажаність якого-небудь каналу або тракту. Роутери порівнюють показники, щоб визначити оптимальні маршрути. Показники відрізняються один від одного в залежності від використаної схеми алгоритму маршрутизації.

Роутери зв’язуються один з одним (і підтримують свої маршрутні таблиці) шляхом передачі різних повідомлень.

Одним з видів таких повідомлень є повідомлення про "відновлення маршрутизації".

Відновлення маршрутизації зазвичай включають всю маршрутну таблицю або її частину. Аналізуючи інформацію про відновлення маршрутизації, що надходить від усіх роутерів, будь-який з них може побудувати детальну картину топології мережі. Іншим прикладом повідомлень, якими обмінюються роутери, є "оголошення про стан каналу" [1].

Оголошення про стан каналу інформує інші роутери про стан каналів відправника. Канальна інформація також може бути використана для побудови повної картини топології мережі. Після того, як топологія мережі стає зрозумілою, роутери можуть визначити оптимальні маршрути до пунктів призначення.

7.2. Алгоритми маршрутизації

Алгоритми маршрутизації можна диференціювати, ґрунтуючись на декількох ключових характеристиках.

По-перше, на роботу результуючого протоколу маршрутизації впливають конкретні завдання, які вирішує розробник алгоритму.

По-друге, існують різні типи алгоритмів маршрутизації, і кожен з них по-різному впливає на мережу і ресурси маршрутизації.

Алгоритми маршрутизації використовують різноманітні показники, які впливають на розрахунок оптимальних маршрутів.

При розробці алгоритмів маршрутизації часто переслідують одну або декілька з перерахованих нижче цілей [2]:

1. Оптимальність
2. Простота і низькі непродуктивні витрати
3. Живучість і стабільність
4. Швидка збіжність
5. Гнучкість

Оптимальність

Оптимальність, ймовірно, є найбільш загальною метою розробки. Вона характеризує здатність алгоритму маршрутізації вибирати «найкращий маршрут».

Найкращий маршрут залежить від показників і від «ваги» цих показників, використовуваних при проведенні розрахунку.

Наприклад, алгоритм маршрутизації міг би використовувати кілька пересилань з певною затримкою, але при розрахунку «вага» затримки може бути їм оцінений як дуже значна.

Природно, що протоколи маршрутизації повинні строго визначати свої алгоритми розрахунку показників

Простота і низькі непродуктивні витрати

Алгоритми маршрутизації розробляються як можна більш простими.

Алгоритм маршрутизації повинен ефективно забезпечувати свої функціональні можливості, з мінімальними витратами програмного забезпечення і коефіцієнтом використання.

Особливо важлива ефективність у тому випадку, коли програма, що реалізує алгоритм маршрутизації, повинна працювати в комп'ютері з обмеженими фізичними ресурсами.

Живучість і стабільність

Алгоритми маршрутизації повинні мати живучість. Вони повинні чітко функціонувати в разі неординарних або непередбачених обставин, таких як відмови апаратури, умови високого навантаження і некоректні реалізації.

Оскільки роутери розташовані в вузлових точках мережі, їх відмова може викликати значні проблеми.

Часто найкращими алгоритмами маршрутизації виявляються ті, які витримали випробування часом і довели свою надійність в різних умовах роботи мережі.

Швидка збіжність

Алгоритми маршрутизації повинні швидко сходитися. Збіжність - це процес угоди між усіма роутерами за оптимальними маршрутами.

Коли якась подія в мережі приводить до того, що маршрути або відкидаються, або стають доступними, роутери розсилають повідомлення про відновлення маршрутизації [2].

Повідомлення про відновлення маршрутизації пронизують мережі, стимулюючи перерахунок оптимальних маршрутів і, в кінцевому підсумку, змушуючи всі роутери дійти згоди по цих маршрутах.

Алгоритми маршрутизації, які сходяться повільно, можуть привести до утворення петель маршрутизації або виходів з ладу мережі.

Петля маршрутизації

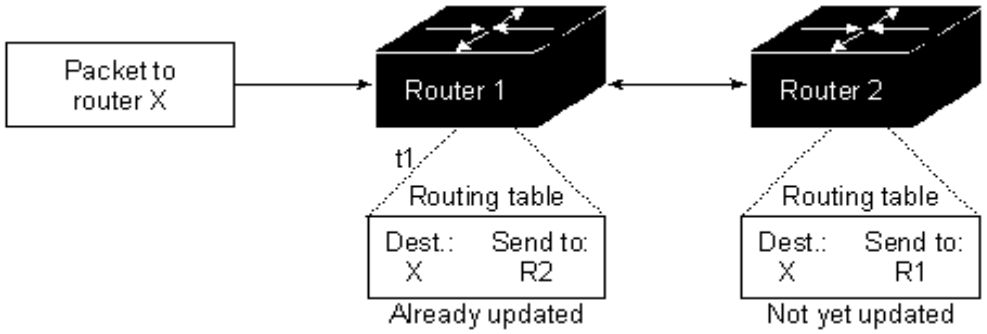


Рис. 7.2. Петля маршрутизації

В даному випадку, в момент часу *t1* до роутеру 1 прибуває пакет.

Роутер 1 уже був оновлений і тому він знає, що оптимальний маршрут до пункту призначення вимагає, щоб наступною зупинкою був роутер 2. Тому роутер 1 пересилає пакет в роутер 2.

Роутер 2 ще не був оновлений, тому він вважає, що наступного оптимальної пересилкою повинен бути роутер 1. Тому роутер 2 пересилає пакет назад в роутер 1.

Гнучкість

Алгоритми маршрутизації повинні бути також гнучкими. Алгоритми маршрутизації повинні швидко і точно адаптуватися до різноманітних обставин в мережі.

Наприклад, припустимо, що сегмент мережі відкинуто. Багато алгоритмів маршрутизації, після того як вони дізнаються про цю проблему, швидко вибирають наступний найкращий шлях для всіх маршрутів, які зазвичай використовують цей сегмент.

Алгоритми маршрутизації можуть бути запрограмовані таким чином, щоб вони могли адаптуватися до змін смуги пропускання мережі, розмірів черги до роутера, величини затримки мережі та інших змінних.

Типи алгоритмів маршрутизації

Алгоритми маршрутизації можуть бути класифіковані за типами. Наприклад, алгоритми можуть бути:

1. Статичними або динамічними.
2. Одномаршрутними або багатомаршрутними.
3. Однорівневими або ієрархічними.
4. З інтелектом у головній обчислювальній машині або в роутері.
5. Внутрідоменними і міждоменними.
6. Алгоритмами стану каналу або вектора відстаней.

Статичні або динамічні алгоритми

Статичні алгоритми маршрутизації взагалі навряд чи є алгоритмами.

Розподіл статичних таблиць маршрутизації встановлюється адміністратором мережі до початку маршрутизації. Воно не змінюється, якщо тільки адміністратор мережі не змінить його.

Алгоритми, що використовують статичні маршрути, прості для розробки і добре працюють в оточеннях, де трафік мережі відносно передбачуваний, а схема мережі відносно проста.

Оскільки статичні системи маршрутизації не можуть реагувати на зміни в мережі, вони, як правило, вважаються непридатними для сучасних великих мереж,

які постійно змінюються. Більшість домінуючих алгоритмів маршрутизації 1990рр. – динамічні.

Одномаршрутні або багатомаршрутні алгоритми

Деякі складні протоколи маршрутизації забезпечують безліч маршрутів до одного і того ж пункту призначення. Такі багатомаршрутному алгоритми уможливлюють мультиплексную передачу трафіку по численних лініях. Одномаршрутні алгоритми не можуть робити цього..Переваги багатомаршрутному алгоритмів очевидні - вони можуть забезпечити значно більшу пропускну здатність і надійність.

Однорівневі або ієрархічні алгоритми

Деякі алгоритми маршрутизації оперують в плоскому просторі, в той час як інші використовують ієрархії маршрутизації.

У однорівневої системи маршрутизації всі роутери рівні по відношенню один до одного.

В ієрархічній системі маршрутизації деякі роутери формують те, що становить основу (backbone - базу) маршрутизації.

Пакети з небазових роутерів переміщаються до базових роутерів і пропускаються через них до тих пір, поки не досягнуть загальної області пункту призначення [2].

Починаючи з цього моменту, вони переміщаються від останнього базового роутера через один або кілька небазових роутерів до кінцевого пункту призначення.

Системи маршрутизації часто встановлюють логічні групи вузлів, які називають доменами, або автономними системами (AS), або областями.

В ієрархічних системах одні роутери будь-якого домену можуть повідомлятися з роутерами інших доменів, в той час як інші роутери цього домену можуть підтримувати зв'язок з роутерами тільки в межах свого домену. У дуже

великих мережах можуть існувати додаткові ієрархічні рівні. Роутери найвищого ієрархічного рівня утворюють базу маршрутизації

Основною перевагою ієрархічної маршрутизації є те, що вона імітує організацію більшості компаній і отже, дуже добре підтримує їх схеми трафіку

Велика частина мережевої зв'язку має місце в межах груп невеликих компаній (доменів). Внутрішньодоменним роутерам необхідно знати тільки про інші роутери в межах свого домену, тому їх алгоритми маршрутизації можуть бути спрощеними. Відповідно може бути зменшений і трафік оновлення маршрутизації, що залежить від алгоритму маршрутизації, що використовується.

Алгоритми з інтелектом у головній обчислювальній машині або в роутері

Деякі алгоритми маршрутизації припускають, що кінцевий вузол джерела визначає весь маршрут. Зазвичай це називають маршрутизацією від джерела.

У системах маршрутизації від джерела роутери діють просто як пристрої зберігання та пересилання пакета, без всяких роздумів відсилаючи його до наступної зупинки.

Інші алгоритми припускають, що головні обчислювальні машини нічого не знають про маршрутах. При використанні цих алгоритмів роутери визначають маршрут через об'єднану мережу, базуючись на своїх власних розрахунках.

У першій системі, інтелект маршрутизації знаходиться в головній обчислювальній машині. В системі, розглянутої в другому випадку, інтелектом маршрутизації наділені роутери.

Компроміс між маршрутизацією з інтелектом у головній обчислювальній машині і маршрутизацією з інтелектом у роутері досягається шляхом зіставлення оптимальності маршруту з непродуктивними витратами трафіку.

Системи з інтелектом у головній обчислювальній машині частіше вибирають найкращі маршрути, тому що вони, як правило, знаходять всі можливі маршрути до пункту призначення, перш ніж пакет буде дійсно відісланий [2].

Потім вони вибирають найкращий маршрут, грунтуючись на визначенні оптимальності даної конкретної системи. Однак акт визначення всіх маршрутів часто вимагає значного трафіку пошуку і великого обсягу часу.

Внутрішньодоменні або міждоменні алгоритми

Деякі алгоритми маршрутизації діють тільки в межах доменів; інші - як в межах доменів, так і між ними. Природа цих двох типів алгоритмів різна.

Тому зрозуміло, що оптимальний алгоритм внутрішньодоменної маршрутизації не обов'язково буде оптимальним алгоритмом міждоменної маршрутизації.

Алгоритми стану каналу або вектора відстані

Алгоритми стану каналу (відомі також як алгоритми "першочерговості найкоротшого маршруту") направляють потоки маршрутної інформації в усі вузли об'єднаної мережі.

Однак кожен роутер посилає тільки ту частину маршрутної таблиці, яка описує стан його власних каналів.

Алгоритми вектора відстані (відомі також як алгоритми Белмана-Форда) вимагають від каждого роутера посилки всієї або частини своєї маршрутної таблиці, але тільки своїм сусідам.

Алгоритми стану каналів фактично направляють невеликі коректування в усіх напрямках, в той час як алгоритми вектора відстаней відсилають більш великі коректування тільки в сусідні роутери.

Відрізняючись більш швидкої збіжністю, алгоритми стану каналів трохи менше схильні до утворення петель маршрутизації, ніж алгоритми вектора відстан.і

З іншого боку, алгоритми стану каналу характеризуються більш складними розрахунками в порівнянні з алгоритмами вектора відстаней, вимагаючи більшої процесорної потужності та пам'яті, ніж алгоритми вектора відстаней.

Внаслідок цього, реалізація та підтримка алгоритмів стану каналу може бути більш дорогою.

Незважаючи на їх відмінності, обидва типи алгоритмів добре функціонують при самих різних обставинах.

7.3. Показники алгоритмів (метрики)

Маршрутні таблиці містять інформацію, яку використовують програми комутації для вибору найкращого маршруту

В алгоритмах маршрутизації використовується багато різних показників. Складні алгоритми маршрутизації при виборі маршруту можуть базуватися на безлічі показників, комбінуючи їх таким чином, що в результаті виходить один окремий (гібридний) показник

Показники, які використовуються в алгоритмах маршрутизації [2]:

1. Довжина маршруту
2. Надійність
3. Затримка
4. Ширина смуги пропускання
5. Навантаження
6. Вартість зв'язку

Довжина маршруту

Довжина маршруту є найбільш загальним показником маршрутизації.

Деякі протоколи маршрутизації дозволяють адміністраторам мережі призначати довільні ціни на кожен канал мережі. В цьому випадку довжиною тракту є сума витрат, пов'язаних з кожним каналом, який був траверсированій.

Інші протоколи маршрутизації визначають "кількість пересилань", тобто показник, що характеризує число проходів, які пакет повинен зробити на шляху від джерела до пункту призначення через вироби об'єднання мереж (такі як роутери).

Надійність

Надійність, в контексті алгоритмів маршрутизації, відноситься до надійності кожного каналу мережі (зазвичай описуваної в термінах співвідношення біт / помилка).

Деякі канали мережі можуть відмовляти частіше, ніж інші.

Відмови одних каналів мережі можуть бути усунуті легше або швидше, ніж відмови інших каналів.

При призначенні оцінок надійності можуть бути прийняті до уваги будь-які фактори надійності.

Оцінки надійності звичайно призначаються каналам мережі адміністраторами мережі. Як правило, це довільні цифрові величини.

Затримка

Під затримкою маршрутизації звичайно розуміють відрізок часу, необхідний для пересування пакета від джерела до пункту призначення через об'єднану мережу.

Затримка залежить від багатьох факторів, включаючи смугу пропускання проміжних каналів мережі, черги в порт кожного роутера на шляху пересування пакета, перевантаженість мережі на всіх проміжних каналах мережі і фізична відстань, на яке необхідно перемістити пакет.

Оскільки тут має місце конгломерація кількох важливих змінних, затримка є найбільш загальним і корисним показником.

Смуга пропускання

Смуга пропускання відноситься до наявної потужності трафика якого-небудь каналу

За інших рівних показниках, канал *Ethernet 10 Mbps* кращий будь орендованій лінії з пропускною здатністю 64 Кбайт / сек

Хоча смуга пропускання є оцінкою максимально досяжної пропускної здатності каналу, маршрути, що проходять через канали з більшою пропускною здатністю, не обов'язково будуть краще маршрутів, що проходять через менш швидкодіючі канали

Наприклад, якщо більш швидкодіючий канал майже весь час зайнятий, то фактичний час, необхідне для відправки пакета в пункт призначення, для цього швидкодіючого каналу може виявитися більше.

Навантаження

Навантаження відноситься до ступеня зайнятості будь-якого джерела мережі (такого, як роутер).

Навантаження може бути обчислено різноманітними способами, в тому числі за коефіцієнтом використання головного процесора і числа пакетів, оброблених в секунду.

Постійний контроль цих параметрів може привести до інтенсивного витрачання ресурсів.

Вартість зв'язку

Іншим важливим показником є вартість зв'язку.

Деякі компанії цікавить не стільки ефективність, скільки операційні витрати.

Навіть якщо затримка в їх лінії може бути великою, вони відправлять пакети через свої власні лінії, а не через лінії загального користування, тому що їм доведеться платити за використаний час.

Routed protocol - це протокол, відправлений за певним маршрутом через об'єднану мережу. Прикладами таких протоколів є ***Internet Protocol (IP), DECnet*** і ***Apple Talk.***

Routing protocol - це протокол, який реалізує алгоритм маршрутизації, тобто , вони відправляють протоколи за певним маршрутом через об'єднану мережу. Прикладами таких протоколів можуть бути:

1.Interior Gateway Routing Protocol (IGRP)

2.Open Shortest Path First (OSPF)

3. Intermediate System to Intermediate System (IS-IS)

4. Routing Information Protocol (RIP)

7.4. Призначення та класифікація протоколів маршрутизації

Протоколи маршрутизації призначені для автоматичної побудови *таблиць маршрутизації (ТМ),* на основі яких виконується переміщення пакетів.

Такі таблиці містять дані яких достатньо для прийняття рішення для пересилання будь-якого пакета, що надійшов до маршрутизатора.

Вміст таблиці залежить від технології складеної мережі. Як правило обирається "*найкоротший*" маршрут (під довжиною маршруту розуміють його ***метрику*** *– числове значення, яке впливає на вибір маршруту: чим менша метрика – тим краще)* [3].

Метрика може визначатись, наприклад, кількістю проміжних вузлів, пропускною здатністю, часом затримки, надійністю каналів між маршрутизаторами).

Усі способи маршрутизації можна поділити на 2 великі групи: *без таблиць* та *з ТМ*.

Маршрутизація без таблиць поділяється на:

- лавинну;
- керовану подіями;
- від джерела.

Лавинна маршрутизація - це найпростіший спосіб передавання, який передбачає, що кожен маршрутизатор відправляє пакет усім своїм сусідам, крім того, від кого він отримав свій пакет. Пропускна здатність мережі в такому випадку використовується дуже неефективно.

Маршрутизація, керована подіями передбачає, що пакет до певної мережі призначення надсилається за маршрутом, який вже приводив до успіху. В такому випадку необхідно, щоб маршрутизатор-відправник міг фіксувати факт успіху доставки пакета.

Маршрутизація від джерела передбачає, що відправник розміщує у пакет інформацію про те, які проміжні маршрутизатори повинні брати участь у передаванні пакетів. Таку інформацію або надає адміністратор вручну, або вузол-відправник формує автоматично.

Маршрутизація на основі таблиць в свою чергу поділяється на *статичну і динамічну (адаптивну).*

Статична маршрутизація передбачає ручне прописування маршрутів адміністратором. Така маршрутизація при зміні структури мережі потребує ручного змінення маршрутів.

У випадку ***динамічної маршрутизації*** мережі можуть оновлювати свої ТМ та швидко адаптуватися до змін топології та стану з'єднань.

Успішне функціонування цього виду маршрутизації залежить від виконання маршрутизатором двох його основних функцій: підтримки ТМ в актуальному стані та своєчасного розповсюдження інформації у вигляді анонсів та оновлень маршрутів серед інших маршрутизаторів.

При розповсюдженні інформації про мережу, механізм динамічної маршрутизації використовує один із протоколів маршрутизації. Такий протокол визначає набір правил, що використовуються маршрутизатором при здійсненні зв'язку із сусідніми маршрутизаторами [3].

Протокол маршрутизації визначає: яким чином розсилаються оновлення маршрутів; яка інформація міститься в оновленнях; як часто розсилаються оновлення; яким чином виконується пошук отримувачів оновлень.

Кожен із алгоритмів маршрутизації використовує свій власний спосіб вибору найкращого шляху. Для цього він генерує певне значення, що називається метрикою для кожного маршруту у мережі. Зазвичай чим менше значення метрики, тим кращим вважається маршрут .

Метрики обчислюються на основі одного або більше параметрів:

- **смуга пропускання** – описує пропускну здатність каналу;
- **затримка** – час, який потрібен пакета для проходження по каналу від відправника до отримувача;
- **навантаження** – ступінь використання мережевих ресурсів на маршрутизаторі чи каналі;
- **надійність** характеризує рівень помилок у мереженому каналі;
- **кількість переходів** – число маршрутизаторів, через які повинен пройти пакет перед надходженням до пункту призначення;
- **вартість** – довільне значення, розраховується на основі ширини смуги пропускання, фінансових затрат або інших характеристик, які обирає мережевий адміністратор.

Отже, ***протокол маршрутизації*** – засіб комунікації між маршрутизаторами, яке дозволяє пристроям сумісно використовувати інформацію про мережі та визначати відстань до різних вузлів та мереж. Інформація, яку один маршрутизатор отримує від другого (шляхом протоколу маршрутизації), використовується для побудови та підтримки в актуальному стані ТМ.

Більшість алгоритмів маршрутизації може бути віднесено до однієї із двох категорій:

• дистанційно-векторний протокол (ДВП);

• протокол з врахуванням стану каналу (ПСК).

Дистанційно-векторний протокол визначає напрям або вектор та відстань до потрібного вузла об’єднаної мережі. Прикладами таких протоколів є *RIP, IGRP, EIGRP, BGP*. Деякий час протокол *EIGRP* вважався гібридним протоколом, оскільки поєднує у собі особливості обох алгоритмів: дистанційно-векторного та з врахуванням стану каналу, але на сьогоднішній день фірма *Cisco* відносить його до *ДВП.* Він має набагато кращі характеристики, ніж класичні *ДВП*.

Протокол з врахуванням стану каналу, який також ще називають алгоритмом вибору найкоротшого шляху (*shortest path first – SPF*), відтворює топологію усієї мережі. Приклади: *OSPF, IS-IS, NLSP*.

7.4.1. Принцип роботи дистанційно-векторних протоколів

При використанні дистанційно-векторних алгоритмів між маршрутизаторами періодично пересилаються копії таблиць маршрутизації. В таких регулярних оновленнях маршрутизатори повідомляють один одного про зміни у топології мережі. Дистанційно-векторні алгоритми маршрутизації також називаються ще алгоритмами *Беллмана-Форда* (кожен маршрутизатор отримує *ТМ* від сусідніх маршрутизаторів).

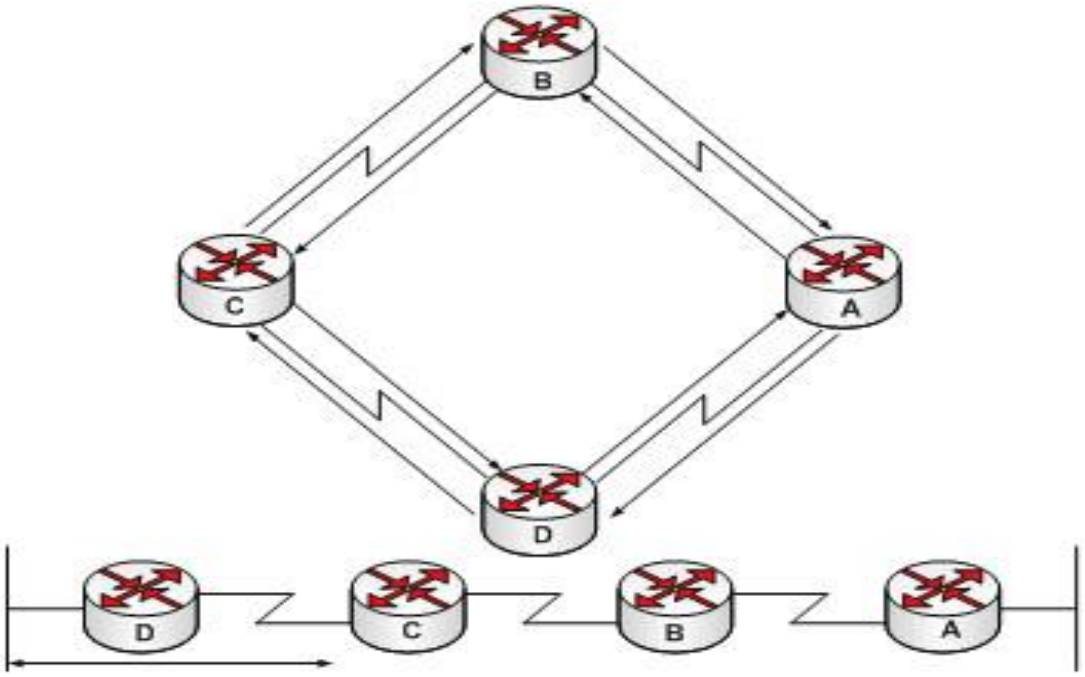


Рис. 7.3. Концепція дистанційно-векторної маршрутизації

Маршрутизатор **Б** отримує таблицю від маршрутизатора **А**. Маршрутизатор додає значення вектора відстані, кількість переходів, що збільшує результуючий вектор відстані. Після цього маршрутизатор **Б** передає свою нову таблицю маршрутизації своєму сусіду маршрутизатору В. Такий покроковий процес відбувається на всіх сусідніх маршрутизаторах.

В дистанційно-векторному алгоритмі накопичуються відстані в мережі, що дозволяє підтримувати базу даних *(БД),* яка містить інформацію про топологію мережі.

Однак дистанційно-векторні алгоритми не надають маршрутизаторам точну топологію всієї мережі, оскільки кожному маршрутизатору відомі лише сусідні (прилеглі) маршрутизатори.

Кожен маршрутизатор, що використовує дистанційно-векторну маршрутизацію, починає свою роботу з визначення сусідніх маршрутизаторів. Для кожного інтерфейсу безпосередньо під'єднаної мережі, вектор відстані встановлюється нульовим. В процесі розрахунку вектора відстані, маршрутизатори знаходять найкращий маршрут до сусідів-отримувачів на основі інформації, отриманої від сусідів [4].

Наприклад, маршрутизатор **А** взнає про інші мережі на основі інформації, яку він отримує від маршрутизатора **Б**. В кожній із позицій ТМ є сумарний вектор відстані, який показує, на якій відстані знаходиться відповідна віддалена мережа

Оновлення ТМ відбувається при зміні топології мережі. В міру формування векторів відстані зміни топології заносяться в ТМ наступних маршрутизаторів. Дистанційно-векторні алгоритми потребують, щоб кожен маршрутизатор пересилав всю ТМ кожному із своїх сусідів.

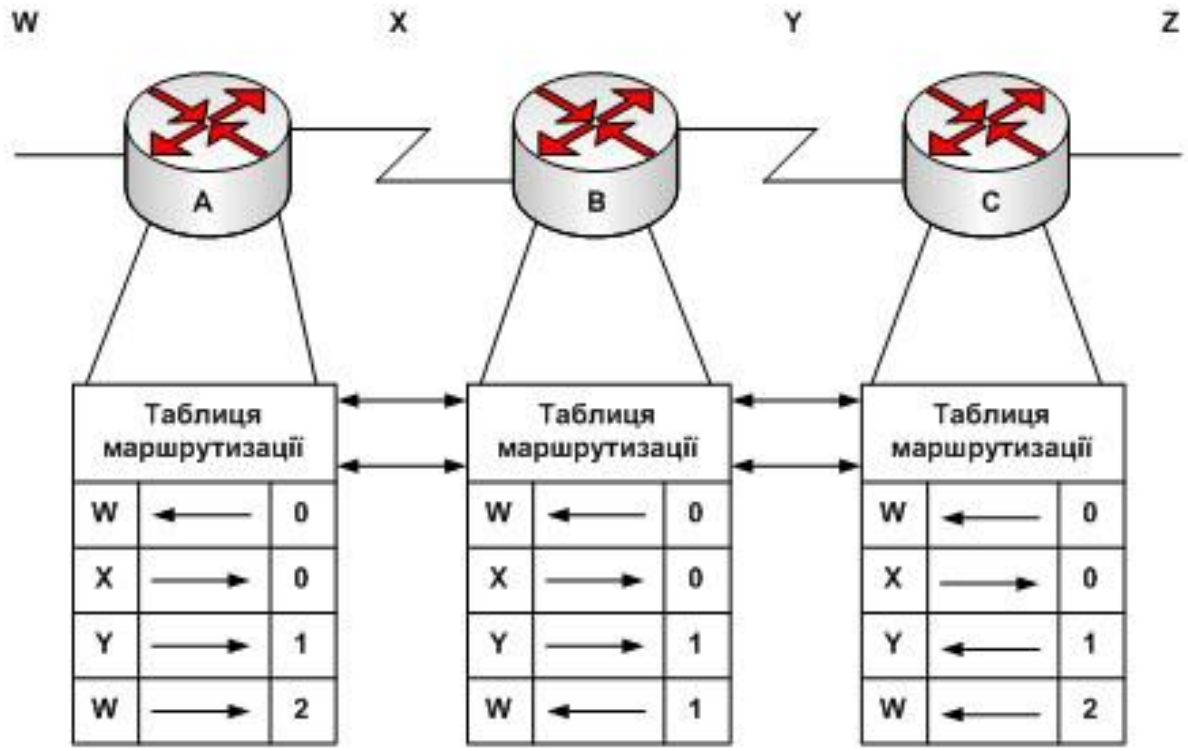


Рис. 7.4. Процес побудови структури мережі в дистанційно-векторному протоколі маршрутизації

Вектор відстані можна порівняти з дорожними знаками на шосе. Ці знаки вказують напрям до пункту призначення та відстань до нього. Далі по цьому ж шосе можуть зустрічатися знаки, що вказують той самий напрям, однак, відстань вказувати вони будуть меншу. Зменшення цієї відстані при русі свідчить про правильний напрям руху.

7.4.2. Алгоритм вибору маршруту за станом каналу

Другим базовим алгоритмом маршрутизації є алгоритм вибору маршруту за станом каналу. Такі алгоритми відомі, як алгоритми Дейкстри або алгоритми вибору найкоротшого шляху (*Shortest Path First*). Вони підтримують складну базу топологічної інформації. Тоді як дистанційно-векторні алгоритми не містять певної інформації про віддалені мережі та маршрутизатори, алгоритми з використанням стану каналу підтримують повну інформацію про віддалені маршрутизатори та їх з'єднання. Під час маршрутизації за станом каналу використовуються:

- **анонси стану каналу** – *(Link-State Advertisement LSA).* Це невеликі пакети, що містять інформацію про маршрути, що розсилаються між маршрутизаторами;
- **топологічна база даних** *(Topological Database).* Ця база містить інформацію, отриману в повідомленнях LSA;
- **алгоритм вибору найкоротшого шляху** *(Shortest Path First).* Відповідний алгоритм здійснює обчислення над базою даних, результатом якого є побудова зв'язного дерева протоколу SPF;
- **таблиця маршрутизації** *(Routing Table).* Ця таблиця містить відомі маршрути та відповідні їм інтерфейси.

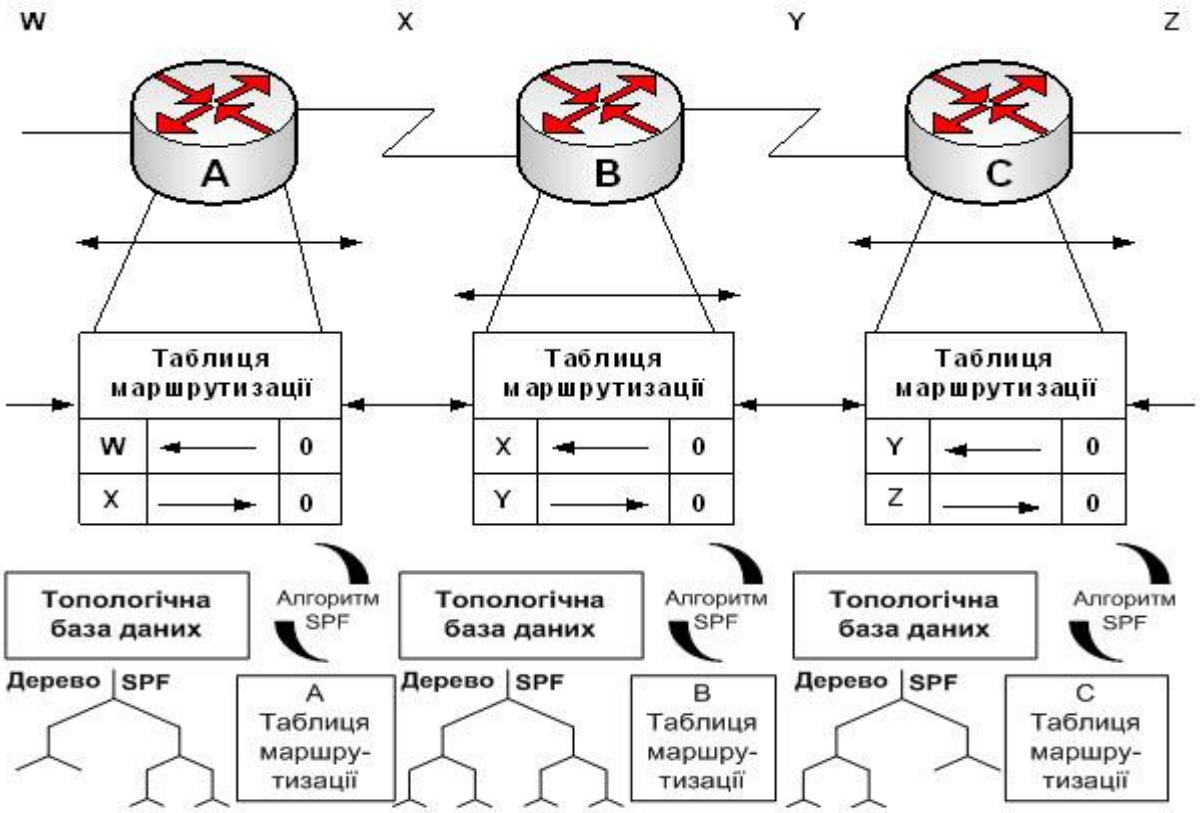


Рис. 7.5. Алгоритм вибору маршруту за станом каналу

Маршрутизатори обмінюються повідомленнями *LSA*, починаючи з безпосередньо під'єднаних мереж. Кожен маршрутизатор паралельно з іншими створює топологічну *БД,* яка складається з інформації, що отримана з цих повідомлень. Якщо маршрутизатор взнає про зміну стану каналу, він розсилає цю інформацію всім іншим маршрутизаторам об'єднаної мережі, щоб вони могли її використовувати для маршрутизації.

В одній мережі можуть одночасно бути кілька різних протоколів маршрутизації. Оскільки інформація про мережу може надійти від кількох протоколів і містити різні раціональні маршрути – встановлюють пріоритети протоколів маршрутизації. Зазвичай перевагу надають *LSA* протоколам, оскільки вони мають повнішу інформацію [3].

За замовчуванням кожен протокол маршрутизації на певному маршрутизаторі розповсюджує лише ту інформацію, котра була отримана маршрутизатором цим же протоколом. Оскільки не завжди кожен маршрутизатор

підтримує усі протоколи для даної мережі, то застосовують внутрішній особливий режим роботи маршрутизатора, який називають *перерозподілом (Redistribute).*

Зі зростанням мереж проблема взаємодії маршрутизаторів дуже зростає і для її розв'язання було знайдено інший підхід – *поділ мережі на автономні системи. Internet* це всесвітня система добровільно об'єднаних *КМ*, побудована на використанні протоколу *IP* та маршрутизації пакетів.

З самого початку *Internet* будувалась як мережа, що об'єднувала велику кількість існуючих систем. В її структурі визначають ***магістральну мережу*** *(core backbone network)*, а мережі, під'єднані до магістралі, розглядаються як ***автономні системи*** *(autonomous systems, AS)*.

Автономна система (АС) – це сукупність мереж, які знаходяться під єдиним адміністративним керуванням і в яких використовується єдина стратегія і правила маршрутизації. *АС* для зовнішніх мереж є єдиним об'єктом.

Кожна *АС* повинна мати свій власний унікальний номер *(Autonomous System Number – ASN).* Номери виділяються організацією *Internet Assigned Numbers Authority (IANA),* яка також виділяє IP-адреси регіональним інтернет-реєстраторам *(Regional Internet Registry, RIR)* блоками. Локальні *RIR* після цього присвоюють організаціям номер *АС* з блоку, отриманого від *IANA*. Організації, що бажають отримати *ASN*, повинні пройти процес реєстрації в своєму локальному *RIR* та отримати схвалення.

Шлюзи, що використовуються для утворення мереж та підмереж всередині автономної системи, називають *внутрішніми шлюзами (interior gateways),* а шлюзи за допомогою яких автономні системи під'єднуються до магістралі мережі, відповідно називають *зовнішніми шлюзами (exterior gateways)*. Сама магістраль також є *АС*. Згідно з цими визначеннями *протоколи маршрутизації* також поділяють на два види: *протокол внутрішнього та протокол зовнішнього шлюзу.*

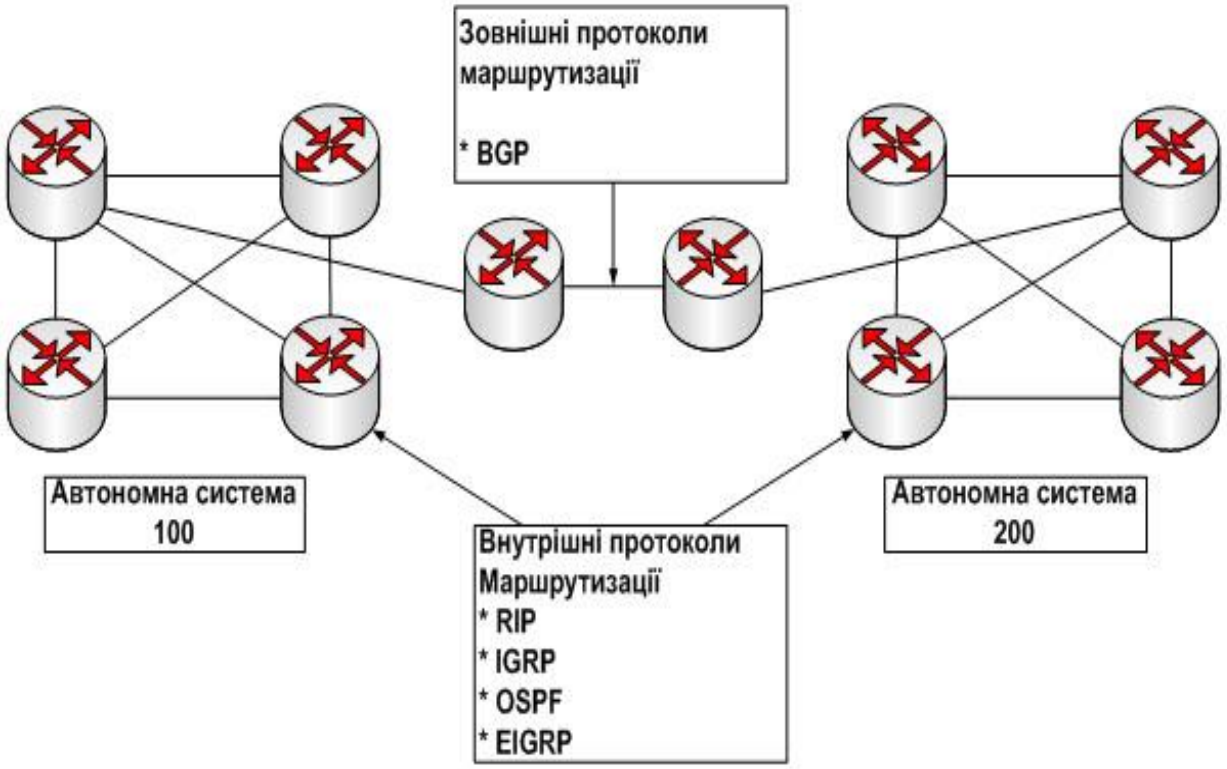


Рис. 7.6. Види протоколів маршрутизації

Протокол внутрішнього шлюзу *(interior gateway protocol, IGP*) призначений для використання у мережі, що керується або адмініструється окремою організацією. Такий протокол служить для знаходження найкращого маршруту в одній мережі. Іншими словами, метрика та характер її використання є найбільш важливими елементами протоколу IGP.

Протокол зовнішнього шлюзу *(exterior gateway protocol – EGP)* призначений для здійснення маршрутизації між мережами, що знаходяться під управлінням різних організацій. Як правило, ці протоколи використовуються при маршрутизації між провайдерами служб *Internet (Internet Service Providers, ISP)* або між окремою компанією та *Internet*-провайдером. Протокол ***EGP*** повинен ізолювати *АС*. Оскільки в кожній *АС* використовуються свої правила, в об’єднаній мережі повинен функціонувати загальний протокол, який дозволить здійснювати зв’язок між ними.

7.5. Порівняння статичної та динамічної маршрутизації

Статична маршрутизація має такі особливості:

- забезпечує підтримку *ТМ* для невеликих мереж, які не передбачено суттєво розширювати;
- забезпечує маршрутизацію для кінцевої (тупикової) мережі;
- задає єдиний маршрут за замовчуванням до будь-якої мережі, якщо ТМ не містить більш специфічного шляху.

Переваги статичної маршрутизації: мінімальне використання процесора; легша для розуміння адміністратора; легша для конфігурування.

Недоліки статичної маршрутизації : конфігурування та обслуговування потребує багато часу; під час конфігурування можливі помилки (особливо у великих мережах); для підтримки заміни маршрутної інформації потрібне втручання адміністратора; зі зростанням мережі погано масштабується; для належного виконання потребує повного знання усієї мережі.

Переваги динамічної маршрутизації:

- потребує меншого втручання адміністратора, при доданні або вилученні мереж;
- протоколи автоматично реагують на зміни топології;
- конфігурація менш схильна до помилок;
- більш масштабована, нарощування мережі зазвичай не породжує проблем.

Недоліки динамічної маршрутизації:

- використовуються ресурси маршрутизатора;
- потребує більших знань адміністратора для конфігурування, перевірки та усунення несправностей.

Таблиця 7. 1. *Порівняння статичної та динамічної маршрутизації*

Критерій порівняння	Статична маршрутизація	Динамічна маршрутизація
Складність конфігурування	Ускладнюється зі зростанням складності мережі	В загальному плані не залежить від складності мережі

Вимоги до знань адміністратора	Потрібен невисокий рівень знань	Потрібен більшиц рівень знань
Зміни топології	Потрібне адміністративне втручання	Автоматично адаптується під зміни
Маштабування	Підходить лише до простих топологій	Підходить і для складних і для простих топологій
Ступінь безпеки	Більш безпечна, ніж дінамічна маршрутизація	Не гарантує безпеки
Ступінь застосовування	Не потребує додаткових ресурсів	Застосовує процесор, оперативну пам’ять смугу пропускання
Передбачуваність	Маршрут завжди постійний	Маршрут залежить від поточної топології

Порівняння деяких протоколів динамічної маршрутизації

В дистанційно-векторних протоколах для знаходження найкрашого шляху використовується *алгоритм Беллмана-Форда*. Деякі *DVA* періодично розсилають сусідам повні *TM*, що може породжувати значний трафік. *DVA* не мають уявлення про топологію усієї мережі. Вони знають про віддалені мережі лише відстань до них і вихідний порт (або адресу наступного хопа).

Протоколи *DVA* працюють найкраще в ситуаціях, коли:

- мережа проста і не потребує спеціальної ієрархічної структури;
- адміністратори не мають достатньо знань щодо вибору конфігурації та підтримки *LSA*;
- використовуються специфічні типи мереж, наприклад, мережі типу *hub-and-spoke*;
- час конвергенції у найгіршому випадку для мережі непринципові.

В *LSA* для знаходження найкрашого шляху використовується алгоритм *Дейкстри*.

Маршрутизатори знають про всю комп’ютерну мережу шляхом збирання інформації від усіх маршрутизаторів [5].

Кожен маршрутизатор має повну топологічну карту комп’ютерної мережі.

Всі маршрутизатори комп’ютерної мережі використовують одну й ту ж топологічну карту. *LSA* не здійснюють періодичних оновлень.

Після конвергенції комп'ютерних мереж оновлення надсилаються лише у випадку змін її топології.

Протоколи *LSA* працюють найкраще в ситуаціях, коли:

- *КМ* велика та ієрархічна;
- адміністратор має достатньо знань;
- швидка конвергенція у *КМ* дуже актуальна.

Таблиця 7.2. *Порівняння традиційних дистанційно-векторних алгоритмів та EIRGP*

Традиційні DVA	**EIRGP**
Використовуть алгоритм Белмана-Форда або Форда-Фалкерсона	Використовує алгоритм дифузії поновлень маршрутизації (Difussijn Update Algorithm)
Використовуються періодичні оновлення і час життя записів ТМ	Не використовуються ні періодичні оновлення, ні час життя записів ТМ
Зберігає лише кращий маршрут до пунктів призначення	Підтримує топологічну таблицю (відмінну від ТМ)
Коли маршрут стає недійсним маршрутизатор повинен чекати до наступного оновлення	Коли маршрут стає недійсним DUAL використовує резервний шлях з топологічної таблиці
Повільна конвергенція завдяки використанню таймера holddown	Швидка конвергенція завдяки відсутності таймера holddown і системи кординування обчислення маршрутів

Таблиця 7.3. *Порівняння деяких протоколів динамічної маршрутизації*

Критерій	DVA				LSA	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Швидкість конвергенції	Повільна	Повільна	Повільна	Висока	Висока	Висока
Маштабованість (розмір мережі)	Мала	Мала	Мала	Велика	Велика	Велика
Підтримка VLSM	-	-	-	+	+	+
Ступінь використання ресурсів	Низька	Низька	Низька	Середня	Висока	Висока
Впровадження та підтримка	Проста	Проста	Проста	Складна	Складна	Складна

Порівняння протоколу OSPF з протоколом RIP

Порівняння протоколів *OSPF* і *RIP* не зовсім правомірно, оскільки ці два протоколи призначені для мережевого середовища абсолютно різних типів.

Протокол *OSPF* призначений для використання у великих, складних мережах, спроектованих на основі продуманого підходу.

Протокол *RIP* призначений для невеликих мереж, в яких застосування простого протоколу дозволяє спростити проектування і скоротити тривалість налаштування конфігурації. По суті, якщо мережа є достатньо невеликою для того, щоб в ній можна було застосовувати протокол *RIP*, то краще зупинитися на протоколі *RIP*, а потім перейти на *EIGRP*.

Переваги *OSPF* у порівнянні з *RIP*:

- набагато більш масштабований;
- підтримує VLSM та CIDR (на відміну від RIPv1);
- в цілому у достатньо стійких мережах споживає менше мережевих ресурсів;
- забезпечує вибір кращих маршрутів;
- дозволяє коректно запобігти маршрутним циклам;
- характеризується кориснішою метрикою;
- сприяє створенню ієрархічних проектів мереж;
- забезпечує швидкий перехід мережі у сталий стан.

Недоліки *OSPF* у порівнянні з *RIP*:

- не допускає використання ієрархічних проектів у поєднанні з погано спроектованими структурами IP;
- є набагато більш складним порівняно з RIP;
- потребує більших ресурсів процесора і оперативної пам’яті;
- потребує більших витрат часу на проектування і реалізацію.

Порівняння OSPF з EIGRP

Протоколи *OSPF* і *EIGRP* фактично багато в чому аналогічні.

У протоколі *EIGRP*, як і в *OSPF* передбачено формування таблиці топології і пошук на її основі маршрутів до одержувачів.

Крім того, при звичайних обставинах протокол *EIGRP*, як і *OSPF* виключає можливість створення маршрутних циклів.

Проте в деяких умовах протокол OSPF є доцільнішим, ніж EIGRP, а в інших – навпаки.

Переваги OSPF у порівнянні з EIGRP:

- сприяє створенню ієрархічних проектів мереж;
- має менш складну метрику порівняно із складеною метрикою EIGRP;
- не схильний до проблем, пов'язаних з постійним перебуванням маршруту в активному стані;
- не залежить від виробника конкретного продукту.

Недоліки OSPF у порівнянні з EIGRP:

- метрика не така гнучка, як складена метрика EIGRP;
- не забезпечує розподілу навантаження по маршрутах з нерівною вартістю;
- не допускає використання ієрархічних проектів в поєднанні з погано спроектованими структурами IP;
- потребує більших ресурсів процесора і оперативної пам’яті;
- потребує більших витрат часу на проектування і реалізацію.

7.6. Конфігурування статичних маршрутів

Після задання адміністратором статичного маршруту маршрутизатор запам’ятовує його у своїй ТМ і використовує для пересилання пакетів.

Команда задання статичного маршруту має такий синтаксис:

Rt(config)#ip route prefix mask {ip | int-type int-num}[dist],

де *prefix, mask* – *IP*-адреса та маска пункту призначення, відповідно; *ip, int-type, int-num* – IP-адреса порту наступного транзитного переходу (хопа), тип та номер локального інтерфейсу на які слід надіслати пакет, котрий повинен дістатися вищевказаного пункту призначення; *dist* – адміністративна відстань.

Адміністративна відстань (AB) – це необов'язковий параметр, який характеризує надійність маршруту. Чим менша AB, тим надійнішим є маршрут. Маршрут з меншою адміністративною відстанню буде занесений у ТМ [5].

Для конфігурування статичних маршрутів слід виконати такі кроки:

1. Визначити усі мережі-отримувачі, їх маски та шлюзи (як адресу шлюзу можна вказати або локальний інтерфейс маршрутизатора або адресу наступного *хопа*, на шляху до потрібного пункту призначення).
2. Увійти в режим глобального конфігурування.
3. Ввести команду *ip route* з відповідними параметрами як показано вище.
4. Повторити третій крок для усіх мереж-отримувачів, до яких слід задати статичний маршрут.
5. Вийти з режиму глобального конфігурування.
6. Виконати команду *copy running-config startup-config*.

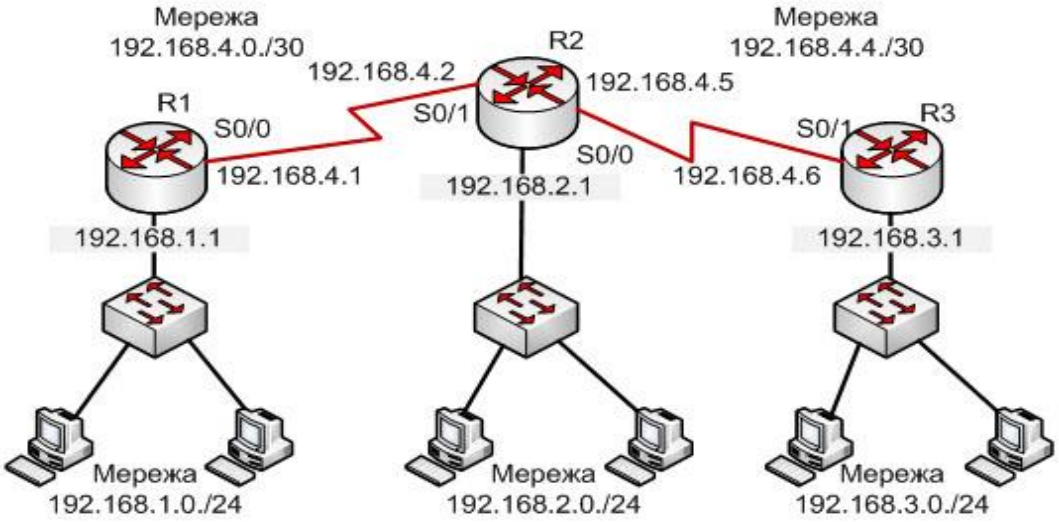


Рис. 7.7. Конфігурування статичних маршрутів

Команди задання статичних маршрутів на прикладі маршрутизатора R2 будуть:

R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.4.1,

R2(config)#ip route 192.168.3.0 255.255.255.0 192.168.4.6,

(статичні маршрути до усіх інших мереж 192.168.2.0/24, 192.168.4.0/30, 192.168.4.4/30 маршрутизатор R2 знає, оскільки вони безпосередньо під'єднані до нього). У вищенаведених командах вказано IP-адреси наступних хопів на шляху до отримувачів. Якщо вказувати вихідні інтерфейси, команди задання статичних шляхів набудуть вигляду

R2(config)#ip route 192.168.1.0 255.255.255.0 s0/1,

R2(config)#ip route 192.168.3.0 255.255.255.0 s0/0.

Перевірка і усунення помилок у конфігурації статичних маршрутів

Після того, як статичні маршрути сконфігуровані – слід впевнитись, що вони є у ТМ і пересилка пакетів за ними виконується правильно. Для цього можна використати команди: *show running-config* та *show ip route*.

Перша команда дозволяє проглянути статичні маршрути у файлі робочого конфігурування маршрутизатора, а друга – у його ТМ. При цьому, якщо деякий маршрут введено неправильно – його слід вилучити, а замість ввести правильний.

Для пошуку та усунення помилок в конфігуруванні статичних маршрутів пропонується виконати такі кроки:

1. Впевнитись, що канал, який буде використовуватись як шлюз є доступним.

2. Виконати команду *show interfaces* і впевнитись у активності інтерфейсу і канального протоколу.

3. Перевірити правильність *IP*-адреси на інтерфейсі.

4. Виконати команду *ping* для *IP*-адреси віддаленого маршрутизатора, безпосередньо під'єднаного до шлюзу маршруту. Якщо результат цієї команди буде негативний – то проблема не пов'язана з маршрутизацією.

5. Якщо команда не спрацьовує на дальньому маршрутизаторі – слід виконати команду *traceroute* – для визначення вузла, де губиться пакет.

6. Під'єднатись до маршрутизатора, на якому не спрацювало трасування і виконати дії, описані у першому кроці.

7. Якщо команда *ping* спрацювала на дальньому кінці маршруту – тест можна вважати успішним і завершеним.

Побудова таблиці маршрутизації

Протокол маршрутної інформації (*Routing Information Protocol – RIP*) початково був визначений в документі RFC 1058 в 1988 році. Найбільш суттєвими є такі його характеристики:

- *RIP* є дистанційно-векторним протоколом маршрутизації;
- як метрики при виборі маршруту використовується кількість переходів (або хопів);
- якщо кількість переходів більше ніж 15, пакет відкидається;
- стандартно оновлення маршрутизації розсилаються широкомовним способом кожних 30 секунд.

Протокол *RIP* значно еволюціонував: від основаного на класах протоколу першої версії (*RIPv1*) до безкласового протоколу другої версії (*RIPv2*). Вдосконалення останнього такі:

- можливість переносити додаткову інформацію про маршрутизацію пакетів;
- механізм аутентифікації для забезпечення безпечного оновлення ТМ;
- підтримка масок змінної довжини.

Протокол *RIP* запобігає появі петель маршрутизації, по яких пакети могли б циркулювати невизначено довго, встановлюючи максимально допустиму кількість переходів на маршруті між відправником та отримувачем. Стандартне максимальне значення кількості переходів становить 15.

При отриманні маршрутизатором оновлення маршрутів, що містить новий або змінений запис, він збільшує значення метрики на одиницю.

Якщо при цьому значення метрики перевищує 15, то мережа-отримувач вважається недосяжною.

У протоколу *RIP* є ряд функцій спільних для нього та інших протоколів маршрутизації. Наприклад, він дозволяє використовувати механізми розщеплення

горизонту та таймери утримання інформації для запобігання розповсюдження некоректних знань про маршрути.

Розглянемо процес побудови таблиці маршрутизації за допомогою протоколу RIPv1 на прикладі мережі (рис.).

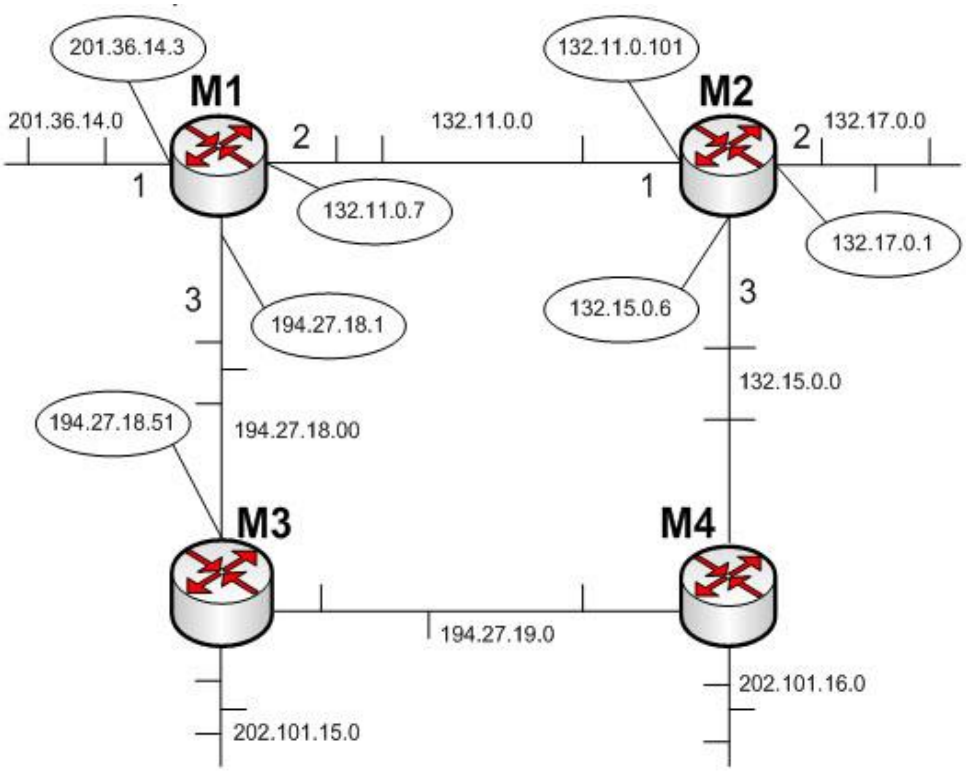


Рис. 7.8. Мережа, об’єднана RIP-маршрутизаторами

Етап 1 – створення мінімальних таблиць маршрутизації

В даній мережі містяться вісім IP-мереж, зв’язаних чотирма маршрутизаторами з ідентифікаторами: M1, M2, M3 та M4.

Маршрутизатори, що працюють за протоколом RIP, можуть мати ідентифікатори, однак, для роботи протоколу вони не є необхідними. В RIP-повідомленнях ці ідентифікатори не передаються.

У вихідному стані в кожному маршрутизаторі програмним забезпеченням стека TCP/IP автоматично створюється мінімальна таблиця маршрутизації, в якій враховуються лише безпосередньо під’єднані мережі.

Мінімальна таблиця маршрутизації маршрутизатора M1:

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Етап 2 – розсилання мінімальних таблиць сусідам

Після ініціалізації кожного маршрутизатора він починає відсилати своїм сусідам повідомлення протоколу *RIP*, в яких міститься його мінімальна *ТМ*.

RIP-повідомлення надсилаються в пакетах протоколу *UDP* і містять для кожної мережі: її *IP*-адресу та відстань до неї від маршрутизатора, що надсилає повідомлення.

Сусідами є маршрутизатори, яким даний маршрутизатор може надіслати *IP*-пакет не користуючись послугами проміжних маршрутизаторів.

Маршрутизатор *M1* надсилає до *M2 і M3* повідомлення:

- мережа *201.36.14.0*, відстань 1;
- мережа *132.11.0.0*, відстань 1;
- мережа *194.27.18.0*, відстань 1.

Етап 3 – отримання RIP-повідомлень від сусідів і оброблення отриманої інформації

Після отримання аналогічних повідомлень від маршрутизаторів *M2* та *M3* маршрутизатор *M1* нарощує кожне отримане поле метрики на одиницю і запам’ятовує, через який порт і від якого маршрутизатора отримана ця інформація (адреса цього маршрутизатора буде адресою наступного хопа, якщо цей запис буде внесений до *ТМ*).

Потім маршрутизатор починає порівнювати нову інформацію з тією, що зберігається в його *ТМ*

Таблиця маршрутизації маршрутизатора *M1*

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2
~~132.11.0.0~~	~~132.11.0.101~~	~~2~~	~~2~~
~~194.27.10.0~~	~~194.27.10.51~~	~~3~~	~~2~~

Протокол *RIP* заміщує запис про будь-яку мережу лише тоді, якщо нова інформація має кращу метрику, ніж наявна.

В результаті в *TM* про кожну мережу лишається лише один запис.

Якщо є кілька рівнозначних за метрикою шляхів до однієї і тієї ж мережі, то в *TM* лишається один запис, що надійшов першим.

Для цього правила є виняток – якщо гірша інформація про будь-яку мережу прийшла від того ж маршрутизатора, на основі повідомлення якого була створено даний запис, то вона заміщує кращу.

Аналогічні операції з новою інформацією виконують й інші маршрутизатори мережі.

Етап 4 – розсилання нової таблиці сусідам

Кожен маршрутизатор відсилає нове RIP-повідомлення всім своїм сусідам. В цьому повідомленні він розміщує дані про всі відомі йому мережі – як безпосередньо під’єднаних, так і віддалених.

Етап 5 – отримання RIP-повідомлень від сусідів та оброблення отриманої інформації

Етап 5 фактично повторює етап 3. Розглянемо, як це робить маршрутизатор M1

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
~~132.15.0.0~~	~~194.27.10.51~~	~~3~~	~~3~~
194.27.19.0	194.27.18.51	3	2
~~194.27.19.0~~	~~132.11.0.101~~	~~2~~	~~3~~
~~202.101.15.0~~	~~194.27.18.51~~	~~3~~	~~2~~
202.101.16.0	132.11.0.101	2	3
~~202.101.16.0~~	~~194.27.10.51~~	~~3~~	~~3~~

На цьому етапі маршрутизатор *M1* отримав від *M3* інформацію про мережу *132.15.0.0*, яку той в свою чергу на попередньому циклі роботи отримав від *M4*. Маршрутизатор вже знає про мережу *132.15.0.0*, причому стара інформація має кращу метрику, ніж нова, тому ця нова інформація відкидається.

Про мережу *202.101.16.0* маршрутизатор *M1* дізнається на цьому етапі вперше, причому дані про неї приходять від двох сусідів – від *M3* та *M4*. Оскільки метрики в цих повідомленнях однакові, то в *TM* потрапляють дані, які прийшли першими. В нашому прикладі вважається, що маршрутизатор *M2* випередив *M3* і першим надіслав *RIP*-повідомлення до *M1*.

Якщо маршрутизатори періодично повторюють етапи розсилки та оброблення *RIP*-повідомлень, то за певний проміжок часу в мережі встановлюється коректний режим маршрутизації, коли всі мережі будуть досяжні з будь-якої мережі за допомогою деякого раціонального маршруту. Пакети будуть доходити до адресатів і не зациклюватися в петлях.

Методи боротьби з фальшивими маршрутами в протоколі RIP

Основними методами боротьби за фальшивими маршрутами в протоколі RIP є:

- розщеплення горизонту,
- вилучення маршруту в зворотному напрямі,
- миттєві оновлення,

- таймери утримання інформації

Маршрутні петлі можуть виникати у тому випадку, якщо для протоколу маршрутизації характерна повільна конвергенція після змін в мережі або для топології мережі в маршрутизаторах виникла невідповідність між записами ТМ.

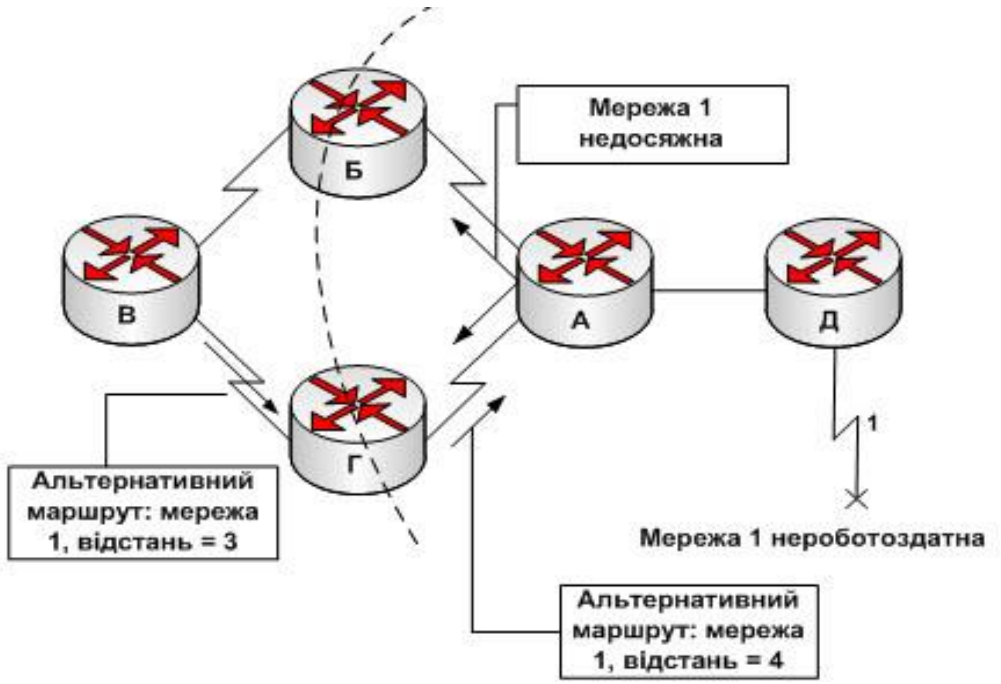


Рис. 7.9. Петлі маршрутизації

Їх виникнення відбувається так:

1. Перед виходом з ладу мережі 1 всі маршрутизатори мають узгоджені та коректні *ТМ*. В цьому випадку говорять, що в мережі відбулася конвергенція. До кінця цього прикладу вважається, що для маршрутизатора ***В*** найкращий маршрут до мережі 1 проходить через маршрутизатор ***Б***, а відстань (метрика) від маршрутизатора ***В*** до мережі 1 дорівнює 3.

2. Якщо мережа 1 виходить з ладу, то маршрутизатор ***Д*** надсилає повідомлення про оновлення маршрутів маршрутизатору ***А***. Після його отримання маршрутизатор А припиняє надсилати пакети у мережу 1, однак, маршрутизатори ***Б, В*** та ***Г*** продовжують, оскільки вони ще не інформовані про збій в мережі 1. Коли маршрутизатор ***А*** надсилає повідомлення про оновлення, маршрутизатори ***Б*** та ***Г*** припиняють надсилання пакетів у мережу 1. Однак в цей момент

маршрутизатор ***В*** ще не отримав повідомлення про оновлення. Для нього мережа, як і раніш, вважається досяжною через маршрутизатор ***Б***.

3. Припустимо, що маршрутизатор ***В*** відправляє періодичне оновлення маршрутів маршрутизатору ***Г***, вказуючи маршрут до мережі 1 через маршрутизатор ***Б***. Маршрутизатор ***Г*** змінює свою *ТМ* для того, щоб врахувати таку некоректну інформацію, і надсилає цю інформацію маршрутизатору ***А***, який надсилає її маршрутизаторам ***Б*** та ***Д*** і т. д. Тепер будь-який пакет, призначений для мережі 1, рухається по кільцевому маршруту (петлі) від маршрутизатора ***В*** до маршрутизатора ***Б***, далі до ***А*** і ***Г*** та знову до маршрутизатора ***В***.

Некоректні відомості про мережу 1 продовжують циркулювати по кільцевому маршруту доти, поки будь-який інший процес це не припинить. При такому стані мережі, яке називають зациклюванням (*count to infinity*), пакети продовжують неперервно рухатись мережею, незважаючи на вихід з ладу мережі-отримувача. І поки маршрутизатор збільшує кількість переходів (потенційно до нескінченності), неправильна інформація допускає існування петлі

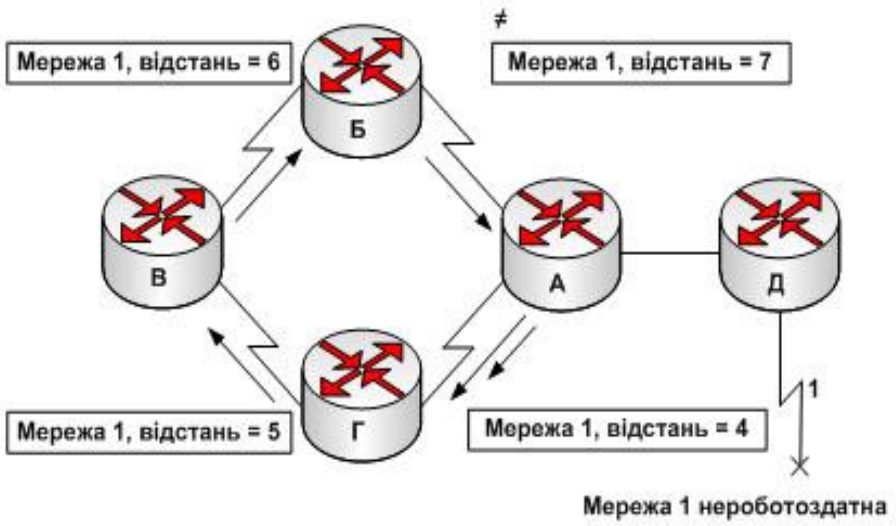


Рис. 7.10. Зациклювання

Якщо не будуть прийняті певні заходи для зупинення цього процесу, вектор відстані або метрика, що відображає кількість переходів, будуть зростати при кожному проходженні пакета через черговий маршрутизатор. Таким чином,

пакети рухаються по колу внаслідок того, що в *ТМ* міститься помилкова інформація [6].

Дистанційно-векторні алгоритми маршрутизації мають здатність до самокорекції, однак, для усунення петлі в маршрутизації та проблеми зациклювання потрібні спеціальні заходи. Для того, щоб уникнути проблеми зациклювання, нескінченність визначається як деяке скінченне число. Для протоколу *RIP* таким числом є 16. Тепер протокол маршрутизації дозволяє петлі існувати лише до того моменту, доки метрика не перевищить 16. Оскільки вектор відстані перевищив стандартний максимум в 15 транзитних переходів, пакет маршрутизатором відкидається. В будь-якому випадку, коли значення метрики перевищує максимально допустиме, мережа 1 є вважається недосяжною.

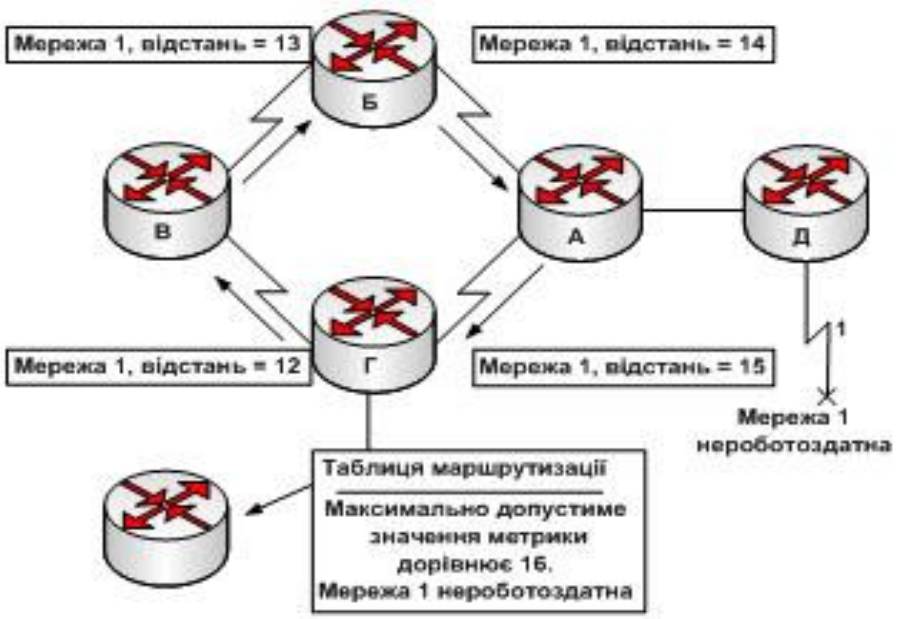


Рис. 7.11. Задання максимального значення метрики

Розщеплення горизонту

Друге можливе джерело петлі в маршрутизації виникає у випадку, коли маршрутизатору надіслана інформація, що суперечить правильній, яку він спочатку розповсюдив.

1. Маршрутизатор ***А*** надсилає маршрутизаторам ***Б*** та ***Г*** оновлення, в якому вказується, що мережа 1 не працює.

2. Однак маршрутизатор ***В*** передає маршрутизатору ***Б*** інше повідомлення, в якому вказується, що мережа 1 доступна через маршрутизатор ***Г*** з відстанню, що дорівнює чотирьом переходам. Така дія не порушує правил розщеплення горизонту.

3. Після отримання останнього повідомлення маршрутизатор ***Б*** неправильно робить висновок, що у маршрутизатора ***В*** як і раніше є дійсний маршрут до мережі 1. Маршрутизатор ***Б*** відсилає повідомлення про оновлення маршрутизатору *А*, повідомляючи його про новий маршрут до мережі 1.

4. Отримавши його, пристрій ***А*** робить висновок, що він може надсилати інформацію у мережу 1 через маршрутизатор ***Б***. Маршрутизатор ***Б*** вирішує, що він може надсилати інформацію у мережу 1 через маршрутизатор ***Г***. В такій ситуації будь-який пакет буде рухатись по кільцевому маршруту між цими маршрутизаторами.

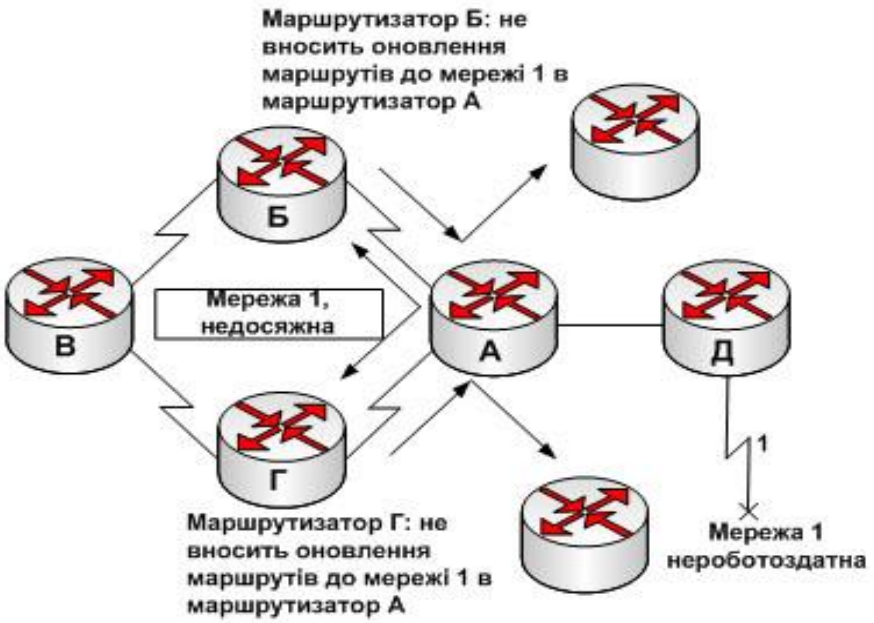


Рис. 7.12. Розщеплення горизонту

Розщеплення горизонту *(split horizon)* намагається запобігти виникненню такої ситуації. Згідно з цим методом, при надходженні повідомлення про оновлення маршрутів для мережі 1 від маршрутизатора *А* маршрутизатори *Б* та *Г* не можуть посилати інформацію про мережу 1 в зворотному напрямі, тобто маршрутизатору *А*. Таким чином, розщеплення горизонту не дозволяє

розповсюджувати неправильну інформацію маршрутизації та зменшує об’єм службових повідомлень, що передаються.

Вилучення маршруту в зворотному напрямку

Вилучення маршруту в зворотному напрямку *(route poisoning)* використовується різними *ДВП* для запобігання виникненню великих петель маршрутизації і наданні явної інформації про маршрути в тих випадках, коли мережа недосяжна. Таке вилучення маршруту зазвичай здійснюється шляхом встановлення кількості переходів на одиницю більшою, ніж максимальне значення. Цей механізм є альтернативним способом попередження петель маршрутизації. Даний підхід може бути сформульовано так: після отримання інформації про маршрут через будь-який інтерфейс необхідно оголосити його недосяжним через цей самий інтерфейс. Краще явно повідомити маршрутизатор про те, що маршрут потрібно ігнорувати, ніж лишити все неконтрольованим.

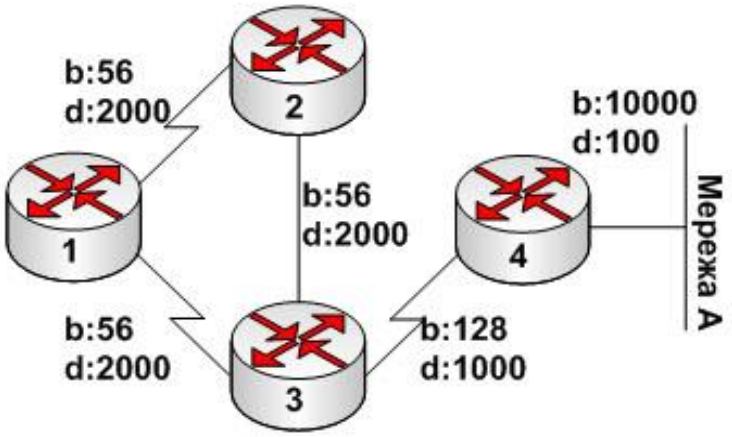


Рис. 7.13. Вилучення маршруту в зворотному напрямку

Припустимо, що на всіх маршрутизаторах увімкнено механізм зворотного вилучення маршрутів. Після отримання інформації маршрутизатором 1 про мережу ***A*** від маршрутизатора 2 пристрій 1 оголошує мережу ***A*** недосяжною через свої канали до маршрутизаторів 2 та 3. Якщо маршрутизатор 3 має будь-який

маршрут до мережі ***A*** через маршрутизатор 1, він видаляє цей маршрут, оскільки отримав повідомлення про недосяжність цієї мережі.

Нові копії *TM* зазвичай регулярно розсилаються сусіднім маршрутизаторам.

Протокол розсилає оновлення кожні 30 секунд. Однак, миттєві оновлення (*triggered updates*) розсилаються негайно у відповідь на будь-яку зміну у *TM*. Маршрутизатор, який виявив зміну в топології, негайно розсилає оновлення суміжним маршрутизаторам. Ті маршрутизатори, в свою чергу, також генерують миттєві оновлення, оповіщаючи про зміни своїх сусідів. При виході будь-якого маршруту з ладу повідомлення надсилається, не очікуючи закінчення часу таймера оновлення. Використання миттєвих оновлень в комбінації з механізмами вилучення маршрутів гарантує, що всі маршрутизатори будуть повідомлені про відмову маршрутів до закінчення часу будь-якого таймера зберігання інформації.

Миттєве оновлення, таким чином, являє собою анонс, який розсилається до закінчення часу таймера оновлення.

Маршрутизатор також негайно надсилає повідомлення оновлення на всі свої інші інтерфейси, не чекаючи закінчення часу таймера. Такий принцип роботи приводить до розсилання оновленої інформації про стан маршруту та скидає таймери на сусідніх маршрутизаторах. Ця хвиля оновлень передається по всій мережі.

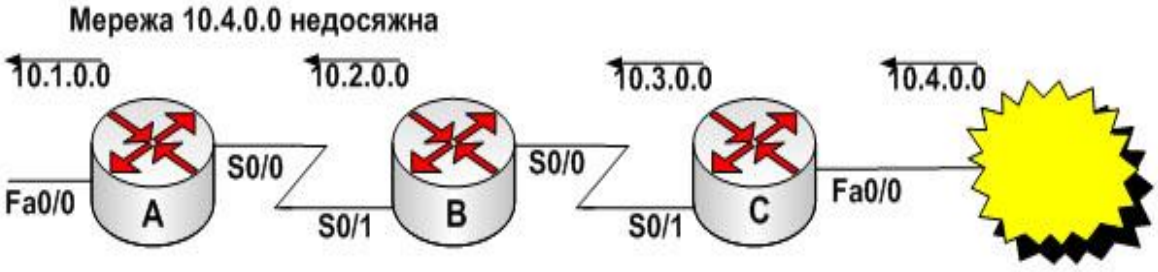


Рис. 7.14. Миттєві оновлення

Маршрутизатор ***B*** генерує миттєве оновлення, повідомляючи про те, що мережа *10.4.0.0* недосяжна. Після отримання цієї інформації маршрутизатор ***B*** повідомляє інші маршрутизатори про вихід з ладу мережі *10.4.0.0* через інтерфейс

S0/1. В свою чергу, маршрутизатор ***A*** надсилає це повідомлення про оновлення через інтерфейс *Fa0/0.*

Зациклювання можна уникнути шляхом використання таймерів утримання інформації (*holddown timer*). Послідовність дій при цьому така:

- 1. Коли маршрутизатор отримує від сусіднього пристрою оновлення маршрутів, яке вказує, що раніш доступна мережа не працює, він помічає цей маршрут як недоступний та запускає таймер.
- 2. Якщо до закінчення часу таймера від того ж сусіднього пристрою надходить нове повідомлення, що мережа, яка вийшла з ладу, знову доступна, то маршрутизатор помічає мережу як доступну та вимикає таймер утримання інформації.
- 3. Якщо нове оновлення надходить від іншого сусіднього маршрутизатора, і вказана в ньому метрика краще раніше зареєстрованої для даної мережі, то маршрутизатор помічає мережу як доступну та вимикає таймер.

Таймери утримання інформації

Якщо до закінчення часу таймера утримання інформації від іншого сусіднього маршрутизатора надходить нове оновлення і вказана у ньому метрика для даної мережі гірша раніш зареєстрованої повідомлення оновлення ігнорується. В такій ситуації ігнорування повідомлень про оновлення надає більше часу для розповсюдження по всій мережі інформації про зміни топології мережі.

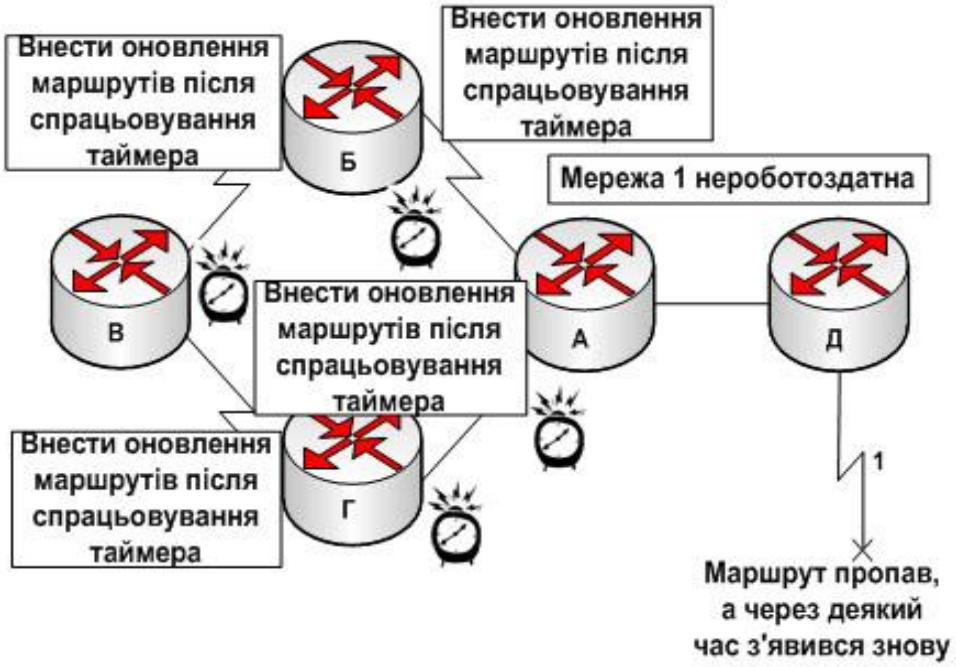


Рис. 7.15. Таймери утримання інформації

Недоліки RIP

RIP не працює з адресами підмереж. Якщо нормальний 16-біт ідентифікатор ЕОМ класу ***B*** НЕ дорівнює 0, *RIP* не може визначити чи є не нульова частина субмережевим *ID*, або повною *IP*-адресою.

RIP вимагає багато часу для відновлення зв'язку після збою в маршрутизаторі (хвилини). В процесі встановлення режиму можливі цикли.

Число кроків важливий, але не єдиний параметр маршруту, та й 15 кроків не межа для сучасних мереж.

7.7. Протокол EIGRP

Дистанційно-векторний протокол маршрутизації *EIGRP (Enhanced Interior Gateway Routing Protocol)* був розроблений та реалізований фірмою Cisco у 1992 р.

Він є суттєвим вдосконаленням свого попередника - протоколу маршрутизації *IGRP*, який сьогодні фактично не використовується.

Переваги використання протоколу EIGRP

• швидка конвергенція. На маршрутизаторах протоколу *EIGRP* конвергенція відбувається значно швидше, оскільки вона базується на сучасному алгоритмі дифузії поновлень маршрутизації *DUAL* (*Diffusing Update Algorithm*).

Цей алгоритм гарантує відсутність петель у кожний момент часу на всьому маршруті та дозволяє усім маршрутизаторам, що належать до даної топології, виконати одночасну синхронізацію. Крім того, якщо у традиційних дистанційно-векторних протоколів певний маршрут став недоступним, маршрутизатори повинні чекати чергового періодичного поновлення, а протокол *EIGRP* буде при цьому використовувати резервний шлях (якщо такий існує);

• ефективне використання смуги пропускання.

По-перше, протокол *EIGRP* використовує розсилання часткових, обмежених за обсягом поновлень (*Partial, bounded updates*) маршрутизації, і як наслідок цього забезпечується мінімальне використання такими поновленнями смуги пропускання в умовах стабільної роботи мережі. Маршрутизатори *EIGRP*, як правило, розсилають часткові, поетапні поновлення маршрутизації, а не повні таблиці маршрутизації. Цей процес аналогічний роботі протоколу *OSPF*, однак на відміну від нього, маршрутизатори протоколу *EIGRP* розсилають ці часткові поновлення не всім маршрутизаторам даної області, лише тим, яким вони дійсно потрібні. Саме тому такі поновлення називаються обмеженими. По-друге, у протоколі *EIGRP* замість регулярного розсилання поновлень маршрутизації маршрутизатори підтримують постійний контакт один з одним шляхом розсилання невеликих пакетів вітання. Хоча пакети вітання розсилаються регулярно, внаслідок невеликого розміру вони досить незначно використовують смугу пропускання (на відміну від протоколів *RIP* та *IGRP*, які розсилають сусіднім пристроям свою повну таблицю маршрутизації кожні 30 або 90 секунд, відповідно);

• підтримка масок підмереж змінної довжини *VLSM* (*Variable-Length Subnet Mask*) і безкласової міждоменної маршрутизації *CIDR* (*Classless Interdomain Routing*). На відміну від протоколу *IGRP, EIGRP* забезпечує повну підтримку безкласового IP шляхом обміну масками підмереж у повідомленнях поновлення

маршрутів. Це дозволяє мережевим проектувальникам максимально використовувати адресний простір;

• підтримка декількох протоколів мережевого рівня. Протокол *EIGRP* підтримує протоколи *IP, IPX* та *AppleTalk* шляхом використання залежних від протоколу модулів (protocol-dependent module, *PDM*);

• використання складної та гнучкої метрики маршрутів. Метрика протоколу *EIGRP*, на відміну від багатьох інших протоколів маршрутизації (крім протоколу *IGRP*), може враховувати одразу чотири показники (пропускна спроможність, час затримки, завантаженість та надійність каналу). При цьому адміністратор може задавати значимість кожного з цих показників [6].

Таблиці протоколу EIGRP

Протокол EIGRP у своїй роботі використовує дані трьох таблиць: *маршрутизації, сусідніх пристроїв та топології*. Ці таблиці ще називають базами даних протоколу. Призначення ТМ нам вже відоме. Тому розглянемо призначення двох інших таблиць.

Таблиця сусідніх пристроїв

Кожний маршрутизатор *EIGRP* підтримує таблицю сусідніх пристроїв (*neighbor table*), в якій перераховані суміжні маршрутизатори. Для кожного протоколу (наприклад, *IP, IPX*), що підтримується протоколом *EIGRP*, є своя *таблиця сусідніх пристроїв* (*ТСП*). При виявленні нових сусідніх пристроїв їх адреси та інтерфейси заносяться у ці таблиці. Проглянути зміст ТСП можна за командою *show ip eigrp neighbors).*

При відправленні пакета привітання сусідній пристрій повідомляє час утримання, що вказує, як довго маршрутизатор розглядає свій сусідній пристрій як досяжний та працездатний. Якщо за період утримання від маршрутизатора не надійшов пакет привітання, то вважається, що час утримання вичерпано. В такому випадку алгоритм *DUAL* інформується про зміну топології і повинен знову обчислити параметри нової топології.

ТСП має, зокрема, такі поля.

- *Порядковий номер (H)* запису в міру навчання даного пристрою стосовно сусідніх пристроїв.
- *Адреса сусіднього пристрою (Neighbor Address)* – адреса мережевого рівня сусіднього пристрою.
- *Інтерфейс (Interface)* – локальний інтерфейс, через який було отимано пакет Hello від сусіднього пристрою.
- *Час утримання (Hold Time)* – часовий інтервал, після закінчення якого, у випадку відсутності будь-яких повідомлень від сусіднього пристрою, канал розглядається як нероботоздатний. При отриманні ж будь-якого пакета протоколу *EIGRP*, таймер приймає початкове значення.
- *Доступний час (Uptime)* – час, що минув з моменту додання даного сусіднього пристрою у *ТСП*.
- *Таймер циклу обміну повідомленнями (Smooth Round-Trip Timer – SRTT)* – середній час, потрібний для того, щоб надіслати пакет сусідньому пристрою та одержати від нього відповідний пакет. Цей таймер визначає інтервал повторного передавання (*Retransmit Interval – RTI*).
- *Час ретрансляції (Retransmission Timeout – RTO)* – час в мілісекундах, протягом якого програмне забезпечення очікує моменту повторного пересилання пакета з черги повторного розсилання.
- *Лічильник черги (Queue Count – Q Cnt)* – число пакетів, які перебувають у черзі очікуючи передавання. Якщо це значення постійно більше нуля – ймовірно маршрутизатор зазнає переповнення. Нульове значення свідчить, що пакетів протоколу *EIGRP* у черзі немає.
- *Послідовний номер (Sequence Number – Seq No)* – номер останнього пакета, отриманого від даного сусіднього пристрою. Протокол *EIGRP* використовує це поле для підтвердження отримання пакета, переданого сусіднім пристроєм, та для ідентифікації пакетів, що передані з порушенням порядку. *ТСП* забезпечує надійне та впорядковане доставлення пакетів.

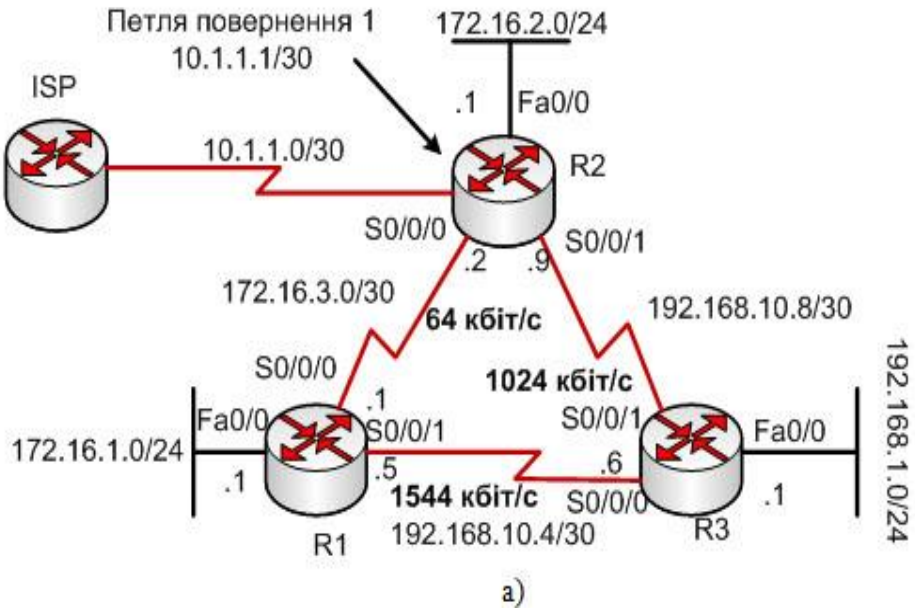


Рис. 7.16. Таблиця сусідніх пристроїв

Наприклад, ТСП для маршрутизатора R2 має вигляд:

R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
1 192.168.10.10 Ser0/0/1 10 00:01:44 20 200 0 7
0 172.16.3.1 Ser0/0/0 10 00:03:27 25 200 0 12

Топологічна таблиця

Топологічна таблиця (topology table) містить всі *ТМ* протоколу *EIGRP*, наявні на пристроях даної автономної системи (проглянути зміст топологічної таблиці можна за командою *show ip eigrp topology*).

Алгоритм *DUAL* отримує інформацію з *ТСП* і топологічної таблиці (*ТТ*) та обчислює маршрути з найменшою оцінкою до кожного пункту призначення. Завдяки цьому маршрутизатори протоколу *EIGRP* можуть швидко визначити альтернативні маршрути та використати їх у разі потреби [4].

Первинний маршрут (*successor*) записується у *ТМ*, а його копія – у *ТТ*. Усі маршрутизатори *EIGRP* підтримують *ТТ* для кожного зконфігурованого мережевого протоколу. У цій таблиці містяться маршрути до усіх пунктів призначення, які стали відомі маршрутизатору.

ТТ має такі поля:

Передбачувана відстань (Feasible Distance – FD) – це найменша обчислена метрика до кожного пункту призначення. У прикладі показано *ТТ* для маршрутизатора R2, з прикладу, наведеного на рис. Тут передбачувана відстань, наприклад, до мережі *192.168.1.0* становить *3014400*, на що вказує запис „*FD is 3014400”.*

R2# show ip eigrp topology
IP-EIGRP Topology Table AS(1)/ID 10.1.1.1
Codes: P - Passive, A - Active, U - Update,
Q - Query, R - Reply, r - Reply Status s – sia Status
P 192.168.10.4/30, 1 successors, FD is 3523840
via 192.168.10.10 (3523840/2169856), Serial0/0/1
via 172.16.3.1 (410240000/2169856), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
via 192.168.10.10 (3014400/28160), Serial0/0/1
via 172.16.3.1 (410240000/2172416), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
via connected Serial0/0/1
P 172.16.1.0/24, 1 successors, FD is 3526400
via 192.168.10.10 (3526400/2172416), Serial0/0/1
via 172.16.3.1 (40514560/28160), Serial0/0/0
P 172.16.2.0/24, 1 successors, FD is 28160
via connected FastEthernet 0/0
P 172.16.3.0/30, 1 successors, FD is 40512000

Джерело маршруту (*Route Source*) – це ідентифікаційний номер маршрутизатора, який анонсував цей маршрут. Дане поле заповнюється лише тільки для маршрутів, які стали відомі ззовні від інших мереж протоколу EIGRP. У прикладі джерелами маршруту до мережі *192.168.1.0 є 192.168.10.10* та *172.16.3.1*, про що свідчать записи „*via 192.168.10.10*” та „*via 172.16.3.1*”, відповідно.

Повідомлена відстань *(Reported Distance – RD) або об’явлена відстань (Advertised Distance – AD)* – це значення відстані, яке сусідній маршрутизатор повідомляє конкретному одержувачу. У прикладі повідомлена відстань до мережі 192.168.1.0 дорівнює 28160, на що вказує значення поля RD (3014400/28160).

Інформація про інтерфейс *(Interface Information)* – це номер інтерфейсу, через який можна досягти пункту призначення. З прикладу видно, що мережу

192.168.10.10 можна досягнути через інтерфейс Serial0/0/1 (via 192.168.10.10 (3014400/28160), Serial0/0/1), а можна резервним шляхом через Serial0/0/0 (via 172.16.3.1 (410240000/2172416), Serial0/0/0)

Статус маршруту *(Route Status)* – може бути *пасивний* або *активний*. *Пасивні (Passive – P)* – це стійкі та готові до використання маршрути, активні (*Active – A*) це ті, для яких алгоритм *DUAL* продовжує процес перерахування маршруту. Протокол *EIGRP* сортує записи *TT* так, щоб первинні маршрути знаходились у її верхній частині, а за ними йшли резервні. У нижній частині цієї таблиці розташовуються маршрути, які алгоритм *DUAL* розглядає як можливі петлі маршрутизації.

Протокол *EIGRP* використовує багато нових технологій, кожен з яких поліпшує операційну ефективність, підвищує швидкість конвергенції та розширює набір функцій протоколу *IGRP* та інших протоколів маршрутизації.

Ці технології можна поділити на такі чотири категорії:

- Виявлення сусідніх пристроїв і відновлення загубленого з ними зв’язку.
- Надійний транспортний протокол (Reliable Transport Protocol).
- Алгоритм DUAL кінцевих станів машини.
- Модулі конкретних протоколів.

Звичайні прості дистанційно-векторні маршрутизатори не встановлюють зв’язків зі своїми сусідами. На відміну від них маршрутизатори протоколу EIGRP встановлюють зв’язки зі своїми сусідніми пристроями.

Рис. 7.17. Виявлення сусідніх пристроїв і відновлення втраченого з ними зв'язку

Маршрутизатори *EIGRP* встановлюють відношення суміжності із сусідніми маршрутизаторами шляхом розсилання невеликих пакетів-вітань. Ці пакети за замовчуванням розсилаються кожні 5 секунд на каналах з великою смугою пропускання й кожні 60 секунд на низькошвидкісних багатоточкових каналах. Маршрутизатор *EIGRP* припускає, що поки від відомих йому сусідніх пристроїв надходять пакети вітання, ці пристрої та відповідні маршрути залишаються діючими.

Формуючи відношення суміжності маршрутизатори EIGRP одержують можливості:

- динамічно дізнаватися про нові маршрути, що з'являються у мережі;
- ідентифікувати маршрутизатори, які стали недосяжними або нероботоздатними;
- виявляти маршрутизатори, які раніше були недосяжні.

Надійний транспортний протокол (Reliable Transport Protocol, RTP) – це протокол транспортного рівня, який може гарантувати впорядковане доставлення пакетів *EIGRP* всім сусідам. У мережах *IP*-протоколу для впорядкування і своєчасного доставлення пакетів використовується протокол *TCP*. Однак протокол *EIGRP* незалежний від використовуваного мережевого протоколу і не

використовує протокол *TCP/IP* для обміну інформацією маршрутизації (як це роблять протоколи *RIP, IGRP, OSPF*). Для реалізації такої незалежності від *IP*, протокол *EIGRP* використовує свій фірмовий транспортний протокол для гарантованого доставлення інформації.

EIGRP може активізувати протокол *RTP* для забезпечення служби надійної або негарантованої доставки залежно від конкретної ситуації. Наприклад, пакети вітання не потребують додаткового навантаження на мережу за рахунок гарантованого доставлення, оскільки вони розсила-ються часто і їх розмір повинен бути невеликим. Проте гарантоване доставлення інформації про маршрути може прискорити конвергенцію, оскільки маршрутизатори *EIGRP* не очікують завершення часу таймера до повторного передавання. Використання надійного транспортного протоколу дозволяє протоколу *EIGRP* одночасно здійснювати багатоадресне та одноадресне розсилання, що забезпечує максимальну ефективність.

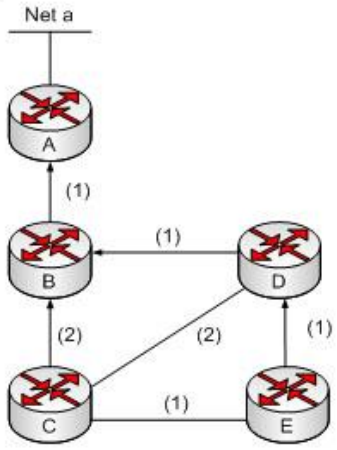
Головним компонентом протоколу *EIGRP* є алгоритм обчислення маршрутів. Повна назва цієї технології – *абстрактна машина кінцевих станів (finite-state machine, FSM) алгоритму DUAL*. Вона визначає набір можливих станів, через які можна пройти, які події викликають ці стани, а які є результатом цих станів. *FSM* містить всі логічні операції, необхідні для обчислення й порівняння маршрутів у мережі протоколу *EIGRP*.

Алгоритм *DUAL* стежить за всіма маршрутами, анонсованими сусідніми пристроями й використовує складену (композитну) метрику для кожного маршруту. Він гарантує, що кожний маршрут не містить петель. Після відповідних обчислень алгоритм *DUAL* заносить маршрути з найменшими оцінками в *TM* (тобто первинні маршрути), а їх копії – у *TT*.

Протокол зберігає важливу маршрутну й топологічну інформацію в *ТСП* і *TT*, які надають алгоритму *DUAL* маршрутну інформацію у випадку порушень у роботі мережі. Використовуючи інформацію цих таблиць *DUAL* може при необхідності швидко знаходити альтернативні маршрути: якщо будь-який канал стає непрацездатним, то він шукає у *TT* альтернативний (потенційно первинний або резервний) маршрут.

Пакети, надіслані у мережу-одержувач, негайно надсилаються за резервним маршрутом, що у цей момент одержує статус первинного, як показано на рис.7.18 *а*. Тут маршрутизатор *D* втрачає прямий зв'язок з маршрутизатором *B* і не має ідентифікованого первинного маршруту. Ймовірна відстань *FD* (обчислена оцінка) для маршруту від маршрутизатора D до маршрутизатора *A* дорівнює 2, а анонсована відстань через маршрутизатор *C* дорівнює 3. Оскільки значення *RD* менше, ніж метрика найкращого маршруту, але більше, ніж відстань *FD*, жоден резервний маршрут не заноситься у *TT*. Маршрутизатор *C* має ідентифікований резервний маршрут, так само як і маршрутизатор *E*, оскільки маршрут вільний від петель, а відстань *RD* до маршрутизатора наступного переходу менша, ніж відстань *FD* для первинного маршруту. Кінцевий результат роботи алгоритму *DUAL* наведено на рис. 7.18 *б*.

а)

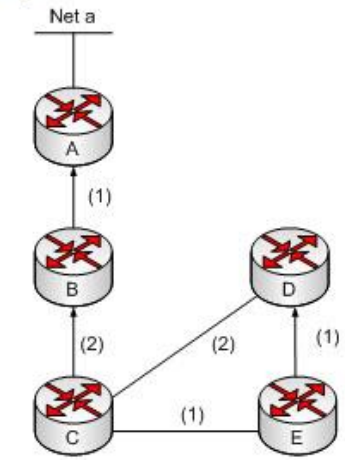


C	EIGRP	FD	RD	Топологія
Net a		3		(FD)
	Через B	3	1	(Наступник)
	Через D	4	2	(FS)
	Через E	4	3	

D	EIGRP	FD	RD	Топологія
Net a		2		(FD)
	Через C	2	1	(Наступник)
	Через E	5	3	(Наступник)

E	EIGRP	FD	RD	Топологія
Net a		3		(FD)
	Через D	3	2	(Наступник)
	Через C	4	3	

б)



C	EIGRP	FD	RD	Топологія
Net a		3		(FD)
	Через B	3	1	(Наступник)
	Через D			
	Через E			

D	EIGRP	FD	RD	Топологія
Net a		5		(FD)
	Через C	5	3	(Наступник)
	Через E	5	4	(Наступник)

E	EIGRP	FD	RD	Топологія
Net a		4		(FD)
	Через C	4	3	(Наступник)
	Через D			

Рис. 7.18. Робота алгоритму *DUAL*

Однією з привабливих якостей *EIGRP* є його модульна структура, що забезпечує максимальний рівень масштабованості та адаптованості. Підтримка різних мережевих протоколів (*IP, IPX, AppleTalk*), реалізована в протоколі *EIGRP* за допомогою модулів PDM. Фактично *EIGRP* може бути легко адаптований до нових або модифікованих мережевих протоколів (наприклад, IPv6) шляхом додання нового модуля PDM.

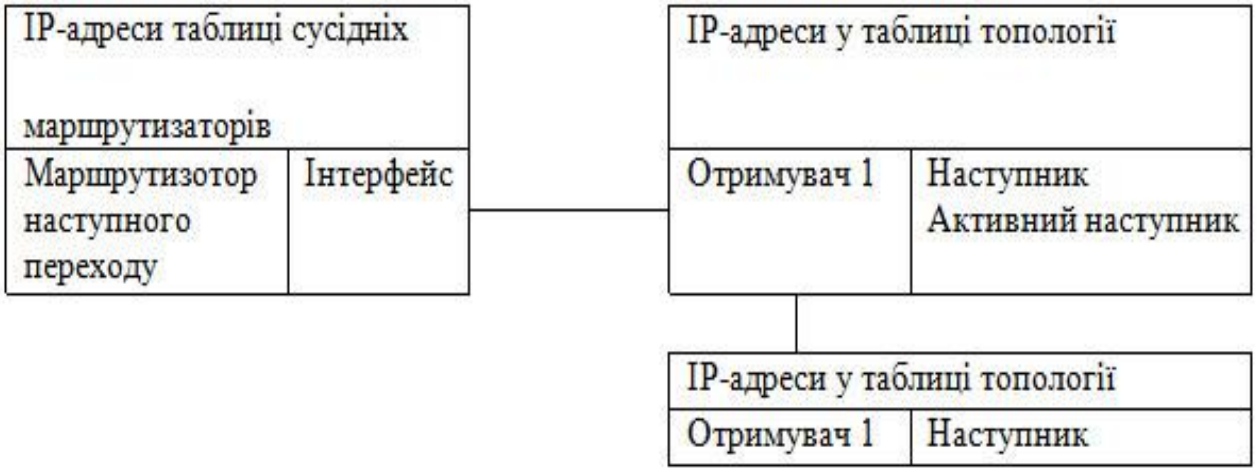


Рис. 7.19. Загальна схема роботи модуля *PDM*

Кожний модуль *PDM* відповідає за виконання всіх функцій, пов’язаних з відповідним мережним протоколом.

Зокрема, модуль *IP-EIGRP* відповідає за виконання таких функцій:

- відправлення та одержання інформації протоколу *EIGRP*, що містить дані протоколу *IP*;
- повідомлення алгоритму *DUAL* про одержання нової інформації, що стосується *IP*-маршрутизації;
- підтримка результатів прийнятих алгоритмом *DUAL* рішень про маршрутизацію в таблиці *IP*-маршрутизації;
- подальше поширення інформації про маршрути, яка стала відома іншим протоколам маршрутизації, що підтримують *IP*.

Протокол *EIGRP* використовує кілька різних типів пакетів для підтримки різних своїх таблиць і встановлення складних (комплексних) зв'язків із сусідніми маршрутизаторами. Існують п'ять типів пакетів протоколу *EIGRP*:

- *пакети вітання (Hello);*
- *пакети підтвердження (Acknowledgment);*
- *пакети відновлення маршрутів (Update);*
- *пакети запитів (Query);*
- *пакети відповідей на запити (Reply).*

Пакети вітання

Протокол *EIGRP* використовує пакети вітання для виявлення сусідніх маршрутизаторів, їх тестування та повторного виявлення після збоїв. Повторне виявлення відбувається в тому випадку, якщо маршрутизатори не одержують один від одного пакетів вітання протягом часу утримання, але пізніше поновлюють зв'язок.

Маршрутизатори *EIGRP* розсилають пакети вітання з фіксованим інтервалом (задається у файлі конфігурації), який називається інтервалом розсилання вітання *(hello interval).*

Прийнятий за замовчуванням інтервал вітання залежить від ширини смуги пропускання інтерфейсу. Для відправлення пакетів вітання протокол *EIGRP* використовує багатоадресне розсилання.

Таблиця *7.4. Залежність інтервалу вітання від ширини смуги пропускання каналу*

Ширина смуги пропускання	Тип каналу	Інтервал вітання за замовчуванням	Час утримання за замовчуванням
Менше або дорівнює 1,544 Мбіт/с	Протокол *Multipoint Frame Relay*	60 секунд	180 секунд
Більше 1,544 Мбіт/с	Лінія T1, з'єднання «точка-точка»	5 секунд	15 секунд

Маршрутизатор протоколу *EIGRP* зберігає інформацію про сусідні пристрої у *ТСП.* В ній для кожного сусіднього пристрою є поле послідовного номера, у якому записується номер останнього отриманого від цього пристрою пакета протоколу *EIGRP*.

Іншим полем *ТСП* є поле часу утримання, в якому записується час одержання останнього пакета. Для того, щоб у сусіднього маршрутизатора зберігався статус пасивного (досяжного і працездатного) необхідно, щоб за час утримання від нього надійшов хоча б один пакет. В протилежному випадку протокол *EIGRP* розглядає цей сусідній маршрутизатор як непрацездатний і алгоритм *DUAL* починає перераховувати *ТМ*. Стандартно час утримання втричі більший інтервалу вітань, однак, адміністратор може зконфігурувати обидва таймери.

У протоколі *EIGRP* (на відміну від *OSPF*) для здійснення зв'язку відсутня умова рівності значень інтервалів вітання й блокування на сусідніх маршрутизаторах. При цьому останні дізнаються про інтервали таймерів з пакетами вітання і використовують дану інформацію для встановлення стійкого зв'язку незважаючи на різні інтервали таймерів.

Пакети вітання завжди розсилаються методом негарантованого доставлення і не вимагають підтвердження.

Пакети підтвердження

Маршрутизатор *EIGRP* використовує пакети підтвердження для того, щоб повідомити інші маршрутизатори про одержання ним пакета *EIGRP* протягом сеансу „надійного" обміну даними.

Надійний транспортний протокол може забезпечити надійний зв'язок між вузлами *EIGRP*.

Для забезпечення гарантованого доставлення, вузол що приймає повинен підтвердити отримання повідомлення від джерела. Для цього використовуються пакети підтвердження (які можна назвати пакетами вітання „без даних").

На відміну від багатоадресних пакетів вітання, ці пакети є одноадресними. Підтвердження також може бути здійснене шляхом суміщення передавання

прямих і зворотних пакетів інших типів пакетів *EIGRP*, таких як пакети відповідей на запити.

Пакети відновлень маршрутів

Пакети відновлень маршрутів використовуються в тих випадках, коли маршрутизатор виявляє новий сусідній пристрій.

Тоді маршрутизатор *EIGRP* надсилає одноадресні пакети відновлення маршрутів цьому новому сусідньому пристрою для того, щоб він міг додати цю інформацію у свою *TT*. Для передавання новому сусідньому пристрою всієї топологічної інформації може знадобитись більше одного пакета.

Пакети відновлення використовуються також коли маршрутизатор виявляє зміну топології мережі, тоді він надсилає багатоадресні пакети відновлення усім своїм сусідам, попереджаючи їх про таку зміну. Всі пакети відновлення розсилаються методом гарантованого доставлення.

Пакети запитів і відповідей на запити

Маршрутизатор протоколу *EIGRP* використовує пакети запитів щоразу, коли йому потрібна конкретна інформація від будь-якого зі своїх сусідніх пристроїв. Пакет відповіді використовується для відповіді на запит.

Якщо у маршрутизатора *EIGRP* зникає первинний маршрут і він не може знайти резервного, то алгоритм *DUAL* переводить маршрут в активний стан. Після цього маршрутизатор виконує багатоадресне розсилання запиту всім своїм сусідам для знаходження первинного маршруту. Сусідні пристрої повинні надіслати відповіді на запити, в яких або надається інформація про первинний маршрут, або повідомляється про відсутність у них такої інформації.

Запити можуть бути як багато-, так і одноадресними, у той час як відповіді на запити завжди є одноадресними. Обидва типи пакетів розсилаються методом гарантованого доставлення.

7.8. Протокол OSPF

Протокол *OSPF (Open Shortest Path First)* є протоколом маршрутизації за станом каналів, що базується на відкритих стандартах. Він описаний в декількох стандартах інженерної групи *Internet (Internet Engineering Task Force – IETF)*, останнім з яких є стандарт *RFC 2328*. Термін „відкритий" в протоколі *OSPF* означає його доступність всім користувачам.

Протокол *OSPF* - це надійний, масштабований та ефективний протокол, який може бути використаний в окремій зоні у невеликих *КМ* і в кількох зонах для великих *КМ*.

Маршрутизація OSPF може бути розширена на великі мережі за умови, що під час проектування *КМ* використовувались ієрархічні принципи її побудови, які полягають у під'єднанні кількох зон до зони розподілення (нульової зони), яку також називають магістраллю. Таке проектування дозволяє здійснювати повний контроль над повідомленнями про оновлення маршрутів. Завдання зон зменшує об'єм службового навантаження маршрутизації, прискорює збіжність, обмежує можливу нестабільність мережі однією зоною та підвищує продуктивність мережі.

Протокол *OSPF* функціонує не так як дистанційно-векторні протоколи. Маршрутизатори ідентифікують сусідні маршрутизатори та обмінюються з ними інформацією. У протоколу *OSPF* є свій набір термінів [7].

Інформація, зібрана від сусідніх маршрутизаторів *OSPF* не є повною *ТМ*. Кожен *OSPF*-маршрутизатор повідомляє своїм сусідам про стан своїх зв'язків або каналів. Ця інформація розповсюджується методом лавинного розсилання. Під цим поняттям розуміється відправлення однієї і тієї ж інформації з усіх портів, за виключенням того, на який вона надійшла. Маршрутизатор *OSPF* оголошує стан своїх каналів та передає далі отриману ним інформацію про стани каналів інших маршрутизаторів.

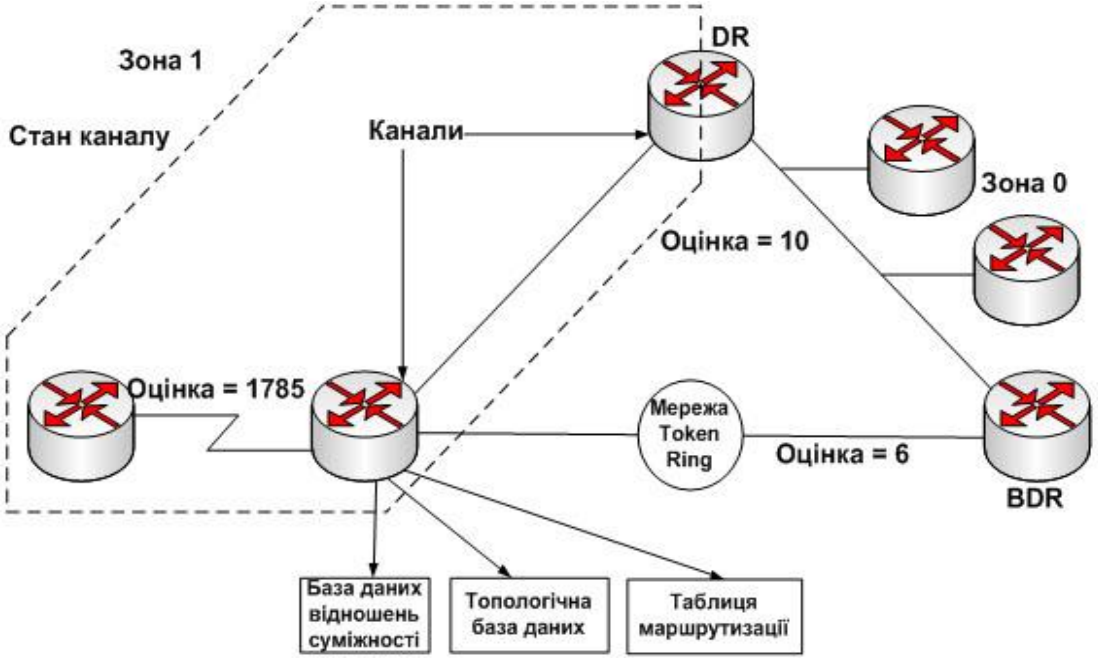


Рис. 7.20. Метод лавинного розсилання

Маршрутизатори в зоні 1 обробляють цю інформацію та будують свою топологічну *БД*, яку називають також *БД* стану каналів. Всі маршрутизатори в одній *OSPF*-зоні мають одну й ту ж *БД* стану каналів. Автономна система може бути розділена на ряд зон, що являють собою групи зв'язних (неперервних) мереж і під'єднаних до них пристроїв. Маршрутизатори з кількома інтерфейсами можуть бути учасниками кількох зон – їх називають граничними маршрутизаторами зон (*Area Border Routers*). Вони підтримують окремі топологічні *БД* для кожної зони.

Після цього кожен маршрутизатор застосовує алгоритм вибору найкоротшого шляху *SPF*, який також називають алгоритмом *Дейкстри,* до своєї бази даних. Ці обчислення визначають найкращий шлях до пункту призначення. Алгоритм *SPF* додає вартості (оцінки) для окремих переходів, які зазвичай базуються на ширині смуги пропускання. Мінімальна оцінка маршруту додається до *TM*, що також називається таблицею пересилання.

OSPF-маршрутизатори записують інформацію про своїх сусідів в *ТСП*. Для зменшення об'єму інформації, якою обмінюються сусідні пристрої в одній мережі, маршрутизатори *OSPF* обирають призначений маршрутизатор (*Designated Router*,

DR) та резервний призначений маршрутизатор (*Backup Designated Router, BDR*), які служать точками централізації при обміні інформацією маршрутизації [6].

OSPF-маршрутизатори встановлюють зв’язки або стани *(states)* зі своїми сусідами для ефективного сумісного використання інформації канального рівня.

Формат пакета OSPF

Існує п'ять типів *OSPF*-пакетів. Все *OSPF*-пакети починаються зі стандартного 24-байтного заголовка.

Version	Type	Packet Length
Router ID		
Area ID		
Checksum		Autype
Authentication		
Authentication Data		

Рис. 7.21. Заголовок пакету OSPF

Version (1 байт). Поле означає номер версії OSPF-пакета протоколу, що використовує даний пакет.

Type (1 байт). Залежно від типу, пакет виконує ті чи інші функції:

Packet Length (16 біт). Поле довжини пакета (в байтах) разом зі стандартним заголовком.

RouterlD (32 біта). Поле ідентифікатора відправника.

ArealD (32 біта). Поле ідентифікує область, до якої належить даний пакет.

Checksum (16 біт). Поле контрольної суми пакета.

Authentication (16 біт). Поле типу аутентифікації. Наприклад, "простий пароль". Всі обміни протоколу OSPF проводяться з аутентифікацією відправника і його прав. Тип аутентифікації встановлюється за принципом "окремий для кожної області".

Authentication data (64 біта). Поле містить інформацію аутентифікації.

Таблиця 7.5. *Тип пакетів протоколу OSPF*

Тип пакета протоколу OSPF	
Тип 1 - *Hello*	Використовується для створення та підтримки таблиці сусідних пристроїв
Тип 2 – Пакет опису бази даних (*Database description packet, DBD*)	Описує вміст бази даних стану каналів *OSPF*-маршрутизатора
Тип 3 – Запит інформації про стан каналів (*Link-state requests – LSR*)	Здійснює запит окремих фрагментів бази даних стану каналів маршрутизатора
Тип 4 – оновлення стану каналів (*Link-state update, LSU*)	Передає повідомлення про стан каналів (*Link-state advertisements, LSA*) сусіднім маршрутизаторам
Тип 5 – Підтвердження отримання повідомлення про стан каналів (*Link-state acknowledgement, LSAck*)	Підтверджує отримання від сусіднього пристрою повідомлення *LSA*

Ключовим фактором при проектуванні *OSPF*-мереж та при усуненні помилок в них є розуміння зв’язків або станів, які виникають між *OSPF*-маршрутизаторами. Інтерфейси *OSPF*-маршрутизаторів можуть знаходитися в одному з наведених нижче семи станів. Зв’язки між сусідніми маршрутизаторами послідовно проходять ці стани зверху вниз:

- *вимкнений стан (Down State);*
- *ініціалізація (Init State);*
- *двостороннє з’єднання (Two-way);*
- *ExStart;*
- *обмін (Exchange);*
- *завантаження (Loading);*

• *стан встановлення повного зв'язку між сусідніми (суміжними) пристроями (Full adjacency).*

Вимкнений стан

Вимкнений стан має місце, коли обмін інформацією між сусідніми пристроями не відбувався. Маршрутизатори очікують переходу в наступний стан – стан ініціалізації.

Стан ініціалізації

В стані ініціалізації *OSPF*-маршрутизатори регулярно (зазвичай 10 секунд) відсилають пакети першого типу (*Hello*) для встановлення зв'язку з сусідніми маршрутизаторами. Коли деякий інтерфейс отримує перший *Hello*-пакет, відповідний маршрутизатор переходить в стан ініціалізації. Це означає, що маршрутизатору відомо про наявність у нього сусіднього пристрою і він чекає переходу зв'язку з ним в наступний стан.

Існує два типи зв'язку між маршрутизаторами: двосторонній зв'язок та стан повного зв'язку сусідніх пристроїв, хоча між цими двома станами і знаходяться декілька проміжних станів. Перед тим, як стане можливим встановлення будь-якого типу зв'язку, маршрутизатор повинен отримати від свого сусіда повідомлення *Hello*.

Стан ExStart

В технічному аспекті в момент, коли маршрутизатор та його сусідній пристрій входять у стан *ExStart*, їх зв'язок характеризується як стан суміжності, однак, в дійсності ці пристрої ще не є повністю суміжними. Стан *ExStart* встановлюється за допомогою пакетів опису бази даних (*DBD*). Для обговорення того, який маршрутизатор в даному з'єднанні буде головним (*master*), а який підлеглим (*slave)*, маршрутизатори використовують пакети *Hello*, а для обміну вмістом *БД* використовуються пакети *DBD.*

Маршрутизатор з максимальним значенням *OSPF*-ідентифікатора (*ID*) стає головним. Коли два сусідніх маршрутизатора визначають свої ролі як головного та підлеглого, вони входять у стан обміну (*Exchange*) та починають надсилати один одному інформацію маршрутизації.

Стан обміну

В стані обміну сусідні маршрутизатори використовують пакети *DBD* для відправлення один одному своєї інформації про стан каналів.

Іншими словами маршрутизатори описують один одному свої *БД* стану каналів. При цьому маршрутизатори порівнюють отриману інформацію з тією, що міститься в їх власних *БД* стану каналів.

Якщо будь-який з маршрутизаторів отримує інформацію про канал, яка відсутня в його *БД* – він запитує у сусіднього маршрутизатора повне оновлення.

Повний обмін інформації відбувається в стані завантаження (*Loading)*.

Стан завантаження

Після того, як обидва маршрутизатора описали один одному свої *БД*, вони можуть запитати більш повну інформацію, використовуючи пакети запиту стану каналів (*LSR*). Коли маршрутизатор отримує запит *LSR,* він відповідає відправкою оновлення маршрутизації, використовуючи пакет оновлення стану каналів (*LSU*). Ці *LSU*-пакети містять оголошення актуального стану каналів (*LSA*), які складають сутність протоколів маршрутизації стану каналів. Підтвердження отримання *LSU*-пакетів здійснюється за допомогою пакетів підтвердження стану каналів (***LSAck***).

Стан повної суміжності

Після того, як повністю реалізований стан завантаження, маршрутизатори повністю суміжні. Кожен маршрутизатор підтримує свій список суміжних сусідніх маршрутизаторів (*БД* суміжних пристроїв).

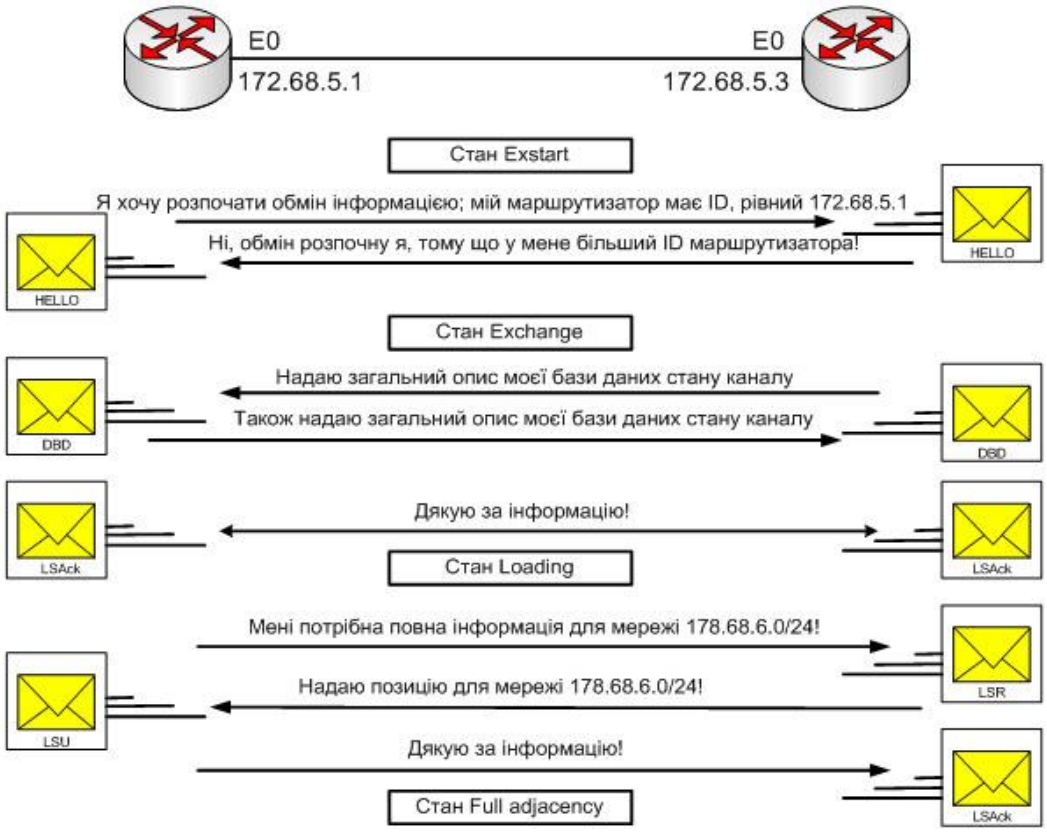


Рис. 7.22. Виявлення маршрутизатора за протоколом OSPF

Бази даних протоколу OSPF

Таблиця 7.6. *Бази даних протоколу OSPF*

База даних	Опис
База суміжних пристроїв	Список усіх сусідніх пристроїв, з якими даний маршрутизатор встановив двосторонні зв’язки
База даних стану каналів або топологічна база даних (Link State Data Base)	Інформація про усі маршрутизатори мережі. Ця база даних відображає поточну мережеву топологію. Усі маршрутизатори однієї і тієї ж області мають ідентичні бази даних канального рівня
База даних пересилання або таблиця	Список маршрутів, що генерується при виконанні алгоритма над топологічною базою даних. Таблиця маршрутизації кожного маршрутизатора унікальна та

маршрутизації (Routing Table)	містить інформацію про те, яким чином і за якими маршрутами слід направляти пакети призначені іншим маршрутизаторам

Основи функціонування протоколу OSPF

Для того, щоб сумісно використовувати інформацію про маршрутизацію, *OSPF*-маршрутизатори повинні встановити зв'язок з сусідним.

Кожен маршрутизатор намагається встановити відношення суміжності або сусідства хоча б з одним маршрутизатором кожної *IP*-мережі, до якої під'єднані усі його порти. Деякі маршрутизатори можуть намагатися встановити відношення суміжності з усіма сусідніми маршрутизаторами, в той час як інші – тільки з одним або двома.

OSPF-маршрутизатори визначають, з якими іншими маршрутизаторами їм слід встановити відношення суміжності, на основі типу мережі, яка їх поєднує.

Для визначення найкращого шляху до пункту призначення протокол *OSPF* використовує алгоритм вибору найкоротшого маршруту (тобто маршруту з найменшою оцінкою).

Цей алгоритм було розроблено голандським комп'ютерним спеціалістом *Дейкстра (Dijkstra)* та опубліковано у 1959 році.

В цьому алгоритмі *КМ* розглядається як множина вузлів, що з'єднані між собою каналами типу *„точка-точка"*.

Кожному каналу присвоюється деяке значення оцінки, а кожному вузлу - деяке ім'я. Кожен вузол має повну *БД* всіх каналів, тому всім вузлам відома вся інформація про фізичну топологію мережі.

Після цього алгоритм вибору найкоротшого шляху обчислює вільну від петель топологію, використовуючи даний вузол як початкову точки та послідовно аналізуючи його інформацію про суміжні вузли.

Після того, як між сусідніми пристроями встановлені відношення суміжності, між ними відбувається обмін інформацією про стан каналу.

Інтерфейси *OSPF*-маршрутизаторів розпізнають три типи мереж:

1. Широкомовні мережі множинного доступу.

2. Нешироковмовні мережі множинного доступу (nonbroadcast multi-access – NBMA).

3. Мережі з каналами типу „точка-точка” .

Типи OSPF-мереж

Мережевий адміністратор може сконфігурувати на будь-якому типі інтерфейсу і четвертий тип мереж – мережа типу „точка – декілька точок” [7].

В мережі множинного доступу (*multiaccess network*) неможливо заздалегідь знати, скільки маршрутизаторів буде з’єднано.

В мережах типу „точка-точка” (*point-to-point*) можуть бути з’єднані тільки два маршрутизатори. Якщо всі маршрутизатори встановлять відношення суміжності з усіма іншими і будуть обмінюватися інформацією про стан каналів, то об’єм службових повідомлень стане занадто великим.

Проблема великого об’єму службових повідомлень, може бути вирішена вибором призначеного маршрутизатора .

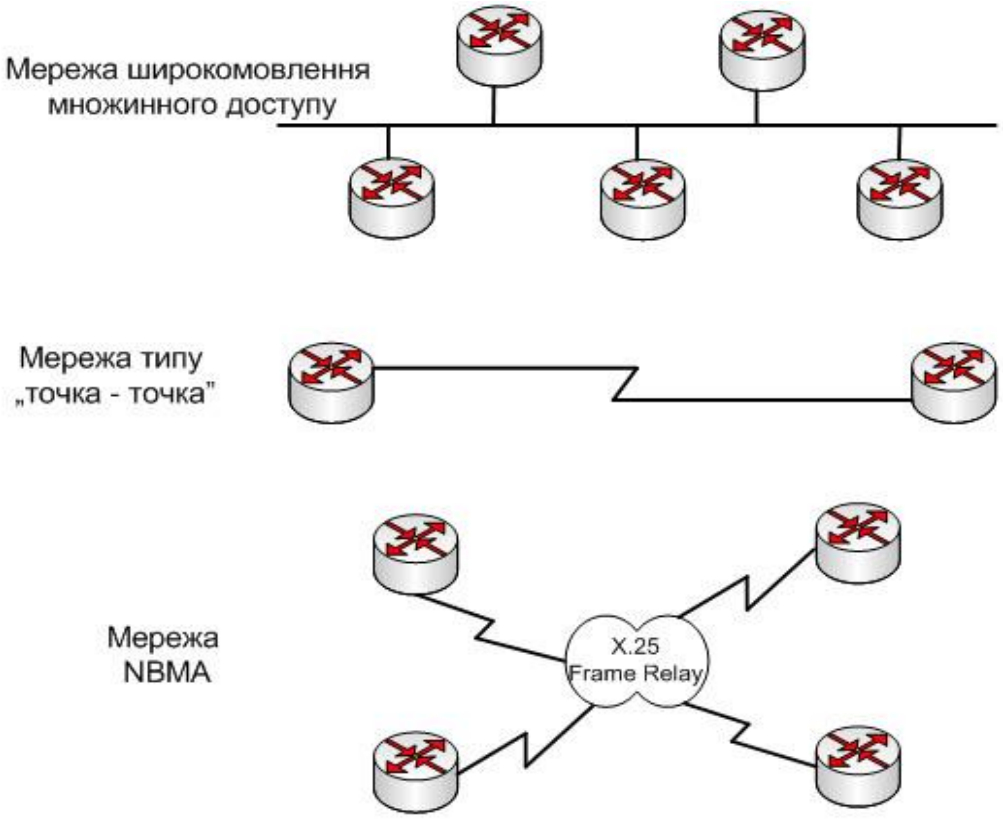


Рис. 7.23. Типи OSPF-мереж

Виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR)

Цей призначений маршрутизатор (*DR*) стає суміжним пристроєм для всіх маршрутизаторів широкомовного сегмента.

Всі інші маршрутизатори цього сегмента надсилають інформацію про стан каналу до *DR*, який стає джерелом інформації для даного сегмента і розсилає інформацію про стан каналів всім іншим маршрутизаторам сегмента, використовуючи адресу багатоадресного розсилання *224.0.0.5* для всіх *OSPF*-маршрутизаторів.

Незважаючи на підвищення ефективності роботи *КМ*, яке забезпечується використанням *DR*, в даному підході є й недолік – *призначений маршрутизатор являє собою точку, від якої залежить робота всього сегмента і у випадку виходу його з ладу весь сегмент припиняє працювати.* Тому вибирається також резервний призначений маршрутизатор (*BDR*), який приймає на себе виконання функцій

призначеного маршрутизатора у випадку відмови останнього. Для того, щоб обоє маршрутизатори *DR* та *BDR* отримували всі повідомлення про стан каналу, які надсилаються в сегмент, використовується адреса багатоадресого розсилання 224.0.0.6.

Маршрутизатор стає *DR*, якщо він має найвищий (найбільший) пріоритет інтерфейсу (*OSPF interface priority*), маршрутизатор з другим за величиною пріоритетом стає *BDR*. Якщо значення цих пріоритетів однакові (а за замовчуванням вони однакові і дорівнюють одиниці) - враховується найбільша *IP*-адреса маршрутизатора. Ідентифікатором маршрутизатора стає найбільша *IP*-адреса *Loopback*-інтерфейсу або, якщо *Loopback*-інтерфейс не налаштований – то до уваги береться ідентифікатор маршрутизатора (*Router ID*). Маршрутизатор з найбільшим значенням *ID* стає *DR*, а з другим за величиною пріоритетом – *BDR*.

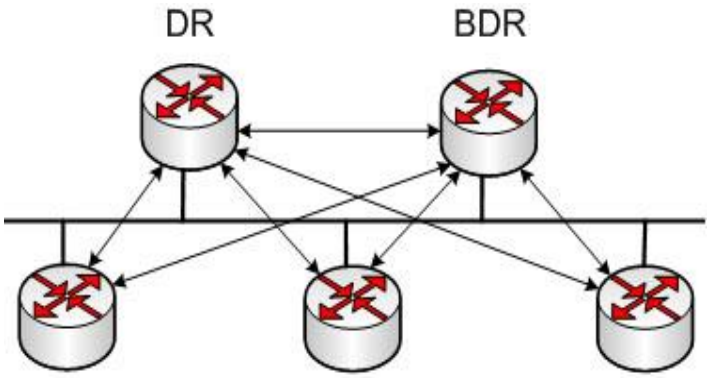


Рис. 7.24. Виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR)

7.9. Протокол BGP

Загальна схема роботи ***BGP*** така. *BGP*-маршрутизатори сусідніх АС, які вирішили обмінюватися маршрутною інформацією, встановлюють між собою з'єднання по протоколу *BGP* і стають *BGP*-сусідами (*BGP-peers*).

Далі *BGP* використовує підхід під назвою *path vector*, який є розвитком дистанційно-векторного підходу. *BGP*-сусіди розсилають (анонсують, *advertise*)

один одному вектори шляхів (*path vectors*). Вектор шляхів, на відміну від вектора відстаней, містить не просто адреса мережі та відстань до неї, а адреса мережі та список атрибутів (*path attributes*), що описують різні характеристики маршруту від маршрутизатора-відправника в зазначену мережу. Надалі для стислості ми будемо називати набір даних, що складаються з адреси мережі і атрибутів шляху до цієї мережі, маршрутом в дану мережу.

Даних, що містяться в атрибутах шляху, має бути достатньо, щоб маршрутизатор-одержувач, проаналізувавши їх з точки зору політики своєї *AC*, міг прийняти рішення про прийнятність або неприйнятність отриманого маршруту.

Пара *BGP*-сусідів встановлює між собою з'єднання по протоколу *TCP*, порт 179. Сусіди, що належать різним *AC*, повинні бути доступні один одному безпосередньо; для сусідів з однієї *AC* такого обмеження немає, оскільки протокол внутрішньої маршрутизації забезпечить наявність всіх необхідних маршрутів між вузлами однієї автономної системи.

Потік інформації, яким обмінюються *BGP*-сусіди по протоколу *TCP*, складається з послідовності *BGP*-повідомлень. Максимальна довжина повідомлення 4096 октетів, мінімальна - 19. Є 4 типи повідомлень.

Формат BGP-повідомлення

Повідомлення протоколу *BGP* складається з заголовка і тіла. Тема має довжину 19 октетів і складається з наступних полів:

- маркер: в повідомленні OPEN завжди, і при роботі без аутентифікації в інших повідомленнях заповнений одиницями. Інакше містить аутентифікаційну інформацію. Супутня функція маркера - підвищення надійності виділення кордону повідомлення в потоці даних.
- довжина повідомлення в октетах, включаючи заголовок.
- тип повідомлення:

1 – OPEN

2 – KEEPALIVE

3 – UPDATE

4 – NOTIFICATION

OPEN - надсилається після встановлення *TCP*-з'єднання. Відповіддю на *OPEN* є повідомлення *KEEPALIVE*, якщо друга сторона згодна стати *BGP*-сусідом; інакше надсилається повідомлення *NOTIFICATION* з кодом, що пояснюють причину відмови, і з'єднання розривається.

KEEPALIVE - повідомлення призначене для підтвердження згоди встановити сусідські відносини, а також для моніторингу активності відкритого з'єднання: для цього *BGP*-сусіди обмінюються *KEEPALIVE*-повідомленнями через певні інтервали часу.

UPDATE - повідомлення призначене для анонсування та відкликання маршрутів. Після встановлення з'єднання за допомогою повідомлень UPDATE пересилаються всі маршрути, які маршрутизатор хоче оголосити сусідові (*full update*), після чого пересилаються тільки дані про доданих або видалених маршрутах у міру їх появи (*partial update*).

NOTIFICATION - повідомлення цього типу використовується для інформування сусіда про причини закриття з'єднання. Після відправлення цього повідомлення *BGP*-з'єднання закривається.

Контрольні питання до розділу

1. Алгоритми маршрутизації можуть бути класифіковані за типами:
    a. *Статичними або динамічними;*
    b. *Двомаршрутними або багатомаршрутними;*
    c. *Однорівневими або ієрархічними;*
    d. *З інтелектом у сервері або в маршрутизаторі*
    e. *Внутрідоменними і міждоменними;*
    f. *Алгоритмами стану відстаней або вектора каналу.*
2. При розробці алгоритмів маршрутизації часто переслідують одну або декілька з перерахованих нижче цілей:
    a. *Оптимізація;*
    b. *Простота і низькі непродуктивні витрати;*
    c. *Живучість і стабільність;*
    d. *Повільна збіжність;*
    e. *Гнучкість.*
3. Поясніть сутність багатомаршрутних алгоритмів маршрутизації?
4. Що собою представляють динамічні алгоритми маршрутизації?
5. Поясніть особливості алгоритму маршрутизації стану каналу?

6. Показники, які використовуються в алгоритмах маршрутизації:
    a. *довжина маршруту;*
    b. *гнучкість;*
    c. *затримка;г).ширина смуги пропускання;*
    d. *живучість;*
    e. *вартість зв'язку.*
7. Що собою представляють статичні алгоритми маршрутизації?
8. Поясніть особливості алгоритмів маршрутизації вектора відстані?
9. Поясніть відмінності між алгоритмами маршрутизації з інтелектом у головній обчислювальній машині або в роутері?
10. Протокол, який реалізує алгоритм маршрутизації:
    a. *Interior Gateway Routing Protocol (IGRP)*
    b. *Open Shortest Path First (OSPF)*
    c. *Intermediate System to Intermediate System (IS-IS)*
    d. *Routing Information Protocol (RIP)*
    e. *Border Gateway Protocol (BGP)*
    f. *Internet Control Message Protocol (ICMP)*
    g. *Internet Group Management Protocol (IGMP)*
    h. *Resource Reservation Protocol (RSVP)*
11. Що собою представляють однорівневі алгоритми маршрутизації?
12. Що представляє собою такий показник в алгоритмах маршрутизації як «надійність»?
13. Що представляє собою такий показник в алгоритмах маршрутизації як «затримка»?
14. Поясніть відмінності між однорівневими та ієрархічними алгоритмами маршрутизації?
15. Що представляє собою такий показник в алгоритмах маршрутизації як «навантаження»?
16. Алгоритми маршрутизації стану каналу та вектора відстані. Переваги та недоліки?
17. Поясніть призначення таблиці маршрутизації?
18. Що характеризує оптимальність при розробці алгоритму маршрутизації?
19. Що характеризує живучість і стабільність при розробці алгоритму маршрутизації?
20. Що характеризує швидка збіжність при розробці алгоритму маршрутизації?
21. Що таке петля маршрутизації і чому вона виникає в мережі?
22. Що характеризує гнучкість при розробці алгоритму маршрутизації?
23. Поясніть сутність одномаршрутних алгоритмів маршрутизації?
24. Які існують показники алгоритмів (метрики) маршрутизації?
25. Маршрутизація без таблиць поділяється на:
    a. *лавинну;*
    b. *керовану подіями;*
    c. *статичну;*
    d. *від джерела.*
26. Що собою представляє лавинна маршрутизація?

27. Що собою представляє маршрутизація, керована подіями?

28. Що собою представляє маршрутизація від джерела?

29. На які категорії поділяється більшість алгоритмів маршрутизації?

30. Що собою представляє автономна система?

31. В чому різниця між протоколом внутрішнього та зовнішнього шлюзу?

32. Наведіть переваги та недоліки статичної маршрутизації?

33. Наведіть переваги та недоліки динамічної маршрутизації?

34. Протокол RIP. Особливості застосування. Переваги та недоліки.

35. В яких випадках найкраще застосовувати протоколи LSA?

36. В яких протоколах маршрутизації використовуються алгоритм Беллмана-Форда?

37. Протокол EIGRP. Особливості застосування. Переваги та недоліки.

37. Протокол OSPF. Особливості застосування. Переваги та недоліки.

38. Яким чином проводиться перевірка і усунення помилок у конфігурації статичних маршрутів?

39. В чому полягає відмінність між протоколами RIPv1та RIPv2?

40. Які етапи побудови таблиці маршрутизації за допомогою протоколу RIPv1необхідні?

41. Які існують методи боротьби з фальшивими маршрутами в протоколі RIP?

42. Поясніть в чому полягає сутність такого методу боротьби з фальшивими маршрутами, як розщеплення горизонту?

43. Поясніть в чому полягає сутність такого методу боротьби з фальшивими маршрутами, як вилучення маршруту в зворотному напрямку?

44. Поясніть в чому полягає сутність такого методу боротьби з фальшивими маршрутами, як таймери утримання інформації?

45. Що собою представляє таблиця сусідніх пристроїв в протоколі EIGRP?

46. Що собою представляє топологічна таблиця в протоколі EIGRP?

47. Які існують типи OSPF-пакетів?

48. Які існують бази даних протоколу OSPF?

49. Які існують типи OSPF-мереж?

50. Яким чином призначаються виділений маршрутизатор (DR) і резервний виділений маршрутизатор (BDR) в мережі протоколу OSPF?

51. Поясніть принцип роботи протокол BGP?

Список рекомендованої літератури

1. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
2. *Новиков Ю. В., Кондратенко С. В.* Основы локальных сетей. Курс лекций. [Електронний ресурс] – М.: Интернет-университет информационных

технологий, 2005. – ISBN 5-9556-0032-9. Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/57/57/info.
3. *Шварц М.* Сети связи: протоколы, моделирование и анализ. Ч.1. – М.: Наука, 1992. – 336 с.
4. *Семенов Ю.А.* Алгоритмы и протоколы каналов и сетей передачи данных. Курс лекций. [Електронний ресурс] - М.: Интернет-университет информационных технологий, 2014. ISBN: 978-5-94774-706-5. Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/9/9/info
5. *Блэк Ю.* Сети ЭВМ: протоколы, стандарты, интерфейсы. – М.: Мир, 1990. – 506 с.
6. *Семенов Ю.А.* Протоколы и алгоритмы маршрутизации в Интернет. Курс лекций. [Електронний ресурс] - М.: Интернет-университет информационных технологий, 2011. ISBN: 978-5-94774-707-2. Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/1123/200/info
7. Комп'ютерні мережі [Електронний ресурс] : навчальний посібник для виконання лабораторних робіт для студ. спеціальності 126 «Інформаційні системи та технології»/ *Б. Ю. Жураковський; І.О. Зенів,* КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 10,08 Мбайт). – Київ : КПІ ім.Ігоря Сікорського, 2020. – 213 с.

Розділ 8. АДРЕСАЦІЯ В СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

8.1.Загальні принципи адресації у сучасних комп'ютерних мережах

Важливими питаннями функціонування сучасних комп'ютерних та телекомунікаційних мереж є питання, пов'язані з адресацією кінцевих вузлів та комунікаційних пристроїв, зокрема питання:

– забезпечення унікальності адрес у межах мережі;

– узгодження застосування адрес різних типів;

– конфігурування адрес мережних адаптерів/інтерфейсів та адрес мережних додатків.

Для ідентифікації мережних адаптерів/інтерфейсів у сучасних мережах застосовується три типи адрес:

– фізичні, локальні, апаратні адреси (Physical, Local, Hardware Addresses);

– логічні, мережні адреси (Logical, Network Addresses);

– символьні, текстові адреси (Symbolic, Text Addresses).

Фізичні або апаратні адреси – це адреси, які призначаються мережним адаптерам/інтерфейсам на етапі виробництва. Формально вважається, що ці адреси змінити не можливо. Прикладами апаратних адрес можуть бути MAC-адреси технологій Ethernet, Wi-Fi, BlueTooth тощо; IMEI-ідентифікатори мобільних пристроїв [1].

Логічні або мережні адреси – це змінні адреси, які призначаються мережним адаптерам/інтерфейсам адміністраторами систем з дотриманням певних логічних правил. Прикладами мережних адрес є IP-адреси версій 4 та 6 стеку TCP/IP, номери мобільних телефонів тощо.

Для забезпечення інформаційного обміну у сучасній мережі використовуються фізичні і логічні адреси. Проте з точки зору користувача звернення до ресурсів із використанням фізичних або логічних адрес є складним процесом, оскільки потребує запам'ятовування великої кількості цифрових комбінацій, а людині простіше запам'ятовувати текст. Тому для

полегшення роботи користувачів було введено ще один тип адрес – текстові адреси. Прикладами текстових адрес є доменні імена вузлів мережі Internet, Windows-імена комп'ютерів тощо.

Важливою проблемою адресації сучасних мереж є узгодження використання адрес різних типів, зокрема:

– встановлення і дотримання відповідностей між логічними і фізичними адресами;

– встановлення і дотримання відповідностей між текстовими і логічними адресами.

Схема встановлення відповідностей між текстовими, логічними та фізичними адресами на прикладі доменних імен глобальної мережі Інтернет, IP-адрес версії 4 та MAC-адрес технології Ethernet наведена на рис. 8.1. У даному випадку встановлення відповідностей між IP-адресами і MAC-адресами забезпечує протокол ARP, а встановлення відповідностей між доменними іменами і IP-адресами – система DNS.

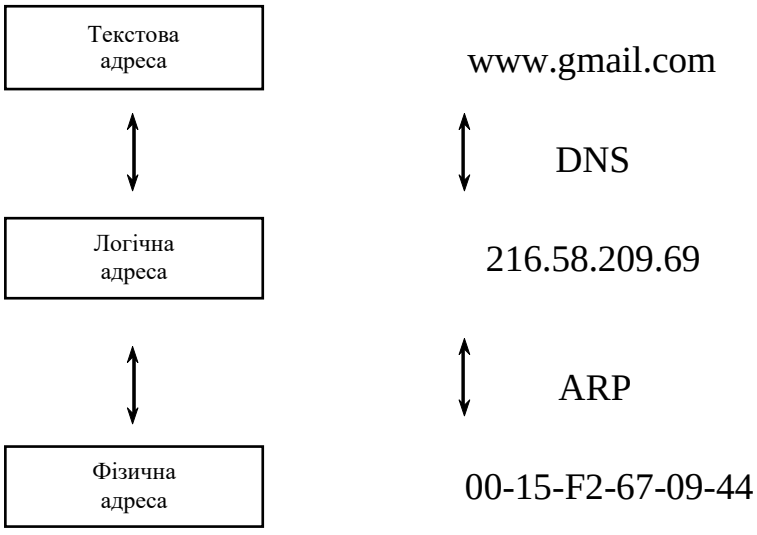


Рис. 8.1. Схема встановлення відповідностей між адресами різних типів

8.2.MAC-адреси та їх застосування у сучасних мережах

MAC-адреса (MAC-Address, Media Access Control Address) – унікальний числовий ідентифікатор, який призначається виробником мережному

адаптеру/інтерфейсу і застосовується у процесі передачі даних у межах окремого канального сегмента мережі. Досить часто як синонім терміна „MAC-адреса" застосовують термін „прошита адреса" (BIA, Burned-In Address). Стосовно моделі OSI MAC-адреса - це адреса канального рівня, тому іноді її називають канальною адресою. Стосовно стеку TCP/IP MAC-адреса – це адреса рівня ме- режних інтерфейсів [1].

Керування загальним адресним простором MAC-адрес здійснює Інститут інженерів електриків та електронників (IEEE, Institute of Electrical and Electronics Engineers). Увесь адресний простір розби- вається на три підпростори, які позначаються як MAC-48, EUI-48, EUI-64. Відмітності між MAC-48 і EUI-48 є номінальними: MAC-48 застосовується для ідентифікації мережних адаптерів/інтерфейсів, EUI-48 – для ідентифікації інших пристроїв та програм. EUI-64 є розширенням EUI-48 [2].

MAC-адреса має довжину 48 бітів (6 байтів). Як правило, відображення MAC-адреси здійснюється у шістнадцятковій формі числення. Існують три загальноприйняті формати запису MAC-адрес, які відрізняються групуванням байтів та роздільними знаками:

– формат запису IEEE EUI-48;

– формат запису Unix Zero-Padded;

– формат запису Cisco.

Приклади запису за вказаними форматами відповідно виглядають як: 0C-8B-FD-93-63-EB, 0c:8b:fd:93:63:eb, 0c8b.fd93.63eb. У деяких випадках запис MAC-адреси здійснюється без роздільників, як проста послідовність із шести байтів – 0C8BFD9363EBh.

Залежно від застосування MAC-адреса може бути ідентифікована як:

– унікальна MAC-адреса (Unicast MAC-Address);

– групова MAC-адреса (Multicast MAC-Address);

– широкомовна MAC-адреса (Broadcast MAC-Address).

У повідомленні (кадрі) унікальні MAC-адреси можуть зазначатися і як адреси відправника (Source MAC-Address), і як адреси отримувача (Destination MAC-Address). Групові і широкомовні MAC-адреси – лише як адреси

отримувача. MAC-адреса отримувача визначає, яким є кадр: унікальним, груповим чи широкомовним.

Структурно MAC-адреса містить два однакових за довжиною 24-бітних блоки:

– унікальний ідентифікатор виробника (OUI, Organizationally Unique Identifier);

– унікальна адреса адаптера/інтерфейсу (OUA, Organizationally Unique Address).

У старшому байті ідентифікатора виробника виділяється два біти, за допомогою яких визначається, якою є MAC-адреса: унікальною, груповою чи широкомовною. Це біти I/G (Individual/Group Bit) та G/L (Global/Local Bit). Біт G/L іноді позначають як U/L (Universal/Local Bit). Біт I/G – це ознака унікальної чи групової/широкомовної адреси, біт G/L – ознака глобальної чи локальної адреси [2].

Адресний простір MAC-48 контролюється IEEE таким чином, щоб забезпечити дотримання унікальності MAC-адрес. В одному канальному сегменті MAC-адреси повинні бути унікальними, оскільки використання однакових MAC-адрес призведе до неможливості здійснення інформаційного обміну.

Розподіл адресного простору MAC-48 здійснюється за простими правилами. Будь-який виробник мережних адаптерів/інтерфейсів подає заявку на отримання одного або діапазону унікальних OUI. Після отримання OUI на виробника покладається функція контролю унікальності OUA. Такий підхід теоретично повинен забезпечити унікальність усіх MAC-адрес.

Слід зазначити, що деякі OUI застосовуються для спеціальних цілей, зокрема для формування MAC-адрес отримувачів під час передавання повідомлень певних мережних протоколів. Це можуть бути як OUI виробників (наприклад, Cisco Systems), так і зарезервовані OUI (наприклад, IP-Multicast).

Перелік найбільш уживаних спеціалізованих MAC-адрес наведений у табл. 8.1.

Таблиця 8.1 *Перелік найбільш уживаних спеціалізованих MAC-адрес*

MAC-адреса	Протокол
01000CCCCCCC	CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), UDLD (Unidirectional Link Detection), DTP (Dynamic Trunking Protocol), PAgP (Port Aggregation Protocol)
01000CCCCCCD	VSTP (VLAN Spanning Tree Protocol)
0180C2000000	STP (Spanning Tree Protocol), RSTP (Rapid STP), MSTP (Multiple STP)
0180C2000001	Pause (Flow Control, MAC-Control)
0180C2000002	LACP (Link Aggregation Control Protocol) – EtherType 8809 Sub- type 01, LAMP (EtherType 8809 Subtype 02), Link OAM (Ether- Type 88-09 Subtype 03)
0180C2000003	Port Authentication 802.1x
0180C2000007	E-LMI (Ethernet Local Management Interface)
0180C2000008	Provider MSTP
0180C200000D	Provider MMRP
0180C2000000, 0180C2000003, 0180C200000E	LLDP (Link Layer Discovery Protocol)
0180C2000020– 0180C200002F	GARP (Generic Attribute Registration Protocol), GMRP (GARP Multi- cast Registration Protocol), GVRP(GARP VLAN Registration Protocol)
0180C2000020	MMRP (Multiple MAC Registration Protocol)
0180C2000021	MVRP (Multiple VLAN Registration Protocol)
01005E000000– 01005E7FFFFF	IPv4-Multicast (Групова розсилка протоколу IP версії 4)
3333xxxxxxxx	IPv6-Multicast (Групова розсилка протоколу IP версії 6)
011B19000000, 0180C200000E	PTP (Precision Time Protocol) version 2 over Ethernet (Layer-2)
FFFFFFFFFFFF	Широкомовна MAC-адреса

8.3.IP-адреси та їх застосування у сучасних мережах

IP-адреса (IP-Address, Internet Protocol Address) – унікальний числовий ідентифікатор, який призначається мережному адаптеру/інтерфейсу і застосовується у процесі передачі даних у межах як окремої локальної мережі, так і між різними підмережами глобальних мереж. Стосовно моделі OSI IP-адреса – це адреса мережного рівня, стосовно стеку TCP/IP – адреса рівня міжмережної взаємодії. Система IP-адресації є однією з базових складових сучасної мережі Інтернет.

Загальне керування адресним простором IP-адрес здійснює Адміністрація адресного простору Інтернет (IANA, Internet Assigned Numbers Authority), яка є підрозділом неприбуткової Інтернет- корпорації з призначення імен та адрес (ICANN, Internet Corporation for Assigned Names and Numbers). IANA підпорядковуються регіональні Інтернет-реєстратори (RIR, Regional Internet Registries), яким, у свою чергу, підпорядковуються локальні Інтернет-реєстратори (LIR, Local Internet Registries) – провайдери послуг Інтернет. Регіональні Інтернет-реєстратори розподіляють IP-адреси як між кінцевими користувачами, так і між локальним Інтернет-провайдерами. Слід зазначити, що на IANA/ICANN також покладається керування основними зонами системи DNS – системи встановлення відповідностей між IP-адресами та доменними іменами вузлів мережі Інтернет [3].

Перелік регіональних Інтернет-реєстраторів та території їх відповідальності наведено у табл. 8.2.

Таблиця 8.2 *Перелік регіональних Інтернет-реєстраторів та території їх відповідальності*

№ з/п	Регіональний Інтернет-реєстратор	Регіон
1	RIPE NCC, Réseaux IP Européens Network Coordination Centre	Європа, Близький Схід та Центральна Азія
2	ARIN, American Registry for Internet Numbers	Північна Америка
3	LACNIC, Latin American and Caribbean Internet Addresses Registry	Південна Америка та басейн Карибського моря
4	APNIC, Asia-Pacific Network Information Centre	Азійсько-Тихоокеанський регіон
5	AfriNIC, African Network Information Centre	Африка

Існують дві версії IP-адресації – версії 4 та 6. Основним стандартом, у якому описуються вимоги до IP-адрес версії 4, є прийнятий у вересні 1981 року стандарт RFC-791 „Internet Protocol. DARPA Internet Program Protocol Specification”. Основним стандартом, у якому описуються вимоги до IP-адрес версії 6, є прийнятий у грудні 1998 року стандарт RFC-2460 „Internet Protocol, Version 6 (IPv6) Specification”. Пізніше ці стандарти були доповнені іншими

стандартами RFC, що тією чи іншою мірою стосуються питань IP-адресації.

IP-адреса версії 4 має довжину 32 біти (4 байти). Як правило, запис IP-адреси версії 4 здійснюється побайтово у десятковій формі числення, і як роздільник байтів застосовується крапка. Такий запис називають десятково-крапковим форматом запису (Decimal-Dotted Notation). Іноді цей запис за кількістю байтів називають Quad-Dotted Notation. У деяких специфічних випадках запис IP-адреси версії 4 здійснюється у шістнадцятковій формі без роздільників.

Діапазон можливих IP-адрес версії 4 має вигляд: 0.0.0.0 – 255.255.255.255

У цьому діапазоні наявно 4294967296 (2^{32}) IP-адрес. Фактично, за рахунок певних правил та винятків, застосовується менша кількість адрес. Насправді доступних IP-адрес ще менше, оскільки частина з адрес мають спеціальне призначення.

Залежно від застосування IP-адреса версії 4 може бути ідентифікована як:

– унікальна IP-адреса (Unicast IP-Address);

– групова IP-адреса (Multicast IP-Address);

– широкомовна IP-адреса (Broadcast IP-Address).

У повідомленні (IP-пакеті) унікальні IP-адреси можуть зазнача- тися як адреси відправника (Source IP-Address), так і як адреси отримувача (Destination IP-Address). Групові і широкомовні IP- адреси можуть зазначатися лише як адреси отримувача. IP-адреса отримувача визначає яким є IP-пакет: унікальним, груповим чи широкомовним.

Структурно IP-адреса версії 4 складається з двох частин – одна частина (ліворуч) містить IP-адресу (номер) мережі, до якої нале- жить вузол, інша (праворуч) – IP-адресу (номер) вузла в цій мережі.

Поділ IP-адреси версії 4 на частини здійснюється з використан- ням двох підходів:

– класовий, класова IP-адресація (Classful IP-Addressing);

– безкласовий, безкласова IP-адресація (Classless IP-Addressing).

– *Класова IP-адресація* (класовий підхід) була розроблена як основна система адресації на початковому етапі розвитку мережі Internet. Інтенсивний

розвиток мережі поставив перед фахівцями основну проблему класового підходу до IP-адресації – неефективне використання адресного простору, наслідком якого став дефіцит IP-адрес. Організації, що підключалися до мережі, у багатьох випадках отримували IP-адреси мереж, адресні діапазони яких використовувалися у межах 10 – 20%. Саме потреба економного використання адресного простору і призвела до необхідності розробки безкласового підходу до IP-адресації. Основним завданням, яке необхідно було ви- рішити фахівцями у ході розробки нової системи адресації, було збереження сумісності з класовою IP-адресацією. Тому базові принципи, що були покладені в основу класової адресації, збереглися і в безкласовій IP-адресації [4].

Безкласова адресація розв'язала проблему дефіциту IP-адрес на період, менший, ніж десять років. Подальше стрімке зростання мережі Інтернет зумовило потребу значного розширення адресного простору. Фахівцями було запропоновано йти двома шляхами. Перший із них – розробка механізмів та засобів розширення адресного простору існуючої системи IP-адресації версії 4, другий – перехід до нової системи IP-адресації.

Розширення адресного простору існуючої системи IP-адресації версії 4 було здійснено за рахунок упровадження спеціальної технології заміни адрес NAT (Network Address Translation). Дана технологія і нині широко застосовується і розвивається.

Перехід на нову систему IP-адресації, яка отримала назву IP- адресація версії 6, був здійснений у межах розробки нової, більшпродуктивної та ефективної версії протоколу IP – версії 6. Довжину IP-адреси версії 6 було збільшено до 128 бітів, що надало можливість позбутися проблеми дефіциту IP-адрес на тривалий період.

8.4.Класова IP-адресація

У класовому підході діапазон можливих IP-адрес поділяється на п'ять класів. У кожному з класів формуються діапазони IP-адрес мереж за

правилами, які визначають структуру адреси та структуру старшого її байта (табл. 8.3).

Таблиця 8.3 *Правила формування класів IP-адрес*

Клас	Правило I (структу- ра IP- адреси)	Правило II (структура старшого байта)				
		Значення двійкове			Значення десяткове	
		Загальний вигляд	Мінімальне	Максимальне	Мінімальне	Максимальне
A	N.H.H.H	0xxxxxxx	00000000	01111111	0	127
B	N.N.H.H	10xxxxxx	10000000	10111111	128	191
C	N.N.N.H	110xxxxx	11000000	11011111	192	223
D	Multicast	1110xxxx	11100000	11101111	224	239
E	Reserved	11110xxx	11110000	11110111	240	247

Примітка: *N*, Network – байт(и) IP-адреси мережі; *H*, Host – байт(и) IP-адреси вузла.

Правило I визначає структуру адреси, тобто показує, яка частина IP-адреси є IP-адресою (номером) мережі та яка частина – IP-адресою (номером) вузла. У класі A на IP-адресу мережі виділяється один байт, а на IP-адресу вузла – три байти. У класі B як на IP-адресу мережі, так і на IP-адресу вузла виділяється по два байти. У класі C на IP-адресу мережі виділяється три байти, а на IP-адресу вузла – один байт. IP-адреси класу D застосовуються як групові. IP-адреси класу E зарезервовані для експериментального використання. На практиці застосовуються адреси всіх класів, крім класу E.

Правило II стосується лише старшого байта. За його допомогою формується і відображається структура цього байта у двійковій формі для кожного класу. Правило II дає змогу сформувати різні за розміром діапазони IP-адрес мереж, що належать певним класам.

Інформацію про діапазони IP-адрес мереж відповідних класів та їх кількісні параметри наведено у табл. 8.4. Слід зазначити, що у ході формування діапазону класу A дві IP-адреси мереж були вилучені. Під час формування класу E було вилучено діапазон 248.0.0.0 – 255.255.255.255. Інформацію про згадані IP-адреси вилучення та їх призначення наведено у табл. 8.5.

Таблиця 8.4 *Класи IP-адрес*

Клас	Мінімальна IP-адреса мережі	Максимальна IP-адреса мережі	Кількість IP-мереж	Кількість IP-адрес вузлів у мережі
A	**1**.0.0.0	**126**.0.0.0	126 (2^7–2)*	16777214 (2^{24}–2)**
B	**128.0**.0.0	**191.255**.0.0	16384 (2^{14})	65534 (2^{16}–2)**
C	**192.0.0**.0	**223.255.255**.0	2097152 (2^{21})	254 (2^8–2)**
D	224.0.0.0	239.255.255.255	–	–
E	240.0.0.0	247.255.255.255	–	–

Примітка: * – дві IP-адреси мереж класу A (0.0.0.0 та 127.0.0.0) вилучено із звичайного застосування; ** – дві IP-адреси з діапазону окремої мережі (нульова й остання) зарезервовані для спеціальних цілей і не можуть бути призначені вузлам: нульова IP-адреса – це IP-адреса мережі; остання IP-адреса – це широкомовна IP-адреса мережі.

Таблиця 8.5 *IP-адреси вилучення та їх призначення*

№ з/п	IP-адреса вилучення	Назва	Застосування
1	0.0.0.0	Невизначена IP-адреса (Unknown IP-Address)	Позначення поточного вузла. Адреса відправника повідомлення у випадку, коли вузол не має адресної інформації
2	127.0.0.1 (127.x.x.x)	IP-адреса зворотної петлі (Loopback, Localhost IP-Address)	Тестування роботи стеку TCP/IP, а також організація роботи клієнтсь- кої і серверної частин додатка, які функціонують на одному вузлі
3	255.255.255.255	Обмежена широкомовна IP-адреса (Limited Broadcast IP-Address)	Пересилання повідомлення всім вузлам поточної мережі, без пересилання через маршрутизатори

На початковому етапі впровадження класової IP-адресації передбачалося, що всі IP-адреси класів A, B та C будуть застосовуватися для адресації вузлів у глобальній мережі Інтернет, однак із часом деякі IP-адреси мереж були вилучені для спеціального застосування. Серед них слід згадати так звані приватні IP-адреси (Private IP-Addresses), які були виділені для застосування у локальних мережах, що взагалі не мають підключення до глобальної мережі Інтернет або підключаються за допомогою технології заміни адрес NAT [5].

Інформацію про приватні IP-адреси (відповідно до першого стандарту RFC-1918 ,,Address Allocation for Private Internets”) наведено у табл. 8.6.

Таблиця 8.6 *Приватні IP-адреси*

Клас	Діапазон	Кількість IP-мереж
A	**10**.0.0.0 – **10**.255.255.255	1
B	**172.16**.0.0 – **172.31**.255.255	16
C	**192.168.0**.0 – **192.168.255**.255	256

Найбільш актуальну і повну інформацію стосовно IP-адрес вилучень та IP-адрес мереж спеціального призначення наведено в останньому на сьогодні стандарті, що стосується IP-адресації – стандарті RFC-6890 „Special-Purpose IP Address Registries”.

Класовий підхід до IP-адресації передбачає, що IP-адреси цілком достатньо для однозначної адресації вузла чи мережі. Але подальший перехід до безкласового підходу зумовив уведення нового параметра адресації – спеціальної IP-адреси, відомої як маска мережі/підмережі [6].

Маска мережі/підмережі (Network/Subnet Mask) – додаткова спеціальним чином сформована IP-адреса, за допомогою якої зазначається, яка частина IP-адреси є IP-адресою мережі, а яка – IP-адресою вузла. У сучасній практиці маски застосовуються як у класовій, так і у безкласовій адресації. Для класової адресації маска мережі фактично є записом правила I.

Виділяють три види масок:

– пряма маска (Subnet Mask);

– інверсна маска (Inverse Mask);

– шаблонна маска (Wildcard Mask).

Пряма маска у першу чергу застосовується для налагодження параметрів IP-адресації мережних адаптерів/інтерфейсів. Також може використовуватися для налагодження статичної маршрутизації та протоколів динамічної маршрутизації *RIP, IGRP*. У класовій прямій масці байтам, що співвідносяться з байтами IP-адреси мережі, відповідають значення 255, а байтам, що співвідносяться з байтами IP-адреси вузла, відповідають значення 0.

Інверсна маска застосовується для налагодження параметрів протоколів

динамічної маршрутизації *OSPF, EIGRP*. У класовій інверсній масці байтам, що співвідносяться з байтами IP-адреси мережі, відповідають значення 0, а байтам, що співвідносяться з байтами IP-адреси вузла, відповідають значення 255.

Шаблонні маски застосовуються для формування списків доступу (*ACLs, Access Control Lists*), за допомогою яких здійснюється фільтрація трафіка між різними IP-мережами. Списки доступу є невід'ємними складовими сучасних програмних та апаратних міжмережних екранів. Слід зазначити, що поняття класового чи безкласового підходів до шаблонних масок не застосовується.

Досить часто поняття „шаблонна" та „інверсна маска" не розрізняють. Такий підхід є некоректним. Відмітності у принципах формування інверсних і шаблонних масок стають зрозумілими саме під час детального аналізу роботи списків доступу.

Поряд з терміном „маска" (пряма маска) у практиці набув значного поширення термін „префікс мережі" (*Network Prefix*). Префікс мережі – це число, яке зазначає кількість бітів, що виділені у певній IP-адресі на номер мережі. Функціонально префікс і маска є повними аналогами. Фактично префікс мережі – це інша, коротша форма запису маски мережі. Прямі та інверсні класові маски і класові префікси наведені у табл. 8.7.

Таблиця 8.7 *Класові маски/префікси*

Клас	Класова маска	Інверсна класова маска	Класовий префікс
A	255.0.0.0	0.255.255.255.	/8
B	255.255.0.0	0.0.255.255	/16
C	255.255.255.0	0.0.0.255	/24

На основі IP-адреси та маски мережного адаптера/інтерфейсу можна визначити, до якої IP-мережі належить вузол/пристрій, а також детальні параметри IP-адресації цієї мережі.

8.5. Безкласова IP-адресація

Безкласова IP-адресація, також відома як механізм використання масок підмереж змінної довжини (*VLSM, Variable-Length Subnet Masking*), передбачає, що ідентифікація мережного адаптера/інтерфейсу або мережі здійснюється за

допомогою двох параметрів – IP-адреси та мережної маски/префікса мережі. *VLSM* складовою безкласової маршрутизації (*CIDR, Classless Inter-Domain Routing*) – методу IP-адресації та IP-маршрутизації різних за розмірами IP-мереж [6].

На відміну від класової IP-адресації у безкласовій IP-адресації поділ IP-адреси на частини – IP-адресу (номер) мережі та IP-адресу (номер) вузла, – здійснюється не побайтово, а побітово. Побітовий поділ надав можливість збільшити кількість варіантів формування IP-адрес мереж та можливість більш економно використовувати загальний адресний простір.

Для аналізу та розрахунку параметрів IP-мережі за умови застосування безкласової IP-адресації користуються залежностями, що описують довжини IP-адреси та префікса у загальному вигляді:

$N + H = 32$ біти,

$P = N$,

$0 \le N \le 32$ біти,

$0 \le H \le 32$ біти,

$0 \le P \le 32$ біти,

де N – кількість бітів, які виділені для адресації мережі (номер мережі);

H – кількість бітів, які виділені для адресації вузлів мережі;

P – кількість бітів, які виділені для формування префікса мережі.

Граничні значення параметрів N, H, P мають спеціальне тлумачення. Зокрема це стосується значень 0, 31, 32.

Відповідно кількість IP-адрес однієї IP-мережі, що можуть призначатися вузлам, розраховується за формулою:

$$K_{вузлів} = 2^{(32-P)} - 2 .$$

Дана формула має сенс для значень префіксів від $P = 0$ до $P = 30$ включно. Граничні значення префікса $P = 31$ та $P = 32$ мають специфіку трактування і у вказаній формулі не застосовуються.

Очевидко, що збільшення значення префікса дає змогу зменшити кількість IP-адрес вузлів мережі, і навпаки, зменшення значення префікса дає змогу збільшити кількість IP-адрес вузлів мережі.

Таблиця 8.8 *Мережні префікси/маски*

Префікс	Маска мережі	Інверсна маска мережі	Кількість IP-адрес вузлів в IP-мережі
/0	0.0.0.0	255.255.255.255	4294967294
/1	128.0.0.0	127.255.255.255	2147483646
/2	192.0.0.0	63.255.255.255	1073741822
/3	224.0.0.0	31.255.255.255	536870910
/4	240.0.0.0	15.255.255.255	268435454
/5	248.0.0.0	7.255.255.255	134217726
/6	252.0.0.0	3.255.255.255	67108862
/7	254 0 0.0	1.255.255.255	33554430
/8	255.0.0.0	0.255.255.255	16777214
/9	255.128.0.0	0.127.255.255	8388606
/10	255.192.0.0	0.63.255.255.	4194302
/11	255.224.0.0	0.31.255.255	2097150
/12	255.240.0.0	0.15.255.255	1048574
/13	255.248.0.0	0.7.255.255	524286
/14	255.252.0.0	0.3.255.255	262142
/15	255.254.0.0	0.1.255.255	131070
/16	255.255.0.0	0.0.255.255	65534
/17	255.255.128.0	0.0.127.255	32766
/18	255.255.192.0	0.0.62.255	16382
/19	255.255.224.0	0.0.31.255	8190
/20	255.255.240.0	0.0.15.255	4094
/21	255.255.248.0	0.0.7.255	2046
/22	255.255.252.0	0.0.3.255	1022
/23	255.255.254.0	0.0.1.255	512
/24	255 255 255 0	0.0.0.255	254
/25	255.255.255.128	0.0.0.127	126
/26	255.255.255.192	0.0.0.63	62
/27	255.255.255.224	0.0.0.31	30
/28	255.255.255.240	0.0.0.15	14
/29	255.255.255.248	0.0.0.7	6
/30	255.255.255.252	0.0.0.3	2
/31	255.255.255.254	0.0.0.1	2*
/32	255.255.255.255	0.0.0.0	1*

Примітка: * – для адресації вузлів з такими префіксами зроблено виняток із загальних правил адресації.

Повний перелік мережних префіксів, прямих та інверсних безкласових масок, а також кількість можливих IP-адрес вузлів для кожного префікса наведено у табл. 8.8.

8.6. IP-адресація версії 6

IP-адреса версії 6 має довжину 128 бітів (16 байтів). Запис такої адреси здійснюється у шістнадцятковій формі числення як вісім груп по 16 бітів (два байти), як роздільник груп застосовується двокрапка.

Діапазон можливих IP-адрес версії 6 містить 2^{128} IP-адрес і має вигляд: 0000:0000:0000:0000:0000:0000:0000:0000 – FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

На практиці застосовуються повна і спрощена форми запису IPадрес версії 6. Повна форма передбачає запис усіх цифр IP-адреси. Спрощена форма дозволяє не записувати ведучі нулі у групах та замінювати одну з послідовностей нульових груп записом.

Приклад повної форми запису IP-адреси версії 6: 2001:0DB8:0000:0000:0000:FF00:0042:8329.

Приклад частково спрощеної форми запису IP-адреси версії 6: 2001:DB8:0:0:0:FF00:42:8329.

Приклад спрощеної форми запису IP-адреси версії 6: 2001:DB8::FF00:42:8329.

Таблиця 8.9 *Основні спеціальні IP-адреси версії 6 та їх призначення*

№ з/п	IPv6-адреса вилучення	Назва	Застосування
1	:: /128	Невизначена IPv6-адреса (Unknown IPv6-Address)	Позначення поточного вузла. Адреса відправника повідомлення у випадку, коли вузол не має адресної інформації
2	::1 /128	IPv6-адреса зворотної петлі (Loopback, Localhost IPv6-Address)	Тестування роботи стеку TCP/IP, а також організація роботи клієнтсь- кої і серверної частин додатка, які функціонують на одному вузлі
3	FE80::/10	IPv6-адреса локального використання (Linked-Scoped Unicast IPv6-Address)	Адреса локального використання. Формується на основі MAC-адреси вузла. Номер мережі – FE80::
4	FFxx:: /8	IPv6-Групова адреса (IPv6 Multicast Address)	Групова IPv6-адреса

Як і для IP-адрес версії 4, деякі адреси з діапазону IP-адрес версії 6 зарезервовані для спеціального використання. Повний перелік та опис спеціалізованих IP-адрес версії 6 міститься у стандарті RFC- 6890. Основні з них наведені у табл. 8.9

Залежно від застосування IPv6-адреса може бути ідентифікована як:

– унікальна IPv6-адреса (Unicast IPv6-Address);

– групова IPv6-адреса (Multicast IPv6-Address);

– IPv6-адреса одного з групи (Anycast IPv6-Address).

У повідомленні (IPv6-пакеті) унікальні IPv6-адреси можуть зазначатися і як адреси відправника (*Source IPv6-Address*), і як адреси отримувача (*Destination IPv6-Address*). Групові IPv6-адреси і IPv6-дреси одного з групи можуть зазначатися лише як адреси отримувача. IP-адреса отримувача визначає, яким є IP-пакет: унікальним, груповим тощо. Для широкомовної розсилки в IP версії 6 застосовуються групові IPv6-адреси [7].

Таблиця 8.10 *Типові IPv6 префікси*

Префікс	Призначення
/4	
/8	
/12	Виділено IANA для RIR
/16	
/20	Виділено для LIR дуже великого розміру
/24	Виділено для LIR великого розміру
/28	Виділено для LIR середнього розміру
/32	Виділено для LIR малого розміру
/36	Виділено для майбутнього використання для LIR надмалого розміру
/40	
/44	
/48	Типово призначається великим сайтам та провайдерам
/52	
/56	Типово призначається кінцевим сайтам (домашнім мережам)
/60	Обмежене використання
/64	Одна локальна мережа (типовий префікс для SLAAC)

Структурно IP-адреса версії 6 складається з двох однакових за довжиною частин – одна частина (64 біти ліворуч) містить IP-адресу (номер) мережі, до якої належить вузол, інша (64 біти праворуч) – IP-адресу (номер) вузла в цій

мережі. Відокремлення номера мережі від номера вузла здійснюється за допомогою префікса мережі /64. Особливістю IP-адреси версії 6 є те, що номер мережі містить у собі номери багатьох підмереж. Відповідно застосовується кілька префіксів підмереж.

Перелік типових IPv6 префіксів підмереж наведено у табл. 8.10.

Контрольні питання до розділу

1. Наведіть типи адрес, що застосовуються в сучасних мережах?
2. Дайте визначення фізичної адреси? Наведіть приклади фізичних адрес.
3. Дайте визначення логічної адреси? Наведіть приклади логічних адрес.
4. Дайте визначення текстової адреси. Наведіть приклади текстових адрес.
5. Що собою представдяють MAC-адреси? Види та застосування.
6. Наведіть структуру MAC-адреси?
7. Що собою представляють IP-адреса версії 4. Види та застосування.
8. Наведіть структуру IP-адреси версії ?
9. Що собою представдяють IP-адреси вилучення версії 4?
10. Що собою представдяють приватні IP-адреси версії 4?
11. Визначте поняття маски та префікса мережі?
12. Які види масок існуть?
13. Наведіть особливості класової IP-адресації.
14. Що собою представдяють безкласова IP-адресація?
15. Які існують види та застосування IP-адреси версії 6?
16. Наведіть структуру IP-адреси версії 4.

Список рекомендованої літератури

1. *Олифер В. Г., Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
2. *Шварц М.* Сети связи: протоколы, моделирование и анализ. Ч.1. – М.: Наука, 1992. – 336 с.
3. *Дуглас Камер* Сети TCP/IP, том 1. Принципы, протоколы и структура = Internetworking with TCP/IP, Vol. 1: Principles, Protocols and Architecture. – М.: «Вильямс», 2003. – 880 с. – ISBN 0-13-018380-6.
4. *Блэк Ю.* Сети ЭВМ: протоколы, стандарты, интерфейсы. – М.: Мир, 1990. – 506 с.
5. *Уэнделл Одом* Компьютерные сети. Первый шаг // Computer Networking First-step. – М.: «Вильямс», 2005. – С. 432.
6. *Семенов Ю.А.* Алгоритмы телекоммуникационных сетей. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных БИНОМ. Курс лекций. [Електронний ресурс]. Лаборатория знаний, Интернет-

университет информационных технологий, 2007 – ISBN: 978-5-94774-706-5. Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/9/9/info

7. Комп’ютерні мережі [Електронний ресурс] : навчальний посібник для виконання лабораторних робіт для студ.спеціальності 126 «Інформаційні системи та технології»/ *Б. Ю. Жураковський; І.О. Зенів,* КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 10,08 Мбайт). – Київ : КПІ ім.Ігоря Сікорського, 2020. – 213 с.

Розділ 9. БЕЗПЕКА МЕРЕЖІ

9.1. Основні поняття захисту інформації

Захист інформації - це комплекс заходів, що проводяться з метою запобігання витоку, розкрадання, втрати, несанкціонованого знищення, викривлення, модифікації (підробки), несанкціонованого копіювання, блокування інформації, тощо. Оскільки втрата інформації може відбуватися через суто технічні, об'єктивним і ненавмисним причин, під це визначення потрапляють також і заходи, пов'язані з підвищенням надійності сервера через відмови або збоїв в роботі вінчестерів, недоліків у програмному забезпеченні і т.д. [1].

Перехід від роботи на персональних комп'ютерах до роботи в мережі ускладнює захист інформації з наступних причин:

1. велике число користувачів в мережі і їх змінний склад. Захист на рівні імені та пароля користувача недостатня для запобігання входу в мережу сторонніх осіб;

2. значна протяжність мережі і наявність багатьох потенційних каналів проникнення в мережу;

3. уже зазначені недоліки в апаратному та програмному забезпеченні, які найчастіше виявляються нема на передпродажного етапі, званому бета-тестуванням, а в процесі експлуатації. У тому числі неідеальні вбудовані засоби захисту інформації навіть в відомих і "потужних" мережевих ОС.

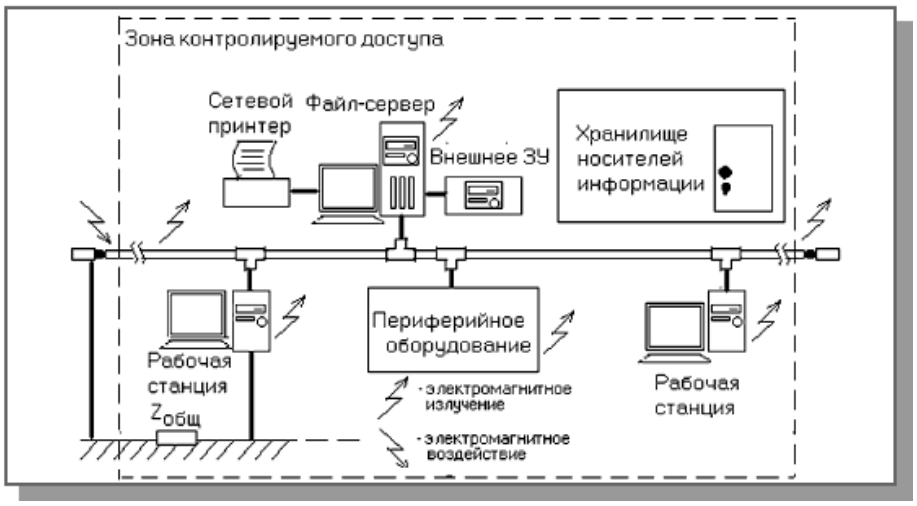


Рис.9.1. Місця і канали можливого несанкціонованого доступу до інформації в комп'ютерній мережі

У мережі є багато фізичних місць і каналів несанкціонованого доступу до інформації в мережі.

Кожен пристрій в мережі є потенційним джерелом електромагнітного випромінювання через те, що відповідні поля, особливо на високих частотах, екрановані неідеально [2].

Система заземлення разом з кабельною системою і мережею електроживлення може служити каналом доступу до інформації в мережі, в тому числі на ділянках, що знаходяться поза зоною контрольованого доступу і тому особливо вразливих.

Крім електромагнітного випромінювання, потенційну загрозу представляє безконтактне електромагнітний вплив на кабельну систему.

Безумовно, в разі використання проводових з'єднань типу коаксіальних кабелів або кручених пар, які називаються часто мідними кабелями, можливо і безпосереднє фізичне підключення до кабельної системі. Якщо паролі для входу в мережу стали відомі або підібрані, стає можливим несанкціонований вхід в мережу з файл-сервера або з однією з робочих станцій [2].

Нарешті можливий витік інформації по каналах, які знаходяться поза мережею:

- сховище носіїв інформації,
- елементи будівельних конструкцій і вікна приміщень, які утворюють

канали витоку конфіденційної інформації за рахунок так званого мікрофонного ефекту,

• телефонні, радіо-, а також інші проводові та безпроводові канали (в тому числі канали мобільного зв'язку).

9.2. Концепції мережевої безпеки

Безпе́ка мере́жі (*Network security*) — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу [3].

Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ID і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформації і програм у рамках своїх повноважень.

Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і зв'язків між підприємствами, державними установами та приватними особами [3].

Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу.

Мережева безпека бере участь в організаціях, підприємствах та інших типів закладів. Найбільш поширений і простий спосіб захисту мережевих ресурсів є присвоєння їм унікального імені та відповідного паролю.

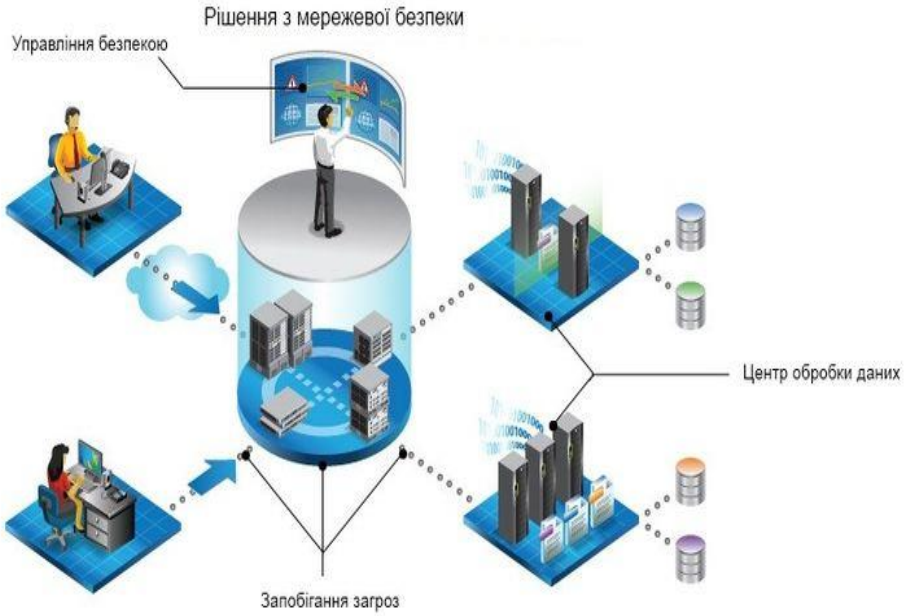


Рис.9.2. Концепції мережевої безпеки

Концепції мережевої безпеки

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією.

При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер забезпечує доступ до послуг користувачам мережі.

Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої компанії від можливих атак.

Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз.

Система безпеки мережі:

- Захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.
- Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації.
- Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями.
- Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

9.3. Ключові елементи захищених мережних служб

Брандмауери. Централізовані брандмауери та брандмауери окремих комп'ютерів можуть запобігати проникненню зловмисного мережного трафіку до мережі, яка підтримує діяльність компанії.

Антивірусні засоби. Більш захищена мережа може виявляти загрози, що створюють віруси, хробаки та інше зловмисне програмне забезпечення, і боротися з ним попереджувальними методами, перш ніж вони зможуть заподіяти шкоду.

Знаряддя, які відстежують стан мережі, грають важливу роль під час визначення мережних загроз.

Захищений віддалений доступ і обмін даними. Безпечний доступ для всіх типів клієнтів із використанням різноманітних механізмів доступу грає важливу роль для забезпечення доступу користувачів до потрібних даних, незалежно від їх місцезнаходження та використовуваних пристроїв.

Критерії оцінки інформаційної безпеки (*Common Criteria*) є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Для характеристики основних критеріїв інформаційної безпеки застосовують модель тріади CIA en:CIA_Triad.

Ця система передбачає такі основні характеристики інформаційної безпеки:

- конфіденційність,
- цілісність,
- доступність (*Confidentiality, Integrity and Availability (CIA)*).

Інформаційні системи аналізуються в трьох головних секторах: *технічних засобах, програмному забезпеченні і комунікаціях*, з метою ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання, на трьох рівнях або шарах: *фізичний, особистий і організаційний*.

По суті, процедури або правила запроваджуються для інформування адміністраторів, користувачів та операторів щодо використовування захисної продукції для гарантування інформаційної безпеки в межах організацій [4].

Нормативний документ ТЗІ 2.5-004-99

В Україні також розробляються і використовуються критерії інформаційної безпеки.

Наприклад департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» який подібний до моделі тріади CIA [3].

Функціональні критерії

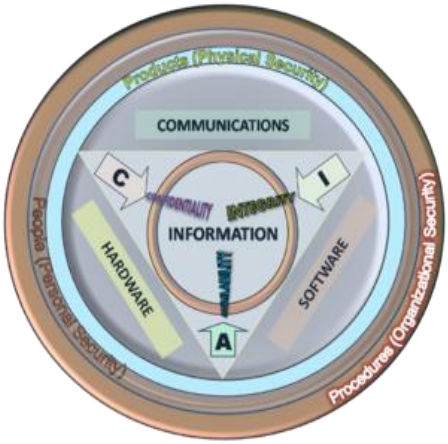


Рис. 9.3. Складові інформаційної безпеки

Складові інформаційної безпеки або властивості: конфіденційність (***C****onfidentiality, privacy*), цілісність (***I****ntegrity*), доступність (***A****vailability*) — тріада CIA.

Функціональні критерії розбиті на чотири групи вимог захисту проти певних типів загроз:

Конфіденційність

Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності. Якщо існують вимоги щодо обмеження можливості ознайомлення з інформацією, то відповідні послуги відносяться до критеріїв конфіденційності.

Цілісність

Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. У випадку, якщо існують вимоги щодо

обмеження можливості модифікації інформації, то їх відносяться до критеріїв цілісності.

Доступність

Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то їх відносяться до критеріїв доступності.

Спостереженість

Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні функції відносяться до критеріїв спостереженості.

Критерії гарантій

Окрім функціональних критеріїв захищеності існують таки критерії гарантій, що дозволяють оцінити коректність реалізації систем захисту. Ці критерії включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

9.4. Загрози інформації

Відповідно до властивостей інформації, виділяють такі загрози її безпеці:

- *загрози цілісності*:
  - знищення;
  - модифікація;
- *загрози доступності*:
  - блокування;
  - знищення;
- *загрози конфіденційності*:
  - несанкціонований доступ (НСД);

– витік;
– розголошення.

9.5. Класифікація засобів захисту інформації

1. ***Технічні (апаратні) засоби***. Це різні за типом пристрою (механічні, електромеханічні, електронні та ін.), які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж відбулося, доступу до інформації, в тому числі за допомогою її маскування.

Першу частину завдання вирішують замки, решітки на вікнах, захисна сигналізація та ін.

Другу - згадувані вище генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, "перекривають" потенційні канали витоку інформації або дозволяють їх виявити. *Переваги технічних засобів* пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високу стійкість до модифікації. *Слабкі сторони* - недостатня гнучкість, відносно великі обсяг і маса, висока вартість [3].

2. ***Програмні засоби*** включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. ***Переваги програмних засобів*** - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. ***Недоліки*** - обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів). До програмних засобів відноситься криптографічний захист інформації.

Криптографі́чний за́хист інформа́ції — вид захисту інформації, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення)

змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Є складовою частиною комплексної системи захисту інформації [4].

Криптогра́фія (від грецького *kryptós* — прихований і *gráphein* — писати) — наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри [5].

3. ***Змішані апаратно-програмні*** засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

4. ***Організаційні засоби*** складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін.) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства).

Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку.

Недоліки - висока залежність від суб'єктивних чинників, в тому числі від загальної організації роботи в конкретному підрозділі.

9.6. Класифікація мережних атак

- Будь-які додаткові з'єднання з іншими сегментами або підключення до Інтернет породжують нові проблеми.
- Атаки на локальну мережу через підключення до Інтернету для того, щоб отримати доступ до конфіденційної інформації, останнім часом набули широкого поширення, що пов'язано з недоліками вбудованої системи захисту інформації в протоколах TCP / IP.
- *Мережеві атаки через Інтернет можуть бути класифіковані в такий спосіб:*

• *Сніффер пакетів* (*sniffer* - в даному випадку в сенсі фільтрація) - прикладна програма, яка використовує мережеву карту, що працює в режимі promiscuous (хто не робить відмінності) mode (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки).

• *IP-спуфинг* (*spoof* - обман, містифікація) - відбувається, коли хакер, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача.

Відмова в обслуговуванні (Denial of Service - DoS). Атака DoS робить мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми.

• *Парольні атаки* - спроба підбору пароля легального користувача для входу в мережу.

• *Атаки типу Man-in-the-Middle* - безпосередній доступ до пакетів, що передаються по мережі.

• *Атаки на рівні додатків.*

• *Мережева розвідка* - збір інформації про мережу за допомогою загальнодоступних даних і додатків.

• *Зловживання довірою всередині мережі*.

• *Несанкціонований доступ (НСД),* який не може вважатися окремим типом атаки, так як більшість мережевих атак проводяться заради отримання несанкціонованого доступу.

• *Віруси і додатки типу "троянський кінь".*

9.7. Шифрування

За ступенем поширення і доступності виділяються програмні засоби, інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

Шифрування даних являє собою різновид програмних засобів захисту інформації і має особливе значення на практиці як єдиний надійний захист інформації, що передається по протяжним послідовним лініях, від витоку.

Шифрування утворює останній, практично нездоланний "кордон" захисту від несанкціонованого доступу.

Поняття "шифрування" часто вживається в зв'язку з більш загальним поняттям криптографії [6].

Криптографія включає способи і засоби забезпечення конфіденційності інформації (в тому числі за допомогою шифрування) і аутентифікації. Конфіденційність - захищеність інформації від ознайомлення з її змістом з боку осіб, які не мають права доступу до неї. У свою чергу аутентифікація є встановлення автентичності різних аспектів інформаційної взаємодії: сеансу зв'язку, сторін (ідентифікація), змісту (імітозащіти) і джерела (встановлення авторства с допомогою цифрового підпису)[6].

Число використовуваних програм шифрування обмежена, причому частина з них є стандартами де-факто або де-юре.

Однак навіть якщо алгоритм шифрування не представляє собою секрету, зробити дешифрування (розшифрування) без знання закритого ключачрезвичайно складно.

Це властивість в сучасних програмах шифрування забезпечується в процесі багатоступінчастого перетворення вихідної відкритої інформації (plain text в англомовній літературі) з використанням ключа (або двох ключів - поодному для шифрування і дешифрування). В кінцевому рахунку, будь-який складний метод (алгоритм) шифрування є комбінацією щодо простих методів.

Класичні алгоритми шифрування даних

Є такі "класичні" методи шифрування:

• *підстановка* (проста - одноалфавітная, Многоалфавитная однопетльовою, Многоалфавитная многопетлевая);

• *перестановка* (проста, ускладнена);

• *гамування* (змішування з короткою, довгою або необмеженої маскою).

Стійкість кожного з перерахованих методів до дешифрування без знання ключа характеризується кількісно за допомогою показника Sк, що представляє

собою мінімальний обсяг зашифрованого тексту, який може бути дешифрований за допомогою статистичного аналізу [7].

Підстановка передбачає використання альтернативного алфавіту (або декількох), замість справжнього. У разі простої підстановки для символів англійського алфавіту можна запропонувати, наприклад, наступну заміну:

Таблиця 9.1. *Приклад заміни символів при подстановці*

Вихідний алфавіт												
	A	B	C	D	E	F	G	H	I	J	K	L
…	X	Y	Z									
Альтернативний алфавіт												
	S	O	U	H	K	T	L	X	N	W	M	Y
…	A	Y	Z									

Тоді *слово* "*cache*" в зашифрованому вигляді представляється як "usuxk".

Існує, однак, можливість дешифрування повідомлення за допомогою відомої статистичної частоти повторюваності символів в довільному, досить довгому тексті.

Символ *E* зустрічається найчастіше - в середньому 123 рази на кожні 1000 символів або в 12,3% випадків, далі йдуть символи *T* - 9,6%, *A* - 8,1%, *O* - 7,9%, *N* - 7, 2%, *I* - 7,2%, *S* - 6,6%, *R* - 6,0%, *H* - 5,1%, *L* - 4,0% і т.д.

Наведені цифри можуть, звичайно, дещо змінюватись в залежності від джерела інформації, з якого вони були взяті, що не змінює принципово ситуації.

Дані щодо дешифрування *Sк* не перевищують 20 ... 30. При багатоалфавітній підстановці можна домогтися того, що в зашифрованому тексті все символи будуть зустрічатися приблизно з однаковою частотою, що істотно ускладнить дешифрування без знання альтернативних алфавітів і порядку, в якому вони використовувалися при шифруванні.

Перестановка потенційно забезпечує більшу в порівнянні з підстановкою стійкість до дешифрування і виконується з використанням цифрового ключа

або еквівалентного ключового слова. Цифровий ключ складається з цифр,що не повторюються, а відповідне йому ключове слово - з символів, які не повторюються. Оригінальний текст (*plain text*) записується під ключем через підрядник. Зашифроване повідомлення (*cipher text*) виписується за стовпцями в тому порядку, як це наказують цифри ключа або в тому порядку, в якому розташовані окремі символи ключового слова.

Гамірування (змішування з маскою) засновано на побітному складання по модулю 2 (відповідно до логіки виключає Або) вихідного повідомлення з заздалегідь обраної двійковій послідовністю (міський). Компактним представленням маски можуть служити числа в десятковій системі числення або деякий текст (в даному випадку розглядаються внутрішні коди символів - для англійського тексту таблиця ASCII). На рис.2 показано, як вихідний символ "A" при додаванні з маскою 0110 10012 переходить в символ "(" в зашифрованому повідомленні) [7].

Операція підсумовування по модулю 2 (виключає Або) є оборотною, так що при додаванні з тієї ж маскою (ключем) зашифрованого повідомлення виходить вихідний текст (відбувається дешифрування). Як маски (ключа) можуть використовуватися константи типу або е. Найбільшу стійкість до дешифрування може забезпечити застосування маски з нескінченної завдовжки, яка утворена генератором випадкових (точніше, псевдовипадкових) послідовностей.

Такий генератор легко реалізується апаратними або програмними засобами, наприклад, за допомогою зсувного регістру з зворотними зв'язками, який використовується при обчисленні перешкодостійкого циклічного коду. Точне відтворення псевдовипадкової послідовності в генераторі на приймальному кінці лінії забезпечується при установці такого ж вихідного стану (вмісту зсувного регістру) і тієї ж структури зворотних зв'язків, що і в генераторі на передавальному кінці.

$$\begin{array}{ll} & "A" \rightarrow 41_{16} = 0100\ 0001_2 \\ \oplus & \text{маска} \rightarrow 69_{16} = 0110\ 1001_2 \\ \hline & "(" \rightarrow 28_{16} = 0010\ 1000_2 \end{array}$$

Перераховані "класичні" методи шифрування (підстановка, перестановка і гамування) є лінійними в тому сенсі, що довжина зашифрованого повідомлення дорівнює довжині вихідного тексту.

Можливо нелінійне перетворення типу підстановки замість вихідних символів (або цілих слів, фраз, пропозицій) заздалегідь вибраних комбінацій символів іншої довжини.

Ефективний також захист інформації методом розсічення-рознесення, коли вихідні дані розбиваються на блоки, кожен з яких не несе корисної інформації, і ці блоки зберігаються і передаються незалежно один від одного. Для текстової інформації відбір даних для таких блоків може проводитися по групам, які включають фіксований число біт, менше, ніж число біт на символ в таблиці кодування.

9.8. Сучасна криптографія

Стандартні методи шифрування (національні або міжнародні) для підвищення ступеня стійкості до дешифрування реалізують кілька етапів (кроків) шифрування, на кожному з яких використовуються різні "класичні" методи шифрування відповідно до обраного ключем (або ключами). Існують дві принципово різні групи стандартних методів шифрування:

• шифрування із застосуванням одних і тих же ключів (шифрів) при шифрування і дешифрування (симетричне шифрування або системи із закритими ключами - private-key systems);

• шифрування з використанням відкритих ключів для шифрування і закритих - для дешифрування (несиметричне шіфрованіеілі системи з відкритими ключами - public-key systems) [8].

Строгий математичний опис алгоритмів стандартних методів шифрування

занадто складно. Для користувачів важливі в першу чергу "споживчі" властивості різних методів (ступінь стійкості до дешифрування, швидкість шифрування і дешифрування, порядок і зручність поширення ключів), які і розглядаються нижче.

Для подальшого підвищення стійкості до дешифрування можуть застосовуватися послідовно кілька стандартних методів або один метод шифрування (але з різними ключами).

9.8.1. Симетричне шифрування

До алгоритмів симетричного шифрування належать методи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або, менш поширено, ключі різні але споріднені та легко обчислюються). Ці алгоритми шифрування були єдиними загально відомими до липня 1976.

Сучасні дослідження симетричних алгоритмів шифрування зосереджено, в основному, навколо блочних та потокових алгоритмів шифрування та їхньому застосуванні. Блочний шифр подібний до поліалфавітного шифру Альберті: блочні шифри отримують фрагмент відкритого тексту та ключ, і видають на виході шифротекст такого самого розміру. Оскільки повідомлення зазвичай довші за один блок, потрібен деякий метод склеювання послідовних блоків. Було розроблено декілька методів, що відрізняються в різних аспектах. Вони є режимами дії блочних шифрів та мають обережно обиратись під час застосування блочного шифру в криптосистемі.

Стандарт шифрування США ***DES (Data Encryption Standard*** - стандарт шифрування даних) відноситься до групи методів симетричного шифрування і діє з 1976 р Число кроків - 16. Довжина ключа - 64 біта, з яких 8 біт - перевірочні розряди парності / непарності. Довгий час ступінь стійкості до дешифрування цього методу вважалася достатньою, проте в даний час він застарів. Замість DES пропонується "*потрійний DES*" - *3DES*, в якому алгоритм DES використовується 3 рази, зазвичай в послідовності "шифрування - дешифрування - шифрування" з трьома різними ключами на кожному етапі.

Шифр ***Advanced Encryption Standard (AES)*** є стандартом блочних шифрів затверджених урядом США (стандартизацію *DES* було скасовано після прийняття стандарту *AES*) [8].

Не зважаючи на те, що стандарт *DES* було визнано застарілим, він (та особливо його все ще дійсний варіант *triple-DES*) залишається досить популярним; він використовується в багатьох випадках, від шифрування в банкоматах до забезпечення приватності електронного листування та безпечному доступі до віддалених терміналів.

Надійним вважається алгоритм ***IDEA (International Data Encryption Algorithm)***, розроблений в Швейцарії і має довжину ключа 128 біт.

Вітчизняний ***ГОСТ28147-89*** - це аналог DES, але з довжиною ключа 256 біт, так що його ступінь стійкості до дешифрування спочатку істотно вище. Важливо також і те, що в даному випадку передбачається ціла система захисту, яка долає "родової" недолік симетричних методів шифрування - можливість підміни повідомлень. Такі удосконалення, як имитовставки, хеш-функції і електронні цифрові підписи дозволяють "авторизувати" передані повідомлення.

До переваг симетричних методів шифрування відноситься висока швидкість шифрування і дешифрування, *до недоліків* - мала ступінь захисту в разі, якщо ключ став доступний третій особі.

Потокові шифри, на відміну від блочних, створюють ключ довільної довжини, що накладається на відкритий текст побітово або політерно, в дечому подібно до одноразової дошки. В потокових шифрах, потік шифротексту обчислюється на основі внутрішнього стану алгоритму, який змінюється протягом його дії. Зміна стану керується ключем, та, в деяких алгоритмах, ще і потоком відкритого тексту. RC4 є прикладом добре відомого, та широко розповсюдженого потокового шифру.

Криптографічні хешувальні функції (*cryptographic hash functions*, або англ. *message digest functions*) не обов'язково використовують ключі, але часто використовуються і є важливим класом криптографічних алгоритмів. Ці функції отримують дані (часто, ціле повідомлення), та обчислюють коротке, фіксованого розміру число (*хеш*). Гарні хешувальні функції створені таким

чином, що дуже важко знайти колізії (два відкритих тексти, що мають однакове значення хешу).

9.8.2. Асиметричне шифрування

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів — відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.

В асиметричних криптосистемах, відкритий ключ може вільно розповсюджуватись, в той час як приватний ключ має зберігатись в таємниці. Зазвичай, *відкритий ключ* використовується для шифрування, в той час як *приватний* (*секретний*) ключ використовується для дешифрування. Діффі та Хелман показали, що криптографія з відкритим ключем можлива за умови використання протоколу обміну ключами Діффі-Хелмана [7].

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) — криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел [9].

RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм застосовується до великої кількості криптографічних застосунків. [10]

Рис.9.4. RSA шифрування

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — *відкритий (public)* і *секретний (private),* разом відкритий і відповідний йому секретний ключі утворюють *пари ключів (keypair).* Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем.

Шифрування і розшифрування

- Інформація, що може бути прочитана, осмислена і зрозуміла без яких-небудь спеціальних заходів, називається відкритим текстом (plaintext, clear text). Метод перекручування відкритого тексту таким чином, щоб сховати його суть, називається шифруванням (encryption або enciphering).
- Шифрування відкритого тексту приводить до його перетворення в незрозумілу абракадабру, іменовану шифртекстом (ciphertext).

Шифрування дозволяє сховати інформацію від тих, для кого вона не призначається, попри те, що вони можуть бачити сам шифртекст. Протилежний процес перетворення шифртекста в його вихідний вид називається

розшифруванням (decryption або deciphering).

Несиметричні методи шифрування мають переваги і недоліки, зворотні тим, якими володіють симетричні методи. Зокрема, в несиметричних методах за допомогою посилки і аналізу спеціальних службових повідомлень може бути реалізована процедура аутентифікації (перевірки легальності джерела інформації) і цілісності (відсутності підміни) даних. При цьому виконуються операції шифрування і дешифрування за участю відкритих ключів і секретного ключа даного користувача.

Таким чином, несиметричні системи можна з достатньою підставою назвати повноцінними криптографічних систем.

На відміну від симетричних методів шифрування, проблема розсилки ключів в несиметричних методах вирішується простіше - пари ключів (*відкритий і закритий)* генеруються "на місці" за допомогою спеціальних програм.

Для розсилки відкритих ключів використовуються такі технології як ***LDAP (Lightweight Directory Access Protocol*** - *протокол полегшеного доступу до довідника*).

Розсилаються ключі можуть бути попередньо зашифровані за допомогою одного з симетричних методів шифрування.

Традиційні і обов'язкові для сучасних криптографічних систем способи забезпечення аутентифікації і перевірки цілісності даних, що отримуються (хеш-функції і цифрові підписи), які реалізуються безпосередніми учасниками обміну, не є єдино можливими.

Поширений також спосіб, який здійснюється за участю третьої сторони, якій довіряють всі учасники обмінів. Йдеться про використання так званих цифрових сертифікатів - посилаються по мережі повідомлень з цифровим підписом, що засвідчує справжність відкритих ключів.

9.9. Програмні засоби захисту інформації

Спеціалізовані програмні засоби захисту інформації від несанкціонованого

доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби мережевих ОС. Крім програм шифрування і криптографічних систем, існує багато інших доступних зовнішніх засобів захисту інформації. З найбільш часто згадуваних рішень слід відзначити наступні дві системи, що дозволяють обмежити і контролювати інформаційні потоки.

1. *Firewalls - брандмауери (дослівно firewall - вогненна стіна).* Між локальної та глобальної мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь проходить через них трафік мережевого / транспортного рівнів. Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищена різновид методу - це спосіб маскараду (*masquerading*), коли весь вихідний з локальної мережі трафік посилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

2. *Proxy-servers (proxy - довіреність, довірена особа).* Весь трафік мережевого / транспортного рівнів між локальної та глобальної мережами забороняється повністю - маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому звернення з глобальної мережі в локальну стають неможливими в принципі. Цей метод не дає достатнього захисту проти атак на більш високих рівнях - наприклад, на рівні додатку (віруси, код Java і JavaScript) [11].

9.10. Осоливості безпеки бездротових мереж

Головна відмінність бездротових мереж від провідних пов'язано з абсолютно неконтрольованою областю між кінцевими точками мережі. У досить широкому просторі мереж безпровідного середовища ніяк не контролюється.

Сучасні бездротові технології пропонують обмежений набір засобів управління всією областю розгортання мережі. Це дозволяє атакуючим, що знаходяться в безпосередній близькості від бездротових структур, виробляти

цілий ряд нападів, які були неможливі в кабельній мережі.

Обговоримо характерні тільки для бездротового оточення загрози безпеки, обладнання, яке використовується при атаках, проблеми, що виникають при роумінгу від однієї точки доступу до іншої, укриття для бездротових каналів і криптографічний захист відкритих комунікацій.

Найбільш поширена проблема в таких відкритих і некерованих середовищах, як бездротові мережі, - можливість анонімних атак. Анонімні шкідники можуть перехоплювати радіосигнал і розшифровувати дані, що передаються.

Обладнання, що використовується для підслуховування в мережі, може бути не складніше того, яке використовується для звичайного доступу до цієї мережі.

Щоб перехопити передачу, зловмисник повинен знаходитися поблизу від передавача.

Перехоплення такого типу практично неможливо зареєструвати, і ще важче перешкодити їм.

Використання антен і підсилювачів дає зловмиснику можливість перебувати на значній відстані від мети в процесі перехоплення.

Підслуховування дозволяє зібрати інформацію в мережі, яку згодом передбачається атакувати.

Первинна мета зловмисника - зрозуміти, хто використовує мережу, які дані в ній доступні, які можливості мережевого обладнання, в які моменти його експлуатують найбільш і найменш інтенсивно і яка територія розгортання мережі. Все це стане в нагоді для того, щоб організувати атаку на мережу.

Багато загальнодоступних мережевих протоколів передають таку важливу інформацію, як ім'я користувача і пароль, відкритим текстом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Навіть якщо передана інформація зашифрована, в руках зловмисника виявляється текст, який можна запам'ятати, а потім вже розкодувати.

Інший спосіб підслуховування - *підключення до бездротової мережі*.

Активне підслуховування в локальній бездротовій мережі зазвичай засноване на неправильному використанні протоколу *Address Resolution Protocol (ARP).* Спочатку ця технологія була створена для "прослуховування" мережі. Насправді ми маємо справу з атакою типу *MITM (Man In The Middle - "людина посередині")* на рівні зв'язку даних. Вони можуть приймати різні форми і використовуються для руйнування конфіденційності і цілісності сеансу зв'язку.

Атаки *MITM* більш складні, ніж більшість інших атак: для їх проведення потрібно детальна інформація про мережу. Зловмисник зазвичай підміняє ідентифікацію одного з мережевих ресурсів. Коли жертва атаки ініціює з'єднання, шахрай перехоплює його і потім завершує з'єднання з необхідним ресурсом, а потім пропускає все з'єднання з цим ресурсом через свою станцію. При цьому атакуючий може посилати і змінювати інформацію чи підслуховувати всі переговори і потім розшифровувати їх.

Атакуючий посилає ARP-відповіді, на які не було запиту, до цільової станції локальної мережі, яка відправляє йому весь проходить через неї трафік. Потім зловмисник буде відсилати пакети зазначеним адресатам.

Таким чином, бездротова станція може перехоплювати трафік іншого бездротового клієнта (або проводового клієнта в локальній мережі).

Відмова в обслуговуванні (*Denial of Service - DOS*)

Повну паралізації мережі може викликати атака типу DOS. У всій мережі, включаючи базові станції і клієнтські термінали, виникає така сильна інтерференція, що станції не можуть зв'язуватися один з одним. Ця атака вимикає всі комунікації в певному районі. Якщо вона проводиться в досить широкій області, то може вимагати значних потужностей. Атаку DOS на бездротові мережі важко запобігти або зупинити. Більшість бездротових мережевих технологій використовує неліцензовані частоти - отже, допустима інтерференція від цілого ряду електронних пристроїв.

Глушіння клієнтської станції

Глушіння в мережах відбувається тоді, коли навмисна або ненавмисна

інтерференція перевищує можливості відправника або одержувача в каналі зв'язку, і канал виходить з ладу. Атакуючий може використовувати різні способи глушіння.

Глушіння клієнтської станції дає шахраєві можливість підставити себе на місце заглушеного клієнта. Також глушіння може використовуватися для відмови в обслуговуванні клієнта, щоб йому не вдавалося реалізувати з'єднання. Більш витончені атаки переривають з'єднання з базовою станцією, щоб потім вона була приєднана до станції зловмисника.

Глушіння базової станції

Глушіння базової станції надає можливість підмінити її атакуючої станцією. Таке глушіння позбавляє користувачів доступу до послуг.

Більшість бездротових мережевих технологій використовує неліцензовані частоти. Тому багато пристроїв, такі як радіотелефони, системи стеження і мікрохвильові печі, можуть впливати на роботу бездротових мереж і глушити бездротове з'єднання. Щоб запобігти таким випадкам ненавмисного глушіння, перш ніж купувати дороге бездротове обладнання, треба ретельно проаналізувати місце його установки. Такий аналіз допоможе переконатися в тому, що інші пристрої не завадять комунікацій.

Контрольні питання до розділу

1. Дайте визначення поняттю «*Захист інформації»?*
2. Які причини ускладнюють захист інформації при перехід від роботи на персональних комп'ютерах до роботи в мережі?
3. Назвіть фізичні місця і канали несанкціонованого доступу до інформації в мережі?
4. По яких каналах, що знаходяться поза мережею можливий витік інформації?
5. В чому поягає концепції мережевої безпеки?
6. Які функції виконує система безпеки мережі ?
7. Що є ключовими елементами захищених мережних служб?
8. Що є складовими інформаційної безпеки?
9. Які існують типи загроз інформації?
10. Наведіть класифікацію засобів захисту інформації?
11. Організаційні засоби захисту інформації. Переваги та недоліки?
12. Технічні (апаратні) засоби захисту інформації. Переваги та недоліки?

13. Програмні засоби захисту інформації. Переваги та недоліки?
14. Наведіть класифікацію мережних атак?
15. Що собою представляє шифрування даних?
16. Наведіть класичні алгоритми шифрування даних?
17. Симетричне шифрування. Переваги та недоліки.
18. Асиметричне шифрування. Переваги та недоліки.
19. Які існують програмні засоби захисту інформації?
20. Особливості безпеки бездротових мереж.

Список рекомендованої літератури

1. *Menezes A. J., van Oorschot P. C., Vanstone S. A.* Handbook of Applied Cryptography. — CRC Press, 1996. — 794 p. (pdf)
2. *Бауэр Ф.* Расшифрованные секреты. — М.: Мир, 2007. — 550 с.
3. *Бурячок В.Л., Толюпа С.В., Семко А.А.* Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник], К.: ТОВ «СІК ГРУП Україна, 2015. – 345 с.
4. *Эрик Мэйволд* Безопасность сетей. Курс лекций. [Електронний ресурс] - М.: Интернет-университет информационных технологий, 2014. ISBN: 978-5-9570-0046-9, Режим доступу до матеріалу: https://www.intuit.ru/studies/courses/102/102/info.
5. *Земор Ж.* Курс криптографии. — Ижевск: РХД, 2006. — 256 с.
6. *Ван Тилборг Х. К. А.* Основы криптологии. — М.: Мир, 2006. — 472 с.
7. *Фергюсон Н., Шнайер Б.* Практическая криптография. — М.: Диалектика, 2004. — 431 с.
8. *Ященко В. В.* Введение в криптографию. — М.: МЦНМО, 2012. — 352 с.
9. *Ян С.* Криптоанализ RSA. — Ижевск : РХД, 2011. — 312 с.
10. [Електронний ресурс] Режим доступу до матеріалу: https://uk.wikipedia.org/wiki/RSA
11. *Vladimir A. Oleshchuk* On Public-Key Cryptosystem Based on Church-Rosser String-Rewriting Systems. — Proceedings of COCOON’95, Lecture Notes in Computer Science 959, 1995. — pp. 264–269 с.

Розділ 10. МЕРЕЖЕВІ ПРОТОКОЛИ

10.1. Основні поняття

Протокол взаємодії – формалізовані правила, які визначають послідовність і формат інформаційних блоків під час взаємодії компонент (об'єктів), що знаходяться на одному рівні у різних вузлах.

Інтерфейс – формально визначений набір функцій, які виконує даний рівень для вищого рівня, а також формати інформаційних блоків, якими обмінюються два сусідніх рівні в процесі своєї взаємодії

По суті, терміни «протокол» і «інтерфейс» виражають одне і теж поняття — формалізований опис процедури взаємодії двох об'єктів, але традиційно в мережах за ними закріпили різні зони дії: протоколи визначають правила взаємодії модулів одного рівня в різних вузлах, а інтерфейси — правила взаємодії модулів сусідніх рівнів в одному вузлі (рис.10.1).

Стек протоколів – погоджений набір протоколів різних рівнів, достатній для організації між мережевої взаємодії.

Стек протоколів – це ієрархічно впорядкована сукупність протоколів, достатніх для реалізації взаємодії вузлів у мережі.

Стек протоколів представляє собою набір специфікацій, що дозволяє реалізувати мережеву взаємодію [1].

Специфікація – формалізований опис апаратних та (або) програмних компонентів, способів їх функціонування, взаємодії з іншими компонентами, обмежень і особливих характеристик.

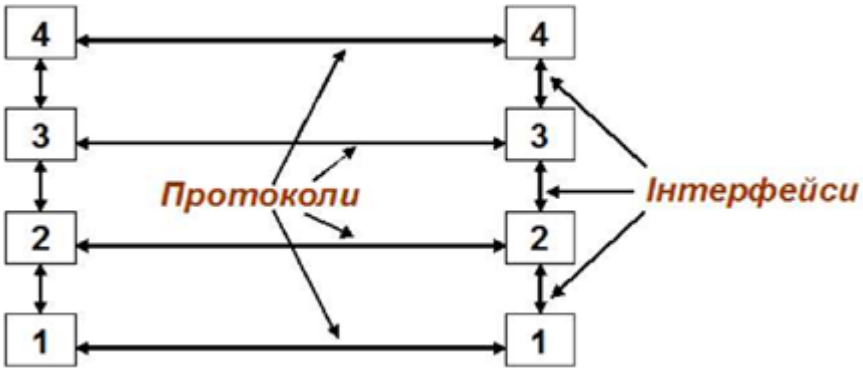


Рис.10.1. Поняття протоколу та інтерфейсу

Отже, взаємодія в мережах відбувається відповідно до певних правил обміну повідомленнями та їх форматами, тобто відповідно до ієрархічно організованої сукупності протоколів – стеку комунікаційних протоколів.

Існує достатньо багато стеків протоколів, що широко використовуються в телекомунікаційних мережах. Це і стеки за міжнародними чи національними стандартами, і фірмові стеки, що набули поширення завдяки поширеності устаткування тієї або іншої фірми. Прикладами популярних стеків протоколів є стек TCP/IP, що використовується в мережі Інтернет і в багатьох мережах на основі операційної системи UNIX, стек OSI міжнародної організації зі стандартизації, стек IPX/SPX фірми Novell, та інші [2].

Існує досить багато стеків протоколів, які використовуються у мережах. Це стеки, які з'явилися:

- *на основі міжнародних і національних стандартів*
- *стеки, запропоновані фірмами-виробниками мережевого обладнання, які одержали поширення завдяки поширеності обладнання саме цих фірм.*

10.2. Стек OSI

Варто чітко розрізняти ***модель OSI і стек OSI.*** У той час як модель OSI є концептуальною схемою взаємодії відкритих систем, ***стек OSI становить набір цілком конкретних специфікацій протоколів*** (табл 10.1) [3]. На відміну від інших стеків протоколів стек OSI повністю відповідає моделі OSI, він включає специфікації протоколів для всіх семи рівнів взаємодії, визначених у цій моделі. На нижніх рівнях OSI підтримує *Ethernet, TokenRing, FDDI*, а також такі протоколи, як *LLC, X.25 і ISDN* [1]. Сервіси мережного, транспортного й сеансового рівнів цього стека поки мало поширені. Найбільш популярними протоколами стека OSI є протоколи, що реалізують високорівневі сервіси з передачі файлів, емуляції терміналу, ведення каталогів імен і з організації електронної пошти. Хоча в стеці OSI передбачається ще ряд додаткових високорівневих сервісів, багато з них ще не реалізовані або реалізовані

частково.

Таблиця 10.1. *Перелік основних протоколів стеку OSI*

Рівень моделі 0SI	Протоколи OSI
7.Прикладний	FTAM,VTP,X.400 і X.500
6.Представлення	Протокол представлення OSI
5.Сеансовий	Сеансовий протокол OSI
4.Транспортний	Транспортний протокол 0S1
3.Мережевий	ES-IS, IS-IS
2.Канальний	Ethernet, TokenRing, FDDI, X.25, ISDN, ATM, LAP-D, PPP та інші.
1.Фізичний	Специфікації фізичних середовищ

Через свою складність протоколи OSI вимагають більших витрат обчислювальної потужності центрального процесора, що робить їх більш підходящими для потужних машин, а не для мереж персональних комп'ютерів.

Стек OSI - міжнародний, незалежний від виробників, стандарт. Його підтримує уряд США у своїй програмі GOSIP, відповідно до якої всі мережі, які установлювалися в урядових закладах США після 1990 року, повинні або безпосередньо підтримувати стек OSI, або забезпечувати засоби для переходу на цей стек у майбутньому. Проте, стекOSI більш популярний у Європі, а не в США, тому що в Європі менше встановлено старих мереж, що використовують свої власні протоколи. Більшість організацій поки тільки планують перехід до стеку OSI, і далеко не всі приступили до створення пілотних проектів. З тих, хто працює в цьому напрямку, можна назвати Військово-морське відомство США й мережа NFSNET. Одним з найбільших виробників, що підтримують OSI, є компанія AT&T, її мережа Stargroup повністю базується на цьому стеці.

Кожному рівню моделі OSI відповідає один або кілька протоколів, які виконують функції забезпечення мережевої взаємодії [3].

На фізичному і канальному рівнях стека OSI використовуються стандартні протоколи Ethernet, TokenRing тощо.

Мережевий рівень реалізований за допомогою протоколів ES-IS і IS-IS.

ES-IS (End System to Intermediate System routing exchange protocol) –

протокол маршрутизації кінцевих систем, за допомогою якого кінцеві системи (робочі станції) сповіщають про себе проміжні системи (наприклад, концентратори).

IS-IS (Intermediate System to Intermediate System routing exchange protocol) – протокол маршрутизації проміжних станцій, за допомогою якого проміжні системи обмінюються інформацією про діючі маршрути в мережі [1].

Ці протоколи використовуються для "розвідки" і побудови повної, послідовної картини топології мережі, щоб забезпечити можливість маршрутизації пакетів, які пересилаються.

Транспортний, сеансовий і рівень представлення реалізовані відповідними протоколами OSI, які мають мале поширення.

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

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

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

X.400 – являє собою набір рекомендацій Міжнародного союзу електрозв'язку (ITU)**,** у яких описуються системи пересилання електронних повідомлень. Протокол X.400 визначає структуру повідомлень електронної пошти так, що всі повідомлення задовольняють стандартний формат [3].

X.500 – розширення стандарту X.400, який визначає формат адреси повідомлення, що й дозволяє всім системам електронної пошти зв'язуватися міжсобою. З самого початку метою рекомендацій X.500 є розробка стандартів глобальної довідкової служби. Однак процес доставки повідомлення вимагає знання адреси одержувача. При великих розмірах мереж виникає проблема зберігання, пошуку й одержання адрес. Рішенням цієї проблеми є довідкова служба, яка допомагає одержувати адреси відправників і одержувачів, що й являє собою розподілену базу даних імені адрес [3].

Модель OSI зробила популярною ідею загальної моделі рівнів протоколів, яка визначає взаємодію міжмережевим обладнанням і програмним

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

Таким чином, колибули реалізовані протоколи для моделі OSI, виявився ряд проблем:

- Протоколи засновані на концепціях, які не мають актуальності в сучасних мережах;
- Специфікації у деяких випадках виявилися неповними або такими, що суперечать одна одній;
- За функціональними можливостями протоколи ISO/OSI поступалися іншим протоколам;
- Наявність великої кількості рівнів вимагає більшої обчислювальної потужності і, як наслідок, призводить до зменшення швидкодії.

10.3. Стек протоколів TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol)* — це *Протокол керування передачею/міжмережевий протокол*. Фактично TCP/IP представляє базовий набір протоколів, відповідальний за розбивання вихідного повідомлення на пакети (TCP), доставку пакетів на вузол адресата (IP) і збирання (відновлення) вихідного повідомлення з пакетів (TCP) .

Протоколи сімейства TCP/IP можна представити у вигляді спрощеної моделі взаємодії відкритих систем, що складається з чотирьох рівнів: *прикладного (Application layer), транспортного (Transport layer), міжмережного, чи рівня Інтернету (Internet layer)* і *мережного інтерфейсу (Network Interface layer)*. Основні протоколи TCP/IP - це набір стандартів, що

необхідні для з'єднання комп'ютерів і міжмережної взаємодії. В табл. 10.2 приведено перелік основних протоколів у відповідності до рівня на якому вони працюють [4].

Таблиця 10.2. *Перелік основних протоколів стеку TCP/IP*

<table>
<tr><td colspan="2">HTTP, FTP, SSH, TELNET, SMTP, DNS …</td><td>Прикладний рівень</td></tr>
<tr><td>TCP</td><td>UDP</td><td>Транспортний рівень</td></tr>
<tr><td colspan="2">IP, ARP, ICMP,RIP,OSPF</td><td>Міжмережний рівень</td></tr>
<tr><td colspan="2">Ethernet, PPP, SLIP, HDLC, FrameRelay</td><td>Мережний рівень</td></tr>
</table>

В основі цієї моделі лежить рівень мережного інтерфейсу. Відповідні компоненти відповідають за відправлення в мережу і прийом з мережі кадрів, що містять пакети інформації. Кадри передаються по мережі як єдине ціле. Мережний рівень стеку TCP/IP відповідає фізичному і канальному рівням моделі взаємодії відкритих систем OSI (Open System Interconnection). Цей рівень у протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного і канального рівня. Розроблена також спеціальна специфікація, що передбачає використання технології ATM як транспорт канального рівня.

Протоколи міжмережного рівня інкапсулюють пакети даних у датаграми Інтернету і проводять необхідну маршрутизацію. До протоколів міжмережного рівня відносяться [4]:

- IP (Internet Protocol) - в основному для відправлення і маршрутизації пакетів між мережами і вузлами.
- ARP (Address Resolution Protocol) - для одержання адрес мережних адаптерів вузлів у рамках однієї фізичної мережі.
- ICMP (Internet Control Message Protocol) - для відправлення повідомлень та інформації про помилки, що пов'язані з доставкою пакетів.
- RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First) - складання і модифікація таблиць маршрутизації, збір маршрутної інформації

Транспортний рівень забезпечує сеанси зв'язку між комп'ютерами. Існує два транспортних протоколи: TCP (Transmission Control Protocol) і UDP (User Datagram Protocol). Використання одного з них залежить від обраного методу доставки даних.

TCP орієнтований на з'єднання і використовується прикладеннями, що зазвичай передають великі обсяги даних за одну операцію, тому що забезпечує надійне з'єднання, а також прикладеннями, яким необхідне підтвердження прийому даних.

Протокол UDP забезпечує не орієнтовану на з'єднання передачу даних і не гарантує доставку пакетів. Прикладення, що використовують протокол UDP, звичайно передають невеликі обсяги даних за одну операцію. Відповідальність за надійну доставку даних несе прикладення.

Завершує модель TCP/IP рівень, на якому прикладення одержують доступ до мережних компонентів. Тут працює безліч стандартних утиліт і сервісів протоколу TCP/IP, наприклад FTP, Telnet, SNMP і DNS.

Основними протоколами стека, що дали йому назву, є протоколи IP і TCP. Ці протоколи в термінології моделі OSI належать до мережного і транспортного рівнів, відповідно. IP забезпечує просування пакета по складеній мережі, а TCP гарантує надійність його доставки.

Упродовж тривалого часу використання в мережах різних країн і організацій стек TCP/IP увібрав у себе велику кількість протоколів прикладного рівня. До них належать такі популярні протоколи, як протокол пересилання файлів FTP, протокол емуляції терміналу telnet, поштовий протокол SMTP, що використовується в електронній пошті мережі Інтернет, гіпертекстові сервіси служби WWW і багато інших.

Оскільки стек TCP/IP спочатку створювався для глобальної мережі Інтернет, він має багато особливостей, які забезпечують йому перевагу перед іншими протоколами, коли йдеться про побудову мереж, що включають глобальні зв'язки. Зокрема, дуже корисною властивістю, завдяки якій цей протокол може застосовуватися у великих мережах, є його здатність фрагментувати пакети. Дійсно, складна складена мережа часто складається з

мереж, побудованих за зовсім різними принципами. У кожній із цих мереж може бути встановлена власна величина максимальної довжини одиниці переданих даних (кадру). У такому разі при переході з однієї мережі, що має більшу максимальну довжину кадру, в іншу, з його меншою максимальною довжиною, може виникнути необхідність поділу переданого кадру на кілька частин. Протокол IP стека TCP/IP ефективно розв'язує це завдання [5].

Іншою особливістю технології TCP/IP є гнучка система адресації, що дозволяє більш просто в порівнянні з іншими протоколами аналогічного призначення включати до інтермережі (об'єднаної мережі) мережі інших технологій. Ця властивість також сприяє застосуванню стека TCP/IP для побудови великих гетерогенних (різнорідних) мереж.

Рівень мережевого інтерфейсу – рівень доступу (Network Interface – Network Access Layer) стека TCP/IP. Найнижчий рівень стека TCP/IP відповідає фізичному і канальному рівням моделі OSI. У стеку протоколів TCP/IP цей рівень не регламентує. Рівень мережевого інтерфейсу відповідає за прийом дейтаграмм і передачу їх конкретною мережею. Інтерфейс із мережею може бути реалізований драйвером пристрою або системою (комутатор, маршрутизатор), що використовує свій протокол канального рівня. Він підтримує стандарти фізичного і канального рівнів популярних локальних мереж: Ethernet, Token Ring, FDDI тощо. Для територіально-розподілених мереж підтримуються протоколи з'єднань PPP і SLIP, а для глобальних мереж — протокол X.25. Передбачено підтримку технології асинхронної комутації — ATM. Звичайною практикою стало включення до стеку протоколів TCP/IP нових технологій локальних або розподілених мереж і регламентація їх новими документами RFC.

Мережевий рівень стека TCP/IP — це рівень міжмережної взаємодії. Рівень управляє взаємодією між користувачами в мережі.Він приймає запит на посилку пакета від транспортного рівня разом із зазначенням адреси одержувача. Рівень інкапсулює пакету дейтаграму, заповнює її заголовок і за необхідності використовує алгоритм маршрутизації. Рівень обробляє дейтаграми, що надходять, і перевіряє правильність інформації. На стороні

одержувача програмне забезпечення мережного рівня видаляє заголовок дейтаграми і визначає, який із транспортних протоколів оброблятиме пакет.

Як основний протокол мережного рівня в стеку протоколів TCP/IP використовується протокол IP, що створювався саме з метою передачі інформації в розподілених мережах. Перевагою протоколу IP є можливість його ефективної роботи в мережах зі складною топологією. При цьому протокол раціонально використовує пропускну здатність низькошвидкісних ліній зв'язку. В основі протоколу IP закладений неорієнтований на з'єднання та ненадійний протокол передавання [4].

Термін «неорієнтований на з'єднання» означає, що сеанс для обміну даними не встановлюється. Термін «ненадійний» означає, що доставка не гарантується. IP – пакет може бути втрачено, передано поза чергою, продубльовано або затримано.

Транспортний рівень стека TCP/IP. Основним завданням транспортного рівня стека TCP/IP є взаємодія між прикладними програмами. Транспортний рівень виконує дві функції:

- Управляє потоком;
- Гарантує надійність передачі.

Для цього в TCP/IP використаний механізм підтвердження правильного прийому з дублюванням передачі загублених пакетів або пакетів, що надійшли з помилками. Транспортний рівень приймає дані від декількох прикладних програм і надсилає їх нижньому рівню. При цьому він долучає додаткову інформацію до кожного пакета, у тому числі контрольну суму [5].

В основі транспортного рівня стека TCP/IP лежить ***TCP (Transmission Control Protocol)*** – протокол керування передачею, що працює з установкою логічного з'єднання між віддаленими прикладними процесами, а також використовує принцип автоматичної повторної передачі пакетів, які містять помилки [4].

На транспортному рівні використовуються два протоколи:

- TCP — протокол зі встановленням з'єднання і квитуванням. Він відповідає за розбиття повідомлень на сегменти, їх збирання у вузлі

призначення, повторне відсилання всього, що виявилося неотриманим, ізбирання повідомлень із сегментів. Протокол TCP забезпечує гарантовану доставку даних за рахунок утворення логічних (віртуальних) з'єднань між віддаленими прикладними процесами;

- Протокол дейтаграм користувача (User Datagram Protocol, UDP), не орієнтований на встановлення з'єднання. Хоча протокол UDP і відповідає за передачу повідомлень, на цьому рівні квитування не застосовується, оскільки відсутнє програмне забезпечення для перевірки доставки сегментів.

10.4. Стек протоколів IPX/SPX

Протоколи без встановлення з'єднання використовуються для передачі не дуже важливих повідомлень, а також у тому разі, якщо повідомлення досить коротке і при його втраті аплікація користувача можена дислати повторний запит. Наприклад, UDP використовується для передачі широкомовних повідомлень усім вузлам підмережі. Незважаючи на низьку надійність, протоколи без встановлення попереднього з'єднання все – таки мають деякі переваги: їх простота і швидкість передачі обумовлюють нижчу вартість комунікації.

Цей стек є оригінальним стеком протоколів фірми Novell, розробленим для мережевої операційної системи NetWare ще на початку 80-х років. Протоколи Internetwork Packet Exchange (IPX) і Sequenced Packet Exchange (SPX), якій дали назву стеку, є прямою адаптацією протоколів XNS фірми Xerox, поширених набагато менше, ніж стек IPX/SPX. Популярність стека IPX/SPX безпосередньо пов'язана з операційною системою (ОС) Novell NetWare [3].

Цей стек орієнтувався на роботу в локальних мережах невеликих розмірів, які мають невеликі обчислювальні потужності, тому протоколи IPX/SPX мають свої особливості (табл.10.3).

Таблиця10.3. *Стек протоколу IPX/SPX*

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

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

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

IPX (Internetwork packet exchange) – між мережевий обмін пакетами - протокол, що регламентує обмін даними мережею і працює за дейтаграмним принципом, тобто без встановлення попереднього логічного з'єднання, що забезпечує більш економне споживання обчислювальних ресурсів.

RIP (Routing InformationProtocol) – протокол маршрутної інформації, являє собою один з найстарших протоколів, які реалізують процеси обміну маршрутною інформацією, однак він дотепер надзвичайно розповсюджений в обчислювальних мережах.

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

На рівні, який відповідає транспортному, використовується протокол SPX, що дав частину назви стеку, у якому він і використовується.

SPX (Sequenced Packetexchange) – упорядкований обмін пакетами – комунікаційний протокол, розроблений для використання в мережах NetWare.

SPX працює з встановленням логічного з'єднання й забезпечує гарантовану доставку й порядок повідомлень у потоці пакетів, для посилки яких використовує протокол IPX.

На верхніх рівнях використовуються протоколи NCP і SAP.

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

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

На сьогоднішній день стек IPX/SPX реалізований не тільки в NetWare, але й у декількох інших популярних мережевих ОС, наприклад Microsoft Windows. Починаючи з версії 5.0 фірма Novell в якості основного протоколу своєї серверної операційної системи стала використовувати протокол TCP/IP, і з того часу практичне застосування IPX/SPX стало неухильно знижуватися.

10.5. Стек протоколів NetBIOS/SMB

Стек NetBIOS/SMB – спільний проект компаній Microsoft та IBM, розроблений у1984р.(табл.10.4).

Стек працює з усіма найбільш розповсюдженими протоколами нижнього рівня.

На верхніх рівнях працюють протокол NetBEUI та SMB.

Протокол NetBIOS (Network BasicInput/Output System) став розширенням стандартних функцій базової системи введення/виведення (BIOS-BaseInput/Output System), який забезпечує підтримку роботи в мережі. Уподальшому Net BIOS був замінений протоколом NetBEUI. При цьому

NetBIOS все ж був збережений для забезпечення сумісності додатків [1].

NetBEUI (NetBIOS Extended UserInterface) – протокол розширеного користувальницького інтерфейсу NetBIOS, який надає функції, що відносяться до сеансового, транспортного і частково до мережевого рівнів моделі OSI.

NetBIOS підтримує як дейтаграмний спосіб обміну даними, так і обміні з установленням логічних з'єднань. Однак цей протокол не забезпечує маршрутизацію пакетів, тому його застосування обмежується тільки невеликими локальними мережами. Для вирішення цієї проблеми використовується NBF (NetBEUI Frame) – реалізація цього протоколу, який вперше з'явився в операційній системі Microsoft Windows NT. Проте в складних мережах використовують більш універсальні протоколи стеків TCP/Ip та IPX/SPX.

SMB (Server Message Block) - протокол, який виконує функції прикладного рівня і рівня представлення моделі OSI, визначає взаємодію робочої станції та сервера.

Таблиця 10.4. *Стек протоколів NetBIOS/SMB*

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

SMB надає основні мережеві сервіси, необхідні додаткам: керування сесіями передачі даних, встановлення та ліквідацію логічного з'єднання, доступ для роботи з файлами, друк по мережі, передачу повідомлень тощо.

Такі стеки, як AppleTalk компанії Apple, SNA фірми IBM або стек DECnet корпорації Digital Equipment, одержали менше поширення, тому що застосовуються в основному в операційних системах і мережевому обладнанні, вироблених перерахованими фірмами, і, відповідно, орієнтованих на використання системних архітектурі апаратних платформ цих же фірм [1].

Будь-який протокол за тими або іншими умовами може відповідати деякому рівню моделі OSI. Однак, у силу того, що розробники не суворо дотримуються моделі OSI і багато протоколів і стеків з'явилося до розробки еталонної моделі, найчастіше протоколи можуть відноситися відразу до декількох рівнів, або навпаки, виконувати тільки частину функцій одного з рівнів. Усе це приводить до того, що для того щоб забезпечити успішну роботу протоколів і реалізувати закінчений набір функцій, що забезпечують обмін даними мережею, доводиться використовувати протоколи з одного стеку. Це приводить до несумісності зі стандартною моделлю відкритих систем.

10.6. Особливості поширених протоколів

Протоколи, що використовуються для обміну даними в локальних мережах, поділяються за своєю функціональністю на три типи [3]:

- прикладні;
- транспортні;
- мережеві.

Прикладні протоколи виконують функції трьох верхніх рівнів моделі OSI - прикладного, рівня представлення і сеансового. Вони забезпечують взаємодію додатків і обмін даними між ними. До найбільш популярних прикладних протоколів відносяться:

- ***FTAM (File Transfer Access and Management) – протокол OSI доступу до файлів;***
- ***X.400*** – протокол OSI для міжнародного обміну електронною поштою;
- ***X.500*** - протокол OSI служб файлів і каталогів на декількох системах;
- ***SMTP (Simple Mail Transfer Protocol)*** – протокол Інтернету для обміну

електронною поштою;

- ***FTP (File Transfer Protocol)*** – протокол Інтернету для передачі файлів;
- ***Telnet*** – протокол Інтернету для реєстрації на віддалених серверах і обробки даних на них;
- ***SMB (Server Message Blocks)*** – протокол взаємодії робочої станції і серверу фірми Microsoft;
- ***NCP (Net Ware Core Protocol)*** – протокол передачі даних між сервером NetWare і робочою станцією фірми Novell;
- ***Apple Talku Apple Share*** – набір мережевих протоколів фірми Apple;
- ***AFP (AppIe Talk Filling Protocol)*** – протокол віддаленого доступу до файлів фірми Apple;
- ***DAP (Data Access Protocol)*** – протокол доступу до файлів мереж DECnet.

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

- ***TCP (Transmission Control Protocol)*** – протокол Інтернету для гарантованої доставки даних, розбитих на послідовність фрагментів;
- ***SPX (Sequential Packet Exchange)*** – протокол стеку IPX/SPX для передачі даних, розбитих на послідовність фрагментів, фірми Novell;
- ***NetBIOS (Network Basic Input/Output System)*** – протокол встановлення і контролю сеансів зв'язку між комп'ютерами;
- ***ATP (AppIe Talk Transaction Protocol), NBP (Name Binding Protocol)*** – протоколи сеансів зв'язку і транспортування даних фірми Apple.

Мережеві протоколи виконують функції трьох нижніх рівнів моделі OSI-мережевого, канального й фізичного. Ці протоколи управляють адресацією, маршрутизацією, перевіркою помилок і повторною передачею кадрів, забезпечуючи послуги зв'язку, і визначають правила здійснення зв'язку в окремих середовищах передачі даних, наприклад, Ethernet або Token Ring. До найпопулярніших мережевих протоколів відносяться:

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

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

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

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

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

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

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

Транспортні протоколи здійснюють передачу даних, використовуючи послуги мережевих протоколів, відповідальних за керування адресацією, маршрутизацію в мережах, забезпечення надійності передачі даних тощо.

10.7. Протоколи сигналізації для управління з'єднаннями

Основними протоколами сигналізації для управління з'єднаннями сьогодні є **SIP, СКС-7, H.323.**

Основними протоколами сигналізації управління транспортними шлюзами є **MGCP і MEGACO/H.248**, а основними протоколами сигналізації взаємодії між Softswitch – **SIPT і BICC** [3].

Протокол RTP дозволяє компенсувати негативний вплив джіттера на якість мовної і відео інформації, але в той же час він не має власних механізмів, що гарантують своєчасну доставку пакетів або інші параметри якості послуг, - це здійснюють ніжележащие протоколи. Він навіть не забезпечує всі ті функції,

які зазвичай надають транспортні протоколи, зокрема функції виправлення помилок і управління потоком. Зазвичай протокол RTP базується на протоколі UDP і використовує його функції, але може працювати і поверх інших транспортних протоколів.

Протокол H.323. Для побудови мереж IP-телефонії першою стала рекомендація H.323 MCE-T, яка є також першою специфікацією систем мультимедійного зв'язку для роботи в мережах з комутацією пакетів, що не забезпечують гарантовану якість обслуговування.

Протокол SIP. Протокол ініціації сеансів – Session Initiation Protocol SIP) – є протоколом прикладного рівня і призначається для організації, модифікації і завершення сеансів зв'язку: мультимедійних конференцій, телефонних з'єднань і розподілу мультимедійної інформації. Протокол SIP може бути використаний спільно з протоколом H.323. Можливо також взаємодія протоколу SIP з системами сигналізації ТФЗК - DSS1 і СКС7.

Протокол MGCP. Робоча група MEGACO комітету IETF розробила протоколу правління шлюзами – Media Gateway Control Protocol (MGCP).

При розробці протоколу управління шлюзами робоча група MEGACO спиралася на принцип декомпозиції, згідно якому шлюз розбивається на окремі функціональні блоки. Протокол MGCP є внутрішнім протоколом, що підтримує обмін інформацією між функціональними блоками розподіленого шлюзу. Протокол MGCP використовує принцип master/slave, при чому пристрій управління шлюзами є таким, що веде, а транспортний шлюз - пристроєм, який виконує команди, що поступають від пристрою управління.

Контрольні питання до розділу

21.Дайте визначення поняттю «Протокол взаємодії»*?*
22.Дайте визначення поняттю «Стек протоколів**»**?
23.В чому полягає різниці між пняттми «модель OSI» і «стек OSI»***?***
24.Наведіть перелік основних протоколів стеку OSI?
25.Дайте визначення поняттю «Стек протоколів TCP/IP»?
26.Особливості рівня мережевого інтерфейсу стека TCP/IP?
27.Особливості мережевого рівня стека TCP/IP?
28.Особливості транспортного рівня стека TCP/IP?
29. Стек протоколів IPX/SPX?

30. Стек протоколів NetBIOS/SMB?
31. Наведіть особливості поширених протоколів?
32. Які протоколи відносяться до протоколів сигналізації для управління з'єднаннями.

Список рекомендованої літератури

1. *Олифер В. Г.*, *Олифер Н. А.* Компьютерные сети. Принципы, технологии, протоколы. — 4-е изд. — СПб.:Питер, 2010. — С. 438. — 4500 экз. — ISBN 978-5-49807-389-7.
2. Компьютерные сети. 4-е изд./ *И. Таненбаум*. – СПб.: Питер, 2003. – 992 с.
3. *Стрихалюк Б. М.* Теорія побудови та протоколи інфокомунікаційних мереж: Конспект лекцій. – Львів: Львівська політехніка, 2017. – 121 с.
4. *Р. Стивенс* Протоколы TCP/IP. Практическое руководство. – Спб.: БХВ, 2003
5. *Дуглас Камер* Сети TCP/IP, том 1. Принципы, протоколы и структура = Internetworking with TCP/IP, Vol. 1: Principles, Protocols and Architecture. – М.: «Вильямс», 2003. – С. 880. – ISBN 0-13-018380-6.