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

ОСНОВИ ТЕОРІЇ ТЕЛЕКОМУНІКАЦІЙ І РАДІОТЕХНІКИ

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського як навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Інформаційно-обчислювальні засоби радіоелектронних систем» спеціальності 172 «Телекомунікації та радіотехніка»

Київ

КПІ ім. Ігоря Сікорського

2020

Основи теорії телекомунікацій і радіотехніки [Електронний ресурс] : навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка»/ КПІ ім. Ігоря Сікорського ; уклад.: П. В. Кучернюк. – Електронні текстові дані (1 файл: 4,3 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 290 с.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 10 від 18.06.2020 р.) за поданням Вченої ради Факультету електроніки (протокол № 05/2020 від 25.05.2020 р.)

Електронне мережне навчальне видання

ОСНОВИ ТЕОРІЇ ТЕЛЕКОМУНІКАЦІЙ І РАДІОТЕХНІКИ

Укладач Кучернюк Павло Валентинович, канд. техн. наук, доц.

Відповідальний редактор Корнєв В.П., канд. техн. наук, доц.

Рецензент Цурін О.П., канд. техн. наук, доц., КПІ ім. Ігоря Сікорського

Навчальний посібник містить матеріали, які використовуються як безпосередньо у теоретичному курсі, так і матеріали для самостійної роботи студентів і підготовки до лабораторних робіт. У посібнику докладно розглянуто основні характеристики інформаційних каналів та поняття, які використовуються у теорії телетрафіку, базові методи та підходи до побудови систем передачі даних, особливості представлення даних в інформаційних каналах, особливості різних типів фізичних середовищ передачі даних та їх основні характеристики, різні типи мережних топологій, модель мережної архітектури, базові методи передачі даних, які покладено в основу побудови різних протоколів канального рівня, особливості архітектури та протоколів локальних мереж, особливості протоколів стеку TCP/IP, протоколу IPv6, системи доменних імен, питання маршрутизації.

Посібник призначений для студентів-здобувачів ступеня бакалавра за освітньою програмою «Інформаційно-обчислювальні засоби радіоелектронних систем» спеціальності 172 «Телекомунікації та радіотехніка».

ЗМІСТ

	ВСТУП	7
1.	БАЗОВІ ПОНЯТТЯ Й ОСНОВИ ПЕРЕДАЧІ ДАНИХ	9
	1.1. Основні характеристики інформаційних каналів	9
	1.2. Деякі поняття, що використовують в теорії телетрафіку	13
	1.3. Базові методи представлення та передачі даних	15
	1.3.1. Модуляція сигналу	15
	1.3.2. Концентрація й ущільнення	18
	1.3.3. Технології спектрального ущільнення WDM	21
	1.3.4. Імпульсно-кодова модуляція	25
	1.3.5. Синхронізація елементів мережі	28
	1.3.6. Логічне кодування	31
	1.3.7. Методи комутації	34
	1.3.8. Асинхронна/синхронна передача	37
	Питання для самоперевірки та контролю засвоєння знань	39
2.	ФІЗИЧНЕ СЕРЕДОВИЩЕ ПЕРЕДАЧІ	42
	2.1. Основні характеристики обмежених середовищ передачі	42
	2.2. Основні типи кабельних систем	48
	2.2.1. Поняття структурованих кабельних систем	48
	2.2.2. Кабель «вита пара» («Twisted Pair» - TP)	49
	2.2.3. Коаксіальний кабель	54
	2.2.4. Волоконно-оптичний кабель	56
	2.2.5. Розрахунок бюджету втрат оптичної системи	69
	2.3. Необмежене середовище передачі	73
	Питання для самоперевірки та контролю засвоєння знань	76
3.	ТОПОЛОГІЯ МЕРЕЖ	78
	3.1. Зіркоподібна структура	78
	3.2. Кільцева мережа	80

3.3. Петльова мережа 83
3.4. Шинна топологія 84
3.5. Деревоподібна топологія 85
3.6. Повнозв’язана структура (сітка) 87
3.7. Гібридна структура 88
Питання для самоперевірки та контролю засвоєння знань 88
4. МЕРЕЖНА АРХІТЕКТУРА 90
4.1. Модель мережної архітектури 91
4.2. Способи організації обміну даними 95
4.3. Методи доступу і управління каналом передачі даних 98
4.3.1.Система опиту/вибору 99
4.3.2. Опит/вибір з зупинкою та очікуванням 103
4.3.3. Безперервний автоматичний запит на повторення (безперервний ARQ або «ковзаючи вікна») 104
4.3.4. Системи без опиту 107
4.3.5. Множинний доступ з часовим розділенням (TDMA) 109
4.3.6. Рівнорангові методи 110
4.3.7. Мультиплексна передача з часовим розділенням (TDM) 110
4.3.8. Вставка регістру або буферу 110
4.3.9. Система з контролем несучої і виявленням колізії 111
4.3.10. Маркерні системи 115
4.3.11. Пріоритетні слотові системи 118
4.3.12. Системи з контролем несучої без колізій 118
4.3.13. Пріоритетні маркерні системи 119
4.4. Особливості моделі і архітектури локальних мереж 120
4.4.1. Керування логічним каналом (LLC) і стандарт 802.2 122
4.4.2. Множинний доступ з контролем несучої і виявленням колізій (стандарт 802.3) 127
4.4.3. Пріоритетне маркерне кільце (стандарт 802.5) 138

Питання для самоперевірки та контролю засвоєння знань 143
5. СТРУКТУРА СТЕКУ ПРОТОКОЛІВ TCP/IP 148
5.1. Характеристика рівнів стеку TCP/IP 148
5.2. Особливості протоколу IP 151
5.3. Особливості IP- адресації 155
5.3.1. Класи IP-адрес 156
5.3.2. Особливі типи IP-адрес 159
5.3.3. Використання масок для сегментації IP- мереж 162
5.4. Протокол ICMP 166
5.4.1. Формат повідомлень протоколу ICMP 167
5.4.2. Типи повідомлень ICMP 167
5.5. Протокол перетворення адрес ARP 171
5.6. Протокол зворотного перетворення адрес RARP 174
5.7. Протокол TCP 174
5.7.1. Встановлення TCP-з'єднання 175
5.7.2. Ковзаюче вікно TCP 177
5.7.3. Регулювання трафіку 178
5.7.4. Формат TCP-пакету 182
5.8. Протокол UDP 183
5.9. Особливості протоколу IPv6 185
5.9.1. Особливості адресації в IPv6 186
5.9.2. Типи адрес 187
5.9.3. Агрегування адрес 194
5.9.4. Формат заголовка IP-пакета 197
5.9.5. Зниження навантаження на маршрутизатори 200
5.10. Особливості системи доменних імен (DNS) 201
Питання для самоперевірки та контролю засвоєння знань 211
6. ПРОТОКОЛИ МАРШРУТИЗАЦІЇ 218
6.1. Класифікація алгоритмів маршрутизації 221

6.2. Поняття метрики маршрутів 225
6.3. Дистанційно-векторний протокол RIP 227
6.3.1. Формат пакету RIP v2 228
6.3.2. Алгоритм побудови таблиць маршрутизації 229
6.3.3. Адаптація RIP-маршрутизаторів до змін стану мережі 231
6.3.4. Методи боротьби з помилковими маршрутами в протоколі RIP 237
6.4. Протокол стану каналів OSPF 239
6.4.1. Ієрархічна маршрутизація (розбиття на області) 240
6.4.2. Побудова маршрутів 240
6.4.3. Алгоритм SPF 245
6.4.4. Формат пакета 247
6.5. Протоколи IGRP і EIGRP 249
6.5.1. Особливості протоколу IGRP 249
6.5.2. Особливості протоколу EIGRP 252
6.6. Протоколи EGP і BGP 258
6.6.1. Особливості протоколу EGP 258
6.6.2. Особливості протоколу BGP 262
6.7. Протоколи групової маршрутизації IGMP, DVMPR, MOSPF, PIM 271
6.7.1. Особливості протоколу IGMP 272
6.7.2. Особливості протоколу DVMRP 277
6.7.3. Особливості протоколу MOSPF 278
6.7.4. Особливості протоколу PIM 279
Питання для самоперевірки та контролю засвоєння знань 281
БІБЛІОГРАФІЧНИЙ СПИСОК 284
ПЕРЕЛІК СКОРОЧЕНЬ 286

ВСТУП

Розвиток нових технологій представлення та передачі даних, безперервно зростаючі обсяги потоків даних, серед яких значне місце відіграє аудіо та відеоінформація, потребує перегляду базових принципів створення та обслуговування сучасних телекомунікаційних мереж, а також апаратних та програмних засобів телекомунікаційних систем. Аналіз розвитку світової економіки дає підстави вважати, що під впливом нових задач та нових галузей застосування телекомунікаційні технології є тим напрямом сучасної інженерії, що найбільш динамічно змінюється.

Втілення новітніх телекомунікаційних технологій, стрімке зростання номенклатури та галузей застосування мережного обладнання, що має різноманітне призначення, висувають нові вимоги до підготовки інженерно-технічних кадрів у вищих навчальних закладах. Сучасні спеціалісти мають бути здатні вирішувати широке коло питань проектування інформаційних мереж, інсталяції та обслуговування телекомунікаційного обладнання, планування його роботи та адміністрування, а також розв’язувати задачі проектування електронної апаратури, що входить до складу телекомунікаційних систем, її тестування, модернізації, експлуатації, наладки та ремонту, створення відповідного програмного забезпечення.

Дисципліна «Основи теорії телекомунікацій і радіотехніки» відноситься до циклу нормативних навчальних дисциплін першого (бакалаврського) рівня вищої освіти за спеціальністю 172 – телекомунікації та радіотехніка. Навчальна програма дисципліни враховує особливості підготовки студентів за освітньою програмою «Інформаційно-обчислювальні засоби радіоелектронних систем».

Навчальний посібник з дисципліни «Основи теорії телекомунікацій і радіотехніки» є першим з групи навчальних посібників по дисциплінам інформаційно-телекомунікаційного напрямку за освітньою програмою «Інформаційно-обчислювальні засоби радіоелектронних систем». Крім цієї дисципліни студентам другого (магістерського) рівня вищої освіти

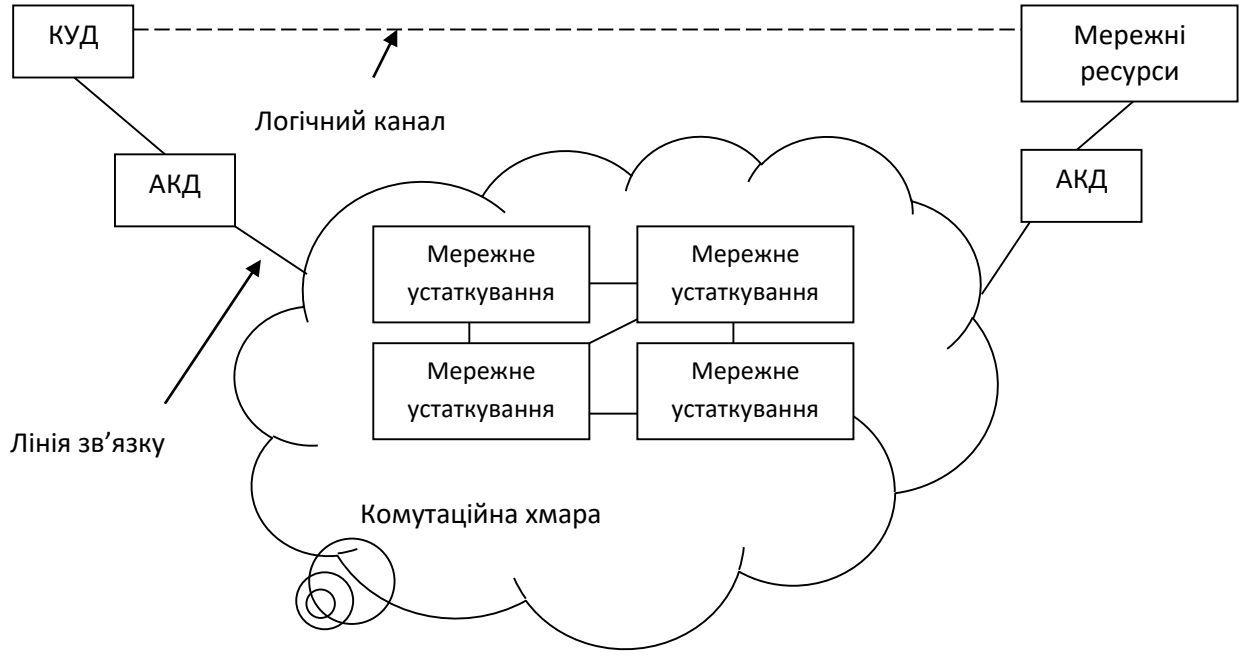
викладається дисципліна «Комп'ютерні мережі та засоби телекомунікацій», у якій вивчаються базові технології передачі даних локальних та глобальних мереж та особливості різних типів телекомунікаційного обладнання, і дисципліна «Технології та засоби керування в інформаційних мережах», у якій вивчаються протоколи управління мережним обладнанням, міжнародні стандарти і концепції побудови систем управління, програмні засоби аналізу та управління інформаційними мережами.

Начальний посібник з дисципліни «Основи теорії телекомунікацій і радіотехніки» містить матеріали, які використовуються як безпосередньо у теоретичному курсі, так і матеріали для самостійної роботи студентів і підготовки до лабораторних робіт. Ці матеріали поділено на шість розділів. У першому розділі посібника розглядаються основні терміни та визначення, базові методи та підходи до побудови систем передачі даних, особливості представлення даних в інформаційних каналах. У другому розділі посібника розглянуто особливості різних типів фізичних середовищ передачі даних та їх основні характеристики. Третій розділ посібника знайомить студентів з різними типами мережних топологій. У четвертому розділі посібника розглянуто модель мережної архітектури, базові методи передачі даних, які покладено в основу побудови різних протоколів канального рівня, особливості архітектури та протоколів локальних мереж. П'ятий розділ посібника присвячений вивченню особливостей протоколів стеку TCP/IP, IP – адресації, протоколу IPv6, системи доменних імен. У шостому розділі розглядаються питання маршрутизації між різними мережами, особливості протоколів маршрутизації внутрішнього та зовнішнього шлюзів, протоколів групової маршрутизації.

1. БАЗОВІ ПОНЯТТЯ Й ОСНОВИ ПЕРЕДАЧІ ДАНИХ

1.1. Основні характеристики інформаційних каналів

Спрощена структура будь-якої мережі передачі даних (глобальної або локальної) може бути подана в наступному вигляді (рис.1.1) [О: 1].



КУД(DTE) - кінцеве устаткування даних

АКД(DCE) - апаратура каналу даних

Рисунок 1.1 - Узагальнена структура мережі передачі даних

КУД (DTE) - кінцеве устаткування даних, виконує функції генерації, прийому й передачі даних. Прикладами таких пристроїв можуть служити персональні комп'ютери, касові апарати, банкомати, різного типу термінали й т.д.

АКД (DCE) - апаратура каналу даних, виконує інтерфейсні функції для забезпечення комунікацій кінцевих вузлів з мережею (наприклад, мережний адаптер, модем і т.д.). Підключення до мережі й передача даних здійснюється

за допомогою ліній зв'язку (проводових або безпроводових) з використанням відповідного протоколу передачі даних (наприклад, протоколу Ethernet у випадку локальної мережі).

Комутаційна хмара - мережа передачі даних, що складається з мережного устаткування (концентратори, комутатори, маршрутизатори й т.п. пристрої), з'єднаного каналами передачі даних (проводових/бездротових).

Протоколи передачі даних у комутаційній хмарі можуть збігатися із протоколами, що використовуються у лініях зв'язку (у випадку локальних мереж), або відрізнятися від них (у випадку територіально-розподілених або глобальних мереж).

Мережні ресурси – ресурси, що колективно використовуються багатьма користувачами (сервери різного призначення, дискові масиви інформації, периферійні пристрої й т.п.).

Кінцеві пристрої й мережні ресурси зв'язані логічним каналом, що утворюється за допомогою мережного програмного забезпечення (UNIX, Windows) і відповідних мережних протоколів (наприклад, протоколів стеку TCP/IP).

Потік даних, що передається мережею, називається мережним трафіком або просто трафіком .

Приймач-передавач АКД може здійснювати передачу даних у лінію зв'язку з використанням одного з трьох методів [О: 1, 2].

- Симплексний метод - передача даних здійснюється тільки в одному напрямку. Даний метод практично не використовується в інформаційних мережах, а застосовується в радіомовленні, телебаченні й телеметричних схемах, де дані передаються на обробні або виконавчі пристрої.
- Напівдуплексний (двоспрямований по черзі) - передача здійснюється в обох напрямках, але в кожний момент часу передача ведеться тільки в одному напрямку. Метод застосовується в різних системах опитування/вибору (наприклад, багатотермінальних комплексах), деяких

технологіях локальних мереж (наприклад, Ethernet на коаксіальному кабелі).

- Повнодуплексний (одночасно двоспрямований) - у кожний момент часу передача може вестися в обох напрямках.

Поняття напівдуплексний і дуплексний іноді використовують для характеристики й самої лінії зв'язку. Так, у телефонії існує поняття 2-х проводової та 4-х проводової ліній. При цьому, 2-х проводову лінію називають напівдуплексною: по одній парі проводів може вестися або прийом, або передача (хоча, використовуючи різні прийоми, наприклад, диференціальне розділення вхідного й вихідного сигналів, можна й на одній парі проводів реалізувати дуплексну передачу). 4-х проводову лінію називають дуплексною: одна пара проводів використовується для прийомного каналу, друга - для передавального.

Передача даних здійснюється інформаційними каналами. Під каналом розуміють засіб для переміщення в просторі інформаційних сигналів. При цьому кілька інформаційних каналів можуть бути розміщені в одному фізичному середовищі передачі (наприклад, кілька частотних каналів у відкритому ефірі). Незалежно від того, як у каналі представлений сигнал (аналоговий або цифровий), будь-який канал характеризується пропускною здатністю, що визначається кількістю біт інформації переданих за секунду (біт/с).

Передача будь-якого інформаційного сигналу завжди здійснюється в обмеженому частотному діапазоні. У випадку телефонної мережі частотний діапазон аналогового телефонного сигналу має границі: 300 ÷ 3400 Гц. Ширина смуги пропускання частотного каналу (різниця між верхньою та нижньою частотами) для передачі телефонного сигналу становить $\Delta f = 3100$ Гц . Ширина смуги пропускання є основним параметром, що визначає пропускну здатність каналу. Будь-яке фізичне середовище передачі має обмежену смугу пропускання. Так мідний кабель, що використовується у телефонних мережах (багатопарний кабель «вита пара»), має ширину смуги пропускання $10^3 \div 10^4$ Гц,

коаксіальний кабель – $10^5 \div 10^8$ Гц, волоконно-оптичний кабель – $10^{14} \div 10^{15}$ Гц. Слід зазначити, що на ширину смуги пропускання впливають не тільки характеристики фізичного середовища передачі, але й характеристики пристроїв, підключених до цього середовища.

Крім ширини смуги пропускання на пропускну здатність каналу впливає фактична потужність сигналу, що передається й рівень шумів у каналі [О: 1, 2]. Залежність пропускної здатності від названих параметрів описується законом Шеннона:

$$C = W \log_2(1 + S/N),$$

де

C - максимальна пропускна здатність каналу, біт/с;

W - ширина смуги пропускання каналу, Гц;

S - потужність сигналу;

N - потужність шуму.

Із закону Шеннона випливає, що для збільшення максимальної пропускної здатності необхідно збільшувати ширину смуги пропускання, потужність сигналу, і зменшувати потужність шуму.

Для збільшення відношення S/N зазвичай використовують розміщення підсилювачів на каналах зв'язку (малоефективно у випадку аналогового сигналу, тому що одночасно відбувається підсилення як корисного сигналу, так і шумів; крім того, досить складно відновлювати форму корисного аналогового сигналу, що спотворюється при проходженні через лінії зв'язку).

Ширина смуги пропускання каналу буде також впливати на спотворення інформаційного сигналу [О: 1, 2]. Будь-який цифровий сигнал, шляхом розкладання в ряд Фур'є, можна подати у вигляді суми нескінченного числа синусоїд, які утворюються із синусоїдального коливання основної частоти (n Гц) і непарних гармонік (3n, 5n, 7n...), причому амплітуди цих гармонік зменшуються. Передача подібного сигналу через канал з обмеженою смугою пропускання приводить до спотворень, викликаних більш сильним загасанням

високочастотних гармонік і збільшенням затримок для високочастотних гармонік. У результаті, при великих відстанях, які проходить інформаційний сигнал, спотворення можуть бути настільки сильними, що неможливо розрізнити логічні «0» і «1» без спеціальних засобів. Для відновлення форми сигналу застосовуються різні методи обробки сигналу. Крім цього, практично в усіх системах передачі даних реалізована перевірка даних у приймачі на наявність помилок передачі з організацією повторної передачі, у випадку виявлення помилок (хоча при цьому знижується ефективна пропускна здатність каналу).

1.2. Деякі поняття, що використовують в теорії телетрафіку

Для теоретичного дослідження мереж використовується теорія масового обслуговування, яка при використанні стосовно телефонного зв'язку отримала назву теорії телетрафіку. Ця теорія вивчає процеси і закономірності проходження повідомлень по мережі, визначає ефективність використання комутаційних систем і ліній зв'язку, а також питання якості обслуговування абонентів.

Найбільш важливими поняттями теорії телетрафіку є виклики, навантаження і втрати.

Викликом називається заявка (спеціальний сигнал) одного із абонентів на встановлення з'єднання, тобто заявка на створення системи зв'язку між абонентами. Поняття виклику поширюється і на сам процес встановлення з'єднання.

Сукупність заявок, які надходять на станцію, називають потоком викликів. Важливим параметром потоків викликів є інтенсивність викликів, під якою розуміють число викликів, що виникли за одиницю часу. Виклики поступають нерівномірно, тобто інтенсивність виклику є непостійною величиною.

Для правильної побудови комутаційних систем необхідно знати сумарний час обслуговування викликів, які надходять за одиницю часу, який прийнято називати навантаженням. Одиниця виміру навантаження – годино-заняття. Для обчислення навантаження використовується вираз:

$$Y = Nct/T,$$

де N – число джерел навантаження (наприклад, число абонентів), c – кількість викликів за часовий інтервал T від одного джерела, t – тривалість обслуговування виклику.

У випадку паралельного обслуговування викликів використовується параметр інтенсивність навантаження. Інтенсивність навантаження вимірюється в годино-заняттях, розділених на години. Одиниця інтенсивності навантаження – Ерланг. Один Ерланг (Ерл) – це така інтенсивність навантаження, при якій протягом 1 години буде обслуговане навантаження в 1 годино-заняття. Інтенсивність навантаження визначається за формулою:

$$E = ct/T$$

і являє собою відносну величину зайнятості каналу передачі одним абонентом. Наприклад, E = 0,2 Ерл показує, що середньостатистичне сумарне значення всіх викликів абонента складає 12 хвилин за 1 год.

Інтенсивність навантаження підвержена різким коливанням протягом доби. Для розрахунку необхідного числа обладнання комутаційної станції прийнято враховувати так звану годину найбільшого навантаження (ГНН) – неперервні 60 хв. протягом доби, коли спостерігається максимальна інтенсивність навантаження.

На комутаційних станціях не всі виклики, що поступили, можуть бути обслуговані негайно через відсутність в необхідний момент вільних вихідних ліній. В цьому випадку абонент отримує сигнал «Зайнято», необслужений

виклик називають загубленим, а сам факт необслуговування – відмовою. Такі системи одержали назву систем комутації із втратами.

Існують, так звані, системи комутації з очікуванням, у яких при зайнятих вихідних лініях абонент не одержує відмови, а очікує звільнення однієї з ліній, після чого з'єднання буде встановлене.

Кількість загублених викликів в одиницю часу в системах із втратами і кількість абонентів, що одночасно очікують, у системах з очікуванням характеризують якість обслуговування телефонних мереж.

1.3. Базові методи представлення та передачі даних

1.3.1. Модуляція сигналу

Під модуляцією розуміють модифікацію параметрів одного сигналу іншим, який безпосередньо представляє інформаційні дані. Перший сигнал історично називають несучою частотою або частотою – носієм (носієм). Дані, які модулюють несучу, називають модулюючим сигналом [О: 1, 2].

Типовим призначенням модуляції у телекомунікаційних мережах є розподілення абенентських низькочастотних каналів у частотному діапазоні магістрального каналу передачі. Абонентський телефонний канал має частотну смугу 300 – 3400 Гц (Δf=3100 Гц). Смуга пропускання фізичних кабельних систем з проміжними підсилювачами становить від сотень КГц до сотень МГц. На таких фізичних лініях можна організовувати декілька каналів передачі в різних частинах частотного діапазону. Для розподілення абонентських каналів використовується модуляція ВЧ несучого синусоїдального сигналу НЧ мовним сигналом (рис. 1.2).

При потребі передачі цифрових даних через аналогові лінії зв'язку (наприклад, телефонні мережі) необхідно здійснювати перетворення цифрового сигналу в еквівалентні аналогові періодичні коливання й відновлювати вихідний цифровий сигнал у приймаючому пристрої. Такий тип перетворень ще називають цифровою модуляцією, або маніпуляцією. Пристрої, що

виконують цю функцію, називають модемами (скорочення від модулятор/демодулятор).

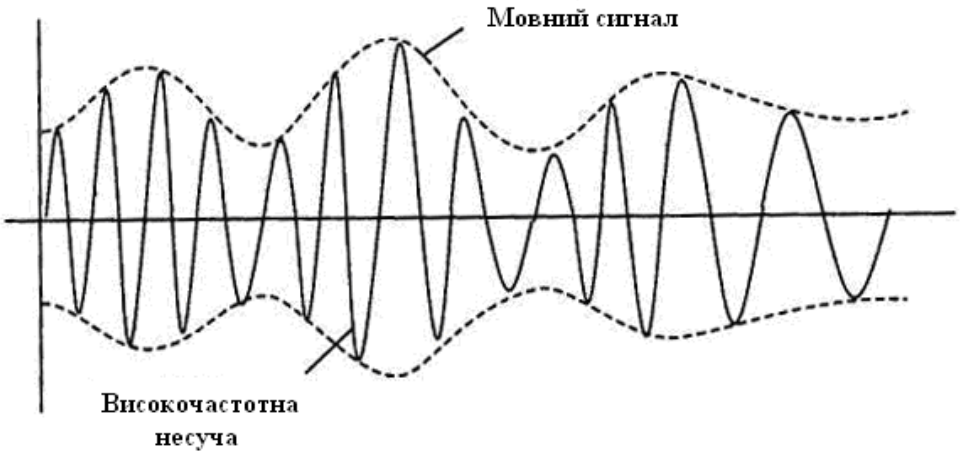


Рисунок 1.2 - Модуляція ВЧ-несучого синусоїдального сигналу НЧ-мовним сигналом

Існують наступні базові методи модуляції.

1. Амплітудна модуляція (АМ)- амплітуда несучого сигналу змінюється відповідно до вхідної послідовності біт (рис. 1.3).

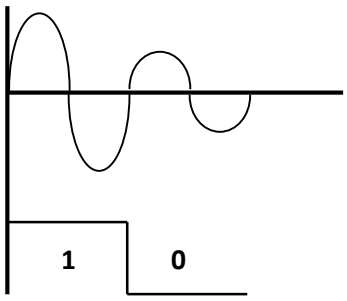


Рисунок 1.3 - Зміна несучого сигналу у випадку АМ

2. Частотна модуляція (ЧМ) – відповідно до вхідної послідовності біт змінюється частота несучого сигналу (рис. 1.4).

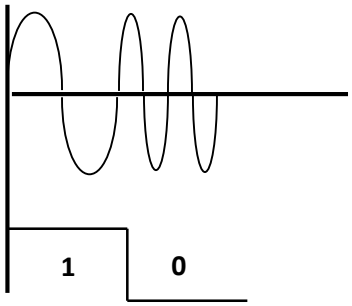


Рисунок 1.4 - Зміна несучого сигналу у випадку ЧМ

3. Фазова модуляція (ФМ) – відповідно до вхідної послідовності біт змінюється фаза несучого сигналу (рис. 1.5).

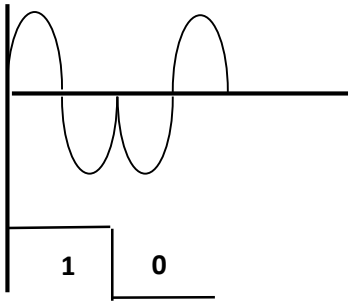


Рисунок 1.5 - Зміна несучого сигналу у випадку ФМ

Модеми, які встановлені на обох кінцях лінії зв'язку, завжди повинні використовувати той самий метод модуляції.

Мірою інтенсивності зміни стану середовища передачі (або будь-яких параметрів, що характеризують інформаційний сигнал) і керуючих пристроїв є швидкість, вимірювана в бодах [О: 1, 2]. Наприклад, у системах з АМ швидкість у бодах визначає швидкість, з якою амплітуда сигналу змінюється від одного значення до іншого. У простих системах, де кожний з можливих рівнів амплітуди модульованого сигналу використовується для подання однієї двійкової цифри (логічного «0» або «1»), швидкість передачі даних у бодах буде дорівнювати швидкості передачі бітової послідовності (біт/с). У системах

з більш складними методами модуляції і при використанні додаткових фізичних кодів, що самосинхронізуються, швидкість у бодах може бути більше або менше бітової швидкості. Наприклад, у системі 4-х рівневої АМ, де кожен рівень амплітуди використовується для подання пари біт («00», «01», «10», «11»), пропускна здатність вимірювана в біт/с буде в 2 рази перевищувати швидкість у бодах. А при використанні фізичних кодів RZ або манчестерського, які будуть розглядатися нижче, швидкість у бодах буде в 2 рази більше швидкості передачі бітового потоку у біт/с.

1.3.2. Концентрація й ущільнення

Мережні пристрої генерують дані з досить високою швидкістю протягом невеликих інтервалів часу. Необхідно, щоб канали передачі дозволяли передавати дані з швидкостями не меншими за швидкість генерації даних і при цьому були досить завантаженими для їхнього ефективного використання. Для вирішення цих завдань зазвичай реалізують поділ загального швидкісного каналу між декількома пристроями за допомогою проміжної апаратури (мультиплексори, концентратори) з використанням методів концентрації та ущільнення [О: 1, 2].

Концентрація - функція з'єднання декількох вхідних каналів зв'язку з одним або декількома вихідними каналами на основі запитів на передачу. Пристрій, що виконує ці функції, називаються концентратором.

Ущільнення (мультиплексування) - функція передачі даних з декількох вхідних каналів у вихідний канал у певні моменти часу або певні частотні смуги загального каналу, які заздалегідь встановлюються для кожного вхідного каналу.

Методи ущільнення діляться на:

- часове ущільнення;
- статистичне часове ущільнення;
- частотне ущільнення.

Часове ущільнення: для організації передачі даних з декількох вхідних каналів встановлюють проміжний пристрій – часовий мультиплексор (пристрій, що забезпечує передачу даних з одного із вхідних каналів у вихідний канал). Для кожного із вхідних каналів, по черзі, мультиплексор виділяє часовий інтервал (часовий такт або тайм-слот), протягом якого дані із вхідного каналу передаються у мультиплексор. Мультиплексор формує пакет з даних, що надійшли під час одного циклу роботи із всіх вхідних каналів (так звана «обойма»), що передається з швидкістю вихідного каналу. З іншої сторони каналу зв'язку встановлюється аналогічний мультиплексор, що розбирає обойму, що надійшла, і передає дані на відповідні вихідні канали.

Довжина часового інтервалу, протягом якого дані із вхідного каналу надходять у мультиплексор, визначається розміром пакета конкретної технології, що реалізує часове мультиплексування. Такий підхід застосовується в технології імпульсно-кодової модуляції (ІКМ-30), технологіях плезіохронної (PDH) і синхронної (SDH) цифрових ієрархій, що застосовуються при побудові первинних телекомунікаційних мереж, у різних багатотермінальних комплексах. Можливий ще один підхід до реалізації часового ущільнення, коли для керування передачею даних із вхідних каналів у вихідний використовують не апаратний пристрій типу мультиплексора, а спеціальний керуючий кадр, що визначає, коли може відбутися передача в загальний вихідний канал (використовується в супутникових системах передачі даних; у кільцевих мережах).

Звичайне часове мультиплексування характеризується досить низькою ефективністю використання вихідного каналу у випадку відсутності даних на одному або декількох вхідних каналах. Через те що мультиплексор буде виділяти тайм-слоти для кожного вхідного каналу по черзі, при відсутності даних на вхідних каналах в обоймі будуть порожні місця, що й приводить до неефективного використання вихідного швидкісного каналу.

Статистичне часове ущільнення: тайм-слоти для передачі даних виділяються вхідним каналам на основі системи пріоритетів, що базується на

інтенсивності передачі даних по кожному з вхідних каналів. У цьому випадку збирається статистика переданих даних із вхідних каналів за певний часовий інтервал, розставляються пріоритети для вхідних каналів і часові такти виділяються відповідно до системи пріоритетів. При зміні інтенсивності даних з якогось каналу його пріоритет може бути підвищений або знижений. У випадку високої інтенсивності даних із всіх каналів статистичний мультиплексор реалізує звичайне часове мультиплексування.

Частотне ущільнення: частотна смуга вихідного каналу ділиться на декілька більш вузьких смуг, кожна з яких може мати різну ширину (пропускна здатність кожного каналу буде відрізнятися). Між частотними смугами реалізуються захисні смуги для мінімізації інтерференції між сусідніми частотами (рис.1.6).

Рисунок 1.6 - Розбиття частотного діапазону на декілька частотних каналів

Наприклад, у коаксіальному кабелі з шириною смуги пропускання 90 Мгц можна організувати порядку 30000 голосових телефонних каналів шириною 3 КГц у різних частинах частотного спектру: канал 1 - 10030300 Гц - 10033300 Гц, канал 2 - 10034300 Гц - 10037300 Гц і т.д.

При використанні частотного мультиплексування можливе закріплення якоїсь частотної смуги за парою вузлів, або розподіл всієї сукупності частотних смуг між всіма пристроями з використання додаткового часового ущільнення.

Метод частотного ущільнення використовується в технології первинних мереж FDM (аналогові телефонні мережі) і в сімействі технологій цифрової абонентської лінії (xDSL).

1.3.3. Технології спектрального ущільнення WDM

Технології спектрального ущільнення або мультиплексування по довжинам хвиль (WDM, CWDM і DWDM) - це сучасні технології передачі та ущільнення в одному оптичному волокні (ОВ) декількох оптичних сигналів з різними довжинами хвиль. WDM-обладнання дозволяє по одній парі оптичних волокон передавати на десятках і навіть сотнях довжин хвиль трафік різних протоколів (SDH / ATM / IP) з різними швидкостями. Ключова перевага WDM в тому, що протокол і швидкість для кожного каналу - незалежні. Оптичні мережі, що використовують WDM технології, можуть передавати дані IP, ATM, SONET / SDH і Ethernet зі швидкостями між 100 Мб/с. і 10 Гб/с. Крім того WDM мережі можуть нести різні типи трафіку з різними швидкостями по одному оптичному каналу.

Системи WDM спочатку об'єднували в одному ОВ дві несучі - 1310 і 1550 нм, що подвоювало ємність системи. В даний час сформувалося нове поняття і клас широкосмугових систем WDM, що перекривають в суміжних вікнах прозорості смугу близько 82 нм (1528-1610 нм). Цей клас використовується системами так званого щільного хвильового мультиплексування - DWDM. Однак дійсно широкосмугові системи вже зараз можуть перекривати смугу 340 нм (1270-1610 нм). Ці системи, що отримали назву розріджених систем WDM, або CWDM, використовують крок між несучими 20 нм і розроблені для зниження вартості систем WDM.

В даний час мережі WDM застосовуються для побудови високошвидкісних транспортних мереж операторів національного масштабу, на основі топологій «точка - точка» або «кільце» і потужних міських транспортних магістралей.

Технологія оптичного, або спектрального, ущільнення була запропонована в 1980 р. Дж. П. Лаудене. Її суть зводиться до того, що потоки даних переносяться світловими хвилями різної довжини. Несучі генеруються окремими джерелами (лазерами), модулюються деяким цифровим сигналом і потім об'єднуються мультиплексором в багаточастотний сигнал. Ранні версії

оптичного ущільнення використовували два вікна прозорості оптоволокна на довжинах хвиль 1300 і 1550 нм. На цьому принципі базується технологія спектрального ущільнення WDM, що є найпростішою. Вона дозволяє ущільнити 2 оптичні довжини хвилі і одночасно передати їх в одному оптичному волокні. Традиційно, такими довжинами є 1310 і 1550 нм (можливі варіанти таких комбінацій з довжинами хвиль в спектрі від 1290 до 1625 нм з кроком 120, 140, 160, 180, 200, 240 нм).

На рис. 1.7 показана типова схема побудови системи WDM.

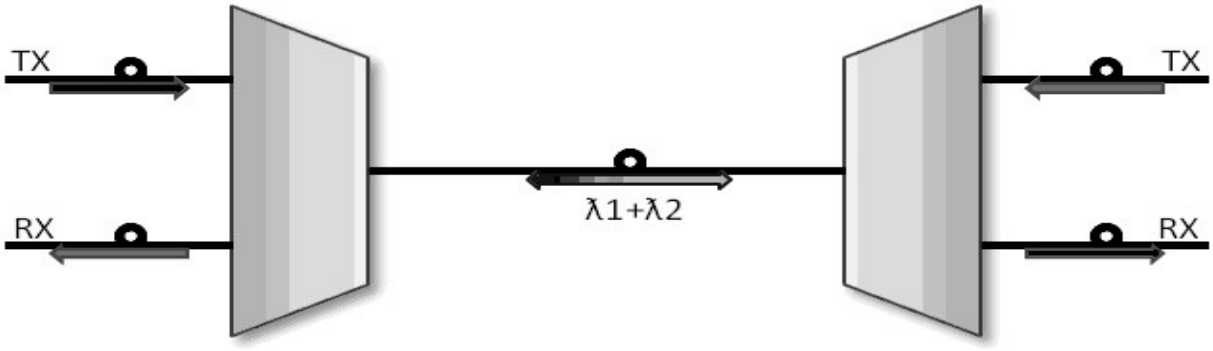


Рисунок 1.7 - Типова схема побудови системи WDM

Традиційно технологія WDM застосовується також для ущільнення декількох каналів передачі даних. Наприклад, 1 GE + 1 GE, 1 GE + STM та інші комбінації. В цьому випадку схема такої системи буде виглядати, як показано на рис. 1.8.

Розвиток WDM привело до появи першого, хоча і тимчасового (класу draft) стандарту Міжнародного союзу електрозв'язку (МСЕ) G.mcs (1997 р.), який згодом був схвалений і опублікований в 1999 році як стандарт для багатоканальних систем SDH з оптичними підсилювачами. Цей стандарт рекомендував використовувати частотний план з кроком несучих 100 ГГц (0,8 нм) і більше, хоча в розробках систем DWDM, вже використовувався крок 50 ГГц (0,4 нм). Результатом подальшого розвитку оптичної інтегральної

схемотехніки стало зменшення кроку між несучими послідовно до 50, 25 і 12,5 ГГц.

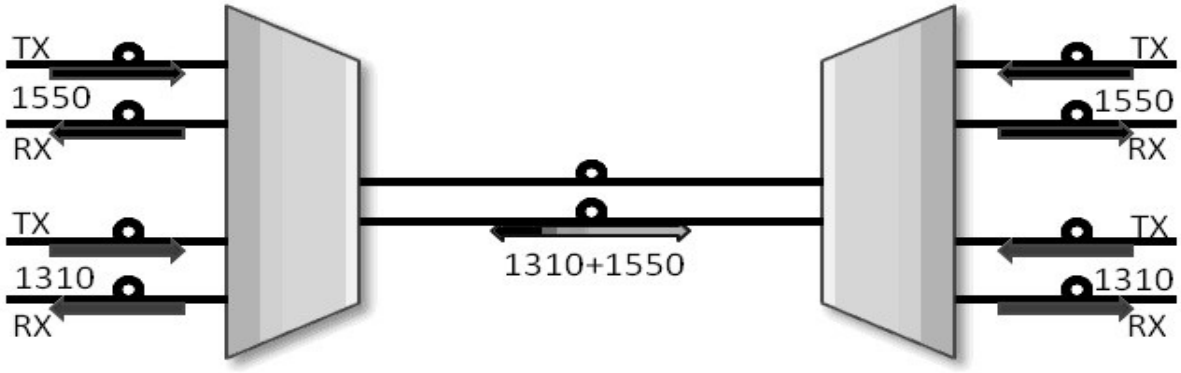


Рисунок 1.8 - Типова схема системи WDM на двох світловодах

Системи щільного мультиплексування по довжинам хвиль (DWDM) - системи з рознесенням каналів не менше 100 ГГц (0,8 нм), що дозволяє мультиплексувати не більше 32 каналів. Частотний план для DWDM систем визначається стандартом ITU G.694.1. Область застосування DWDM - магістральні оптичні мережі. Подальший розвиток систем DWDM, пов'язаний зі зменшенням кроку між несучими частотами до 6,25 ГГц, стримується низкою факторів. Перш за все, це фізичні обмеження (температурна нестабільність частот несучих) і суттєве подорожчання таких надщільних систем WDM (HDWDM). Виходом з цієї ситуації стало використання нового класу систем WDM - розріджених систем WDM, або CWDM, які використовують дуже великий і фіксований крок між несучими - 20 нм - і достатньо дешеві засоби виділення цих несучих: багатошарові тонкоплівкові оптичні фільтри. Реалізація такого рішення стала можливою завдяки різкому розширенню оптичної смуги використання систем WDM: від 1270 до 1610 нм, що було обумовлено успіхами в галузі створення ОВ, що не має піка поглинання на частоті 1383 нм.

Технологія розрідженого мультиплексування по довжинам хвиль (CWDM) використовується для формування в одному волокні до 9 дуплексних каналів зі швидкістю передачі даних до 10 Гб/с на відстані 50 і більше

кілометрів. Частотний план для CWDM систем визначається стандартом ITU G.694.2. Область застосування технології CWDM - міські оптичні мережі. Рішення спектрального ущільнення CWDM дозволяє ущільнити до 18 оптичних довжин хвиль в діапазоні від 1270 до 1610 нм з кроком в 20 нм. А саме - довжини хвиль 1270, 1290, 1310, 1330, 1350, 1370, 1390, 1410, 1430, 1450, 1470, 1490, 1510, 1530, 1550, 1570, 1590 і 1610 нм. Кількість довжин хвиль визначається типом оптоволоконного кабелю, який використовується для передачі даних. Оптичний кабель стандарту G652.C і G.652D і вище має широкосмугове оптичне волокно з поліпшеною структурою, яка дозволяє передати всі 18 довжин хвиль. До широкосмугового волокна використовувалася система або O-діапазону (вікно 1310 нм) або C-, L-діапазонів (1530 нм, 1625 нм). Сьогодні, широкосмугове волокно додатково використовує E-діапазон (вікно 1400 нм) що дозволяє розширити можливості оптичних мереж. Аналогічно WDM технології існують як одноволоконні як і двоволоконні CWDM рішення. Стандартні реалізації існують для 3-х, 4, 6, 8, 16, 18 довжин хвиль. Типова схема реалізації одноволоконного рішення показана на рис. 1.9.

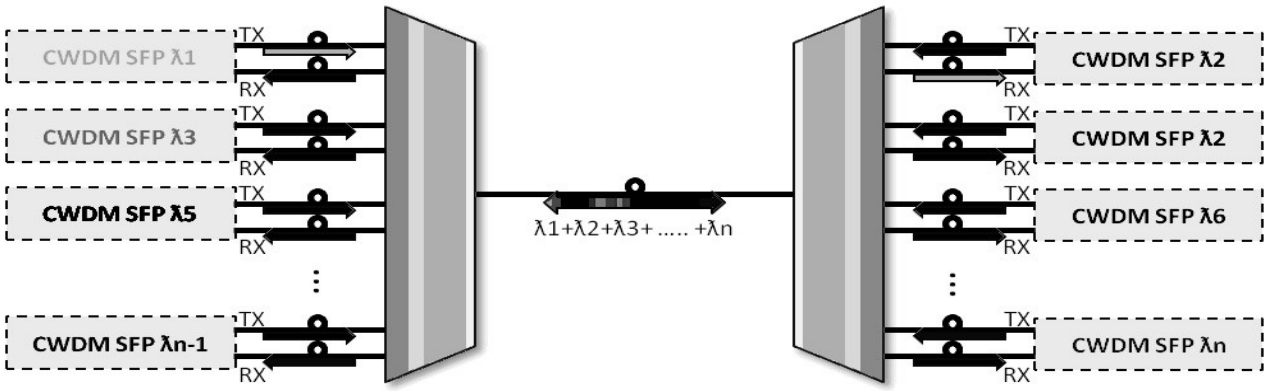


Рисунок 1.9 - Типова схема рішення CWDM

Враховуючи те, що для каналу передачі даних необхідно організувати канал передачі та канал прийому, для кожного потоку використовується по дві

довжини хвилі. Відповідно, наприклад, в рішенні на 8 довжин хвиль в одноволоконному рішенні можна передати 4 потоки.

При побудові двоволоконного CWDM рішення кількість потоків передачі даних дорівнює кількості довжин хвиль, що ущільнюються.

1.3.4. Імпульсно-кодова модуляція

Для перетворення аналогового телефонного сигналу в цифрову форму використовується метод імпульсно-кодової модуляції, оснований на часовому мультиплексуванні.

Спрощено імпульсно-кодову модуляцію (ІКМ) можна розбити на 3 етапи:

1) знімання значень або часова дискретизація;
2) відцифровування або дискретизація по рівнях;
3) двійкове кодування (рис. 1.10).

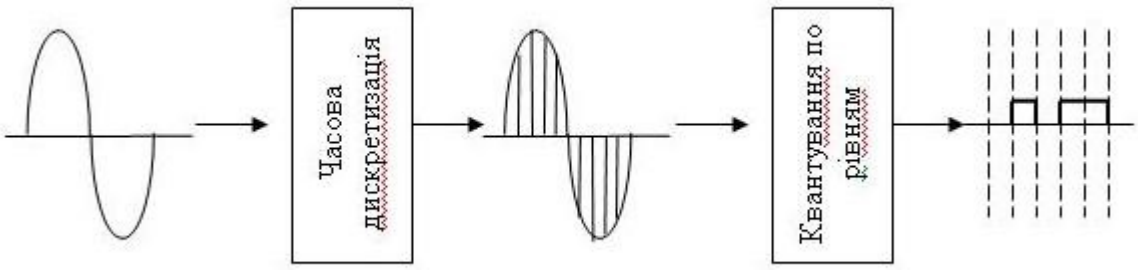


Рисунок 1.10 - Імпульсно-кодова модуляція

Пристрій, що виконує процес перетворення аналогового сигналу в цифрову форму називається первинним ІКМ мультиплексором. Він виконує дві основні функції:

1) перетворення аналогового сигналу в цифрову форму;
2) формування мультиплексованого цифрового потоку даних.

ІКМ базується на теоремі Найквиста – Котельникова, в якій говориться наступне: для однозначного відновлення аналогового сигналу із цифрової

форми частота часової дискретизації повинна бути не менш ніж в 2 рази вище верхньої частоти вихідного аналогового сигналу.

У результаті часової дискретизації (частота дискретизації 8 КГц) одержують відображення, яке називають сигналом ІАМ (імпульсно-амплітудна модуляція). Далі цей сигнал піддається відцифровуванню. Метою відцифровування є призначення кожному відображенню певного рівня амплітуди (128 або 256 рівнів амплітуди). Для наступного кодування у двійковий вид при 128 рівнях знадобиться 7 біт, при 256 – 8 біт. Відцифровування зі 128 рівнями вимагатиме швидкості передачі 56 Кб/с, при 256 – 64 Кб/с. Взагалі, для якісного подання аналогового сигналу (телефонного) необхідно 2048 рівнів (2^{11}) що вимагало б швидкості передачі 88 Кб/с.

Після відцифровування здійснюється двійкове кодування значень.

Для правильного відновлення вихідного сигналу дані повинні бути подані на цифро-аналоговий перетворювач з тією самою швидкістю, з якою здійснювалося вихідне перетворення. Перетворювач видає на виході напругу, що відповідає 8000 знятим значенням. Форма сигналу близька до форми вихідного аналогового сигналу після відповідної фільтрації.

Основні проблеми ІКМ – спотворення сигналу (необхідно збільшувати частоту часової дискретизації) і помилки відцифровки (пов'язані з обмеженою кількістю рівнів амплітуди). Крім цього, при малих амплітудах сигналу мають місце шуми відцифровки, пов'язані з лінійним двійковим кодуванням. Для усунення цього недоліку застосовують схеми нелінійного кодування, коли подання змін сигналу малої амплітуди здійснюється більшою кількістю кодових комбінацій, ніж у випадку великої амплітуди сигналу. Зазвичай використовують логарифмічні залежності. Такі схеми нелінійного кодування називаються μ-закон (Північна Америка, Японія) і А-закон (Європа).

Апаратура ІКМ мереж (мультиплексори, демультиплексори, комутатори) працює у режимі розподілу часу, по черзі обслуговуючи протягом циклу своєї роботи всі вхідні абонентські канали (рис. 1.11). Тривалість циклу становить 125 мкс. Кожному абонентському каналу виділяється один тайм-слот,

тривалість якого визначається числом вхідних абонентських каналів (125 мкс/N, де N – число вхідних каналів).

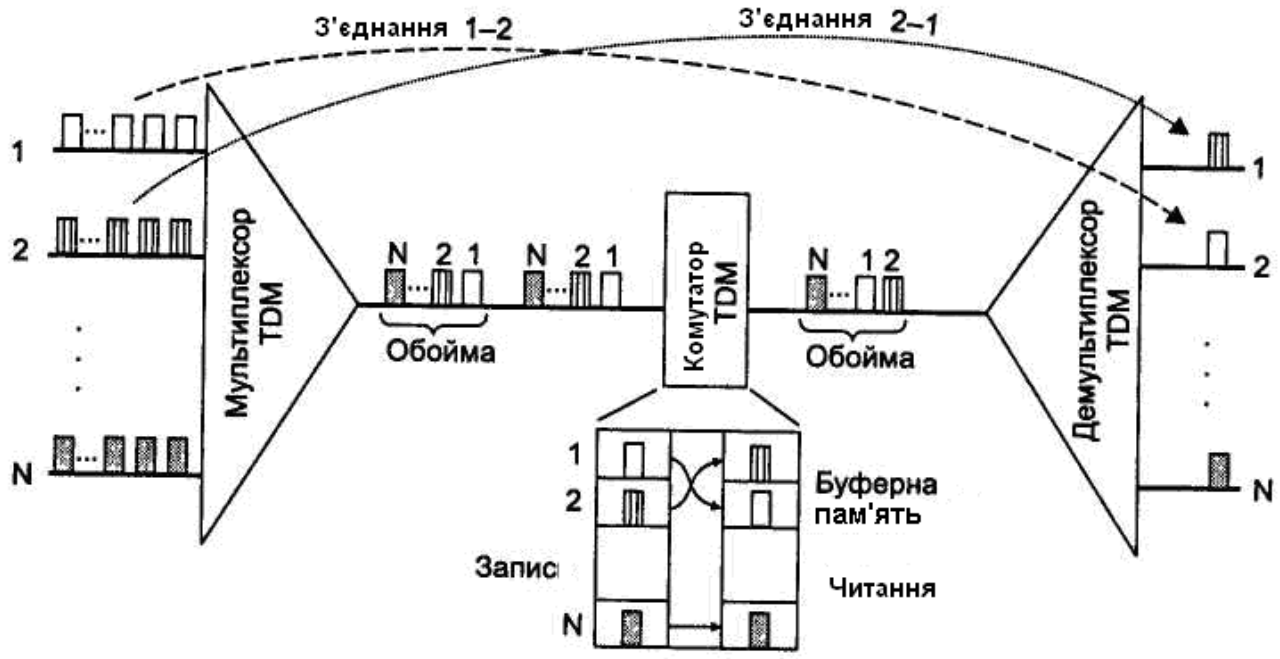


Рисунок 1.11 - Апаратура ІКМ мереж

Мультиплексор приймає дані по N вхідних каналах, кожний з яких має швидкість 64 Кб/с. У кожному циклі мультиплексор виконує наступні функції:

1) прийом з кожного каналу чергового байту даних;
2) формування із прийнятих байт ущільненого кадру, який називають обоймою;
3) передача обойми на вихідний канал з бітовою швидкістю Nx64 Кб/с.

Порядок байт в обоймі відповідає номеру вхідного каналу, з якого він отриманий.

Демультиплексор виконує зворотне завдання – розбиває отриманий кадр на байти і передає їх по черзі на вихідні канали, вважаючи при цьому, що номер байта в кадрі відповідає номеру вихідного каналу.

Комутатор приймає кадр на швидкості каналу і переставляє байти в обоймі відповідно до встановлених з'єднань. Не всі 64 Кб/с на абонентському

закінченні використаються для передачі даних користувачів. У деяких системах 1 біт з 8-ми використається для передачі службової інформації (максимум 56 Кб/с для передачі даних користувачів), в інших системах для службових цілей використовується 8-й біт у кожному 6-му відображенні.

Мережі на основі ІКМ потребують синхронної роботи всіх пристроїв (синхронний режим передачі). Порушення синхронізації приводить до порушення комутації абонентів. На основі ІКМ систем будуються мережі двох технологій: плезиохронної (майже синхронної) цифрової ієрархії (PDH) і синхронної цифрової ієрархії (SDH).

1.3.5. Синхронізація елементів мережі

Для організації обміну даними приймач і передавач повинні сповіщати один одного про готовність до прийому й передачі, інформувати пристрої про повідомлення, що передаються. Цей процес є частиною протоколу зв'язку й називається синхронізацією [О: 1, 2].

У випадку невеликої відстані між пристроями мережі для забезпечення синхронізації може бути використана окрема фізична лінія, по якій передаються синхросигнали. Синхросигнали виконують дві основні функції:

1) забезпечують настроювання приймача на дані, що надходять, перш ніж вони надійдуть до приймача;

2) підтримують синхронізацію приймача із бітами даних, що надходять.

У випадку великих відстаней можливе порушення синхронізації між приймачем і передавачем. Фізичні характеристики ліній передачі синхросигналів і інформаційних сигналів завжди будуть мати деякі відмінності, що призводить до відмінності у швидкостях поширення сигналів у цих лініях. У результаті, синхросигнал може вповільнюватися або прискорюватися відносно інформаційного сигналу, що може призвести до неузгодженості приймача й передавача. У цьому випадку більш ефективним є використання синхросигналів вбудованих у інформаційні повідомлення, що передаються,

замість окремої фізичної лінії для передачі синхросигналів. Для цього використовуються коди, що самосинхронізуються.

При використанні коду, що самосинхронізується, приймаючий пристрій може періодично перевіряє себе, щоб переконатися, що він опитує лінію саме в моменти надходження інформаційних бітів. Для цього потрібно, щоб у лінії дуже часто змінювалися параметри електричного сигналу. Ідея полягає в тому, щоб кодування призводило до регулярних і частих змін рівнів електричного сигналу в лінії. Ці зміни дозволяють у приймачі розділяти логічні «0» і «1» і відслідковувати стан лінії для настроювання. Стробування або опитування лінії звичайно проводиться приймачем із швидкістю більшою за швидкість передачі даних для більш точного визначення елементів даних.

Всі схеми кодування можна розділити на 2 класи:

- фізичне кодування - визначає форму електричного сигналу в лінії;
- логічне кодування - заміняє одну бітову послідовність іншою.

Найбільш розповсюджені наступні схеми двійкового фізичного кодування:

- уніполярний код - напруга всіх сигналів або не негативна, або не позитивна (наприклад, «1» - 0В, «0» - +3В);

- полярний код - сигнал має позитивні й негативні потенціали (наприклад, «0» - +3В, «1» - -3В);

- біполярний код - зміна сигналу відбувається між 3-ма рівнями;

- код AMI - для кодування логічної «1» використовуються імпульси різної полярності.

Фізичні коди поділяються на потенціальні та імпульсні. У потенціальних кодах для подання «0» і «1» використовуються певні рівні потенціалів, а в імпульсних кодах використовуються або імпульси різної полярності, або фронти імпульсів.

На базі розглянутих схем будуються наступні основні фізичні коди (рис. 1.12).

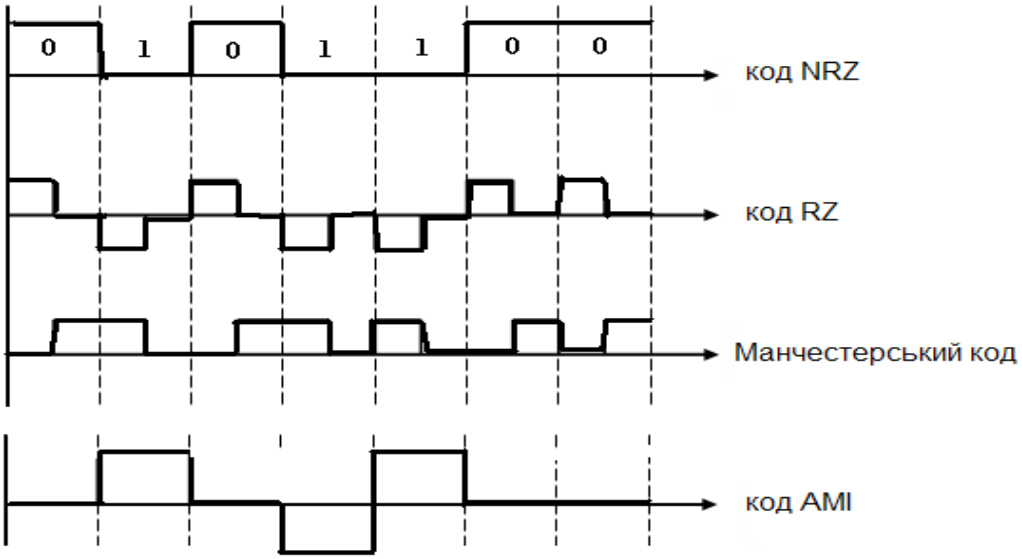


Рисунок 1.12 - Типи фізичних кодів

NRZ (код без повернення до нуля) - потенціальний код, у якому рівні потенціалів залишаються постійними для послідовності однойменних біт. Зазвичай, низький рівень відповідає логічної «1», високий - логічному «0». Має найпростішу схему реалізації, ефективно використовує частотну смугу каналу; швидкість у бодах відповідає пропускній здатності біт/с (1 бод = 1 біт/с). Недоліком даного коду є відсутність властивості самосинхронізації - довгі послідовності «0» або «1» не призводять до зміни стану в лінії. Код може бути полярним або біполярним, не вимагає схем кодування-декодування.

RZ (код з поверненням до нуля) - біполярний імпульсний код. Для подання кожного біта сигнал у лінії змінюється, щонайменше, один раз. У результаті код має гарні властивості самосинхронізації. Недолік даного коду - потрібна подвоєна швидкість у бодах для передачі одного біта даних. Код застосовується в лазерних й оптоволоконних системах передачі, у деяких технологіях локальних мереж.

Манчестерський код - для подання «0» і «1» використовується фронт імпульсу. Код забезпечує зміну стану середовища передачі для кожного біта і має гарні властивості самосинхронізації. Також як і RZ код, манчестерський

код вимагає подвоєної швидкості в бодах для передачі біта даних (використовується в технології Ethernet на коаксіальному кабелі, технології IBM Token Ring).

Код AMI або NRZI (біполярний з почерговою інверсією рівнів) - для подання логічних «1» використовуються імпульси різної полярності - полярність імпульсу наступної «1» протилежна полярності імпульсу попередньої «1». При використанні даного коду можливі проблеми із синхронізацією при передачі довгих послідовностей «0», які не приводять до зміни стану лінії.

Для поліпшення властивостей синхронізації потенціальних фізичних кодів використовуються схеми логічного кодування.

1.3.6. Логічне кодування

Логічне кодування використовується разом з потенціальними фізичними кодами й дозволяє вирішувати наступні завдання [О: 1, 2]:

- усуває довгі послідовності однотипних біт - «0» або «1», поліпшуючи, таким чином, властивості самосинхронізації;

- полегшує виявлення помилок передачі.

При логічному кодуванні виділяють наступні підходи:

- надлишкове кодування;

- скремблювання.

Надлишкове кодування ґрунтується на розбивці початкової послідовності біт на певні порції, що називаються символами. Потім, кожний початковий символ заміняється на новий, котрий буде мати більшу кількість біт, ніж початковий. Наприклад, логічний код 4В/5В, що застосовується в технологіях FDDI і Fast Ethernet, заміняє початкові символи довжиною 4 біти на нові символи довжиною 5 біт. Завдяки тому, що результуючі символи містять надлишковий біт, загальне число бітових комбінацій у них буде більше, ніж у вихідних символах (4В – кількість комбінацій для вихідних символів становить 2 у 4-ому ступені, тобто 16; 5В - кількість комбінацій для нових символів

становить 2 у 5-ому ступені, тобто 32). У результаті з 32 комбінацій можна відібрати 16, які не будуть містити довгих послідовностей повторюваних «0» або «1». Інші 16 комбінацій вважаються забороненими. Надходження кожної із заборонених комбінацій на вхід приймача відразу свідчить про помилку передачі. Символи коду 4В/5В гарантують, що при будь-яких комбінаціях біт у вихідній послідовності в результуючій послідовності буде не більше 3-х однакових бітів, що повторюються.

Крім логічних кодів із двома станами (В – бінарних), є також коди з 3-ма станами. Прикладом таких кодів може служити код 8В/6Т. У цьому коді для кодування вихідного символу довжиною 8 біт використовується комбінація з 6 тернарних символів. У тернарному наборі символів існує позитивна логічна «1», для подання якої зазвичай використовується рівень потенціалу +3,5 В, логічний «0», що представляється рівнем потенціалу 0 В, негативна логічна «1», для подання якої використовується рівень потенціалу -3,5 В. У даному коді кількість бітових комбінацій буде $2^8 = 256$ – для вихідних символів і $3^6 = 729$ – для результуючих символів. Таким чином надмірність даного коду вище, ніж у коду 4В/5В. Цей код застосовується в технології 100VG AnyLAN і в специфікації фізичного рівня 100 Base-T4 технології Fast Ethernet.

Реалізується логічне кодування шляхом прошивання таблиць перекодування в приймачах-передавачах портів мережних адаптерів і активного мережного устаткування.

Слід зазначити, що при використанні надлишкових логічних кодів, для забезпечення необхідної пропускної здатності лінії передавач повинен працювати з підвищеною тактовою частотою. Так, при використанні коду 4В/5В, для забезпечення швидкості 100 Мбіт/с, тактова частота повинна бути 125 Мгц (125 Мгц х 4/5 = 100 Мб/с). Однак, при використанні імпульсного коду типу RZ або манчестерського, для забезпечення швидкості 100 Мб/с потрібна була б тактова частота 200 Мгц (необхідно два бода для передачі одного біта).

Скремблювання – перемішування даних скремблером перед передачею їх у лінію. Скремблювання полягає в побітовому обчисленні результуючого

коду виходячи з бітів вихідного коду й отриманих у попередніх тактах роботи скремблера бітів результуючого коду. Наприклад, для обчислення бітів результуючого коду може бути використаний наступний логічний вираз:

$$b_i = A_i \oplus b_{i-3} \oplus b_{i-5},$$

де, b_i – результуючий біт на і-му такті роботи скремблера;

A_i – вихідний біт на і-му такті;

b_{i-3}, b_{i-5} – результуючі біти, отримані на 3 і 5 тактів раніше;

$\oplus$ - логічна операція «виключне або» (додавання по модулю «2»).

Приклад

Вихідна комбінація: 10000001

$B_1 = A_1 = 1$

$B_2 = A_2 = 0$

$B_3 = A_3 = 0$

$B_4 = A_4 \oplus B_1 = 0 \oplus 1 = 1$

$B_5 = A_5 \oplus B_2 = 0 \oplus 0 = 0$

$B_6 = A_6 \oplus B_5 \oplus B_1 = 0 \oplus 0 \oplus 1 = 1$

$B_7 = A_7 \oplus B_4 \oplus B_2 = 0 \oplus 1 \oplus 0 = 1$

$B_8 = A_8 \oplus B_5 \oplus B_3 = 1 \oplus 0 \oplus 0 = 1$

Результуюча комбінація: 10010111 - відсутня послідовність з шести «0».

Після одержання результуючої комбінації, приймач передає її дескремблеру, що відновлює вихідну послідовність за допомогою зворотного перетворення:

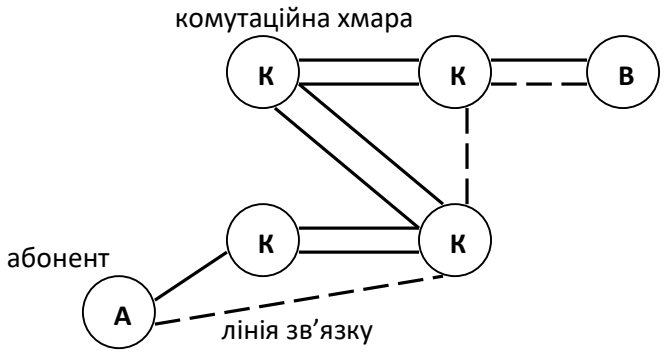
$$c_i = bi \oplus b_{i-3} \oplus b_{i-5}$$

Існує ще одна група кодів, що ставиться до класу скремблювання, заснована на штучному спотворенні довгої послідовності «0» забороненими символами. Таким чином, наприклад, можна поліпшити властивість

самосинхронізації коду AMI, вставляючи в послідовності «0» імпульс логічної «1» неправильної полярності. Даний імпульс не буде сприйматися приймачем як інформаційний біт, а буде використаний для синхронізації.

1.3.7. Методи комутації

Застосовуються для організації в каналах передачі даних декількох одночасних сеансів зв'язку між різними вузлами [О: 1, 2]. Абоненти з'єднані з комутаторами індивідуальними лініями зв'язку. Канали між комутаторами використовуються спільно всіма абонентами (рис. 1.13).



А, В - абоненти
К – комутатор

Рисунок 1.13 - Приклад створення комутованого каналу між парою абонентів

Для визначення елемента даних використовуються такі терміни, як «повідомлення», «блок», «пакет», «кадр». Часто ці терміни використовуються взаємозамінно і під усіма ними розуміється самостійний і незалежний об’єкт керування та/або даних користувача. Хоча звичайно під «повідомленням» розуміється набір даних прикладного процесу або протоколів верхніх рівнів, «пакетом» називають елемент даних мережного рівня, «кадром» - елемент даних канального рівня.

Існують 3 базові схеми комутації:

- комутація каналів;

- комутація пакетів;
- комутація повідомлень.

Мережі з комутацією каналів і комутацією пакетів поділяються на 2 класи: мережі з динамічною комутацією й мережі з постійною комутацією.

У першому випадку мережа встановлює з'єднання з ініціативи користувача на час сеансу зв'язку на основі адресної інформації. У другому випадку адміністратором мережі прописується якесь з'єднання через всі необхідні проміжні пристрої на досить тривалий час для обміну даними між парою вузлів (прикладом такого з'єднання може служити «виділена» лінія).

Комутація каналів – організація безперервного складеного фізичного каналу з послідовно з'єднаних окремих канальних ділянок для прямої передачі даних між парою вузлів. Окремі канальні ділянки з'єднуються між собою комутаторами. При такому методі комутації перед передачею даних завжди необхідно виконати процедуру встановлення з'єднання, у ході якої й організується складений канал. Прикладом мережі з комутацією каналів виступає комутована телефонна мережа загального користування (КТМЗК).

Комутатори, а також канали, що їх з’єднують, повинні забезпечувати одночасну передачу даних з декількох абонентних каналів. Для цього вони повинні бути швидкісними й підтримувати мультиплексування абонентських каналів (частотне або часове).

Якщо з'єднання може бути встановлене (не вичерпана ємність магістральних каналів, що з'єднують комутатори; вузол, що викликають, вільний), то для організації даного з'єднання виділяється канал з фіксованою пропускною здатністю й вузли на такому з'єднанні повинні працювати тільки з даною швидкістю передачі.

Метод комутації каналів досить неефективно використовує ресурси магістральних каналів у випадку пульсуючого трафіку, характерного для звичайних комп'ютерних мереж. У цьому випадку, дані до каналу будуть надходити з кінцевих пристроїв порціями, у проміжках між якими канал буде «простоювати».

Комутація пакетів – повідомлення користувачів у вихідному вузлі розбиваються на окремі пакети, кожний з яких має адресну інформацію, необхідну для доставки пакета в пункт призначення, і порядковий номер, для складання повідомлення в кінцевому вузлі. Пакети передаються через мережу як незалежні інформаційні об'єкти.

Комутатори пакетної мережі мають буферну пам'ять для зберігання пакетів, у випадку якщо вихідний канал зайнятий. Така схема дозволяє згладжувати пульсації трафіку на магістральних каналах і є досить ефективною для передачі пульсуючого трафіку комп'ютерних мереж.

Пересування пакетів по мережі здійснюється на базі маршрутної інформації. При цьому виділяють два режими передачі:

- дейтаграмний (незалежна маршрутизація кожного пакета);

- передача пакетів віртуальним каналом (перед передачею даних, на основі запитів на встановлення з'єднання між двома вузлами через всю проміжну мережу формується віртуальний канал або віртуальне з'єднання, що одержує певний ідентифікатор. Всі пакети, що належать до даного сеансу зв'язку, будуть відсилатися тільки по даному віртуальному каналу або з'єднанню).

При комутації пакетів неможливо точно визначити пропускну здатність каналу або з'єднання між парою вузлів. Це пов'язане із затримками на формування пакетів, міжпакетними інтервалами, затримками в комутаторах і т.д. На ефективність істотно впливає розмір пакетів - занадто великий наближає до мережі з комутацією каналів, занадто малий збільшує частку службової інформації.

Комутація повідомлень – передача єдиного блоку даних через проміжні вузли з організацією тимчасового зберігання цих даних у пам'яті проміжних вузлів. При цьому час зберігання може бути досить великим. За такою схемою звичайно передають повідомлення, що не вимагають негайної відповіді (наприклад, електронна пошта в режимі off-line).

1.3.8. Асинхронна/синхронна передача

У багатьох системах передачі даних пристрої для кодування сигналів використовують NRZ код. Для підтримки синхронізації в лінії використовується дві домовленості відносно форматування [О: 1, 2].

1. Асинхронна передача.

$Б_N$	...	$Б_2$	$Б_1$

Кожний байт даних містить 2 службових біти «Старт» і «Стоп», які поміщаються відповідно у початок і кінець байта (це сигнали синхронізації). Їхнє призначення:

- сповістити приймач про прихід даних;

- дати приймачу досить часу для виконання функцій, зв'язаних з синхронізацією, до надходження наступного байта даних. Біти «Старт» і «Стоп» є спеціальними сигналами, які розпізнаються приймачем. Даний вид передачі характеризується простотою реалізації, але досить неефективно використовується канал через велику кількість службових біт. Широко застосовується при обміні даними з периферійними пристроями, у багатотермінальних комплексах, у модемах на комутовній лінії.

2. Синхронна передача.

Синхробайт	Блок даних	Синхробайт

Кожний блок даних містить спеціальний елемент – синхробайт, що називають прапором. Прапори містять заздалегідь відому послідовність символів – зазвичай 01111110. Їхня функція полягає у сповіщенні приймача про прихід даних. Процес додавання синхробайтів до блоку даних називають

кадруванням. Для більш надійної синхронізації може бути вставлено декілька синхробайтів.

Типовий синхронний формат кадру має такий вигляд (рис. 1.14).

Поле управління	Поле ідентифікації	Дані	Контрольна послідовність кадра	Прапор

Рисунок 1.14 - Типовий синхронний формат кадру

Дані, що передаються каналами, оформляються у вигляді кадрів, які зазвичай містять, як мінімум, п'ять полів:

- синхробайти;
- поле керування, що містить службову інформацію, необхідну для керування процесом передачі кадрів по мережі (реалізує протокол передачі кадрів);
- поле ідентифікації - містить інформацію для ідентифікації, як мінімум, приймача (наприклад, фізична адреса вузла);
- поле даних - містить дані прикладного процесу;
- поле контролю помилок або контрольна послідовність кадру - містить інформацію для виявлення помилок передачі.

Поле керування, або поле ідентифікації можуть містити також порядкові номери кадрів, необхідні для перевірки правильності надходження кадрів, реалізації повторної передачі помилкових кадрів, складання з кадрів єдиного повідомлення.

Слід зазначити, що не всі кадри містять дані користувача. Значну частину мережного трафіка становлять допоміжні кадри або службові кадри, що виконують інтерфейсні й протокольні функції. У таких кадрах поле даних може бути відсутнє.

Контрольна послідовність кадру використовується для виявлення помилок передачі даних. Стандартно застосовується наступний алгоритм: відповідно до певного математичного виразу (зазвичай степеневий ряд),

використовуючи як аргументи вміст інших полів кадру, передавач проводить обчислення й записує отримане значення в поле контрольної послідовності кадру. Приймач, одержавши кадр, робить аналогічні обчислення й порівнює отримане значення зі значенням, записаним у полі контрольної послідовності. Якщо ці величини співпали, то є велика ймовірність того, що кадр переданий без помилок. Цей процес називається циклічним контролем по надлишковості (CRC).

Наведений типовий формат кадру застосовується у всіх технологіях, що використовують синхронну передачу на канальному рівні.

Питання для самоперевірки та контролю засвоєння знань

1. Визначити, які пристрої належать до КУД (DTE) пристроїв.
2. Визначити, які пристрої належать до АКД (DCE) пристроїв.
3. Визначити, з яких складових складається комутаційна хмара.
4. Визначити, що розуміється під трафіком.
5. Визначити, який з наведених методів підтримує передачу даних в обох напрямках (дуплексний, напівдуплексний, симплексний).
6. Визначити, який з наведених методів підтримує передачу даних в обох напрямках одночасно (дуплексний, напівдуплексний, симплексний).
7. Визначити, що розуміють під інформаційним каналом.
8. Визначити, скільки інформаційних каналів може одночасно існувати в одному середовищі передачі.
9. Визначити, які фактори впливають на пропускну спроможність каналу.
10. Визначити, які фактори впливають на спотворення інформаційного сигналу.
11. Визначити, що розуміють під модулюючим сигналом.
12. Дати оцінку, що характеризує швидкість у бодах.
13. Проаналізувати та визначити, чи співпадають швидкість у бодах з бітовою швидкістю.

14. Дати оцінку, яке співвідношення між бітовою швидкістю та швидкістю у бодах в системах з 4-х рівневою амплітудною модуляцією.
15. Дати оцінку, яке співвідношення між бітовою швидкістю та швидкістю у бодах при використанні NRZ-коду.
16. Дати оцінку, яке співвідношення між бітовою швидкістю та швидкістю у бодах при використанні RZ-коду.
17. Дати оцінку, яке співвідношення між бітовою швидкістю та швидкістю у бодах при використанні манчестерського коду.
18. Визначити, для яких цілей використовують методи концентрації.
19. Визначити, для яких цілей використовують методи ущільнення.
20. Проаналізувати принци роботи мультиплексору та визначити, коли дані з вхідного каналу можуть бути передані до мультиплексору.
21. Проаналізувати принци роботи мультиплексору та визначити, в якому порядку мультиплексор виділяє тайм-слоти для передачі даних з вхідних каналів.
22.Визначити, чи можна реалізувати часове мультиплексування без використання мультиплексору.
23. Проаналізувати особливості та визначити, який недолік звичайного часового мультиплексору усуває статистичний часовий мультиплексор.
24. Проаналізувати особливості та визначити критерій, який використовується для встановлення пріоритетів в статистичному часовому мультиплексорі.
25. Визначити, для чого використовується частотне мультиплексування.
26. Визначити, який код дозволяє синхронізувати приймач та передавач без передачі додаткових синхросигналів.
27. Проаналізувати особливості та визначити, які з наведених кодів не мають властивості самосинхронізації (NRZ, RZ, манчестерський код, код AMI).
28. Проаналізувати особливості та визначити, які з наведених кодів мають властивість самосинхронізації (NRZ, RZ, манчестерський код, код AMI).
29. Проаналізувати особливості та визначити, які коди відносяться до фізичних.
30. Проаналізувати особливості та визначити, які коди відносяться до логічних.

31. Проаналізувати особливості та визначити, використання якого коду потребує меншої тактової частоти при однаковій швидкості передачі даних.
32. Проаналізувати особливості та визначити, який з методів комутації найкраще підходить для передачі даних комп'ютерних мереж.
33. Проаналізувати особливості та визначити, який з методів комутації найкраще підходить для передачі голосових даних.
34. Проаналізувати особливості та визначити, який з методів комутації забезпечує постійну швидкість передачі через проміжну мережу.
35. Проаналізувати особливості та визначити, який з методів комутації гарантує проходження усіх пакетів по єдиному маршруту.
36. Дати оцінку, при використання якого підходу до форматування передається більший обсяг службової інформації.
37. Проаналізувати формат кадру та визначити, яке поле містить адресу одержувача.
38. Проаналізувати формат кадру та визначити, яке поле містить адресу відправника.
39. Проаналізувати формат кадру та визначити, яке поле використовується для синхронізації.
40. Проаналізувати формат кадру та визначити, яке поле використовується для виявлення помилок передачі.
41. Визначити, для чого використовується процедура циклічного контролю по надлишковості.

2. ФІЗИЧНЕ СЕРЕДОВИЩЕ ПЕРЕДАЧІ

Фізичне середовище передачі призначене для передачі даних за допомогою електромагнітних сигналів. Поділяється на обмежене середовище й необмежене середовище передачі [О: 1, 3; Д: 1, 2].

Обмежене середовище – електромагнітний сигнал передається всередині замкнутого простору (фізичного провідника). Прикладом обмеженого середовища виступають кабелі будь-яких типів.

Необмежене середовище – електромагнітний сигнал не обмежений яким-небудь замкненим простором. Прикладом необмеженого середовища є відкритий ефір.

На основі фізичних середовищ будуються кабельні системи й бездротові канали передачі даних локальних і глобальних мереж.

2.1. Основні характеристики обмежених середовищ передачі

Будь-яка кабельна система, призначена для передачі електричних сигналів, може бути представлена у вигляді довгої лінії з розподіленими параметрами, які й будуть визначати основні характеристики лінії передачі (частотні властивості, швидкість поширення електричного сигналу й т.п.) [О: 1, 3; Д: 3, 4, 5].

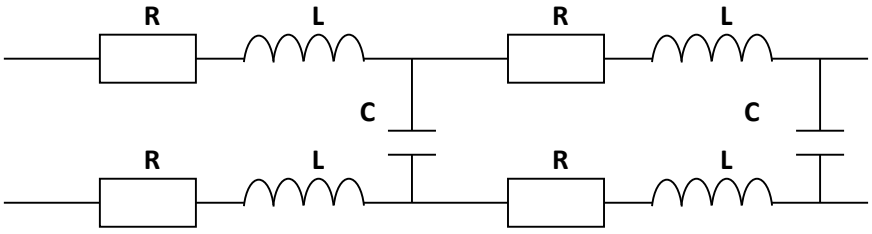


Рисунок 2.1 - Довга лінія з розподіленими параметрами

Електричні властивості лінії характеризуються її первинними параметрами (R, L, C), які визначають динамічні й частотні характеристики лінії.

R – опір постійному струмові. Чим менше ця величина, тим більше здатність провідника проводити електричний струм. Практично незалежить від частоти. Зазвичай наводиться питомий опір кабелю на одиницю довжини (Ом/м) або опір кабельного відрізка певної довжини (може наводитися для кабельного сегмента довжиною 1000 футів (305 м) або 100 м).

C – ємність, характеризує властивості електричних провідників накопичувати електричний заряд. Високе значення ємності в кабелі приводить до зниження смуги пропускання лінії й спотворення електричного сигналу. Звичайно наводиться питоме значення ємності на одиницю довжини (нф/м) або ємність кабельного відрізка певної довжини (може наводитися для кабельного сегмента довжиною 1000 футів (305 м) або 100 м).

L – індуктивність, характеризує властивості електричних провідників накопичувати енергію магнітного поля. Характеризує електричну інерційність системи.

Для оцінки характеристик різних кабельних систем використовують вторинні параметри, які або розраховуються з первинних, або визначаються експериментально.

Імпеданс (хвильовий опір) Z (Rв) – являє собою повний (активний і реактивний опір лінії). Залежить від геометрії провідників і фізичних характеристик матеріалів провідника й ізоляції.

Важливо, щоб імпеданс навантаження збігався з імпедансом лінії (Zн = Zл). У цьому випадку вся енергія переданого електричного сигналу поглинається навантаженням.

У випадку, коли Zн > Zл, частина енергії сигналу буде відбиватися від кінця лінії й поширюватися назад. Полярність відбитого сигналу буде збігатися з полярністю вихідного сигналу. Коли Zн = ∞ («розімкнута» лінія) буде мати місце повне відбиття сигналу.

У випадку, коли Zн < Zл також частина сигналу відбивається від навантаження, але полярність відбитого сигналу протилежна полярності вихідного сигналу. Коли Zн = 0 («закорочена» лінія) спостерігається повне відбиття зі зворотним знаком.

Слід зазначити, що процеси відбиття відбуваються не тільки на кінцях лінії, але й у будь-яких точках лінії, у яких має місце відхилення імпедансу від номінального значення. Такі випадки виникають при з'єднанні кабелів з різних партій, внаслідок неякісного виготовлення кабелю, а також на роз'ємах, якщо їхній імпеданс відрізняється від імпедансу кабелю. До змін імпедансу в кабелі призводять порушення геометрії провідників і ізоляції (різкі вигини кабелю, розтягання). Відбиття сигналу призводять до додаткових спотворень і , як наслідок, додаткових помилок передачі.

Мірою ступеня погодженості імпедансу є ослаблення відбитого сигналу або «**зворотні втрати**» (R_l):

$$R_l = 20 lg \frac{U_{RA}}{U_A}$$

де, U_A – амплітуда переданого сигналу,

U_{RA} – амплітуда відбитого сигналу з боку передавача.

Загасання (Att) – характеризує втрати потужності електричного сигналу, при його проходженні через лінію.

$$Att = -20 lg \frac{U_B}{U_A} = -10 lg \frac{P_B}{P_A}$$

де, U_A, P_A – амплітуда й потужність переданого сигналу, U_B, P_B – амплітуда й потужність прийнятого сигналу.

Загасання залежить від частоти сигналу. Звичайно кабелі характеризуються «погонним» загасанням - загасанням на одиницю довжини

дБ/м (може наводитися для кабельного сегмента довжиною 1000 футів (305 м) або 100 м).

Перехресні наведення. Являють собою результат інтерференції електромагнітних сигналів, переданих по сусідніх парах проводів.

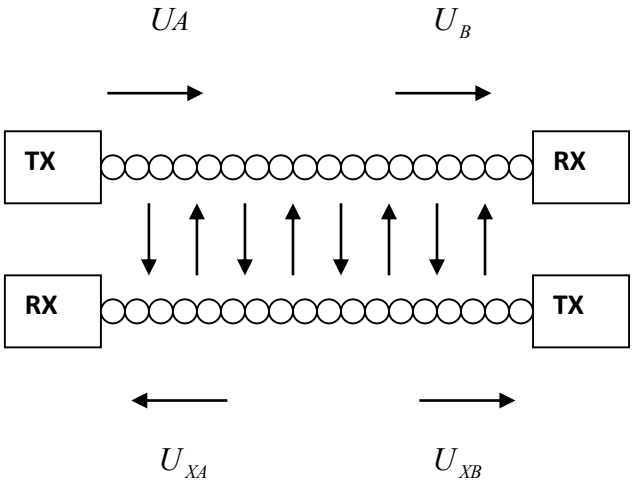


Рисунок 2.2 - Перехресні наведення

Виникають за рахунок наявності паразитних ємнісних і індуктивних зв'язків між парами. Характеризуються коефіцієнтом ослаблення перехресних наведень. Звичайно розглядаються на ближньому від передавача кінці кабелю (тут розташований приймач другої пари, що може сприйняти сигнал наведення як вхідний; потужність сигналу наведення тут буде максимальною).

Мірою завади є **коефіцієнт загасання перехресного наведення на ближньому від передавача кінці** (NEXT)

$$NEXT = -20\,lg\,\frac{U_{XA}}{U_A}$$

де, U_{XA} - амплітуда наведення на ближньому від передавача кінці лінії,

U_A - амплітуда сигналу, що передається.

Для кабелів витої пари категорії 5E(5+) і вище додатково вводяться параметри FEXT (**коефіцієнт загасання перехресного наведення на дальньому від передавача кінці**)

$$FEXT = -20 lg \frac{U_{XB}}{U_A},$$

де U_{XB} - амплітуда наведення на дальньому від передавача кінці лінії,

і ELFEXT (**еквівалентний коефіцієнт загасання перехресних наведень**)

$$ELFEXT = FEXT - Att.$$

Даний параметр характеризує еквівалентний рівень загасання перехресного наведення, що дорівнює різниці між загасанням перехресного наведення на дальньому від передавача кінці лінії й загасанням сигналу, що викликав дане наведення. Чим вище цей параметр, тим більше загасання власне перехресного наведення в порівнянні із загасанням корисного сигналу.

Критерієм можливості використання кабельного з'єднання для дуплексної передачі є параметр ***ACR*** – відношення загасання сигналу до загасання перехресного наведення на ближньому від передавача кінці лінії:

$$ACR = NEXT - Att.$$

Даний параметр можна трактувати як відношення сигнал/шум. Коли $ACR > 0$, рівень сигналу більше рівня шуму. *ACR* залежить від частоти сигналу. Частота сигналу, на якій $ACR = 0,$ є гранично припустимою частотою для даного кабелю. Для відносно надійної роботи *ACR* на максимальній частоті повинен бути не менше + 2…+4 дБ. *ACR* залежить від довжини кабельного сегмента й, зазвичай наводиться для сегмента довжиною 1000 футів (305 м) або 100 м.

Залежність наведених вище параметрів від частоти визначається конструктивними особливостями кабелю (діаметр провідників і ізоляції, матеріал ізоляції, наявність і вид екрана, крок скрутки для кабелю «вита пара»), дефектами виробництва, механічними впливами на кабель (розтягання, різкі вигини) і температурою навколишнього середовища.

Для розрахунку часових параметрів, що характеризують поширення сигналу у кабелі, використовується **номінальна швидкість поширення сигналу** (*NVR*), що характеризує ефект зменшення швидкості поширення електромагнітної хвилі в кабелі й визначається як відношення фактичної швидкості поширення до швидкості світла у вакуумі. Величина *NVR* у загальному випадку залежить від діаметра провідників, відстані між ними й типу діелектричної ізоляції. Звичайно наводиться в % від швидкості світла у вакуумі (типовий діапазон 60 % - 80 %).

З величиною швидкості поширення електромагнітної хвилі у кабелі зв'язана затримка надходження сигналу на вхід приймача після його подачі в лінію (затримка в кабельному сегменті без урахування затримок у проміжних активних вузлах). У кабелях, що містять кілька пар провідників, де є можливість організувати кілька окремих фізичних ліній передачі, матимуть місце різні величини затримок у кожній окремій фізичній лінії. Це зв'язано з двома факторами: відмінність у швидкості поширення електромагнітної хвилі у кожній окремій фізичній лінії (залежить від розкиду фізичних і геометричних характеристик матеріалів провідника й ізоляції); відмінність в електричній довжині різних фізичних ліній (що особливо помітно у випадку кабелю «вита пара», де кожна пара провідників має свій крок скрутки). Нормуванню підлягає максимальна різниця затримок проходження сигналу різними фізичними лініями у кабелі. Цю величину називають **асиметрією або перекосом затримок** (Skew). Даний параметр особливо важливий у випадку використання багатоканального розбиття даних, коли бітова послідовність даних розбивається на кілька частин і виконується одночасна передача кожної частини по окремих фізичних каналах (технологія Gigabit Ethernet, специфікація фізичного рівня 1000 Base-T).

Всі зазначені параметри наводяться виробниками кабельних систем у документації на відповідні кабелі. Існуючі стандарти на структуровані кабельні системи визначають тільки граничні припустимі значення даних параметрів.

Додатково для кабельних систем враховують рівень зовнішнього електромагнітного випромінювання або **електромагнітний шум**, під яким розуміється небажана змінна напруга в провіднику. Шум буває двох типів: імпульсний і фоновий. Шум підрозділяється також на низько - середньо - і високочастотний (НЧ, СЧ, ВЧ).

Джерелами фонового шуму є:

- у діапазоні до 150 кГц - лінії електропередач, телефони, лампи денного світла;
- у діапазоні від 150 кГц до 20 МГц - комп'ютери, принтери, копіювальні апарати й т.п.;
- у діапазоні від 20 МГц до 1 ГГц - телевізійні й радіопередавачі, мікрохвильові печі.

Основними джерелами імпульсного шуму є різного типу електродвигуни, електромеханічні перемикаючі пристрої (реле), зварювальні апарати. Рівень шуму виміряється в мілівольтах (мВ).

2.2. Основні типи кабельних систем

2.2.1. Поняття структурованих кабельних систем

Проектування сучасних кабельних систем відбувається відповідно до концепції структурованої кабельних системи (СКС) [О: 1, Д: 3, 4, 5], що визначається рядом стандартів:

- міжнародний стандарт ISO/IEC 11801;
- американський стандарт EIA/TIA 568B (найпоширеніший);
- європейський стандарт EN 5050173.

Принципово, вимоги всіх трьох стандартів збігаються, є лише відмінності в позначенні категорій кабелів і відповідності кабельних систем певним категоріям і класам.

Загалом, під структурованою кабельною системою розуміють ієрархічну слабкострумову кабельну систему будинку або групи будинків, розділену на функціональні підсистеми (магістральна підсистема, вертикальна підсистема,

горизонтальна підсистема) і призначену для підтримки різних інформаційних сервісів (комп'ютерна мережа, телефонія, охоронна й пожежна сигналізація, системи відеоспостереження й т.д.).

Зараз у якості одного з компонентів СКС додають ще систему електроживлення.

Стандарти на СКС визначають:

- основні характеристики компонентів кабельних систем, які повинні підтримуватися різними виробниками;
- вимоги до проектування й інсталяції кабельних систем;
- технічні характеристики для різних конфігурацій кабельних систем.

У стандартах наведені рекомендації із проектування й встановлення кабельних систем, складу й параметрам вертикальної й горизонтальної проводки, сполучних шнурів, типу використовуваних з'єднувачів і т.п.

Вимоги до заземлення визначені в стандарті EIA/TIA 607.

2.2.2. Кабель «вита пара» («Twisted Pair» - TP)

Кабель «вита пара» (ВП) є симетричним кабелем і використовується для диференціальної (балансової) передачі сигналу (обидва проводи в парі є рівноправними, інформативною є різниця потенціалів між ними) [О: 1 ; Д: 3, 4, 5].

Являє собою декілька пар проводів (у кожній парі проводи скручені на зразок спіралі), які поміщені в спільну діелектричну оболонку.

За рахунок скручування провідники в парі йдуть під деяким кутом один до одного, що зменшує паразитні ємнісні й індуктивні зв'язки між ними і, відповідно, зменшує перехресні наведення. Чим менше крок скрутки, тим менше перехресні наведення, але вище погонне загасання сигналу й вище затримка поширення сигналу.

Кабелі витої пари мають різні характеристики, що залежать від діаметра проводів, матеріалу діелектричної ізоляції, кроку скрутки, наявності захисних екранів з фольги або з міді. Діюча редакція стандарту ISO/IEC 11801 поділяє всі

види мережних додатків, які потребують обміну даними по кабелю ВП, на 6 класів - A, D, C, D, E, F. Для додатків кожного класу визначається відповідний клас ліній зв'язку, що задає граничні електричні характеристики лінії, необхідні для нормального функціонування додатку відповідного або більш низького класу. В американському стандарті EIA/TIA 568B використовується поняття категорії кабелю. Як критерій класифікації в стандартах на СКС використовується максимальна частота сигналу (таблиця 2.1).

Таблиця 2.1 - Класифікація кабелів витої пари

Клас додатку (ISO/IEC 11801)	**Категорія кабелю й роз'єма (EIA/TIA 568B)**	**Максимальна частота сигналу, МГц**	**Типові мережні додатки**
A	1	0,1	Телефонні голосові канали й низькочастотний обмін даними
B	2	1	Передача цифрових даних зі швидкостями до 4 Мб/с
C	3	16	Локальні мережі IBM Token Ring (4 Мб/с), Ethernet 10 Base-T, 100 Base-T4
	4	20	Локальні мережі IBM Token Ring (16 Мб/с), передача даних зі швидкостями до 25 Мб/с
D	5	100	Передача даних зі швидкостями до 100 Мб/с (синхронна передача - Ethernet 100 Base-TX і асинхронна передача (ATM) - 155 Мб/с)
D	5E(5+)	125	Передача даних зі швидкостями до 1000 Мб/с (Gigabit Ethernet 1000 Base-T)
E	6	200	Передача даних зі швидкостями до 1000 Мб/с
F	7	600	Передача даних зі швидкостями до 1000 Мб/с
	7e	1000	Широкосмугова передача даних на частотах до 900 МГц (передача даних зі швидкостями до 10 Гб/с, кабельне телебачення до 900 МГц)
	8	1200	Широкосмугова передача даних на частотах до 1200 МГц (передача даних зі швидкостями до 10 Гб/с, кабельне телебачення до 1200 МГЦ)

Стандарти ISO/IEC 11801 і EIA/TIA 568B визначають, що лінії зв'язку СКС будуть відповідати вимогам певної категорії при дотриманні наступних трьох умов:

- технічні характеристики всіх кабелів, роз’ємів, сполучних шнурів цієї лінії відповідають вимогам цієї категорії або перевищують їх;
- лінія зв'язку спроектована з урахуванням вимог стандартів (тобто дотримані обмеження на довжини кабельних сегментів, кількість точок комутації й т.д.);
- монтаж виконаний у повній відповідності з вимогами зазначених стандартів.

Конструктивно кабелі однієї категорії відрізняються від кабелів іншої категорії кроком скрутки й витримуванням постійної кількості скруток на одиницю довжини кабелю. Чим вище категорія, тим більше кількість скруток на одиницю довжини. Починаючи з 5 категорії й вище, обов'язково витримується постійне число скруток на одиницю довжини. У кабелях високих категорій (з категорії 5 і вище) крок скрутки в кожній парі відрізняється, що дозволяє зменшити паразитні зв'язки між парами й, відповідно, перехресні наведення.

Зараз при проектуванні нових мереж мінімально припустимою градацією є кабель категорії 5 (а краще 5E(5+), що повністю відповідають вимогам технології Gigabit Ethernet 1000 Base-T).

За критерієм наявності захисних екранів вита пара поділяється на: незахищену виту пару (UTP), у якої відсутні будь-які екранувальні елементи захисту, і захищену виту пару (STP), у якої присутній металевий екран. Екранування дозволяє зменшити електромагнітне випромінювання у кабелі та із кабелю. Спочатку, під STP розумівся спеціалізований кабель фірми IBM - STP type 1, характеристики якого відрізняються від характеристик кабелів витої пари різних категорій, наведених у стандартах на СКС. У наш час у захищеному варіанті випускаються кабелі різних категорій. При цьому, зазвичай, використовують термін «екранований» (Screened) - у випадку використання фольги, що екранує, і термін «захищений» (Shielded) - у випадку використання екранувального обплетення або складних екранів (фольга + обплетення). За цією конструктивною ознакою можна виділити наступні типи кабелів:

FTP - фольгована вита пара: містить один спільний екран з алюмінієвої фольги навколо всіх пар;

ScTP, STP (категорії 5 і вище) - містить екран з мідного обплетення, що може бути спільним для всіх пар, або виконуються окремі екрани для кожної пари;

S/FTP - містить 2 екрани з фольги й мідного обплетення(можливо окреме екранування фольгою кожної пари із спільним екраном з мідного обплетення);

S/STP - містить 2 екрани з мідного обплетення (окреме екранування мідним обплетенням кожної пари із спільним екраном з мідного обплетення);

PIMF - кожна пара в окремому екрані з фольги й спільне зовнішнє мідне обплетення.

Кабелі категорії 5 і 6 можуть випускатися в будь-якому варіанті: від UTP до S/STP. Кабелі категорії 7 і вище випускаються тільки у варіанті S/STP або PIMF (обов'язково містить 2 екрани).

Граничні значення параметрів UTP категорії 3 і 5 наведені в таблиці 2.2.

Таблиця 2.2 - Граничні значення параметрів UTP категорії 3 і 5

Характеристики (на 1000 футів або 305 метрів)	Категорія 3	Категорія 5	STP type 1 IBM
Ємність, нФ	20	17	9
Активний опір, Ом	28,7	28,7	-
Хвильовий опір	100±15%	100±15%	150±15%
Загасання, дБ:			
10 МГц	30	20	-
62,5 МГц	-	-	39
100 МГц	-	67	-
NEXT, дБ			
10 МГц	26	47	-
16 МГц	23	44	40
100 МГц	-	32	-

Для позначення діаметра струмоведучих провідників використовують умовні одиниці, що називаються AWG (американська градація проводів), наприклад, AWG22, AWG24, AWG26. Чим менше значення AWG, тим більше діаметр струмоведучого провідника, тим менше погонний опір.

Вита пара звичайно випускається у двох варіантах AWG24 і AWG22.

AWG	Діаметр, мм	Погонний опір, Ом/км
24	0,51	87,5
22	0,64	51,7

Структура лінії горизонтальної підсистеми СКС

Вимоги до характеристик кабельної системи визначаються стандартами на структуровані кабельні системи (наприклад, EIA/TIA – 568B), де обумовлюється наступна структура лінії (рис. 2.3).

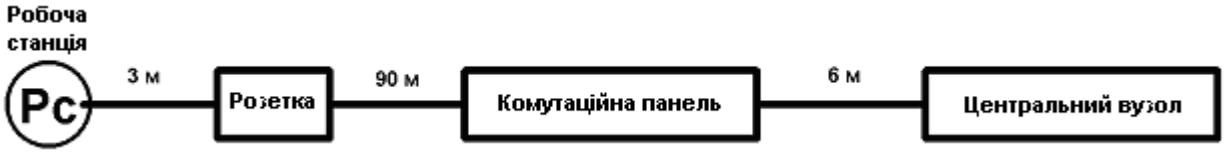


Рисунок 2.3 - Структура лінії

Дані стандарти регламентують віддалення робочої станції від центрального вузла на відстань не більш 100 м (пов'язано з загасанням електричного сигналу при проходженні через лінію).

Зазначені на структурі довжини сегменту і сполучних кабелів не є жорстко регламентованими. Головне, щоб сумарна довжина не перевищувала 100 м.

У кабелі задіяні 2 пари, одна – для передачі, друга – для прийому і виявлення колізій (ще дві пари не використовуються).

Розкладка проводів в кабельних сегментах виконується за наступною схемою (прямий кабель) (рис. 2.4.).

Порт мережного адаптера називається MDI портом (DTE). На цьому порту пара 2 (білий/оранжевий) підключена до передавача, пара 3 (білий/зелений) – до приймача; пари 1 (білий/синій) і пара 4 (білий/коричневий) не використовуються. Порт на центральному вузлі (концентратори,

комутатори) називається MDI-x портом, у якому пара 2 підключається до приймача, а пара 3 – до передавача.

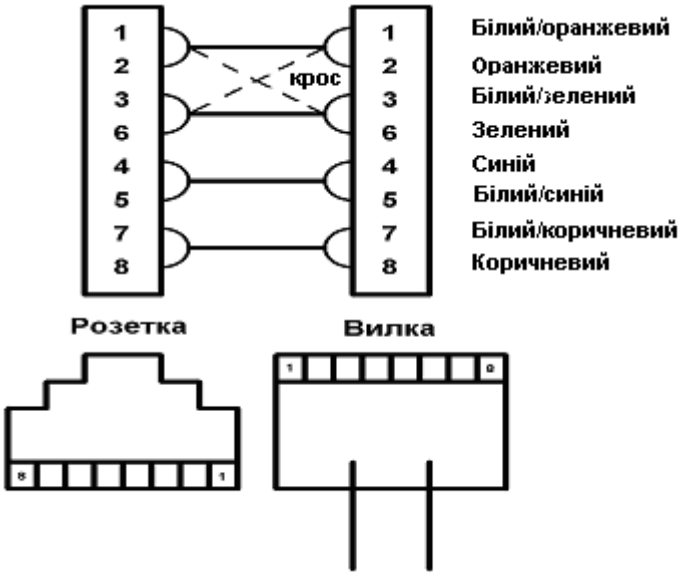


Рисунок 2.4 - Схема розкладки проводів по стандарту EIA/TIA 568 B

Таким чином, за прямою схемою з'єднання мережний адаптер може бути з'єднаний лише з центральним вузлом. При необхідності з'єднання двох мережних адаптерів використовують крос-кабель.

У стаціонарній частині кабельного каналу (між розеткою і комутаційною панеллю) необхідно використовувати тільки пряму схему розкладки. При необхідності, по крос-схемі розкладається тільки один зі сполучних кабелів (патч-корд).

2.2.3. Коаксіальний кабель

Коаксіальний кабель (КК) є асиметричним або небалансовим кабелем (екранувальний шар є спільним проводом, підключеним до «землі», інформативним є електричний сигнал, що знімається із центрального провідника відносно «землі») [О: 1 ; Д: 3, 4, 5].

КК складається із центрального мідного провідника (одножильного або багатожильного), оточеного шаром діелектрика, матеріал якого відокремлює

центральний провідник від оболонки, що екранує (екранувальне металеве обплетення, суцільний металевий циліндр, комбінація з алюмінієвої фольги й металевого обплетення). Зовні кабель покритий захисною діелектричною оболонкою (рис. 2.5).

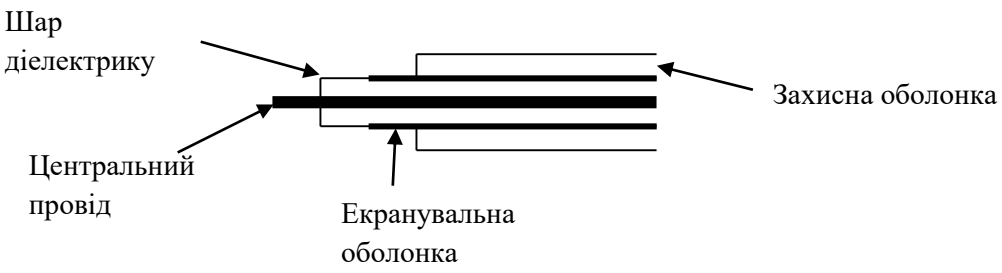


Рисунок 2.5 - Структура коаксіального кабелю

Існують різновиди кабелю різного діаметра. Діаметр центрального провідника й ізолюючого шару, а також характеристики матеріалів ізоляції визначають частотні властивості кабелю, загасання й імпеданс.

Таблиця 2.3 - Основні типи коаксіальних кабелів

Кабель	Імпеданс, Ом	Діаметр, мм		Застосування
		Зовнішній	Центральний провідник	
RG-8	50	~12	2.17 о/ж*	Специфікація 10 Base-5 («товстий» «Thick» Ethernet)
RG-58 /U	50	5	0.66 або 0.695 о/ж*	Специфікація 10 Base-2 («тонкий» «Thin» Ethernet)
RG-58 A/U	50	5	0,66 або 0,78 б/ж**	
RG-58 C/U	50	5	0,66 б/ж**	
RG-62	93			Локальні мережі Arcnet, IBM Token Ring
RG-6	75			Локальні мережі Arcnet, CATV (кабельне телебачення)
RG-11				
RG-59				

* - одножильний;
** - багатожильний.

В ідеальному випадку електромагнітне поле, що утвориться при проходженні електричного сигналу по кабелю, не виходить за межі оболонки, що екранує. Таким чином КК не створює електромагнітних завад і малочутливий до зовнішніх завад. На практиці завжди існує електромагнітне випромінювання у кабелі та із кабелю.

Основні типи коаксіальних кабелів наступні (табл. 2.3). Сучасні версії стандартів на структуровані кабельні системи не допускають використання коаксіального кабелю як середовища передачі.

2.2.4. Волоконно-оптичний кабель

Волоконно-оптичний кабель (ВОК) використовується для передачі даних у вигляді оптичних імпульсів ІЧ-діапазону [О: 1 ; Д: 3, 4, 5]. Інформаційний сигнал передається через оптичне волокно у вигляді модульованого світлового випромінювання. Завдяки явищу повного внутрішнього відображення, світло, що потрапив в оптоволокно, поширюється по ньому на великі відстані.

ВОК складається із центрального оптичного ядра (звичайно кварц із легуючими добавками) або світловоду, навколо якого розміщений первинний (відбивний) буфер (рис. 2.6). Коефіцієнт заломлення матеріалу буфера набагато менше коефіцієнта заломлення матеріалу ядра. За рахунок цього досягається практично повне відбиття світлових променів від границі *ядро - первинний буфер*. Для забезпечення захисту від вологи й зовнішніх впливів наноситься захисний буферний шар.

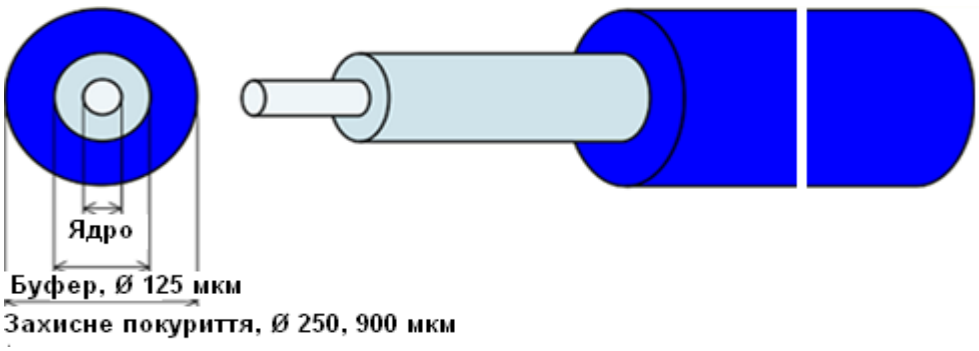


Рисунок 2.6 - Структура оптичного кабелю

Світлові хвилі (моди), що потрапили в ядро під кутами, меншими деякого критичного значення, багаторазово відбивається від оболонки і поширюються на значні відстані (рис. 2.7). Під оптичною модою розуміється певний тип електромагнітної хвилі.

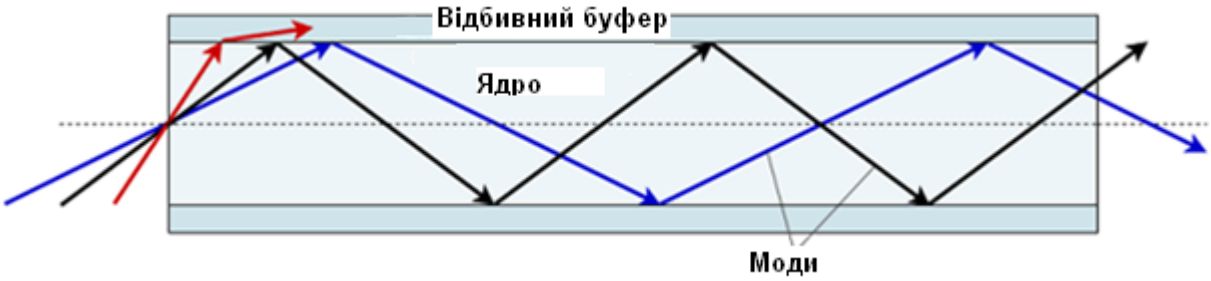


Рисунок 2.7 - Поширення світлових хвиль через оптичне волокно

Крім різниці між показниками заломлення ядра і відбивного буферу важливу роль відіграє профіль показника заломлення ядра, тобто залежність величини показника заломлення від радіусу поперечного перерізу оптоволокна. Якщо показник заломлення залишається однаковим в усіх точках перетину ядра, такий профіль називається ступінчастим, якщо плавно зменшується від центральної осі до оболонки, - градієнтним (рис. 2.8). Зустрічаються і більш складні профілі. Профіль показника заломлення впливає на характеристики оптичного волокна як середовища передачі інформації.

Серед великого числа характеристик і параметрів, що описують оптичне волокно як середовище передачі даних, найбільш важливими є загасання (втрати) і дисперсія.

Загасання - це поступове ослаблення потужності оптичного сигналу при поширенні по оптоволокну, викликане різними фізичними процесами. Величина загасання має складну залежність від довжини хвилі випромінювання і вимірюється в дБ/км. Загасання служить одним з головних факторів, що обмежують дальність передачі сигналу через оптичне волокно (без ретрансляції).

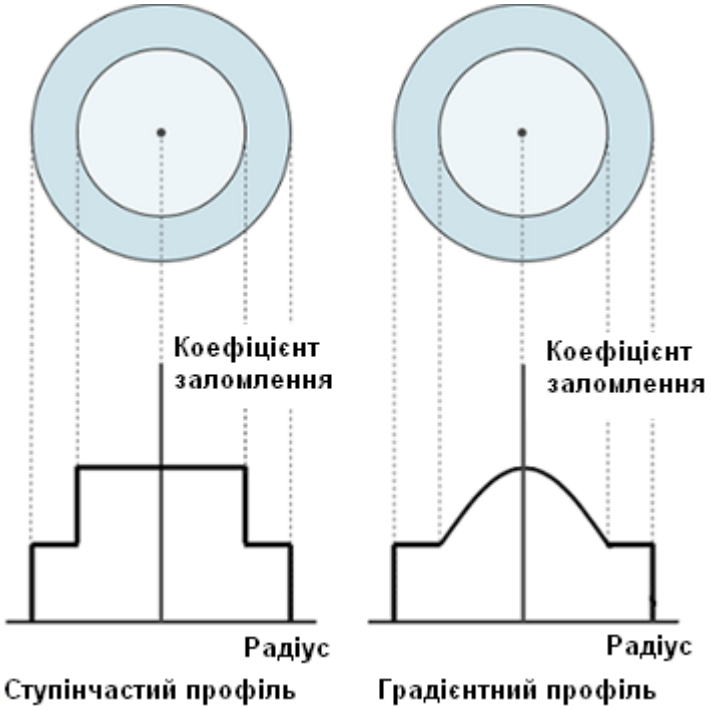


Рисунок 2.8 - Типи профілів показника заломлення ядра

Дисперсія - це розширення оптичного імпульсу, переданого по оптоволокну, в часі (рис. 2.9). При високій частоті проходження імпульсів таке розширення на деякій відстані від передавача призводить до перекривання сусідніх імпульсів і помилкового прийому даних. Дисперсія обмежує дальність, так і швидкість передачі інформації.

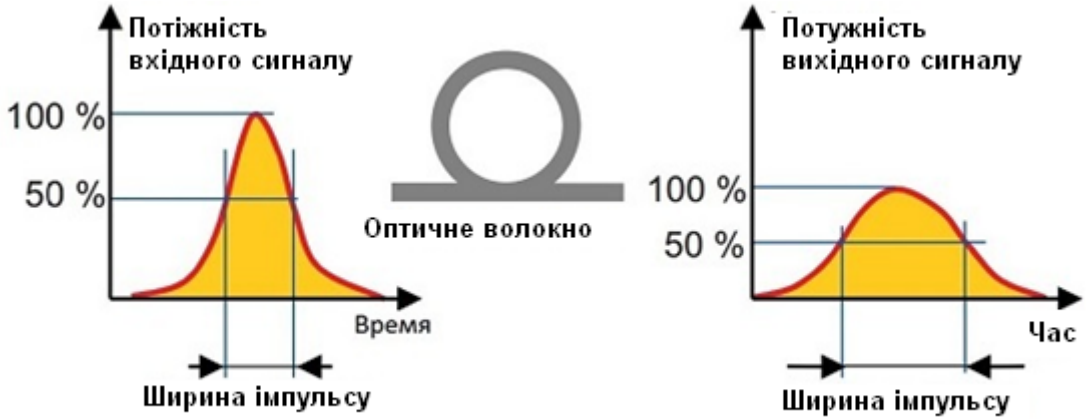


Рисунок 2.9 - Розширення оптичного імпульсу при походженні по волокну

Різновиди і класифікація оптичних волокон

Класифікація оптичних волокон найчастіше проводиться по двом критеріям:

• матеріал, з якого виготовляється ядро і оптична оболонка;

• кількість мод, що поширюються по волокну.

В залежності від матеріалу ядра й первинного буфера існує наступна класифікація оптичних волокон.

1. Скляні волокна: ядро й буфер виготовляються з оксиду кремнію (SiO_2) або кварцу. Діаметр ядра/діаметр оболонки (мкм) – 50/125 (багатомодовий кабель), 9/125 (одномодовий кабель).

2. Скляні волокна із пластиковим первинним буфером (HCS або PCS-волокна). Діаметр ядра/діаметр оболонки (мкм) - 200/230, 200/350.

3. Пластикові волокна (POF – волокна): ядро й первинний буфер виготовляються із пластику. Діаметр ядра/діаметр оболонки (мкм): 485/500, 735/750, 980/1000.

Пластикові й PCS волокна зазвичай не містять захисного буфера. На рис. 2.10 зображені поперечні перерізи цих типів волокон.

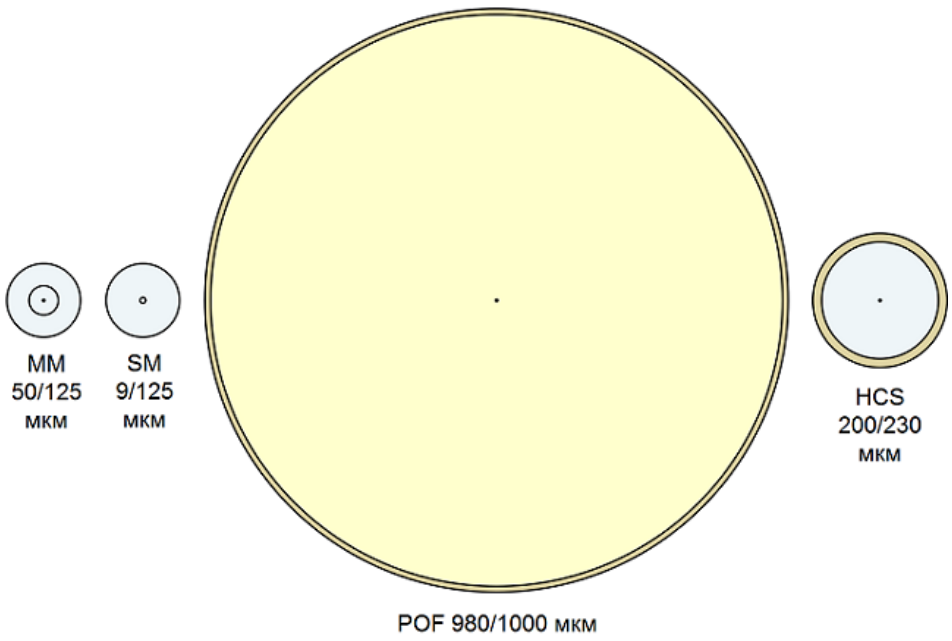


Рисунок 2.10 - Поперечні перерізи різних типів оптичних волокон

В залежності від геометричних розмірів ядра і оболонки і величин показників заломлення їх матеріалів в оптичному волокні може поширюватися тільки одна або ж велику кількість просторових мод. Тому всі оптичні волокна ділять на два великі класи: одномодові (SM) та багатомодові (MM) .

Багатомодове кварцове волокно має і серцевину, і оптичну оболонку з кварцового скла. Перенесення сигналу здійснюється декількома оптичними модами, які входять у ядро під різними кутами. Відповідно, моди по різному відбиваються від первинного буфера й проходять різну оптичну довжину у кабелі. Як правило, таке оптоволокно має градієнтний профіль показника заломлення (рис. 2.11). Це необхідно для зниження впливу міжмодової дисперсії. Як було показано вище (рис. 2.7), моди поширюються в оптичному волокні по різних траєкторіях і, відповідно, час поширення кожної моди буде відрізнятися. Це приводить до розширення переданого імпульсу. Градієнтний профіль зменшує різницю в часі поширення мод. За рахунок плавної зміни показника заломлення моди вищого порядку, які потрапляють в волокно під великим кутом і поширюються по довшим траєкторіях, мають і більшу швидкість, ніж ті, які поширюються ближче до центру ядра. Повністю усунути вплив міжмодової дисперсії неможливо, тому багатомодове волокно поступається одномодовому по дальності і швидкості передачі інформації.

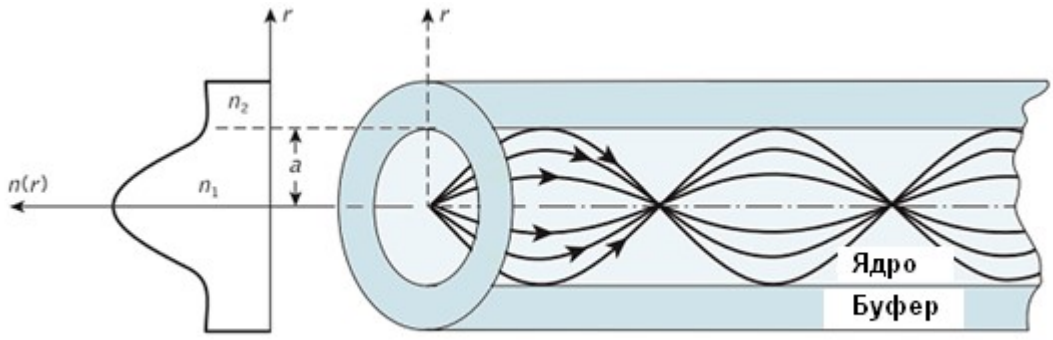


Рисунок 2.11 - Особливості передачі оптичного сигналу через багатомодове волокно

У багатомодовому кабелі діаметр ядра набагато більше довжини хвилі випромінювання, як джерело випромінювання використовуються світлодіоди. Робочими для багатомодового волокна зазвичай є довжини хвиль 850 і 1300 (1310) нм. Типове загасання на цих довжинах хвиль - 3,5 і 1,5 дБ/км відповідно. За рахунок інтерференції між модами у багатомодового кабелю менше смуга пропускання у порівнянні з одномодовим.

Класифікація. Кварцове багатомодове волокно було першим типом волокна, яке стало широко застосовуватися на практиці. Поширення отримали два стандартних розміру багатомодових волокон (діаметр ядра/оболонки): 62,5 / 125 мкм і 50/125 мкм. Загальноприйнята класифікація багатомодових кварцових волокон наводиться у стандарті ISO / IEC 11801. Цей стандарт виділяє чотири класи багатомодових волокон (OM - Optical Multimode), що відрізняються шириною смуги пропускання (параметр, що характеризує міжмодову дисперсію і визначає швидкість передачі інформації):

• OM1 - стандартне багатомодове волокно 62,5 / 125 мкм;

• OM2 - стандартне багатомодове волокно 50/125 мкм;

• OM3 - багатомодове волокно 50/125 мкм, оптимізоване для роботи з лазером;

• OM4 - багатомодове волокно 50/125 мкм, оптимізоване для роботи з лазером, з поліпшеними характеристиками.

Типові характеристики багатомодових кабелів наведені в таблиці 2.4.

Таблиця 2.4 - Типові характеристики багатомодових оптичних кабелів

Тип волокна	50/125	62,5/125	100/140
Позначення	GI	GK	GN
Діаметр ядра, мкм	50÷3	62,5÷3	100÷4
Діаметр первинного буфера, мкм	125÷3	125÷2	140÷6
Коефіцієнт загасання дБ/км			
850 нм	2,4÷3	3÷3,8	3,5÷4,5
1300 нм	0,6÷1,2	0,7÷1,5	1,5÷2,0
Ширина смуги пропускання, МГц*км			
850 нм	400÷1000	160÷200	100÷300
1300 нм	400÷1500	200÷600	100÷500

У **одномодовому волокні** поширюється тільки одна (основна) мода випромінювання. Це досягається за рахунок дуже маленького діаметру ядра (зазвичай, 8-10 мкм) (рис. 2.12). Діаметр оптичної оболонки такий же, як і у багатомодового волокна - 125 мкм. Відсутність інших мод позитивно позначається на характеристиках оптоволокна (немає міжмодової дисперсії), збільшуючи дальність передачі без ретрансляції до сотень кілометрів і швидкість до десятків Гб/с. Загасання в одномодовому волокні також вкрай низьке (менше 0,4 дБ / км).

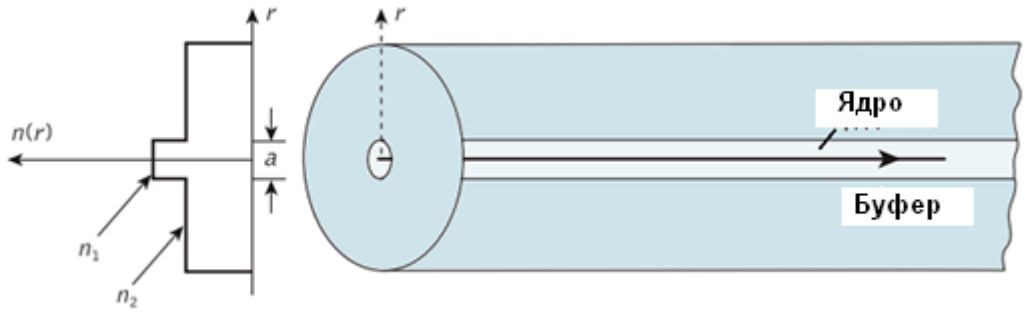


Рисунок 2.12 - Особливості передачі оптичного сигналу через одномодове волокно

Діапазон довжин хвиль для одномодового волокна досить широкий. Зазвичай передача здійснюється на довжинах хвиль 1310 і 1550 нм. Як джерело випромінювання використовуються напівпровідникові лазери. При використанні технології спектрального ущільнення каналів використовуються і інші довжини хвиль.

Класифікація. Асортимент кварцових одномодових волокон дуже різноманітний. Міжнародний стандарт ISO / IEC 11801 та європейський EN 50173 по аналогії з багатомодовим волокном виділяють два великі класи одномодових волокон: OS1 і OS2 (OS - Optical Single-mode). Однак у зв'язку з існуючою плутаниною, пов'язаної з цим поділом, така класифікація використовується дуже рідко. Набагато більш інформативними є рекомендації ITU-T G.652-657, що виділяють більше типів одномодових волокон. У таблиці

2.5. представлена коротка характеристика типів волокон і області їх застосування.

Таблиця 2.5 - Характеристики типів одномодових волокон згідно рекомендацій ITU-T G.652-657

Тип волокна	Опис	Застосування
G.652. Одномодове волокно з незміщеною дисперсією	Найбільш поширений тип одномодового волокна з точкою нульової дисперсії на довжині хвилі 1300 нм. Розрізняють 4 підкласу (A, B, C і D). Волокна G.652.C і G.652.D відрізняються низьким загасанням поблизу «водного піку» («водним піком» називають область великого загасання в стандартному волокні при довжині хвилі близько 1383 нм).	Стандартні області застосування.
G.653. Одномодове волокно з нульовою зміщеною дисперсією	Точка нульової дисперсії зміщена на довжину хвилі 1550 нм.	Передача на довжині хвилі 1550 нм.
G.654. Одномодове волокно зі зміщеною довжиною хвилі відсічки	Довжина відсічки (мінімальна довжина хвилі, при якій волокно поширює одну моду) зміщена в область довжин хвиль близько 1550 нм.	Передача на довжині хвилі 1550 нм на дуже великі відстані. Магістральні підводні кабелі.
G.655. Одномодове волокно з ненульовою зміщеною дисперсією	Це волокно має невелике, але не нульове, значення дисперсії в діапазоні 1530-1565 нм (ненульова дисперсія зменшує нелінійні ефекти при одночасному поширенні декількох сигналів на різних довжинах хвиль).	Лінії передачі зі спектральним ущільненням каналів (DWDM).
G.656. Одномодове волокно с ненульовий зміщеною дисперсією для широкосмугової передачі	Ненульова дисперсія в діапазоні довжин хвиль 1460-1625 нм.	Лінії передачі зі спектральним ущільненням каналів (CWDM/DWDM).
G.657. Одномодовое волокно, що не чутливе до втрат на мікровигині	Волокно зі зменшеним мінімальним радіусом вигину і з меншими втратами на вигині. Виділяють кілька підкласів.	Для прокладання в обмеженому просторі.

Типові характеристики одномодових кабелів наступні:

- тип волокна: 9/125 (8/125; 8,3/125; 9,1/125; 9,3/125);

- позначення: SM (Single Mode);

- діаметр модового поля (при довжині хвилі випромінювання 1310 нм), мкм: 9±0,5;
- діаметр первинного буфера, мкм: 125±2;
- діапазон довжин хвиль випромінювання, нм: 1150…1550;
- коефіцієнт загасання дБ/км:

при довжині хвилі випромінювання 1310 нм - 0,35…0,5

при довжині хвилі випромінювання 1550 нм - 0,25…0,3.

Скляні волокна із пластиковим первинним буфером (HCS)

HCS-волокно - це багатомодове оптичне волокно великого діаметру з ядром з кварцового скла і оболонкою з полімерного матеріалу (рис. 2.13). Найбільшого поширення в телекомунікації отримало HCS-волокно з діаметром серцевини і оболонки 200/230 мкм і ступінчастим показником заломлення. В інших областях, таких як медицина і наукові дослідження, можуть використовуватися HCS-волокна з великим діаметром серцевини (300, 400, 500 мкм ...).

За своїми оптичним характеристикам HCS-волокно також займає проміжне положення між кварцовим оптоволокном і POF. Мінімум загасання стандартного HCS-волокна припадає на довжину хвилі 850 нм і становить одиниці-десятки дБ/км. Для роботи з HCS-волокном можна використовувати ті ж активні компоненти, що і для POF (з довжиною хвилі 650 нм) або для багатомодового кварцового волокна (світлодіоди з довжиною хвилі 850 нм). Відстань передачі при використанні HCS-волокна може складати декілька кілометрів.

Пластикові волокна (POF)

Пластикове або полімерне оптичне волокно (POF - Plastic / Polymer Optical Fiber) - це багатомодове волокно великого діаметру із ступінчастим показником заломлення, серцевина і оболонка якого виготовлені з полімерних матеріалів, перш за все, з поліметилметакрилату (оргскло). Найчастіше можна зустріти POF із співвідношенням діаметрів серцевини і оболонки 980/1000 мкм.

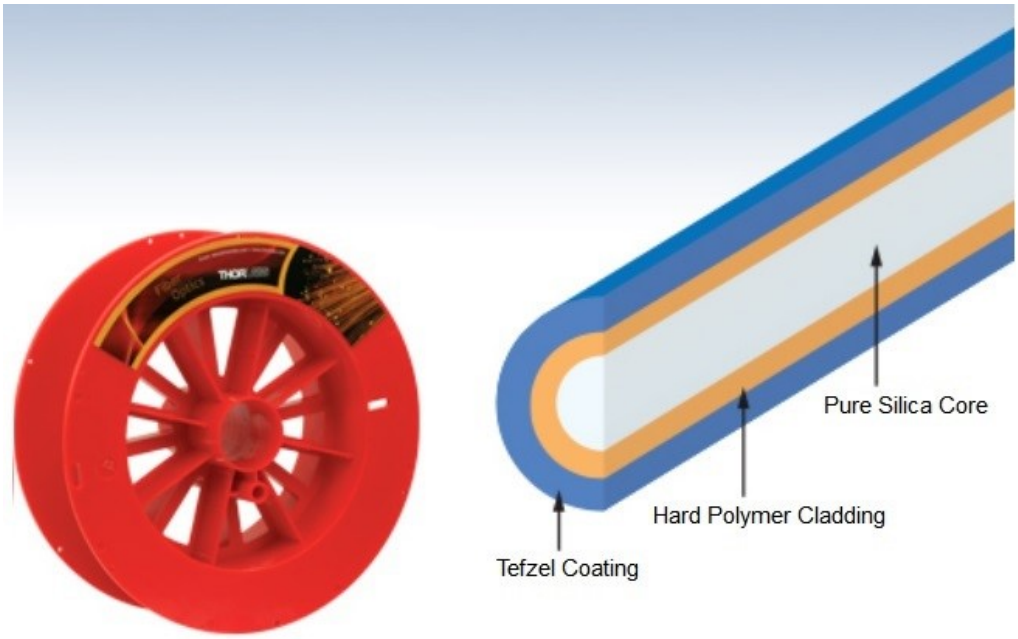


Рисунок 2.13 - Структура HCS-волокна

У порівнянні з кварцовим волокном POF має дуже великі втрати (100-200 дБ/км). З іншого боку, мінімум втрат знаходиться у видимому діапазоні (520, 560 і 650 нм). Це, а також дуже великий розмір поперечного перерізу, дозволяє використовувати в якості джерел випромінювання дешеві світлодіоди. Великий діаметр також значно спрощує процес роботи з пластиковим волокном.

Область застосування POF - короткі низькошвидкісні лінії зв'язку (до 200 Мб/с на кілька десятків метрів). POF часто використовується в промислових лініях зв'язку, автомобільній електроніці, медицині, у телеметричних системах для передачі інформації з різного роду датчиків.

Як вже було зазначено вище, для переносу інформаційних сигналів використовується оптичне випромінювання з довжинами хвиль 850, 1310, 1550 нм. Світлодіоди можуть випромінювати світло з довжиною хвилі 850 нм і 1310 нм. Напівпровідникові лазери - 1310, 1550 нм. Використання зазначених значень довжин хвиль пов'язано з особливостями оптичних характеристик кабелів (на цих довжинах хвиль спостерігається яскраво виражені максимуми передачі потужності оптичного сигналу).

Залежно від умов експлуатації оптичні кабелі діляться на кабелі для внутрішньої прокладки, зовнішньої прокладки й універсальні.

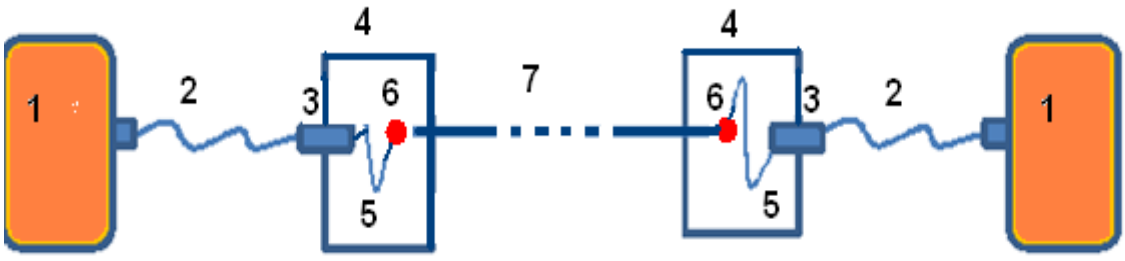
Відмінна риса зовнішніх кабелів полягає у наявності додаткових захисних шарів (акрилові волокна, металева броня) і спеціального наповнювача для захисту від вологи. Такі кабелі не можна використовувати при прокладці усередині будівлі на великі відстані (обмеження по пожежній безпеці через високу задимленість при горінні таких кабелів); допускається введення в будівлю на відстань до 20 метрів.

Кабелі внутрішньої прокладки містять 4…12 світловодів, зовнішні 8…20 (бувають до 144 світловодів).

ВОК являє собою односпрямоване середовище передачі. Кожне оптичне ядро використовується для організації одного каналу в одному напрямку. Для формування дуплексного каналу необхідно два світловоди. У наш час існує технологія мультиплексування по довжинах хвиль, що дозволяє через одне оптичне волокно передавати кілька оптичних сигналів і організовувати дуплексну передачу через один світловод.

Структура оптичної лінії.

Спрощена структура оптичної лінії наведена на рис. 2.14.



1 – вузол з оптичним портом , 2 – оптичний патч-корд, 3 – прохідний адаптер (SC-SC, FC-FC, LC-LC), 4 – оптична розподільна панель/бокс (ODF), 5 – оптичний пігтейл, 6-місце зварки пігтейла з волокном, 7 – оптичний кабель

Рисунок 2.14 - Спрощена структура оптичної лінії

Лінія будується з використанням наступних складових:

- оптичний кабельний сегмент;
- оптична розподільна панель або оптичний бокс для виконання кінцевих підключень;
- пігтейл (відрізок оптичного волокна зі встановленим на одному кінці оптичним з'єднувачем; з'єднується з оптичним світловодом кабелю методом зварювання);
- оптичний патч-корд (відрізок оптичного волокна в захисній оболонці зі встановленими з двох кінців оптичними з'єднувачами) для виконання комутацій та підключення портів кінцевих вузлів до оптичного каналу;
- прохідний адаптер відповідного типу для механічного з'єднання з'єднувачів патч-кордів та пігтейлів.

Типи оптичних з'єднувачів

Існує два методи фізичного з'єднання оптичних волокон: використання сполучних з'єднувачів та використання зварювання двох волокон. Для виконання механічного з'єднання найбільш поширеними є наступні типи оптичних з'єднувачів, які відрізняються формою та розмірами, матеріалом та конструктивом з'єднання (на рис. 2.15 наведені з'єднувачі та прохідні адаптери відповідного типу):

- SC - Subscriber connector (рис. 2.15 а),
- LC - Little Connector або Local Connector (рис. 2.15 б),
- FC - Ferrule Connector або Fiber Channel (рис. 2.15 в).

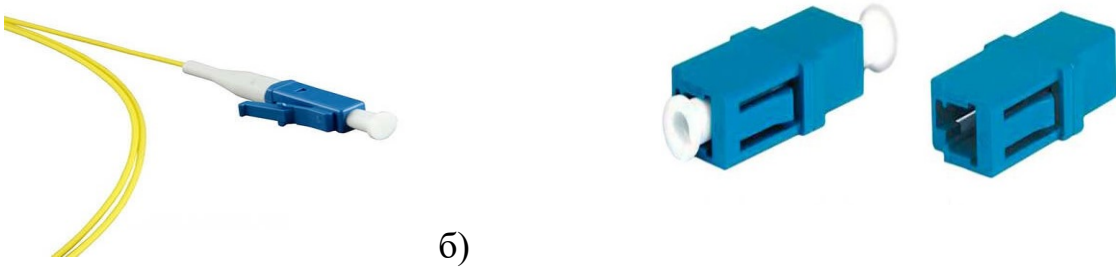
З'єднувачі SC та LC для одномодового оптичного кабелю мають синій колір, для багатомодового кабелю – сірий.

Крім наведених вище ознак з'єднувачі розрізняються ферулою - керамічним (рідше пластиковим) сердечником, яких є два типи (рис. 2.16):

- UPC (UltraPolishedConnector) - сердечник відполірований під кутом 90 ° до поздовжньої осі ферули,

- APC (AnglePolishedConnector) - сердечник скошений під кутом 8 °. APC призначений для того, щоб зменшити вплив відбитого сигналу на сигнал в волокні. З'єднувачі типу SC та LC з такою ферулою мають зелений колір.

а)



б)

в)

Рисунок 2.15 - Оптичні з'єднувачі та прохідні адаптери:
а) типу SC, б) типу LC, в) типу FC

Під кожен вид з'єднувачів є і свої прохідні адаптери (UPC та, відповідно, APC). UPC і APC з'єднувачі між собою з'єднувати не можна. Пов'язано це знову ж з тими самими ферулами, в яких, власне, і відмінність. Їх можна пошкодити (рис. 2.17) і/або отримати на цьому з'єднанні велике загасання (близько 6 дБ).

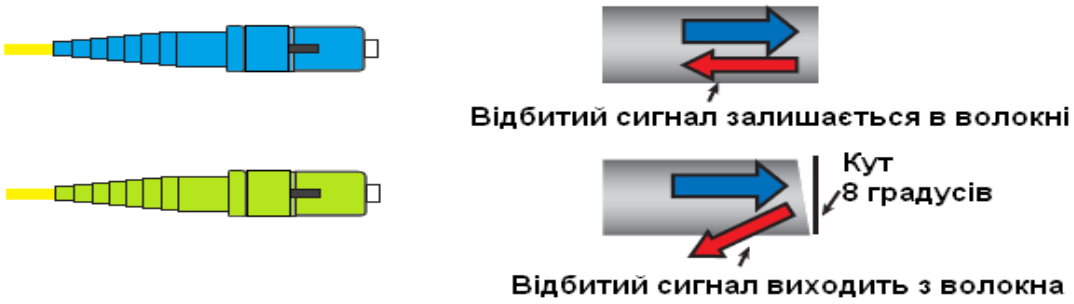


Рисунок 2.16 - Відмінності SC/UPC і SC/APC конекторів

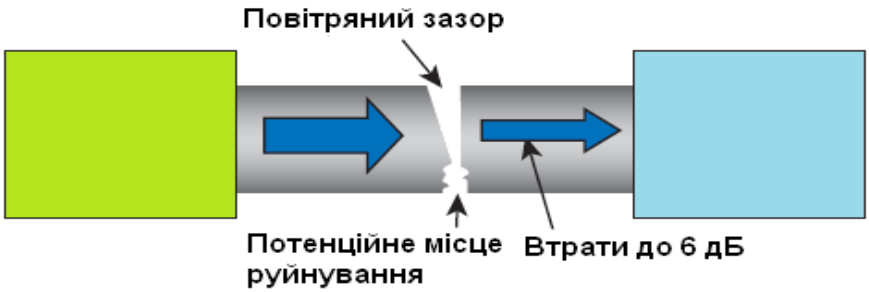


Рисунок 2.17 - Проблеми при з’єднанні SC/UPC і SC/APC з’єднувачів

2.2.5. Розрахунок бюджету втрат оптичної системи

Загальна термінологія

Вікно прозорості - діапазон довжин хвиль оптичного випромінювання, в якому має місце менше, у порівнянні з іншими діапазонами, загасання випромінювання в волокні (для одномодового волокна це, зазвичай, 1310 нм, 1490 нм або 1550 нм).

дБм - децибел на міліват, одиниця виміру потужності в оптичних системах передачі даних. Відрізняється від децибел тим, що рівень еталонного сигналу завжди дорівнює 1мВт. Формула переводу потужності в дБм: A = 10logX, де A - значення в дБм, log - десятковий логарифм, X - значення потужності в мВт.

Оптична потужність - потужність передавача будь-якого оптичного пристрою прийому / передачі даних. Вимірюється в дБм або мВт. Значення оптичної потужності передавачів різних оптичних технологій та виробників знаходяться в діапазоні від -9 дБм до 7дБм.

Оптична чутливість - чутливість приймача будь-якого оптичного пристрою прийому / передачі даних. Вимірюється в дБм або мВт. Значення оптичної чутливості приймачів різних оптичних технологій та виробників, зазвичай, лежать у діапазоні від - 12дБм до -30дБм.

Оптичний бюджет потужності - різниця між значенням потужності передавача і чутливості приймача на різних кінцях лінії зв'язку. Вимірюється в дБ. Параметр, зазвичай, використовується при проектуванні пасивних оптичних мереж (PON) для розрахунку максимальної протяжності оптичного каналу з урахуванням загасань на проміжних механічних з єднаннях та пасивних оптичних розгалужувачах (спліттерах).

Загасання - процес втрати потужності світлового сигналу в лінії зв'язку. Сигнал в лінії зв'язку загасає як природним чином, так і за рахунок неоднорідностей в волокні, спліттерах, механічних з'єднувачах, в місцях зварювання волокна, перегинів, механічних пошкоджень. Вимірюється загасання в дБ/км для волокна і в дБ для всього іншого. Стандартне загасання у волокні на довжині хвилі 1310нм становить 0.36дБ/км, на довжині хвилі 1550нм - 0.22дБ / км. Стандартне загасання на механічному з'єднувачі типу SC / UPC-SC / UPC становить близько 0.5дБ, на зварюванні - 0.05дБ. У пасивних оптичних мережах (PON) основне загасання вносять оптичні розгалужувачі (спліттери) – загасання на них може бути від 4дБ до 21дБ (залежить від кількості виходів розгалужувача та технології його виготовлення).

Оптичний бюджет втрат - сумарне загасання від джерела сигналу до самого віддаленого приймача сигналу. Вимірюється в дБ.

Якщо при проектуванні та побудові оптичних каналів передачі даних з використанням технологій 1Гб/с та 10 Гб/с Ethernet (1GE та 10GE) досить рідко проводять попередні розрахунки оптичного бюджету (виходячи з реальної

довжини оптичного каналу вибираються оптичні прийомо/передавачі на відповідну відстань – бувають на відстані від 2 км до 80 км), то при проектуванні пасивних оптичних мереж, де використовуються проміжні оптичні розгалужувачі з досить високими коефіцієнтами загасання, необхідно провести розрахунки бюджету втрат для конкретної топології мережі, що проектується.

Розглянемо розрахунки бюджету втрат на наступних прикладах.

Приклад 1. Оптичний канал, який з'єднує за топологією «точка-точка» два пристрої з оптичними портами (рис. 2.8), де використовуються оптичні модулі SFP 1000Base-LX (технологія 1GE розрахована на одномодовий оптичний кабель). Для оцінки бюджету втрат будемо використовувати такі вихідні дані.

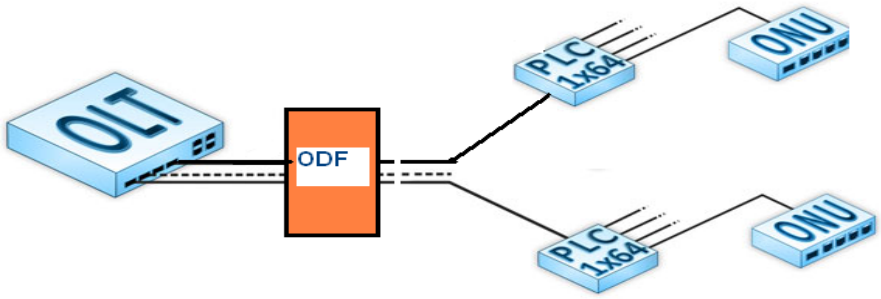
- Мінімальна вихідна потужність оптичного модуля SFP (на прикладі D-Link DEM-310GT) = - 9 дБм.
- Чутливість оптичного модуля SFP = -22 дБм.
- Втрати на механічному з'єднанні типу SC/UPC-SC/UPC = 0,5 дБ.
- Загасання в стандартному одномодовому волокні на довжині хвилі 1310 = 0,36 дБ/км.

Максимальна протяжність оптичного каналу розраховується наступним чином.

- Оптичний бюджет потужності системи з використанням наведених вище SFP модулів становить – 9 дБм – (-22 дБм) = 13 дБ.
- Кількість механічних з'єднань SC/UPC-SC/UPC – 2 (з'єднання (3) на портах оптичної розподільної панелі (ODF) - рис. 2.8).
- Оптичний бюджет втрат з урахуванням механічних з'єднань 2х0,5 дБ= 1 дБ.
- Різниця між оптичним бюджетом системи і бюджетом втрат: 13 - 1 = 12 дБ.

- Стандартний запас оптичного бюджету (для урахування втрат на зварках волокна, втрат, пов’язаних з механічними навантаженнями на кабель, перегинами кабелю і т. і.; вибирається у діапазоні від 0 до 3 дБ): 3 дБ.
- Залишковий оптичний бюджет: 12 - 3 = 9 дБ.
- Сумарна довжина ОВ, яке «вписується» в залишковий оптичний бюджет (при загасання 0,36дБ / км на довжині хвилі 1310nm): 9 / 0,36 = 25 км. Тим не менш, виробник пропонує SFP модулі D-Link DEM-310GT для роботи на відстанях до 10 км.

Приклад 2. Пасивна оптична мережа (PON) з топологією «зірка» на одному розгалужувачі на 64 виходи (рис. 2.18).



OLT - Optical Line Terminal - оптичний термінал – центральний вузол PON мережі, Optical Networking Unit – оптичний мережний пристрій, PLC 1x64 – планарний Y-подібний розгалужувач оптичного сигналу на 64 виходи.

Рисунок 2.18 - Топологія «зірка» пасивної оптичної мережі

Для оцінки бюджету втрат будемо використовувати такі вихідні дані.

- Мінімальна вихідна потужність оптичного модуля на порту OLT = 4 дБм.
- Чутливість оптичного модуля на порту ONU = -26 дБм.
- Втрати на механічному з’єднанні типу SC/UPC-SC/UPC = 0,5 дБ.
- Втрати на оптичному розгалужувачі PLC 1x64 = - 21,5 дБ
- Загасання в стандартному одномодовому волокні на довжині хвилі 1310 = 0,36 дБ/км.

Максимальна протяжність оптичного каналу розраховується наступним чином.

- Оптичний бюджет потужності системи становить 4 дБм – (-26 дБм) = 30 дБ.
- Кількість механічних з’єднань SC/UPC-SC/UPC – 2 (1 з’єднання на порту оптичної розподільної панелі (ODF) зі сторони OLT, 1 з’єднання на виході розгалужувача в бік ONU - рис. 2.9).
- Оптичний бюджет втрат з урахуванням розгалужувача 1x64 та механічних з'єднань 21,5 дБ + 2x0,5 дБ= 22,5 дБ.
- Різниця між оптичним бюджетом системи і бюджетом втрат: 30 – 22,5 = 7,5 дБ.
- Стандартний запас оптичного бюджету (для урахування втрат на зварках волокна, втрат, пов’язаних з механічними навантаженнями на кабель, перегинами кабелю і т. і.; вибирається у діапазоні від 0 до 3 дБ): 3 дБ.
- Залишковий оптичний бюджет: 7,5 - 3 = 4,5 дБ.
- Сумарна довжина ОВ, яке «вписується» в залишковий оптичний бюджет (при загасання 0,36дБ / км на довжині хвилі 1310nm): 4,5 / 0,36 = 12, 5 км.

2.3. Необмежене середовище передачі

Необмежене середовище (бездротове) забезпечує передачу й прийом електромагнітних сигналів через зовнішній простір [О: 1, 3; Д: 2].

. Таке середовище передачі використовується в наступних комунікаційних системах:

- радіозв'язок;
- мікрохвильові системи передачі;
- лазерні системи передачі;
- інфрачервоні системи передачі.

Радіозв'язок

Найпоширенішими частотними діапазонами для систем передачі даних є: 136 – 174 МГц, 400 – 512 МГц, 820 – 960 МГц, 2,4 ГГц, 5 ГГц, 10 – 12 ГГц, 30 – 35 ГГц і вище.

Чим вище частота, тим вище швидкість передачі, менше дальність, вище вимоги до забезпечення прямої видимості й більше чутливість до зовнішніх факторів (погодні умови). Для частот більше 30 МГц іоносфера землі прозора для електромагнітних хвиль, отже, хвилі з такими частотами поширюються тільки в межах прямої видимості. Для частот менше 30 МГц хвилі відбиваються від іоносфери, і за рахунок множинних відбивань від іоносфери й Землі, можуть поширюватися на великі відстані без дотримання вимоги прямої видимості між приймачем і передавачем.

Електромагнітні хвилі в діапазоні менше 1 ГГц звичайно розглядаються як радіохвилі й поширюються відносно всенаправлено від передавальної антени.

Існує наступний розподіл радіодіапазону:

- середні частоти (MF): 535 – 1605 кГц (амплітудно-модульоване радіомовлення);
- високі частоти (HF): 3 – 30 МГц (короткохвильове радіомовлення). Цей діапазон використовується в деяких глобальних системах передачі даних зі швидкістю до 2,4 Кбіт/с;
- дуже високі частоти (VHF): 88 – 108 МГц - частотно-модульоване радіомовлення; 54 – 88, 108 – 174, 174 – 216 МГц – VHF телемовлення;
- ультрависокі частоти (UHF): 216 – 470 МГц, 470 – 890 МГц – кабельне телемовлення. Використовується в системах передачі даних зі швидкістю 100-400 Кбіт/с.

Мікрохвильові комунікації

Системи передачі, що використовують електромагнітні хвилі із частотою більше 1 ГГц, відносять до мікрохвильових. Мікрохвильова передача даних здійснюється у двох видах: наземна й супутникова.

Наземна мікрохвильова передача здійснюється між приймальною та передавальною антенами, розташованими на поверхні землі, дахах будинків і т.п., і використовується, в основному, для передачі телефонних потоків на

великі відстані та побудови систем передачі даних, коли прокладка кабельних систем ускладнена або потребує великих фінансових витрат.

Мікрохвильовий зв'язок підтримує високі швидкості передачі, однак, підвладний впливу погодних умов.

До таких систем належать наступні:

- радіорелейні системи передачі (використовують лінійку приймально-передавальних антен, які ретранслюють сигнал на великі відстані (до 30 км); швидкість передачі 2-20 Мбіт/с;
- Radio Ethernet і WiMAX: можуть використовувати частоти від 2,4 до 23 ГГц, швидкість передачі 2-52 Мбіт/с;
- HyperLAN: частоти 5, 15 – 15,25 ГГц; потужність передавача 1Вт; швидкість передачі до 25 Мбіт/с; частоти 17, 15 – 17,3 ГГц, потужність передавача 100 мВт; швидкість передачі 100-150 Мбіт/с;
- Bluetooth: частоти 2,4 – 2,48 ГГц, швидкість передачі до 723 Кб/с, відстань від 10 см при потужності передавача 1 мВт, до 100 м при потужності передавача 100 мВт.

Супутникові мікрохвильові комунікації

Використовуються мікрохвильові промені, спрямовані до супутника та від нього, що перебуває на геостаціонарній орбіті. Такий супутник робить оберт навколо Землі з такою ж швидкістю, з якою Земля обертається навколо своєї осі. У результаті, такий супутник з будь-якої точки на поверхні Землі здається нерухомим.

Висота розміщення супутника над поверхнею землі становить 36 000 км, час затримки проходження сигналу – 240 – 270 мс.

Зазвичай використовуються частоти 6/4 ГГц (38 Мбіт/с), 14/12 ГГц (48 Мбіт/с).

Різновидами супутникових систем є системи DirectPC і DVB (супутниковим або мікрохвильовим є тільки прийомний канал, для передачі даних необхідний окремий канал, зазвичай провідний). Існує також система NetSat Direct, що є повністю супутниковою.

Супутникові приймально-передавальні системи мають досить високу надійність, мають високий коефіцієнт готовності каналу, але робота таких систем підвладна впливу зовнішніх факторів.

Лазерні комунікації

У лазерних системах передачі використовується лазерне випромінювання ІЧ-діапазону, модульоване даними, що передаються. Зазвичай використовується два лазерних промені для організації дуплексного каналу передач. Система обмежена границями прямої видимості й чутлива до зовнішніх факторів. Зазвичай відстань між приймачем і передавачем у таких системах не перевищує 150 м; швидкість передачі до 155 Мбіт/с.

Інфрачервоні системи передачі

Системи інфрачервоної (ІЧ) комунікації використовують недорогі ІЧ приймачі й передавачі і застосовуються для передачі даних всередині одного приміщення. ІЧ промінь зазнає безліч відбиттів від стін і стелі й попадає в приймач. Для зменшення загасання можуть використовуватися відбивальні ковпаки. Радіус дії обмежується невеликими відстанями. Швидкість передачі даних становить 1-2 Мбіт/с.

Питання для самоперевірки та контролю засвоєння знань

1. Визначити, які параметри фізичного середовища передачі відносяться до первинних.
2. Визначити, які параметри фізичного середовища передачі відносяться до вторинних.
3. Визначити, до якого типу відноситься кабель «вита пара».
4. Визначити, для чого скручують проводи в парі кабелю «вита пара».
5. Визначити, який критерій покладено в основу розподілу кабелів «вита пара» на категорії.
6. Дати оцінку, чим конструктивно відрізняються кабелі «вита пара» різних категорій.

7. Визначити, який параметр кабелю покладено в основу розподілу кабелів по категоріям AWG.

8. Визначити, як змінюється діаметр токоведучого провідника зі збільшенням значення AWG.

9. Визначити, до якого типу відноситься коаксіальний кабель.

10. Визначити, який тип оптичного кабелю забезпечує передачу сигналу на більшу відстань.

11. Визначити, скільки типів хвиль оптичного випромінювання використовується при передачі сигналу через одномодовий кабель.

12. Визначити, скільки типів хвиль оптичного випромінювання використовується при передачі сигналу через багатомодовий кабель.

13. Визначити, в якому кабелі діаметр оптичного ядра сумірний з довжиною хвилі випромінювання.

14. Визначити, яке джерело оптичного випромінювання застосовується при передачі сигналу через одномодовий кабель.

15. Визначити, яке джерело оптичного випромінювання застосовується при передачі сигналу через багатомодовий кабель.

16. Визначити, випромінювання якого частотного діапазону відносять до мікрохвильового.

17. Визначити, випромінювання якого частотного діапазону не потребує забезпечення прямої видимості між приймачем та передавачем.

18. Визначити, випромінювання якого частотного діапазону потребує забезпечення прямої видимості між приймачем та передавачем.

3. ТОПОЛОГІЯ МЕРЕЖ

Топологія мережі описує фізичне розташування середовища передачі й підключених до нього вузлів [О: 1, 4; Д: 6].

Виділяють наступні типи топологій:

- зіркоподібна структура або «зірка»;
- кільцева структура або «кільце»;
- петльова структура або «петля»;
- шинна структура або «шина»;
- деревоподібна структура або «дерево»;
- повнозв’язана структура або «сітка»;
- гібридна структура.

Вибір тієї або іншої топології визначається призначенням мережі, вимогами по надійності, що пред’являються до неї, використовуваними в мережі технологіями доставки даних.

3.1 Зіркоподібна структура

У такій топології кожний вузол з'єднаний із центральним вузлом окремим фізичним каналом (рис. 3.1).

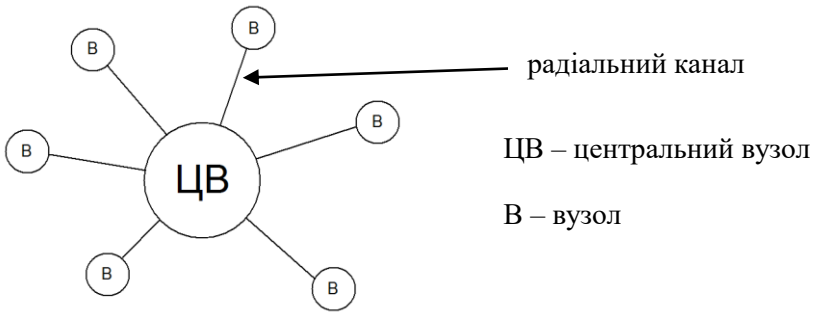


Рисунок 3.1 - Зіркоподібна топологія

Як центральні вузли можуть виступати наступні пристрої:

- концентратори,
- комутатори,
- мультиплексори (MUX),
- багатопортові повторювачі,
- маршрутизатори.

У такій топології дані, згенеровані одним вузлом, завжди будуть проходити через центральний вузол, піддаватися в ньому додатковій обробці (не у всіх системах) і перенаправлятися в один або більше радіальних каналів.

Різновидом такої топології є ***«гірлянда»*** (рис. 3.2) ***і «складна зірка»*** (рис. 3.3).

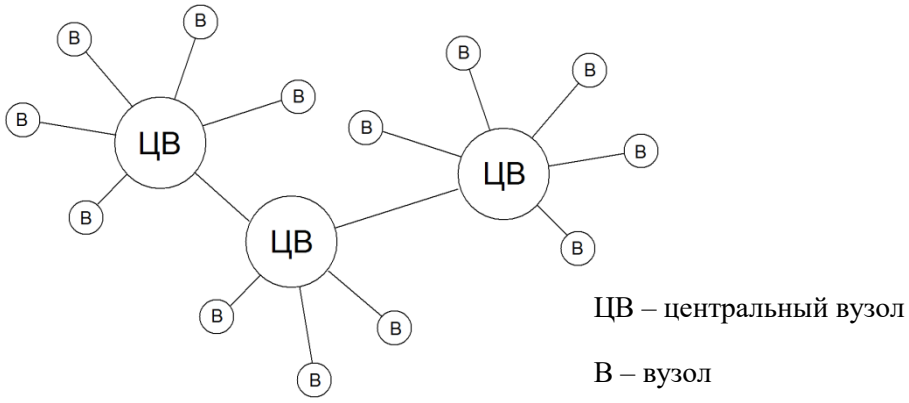


Рисунок 3.2 - Топологія «гірлянда»

Застосовується при необхідності збільшення довжини мережі, або кількості портів для підключення вузлів.

Центральні вузли в такій топології звичайно з'єднують між собою більше швидкісними каналами передачі з можливістю організації декількох маршрутів передачі даних між вузлами. Складна зірка застосовується для побудови магістралей у великих мережах.

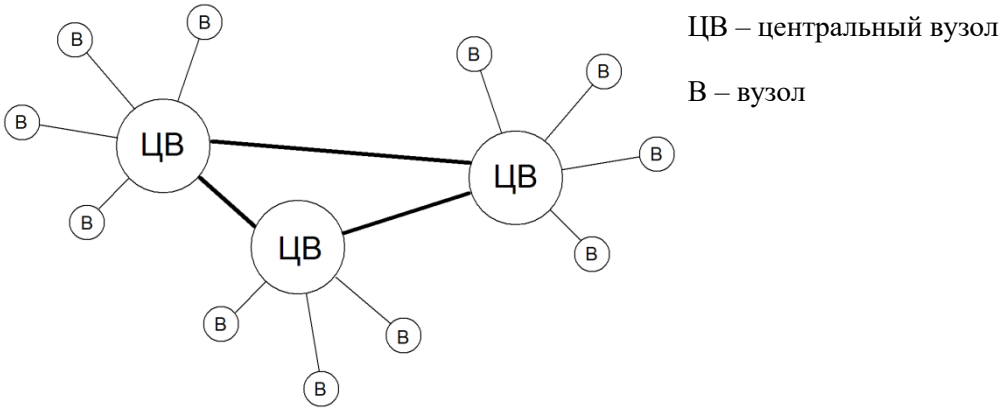


Рисунок 3.3 - Топологія «складна зірка»

Крім комутації каналів або пакетів, центральні вузли можуть виконувати додаткові функції узгодження швидкостей передачі й перетворення протоколів передачі. Програмне забезпечення центральних вузлів дозволяє реалізувати додаткові функції з контролю доступу й забезпеченню інформаційної безпеки.

У зіркоподібній топології досить легко здійснювати пошук несправностей і легко додавати нові вузли в мережу при наявності вільних портів.

Основний недолік даної топології – при виході з ладу центрального вузла вся мережа буде непрацездатною. Крім того, мають місце додаткові затримки, пов'язані з обробкою кадрів у центральних вузлах.

Зіркоподібна топологія є основною топологією в локальних мережах.

3.2. Кільцева мережа

Всі вузли підключені до загального кільцевого каналу (звичайно через проміжні пристрої – багатопортові повторювачі) (рис. 3.4). Повторювачі виконують функції регенерації сигналу, одержання й передачі даних з кільця і в кільце; забезпечують доступ до загального кільцевого каналу.

Передача даних по кільцю завжди виконуєьбся тільки в одному напрямку. Пакет, згенерований певним вузлом, надходить у загальний кільцевий канал і

проходить повний оберт по кільцю. При цьому вузол одержувач (адреса якого зазначена у пакеті) при одержанні пакета з кільця вичитує поле даних для передачі його вмісту протоколам верхніх рівнів для наступної обробки й відправляє пакет далі в кільце. Коли пакет досягає вузла відправника, останній повинен видалити його з кільця.

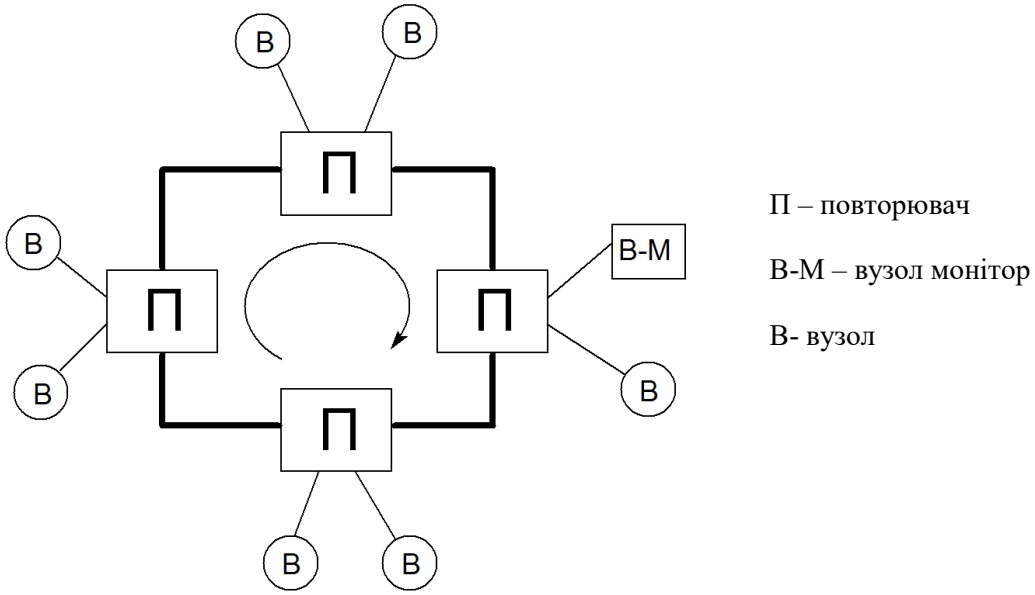


Рисунок 3.4 - Кільцева топологія

Вузол-монітор використовується не завжди. Звичайно він служить для видалення з кільця спотворених пакетів, які не може розпізнати вузол-відправник, або пакетів, відправлених вузлом, що вже припинив свою роботу. Крім цього, вузол-монітор запускає кільце в роботу, виконує функції по тестуванню кільця й обробляє різні помилкові ситуації. Деякі способи організації кілець вимагають спеціального управління, що виконується вузлом-монітором.

Для підключення нових вузлів у кільце використовуються спеціальні з'єднувачі на повторювачах, що забезпечують швидке підключення до повторювача без зупинки роботи мережі. Таке підключення вносить слабку заваду в передачу даних, а процедури обробки помилок дозволяють

продовжити функціонування кільця. Зупинка мережі може знадобитися у випадку збільшення кільця за допомогою нових сегментів і повторювачів.

Використання тільки одного напрямку передачі даних дозволяє спростити протоколи передачі. У мережах з кільцевою топологією досить просто здійснюється маршрутизація й легко реалізуються пріоритетні схеми. Як середовище передачі можуть бути використані всі типи кабелів (КК, ВП, ВОК). Така топологія застосовується в мережах стандарту 802.5 («маркерне кільце»), у попереднику цього стандарту - мережі IBM Token Ring, а також, у мережах FDDI.

Одним із критичних питань при використанні кільцевої топології є надійність роботи мережі. Для підвищення надійності використовують два підходи.

1. Подвійне кільце (застосовується в мережах FDDI) (рис. 3.5).

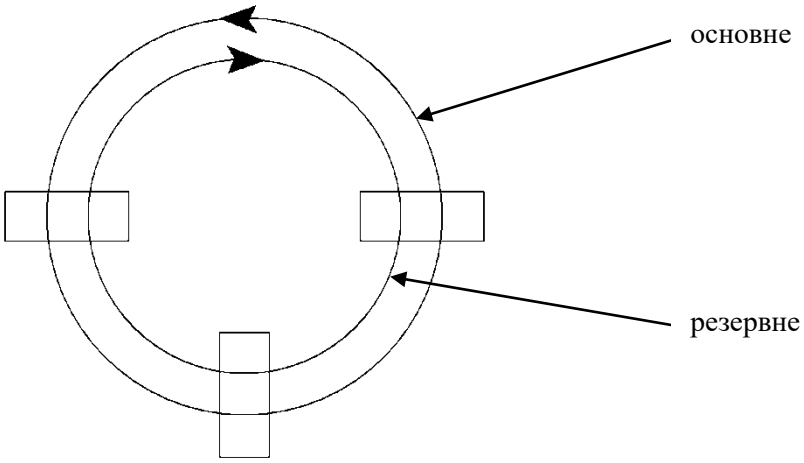


Рисунок 3.5 - Топологія «подвійне кільце»

У звичайному режимі роботи для передачі даних використовується тільки основне кільце, сегменти резервного кільця підключаються до основного тільки при виході з ладу якого-небудь сегмента основного кільця або проміжного концентратора. Протилежні напрямки передачі даних в основному й

резервному кільці дозволяють у цьому випадку легко відновити кільцеву топологію.

2. Використання обхідних шляхів (рис. 3.6).

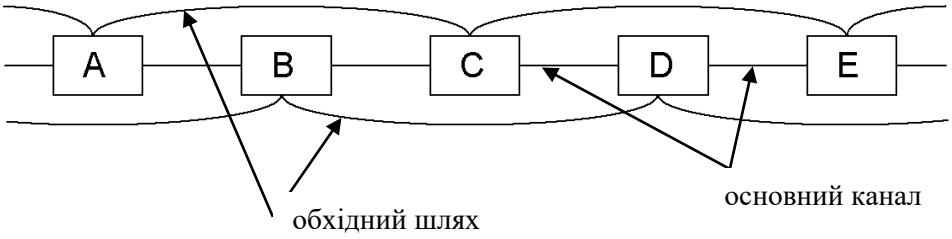


Рисунок 3.6 - Використання обхідних шляхів

Якщо виходить із ладу повторювач С або один з каналів (B-C або C-D), то, вручну або автоматично, підключається обхідний каналу (B-D). Це спосіб має обмеження – якщо несправні два або більше суміжні повторювачі, то мережа працювати не буде.

3.3. Петльова мережа

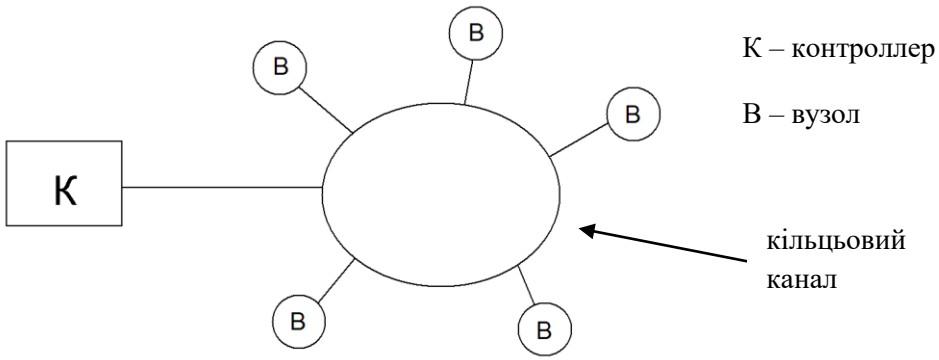


Рисунок 3.7 - Петльова топологія

Всі вузли приєднані до кільцевого каналу й один з вузлів (контролер) виконує керуючі функції й реалізує протокол передачі даних (рис. 3.7). Він або проводить циклічне опитування вузлів на наявність даних для передачі, або

посилає спеціальний пакет у кільцевий канал. Така топологія використовується для підключення низькошвидкісних пристроїв (наприклад, у багатотермінальних комплексах). Так як керування мережею реалізовано в одному місці (на контролері), легко реалізовувати пріоритетні схеми. Повторювачі в таких мережах використовуються рідко, тому що доступ до загального каналу контролюється централізовано контролером. Петльові мережі зазвичай короткі, а швидкість передачі досить низька.

3.4. Шинна топологія

Шинна топологія являє собою лінійне середовище передачі, до якого підключаються вузли за допомогою відносно коротких з'єднувачів. Дані від вузлів відправляються в обидва боки по загальному шинному каналу. Для запобігання відбиття сигналів від кінців шини, шина термінується з обох кінців пристроями, що поглинають сигнал - термінаторами. Термінатори являють собою узгоджувальне навантаження, хвильовий опір якого дорівнює хвильовому опору кабелю. Як середовище передачі використовується тонкий або товстий коаксіальний кабель. Середовище передачі повністю пасивне. На шляху проходження сигналу відсутні будь-які активні пристрої (сигнал не піддається якій-небудь обробці).

Приєднання вузлів до кабельного сегмента можуть бути виконані за допомогою Т-конекторів («тонкий» коаксіальний кабель), або за допомогою зовнішніх приймачів-передавачів («тонкий» і «товстий» коаксіальний кабель) (рис. 3.8). Такі урізання в кабель завжди вносять погрішності в електричні характеристики кабельного каналу, тому існує обмеження на максимальну кількість урізань на кабельному сегменті й мінімальна відстань між ними.

Така топологія має відносно низьку надійність. У шинних мережах пошук несправностей є досить трудомістким процесом.

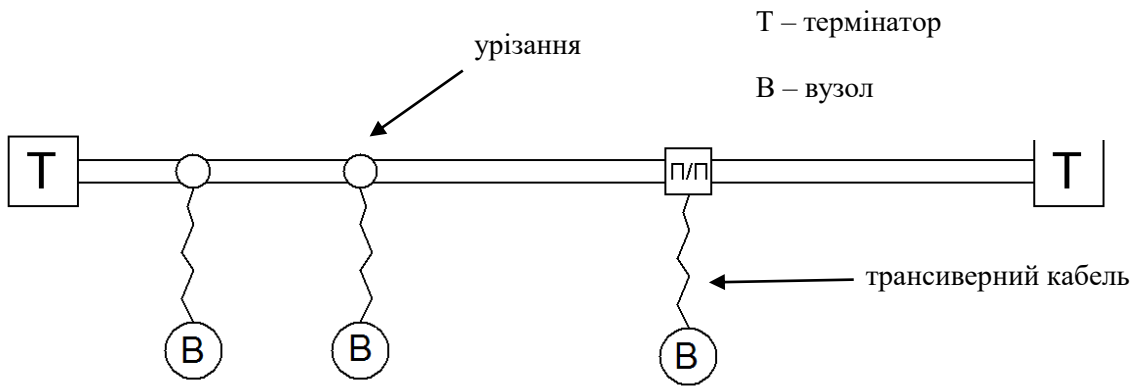


Рисунок 3.8 - Шинна топологія

3.5. Деревоподібна топологія

Являє собою кілька шин, з'єднаних між собою. При цьому одна із шин основна (магістральна), до якої підключені бічні шини.

Є два варіанти підключення бічних шин: через пасивні розгалужувачі (рис. 3.9) і через активні розгалужувачі (рис. 3.10).

Основним недоліком таких топологій є те, що сигнал через магістральну й бічні шини буде проходити з різною швидкістю й по-різному відбиватися від країв за рахунок розходжень електричних характеристик шин. Це приводить до додаткових помилок передачі й, у результаті, пропускна здатність таких мереж буде менше, ніж у звичайної шини.

Є ще один варіант побудови деревоподібної мережі, що застосовується у мережах Ethernet на коаксіальному кабелі. Одна шина тут буде магістральною, до якої підключаються звичайні вузли й, через проміжні повторювачі, бічні шини. Додаткове підключення шин до бічних шин не допускається (рис. 3.11).

У такій структурі існує обмеження на максимальну кількість повторювачів на шляху проходження сигналу від вузла до вузла (пов'язане із затримкою проходження сигналу через кабельні сегменти й проміжні повторювачі).

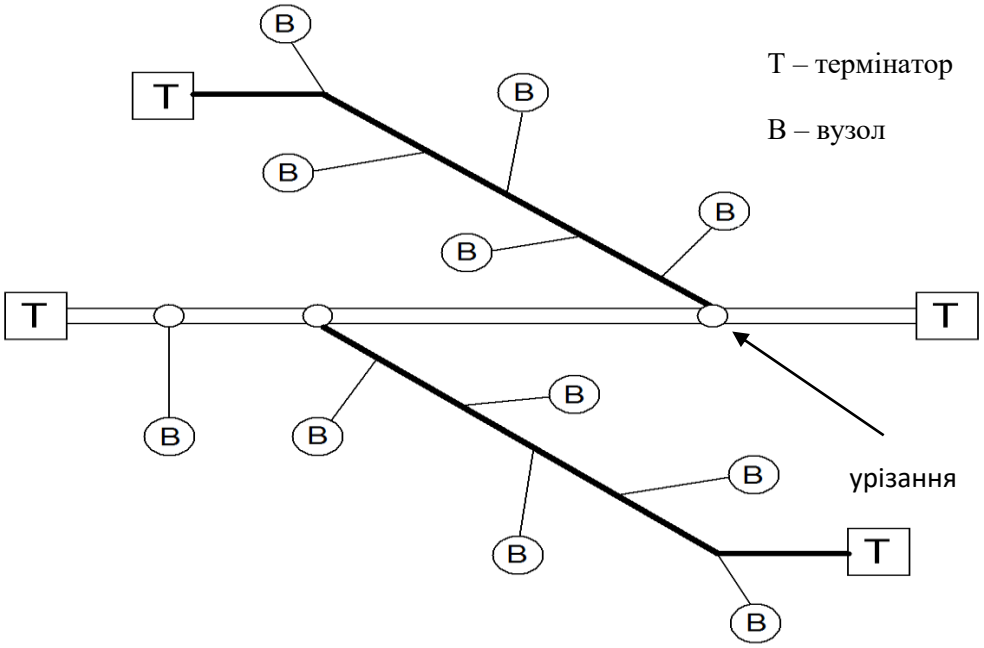


Рисунок 3.9 - Підключення бічних шин через пасивні розгалужувачі

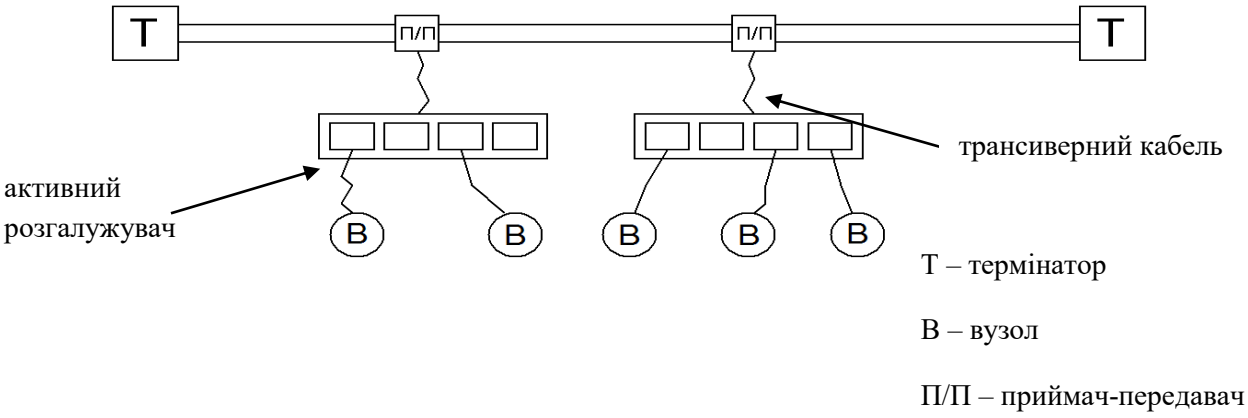


Рисунок 3.10 - Підключення бічних шин через активні розгалужувачі

У порівнянні зі звичайною шинною топологією дана топологія має більш високу надійність – відмова бічного сегмента не приводить до зупинки роботи всієї мережі.

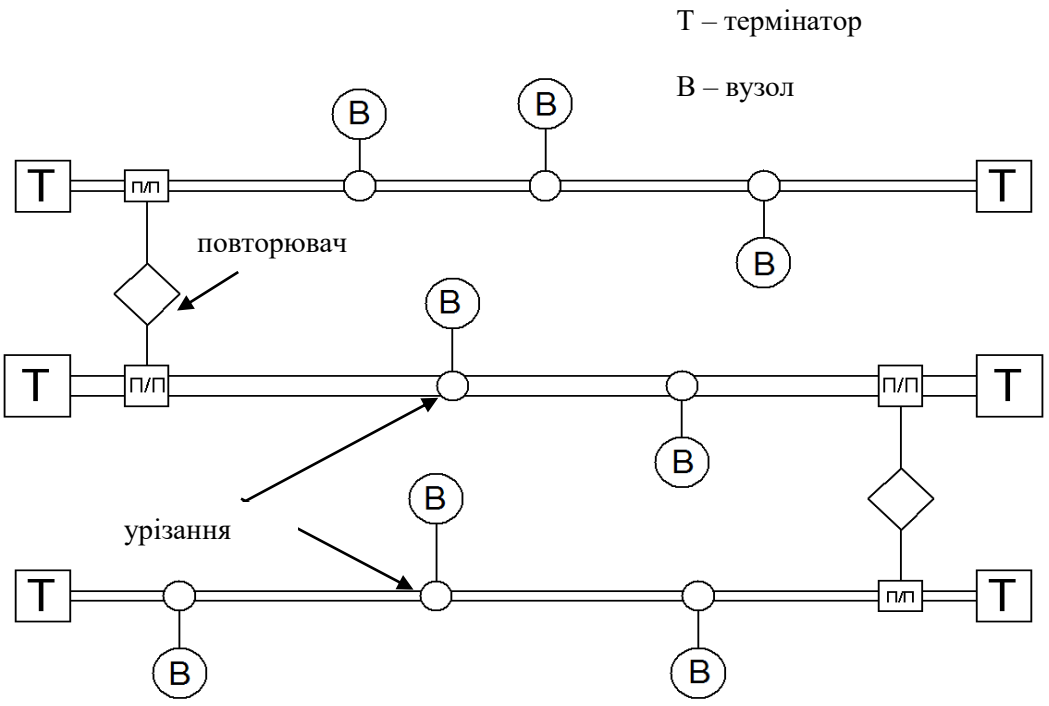


Рисунок 3.11 - Хребетно-реберна топологія

3.6. Повнозв’язана структура (сітка)

Кожний вузол з'єднаний окремим фізичним каналом з будь-яким іншим вузлом мережі. У результаті, кожний вузол повинен мати безліч інтерфейсів для підключення до всіх ліній зв'язку (рис. 3.12).

Дана топологія має найвищу надійність і дозволяє організовувати безліч маршрутів передачі даних. Зазвичай, у ролі вузлів виступають такі пристрої, як комутатори й маршрутизатори.

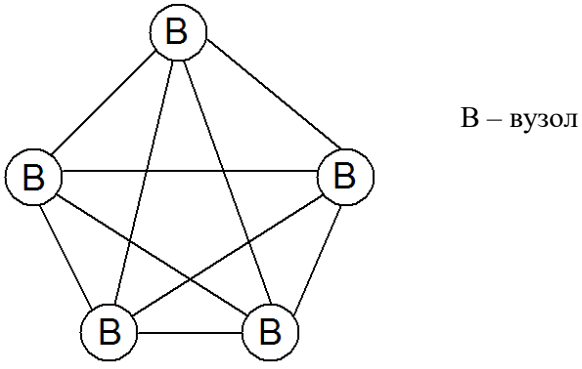


Рисунок 3.12 - Топологія «сітка»

Недоліком топології є висока надлишковість інтерфейсів на вузлах і каналів передачі, ефективність використання яких є досить низкою у випадку, коли вузли не дуже інтенсивно обмінюються даними. У чистому вигляді ця топологія не використовується. Зазвичай організовується кілька фізичних каналів, які з'єднують найбільш критичні вузли.

3.7. Гібридна структура

Являє собою сполучення різних топологій і зазвичай застосовується в глобальних або територіально-розподілених мережах. У цьому випадку до магістралі, побудованої з використанням однієї з топологій (складна зірка, шина, сітка, кільце) приєднуються периферійні сегменти мережі, у яких використовуються топології кільце або зірка.

Питання для самоперевірки та контролю засвоєння знань

1. Визначити, що описує топологія мережі?
2. Які виділяють основні види топологій мереж?
3. Визначити, яка з топологій передбачає наявність центрального керуючого вузла
4. Визначити, в якій з топологій усі вузли безпосередньо з’єднані з центральним вузлом.
5. Наведіть приклади пристроїв, які можуть виступати у якості центральних вузлів в зіркоподібній топології.
6. Які функції може виконувати центральний вузол в зіркоподібній топології?
7. Для вирішення яких задач використовують топологію «складна зірка»?
8. Визначити, яка з топологій передбачає передачу даних від вузла тільки в одному напрямку по загальному каналу.

9. За допомогою яких пристроїв підключаються вузли до загального кільцевого каналу?

10. Наведіть основну відмінність петльової топології від кільцевої.

11. Визначити, яка з топологій передбачає передачу даних по каналу в усі сторони від вузла.

12. Визначити, які методи збільшення надійності застосовують у кільцевій топології.

13. Визначити, для чого термінують кінці шини.

14. Які існують варіанти підключення вузлів до загального шинного каналу?

15. Що характерно для деревоподібних топологій?

16. Які існують варіанти підключення бокових шин у деревоподібних топологіях?

17. Який основний недолік деревоподібних топологій?

18. Що являє собою хребетно-реберна топологія?

19. За рахунок чого збільшена надійність у хребетно-реберній топології у порівнянні з деревоподібною?

20. Що характерно для топології «сітка»?

3. МЕРЕЖНА АРХІТЕКТУРА

Під архітектурою розуміється концепція обчислювальної системи зв'язку, що визначає її функції, інтерфейси та процедури [О: 1, 3; Д: 7, 8].

Виходячи з принципів організації мережних ресурсів, можна виділити два базові різновиди мережних архітектур:

- однорангові, або рівнорангові мережі;
- мережі типу клієнт-сервер.

Рівнорангова мережа (Peer – to – Peer)

Всі вузли мережі являються рівноправними, виконують однакові функції по керуванню доступом до мережі та мережним ресурсам. Загальні мережні ресурси розподіляються між вузлами в мережі; всі мережні додатки виконуються на локальних вузлах. Прикладом таких мереж виступає "робоча група", побудована на Windows-системах.

Мережа клієнт-сервер

Складається з множини робочих станцій (клієнтів), що обмінюються інформацією з обмеженою кількістю вузлів, називаних серверами. Під сервером розуміють вузол, які-небудь ресурси якого виділені в загальне використання з організацією єдиного централізованого доступу до цих ресурсів (файл-сервер, принт-сервер, сервер додатків и т.п.). В такій архітектурі всі загальні мережні ресурси зосереджені на серверах. Всі мережні додатки в клієнт-серверній архітектурі мають наступну особливість: одна частина процесу обробки інформації виконується на клієнті, інша – на сервері. Прикладом такої архітектури являється домен Windows.

4.1. Модель мережної архітектури

Теоретичну основу функціонування будь-яких інформаційних систем утворює еталонна модель взаємодії відкритих систем OSI/ISO (міжнародний стандарт ISO 7498 (1977 р.)) [О: 1, 2, 3; Д: 7, 8].

Модель OSI визначає рівні мережної архітектури і процедури взаємодії в інформаційних системах. Основа ідея моделі полягає в тому, що весь процес взаємодії розбивається на окремі рівні, кожен з яких виконує визначенні функції і взаємодіє з сусідніми рівнями через міжрівневі інтерфейси. Функції рівнів можуть реалізовуватись програмними, апаратними або апаратно-програмними засобами.

Основні задачі, що вирішуються моделлю, наступні:

- стандартизація обміну даними між системами;
- усунення будь-яких технічних перешкод для зв’язку систем;
- визначення точок взаємодії для обміну даними між системами;
- забезпечення розумної можливості відходження від стандартів, якщо вони не задовольняють всім вимогам конкретних систем.

Модель складається з семи рівнів, кожен з яких для виконання своїх функцій використовує послуги рівнів, що розташовані нижче і надає визначений набір послуг вищерозташованим рівням.

В моделі OSI визначені два механізми взаємодії систем:

- горизонтальна модель – орієнтована на протоколи. Слугує для опису взаємодії між програмами або процесами на різних кінцевих системах або вузлах, розташованих на одному рівні моделі;
- вертикальна модель – орієнтована на додатки. Слугує для опису взаємодій між рівнями всередині однієї кінцевої системи або вузла. В цьому випадку взаємодія відбувається за допомогою інтерфейсів прикладних програм, що визначають функціональний склад

кожного рівня і забезпечують механізми використання окремих функцій.

Структура моделі OSI має наступний вигляд (рис. 4.1).

Рисунок 4.1 - Структура моделі OSI

1. Прикладний рівень – містить прикладні процеси, служби, протоколи, що забезпечують обробку інформації. Забезпечує безпосередній обмін інформацією між кінцевими додатками, користувачами і вузлами. На цьому рівні існує кілька типів протоколів. Це протоколи для конкретних специфічних додатків і загальні протоколи для підтримки користувачів і мережі (керування доступом, перевірка повноважень користувачів і комп'ютерів і т.п.). Прикладами протоколів даного рівня являються протоколи FTP, SMTP, POP3, NNTP та інші зі стеку TCP/IP.
2. Представницький рівень – виконує функції перетворення синтаксису та форматів даних, а також шифрування і дешифрування даних в процесі їх проходження по мережі. Основна задача рівня – забезпечити незалежність прикладних процесів від форматів і синтаксисів даних, що передаються. Наприклад, на цьому рівні реалізовані різноманітні системи кодування, додаткові процедури шифрування/дешифрування даних.
3. Сеансовий рівень – визначає механізми встановлення, підтримки і завершення сеансу зв'язку між додатками або процесами на різних кінцевих

системах. На цьому рівні визначається структура керування взаємодією, початок і кінець завдань, тривалість і режим ведення сеансу зв'язку, відновлення сеансу зв'язку без втрати даних в випадку будь-яких збоїв. Прикладом виступають різноманітні механізми обміну даними (з використанням іменованих каналів, через виклик віддалених процедур, через сокети і т.п.). Інформаційний об'єкт сеансового рівня, що включає дані верхніх рівнів, зазвичай називають повідомленням.

4. Транспортний рівень – забезпечує стійкий до збоїв механізм передачі даних між кінцевими вузлами. На цьому рівні здійснюється збірка і розбірка повідомлень сеансового рівня, формування пакетів, доставка даних від системи-відправника до системи-отримувача. Прикладами протоколів цього рівня являються протоколи TCP і UDP зі стеку протоколів TCP/IP і протокол NetBEUI зі стеку NetBEUI/NetBios. Інформаційний об'єкт транспортного рівня називають пакетом.
5. Мережний рівень – виконує функції адресації, формування і розформування пакетів даних, організації і підтримки віртуальних з'єднань, маршрутизації пакетів даних. Прикладом протоколів мережного рівня виступає протокол IPX зі теку протоколів IPX/SPX, протокол IP зі стеку TCP/IP, протокол NetBEUI зі стеку NetBEUI/NetBios, різноманітні протоколи маршрутизації (RIP, OSPF і т.д.). На цьому рівні працюють такі апаратно-програмні засоби, як маршрутизатори і комутатори третього рівня. Інформаційний об'єкт мережного рівня називають пакетом.
6. Канальний рівень – визначає протокол керування каналом передачі даних. Інформаційний об'єкт канального рівня називають кадром. На цьому рівні вирішуються задачі встановлення, підтримки і роз'єднання каналу передачі даних, керування потоком кадрів канального рівня через канал передачі, а також виявлення помилок передачі, пов'язаних з фізичним рівнем. Прикладом протоколів канального рівня є протокол стандарту 802.3 – МДКН/ВК (множинний доступ з контролем несучої та виявленням колізії),

або протокол Ethernet. На цьому рівні працюють такі апаратні засоби, як мережні адаптери, комутатори.

7. Фізичний рівень – забезпечує механічні, електричні, функціональні та процедурні засоби підключення до фізичної середи передачі і передачу даних через фізичну середу у вигляді електричних або оптичних сигналів. Прикладами специфікацій фізичного рівня виступають специфікації мережі Ethernet 10Base-2, 10Base-T, 100Base-TX, 100Base-FX, 1000Base-SX, 1000Base-LX і т.п.

При проходженні одиниці даних між рівнями, до них на кожному рівні додається у вигляді заголовка і кінцевика протокольна керуюча інформація (ПКІ). Обмін даними між логічними об'єктами одного і того ж рівня різних систем (горизонтальна взаємодія) здійснюється у вигляді протокольних блоків даних (ПБД), а між логічними об'єктами суміжних рівнів (вертикальна взаємодія) – у вигляді сервісних блоків даних (СБД). Один СБД може передаватися між логічними об'єктами у вигляді одного або декількох інтерфейсних блоків даних (ІБД). В цьому випадку ІБД складається з ПКІ і СБД або його частини.

Інтерфейси між рівнями представляються у вигляді послуг, які один рівень надає іншому. Залучення послуг нижнього суміжного рівня здійснюється за допомогою службових примітивів, якими обмінюються рівні через інтерфейс між ними. Ці примітиви носять абстрактний характер (не залежать від реалізації і не визначають її) і слугують для опису взаємодій між користувачем послуги і постачальником.

В рамках моделі визначено чотири типи службових примітивів:

- "Запит" – видається користувачем послуги для запуску якої-небудь процедури.
- "Індикація" – видається постачальником послуги для вказування про запуск процедури.
- "Відповідь" – видається користувачем послуги для вказування про завершення процедури, що запитувалась.

– "Підтвердження" – видається постачальником послуги для повідомлення про завершення процедури, що запитувалась.

Належить відзначити, що не всі послуги потребують використання всіх чотирьох типів примітивів.

4.2. Способи організації обміну даними

Існує два базових підходи до організації обміну даними між кінцевими системами:

– обмін даними з встановленням логічного з'єднання;

– обмін даними без встановлення логічного з'єднання.

Орієнтована на з'єднання модель має вигляд, представлений на рис. 4.2.

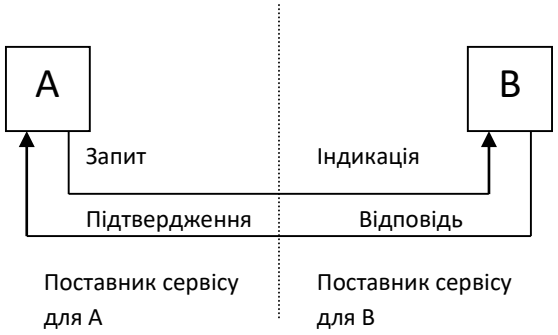


Рисунок 4.2 - Модель взаємодії з встановленням з'єднання

При цьому способі обміну даними встановлюється логічне з'єднання між кінцевими системами, перед безпосередньою передачею даних. Запит, що видається вузлом А, проходить через постачальника сервісу (прикладом якого може слугувати локальна мережа) і приймається у вузлі В як індикація. Якщо вузол В готовий до прийому, видається підтвердження встановлення логічного з'єднання. По цьому логічному з'єднанні ведеться передача даних. По завершенні передачі відправляється підтвердження прийому даних.

Діаграма обміну пакетами має наступний вигляд (рис. 4.3).

Передача в режимі встановлення логічного з'єднання потребує згоди між трьома сторонами (вузлами А і В і постачальником сервісу).

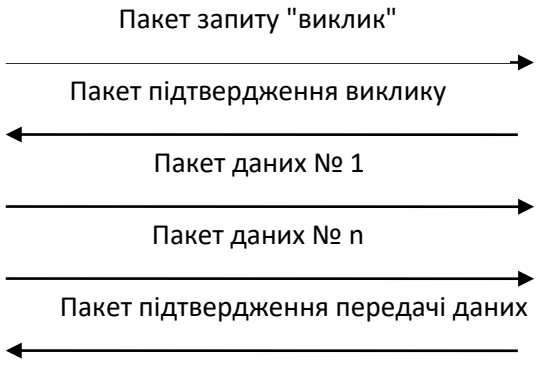


Рисунок 4.3 - Діаграма обміну пакетами

Не всі мережні додатки виконують функцію підтримання цілісності потоку даних, яку забезпечує орієнтована на встановлення з'єднання модель. Крім того, для високошвидкісних додатків можуть стати критичними додаткові накладні витрати, пов'язані з встановленням з'єднання і підтвердженнями доставки даних. Для таких додатків використовують обмін даними без встановлення з'єднання, або дейтаграмний режим.

Дейтаграмний (датаграмний) режим

При використання такого методу передачі даних кожний пакет розглядається як незалежний інформаційний об'єкт і має адресну інформацію, необхідну для його доставки адресату та вивільнює систему від попереднього обміну службовою інформацією між передаючим та приймаючим вузлами.

У даному випадку присутня згода між двома сторонами: А і В, або А і постачальником сервісу (рис. 4.4). У варіантах а) і б) постачальник сервісу знає про з'єднання; у варіанті в) у постачальника відсутня інформація про з'єднання між А і В. Як тільки здійснилась передача інформації між А і В та постачальником сервісу, в подальшому буде відсутня передача будь-якої

службової інформації між постачальником сервісу та прикладними рівнями на кінцевих системах відносно долі чи місцезнаходження відправлених даних.

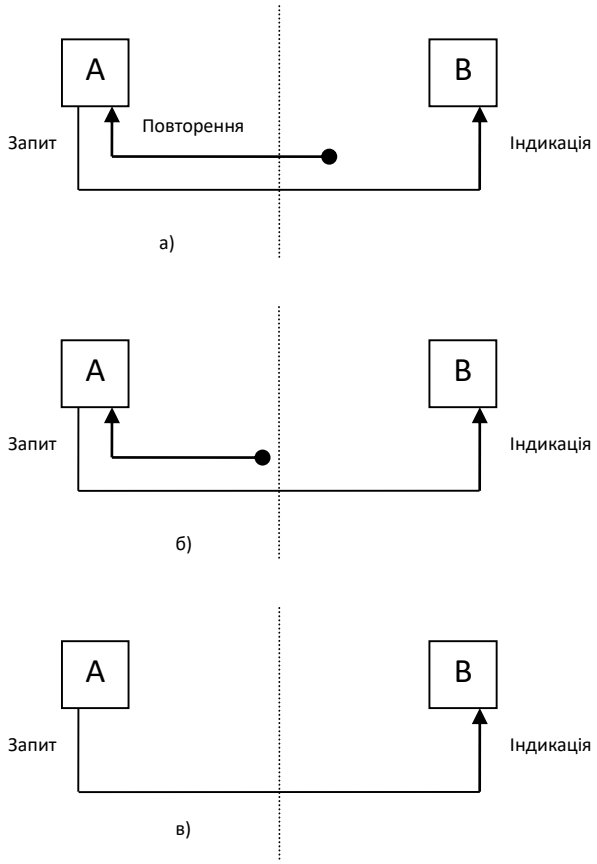


Рисунок 4.4 - Модель взаємодії у дейтаграмному режимі

В даному випадку постачальник сервісу є пасивним засобом передачі між вузлами А і В. Тобто, в даному методі відсутні будь-які підтвердження про доставку даних и засоби обробки можливих помилкових ситуацій.

Виходячи з двох розглянутих режимів обміну даних, розрізняють мережі, що забезпечують сервіс без встановлення логічного з'єднання (тип 1) і зі встановленням логічного з'єднання (тип 2).

4.3. Методи доступу і управління каналом передачі даних

Дані методи визначають доступ вузлів до загального каналу передачі і керування потоком кадрів в каналі і реалізуються у вигляді протоколів канального рівня (апаратна реалізація в мережних адаптерах і мережних пристроях канального рівня) [О: 1; Д: 7, 8].

За імовірнісною ознакою (імовірність доставки даних) методи діляться на два класи:

- **детерміновані методи** – доступ до загального каналу передачі даних розподіляється між усіма підключеними до каналу вузлами за допомогою спеціальних механізмів. Дані механізми гарантують передачу даних від кожного вузла на протязі визначеного часового інтервалу, якій може бути завчасно підрахований (прикладом є методи опиту та маркерні методи);
- **недетерміновані (стохастичні або імовірнісні) методи** – всі вузли конкурують за доступ до загального каналу передачі. У випадку неможливості захоплення каналу вузли генерують випадкові інтервали очікування, після чого роблять чергову спробу захопити канал. В результаті неможливо наперед визначити час, на протязі якого вузол зможе здійснити передачу. Існує ненульова ймовірність того, що вузол взагалі не зможе провести передачу даних. Прикладом виступає метод множинного доступу з контролем несучої і виявленням колізії (МДКН/ВК) або протокол Ethernet.

Одна з можливих класифікацій методів доступу має вигляд, представлений на рис. 4.5.

Одним з найбільш розповсюджених підходів до керування каналом передачі є метод первинний/вторинний або головний/підлеглий. В методах цього класу один з вузлів є головним, він керує доступом інших вузлів до каналу передачі і визначає, коли вторинні вузли можуть виконувати передачу

даних в загальний канал. Системи типу первинний/вторинний можуть бути реалізовані на основі наступних методів.

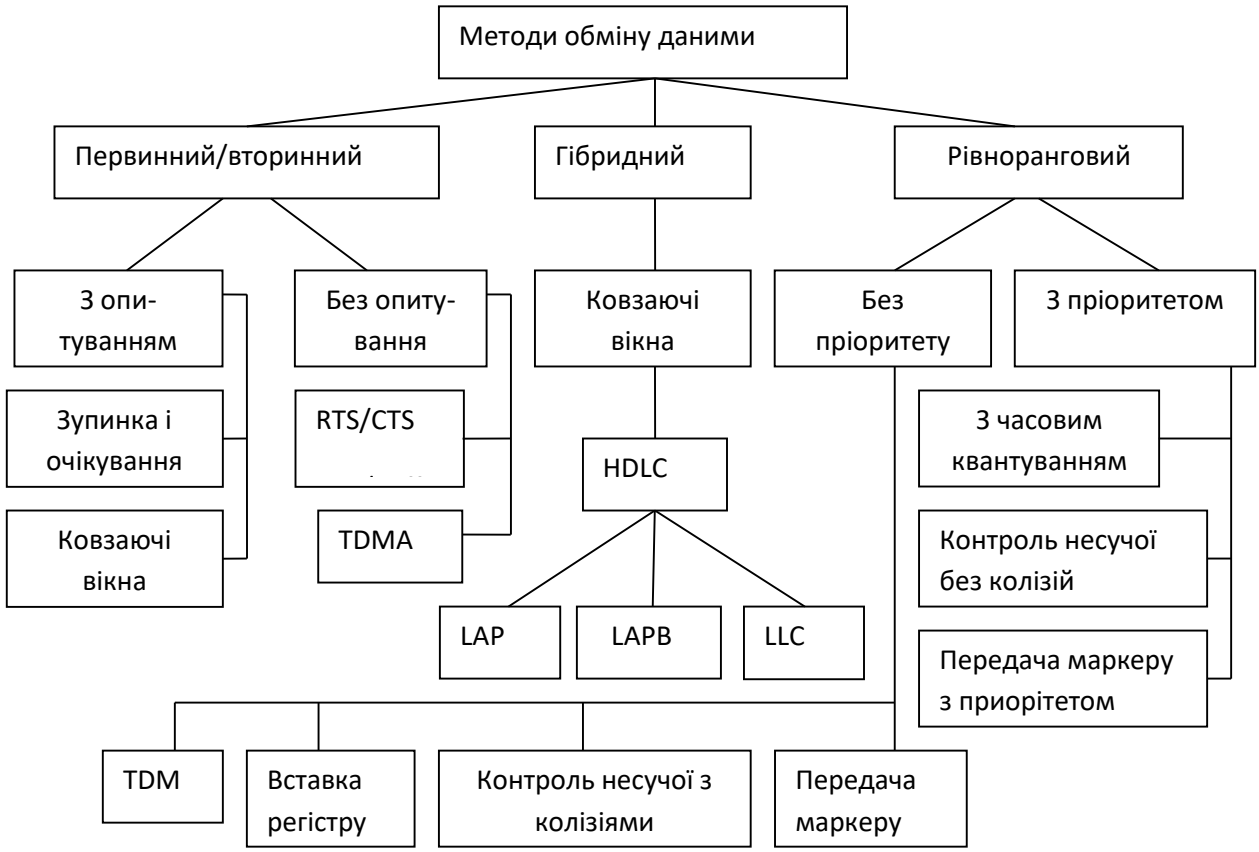


Рисунок 4.5 - Класифікація методів доступу до каналу передачі

4.3.1. Система опиту/вибору

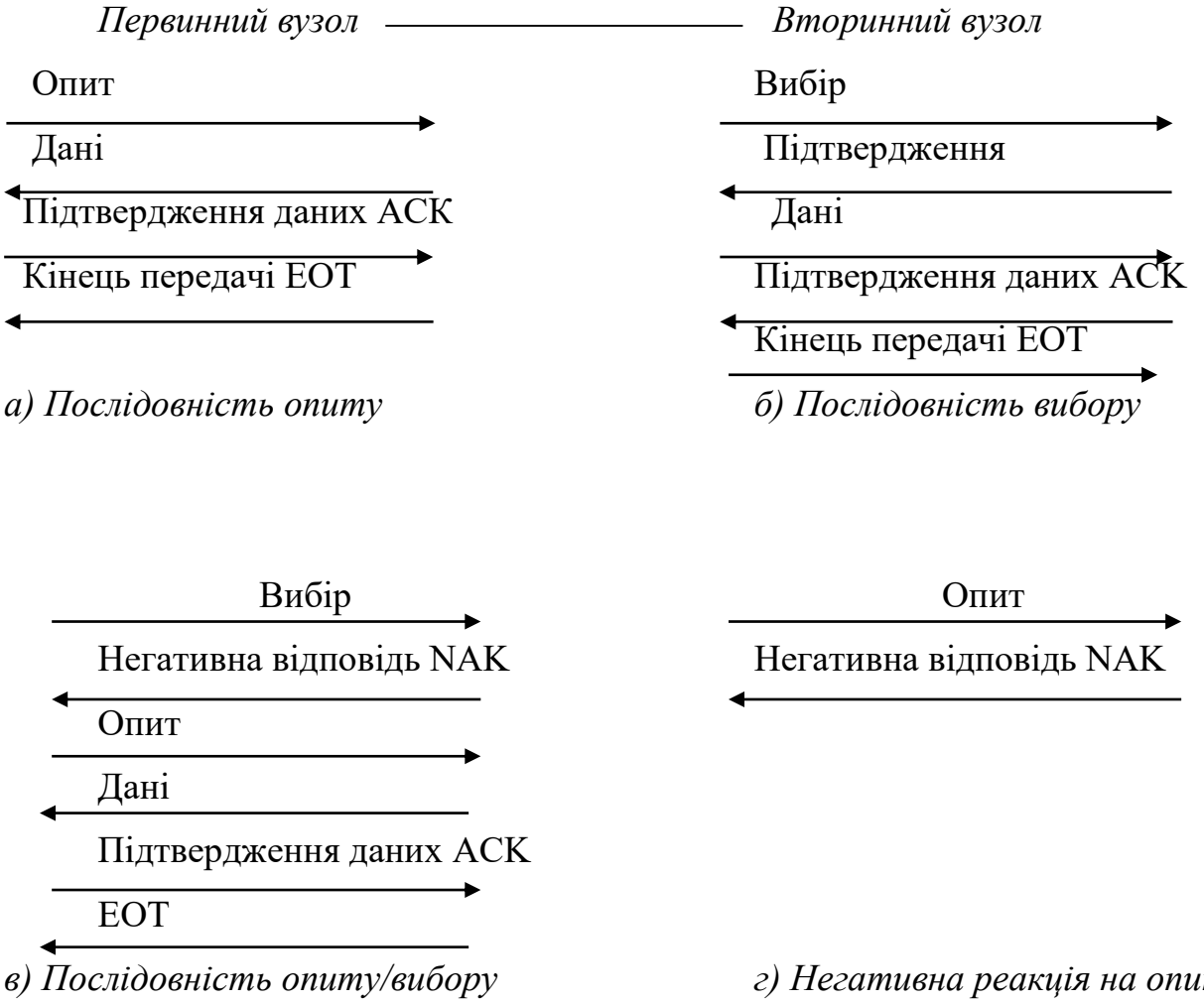
Спрощена структура такої системи має наступний вигляд (рис. 4.6).

Системи опиту/вибору будуються на основі двох команд "опит" і "вибір". Призначення команди "опит"полягає в передачі даних з вторинного вузла на первинний вузол. Призначення команди "вибір" – передача даних з первинного вузла на вторинний вузол.

Розглянемо, як це робиться за допомогою процедури опиту (рис. 4.6 а).

Первинний вузол надсилає запит, і, якщо у вторинному вузлі є дані для передачі, вони передаються в первинний вузол. Первинний вузол здійснює

контроль помилок передачі і надсилається позитивне підтвердження (АСК) у випадку відсутності помилок, або негативне підтвердження (NAK) при їх наявності.



а) Послідовність опиту

б) Послідовність вибору

в) Послідовність опиту/вибору

г) Негативна реакція на опит

Рисунок 4.6 - Структура системи опиту/вибору

Ці два випадки (передача даних і підтвердження) можуть траплятися декілька разів, поки у вторинного вузла не закінчаться дані для передачі. В цьому випадку вторинний вузол надсилає повідомлення про закінчення передачі (може бути спеціальний код кінця передачі (ЕОТ) або деякий службовий біт в керуючому полі останнього кадру).

Процедура вибору пояснюється на рис. 4.6 б. Вибір означає, що наявні дані для вторинного вузла. Підтвердження АСК у відповідь на вибір означає

готовність вторинного вузла до прийму даних. Первинний вузол передає дані на вторинний вузол, де виконується контроль помилок і видається підтвердження прийому. По закінченні передачі первинний вузол надсилає керуюче повідомлення EOT.

На рис. 4.6 в представлена послідовність опиту/вибору. На команду вибору вторинний вузол видає негативне підтвердження NAK. Це може бути пов'язано з тим, що вузол зайнятий виконанням інших задач, місце в буфері зайняте своїми даними, підготовленими для передачі. Для обробки вказаної ситуації первинний вузол надсилає команду "опит", щоб вторинний вузол передав дані і звільнив місце в буфері для прийому даних.

Послідовність на рис. 4.6 г показує, що відбувається в мережі, коли виконується опит вторинного вузла, у якого нема даних для передачі.

Основним недоліком системи опиту/вибору є наявність неодноразових негативних відповідних реакцій на команду "опит", що відображається на ефективності використання каналу передачі. Для зменшення додаткових витрат, пов'язаних з опитом можуть використовуватись динамічні таблиці опиту/вибору з пріоритетними схемами. Якщо на декілька опитів вузол видає негативне підтвердження його пріоритет в таблиці опитів знижується, і він буде опитуватись з меншою інтенсивністю.

Система опиту/вибору, що використовується для керування передачею даних між множиною вузлів на загальному каналі, має наступний вигляд (рис. 4.7).

Нехай вузол В хоче передати дані у вузол А. Для цього необхідно, щоб первинний вузол опитав вузол В (подія 1). Після цього вузол В виконує передачу даних у первинний вузол (2). Первинний вузол виконує контроль помилок передачі і видає підтвердження даних (3). По закінченню передачі вузол В видає код кінця передачі (4).

Після цього первинний вузол генерує вибір вузла А (5). Якщо А готовий до прийому, він видає підтвердження вибору (6), і первинний вузол виконує передачу даних у вузол А (7). Дані, що передаються в події (7), являються

точною копією даних, переданих в події (2). Вузол А виконує контроль помилок передачі і видає підтвердження даних (8), завершуючи квитування проходження даних.

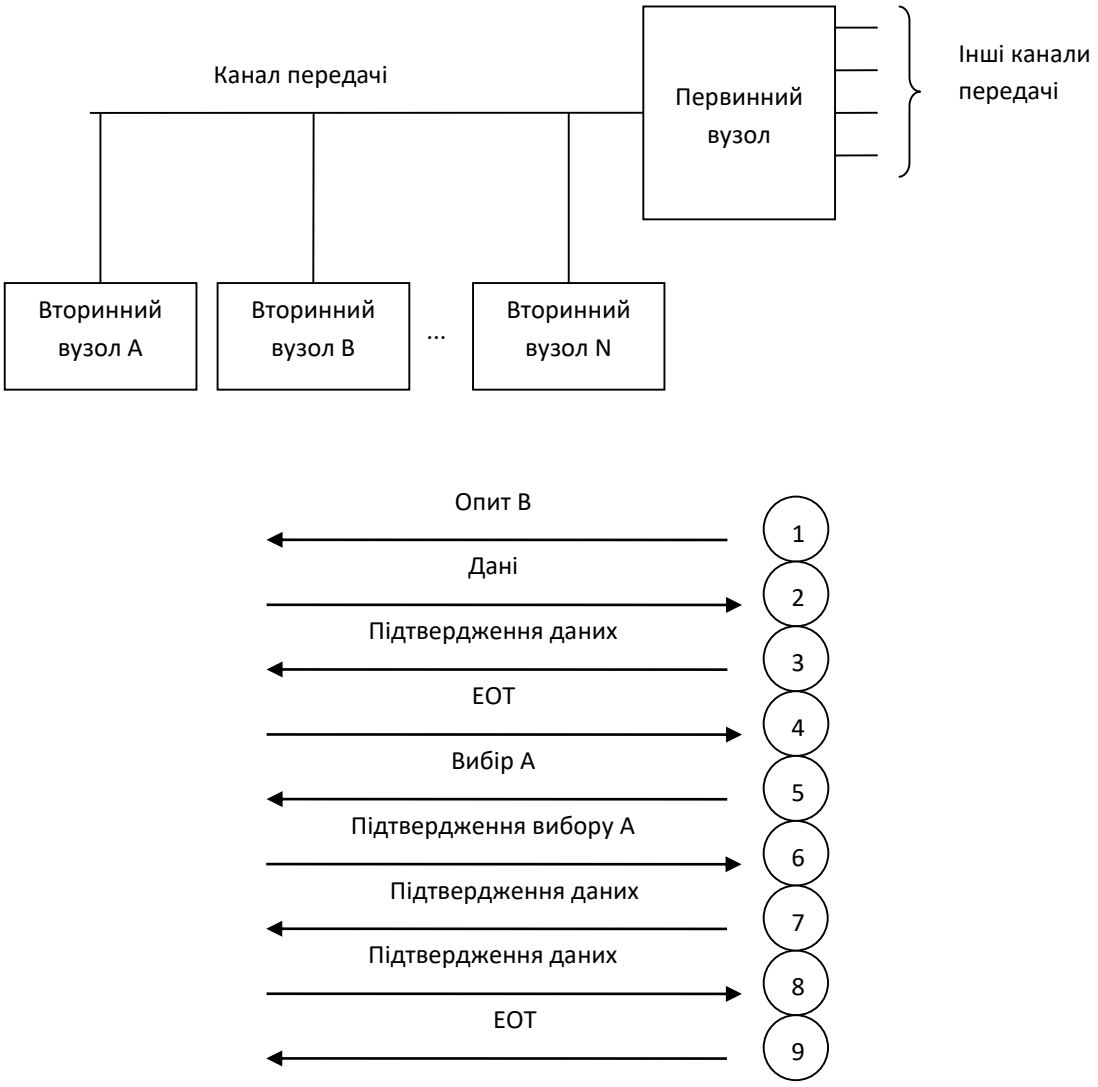


Рисунок 4.7 - Структура системи опиту/вибору з загальним каналом передачі

Квитування – передача службової інформації (квитанцій) про готовність вузлів до прийому і підтвердження отримання даних.

Даний приклад ілюструє ієрархічність структури первинний/вторинний: всі дані, що передаються між вузлами, завжди проходять через первинний вузол. З цією властивістю пов'язана проблема надійності таких систем, тому що

відмова первинного вузла призводить до відмови функціонування всієї системи (необхідно передбачити резервування первинного вузла).

4.3.2. Опит/вибір з зупинкою та очікуванням

Є однією з простіших різновидностей методів опиту/вибору. В таких системах вузол передає дані і чекає відповіді. Метод працює в напівдуплексному режимі і широко використовується завдяки простоті реалізації і низькій вартості.

Основний недолік – відсутність будь-яких засобів, дозволяючих контролювати послідовність кадрів, що передаються. В результаті достатньо складно обробляти помилкові ситуації, пов'язані з зникненням кадрів або помилками передачі.

Подальшим розвиненням цього методу, в якому усувається вказаний недолік, є метод зупинки і очікування з нумерацією. В цьому методі для підтримування квитування і керування потоком передачі використовують порядкові номера кадрів.

В даному методі вузол-відправник підтримує нумерацію відправлених кадрів, вставляючи порядкові номера в поле керування кадрів. Вузол-приймач виконує контроль помилок передачі отриманого кадру (подія 1, рис. 4.8) і видає підтвердження прийому даних, вставляючи в його заголовок номер отриманого кадру (2). По отриманні позитивного підтвердження з номером попереднього відправленого кадру вузол-відправник виконує передачу наступного кадру (3). У випадку втрати кадру даних або підтвердження про доставку (наприклад, загублений кадр підтвердження (4)), вузол-відправник чекає деякий час (бере так званий тайм-аут) і виконує повторну передачу кадру, на які не було отримано підтвердження (5). Дані, які передані у події (5), є копією даних у події (3). Так як вузол-приймач успішно прийняв цей кадр раніше, він відкине отриманий дублікат і видасть повторне підтвердження про прийом кадру.

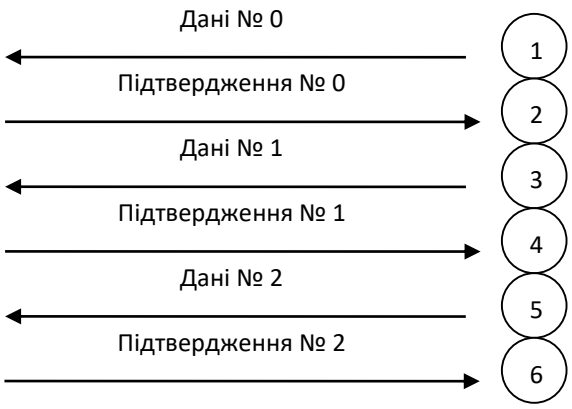


Рисунок 4.8 - Процедура обміну повідомленнями

4.3.3. Безперервний автоматичний запит на повторення (безперервний ARQ або "ковзаючі вікна")

Є одним з найбільш розповсюдженим методом з групи первинний/вторинний, який широко використовується як в протоколах канального рівня, так і в транспортних протоколах (наприклад, в протоколі TCP зі стеку TCP/IP). Метод підтримує дуплексний обмін даними між вузлами і базується на поняттях приймаючого і передаючого вікон.

Вікно встановлюється на кожному кінці каналу зв'язку і використовується для резервування визначених ресурсів вузла для передачі даних. Зазвичай під вікном розуміють деякий буферний простір і правило нумерації кадрів. Вікна встановлюються під час ініціалізації сеансу зв'язку між двома вузлами. При цьому для кожної пари додатків, що обмінюються даними на різних вузлах, потребується відкриття своєї пари вікон. В передаючому і приймаючому вікнах ведеться нумерація кадрів за допомогою змінних стану, які представляють собою стан лічильника.

Передаючий вузол підтримує змінну відправлення, а приймаючий вузол - змінну прийому. Змінна відправлення визначає порядковий номер кадру, який повинен бути переданий. Змінна прийому визначає порядковий номер наступного очікуваного кадру. Змінна відправлення збільшується на одиницю

при передачі кожного кадру і розміщується в полі порядкового номеру відправлення кадру. Отримавши кадр, приймаючий вузол проводить контроль помилок передачі і порівнює порядковий номер кадру зі своїм значенням змінної прийому. Якщо кадр може бути прийнятий, приймаючий вузол збільшує на одиницю змінну прийому і розміщує це значення в полі порядкового номеру прийому позитивного підтвердження (ACK) і відправляє дане підтвердження вузлу-відправнику, завершуючи квитування про проходження даного кадру. Позитивні підтвердження йдуть декількома кадрами один за одним.

Якщо вузол-приймач знайшов помилку передачі (по контрольній послідовності кадру) або порядковий номер кадру не відповідає значенню змінної прийму, то після деякого тайм-ауту у вузол-відправник надсилається негативне підтвердження (NAK) з поточним значенням змінної прийому. Отримавши таку квитанцію передавач відновлює старе значення змінної відправлення і виконує повторну передачу кадру з таким порядковим номером.

Рисунок 4.9 - Розподіл кадрів у вікні

Якщо розмір вікна дорівнює W-кадрів, а остання по часу прийому квитанція має значення N, то відправник може надсилати кадри у відкрите вікно до тих пір, поки номер кадру не буде рівним N+W. Кадр з таким номером

виходить за межі вікна і відправник повинен зупинити передачу до отримання наступної квитанції (рис. 4.9).

Розмір вікна і час тайм-ауту є важливими параметрами, що характеризують ефективність роботи методу. Так, в протоколах локальних мереж, де рівень помилок достатньо низький, а вузли мають достатньо великий об'єм ресурсів, розмір вікна зазвичай складається з 127 кадрів, тобто для нумерації використовується 8 біт. 127-й номер - номер наступного очікуваного кадру. При використанні методу в протоколах канального рівня глобальних мереж розмір вікна звичайно складає 7 кадрів (для нумерації залучено 3 біти).

Для зменшення накладних витрат, пов'язаних з передачею позитивних квитанцій, може бути використане так зване включаюче підтвердження прийому. Так, наприклад, АСК з номером 5 означає підтвердження прийому чотирьох попередніх кадрів і очікування кадру з номером 5.

Метод ковзаючих вікон широко використовується в протоколах глобальних мереж. Важливою особливістю таких мереж є знаходження і виправлення помилок передачі. Для вирішення цієї задачі використовують два методи (рис. 4.10):

- вибіркове повторення (Selective Repeat) – виконується повторна передача тільки того кадру, в якому була знайдена помилка;
- повернення на N (Go – Back - N) – виконується повторна передача не тільки помилкового кадру, але і всіх кадрів, які були відправлені після нього.

У випадку вибіркового повтору більш ефективно використовується канал передачі, однак приймач повинен задіяти додаткові ресурси для зберігання отриманих правильних кадрів і відновлення правильної послідовності кадрів після отримання повторного кадру для передачі цієї послідовності протоколам верхнього рівня.

Повернення на N – більш простий метод. Він не потребує постановки кадру в чергу приймача. Але ефективна пропускна здатність каналу у цьому

випадку буде нижча, так як повторно будуть передаватись і кадри, передані без помилок.

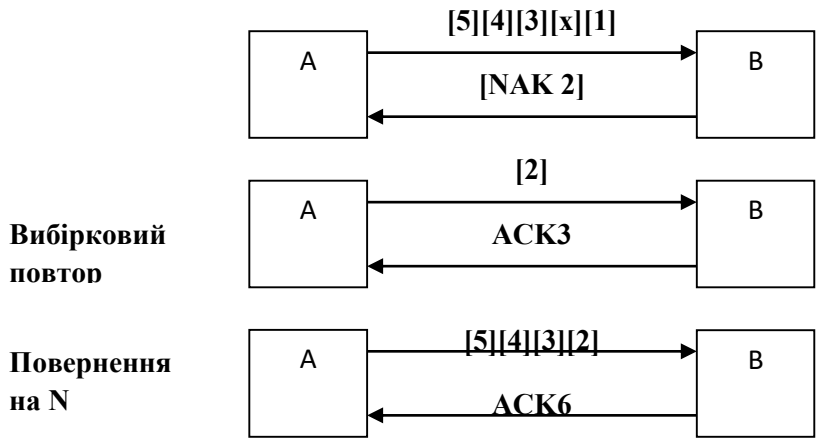


Рисунок 4.10 - Методи повторної передачі

Метод ковзаючих вікон використовується в наступних протоколах:

- глобальні обчислювальні мережі: протоколи HDLC, SDLC, LAP, LAPB, LAPD, LAPF;
- локальні обчислювальні мережі: протокол LLC.

4.3.4. Системи без опиту

До систем без опиту відносять наступні методи:

- RTS/CTS (запит передачі/дозвіл передачі);
- Xon/Xoff;
- TDMA – множинний доступ з часовим розділенням.

Запит передачі/дозвіл передачі

Відноситься до апаратних методів керування каналом передачі, в якому для призупинення передачі даних і послідуючого відновлення передачі використовується зміна рівня електричного потенціалу на визначених лініях інтерфейсу.

Метод достатньо широко використовується при керуванні передачею даних на периферійні пристрої і каналоутворюючі пристрої (наприклад, модеми) і зазвичай використовуються разом з інтерфейсом RS-232.

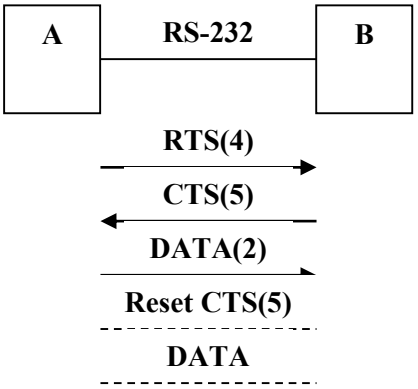


Рисунок 4.11 - Процедура керування та передачі даних в методі RTS/CTS

При наявності даних вузол А видає запит на передачу, підвищуючи рівень потенціалу по 4-й лінії інтерфейсу (рис. 4.11). Якщо вузол В готовий до прийому, він видає сигнал дозволу передачі даних, підвищуючи рівень потенціалу на 5-й лінії інтерфейсу. Дані передаються 2-й лінії. При відсутності місця в буфері для прийому даних вузол В скидає сигнал дозволу передачі, понижуючи рівень на 5-й лінії. Вузол А призупиняє передачу даних.

Xon/Xoff

Відноситься до програмних методів керування каналом передачі, в якому для призупинення і відновлення передачі використовується відправлення спеціальних службових символів по інформаційним лініям інтерфейсу.

Використовується разом з інтерфейсом RS-232 (рис. 4.12).

У даному методі сигнали Xon/Xoff є символами ASCII-коду. Xoff – ctrl-S, Xon – ctrl-Q.

Метод також використовується для керування потоком даних на периферійні і каналоутворюючі пристрої. Принцип роботи аналогічний до попереднього методу.

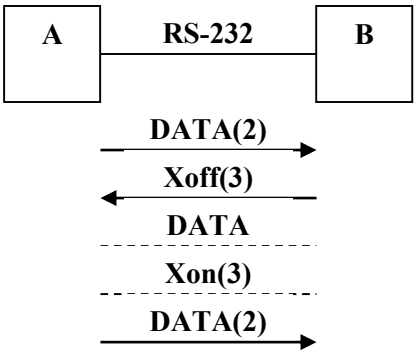


Рисунок 4.12 - Процедура керування та передачі даних в методі Xon/Xoff

4.3.5. Множинний доступ з часовим розділенням (TDMA)

Є подальшим розвиненням методу часового мультиплексування і найбільш широко використовується у супутникових системах передачі (наземні станції, через супутник-ретранслятор, використовуючи один частотний канал, виконують передачу даних). В таких системах одна з наземних станцій призначається в якості еталонної (або головної) і на неї покладаються функції по прийому і обробці запитів інших станцій (вторинних) і видачі дозволів на використання каналу передачі вторинними станціями.

При наявності даних для передачі, вторинні станції надсилають запити на використання загального каналу передачі. Запити надсилаються як частина поточних повідомлень в спеціальному керуючому полі звичайних інформаційних кадрів. Всі ці кадри проходять через супутник-ретранслятор і опиняються на еталонній станції. Ця станція обробляє надіслані запити і видає керуючий кадр, в якому визначено, які станції і в якій часовий інтервал (time-slot) можуть виконувати передачу своїх даних в загальний канал. Отримавши керуючий кадр, всі станції виконують часове підлаштування для того, щоб виконати передачу у відведений їм часовий інтервал.

В даному методі легко може бути реалізована пріоритетна схема, коли в якості пріоритету використовується інтенсивність передачі від станції або тип даних, що передаються (відео, голосовий трафік, звичайний трафік).

4.3.6. Рівнорангові методи

В цих методах не передбачений первинний вузол, а передбачається однаковий статус всіх пристроїв на загальному каналі. Однак вузли можуть не мати рівноправного доступу до загального каналу при використанні пріоритетних схем.

Рівнорангові методи отримали найбільше розповсюдження у протоколах локальних мереж.

4.3.7. Мультиплексна передача з часовим розділенням (TDM)

Даний метод є найпростішим прикладом непріоритетних рівнорангових систем і являє собою звичайне часове мультиплексування.

Кожному вузлу по черзі виділяється часовий інтервал незалежно від наявності у нього даних для передачі; під час цього інтервалу вузол може виконувати передачу даних в загальний канал.

4.3.8. Вставка регістру або буферу

Використовується в мережах з кільцевою топологією. Для управління потоком передачі використовується спеціальний зсувний регістр, який підключається до загального каналу передачі.

Принцип роботи полягає у наступному: коли у вузла є дані для передачі, він розміщує їх в зсувний регістр (рис. 4.13 а).

При наявності зручного моменту регістр підключається до загального кільцевого каналу, і дані передаються в канал (рис. 4.13 б). Регістр залишається підключеним до каналу, і всі кадри, що передаються по загальному каналу, будуть проходити через регістр (рис. 4.13 в). Коли вихідний кадр здійснить повний оберт по кільцю і повністю завантажиться в регістр, регістр відключається від загального каналу (рис. 4.13 г). Вузол-утримувач, отримавши кадр з кільця, у випадку відсутності помилок передачі повинен помітити кадр прапорцем "прочитаний", на основі чого вузол-відправник робить висновок про успішність передачі.

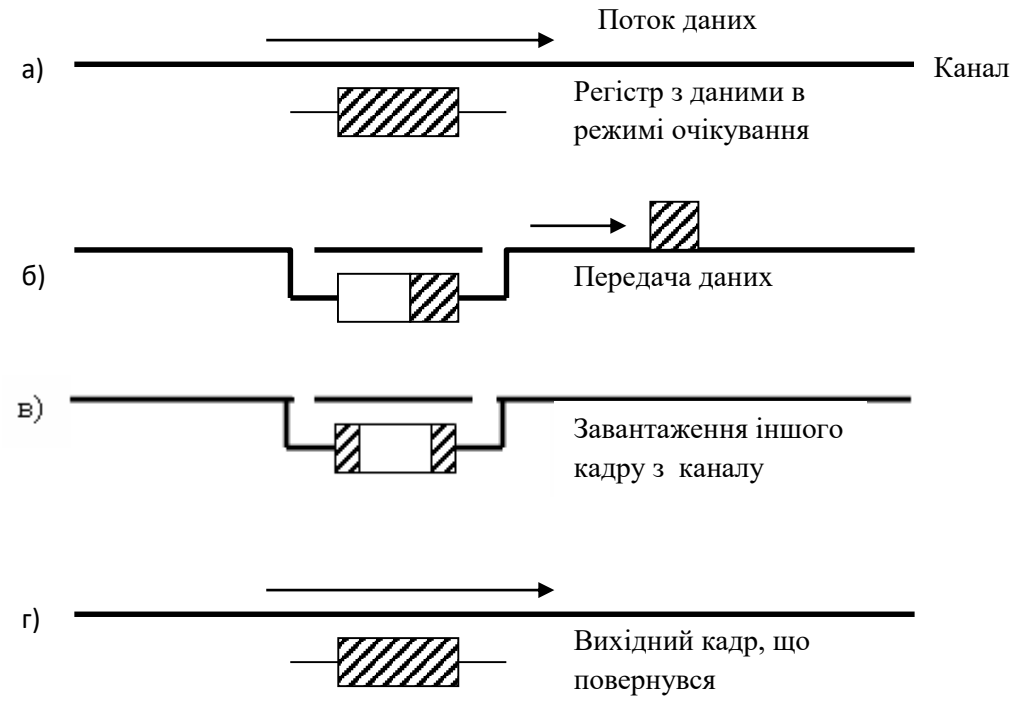


Рисунок 4.13 - Схема роботи зсувного регістру

Існують також варіанти даного методу, що використовують два регістри – приймаючий і передаючий.

4.3.9. Система з контролем несучої і виявленням колізій

Даний метод покладений в основу найбільш широко розповсюдженого протоколу локальних мереж – Ethernet. Використовується в мережах з шинною і зіркоподібною топологією. Всі вузли, що підключені до загального каналу, є рівноправними, хоча можливе використання пріоритетних схем на основі генерації різних часових інтервалів очікування.

Перед тим, як почати передачу даних в загальний канал, вузли прослуховують канал (процедура контролю несучої) для того, щоб визначити вільний чи зайнятий канал.

Наявність або відсутність сигналу в каналі визначається прийомопередавачем мережного адаптеру по наявності електричного

потенціалу в лінії.

У випадку, якщо канал вільний, будь-який вузол може відправити свої дані в канал. При цьому інформаційний сигнал від вузла буде розповсюджуватись у всі боки каналу.

При реалізації даного методу в сучасних системах використовується цифровий сигнал, а термін "несуча" історично використовується починаючи з перших систем, які були аналоговими.

Нехай вузол D веде передачу даних у загальний канал, а вузли A та B мають дані для передачі. Вони контролюють несучу та визначають, що канал зайнятий (рис. 4.14 а). Як тільки канал переходить у стан спокою, вузли A та B намагаються захопити канал, щоб виконати передачу (рис. 4.14 б).

У мережах з контролем несучої існує 3 методи захоплення каналу.

1. "Ненаполегливий" контроль – вузли можуть виконати передачу даних одразу як тільки виявлять, що канал вільний. Якщо канал зайнятий, вузли генерують випадковий час очікування, після чого спочатку контролюють несучу, щоб визначити вільний чи зайнятий канал (табл. 4.1).

2. "P-наполегливий" контроль (в даному методі P означає ймовірність) – метод передбачає для кожного вузла деякий алгоритм очікування. Наприклад, станції A і B не починають миттєву передачу після того, як виявили, що канал знаходиться у стані спокою, а кожна станція генерує випадковий час очікування (звичайно декілька мікросекунд). Якщо по закінченні цього часу станція виявить, що канал зайнятий, вона зачекає деякий період часу та зробить нову спробу захопити канал. В результаті вузол виконає передачу у канал, що звільнився з ймовірністю P та з ймовірністю 1-P відкладе передачу до наступної спроби (табл. 4.1).

3. "1-наполегливий" контроль – вузли виконують передачу відразу після того, як виявляють, що канал вільний. У випадку, коли канал зайнятий, вузли постійно контролюють несучу, щоб визначити момент звільнення каналу. Метод називається "1-наполегливим", так як вузли з ймовірністю рівною 1 будуть намагатися виконати передачу у канал, що звільнився (табл. 4.1).

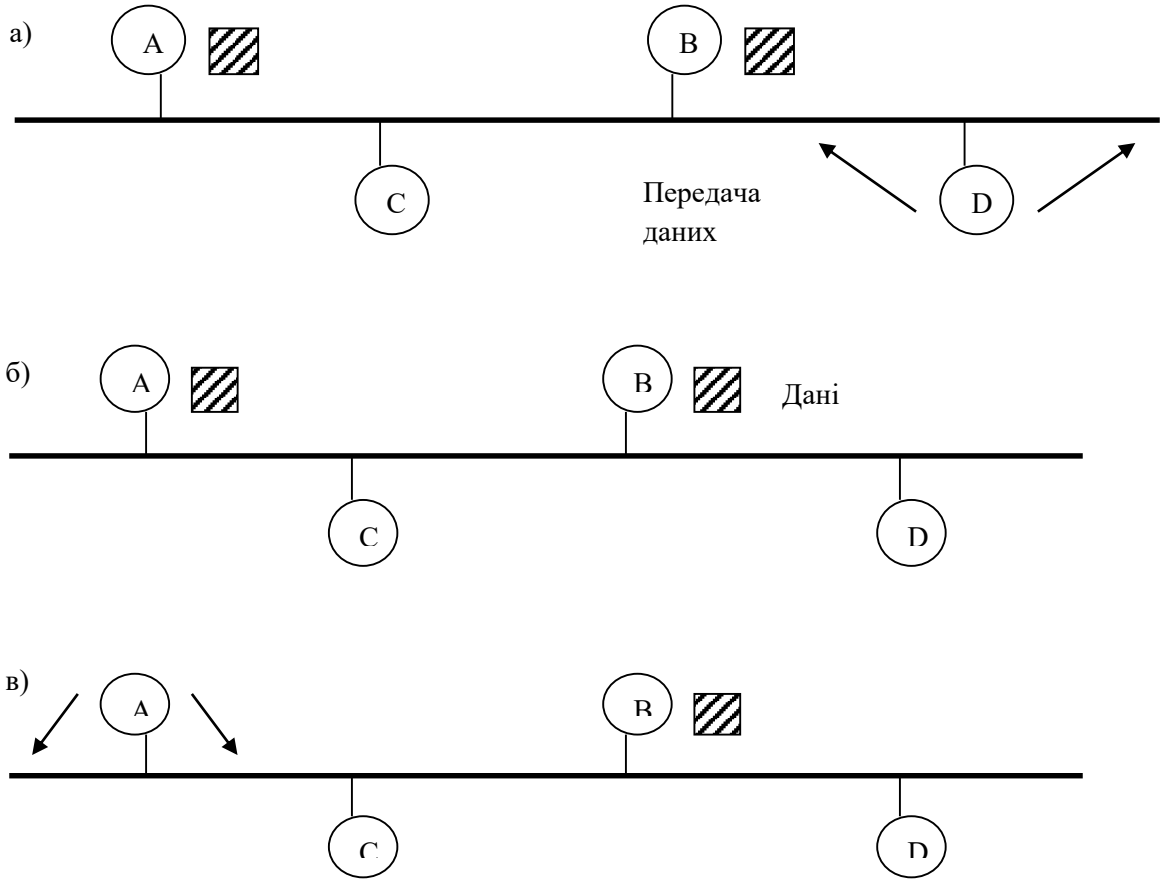


Рисунок 4.14 - Схема роботи системи з контролем несучої і виявленням колізій

Таблиця 4.1 - Порівняльні характеристики методів захоплення каналу

Умова	Ненаполегливий	Р-наполегливий	1-наполегливий
вільний канал	передати негайно	передати з ймовірністю Р, відкласти передачу з ймовірністю (1-Р)	передати негайно
зайнятий канал	випадковий час очікування і контроль несучої	передати з ймовірністю Р, відкласти передачу з ймовірністю (1-Р)	безперервно контролювати несучу
колізія	передати повторно через випадковий проміжок часу очікування	передати повторно через випадковий проміжок часу очікування	передати повторно через випадковий проміжок часу очікування

Метод Р-наполегливого контролю переслідує дві цілі:

– зменшення часу перебування каналу у стані спокою, що забезпечується 1-наполегливим методом;

– зменшення ймовірності виникнення колізій в каналі, що забезпечується методом ненаполегливого контролю.

Однак значення P залежить від особливостей конкретної мережі і для ефективного керування каналом передачі потребує збору багатьох статистичних даних впродовж тривалого часу. Тому розповсюдження в конкретних протоколах даний метод не отримав.

Продовжимо аналіз принципу роботи системи з контролем несучої. Нехай вузол А виявив, що канал вільний і почав передачу в канал до того, як у вузла В закінчився інтервал очікування. По закінченні цього інтервалу вузол В повинен виявити, що канал зайнятий і не відправляти свої дані до каналу. Але є затримка розповсюдження електричного сигналу, що пов'язана з кінцевою швидкістю проходження сигналу по кабелю, затримками в прийомопередавачах мережних адаптерів і проміжних мережних пристроях. В результаті в каналі стикаються дані від декількох вузлів. Така ситуація називається колізією.

Колізія характеризується часовим параметром, відомим під назвою "вікно колізії". Вікно колізії представляє собою подвійний час проходження сигналу між двома найбільш віддаленими вузлами мережі (береться до уваги найгірший випадок, коли кадр від одного вузла стикається з кадром від іншого в його прийомопередавачі і зіпсований колізією сигнал повинен дійти до першого вузла). Цей час також називають часом каналу, або часом подвійного оберту.

Треба відзначити, що виникнення колізій є нормальним для даного методу керування каналом. Зі збільшенням протяжності каналу вікно колізій збільшується, збільшується ймовірність виникнення колізій і, відповідно, зменшується ефективність роботи мережі. Тому даний метод використовується тільки в класі локальних мереж, для яких характерні відносно невеликі протяжності каналів.

Вузли обробляють колізію наступним чином. Кожен вузол, що виконує передачу даних, паралельно постійно контролює несучу. При виникненні колізії в каналі спостерігається аномальний рівень електричного сигналу, з якого передаючі вузли виявляють колізію (друга функція процедури контролю

несучої – виявлення колізій). Виявивши колізію, вузли переривають передачу, генерують випадковий час очікування, після чого роблять спробу знову захопити канал. Генерація випадкового часу очікування є деякою гарантією того, що колізія знову не виникне, хоча в даному методі керування каналом існує теоретична можливість постійного виникнення колізій, в результаті чого вузли не зможуть передавати дані.

4.3.10. Маркерні системи

Передача маркера є ще одним широко розповсюдженим методом, що використовуються в рівнорангових пріоритетних і непріоритетних системах, що реалізуються зазвичай в класі локальних мереж. Маркерні системи можуть бути реалізованими на базі кільцевої та шинної топологій.

Маркерне кільце

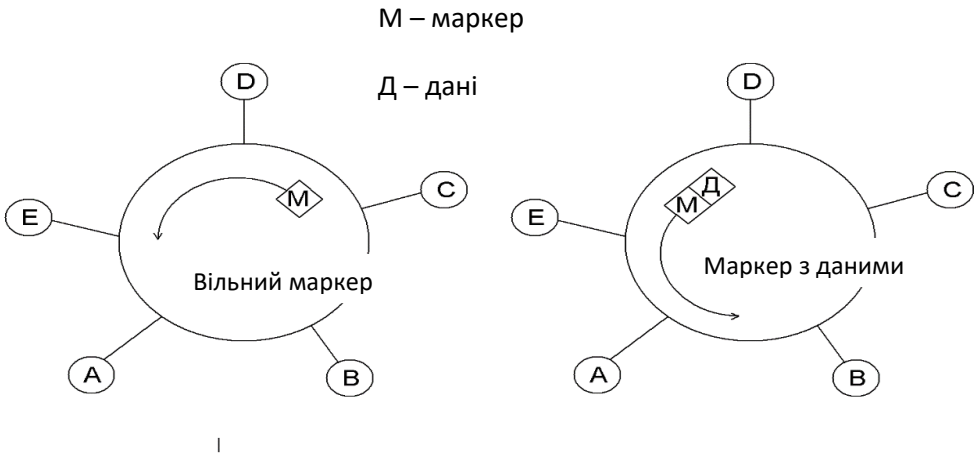


Рисунок 4.15 - Схема роботи маркерного кільця

Зазвичай вузли підключаються до загального каналу за допомогою кільцевого інтерфейсного пристрою (КІП) (мережний адаптер, багатопортовий пристрій підключення) .

КІП відповідає за контроль даних, що проходять через нього, і виконує функції регенерації сигналу і передачі його далі в кільце. Якщо адреса в кадрі відповідає даному вузлу, КІП копіює дані у свій буфер обміну для їх подальшої передачі кінцевому додатку. При цьому КІП помітить кадр прапорцем "прочитаний" і відправить далі у кільце. Якщо кільце знаходиться в стані спокою (ні одна станція не веде передачу даних), по кільцю циркулює маркер, помічений прапорцем "вільний". Маркер являє собою інформаційний службовий кадр довжиною декілька біт, для запису до них необхідних прапорців.

Вільний маркер циркулює по кільцю від вузла до вузла (рис. 4.15), і будь-яка станція, що має дані для передачі, може захопити маркер, додати до нього власний кадр, помітити прапорцем "зайнятий" і відправити його далі в кільце. Такі системи називаються системами з явним маркером – будь-який вузол, що отримав вільний маркер, може розпочати передачу. Маркер з даними проходить від вузла – до вузла. КІП кожного вузла прочитує прапорці і адресне поле маркеру і ретранслює маркер з даними в кільце. Виконавши повний оберт по кільцю, маркер з даними досягає вузла-відправника. Вузол-відправник звільняє маркер (видаляє власний кадр, впевнившись, що він помічений прапорцем "прочитаний", помічає маркер прапорцем "вільний" і відправляє його далі в кільце). Якщо вільний маркер виконає повний оберт по кільцю і знову досягне даного вузла-відправника, то цей вузол має право знову захопити маркер і виконати передачу наступного кадру.

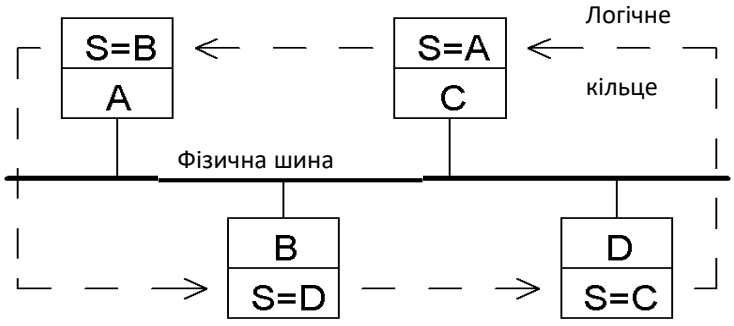
В деяких маркерних системах є можливість одночасної передачі кадрів від декількох вузлів (так звана "підсадка" кадрів). Вузол, що має дані для передачі, видаляє вільний маркер з кільця, генерує власний кадр даних і розташовує маркер позаду кадру даних. Наступний вузол в кільці, у якого також є дані для передачі, знову видаляє маркер, додає до попереднього кадру власний і генерує позаду кадрів даних новий маркер. У результаті по кільцю циркулює декілька кадрів від різних вузлів, що дозволяє більш ефективно використовувати канал у випадку його великої протяжності, коли час оберту

стає достатньо великим. Такий підхід використовується в магістральній технології FDDI.

Маркерна шина

Даний метод реалізується в мережах з шинною топологією і виключає можливість виникнення колізій в таких мережах. Метод не потребує фізичного упорядкування вузлів (тобто, щоб вузли були підключені до шини у визначеному порядку). За допомогою механізму логічної адресації може бути призначена будь-яка послідовність передачі маркеру доступу від вузла до вузла (відповідно, можливо отримати будь-яку конфігурацію кільця).

В даному методі використовується кадр керування, який називається правом доступу, або маркером доступу. Цей маркер надає в монопольне використання загальний канал вузлу, адреса якого вказана в маркері (рис. 4.16). Цей вузол утримує канал впродовж часу, що необхідний для передачі даних, і потім передає маркер у відповідності з логічною конфігурацією кільця. Маркер буде розповсюджуватися в обидві боки по всьому шинному каналу, його отримають і проаналізують всі вузли, але захопити канал зможе тільки той вузол, адреса якого вказана в маркері.



S – адреса наступного вузла, якому передається маркер доступу.

Рисунок 4.16 - Схема роботи маркерної шини

Адреса в маркері змінюється в циклічній послідовності. Це дозволяє реалізувати логічне кільце на фізичній шині.

Даний метод також відноситься до явних маркерних систем. Використовується в протоколі ЛОМ Arcnet (стандарт IEEE 802.4).

4.3.11. Пріоритетні слотові системи

Є подальшим розвитком систем з часовим квантуванням і мультиплексуванням, що були розглянуті вище. В таких системах використання загального каналу передачі виконується на деякій пріоритетній основі. Наприклад, можуть бути використані наступні критерії для встановлення пріоритетів вузлам:

- попереднє володіння часовим слотом;
- час відповіді, що задовольняє заданий вузол;
- об'єм даних, що передаються;
- вимоги до характеристик передачі даних.

Пріоритетні слотові системи можуть бути реалізовані без еталонної станції. В цьому випадку керування використанням часових слотів забезпечується шляхом завантаження параметрів пріоритетів на кожному вузлі (використовується в супутникових системах передачі).

4.3.12. Системи с контролем несучої без колізій

Відмінність даних систем від систем з колізіями заключається в спеціальній логіці для недопущення виникнення колізій.

В системах без колізій використовується спеціальний пристрій, що називається таймером, або арбітром. Цей пристрій визначає, коли вузли можуть виконувати передачу в загальний канал без небезпеки виникнення колізій. Кожному вузлу попередньо встановлюється визначений часовий поріг, після настання якого вузол, на базі деякого часового інтервалу визначає, коли він зможе виконати передачу до загального каналу.

Часові пороги можуть встановлюватися на базі пріоритетних схем, причому у вузла з найбільшим пріоритетом часовий поріг настає раніше, аніж у інших вузлів. У разі, якщо у нього нема даних для передачі, канал буде простоювати до настання часового порогу наступного по пріоритету вузла. Даний вузол визначає, що канал вільний і, так як виділений йому ліміт часу для передачі не вичерпано, він зможе захопити канал і виконати передачу даних. Система без колізій використовує арбітра, щоб надати можливість вузлу з наступним по величині пріоритетом виконати передачу даних у вільний канал. Такий підхід значно зменшує час простою каналу.

4.3.13. Пріоритетні маркерні системи

Являють собою покращену схему передачі маркеру, що передбачає використання пріоритетів в маркерній мережі (зазвичай в маркерному кільці). В таких системах кожний вузол, що підключений до кільцевого каналу, отримує деяке значення пріоритету (стандартно використовується вісім рівнів пріоритетів).

Призначення пріоритетної схеми полягає в тому, щоб вузол намагався зарезервувати кільце для передачі даних в наступному циклі оберту маркеру. Для цього в маркері наявне спеціальне поле резервування. Коли вузол, що має дані для передачі, отримує маркер з даними, він записує в поле резервування власне значення пріоритету. Наступний вузол на загальному каналі, що має дані для передачі, аналізує значення поля резервування і, якщо його пріоритет вищий за це значення, вузол записує власне значення пріоритету в поле резервування. Таким чином, вузол з найбільшим пріоритетом зарезервує використання каналу в наступному циклі.

При звільненні маркеру вузол-відправник перепише значення пріоритету з поля резервування в поле пріоритету, помітить маркер прапорцем "вільний" і відправить маркер в кільце. Перший вузол на загальному кільцевому каналі, що

має дані для передачі і пріоритет якого співпадає з пріоритетом маркеру, має право захопити маркер і виконати передачу даних. Вузли з меншим значенням пріоритету не мають права захопити маркер.

Резервуючи маркер, високопріоритетний вузол запам'ятовує попереднє значення пріоритету. Коли маркер з даними звершить повний оберт по кільцю, вузол перепише це значення з пам'яті в поле пріоритету, даючи таким чином можливість вузлам з меншим пріоритетом виконати передачу даних при високій інтенсивності високопріоритетного трафіку.

Пріоритетна схема використовується в протоколі ЛОМ IBM Token Ring і стандарті IEEE 802.5.

4.4. Особливості моделі і архітектури локальних мереж

Для стандартизації протоколів локальних обчислювальних мереж (ЛОМ) використовується набір стандартів 802 інституту інженерів електронної техніки та радіоелектроніки (IEEE). Цей набір стандартів описує два нижніх рівні моделі OSI (фізичний та канальний) і орієнтований на ЛОМ [О: 1, 2, 3, 4].

Основні стандарти.

802.1 – вступ до ЛОМ – визначає архітектуру ЛОМ і її зв'язок з моделлю OSI, особливості верхніх рівнів моделі і адміністративне керування ЛОМ. Додатково в цей стандарт входять протоколи, що враховують міжмережну взаємодію, наприклад:

802.1 q – віртуальні локальні мережі,

802.1 p – пріоритезація трафіку,

802.1 d – протокол остовного дерева (spaning tree).

802.2 – протокол керування логічною ланкою даних (LLC) – визначає функції інтерфейсу між фізичним середовищем передачі і протоколами верхніх рівнів.

Інші стандарти з набору 802 описують конкретні протоколи керування каналами передачі даних. З них найбільш розповсюджені:

802.3 – протокол множинного доступу з контролем несучої і виявленням колізій (МДКН/ВК) – аналог протоколу Ethernet – перша версія протоколу, в якому специфікація фізичного рівня орієнтована на коаксіальний кабель (КК). Даний стандарт має наступні версії:

802.3i – 10 Base-T,

802.3u – 100 Base-TX, T4, FX,

802.3ab, 802.3z – гігабітна мережа (Gigabit Ethernet).

802.4 – протокол маркерної шини (аналог мережі Arcnet).

802.5 – протокол маркерного кільця (аналог IBM Token Ring).

802.6 – стандарт на побудову міських мереж.

802.11 – бездротові системи Wi-Fi (Radio Ethernet).

802.12 – протокол централізованого доступу на базі пріоритетних запитів.

802.16 – бездротова технологія WiMAX.

У відповідності зі стандартом 802.1 спрощена модель OSI для ЛОМ може бути представлена в наступному вигляді (рис. 4.17).

У відповідності з моделлю ЛОМ, що описана в стандарті 802, канальний рівень розділюється на два підрівні:

- керування логічним каналом або ланкою (LLC),
- керування доступом до середовища (MAC).

В функції LLC входять передача кадрів між вузлами і виявлення помилок передачі. Підрівень LLC є універсальним для всіх протоколів керування каналом 802-го стандарту, незалежно від особливостей реалізації фізичного середовища передачі та конкретних методів доступу до каналу.

Підрівень MAC реалізує алгоритм доступу до загального каналу передачі і фізичну адресацію вузлів.

Фізичний рівень забезпечує підключення до фізичного середовища, кодування та декодування сигналів, їх буферизацію, підтримує і відновлює бітову синхронізацію. Розділяється на два підрівні:

– керування фізичним сигналом (PCS),
– модуль доступу до середовища (PMA).

Рівні		Функції	Реалізація
Пикладний Представницький Сеансовий Транспортний		Підтримка додатків і користувачів	Засоби ОС
Мережний		Маршрутизация і передача даних	TCP/IP Net BIOS/Net BEUI
Канальний	Керування логічним каналом (LLC)	Керування каналом передачі, виявлення і виправлення помилок фізичного рівня	Драйвер NDIS
	Керування доступом до середи (MAC)		Мережний адаптер
Фізичний	Керування фізичним сигналом (PCS)	Формування бітової послідовності, синхронізація	Мережний адаптер
	Модуль доступу до середовища (PMA)		Мережний адаптер
	Інтерфейс, що залежить від середовища (PMD)	Спряження з конкретним фізичним середовищем	Мережний адаптер

Рисунок 4.17 - Модель архітектури ЛОМ

Додатково в архітектурі ЛОМ виділяють інтерфейс, що залежить від середовища (PMD) і враховує характеристики конкретного середовища передачі і особливості підключення до нього.

Функції всіх інших рівнів аналогічні функціям рівнів в стандартній семирівневій моделі OSI, тільки реалізуються за допомогою стеків конкретних протоколів, що використовуються в локальній мережі і засобами мережної операційної системи.

4.4.1. Керування логічним каналом (LLC) і стандарт 802.2

До функцій LLC входить передача кадрів між вузлами, включаючи виявлення і виправлення помилок. Для передачі може бути використаний або

дейтаграмний метод, або процедура з встановленням з'єднання і підтвердженням. Цей протокол не залежить від фізичного середовища і алгоритму доступу до нього і є універсальним для протоколів канального і фізичного рівнів стандарту 802 і стандарту FDDI. В основу протоколу LLC покладено протокол HDLC (високорівневий протокол керування каналом передачі даних) з групи первинний/вторинний, що використовує метод ковзаючих вікон.

У відповідності зі стандартом 802.2, рівень LLC надає верхнім рівням три типи процедур:

1) LLC (тип 1) – процедура без встановлення з'єднання і без підтвердження прийому.

2) LLC (тип 2) – процедура з встановлення з'єднання і з підтвердженням прийому.

3) LLC (тип 3) – процедура без встановлення з'єднання і з підтвердженням прийому.

LLC 1 представляє дейтаграмний режим передачі і використовується тоді, коли функція виявлення і виправлення помилок виконується протоколами верхніх рівнів (наприклад, TCP).

LLC 2 реалізує метод ковзаючих вікон, формуючи при цьому віртуальні канали між відправником і отримувачем.

LLC 3 передбачений для систем, у яких критичні накладні витрати на встановлення з'єднання (наприклад, системи керування технологічними процесами в реальному часі).

Використання конкретного типу процедури LLC 1 – LLC 3 залежить від стеку протоколів верхнього рівня, що використається.

Так, стеки TCP/IP, IPX/SPX використовують LLC 1, стек NetBIOS/NetBEUI – LLC 2, коли сам протокол NetBEUI повинен працювати в режимі відновлення загублених і зіпсованих кадрів і LLC 1, коли NetBEUI працює в дейтаграмному режимі.

Кінцеві вузли можуть забезпечувати декілька типів послуг LLC.

За цим критерієм вони поділяються на наступні класи:

1) пристрій класу 1; забезпечує послуги LLC 1,

2) пристрій класу 2; забезпечує послуги LLC 1 і LLC 2,

3) пристрій класу 3; забезпечує послуги LLC 1 і LLC 3,

4) пристрій класу 4; забезпечує послуги LLC 1, LLC 2 і LLC 3.

Кадри рівня LLC носять назву протокольних блоків даних (PDU) і поділяються на три типи:

1. I-кадри (інформаційні) – передбачені для передачі інформації в процедурах з встановленням логічного з'єднання LLC 2. Вміщують інформацію верхніх рівнів і керуючу інформацію для керування потоком даних в режимі ковзаючого вікна.
2. S-кадри (керуючі) – передбачені для передачі команд і відповідей в процедурах встановлення логічного з'єднання LLC 2. Ці кадри виконують запит і призупиняють передачу, повідомляють про стан і підтверджують прийом інформаційних кадрів.
3. U-кадри (невпорядковані, ненумеровані) – передбачені для передачі ненумерованих команд і відповідей, які забезпечують передачу інформації, ідентифікацію, тестування LLC-рівня в процедурах без встановлення логічного з'єднання, а в процедурах з встановленням логічного з'єднання з'єднують і роз'єднують логічні з'єднання і інформують про помилки.

Всі типи кадрів LLC-рівня мають єдиний формат (рис. 4.18).

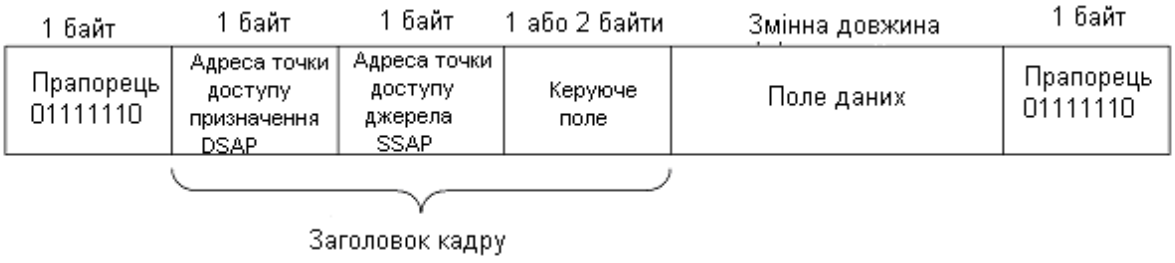


Рисунок 4.18 - Формат LLC-кадру

Прапорці (1 байт - 01111110) – використовується на MAC-рівні для визначення меж LLC-кадру.

Кадр рівня LLC вкладається в кадр відповідного рівня MAC. Ця процедура називається інкапсуляцією. При цьому прапорці відкидаються.

Заголовок LLC-кадру містить три поля: два адресних і керуюче.

Процедури верхніх рівнів використовують процедури LLC через точки доступу до послуг (SAP). Адреса DSAP ідентифікує приймаючий процес верхнього рівня. Адреса SSAP ідентифікує передаючий процес верхнього рівня.

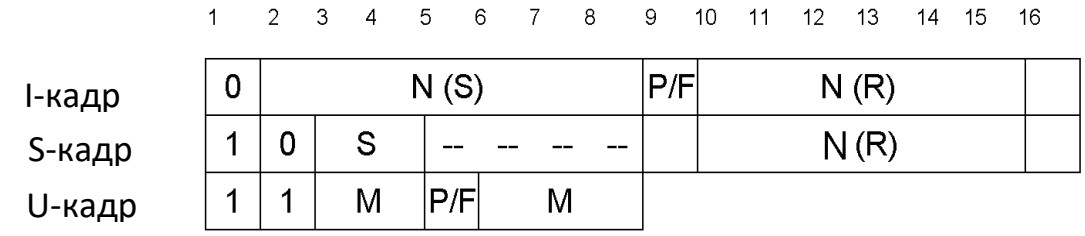
Програмному забезпеченню вузлів при отриманні кадрів канального рівня необхідно розпізнати, який протокол вклав свій пакет в поле даних кадру для того, щоб передати отриманий з кадру пакет потрібному протоколу верхнього рівня для обробки.

Значення адрес SAP приписуються протоколам у відповідності зі стандартом 802.2 (наприклад, IP – SAP 0x6, Net BIOS – 0xF0).

Для одних випадків визначена тільки одна точка входу і, відповідно, один SAP, для інших – декілька.

Адреси DSAP і SSAP при звичайній передачі співпадають. Різні значення DSAP і SSAP використовуються в кадрах, що повідомляють про якісь окремі ситуації, наприклад, при переході протоколу в інший режим передачі (використовується в NetBEUI).

Поле керування залежить від типу кадру (рис. 4.19) .



N(S) – номер послідовності відправки
N(R) – номер послідовності прийому
M – поле команд
P/F – Poll/Final

Рисунок 4.19 - Формат поля керування LLC - кадру

В режимі LLC 1 використовуються тільки U-кадри. В цьому випадку поле керування має 1 байт. Всі підполя мають нульові значення; значимі тільки перших два біти, що визначають ознаку типу кадру (0x03 з урахуванням зворотнього порядку нумерації біт в кадрі).

В режимі LLC 2 використовуються всі три типи кадрів. В цьому режимі кадри поділяються на команди і відповіді. Біт P/F використовується для реалізації функцій керування потоком. В командах він має назву "біт Poll" і потребує видачі негайної відповіді ("1"). У відповідях він називається "біт Final" і вказує на те, чи є поточний кадр останнім у відповіді ("1"), або ("0").

U-кадри використовуються на початковій стадії встановлення логічного з'єднання в процедурі LLC 2. Поле M визначає декілька типів команд, наприклад:

SABME – встановити збалансований асинхронний розширений режим. Команда є запитом на встановлення з'єднання. Розширений режим вказує на використання двобайтового поля керування для кадрів інших типів вузлів;

UA – ненумероване підтвердження. Підтверджує встановлення або розрив з'єднання;

RESET – скидання з'єднання (запит на розрив з'єднання).

Після встановлення з'єднання дані і позитивні квитанції починають передаватися в I-кадрах. Логічний канал протоколу LLC 2 є дуплексним (не плутати з фізичним каналом). Позитивні квитанції на кадри також надходять в інформаційних кадрах. У випадку негативних квитанцій використовуються S-кадри.

В інформаційних кадрах присутнє поле N(S) (номер послідовності відправки), що визначає номер кадру, який повинен бути відправлений наступним. Поле N(R) в інформаційному кадрі (номер послідовності прийому) вказує на наступний кадр, що очікується.

В протоколі LLC 2 використовується вікно на 127 кадрів (нумерація з 0 – по 127; принцип роботи розглянуто в методі ковзаючих вікон). У випадку

прийому негативних квитанцій передавач зобов'язаний повторити передачу кадру, в якому була виявлена помилка, а також всіх кадрів з більшими номерами, які він встиг відправити у відкрите вікно з 127 кадрів (метод повернення на N).

Поле S кадрів визначає декілька типів команд:

REJECT – відмова: видається приймачем, якщо номери посилки і прийому не співпали; кадр при цьому відкидається;

RNR – приймач не готовий;

RR – приймач готовий.

Команда RR з номером послідовності прийому зазвичай використовується як позитивна квитанція, коли потік даних від приймача до передавача відсутній.

Команда RNR використовується для уповільнення потоку кадрів, що надходять на приймач, у випадку, коли приймач не встигає обробляти потік, що надходить. Отримання такої команди передавачем потребує від нього повністю призупинити передачу до отримання кадру з командою RR.

4.4.2. Множинний доступ з контролем несучої і виявленням колізій (стандарт 802.3)

Найбільш розповсюджений протокол локальних мереж.

В 1980 році компанії Intel, Xerox, DEC оприлюднили специфікацію протоколу Ethernet, яка пізніше з невеликими доповненнями лягла в основу стандарту 802.3.

Стандарт 802.3 базується на концепції рівневих протоколів. При цьому в кожному вузлі виділяються приймаюча і передаюча сторони.

Спрощена структура моделі представлена на рис. 4.20.

Верхні рівні обслуговуються двома нижніми – канальним і фізичним.

Підрівень MAC канального рівня реалізує алгоритм доступу до загального каналу передачі і складається з двох логічних об'єктів: блокування/деблокування даних і об'єкт адміністративного керування доступом до середовища.

Основні функції цих об'єктів:

- блокування/деблокування даних – формує кадр, включає в кадр адресу відправника і одержувача, підраховує контрольну послідовність в передаючому вузлі і виконує аналогічні обчислення для виявлення похибок в приймаючому вузлі;
- об'єкт керування доступом до середовища – передає кадр на фізичний рівень і приймає кадр з нього, записує кадр в буфер, забезпечує усунення колізій на передаючій стороні.

Фізичний рівень залежить від типу фізичного середовища. Виконує наступні функції: прийом/передачу електричних сигналів в канал, забезпечення синхронізації в каналі, кодування/декодування даних.

Фізичний рівень також складається з двох логічних об'єктів: "кодування/декодування" і "доступ до каналу".

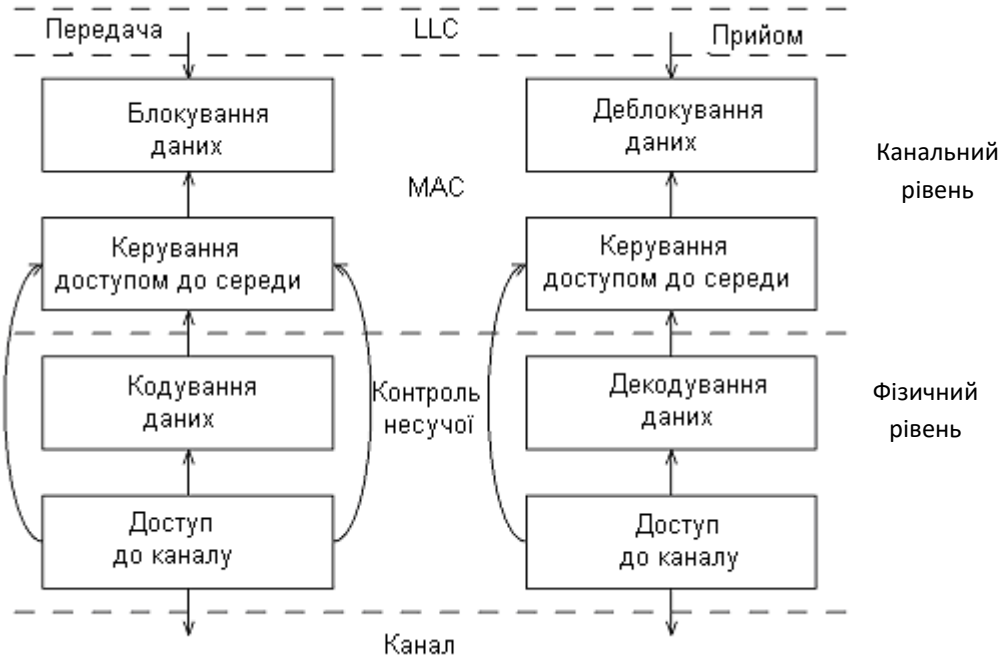


Рисунок 4.20 - Спрощена структура моделі протоколу 802.3

Об'єкт "кодування/декодування" виконує функції:

- формує сигнал для синхронізації (такий синхросигнал називається преамбулою);
- кодує двійковий потік з використанням самосинхронізуючихся логічних або фізичних кодів в передаючому вузлі і виконують зворотню операцію в приймаючому вузлі.

Об'єкт доступу до каналу:

- вводить фізичний сигнал на передаючій стороні і приймає на прийомній стороні;
- контролює несучу на приймаючій і передаючій сторонах;
- виявляє колізії на передаючій стороні.

Узагальнений вигляд кадру канального рівня має такий вигляд (рис. 4.21).

На фізичному рівні до кадру додається преамбула і початковий роздільник і у вигляді бітової послідовності кадр відправляється в фізичне середовище.

Рисунок 4.21 - Узагальнений вигляд кадру канального рівня

Поле "преамбула" містить сім синхробайтів (10101010) і використовується для побітної і побайтової синхронізації приймача і передавача.

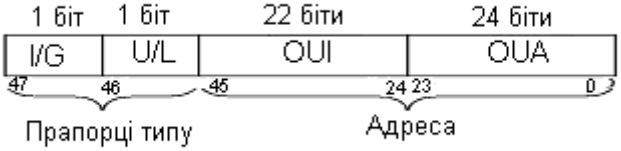
"Початковий роздільник" – 1 байт (10101011). З'явлення такої бітової послідовності вказує на те, що наступний байт буде першим байтом заголовка кадру.

Адресація.

Кожен вузол має унікальну фізичну адресу (MAC-адресу) довжиною у 48 біт. Дана адреса присвоюється мережному адаптеру виробником.

Формат адреси має наступний вигляд (рис. 4.22).

I/G – прапорець індивідуальної/групової адреси. I/G = 0 – індивідуальна адреса, присвоюється тільки одному інтерфейсу, вказує на MAC-адресу мережного адаптеру. I/G = 1 – вказує на групову або багатофункціональну, або багатопунктову адресу. Така адреса може бути присвоєна декільком мережним інтерфейсам. Надіслані на таку адресу кадри будуть копіюватися в буфери і оброблятися інтерфейсами всіх вузлів, що мають таку групову адресу. Якщо I/G = 1, то всі біти з 0-го – по 46-й розглядаються як єдина групова адреса, а не як окремі поля (U/L, OUI, OUA) звичайної MAC-адреси. Призначення групових адрес встановлюється проектувальниками мережних протоколів, наприклад, TCP/IP.



I/G – прапорець індивідуальної/групової адреси
U/L – прапорець універсального/місцевого керування
OUI – організаційно-унікальний ідентифікатор
OUA – організаційно-унікальна адреса

Рисунок 4.22 - Формат MAC-адреси Ethernet

U/L – прапорець універсального/місцевого керування. Визначає, яким чином була присвоєна адреса мережному адаптеру: якщо "0" – то виробником, "1" – користувачем (завжди повинен бути унікальним в межах мережі).

OUI – організаційно-унікальний ідентифікатор. Присвоюється виробникам обладнання комітетом IEEE.

OUA – організаційно-унікальна адреса. Присвоюється виробником унікально для кожного адаптеру.

Комбінація OUI і OUA складає унікально-керовану адресу (UAA) . В такій адресі біти I/G і U/L завжди встановлені в "0".

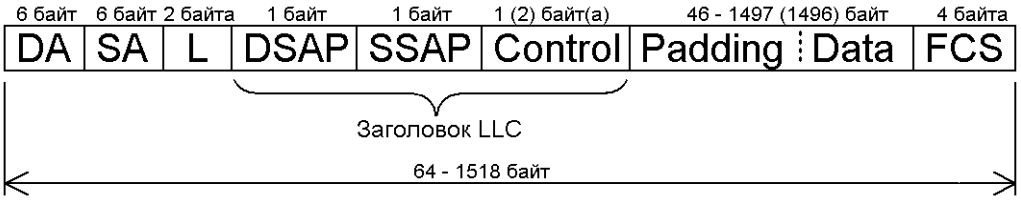
Існує спеціальна багатопунктова адреса – "широкомовленева", у якої всі 48 біт встановлені в "1". Кадр з такою адресою отримують і обробляють всі вузли, що знаходяться у одному домені широкомовлення.

Формати Ethernet-кадрів

В Ethernet-мережах можуть бути використані наступні формати кадрів:

- 802.3/LLC (802.3/802.2, або Novell 802.2)
- Raw 802.3 (Novell 802.3)
- Ethernet DIX (Ethernet II)
- Ethernet SNAP

Кадр 802.3/LLC (802.3/802.2) (рис. 4.23)



DA – адреса отримувача
SA – адреса відправника
L – довжина
DSAP – адреса точки доступу призначення
SSAP – адреса точки доступу джерела
Control – поле керування
Data – поле даних
Padding – поле заповнення
FCS – контрольна послідовність кадрів

Рисунок 4.23 - Формат кадру 802.3/LLC

Заголовок цього кадру є результатом об'єднання полів заголовків кадрів стандартів 802.3 та 802.2.

DA – адреса отримувача. Довжина поля може бути 2 або 6 байт. Звичайно використовується 6 байт (MAC-адреса або групова адреса).

SA – адреса відправника. Довжина поля може бути 2 або 6 байт. Перший біт в адресі завжди рівний "0" (в поле записано MAC-адресу вузла-відправника).

L – довжина; двобайтове поле, що містить значення довжини поля даних в кадрі.

Data – поле даних; 0 – 1497 байт. Якщо довжина поля даних менша 46 байт, то використовується поле заповнення Padding, щоб доповнити поле даних до мінімально припустимої довжини 46 байт.

Padding – поле заповнення; містить необхідну кількість байт-заповнювачів, щоб забезпечити мінімальну довжину поля даних в 46 байтів. Це необхідно для коректної роботи механізму виявлення колізій (треба витримати мінімальну довжину кадру у 64 байти).

FCS – контрольна послідовність кадру довжиною в 4 байти. Містить контрольну суму.

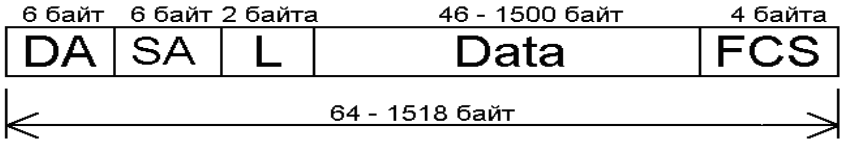
Кадр 802.3 є кадром підрівня MAC і, в відповідності зі стандартом 802.2, в його поле даних вкладається кадр LLC з видаленими прапорцями початку і кінця кадру.

Так як кадр LLC має заголовок довжиною 3 байти (LLC 1) або 4 байти (LLC 2), то максимальний розмір поля даних зменшено з 1500 – до 1497/1496 байтів.

Raw 802.3/Novell 802.3 (рис. 4.24)

Являє собою кадр підрівня MAC без вкладення кадру LLC (використовується в операційній системі Netware фірми Novell при використанні протоколу IPX). У Netware версії 4 і вище фірма Novell використовує кадри 802.3/LLC або Novell 802.2.

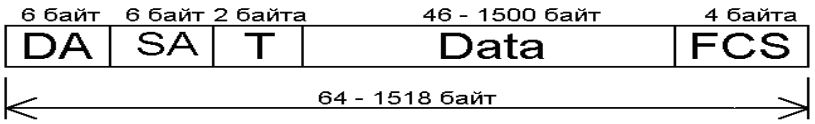
$L \leq 1500$ – довжина, визначає реальну довжину поля даних.



DA – адреса отримувача
SA – адреса відправника
L – довжина
Data – поле даних
FCS – контрольна послідовність кадру

Рисунок 4.24 - Формат кадру Raw 802.3/Novell 802.3

Ethernet DIX / Ethernet II (рис. 4.25)



DA – адреса отримувача
SA – адреса відправника
T – тип
Data – поле даних
FCS – контрольна послідовність кадру

Рисунок 4.25 - Формат кадру Ethernet DIX

T – тип; використовується для тих же цілей, що і поля DSAP, SSAP кадру LLC (визначає тип протоколу верхнього рівня, що вклав свій пакет в поле даних кадру).

Є першим історичним форматом Ethernet-кадру і до сих пір використовується в UNIX-системах.

Ethernet SNAP (рис. 4.26)

Для усунення різнобою в кодуваннях типів протоколів, пакети яких вкладені в поле даних Ethernet-кадру, комітет 802 розробив кадр Ethernet SNAP (протокол доступу до підмереж).

Даний кадр являє собою розширення кадру 802.3/LLC за рахунок введення додаткового заголовку протоколу SNAP.

DA – адреса отримувача
SA – адреса відправника
L – довжина
DSAP адреса точки доступу призначення
SSAP адреса точки доступу джерела
Control – поле керування
OUI - організаційно-унікальний ідентифікатор
Data – поле даних
Padding – поле заповнення
FCS – контрольна послідовність кадру

Рисунок 4.26 - Формат кадру Ethernet SNAP

Поле T – тип; складається з двох байтів і повторює по формату і призначенню поле "тип" кадру Ethernet II (містить код протоколу верхнього рівня).

Поле OUI – організаційно-унікальний ідентифікатор; визначає ідентифікатор організації, що встановлює коди протоколів, що використовуються в полі "тип" (для комітету 802 OUI = 0).

Протокол SNAP являє собою вкладений в LLC протокол. Тому в кадрі Ethernet SNAP в поля DSAP и SSAP він записує код 0xAA.

Поле керування встановлюється в 0x03, що відповідає використанню ненумерованих кадрів. Так як заголовок SNAP є доповненням до заголовку LLC, він припустимий і в інших технологіях стандарту 802 (802.5, 802.12) і технології FDDI.

Поле L/T мережним обладнанням не обробляється. Це поле обробляється протоколами верхнього рівня. Встановлення цього поля виконується драйвером мережного інтерфейсу NDIS.

Принцип роботи протоколу 802.3

Так як мережа, що побудована на базі реалізованого в протоколі 802.3 методу МДКН/ВК, є рівноранговою, то всі вузли намагаються захопити канал коли в них наявні дані для передачі. Конфлікти можливі тоді, коли два і більш вузлів практично одночасно намагаються надіслати кадр до каналу. В цьому випадку в каналі відбувається накладення і зіпсування сигналів – колізія.

Основним параметром, що характеризує ефект колізії, є вікно колізії – подвоєний інтервал часу, необхідний для розповсюдження електричного сигналу по каналу між двома найбільш віддаленими вузлами. Вважається, що за цей час сигнал від одного вузла повинен дістатись прийомопередавача іншого вузла, де виникне колізія і зіпсований колізією сигнал повернеться назад. Цю величину ще називають часом подвійного оберту, або часом каналу.

Розмір вікна колізії в стандарті 802.3 складає 512 біт-таймів, де біт-тайм – тривалість одного біту (1 біт-тайм = 100 нс, при швидкості 10 Мбіт/с; 1 біт-тайм = 10 нс, при швидкості 100 Мбіт/с).

З розміром вікна колізії пов'язане наступне основне правило проектування розділюємих (некомутованих) Ethernet-мереж: найгірше значення часу затримки сигналу в каналі не повинне перевищувати половини значення часу каналу.

З вікном колізії пов'язані ще два параметри Ethernet-мережі:

- мінімальний розмір кадру (512 біт = 64 байти);
- максимальний діаметр мережі (максимальна відстань між двома найбільш віддаленими вузлами).

Діаметр мережі повинен бути достатньо малим, щоб сигнал міг вийти з рівня MAC одного вузла, дійти до рівня MAC найбільш віддаленого вузла, і, у

випадку виникнення колізії на віддаленому вузлі, зіпсований колізією кадр повинен повернутися назад, впродовж часу каналу або вікна колізії. Колізія призводить до помилок в мережі і до зниження ефективної пропускної спроможності (хоча і є нормальним явищем для даного методу роботи).

Обробка колізій реалізується на рівні об'єкту керування доступом до середовища, шляхом переривання передачі кадру відразу же після виявлення колізії. При цьому об'єкт доступу до каналу на передаючій стороні помічає накладення сигналів в каналі (в вигляді аномальних рівнів напруги) і встановлює для об'єктів керування доступом до середовища спеціальний сигнал виявлення колізії. Для обробки колізії об'єкт керування доступом до середи виконує дві функції:

1. Підсилює ефект колізії в каналі шляхом відправлення спеціальної послідовності бітів, що називається "затором" (jam). Ціль затору полягає в тому, щоб зробити колізію настільки тривалою, щоб її змогли виявити всі вузли, залучені до колізії. Сигнал затору 32 – 48 байт. Нижня межа затору обмежена тим, щоб колізію гарантовано виявили всі вузли, верхня межа – щоб вузли помилково не прийняли його за дійсний кадр. Будь-який кадр, що має довжину меншу за 64 байт, вважається фрагментом зіпсованого колізією кадру і відкидається приймаючими вузлами.
2. Після відправлення сигналу затору об'єкт керування доступом до середовища перериває передачу, генерує випадковий час очікування і робить нову спробу виконати передачу кадру. Переривання передачі кадрів зменшує ефект колізії, а генерація випадкового часу очікування є деякою гарантією того, що колізія не виникне знову.

Якщо вузол передав останній біт кадру і не виявив при цьому колізії, він вважає, що кадр передано успішно. Якщо діаметр мережі перевищує припустиме значення, то в мережі виникають пропущені колізії (за 512 біт-тайм зіпсований колізією сигнал не встиг повернутися до вузла-відправника і він вважає, що передача кадру пройшла успішно і робить спробу передати наступний кадр). При виникненні пропущеної колізії таку ситуацію будуть

обробляти протоколи верхніх рівнів, однак при цьому суттєво збільшується кількість помилок передачі і знижується ефективна пропускна спроможність мережі.

В приймаючих вузлах зіпсовані колізією сигнали декодуються фізичним рівнем, фрагменти залучених до колізії кадрів розпізнаються об'єктом керування доступом до середи (приймаюча сторона) як недійсні кадри. Рівень MAC вузла буде відкидати будь-який кадр, що:

- має розмір < 64 байт;
- має неправильну контрольну суму;
- по довжині не складає ціле число октетів.

Як в специфікації Ethernet, так і в стандарті 802.3 використовується 1-наполегливий метод захоплення каналу. Після вдалої відправки кадру рівень MAC передаючого вузла повинен почекати деякий проміжок часу перед відправкою наступного кадру. Цей часовий інтервал називається міжпакетною щілиною (IPG). Його величина складає 9,6 мкс для 10 Мбіт/с і 0,96 мкс для 100 Мбіт/с.

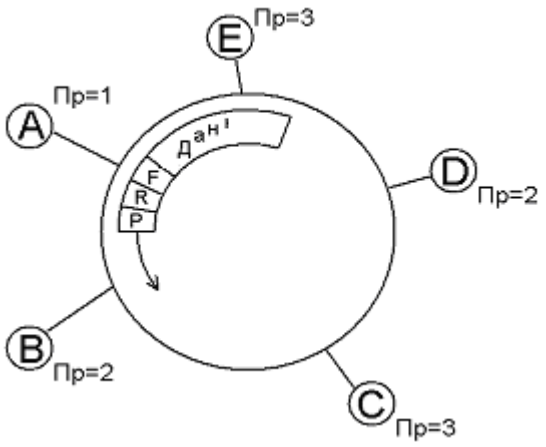
Таблиця 4.2 - Порівняльні характеристики протоколів Ethernet і 802.3

Характеристики	Ethernet	802.3
1. Топологія	Шина	шина, зірка
2. Середовище передачі	КК	КК, ВП, ВОК
3. Метод доступу	МДКН/ВК	МДКН/ВК
4. Тип кадру	Ethernet DIX	Будь-який

Метод МДКН/ВК достатньо ефективний тільки в умовах низького навантаження каналу (менш, ніж 30%) і невеликої кількості вузлів (10 - 12) на загальному каналі передачі. При більшому навантаженні каналу ефективність цього методу стрімко знижується (за рахунок збільшення числа колізій) і більш продуктивними в такому разі будуть детерміновані методи доступу (маркерні) або так званий комутований Ethernet (коли в якості центральних вузлів використовують комутатори).

Протокол стандарту 802.3 є подальшим розвитком протоколу Ethernet, і їх зазвичай ототожнюють. Тим не менш наявні деякі відмінності в цих протоколах (табл. 4.2).

4.4.3. Пріоритетне маркерне кільце (стандарт 802.5)



Пр – значення пріоритету вузла

P – поле пріоритету

R – поле резервування

F – прапорець маркеру (зайнятий/вільний)

A, B, C, D, E – вузли

Рисунок 4.27 - Передача маркеру по кільцю

Нехай вузол A захопив загальний канал для передачі даних. Цей вузол встановлює прапорець F в одиницю ("маркер зайнятий"), додає до маркеру кадр з даними і відправляє його в кільце (рис. 4.27). Маркер досягає вузла B, і, якщо в нього є дані для передачі, він записує власне значення пріоритету в поле резервування маркеру і відправляє маркер з даними далі в кільце. Вузол C аналізує значення в полі резервування і, так як його пріоритет більший за значення в цьому полі, він запише туди власне значення пріоритету, при цьому запам'ятовуючи в себе старе значення. Вузол D проаналізує поле резервування, визначить, що значення в цьому полі вище за його значення пріоритету, і без змін відправить маркер далі в кільце. У вузла E значення пріоритету співпадає зі значенням в полі резервування, тому він без змін відправить маркер з даними в кільце. Таким чином маркер виконає повний оберт. Станція-отримувач повинна помітити кадр прапорцем "прочитаний" (успішний прийом кадру).

Коли маркер з даними досягне вузла-відправника (А), цей вузол видалить кадр, перепише значення пріоритету з поля резервування в поле пріоритету (R=3 → P), помітить маркер прапорцем "вільний" (F=0) і відправить вільний кадр далі в кільце. Отримавши вільній кадр, вузол В аналізує поле пріоритету і, так як його пріоритет менший за значення в цьому полі, він не може захопити маркер і виконати передачу даних. Цей вузол може записати в поле резервування власне значення пріоритету і відправити вільний маркер далі в кільце. Так як пріоритет вузла С співпадає зі значенням в полі пріоритету маркеру, він захоплює маркер, помічає його прапорцем "зайнятий", додає до маркеру власний кадр і відправляє маркер з даними в кільце. Далі всі процедури повторюються. Для того, щоб низькопріоритетні вузли змогли виконати передачу при високій інтенсивності трафіку високопріоритетних вузлів, на кожному вузлі міститься спеціальний таймер. Якщо перевищене граничне значення, що вимірюється з моменту запису низького значення пріоритету в буфер вузла, то вузол, звільнивши маркер, повинен записати в поле пріоритету значення з власного буферу, понижуючи таким чином пріоритет вільного маркеру. Це дає можливість низькопріоритетному вузлу виконати передачу.

Стандарт 802.5 передбачає використання 3 форматів маркерів і кадрів з даними (рис. 4.28).

Формат маркеру складаються з трьох полів: початкового і кінцевого роздільників і поля керування доступом. Роздільники вказують на початок і кінець повідомлення. Поле керування доступом містить вісім бітів: три для індикації пріоритету, три для індикації резервування, Т-біт маркеру (Т=0 – вільний маркер, Т=1 – маркер з даними); М-біт використовується спеціальним моніторинговим вузлом з ціллю виявлення і усунення деяких помилкових ситуацій.

Маркер аварійного завершення може бути надісланий в будь-який момент для переривання попередньої передачі.

Поле керування кадром в маркері з даними вказує на тип кадру (кадр підрівня MAC або LLC) і може використовуватися для розподілення

пріоритетів між вказаними підрівнями канального рівня. Адресні поля ідентифікують отримувача і відправника (містять MAC-адреси). Поле даних містить пакет протоколу верхнього рівня. Поле контрольної послідовності кадру (КПК) використовується для виявлення помилок передачі за допомогою CRC. Поле стану кадру використовується для ідентифікації того, що приймаючий вузол отримав кадр і скопіював інформацію з поля даних в свій буфер.

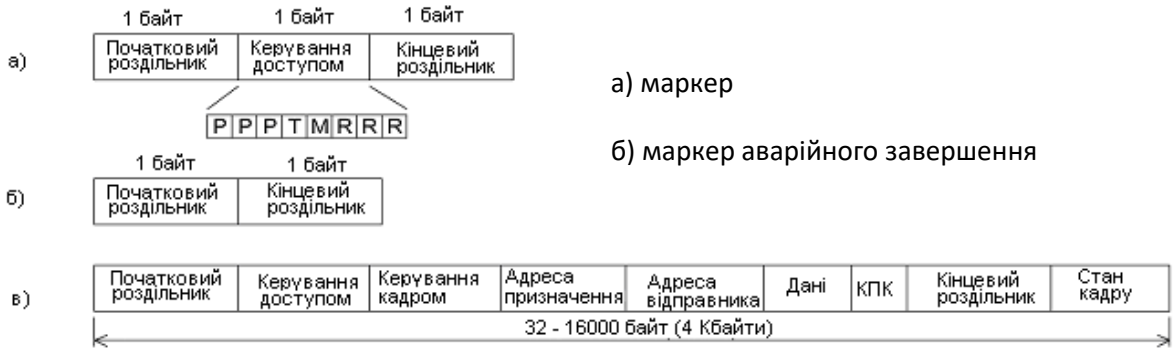


Рисунок 4.28 - Формат маркеру (а,б) і кадру даних (в)

В стандарті 802.5 також передбачені додаткові можливості керування роботою кільця і обробки помилкових ситуацій. Для цього можуть бути використані додаткові керуючі поля.

Особливості маркерного кільця фірми IBM

IBM розробила власну локальну мережу (специфікація IBM Token Ring), яка з невеликими змінами була покладена в основу стандарту 802.5

Формат кадру IBM Token Ring має наступний вигляд (рис. 4.29).

Поле фізичного керування відповідає полю керування доступом в маркері 802.5. Для підтримання цілісності мережі в маркерному кільці IBM завжди використовується моніторинговий вузол, що аналізує біт моніторингу в полі фізичного керування.

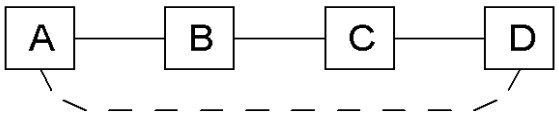
КПК – контрольна послідовність кадру

Рисунок 4.29 - Форрмат кадру IBM Token Ring

При проходженні маркеру з даними через моніторинговий вузол він встановить моніторинговий біт в одиницю. Коли маркер з даними зробить повний оберт по кільцю, вузол-відправник повинен звільнити маркер з даними і скинути моніторинговий біт в нуль. Якщо вузол-відправник не звільнить маркер (наприклад, вузол не існує), маркер з даними знову досягає моніторингового вузла. Той проаналізує моніторинговий біт і, так як там одиниця, він повинен видалити кадр з даними з мережі і згенерувати вільний маркер. Крім цього моніторинговий вузол обробляє помилкову ситуацію, пов'язану зі зникненням маркеру, використовуючи спеціальний таймер. Якщо впродовж заданого часу моніторинговий вузол не отримає з кільця вільний або зайнятий маркер, він згенерує новий і надішле його в кільце.

IBM пропонує наступні конфігурації ЛМ.

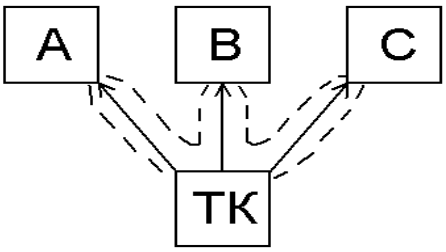
1. Послідовне магістральне сполучення.



Вузли підключені один за одним з обов'язковим збереженням кільцевої структури.

Недолік: ускладнений пошук несправностей і деякі складності при реконфігурації послідовної магістралі.

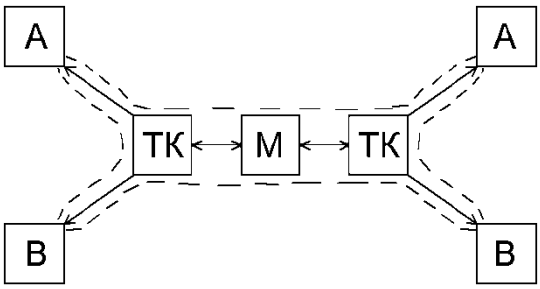
2. З'єднання через точки концентрації (ТК).



ТК – точка концентрації,

А, В, С – вузли.

3. Комбінований підхід – точки концентрації зв'язані за допомогою мостів в послідовну магістраль.



ТК – точка концентрації.

М – міст,

А, В – вузли.

Так як дозволяється організація мережі з декількох маркерних кілець, то для передачі даних з кільця в кільце використовується принцип маршрутизації відправника. Механізм маршрутизації відправника базується на вставці в кадр інформації про маршрут просунення. При цьому маршрутна інформація може формуватися з використанням наступних підходів.

1. Кожний вузол в мережі підтримує свою локальну маршрутну таблицю, яка містить маршрут до вузлів, з якими даний вузол найбільш інтенсивно обмінюється даними. Ця таблиця завантажується в кадр як частина поля даних і використовується проміжними мостами для прийняття рішення про ретрансляцію кадру через проміжні кільця.

2. Перед тим, як відправити кадр в кільце, вузол надсилає запит по своєму локальному кільцю, щоб визначити, чи знаходиться вузол-отримувач в цьому

локальному кільці. Якщо в локальному кільці вузол відсутній, то виконується загальний запит через всю мережу. Відповідь на запит буде містити необхідну маршрутну інформацію для передачі кадру від відправника до отримувача. Ця інформація поміщується відправником в кадр і буде використовуватися мостами для переправлення кадру через мережу (маршрутна інформація містить список мостів, які використовуються для передачі кадру). Передаючі вузли можуть використовувати чотири опції для формування маршрутних директив.

1. Широкомовлення рівня кільцевого сегменту – запит надсилається в межах локального кільця.

2. Обмежене широкомовлення – запит надсилається тільки один раз в кожне кільце.

3. Глобальне широкомовлення – по мережі розповсюджуються багато копій запитів, кожний з яких повинен з'явитися в кожному кільці хоча би одного разу.

4. Двоточкова маршрутизація – кадри передаються від вузла до вузла по визначеному маршруту і в передачі можуть бути задіяні тільки визначені мости і проміжні кільцеві сегменти.

Існує реалізація мереж IBM Token Ring зі швидкостями передачі 4 Мбіт/с, 16 Мбіт/с и 100 Мбіт/с. Незважаючи на явні переваги даної технології (насамперед, гарантована передача кадрів від кожного вузлу впродовж заданого проміжку часу), вона не витримала конкуренції із 100 Мбіт/с комутованою Ethernet-мережею і широкого розповсюдження не отримала.

В якості середи передачі може бути використана "вита пара" STP Type 1 (спеціалізований кабель IBM), UTP і волоконно-оптичний кабель.

Питання для самоперевірки та контролю засвоєння знань

1. Визначити, у якій архітектурі мережі усі вузли виконують однакові функції по керуванню доступом до мережі та мережних ресурсів.

2. Визначити, які мережі можна віднести до однорангових.

3. Визначити, які мережі можна віднести до клієнт-серверних.

4. Визначити, скільки ієрархічних рівнів має модель взаємодіє відкритих систем OSI.

5. Визначити, на якому рівні моделі OSI вирішуються задачі підтримки додатків користувача.

6. Визначити, на якому рівні моделі OSI вирішуються задачі логічної адресації пакетів.

7. Визначити, на якому рівні моделі OSI вирішуються задачі маршрутизації пакетів по мережі.

8. Визначити, на якому рівні моделі OSI формується кадр.

9. Визначити, на якому рівні моделі OSI вирішуються задачі управління потоком кадрів по каналу передачі.

10. Визначити, на якому рівні моделі OSI вирішуються задачі підключення до фізичного середовища передачі.

11. Визначити, на якому рівні моделі OSI вирішуються задачі перетворення кадрів у бітову послідовність.

12. Визначити, який з режимів передачі має механізми виявлення та виправлення помилок передачі.

13. Визначити, який з режимів передачі не має механізмів виявлення та виправлення помилок передачі.

14. Визначити, у якому з режимів передачі не виконується обмін службовою інформацією.

15. Визначити, у якому з режимів передачі використовується квітування даних.

16. Визначити, методи якої групи гарантують передачу даних від кожного вузла через загальний канал.

17. Визначити, методи якої групи не гарантують передачу даних від кожного вузла через загальний канал.

18. Визначити, до якої групи відносяться методи опиту/вибору.

19. Визначити, для чого використовують нумерацію кадрів в методах опиту/вибору.

20. Визначити, до якої групи відноситься метод ковзаючих вікон.

21. Визначити, для чого використовуються послідовності прийому та відправлення у методі ковзаючих вікон.

22. Визначити, за допомогою якого механізму визначається, що кадр передано з помилками у методі ковзаючих вікон.

23. Визначити, який метод передбачає повторну передачу тільки кадру з помилкою.

24. Визначити, який метод передбачає повторну передачу помилкового кадру та усіх кадрів, які були прийняті після нього.

25. Визначити, який метод організації повторної передачі помилкових кадрів більш ефективно використовує канал передачі.

26. Визначити, який метод організації повторної передачі помилкових кадрів задіє більше ресурсів вузла.

27. Визначити, які з методів відносяться до апаратних методів керування каналом передачі.

28. Визначити, які з методів відносяться до програмних методів керування каналом передачі.

29.Визначити до якої групи відноситься метод контролю несучої та виявлення колізій.

30. Визначити, скільки вузлів одночасно можуть вести передачу в загальний канал у методі МДКН/ВК.

31. Визначити, за допомогою якої процедури вузол визначає, що канал вільний у методі МДКН/ВК.

32. Визначити, у яку сторону від вузла розповсюджується сигнал в канал у методі МДКН/ВК.

33. Визначити, як прийомопередавач мережного адаптеру визначає, вільний чи зайнятий канал у методі МДКН/ВК.

34. Визначити, чи можлива у методі МДКН/ВК ситуація, коли декілька вузлів практично одночасно виконує передачу даних в загальний канал

35. Визначити, що характерно для колізії у методі МДКН/ВК.

36. Визначити, яким часовим параметром характеризується колізія у методі МДКН/ВК.

37. Визначити, які параметри визначають розмір вікна колізії в методі МДКН/ВК.

38. Дати оцінку, як зміниться розмір вікна колізії при збільшення протяжності мережі у методі МДКН/ВК.

39. Дати оцінку, як зміниться ймовірність виникнення колізій в методі МДКН/ВК при збільшення протяжності мережі.

40. Визначити, яка процедура використовується у методі МДКН/ВК для визначення колізій.

41. Визначити, чи можливе повторне виникнення колізій у методі МДКН/ВК.

42 Проаналізувати особливості та визначити, до якої групи належить метод маркерного кільця.

43. Визначити, коли вузол має право виконати передачу даних в загальний канал в методі «маркерного кільця».

44. Визначити, який вузол вивільняє маркер в методі «маркерного кільця».

45. Визначити, у який бік від вузла поширюється сигнал по загальному каналу в методі «маркерного кільця».

46. Визначити, коли вузол відправник має право повторно використати маркер для передачі наступного кадру в методі «маркерного кільця».

47. Проаналізувати особливості та визначити, до якої групи методів належить метод «маркерної шини».

48. Визначити, який вузол має право виконати передачу кадру в загальний канал в методі «маркерної шини».

49. Визначити, у який бік від вузла розповсюджується сигнал по загальному каналу в методі «маркерної шини».

50. Визначити, яку функцію забезпечує пріоритетна схема в пріоритетних маркерних системах.
51. Дати оцінку, чи можлива ситуація у пріоритетних системах, коли вузол з низьким пріоритетом не зможе провести передачу даних при високій інтенсивності високо пріоритетного трафіку.
52. Визначити, який набір стандартів визначає архітектуру та протоколи ЛОМ.
53. Визначити, яке поле кадру LLC використовується для визначення його границь.
54. Визначити, яка адреса використовується у кадрі протоколу LLC для ідентифікації відправника та одержувача.
55. Визначити, який метод управління каналом передачі використовується у протоколі LLC.
56. Визначити, який метод повторної передачі реалізовано у протоколі LLC.
57. Визначити, для яких цілей використовується поле «преамбула» в кадрі стандарту 802.3.
58. Визначити, яка адреса використовується у кадрі стандарту 802.3.
59. Визначити, для яких цілей використовується поле «початковий роздільник» в кадрі стандарту 802.3.
60. Визначити, яку довжину має фізична адреса в стандарті 802.3.
61. Визначити, яке поле фізичної адреси стандарту 802.3 вказує на те, що адреса є широкомовною.
62. Визначити, яке поле фізичної адреси стандарту 802.3 вказує на те, що адреса належить конкретному мережному адаптеру.
63. Визначити, яке поле фізичної адреси стандарту 802.3 вказує на те, що адреса надана мережному адаптеру виробником.
64. Визначити, яке поле фізичної адреси стандарту 802.3 вказує на те, що адреса надана мережному адаптеру користувачем.
65. Визначити, які поля фізичної адреси стандарту 802.3 виставлені у «1» в широкомовній адресі.

5. СТРУКТУРА СТЕКУ ПРОТОКОЛІВ TCP/IP

Стек TCP/IP, який одержав свою назву з популярних протоколів IP та TCP, був розроблений за ініціативою Міністерства оборони США більше 20 років назад для зв'язку експериментальної мережі ARPAnet з іншими мережами. Великий внесок у розвиток стека TCP/IP вклав університет Берклі, реалізувавши протоколи стека в своїй версії ОС UNIX. Популярність цієї операційної системи призвела до широкого розповсюдження протоколів TCP, IP і інших протоколів стека.

Стек TCP/IP представляє собою один з найпоширеніших стеків протоколів обчислювальних мереж [О: 2, 5, 6, 7; Д: 9, 10]. У стеку TCP/IP визначені 4 рівні:

- рівень мережних інтерфейсів (рівні 1 і 2 моделі OSI);
- мережний рівень або Інтернет-рівень (рівень 3 моделі OSI);
- транспортний рівень або основний рівень (рівні 4 і 5 моделі OSI);
- прикладний рівень (рівні 6 і 7 моделі OSI).

5.1. Характеристика рівнів стеку TCP/IP

Рівень мережних інтерфейсів

Основною відмінністю архітектури стека TCP/IP від багаторівневої організації інших стеків є інтерпретація функцій найнижчого рівня – рівня мережних інтерфейсів. Протоколи цього рівня повинні забезпечувати інтеграцію в будь-яку мережу незалежно від протоколів канального рівня, які в ній використовуються.

Задачу забезпечення інтерфейсу між стеком протоколів TCP/IP і будь-якими іншими протоколами передачі даних канального рівня можна звести до:

- визначення способу упаковки (інкапсуляції) IP-пакету в одиницю даних проміжної мережі, що передаються;

- визначення способу перетворення мережних адрес в адреси технології даної проміжної мережі.

Рівень мережних інтерфейсів в стеку TCP/IP реалізований набором інтерфейсних засобів для інкапсуляції IP-пакетів в кадри технологій канального рівня. Підтримуються всі популярні стандарти фізичного і канального рівнів: для локальних мереж це, наприклад, Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet; для глобальних мереж – протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay, ATM і т.д.

Мережний рівень (Інтернет-рівень)

Протоколи мережного рівня (IP, ICMP, ARP, RARP) підтримують інтерфейс з вищерозміщеним транспортним рівнем, отримуючи від нього запити на передачу даних по складеній мережі, а також з нижчерозміщеним рівнем мережних інтерфейсів. Завдання рівня полягає в забезпеченні можливості для кожного вузла посилати в будь-яку мережу пакети, які будуть незалежно рухатися до пункту призначення.

На мережному рівні основним протоколом є протокол міжмережної взаємодії IP (Internet Protocol). Основним завданням даного протоколу є доставка IP-пакетів до пунктів призначення. Протокол IP – це датаграмний протокол, що працює без встановлення з'єднань за принципом доставки з максимальними зусиллями.

Транспортний рівень (Основний рівень)

Оскільки на мережному рівні не встановлюються з'єднання, то немає ніякої гарантії, що всі пакети будуть доставлені в місце призначення цілими, або прийдуть в тому ж порядку, в якому вони були відправлені. Це завдання – забезпечення надійного інформаційного зв'язку між двома кінцевими вузлами – вирішує *основний рівень* стеку TCP/IP, що також зветься *транспортним*. До функцій цього рівня відноситься сегментація повідомлень верхніх рівнів для

пересилки по мережі, виконання математичних перевірок цілісності прийнятих даних і мультиплексування потоків даних (як тих, що передаються, так і таких, що приймаються) від декількох прикладних програм.

На цьому рівні існують два протоколи. Перший – TCP (Transmission Control Protocol – протокол управління передачею), який є надійним протоколом, що працює в режимі встановлення з'єднання і має засоби для виявлення і виправлення помилок передачі. Цей протокол дозволяє об'єктам одного рівня на комп'ютері-відправнику і комп'ютері-одержувачі підтримувати обмін даними в дуплексному режимі. Він розбиває вхідне повідомлення на окремі блоки даних (пакети) і передає їх мережному рівню. У пункті призначення TCP-процес збирає з одержаних блоків даних вихідний потік. Крім того, TCP має засоби управління потоком, що дозволяють уникнути перевантаження одержувача пакетами, що поступають.

Другий протокол цього рівня – UDP (User Datagram Protocol – протокол датаграм користувача), який є ненадійним протоколом, що працює в режимі без встановлення з'єднання, який використовується у тому випадку, коли завдання надійного обміну даними (підтвердження доставки, виявлення і виправлення помилок передачі) або взагалі не ставиться, або вирішується засобами більш високого рівня (прикладним рівнем або прикладними програмами користувача).

Прикладний рівень

Прикладний рівень об'єднує всі служби, що надаються системою прикладним програмам користувача. Стек TCP/IP накопичив велику кількість протоколів і служб прикладного рівня (FTP, HTTP, DNS, POP3, SMTP, telnet, тощо). Прикладний рівень реалізується програмними системами, побудованими по архітектурі сервер-клієнта, що базуються на протоколах нижніх рівнів. На відміну від протоколів інших трьох рівнів, протоколи прикладного рівня забезпечують підтримку конкретних прикладних програм і не залежать від

способів передачі даних по мережі. Цей рівень постійно розширюється за рахунок приєднання нових служб.

5.2. Особливості протоколу IP

Основу стеку протоколів TCP/IP складає протокол міжмережної взаємодії IP (Internet Protocol). Основне призначення протоколу – передавати пакети між мережами. У кожній черговій мережі, яка трапляється на шляху переміщення пакету, протокол IP викликає засоби доставки даних, прийняті в цій мережі (технології канального рівня), щоб з їх допомогою передати цей пакет на маршрутизатор, що веде до наступної мережі, або безпосередньо на вузол-одержувач.

Протокол IP є протоколом мережного рівня стека TCP/IP, який містить інформацію про адресацію і управляючу інформацію для маршрутизації пакетів. Протокол IP виконує дві основні функції.

1. Забезпечення передачі датаграм по об'єднаній мережі методом негарантованої доставки в режимі без встановлення з'єднання.

Протокол IP обробляє кожен IP-пакет як незалежну одиницю, що не має зв'язку ні з якими іншими IP-пакетами. У протоколі IP немає механізмів, що зазвичай використовуються для збільшення достовірності доставки даних: відсутнє квітування (обмін підтвердженнями між відправником і одержувачем), немає процедури впорядкування, повторних передач або інших подібних механізмів. Якщо під час просування пакету відбулася яка-небудь помилка, то протокол IP нічого не робить для виправлення цієї помилки. Всі питання забезпечення надійності доставки даних по складеній мережі в стеку TCP/IP вирішує протокол TCP, працюючий безпосередньо над протоколом IP. Саме TCP організовує повторну передачу пакетів, коли в цьому виникає потреба.

2. Забезпечення фрагментації і повторної збірки датаграм для підтримки каналів передачі даних з різними розмірами максимальної одиниці передачі даних (MTU – Maximum Transfer Unit).

Важливою особливістю протоколу IP, що відрізняє його від інших мережних протоколів (наприклад, від мережного протоколу IPX), є його здатність виконувати динамічну фрагментацію пакетів при передачі їх між мережами з різними, максимально допустимими значеннями MTU.

Формат IP-пакету має наступний вигляд (рис. 5.1).

Рисунок 5.1 - Формат IP-пакету

Пакет складається з таких полів.

- ***Номер версії*** характеризує версію IP-протоколу (наприклад, 4 або 6).
- ***Довжина IP-заголовка (Загальна довжина)***. Довжина заголовка датаграми в 32-розрядних словах; зазвичай заголовок містить 20 октетів (HLEN=5).
- ***Тип сервісу*** (ToS – type of service). Задає потрібний протоколам верхнього рівня спосіб обробки поточної датаграми і привласнює датаграмам різні ступені

важливості, характеризуючи те, як повинна оброблятися датаграма. Це поле ділиться на 6 субполів (рис. 5.2).

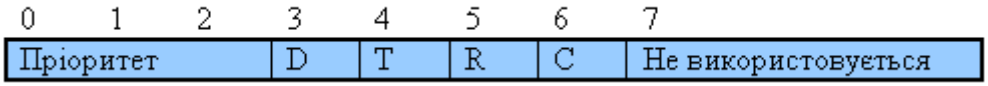


Рисунок 5.2 - Структура поля тип сервісу

Субполе “Пріоритет” надає можливість привласнити код пріоритету кожній датаграмі. Код пріоритету може приймати значення від 0 (звичайний пріоритет) до 7 (мережне управління). Це поле призначене для забезпечення якості обслуговування (QoS) при передачі датаграми.

Біти C, D, T і R характеризують деякі вимоги до способу доставки датаграми. Так D=1 вимагає мінімальної затримки, T = 1 – високу пропускну здатність, R = 1 – високу надійність, а C = 1 – низьку вартість.

Поле ToS враховується при маршрутизації пакетів (передача пакетів через Інтернет не гарантує запрошеного ToS, але багато маршрутизаторів враховують ці запити при виборі маршруту, наприклад, при використанні протоколів OSPF і IGRP).

Тільки один біт з чотирьох в ToS може приймати значення “1”. Значення за умовчанням дорівнюють нулям.

До середини 90-х років поле ToS в більшості реалізацій ігнорувалося. Але після початку розробок засобів забезпечення якості обслуговування (QoS) увага до нього зросла. З'явилася пропозиція заміни поле ToS на поле DSCP (Differentiated Services Code Point) – код точки диференціальної послуги, яке також має 8 біт (рис. 5.3). Іноді це поле називається байтом DS (Differentiated Services).

Біти CU поки не визначені. Біти DS0-DS5 визначають селектор класу. Значення цього коду представлені в таблиці 5.1. Стандартним значенням DSCP за умовчанням є 000000.

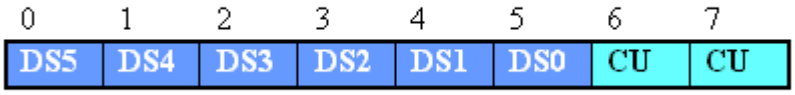


Рисунок 5.3 - Формат поля DSCP.

Таблиця 5.1 - Сумісність поля DSCP з байтом ToS

Пріоритет (байт ToS)	DSCP
Пріоритет 1	001000
Пріоритет 2	010000
Пріоритет 3	011000
Пріоритет 4	100000
Пріоритет 5	101000
Пріоритет 6	110000
Пріоритет 7	111000

- ***Загальна довжина.*** Довжина всього IP-пакету в байтах, визначає повну довжину IP-датаграми (до 65535 октетів), включаючи заголовок і дані.
- ***Ідентифікатор пакету.*** Є унікальним кодом датаграми, що дозволяє ідентифікувати приналежність фрагментів і виключити помилки при "збірці" датаграм.
- ***Прапори.*** Трьохрозрядне поле, в якому 2 молодших біта управляють фрагментацією. Молодший біт (M) визначає, чи може пакет бути фрагментований (0 – фрагментація дозволена; 1 – заборонена), а середній (D) – чи є пакет останнім в серії фрагментованих пакетів (0 – останній фрагмент; 1 – слід чекати продовження). Третій (старший) біт не використовується.
- ***Зміщення фрагмента.*** Позиція даних фрагмента відносно початку даних в початковій датаграмі, що дозволяє IP-процесу правильно відновити початкову датаграму.
- ***Час життя*** (***TTL*** – time to live**).** Лічильник, який поступово зменшується до нуля, після чого датаграма відкидається маршрутизатором, щоб уникнути нескінченного циклу передачі пакетів.

- ***Ідентифікатор протоколу*** верхнього рівня. Указує на протокол верхнього рівня, що приймає вхідні пакети після закінчення обробки їх протоколом IP.
- ***Контрольна сума заголовка.*** Використовується для перевірки цілісності IP-заголовка.
- ***Адреса джерела.*** Визначає вузол-відправник.
- ***Адреса одержувача.*** Визначає вузол-приймач.
- ***Поле опції і вирівнювання.*** Поле опції є необов'язковим і, зазвичай, використовується тільки при відладці мережі. Механізм опцій надає функції управління, які необхідні при певних ситуаціях (можна вказати точний маршрут проходження пакетів, реєструвати маршрутизатори, які проходить пакет, поміщати часові мітки і т.п.) Розмір поля опції залежить від того, які опції застосовані. Якщо використовується декілька опцій, вони записуються підряд без будь-яких роздільників. Кожна опція містить один октет коду опції, за яким може слідувати октет довжини і серія октетів даних. Якщо розмір заголовка не кратний 4-м октетам (32 бітам) використовується заповнювач – додаткові біти заповнюються нулями.

5.3. Особливості IP- адресації

Типи адрес стека TCP/IP

У стеку TCP/IP використовуються два типи адрес вузлів: фізична (або, апаратна) і IP-адреса. Крім адреси вузол може мати символьне доменне ім’я.

У термінології TCP/IP під ***фізичною адресою*** розуміється такий тип адреси, яка використовується засобами базової технології для доставки даних канального рівня (наприклад, MAC – адреси в технології Ethernet).

IP-адреса є основним типом адреси, на підставі якої мережний рівень передає пакети між мережами. IP-адреса призначається адміністратором під час конфігурації комп'ютерів і маршрутизаторів. IP-адреса вузла призначається незалежно від локальної адреси вузла. Кінцевий вузол може належати до

декількох IP-мереж. В цьому випадку вузол повинен мати декілька IP-адрес, по числу мереж, до яких він належить. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а належність вузла конкретній логічній IP-мережі.

Символьні доменні імена

Символьні імена в IP-мережах називаються доменними і будуються за ієрархічним принципом. Складові повного символьного імені в IP-мережах (FQDN – Fully Qualified Domain Name) розділяються крапкою і перераховуються в наступному порядку: спочатку просте ім'я кінцевого вузла (HOST name – ім’я хоста) , потім ім'я групи вузлів, до якої належить вузол (наприклад, ім'я організації), потім ім'я крупнішої групи, до якої належить ім’я організації і так до імені домена самого високого рівня (наприклад, домена об'єднуючого організації за географічним принципом: UA - Україна). Прикладом доменного імені може служити ім'я www.kpi.ua, яке закріплене за ВЕБ-сервером. Для встановлення відповідності між доменним ім'ям і IP-адресою вузла використовують додаткові таблиці або служби. У мережах TCP/IP для вирішення цієї задачі використовується спеціальна розподілена служба DNS (Domain Name System – система доменних імен). Тому доменні імена називають також DNS-іменами.

5.3.1. Класи IP-адрес

IP-адреса має довжину 4 байти і, зазвичай, записується у вигляді чотирьох десяткових чисел, що представляють значення кожного байта в десятковій формі і розділених крапками, наприклад, 128.10.2.30 - традиційна десяткова форма представлення IP- адреси (двійкова форма представлення цієї ж адреси має вигляд 10000000 00001010 00000010 00011110).

Адреса складається з двох логічних частин - номери мережі і номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка - до номера вузла, визначається, так званою, маскою. ***Маска*** - це число, яке використовується в парі з IP-адресою; двійковий запис маски містить одиниці в

тих розрядах, які в IP-адресі належать до номеру мережі. Оскільки номер мережі є цілісною частиною адреси, одиниці в масці також повинні представляти безперервну послідовність.

Усі IP-адреси поділені на 5-ть класів. Структура класів IP-адрес наведена на рис. 5.4. Належність конкретної IP-адреси класу визначається значеннями перших біт двійкового значення адреси.

Якщо перший біт двійкового значення адреси «0», то адресу відносять до класу A. Стандартна маска мережі класу A – 255.0.0.0 (11111111 00000000 00000000 00000000 у двійковому вигляді). Номер мережі займає один байт, останні 3 байти інтерпретуються як номер вузла в мережі. В цей діапазон потрапляють десяткові значення номерів мереж від 0 до 127. З урахуванням того, що номер «0» не використовується, а номер «127» зарезервований для спеціальних цілей, мережі класу A можуть мати десяткові номери в діапазоні від 1 до 126. Мереж класу A небагато, зате кількість вузлів в них може досягати 2 в 24 ступені, тобто 16 777 216 вузлів.

Якщо перші два біти двійкового значення адреси «10», то мережа відноситься до класу B. Стандартна маска мережі класу B – 255.255.0.0 (11111111 11111111 00000000 00000000 у двійковому вигляді). В мережах класу B під номер мережі і під номер вузла відводиться по 2 байти. Таким чином, мережа класу B є мережею середніх розмірів з максимальним числом вузлів 2 в 16 ступені, що складає 65 536 вузлів.

Якщо перші три біти двійкового значення адреси «110», то це мережа класу C. Стандартна маска мережі класу C – 255.255.255.0 (11111111 11111111 11111111 00000000 у двійковому вигляді). В цьому випадку під номер мережі відводиться 3 байти, а під номер вузла - 1 байт. Мережі цього класу найбільш поширені, число вузлів в них не перевищує 2 в 8 ступені, тобто 256 вузлів.

Якщо перші чотири біти двійкового значення адреси «1110», то це адреса мережі класу D. Це, так звана, групова , або multicast - адреса. Така адреса призначається групі вузлів, які повинні отримувати одні й ті ж самі пакети (наприклад, пакети відеопотоку, або каналу IP-TV). Пакет з адресою

призначення класу D отримають усі вузли, які підключилися до даної групи. Такі вузли будуть мати унікальну (unicast) IP-адресу і групову (multicast) адресу. В адресах класу D не використовується розподілення на номер мережі і номер вузла, тому маска для цього класу адрес не застосовується.

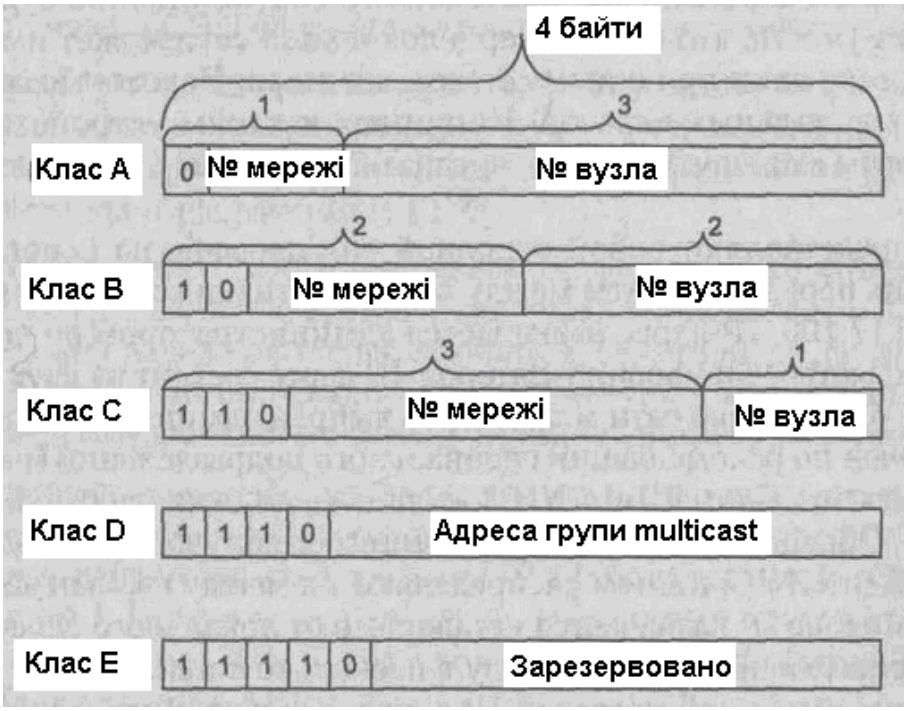


Рисунок 5.4 - Структура класів IP-адрес

Якщо перші п’ять бітів двійкового значення адреси «11110», то це адреса класу E. Адреси цього класу зарезервовані для майбутніх застосувань.

У табл. 5.2 приведені діапазони номерів мереж і максимальне число вузлів, для кожного класу мереж.

Таблиця 5.2 - Характеристики адрес різного класу

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів в мережі
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.0.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервований

5.3.2. Особливі типи IP-адрес

У протоколі IP існує декілька типів особливих IP-адрес. Це:

- «нульова» адреса (0.0.0.0). Така адреса в адресному полі відправника пакету вказує на вузол, який згенерував цей пакет. Прикладом такого пакету є пакет від DHCP-клієнту, який від направляє по мережі для пошуку DHCP-серверу та отримання від нього унікальної IP-адреси;

- обмежена (локальна) «широкомовна» (*limited/local broadcast)* адреса (255.255.255.255). Така адреса може з'явитись тільки в адресному полі призначення пакету. Пакет з такою адресою отримають усі вузли, які знаходяться в тій же IP-мережі, що і вузол, який згенерував даний пакет. В інші IP-мережі такі пакети не передаються (маршрутизатори не пересилають локальні широкомовні пакети на інші свої інтерфейси) Така розсилка називається *обмеженим широкомовним повідомленням;*

- «широкомовна» (*broadcast)* адреса (наприклад, 192.168.1.255) – має конкретний номер мережі і усі двійкові одиниці в полі номера вузла. Пакет з такою адресою в адресному полі призначення пакету, розсилається усім вузлам мережі із заданим номером. Така розсилка називається *направленим широкомовним повідомленням;*

- адреса мережі (наприклад, 192.168.1.0) – така адреса має конкретний номер мережі і усі двійкові нулі в полі номера вузла. Використовується тільки в таблицях маршрутизації для визначення маршруту до конкретної мережі і не може з'явитися у адресних полях IP-пакету;

- адреса «зворотної петлі» (*loopback*). Це адреса з десятковим значенням номера мережі «127» (наприклад, 127.0.0.1). Пакети з такою адресою ніколи не передаються через мережний інтерфейс вузла і використовуються для тестування програм і взаємодії процесів в межах одного вузла. Коли програма посилає дані на IP-адресу 127.0.0.1, то утворюється, так звана, «петля». Дані не передаються по мережі, а повертаються процесам верхнього рівня, як тільки що прийняті.

При адресації вузлів необхідно враховувати обмеження, які вносяться особливим призначенням спеціальних IP-адрес. Так, ні номер мережі, ні номер вузла не може складатися тільки з одних двійкових одиниць або тільки з одних двійкових нулів. Звідси витікає, що максимальна кількість вузлів, приведена в таблиці 1.2 для мереж кожного класу, на практиці повинна бути зменшене на 2. Наприклад, в мережах класу С під номер вузла відводиться 8 біт, що дозволяє задавати 256 номерів від 0 до 255. Але з урахуванням спеціальних типів IP-адрес, вузлам можуть призначатися номери з 1-го по 254-й і максимальна кількість вузлів в мережі класу С не може перевищувати 254 (наприклад, адреса 192.168.1.0 вказує на усю мережу з номером «192.168.1», а адреса 192.168.1.255 є направленою широкомовною адресою в мережу з номером «192.168.1»). Існує ще таке загальне узгодження - якщо в адресному полі призначення пакету в IP-адресі в полі номера мережі записані тільки нулі, то вважається, що вузол призначення належить тій же самій мережі, що і вузол, який відправив цей пакет.

Вже згадувана вище групова IP-адреса типу *multicast* - означає, що даний пакет повинен бути доставлений відразу декільком вузлам, які належать до групи з такою адресою. Один і той же вузол може входити в декілька груп. У одну групу multicast можуть входити вузли з різних IP-мереж, зв’язаних маршрутизаторами. Пакети з груповою адресою обробляється маршрутизаторами особливим образом.

Адреси з 224.0.0.0 до 224.0.0.255 зарезервовані для мережних протоколів локальних мережних сегментів. Пакети з такими адресами ніколи не проходять через маршрутизатор. Їх час життя (TTL) завжди встановлюється рівним 1.

Мережні протоколи використовують ці адреси для автоматичного виявлення маршрутизатора і для передачі важливої маршрутної інформації Наприклад, протокол OSPF використовує адреси 224.0.0.5 і 224.0.0.6 для обміну інформацією про стан каналу .

Адреси в діапазоні від 224.0.1.0 до 238.255.255.255 є глобальними. Вони можуть використовуватися для групової передачі даних між організаціями і для передачі по мережі Internet.

У діапазоні від 239.0.0.0 до 239.255.255.255 адреси зарезервовані для внутрішнього використання у приватних мережах.

Основне призначення multicast-адрес - розповсюдження інформації по схемі «один-до-багатьох». Вузол (наприклад сервер IP-TV), який хоче передавати одну і ту ж інформацію багатьом абонентам, за допомогою спеціального протоколу IGMP (Internet Group Management Protocol) повідомляє про створення в мережі нової multicast-групи з певною адресою. Маршрутизатори поширюють інформацію про створення нової групи в мережах, підключених до своїх інтерфейсів. Вузли, які хочуть приєднатися до новоствореної групи, повідомляють про це свої локальні маршрутизатори і ті передають цю інформацію вузлу, який ініціював створення нової групи.

Для того, щоб маршрутизатори могли автоматично передавати пакети з адресами multicast через проміжні IP-мережі, необхідно використовувати в маршрутизаторах модифіковані протоколи обміну маршрутною інформацією, такі як, наприклад, MOSPF (Multicast OSPF).

Локальні адреси.

В IPv4 виділено декілька блоків адрес, які призначені для локального використання, та не можуть бути глобально маршрутизованими (доступними з будь-якого пристрою, що підключений до мережі Інтернет). Так для приватних IP - адрес ("сірих IP") зарезервовано близько 18 млн адрес. Серед них виділяють два основні блоки: канальні адреси (Link-local - 169.254.0.0/16) та адреси для використання у приватних мережах (клас A - 10.0.0.0/8, клас B - 172.16.0.0/12, клас C - 192.168.0.0/16).

Link-local address — адреси, які призначені тільки для комунікацій в межах одного сегмента локальної мережі або магістральної лінії (один домен широкомовлення). Вони дозволяють звертатися до вузлів, не використовуючи загальний префікс адреси (наприклад, замість адреси 169.254.0.1 може бути

використана адреса 0.0.0.1). Маршрутизатори не передають пакети з адресами отримувача link-local (TTL в таких пакетах дорівнює «1»). Адреси link-local часто використовуються при автоматичному призначенні мережної адреси, у випадках, коли зовнішні джерела для отримання адреси недоступні. Приклад використання link-local адрес — проблеми при автоматичному конфігуруванні IP-адрес. Адреси IPv4 в діапазоні від 169.254.0.0 до 169.254.255.255 призначаються ОС вузла автоматично в разі недоступності DHCP сервера.

5.3.3. Використання масок для сегментації IP- мереж

Як вже було зазначено вище двійковий запис *маски* містить одиниці в тих розрядах, які в IP-адресі належать до номеру мережі. Таким чином, маска визначає кількість старших біт в IP-адресі, виділених під адресацію мережі. Інші біти в IP-адресі визначають номер вузла в даній мережі. Нагадаємо, що існує поняття «стандартної» маски для кожного класу IP-адрес (клас A - 255.0.0.0; клас B - 255.255.0.0; клас C - 255.255.255.0). Існує ще один варіант запису маски - /N, де N – кількість одиничних біт у масці (наприклад, стандартна маска класу A - /8, B - /16, C - /24). Такий тип запису використовується у маршрутних записах в таблицях маршрутизації на маршрутизаторах та адміністраторами при документуванні логічної структури мережі.

Механізм масок дозволяє провести сегментацію конкретної IP-мережі на підмережі меншого розміру, забезпечуючи більш гнучку систему адресації. Наприклад, якщо адресу 77.47.130.1 використовувати з маскою 255.255.255.0, то номером мережі буде 77.47.130.0, а не 77.0.0.0, як це визначено стандартною маскою класу A, до якого належить адреса 77.47.130.1.

У «нестандартних» масках, які використовуються для сегментації мережі, кількість одиниць в послідовності, що визначає межу номера мережі, не обов'язково повинно бути кратним 8, щоб повторювати ділення адреси на байти. Наприклад, для сегментації мережі класу B на дві підмережі необхідно

розширити кількість біт, відведених під номер мережі на 1, тобто використати маску 255.255.128.0. У цьому прикладі для нумерації мереж виділено 17 біт, для адресації вузлів 15 біт. Наприклад,

IP-адреса 129.64.134.5 (10000001.01000000.10000110.00000101),

маска 255.255.128.0 (11111111.11111111.10000000.00000000).

Така комбінація IP-адреси і маски визначає належність вузла з номером 0.0.6.5 до підмережі з номером 129.64.128.0.

Якщо в наведеному прикладі IP-адреси 129.64.134.5 використати стандартну маску мережі класу B, то номером мережі будуть перші 2 байти - 129.64.0.0, а номером вузла - 0.0.134.5.

Механізм масок широко поширений в IP-маршрутизації, причому маски можуть використовуватися для самих різних цілей. З їх допомогою адміністратор може сегментувати свою мережу на окремі IP-мережі без використання додаткових блоків IP-адрес. На основі цього ж механізму можна об'єднувати адресні простори декількох мереж шляхом введення так званих «префіксів» з метою зменшення об'єму таблиць маршрутизації і зменшення, відповідно, навантаження на маршрутизатори.

Поділення на підмережі та агрегування адрес.

Існує два типи операцій, пов'язаних з накладенням маски на IP-адресу:

- агрегування (superneting), коли маска зрушується вліво по полю номера мережі (виділяється загальна кількість біт в ідентифікаторі мережі, однакових для усіх підмереж); при цьому частина адреси, яка виділяється маскою, називається префіксом. Отримана маска має менше значення ніж стандартна маска даного класу мереж (у випадку IPv4);
- розбивка єдиного номера мережі на кілька номерів підмереж за допомогою масок, що використовують частину області номера вузла (subneting).

В IPv4 використовуються і перший (агрегування), і другий (розподіл на підмережі) типи операцій. Агрегування виконують провайдери, правильно виділяючи пули адрес великим абонентам і більш дрібним провайдерам,

налаштовуючи відповідним чином свої маршрутизатори. Мета такої операції – скорочення адресних таблиць маршрутизаторів. Операції другого типу виконуються адміністраторами корпоративних мереж для структуризації мережі (поділу її на підмережі) в умовах дефіциту номерів мереж.

Техніка агрегування має назву безкласової міждоменної маршрутизації (Classless Inter-Domain Routing, CIDR). Суть технології CIDR полягає в наступному. Кожному провайдеру призначається безперервний діапазон у просторі IP-адрес. При такому підході адреси всіх мереж кожного провайдера мають загальну частину в старших розрядах – префікс. В результаті, маршрутизація на магістралях Internet може здійснюватися на основі префіксів, а не повних адрес мереж. Коли клієнт (ним може виявитися й більш дрібний провайдер) звертається до провайдера із проханням про виділення йому деякої кількості адрес, то в наявному пулі адрес "вирізається" безперервна область відповідного розміру. Причому границі цієї області вибираються такими, щоб для нумерації необхідного числа вузлів вистачило деякого числа молодших розрядів, а значення всіх старших розрядів, що залишилися, були однаковими, створюючи префікс адреси даного провайдера-клієнта.

Розглянемо приклад використання механізмів поділу на підмережі та агрегування адміністратором корпоративної мережі (рис. 5.5).

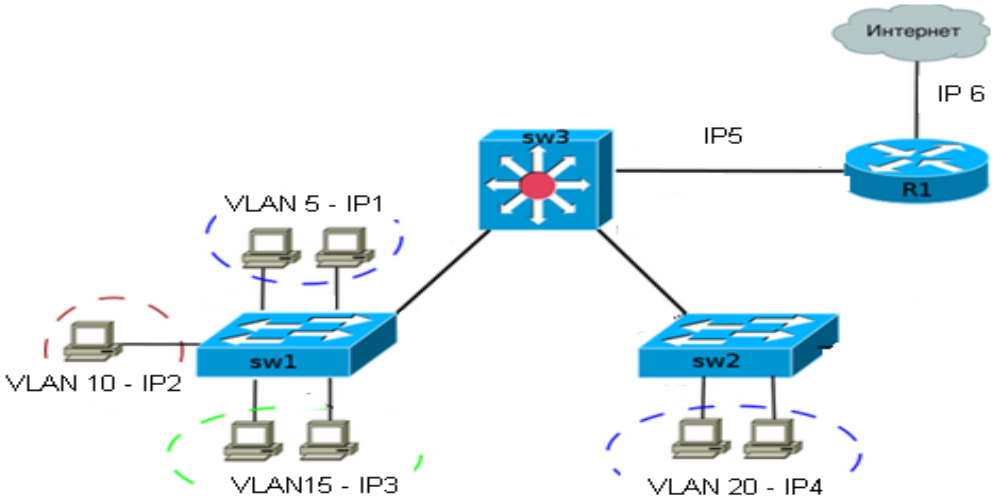


Рисунок 5.5 – Приклад логічної структури корпоративної мережі

Маємо блок адрес для внутрішнього використання 192.168.10.0/24, який необхідно поділити на 4-ри підмережі (VLAN 5, 10, 15, 20).

Розширена маска - /26 (255.255.255.192).

Підмережі:

IP 1 – 192.168.10.0/26 (адреси вузлів 192.168.10.1 – 192.168.10.62),

IP 2 – 192.168.10.64/26 (адреси вузлів 192.168.10.65 – 192.168.10.126),

IP 3 – 192.168.10.128/26 (адреси вузлів 192.168.10.129 – 192.168.10.190),

IP 4 – 192.168.10.192/26 (адреси вузлів 192.168.10.193 – 192.168.10.254).

Маршрутні записи в таблиці маршрутизації маршрутизатора R без агрегування будуть мати вигляд, наведений на рис. 5.6.

Використаємо для агрегування скорочену маску /24. Маршрутні записи в таблиці маршрутизації маршрутизатора R з використанням агрегування будуть мати вигляд, наведений на рис. 5.7. Як видно з рис. 5.7, агрегування адрес дозволяє зменшити обсяг таблиць у маршрутизаторах всіх рівнів, тому що всі мережі з однаковим префіксом представлені в таблиці маршрутизації одним записом.

№ запису	IP мережа призначення	Проміжна мережа	Примітка
1	192.168.10.0/26	IP 5	Маршрут доступу до вузлів VLAN 5
2	192.168.10.64/26	IP 5	Маршрут доступу до вузлів VLAN 10
3	192.168.10.128/26	IP 5	Маршрут доступу до вузлів VLAN 15
4	192.168.10.192/26	IP 5	Маршрут доступу до вузлів VLAN 20
5	0.0.0.0/0 (default)	IP 6	Маршрут доступу до вузлів в Internet

Рисунок 5.6 – Приклад таблиці маршрутизації без агрегування маршрутів

№ запису	IP мережа призначення	Проміжна мережа	Примітка
1	192.168.10.0/24	IP 5	Маршрут доступу до вузлів VLAN 5 - 20
2	0.0.0.0/0 (default)	IP 6	Маршрут доступу до вузлів в Internet

Рисунок 5.7 – Приклад таблиці маршрутизації з використанням агрегування маршрутів

5.4. Протокол ICMP

ICMP (Internet Control Message Protocol – міжмережний протокол управляючих повідомлень). ICMP використовується для передачі повідомлень про помилки і інші виняткові ситуації, що виникли при передачі даних. Також на ICMP покладаються деякі сервісні функції.

ICMP дозволяє маршрутизатору повідомити кінцевий вузол про помилки, з якими він зіткнувся при передачі будь-якого IP-пакету від даного кінцевого вузла. При цьому управляючі повідомлення ICMP не можуть посилатися проміжному маршрутизатору, який брав участь в передачі пакету, з яким виникли проблеми. Це пов'язано з тим, що для такої посилки немає адресної інформації. Пакет несе в собі тільки адресу джерела і адресу призначення, не фіксуючи адреси проміжних маршрутизаторів.

Протокол ICMP – це протокол повідомлення про помилки, а не протокол корекції помилок. Кінцевий вузол може зробити деякі дії для того, щоб помилка більше не виникала, але ці дії протоколом ICMP не регламентуються.

Протокол ICMP генерує декілька видів повідомлень, зокрема повідомлення про недоступність одержувача, перенаправлення маршруту, закінчення ліміту часу, анонсування маршрутизатора, а також запити маршрутизатора: ехо-запит і ехо-відповідь. Кожне повідомлення протоколу ICMP передається по мережі усередині пакету IP. Пакети IP з повідомленнями ICMP маршрутизуються

точно так, як і будь-які інші пакети. Якщо ICMP-повідомлення не може бути доставлено, інше таке повідомлення не створюється щоб уникнути нескінченного потоку ICMP-повідомлень.

5.4.1. Формат повідомлень протоколу ICMP

Кожен тип повідомлення має свій формат, при цьому всі вони починаються із загальних трьох полів: 8-бітового цілого числа, що позначає тип повідомлення (TYPE), 8-бітового поля коду (CODE), який конкретизує призначення повідомлення, і 16-бітового поля контрольної суми (CHECKSUM) (рис.5.8).

Крім того, повідомлення ICMP завжди містить заголовок і перші 64 біти даних пакету IP, який викликав помилку. Це робиться для того, щоб вузол-відправник зміг точніше проаналізувати причину помилки, оскільки всі протоколи прикладного рівня стека TCP/IP містять найбільш важливу інформацію для аналізу в перших 64 бітах своїх повідомлень.

Поле типу може мати значення, наведені в таблиці 5.3.

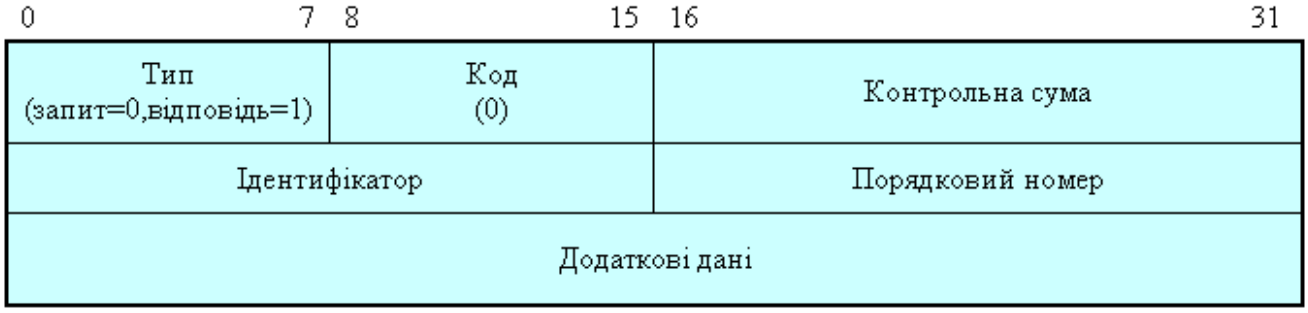


Рисунок 5.8 - Пакет exo-повідомлення запит/відповідь протоколу ICMP

5.4.2. Типи повідомлень ICMP

Exo-протокол

Протокол ICMP надає мережним адміністраторам засоби для тестування досяжності вузлів мережі. Ці засоби представляють собою дуже простий ехо-протокол, що включає обмін двома типами повідомлень: ехо-запит і ехо-відповідь. Комп'ютер або маршрутизатор посилають по мережі ехо-запит, де вказують IP-адресу вузла, досяжність якого потрібно перевірити. Вузол, який одержує ехо-запит, формує і відправляє ехо-відповідь і повертає повідомлення вузлу-відправнику запиту. У запиті можуть міститися деякі дані, які повинні бути повернені в відповіді. Оскільки ехо-запит і ехо-відповідь передаються по мережі усередині IP-пакетів, то їх успішна доставка означає нормальне функціонування всієї транспортної системи інтермережі.

Таблиця 5.3 - Коди поля типу пакету ICMP

Значення	Тип повідомлення
0	Ехо-відповідь (Echo Replay)
3	Вузол призначення недосяжний (Destination Unreachable)
4	Пригнічення джерела (Source Quench)
5	Перенаправлення маршруту (Redirect)
8	Ехо-запит (Echo Request)
11	Закінчення часу датаграми (Time Exceeded for a Datagram)
12	Проблема з параметром пакету (Parameter Problem on a Datagram)
13	Запит відмітки часу (Timestamp Request)
14	Відповідь відмітки часу (Timestamp Replay)
17	Запит маски (Address Mask Request)
18	Відповідь маски (Address Mask Replay)

У багатьох операційних системах використовується утиліта *ping*, яка призначена для тестування досяжності вузлів. Ця утиліта зазвичай посилає серію ехо-запитів до вузла, який тестується, і надає користувачу статистику про загублені ехо-відповіді і середній час реакції мережі на запити.

Повідомлення про недосяжність вузла призначення

Якщо маршрутизатор посилає повідомлення про недосяжність одержувача, то це означає, що маршрутизатор неспроможний передати пакет за кінцевою адресою призначення. Тоді маршрутизатор відкидає початковий пакет. Недоступність одержувача може бути викликана двома причинами. Частіше всього це відбувається тому, що початковий вузол вказує неіснуючу адресу. Рідше виникає ситуація, коли у маршрутизатора відсутній маршрут до вузла-одержувача.

Повідомлення про недоступність одержувача діляться на чотири основні типи: недоступність мережі, вузла, протоколу і порту. Повідомлення про недоступність мережі зазвичай означають помилку в маршрутизації або адресації пакетів. Повідомлення про недоступність вузла зазвичай вказують на помилку доставки, таку як невірна маска підмережі. Повідомлення про недоступність протоколу зазвичай означають, що вузол-одержувач не підтримує протокол верхнього рівня, вказаний в пакеті. Під повідомленням про недоступність порту мається на увазі, що зайняті TCP-сокет або порт.

Коли маршрутизатор не може передати або доставити IP-пакет, він посилає вузлу, що відправив цей пакет, повідомлення "Вузол призначення недосяжний" (тип повідомлення – 3). Це повідомлення містить в полі коду значення, що уточнює причину, через яку пакет не був доставлений. Причина кодується таким чином (таблиця 5.4.).

Маршрутизатор, який виявив, що з будь-якої причини не може передати IP-пакет далі по мережі, повинен відправити ICMP-повідомлення вузлу-джерелу, і тільки потім відкинути пакет. Окрім причини помилки, ICMP-повідомлення включає також заголовок недоставленого пакету і його перші 64 біти поля даних.

Помилка фрагментації виникає тоді, коли відправник послав в мережу пакет з ознакою DF (біт “M” у прапорі IP пакету), що забороняє фрагментацію, а маршрутизатор зіткнувся з необхідністю передачі цього пакету в мережу із значенням MTU меншим, ніж розмір пакету.

Таблиця 5.4 - Помилки ICMP

Код	Причина
0	Мережа недосяжна
1	Вузол недосяжний
2	Протокол недосяжний
3	Порт недосяжний
4	Потрібна фрагментація, а біт DF встановлений
5	Помилка в маршруті, заданому джерелом
6	Мережа призначення невідома
7	Вузол призначення невідомий
8	Вузол-джерело ізольований
9	Взаємодія з мережею призначення адміністративно заборонена
10	Взаємодія з вузлом призначення адміністративно заборонена
11	Мережа недосяжна для заданого класу сервісу
12	Вузол недосяжний для заданого класу сервісу

Перенаправлення маршруту

Маршрутні таблиці у вузлів зазвичай є статичними і, з часом, при зміні топології мережі маршрутні таблиці можуть застарівати. ICMP-повідомлення про перенаправлення маршруту посилається маршрутизатором на початковий вузол для більш ефективної маршрутизації. При цьому маршрутизатор також відправить початковий пакет за призначенням. Але і після отримання ICMP-повідомлення про перенаправлення маршруту деякі вузли можуть продовжувати використовувати менш ефективний маршрут.

Коли маршрутизатор бачить, що вузол відправляє пакет деякій мережі призначення нераціональним чином (не через маршрутизатор локальної мережі, від якого починається коротший маршрут до мережі призначення), він посилає повідомлення "Перенаправлення маршруту" (Redirect – тип повідомлення “5”).

У повідомлення "Перенаправлення маршруту" маршрутизатор поміщає IP-адресу маршрутизатора, яким потрібно користуватися надалі, і заголовок початкового пакету з першими 64 бітами його поля даних. Із заголовка пакету вузол дізнається, для якої мережі необхідно користуватися вказаним маршрутизатором.

Повідомлення про закінчення часу датаграми

ICMP-повідомлення про закінчення часу датаграми посилається маршрутизатором у разі обнуління поля часу життя IP-пакету (вимірюється в кількості пройдених маршрутизаторів (“хопах” – hop), або секундах. Поле часу життя запобігає нескінченній циркуляції пакетів по об'єднаній мережі, якщо остання містить маршрутну петлю. В цьому випадку маршрутизатор відкидає вихідний пакет.

5.5. Протокол перетворення адрес ARP

Будь-який пристрій, підключений до локальної мережі (Ethernet, FDDI і т.д.), має унікальну фізичну мережну адресу, задану апаратним чином (MAC-адреса). Окрім цього, кожен вузол має логічну адресу, наприклад, 4-байтову IP-адресу, яка задається адміністратором з урахуванням положення вузла в IP-мережі. Для формування кадру канального рівня необхідно знати MAC-адресу вузла одержувача, якому повинен бути доставлений IP-пакет. Протокол ARP (address resolution protocol) вирішує цю задачу – встановлює відповідність між IP-адресами вузлів і їх MAC-адресами.

Процедура перетворення адрес при відправленні пакету виглядає таким чином. Оскільки IP-адреса вузла призначення зазвичай відома, то для визначення MAC-адреси продивляється локальна ARP-таблиця вузла. Якщо для необхідної IP-адреси в ній присутній запис з MAC-адресою, то формується і посилається відповідний кадр. Якщо ж в ARP-таблиці відсутній запис, то виконуються наступні дії.

1. Всім машинам в мережі посилається кадр з ARP-запитом (по широкомовній MAC-адресі).
2. Вихідний IP-пакет ставиться в чергу.

Кожен вузол, що прийняв ARP-запит, порівнює власну IP-адресу з IP-адресою в запиті. Якщо IP-адреса співпала, то прямо по MAC-адресі відправника запиту посилається відповідь, що містить IP-адресу вузла, що

відповів, і його MAC-адресу. Після отримання відповіді на свій ARP-запит вузол формує відповідний елемент ARP-таблиці і відправляє IP-пакет, раніше поставлений в чергу. Якщо ж в мережі немає машини з потрібною IP-адресою, то ARP-відповіді не буде і нові записи в ARP-таблицю внесені не будуть. Протокол IP знищуватиме IP-пакети, призначені для відправки за такою адресою. У випадку, якщо IP-адреса не належить локальній мережі, маршрутизатор на відповідний ARP-запит видасть відповідь, вказавши в ньому MAC-адресу свого локального інтерфейсу (режим проксі-ARP).

Функціонально ARP ділиться на дві части. Одна – визначає фізичну адресу при відправці пакету, інша відповідає на запити інших машин. ARP-таблиці мають динамічний характер, кожен запис в ній "живе" певний час після чого видаляється. ARP-пакети вкладаються безпосередньо в кадри канального рівня. Формат ARP-пакету показаний на рис. 5.9.

Призначення полів пакету.

• ***HA-Len*** – довжина апаратної адреси в байтах (для MAC-адреси Ethernet HA-Len = 6).

• ***PA-Len*** – довжина протокольної адреси в байтах (наприклад, для IP-адреси PA-Len=4).

• ***Тип обладнання*** – це тип інтерфейсу, для якого відправник шукає адресу (у разі інтерфейсу Ethernet цей код – “1”).

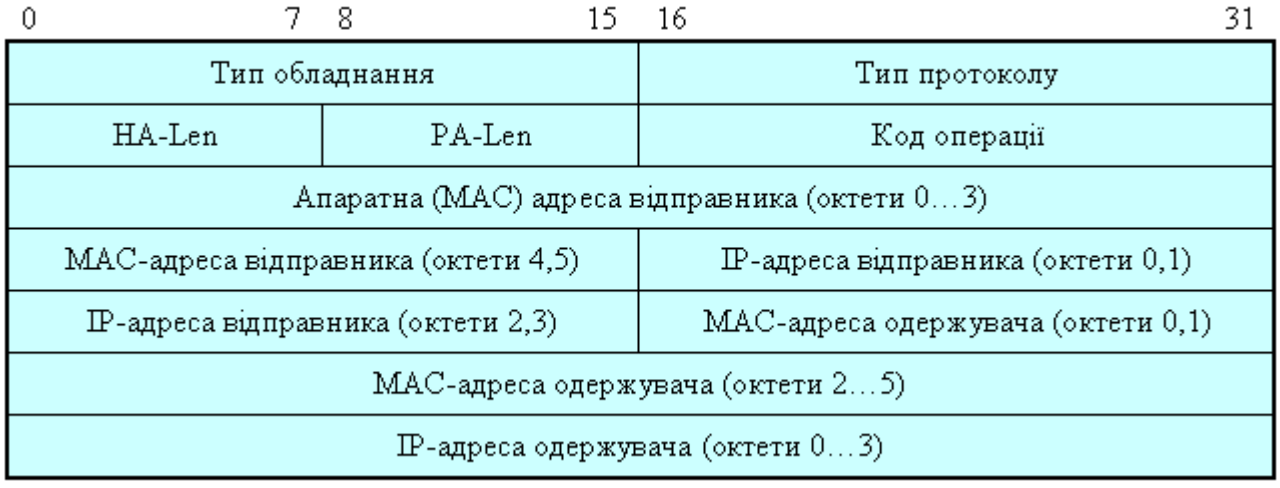


Рисунок 5.9 - Формат пакету ARP

• Поле ***код операції*** визначає, чи є даний пакет ARP-запитом (код = 1), ARP-відгуком (код = 2), RARP-запитом (код = 3), або RARP-відгуком (код = 4). Це поле необхідне для формування поля ***тип протоколу*** або заголовка LLC в кадрах Ethernet (для ARP-запиту і відповіді значення будуть однаковими і вказуватимуть на ARP протокол).

У протоколі ARP можливі самозвернені запити (gratuitous ARP). При такому запиті ініціатор формує пакет, де в якості IP використовується його власна адреса. Самозвернений запит дозволяє вузлу вирішити дві проблеми. По-перше, визначити, чи немає в мережі об'єкту, що має таку ж IP-адресу. По-друге, у разі зміни мережної карти проводиться корегування запису в ARP-таблицях вузлів, які містили стару MAC-адресу ініціатора. Вузол, що одержує ARP-запит з адресою, яка міститься в його таблиці, повинен відновити цей запис. На самозвернений запит відповість тільки той вузол, у якого співпадає IP.

Як правило, мережні адаптери вузлів одержують тільки кадри, що відповідають їхнім MAC-адресам або кадри із широкомовними MAC-адресами. Для того, щоб кілька вузлів multicast - групи могли одержати той самий кадр і, разом з тим, розрізняли різні multicast - групи, були розроблені різні засоби.

Для перетворення MAC-адреси Ethernet в групову адресу виділено спеціальний блок MAC-адрес Ethernet, починаючи із шістнадцяткової адреси 01:00:5E (діапазон MAC-адрес Ethernet від 0100.5e00.0000 до 0100.5e7f.ffff).

Рисунок 5.10 - IP-адреса для групової розсилки

Виділення цих адрес дозволяє встановити відповідність між 23 бітами Ethernet-адреси й IP-адресами групової розсилки. При цьому молодші 23 біта IP-адреси перетворяться в ці 23 біта адреси Ethernet. Оскільки старші 5 бітів IP-адреси групової розсилки при перетворенні губляться, адреса , що вийшла, не є унікальною.

Приклад такої адреси наведено на рис. 5.10.

5.6. Протокол зворотного перетворення адрес RARP

Протокол зворотного перетворення адрес (RARP – Reverse Address Resolution Protocol) вирішує зворотну протоколу ARP задачу – перетворює MAC-адреси в IP-адреси. Формати повідомлень RARP схожі з ARP, хоча принципи роботи протоколів відрізняються. Протокол RARP передбачає наявність спеціального сервера, що обслуговує RARP-запити і зберігає базу даних про відповідність апаратних адрес IP-адресам.

Зазвичай RARP застосовується в мережах з “тонкими” клієнтами (бездискові робочі станції), які для підключення до сервера і перенесення в пам'ять образу операційної системи використовують протокол TFTP.

5.7. Протокол TCP

Протокол управління передачею (Transmission Control Protocol – TCP) забезпечує надійну передачу даних в середовищі IP. TCP надає такі види сервісу, як потокова передача даних, надійність, ефективне управління потоком, дуплексний режим і мультиплексування.

При потоковій передачі даних TCP передає неструктурований потік байтів, що ідентифікуються по порядкових номерах. Ця служба корисна для прикладних програм, оскільки їм не доводиться розбивати дані на блоки перед

їх передачею по протоколу TCP. TCP групує дані в ***сегменти*** і передає їх на рівень протоколу IP для пересилки. Надійність TCP забезпечується наскрізною, орієнтованою на з'єднання, передачею пакетів по об'єднаній мережі. Вона досягається впорядкуванням пакетів за допомогою номерів підтвердження передачі, по яких одержувач визначає, який пакет повинен поступити наступним. По отриманню пакету видається підтвердження. Пакети, що не одержали підтвердження протягом певного часу, передаються наново. Надійний механізм протоколу TCP дозволяє пристроям обробляти втрачені, затримані, дубльовані і невірно прочитані пакети. Механізм ліміту часу (time out) дозволяє пристроям розпізнавати втрачені пакети і посилати запит на їх повторну передачу. Мультиплексування TCP означає одночасну передачу по одному з'єднанню декількох сеансів верхнього рівня.

5.7.1. Встановлення TCP-з'єднання

Пакети, що поступають на транспортний рівень, організовуються операційною системою у вигляді множини черг до точок входу різних прикладних процесів. У термінології TCP/IP такі точки входу називаються ***портами***. Таким чином, адресою призначення, яка використовується протоколом TCP, є ідентифікатор (номер) порту прикладної служби. Номер порту в сукупності з номером мережі і номером кінцевого вузла однозначно визначають прикладний процес в мережі. Цей набір ідентифікуючих параметрів має назву ***сокет*** (socket).

Для використання надійних транспортних служб TCP-вузли повинні встановлювати один з одним сеанси, орієнтовані на з'єднання. З'єднання в TCP ідентифікується парою повних адрес обох взаємодіючих процесів – сокетів. Встановлення з'єднання виконується по механізму, що називається ***трьохетапною синхронізацією*** (рис. 5.11).

Цей механізм синхронізує обидві сторони з'єднання, дозволяючи їм погоджувати початкові порядкові номери. Він також забезпечує готовність

обох сторін до передачі даних і інформованість кожної із сторін про готовність іншої. Це необхідно для уникнення передачі або повторної передачі пакетів в процесі встановлення сеансу або після його розриву.

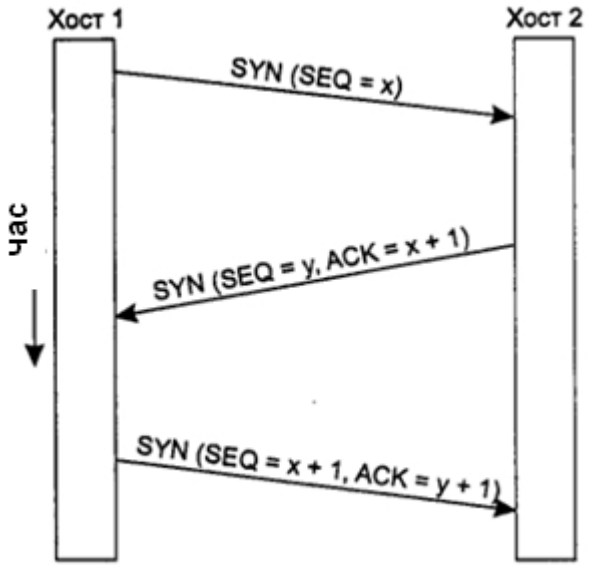


Рисунок 5.11 - Механізм трьохетапної синхронізації

Кожен вузол вибирає випадковим чином порядковий номер, щоб стежити за прийомом і передачею байтів потоку. Потім механізм трьохетапної синхронізації працює таким чином.

Сторона, що посилає запит (яка, як правило, називається клієнт) ініціює з'єднання, відправляючи пакет з початковим номер послідовності – X і бітом синхронізації SYN для індикації запиту з'єднання. Другий вузол (сервер) одержує SYN-сегмент, записує порядковий номер X і відповідає підтвердженням SYN (разом з ACK = X + 1). Сервер вказує власний номер послідовності (SEQ = Y). Потім клієнт підтверджує готовність до прийому, указуючи номер наступного байта, який клієнт чекає одержати (ACK = Y + 1). Після цього може починатися передача даних.

Цих трьох сегментів достатньо для встановлення з'єднання. Часто ця процедура називається *трьохетапним рукостисканням* (three-way handshake).

5.7.2. Ковзаюче вікно TCP

У протоколі TCP "ковзаюче вікно" використовується для регулювання трафіку і запобігання переповнення буферів.

У TCP приймаючий вузол визначає поточний розмір вікна кожного пакету. Оскільки по TCP-з'єднанню дані передаються у вигляді потоку байт, розміри вікон теж виражаються в байтах. Таким чином, вікно являє собою кількість байт даних, які відправник може послати до отримання підтвердження прийому. Початкові розміри вікон визначаються при настройці з'єднання, але можуть змінюватися при передачі даних для управління потоком. Наприклад, нульовий розмір вікна означає заборону на передачу даних.

Ідея "ковзаючого вікна" відображена на рис. 5.12. Тут передбачається, що ширина вікна дорівнює 7 (k=7; це число може мінятися в дуже широких межах).

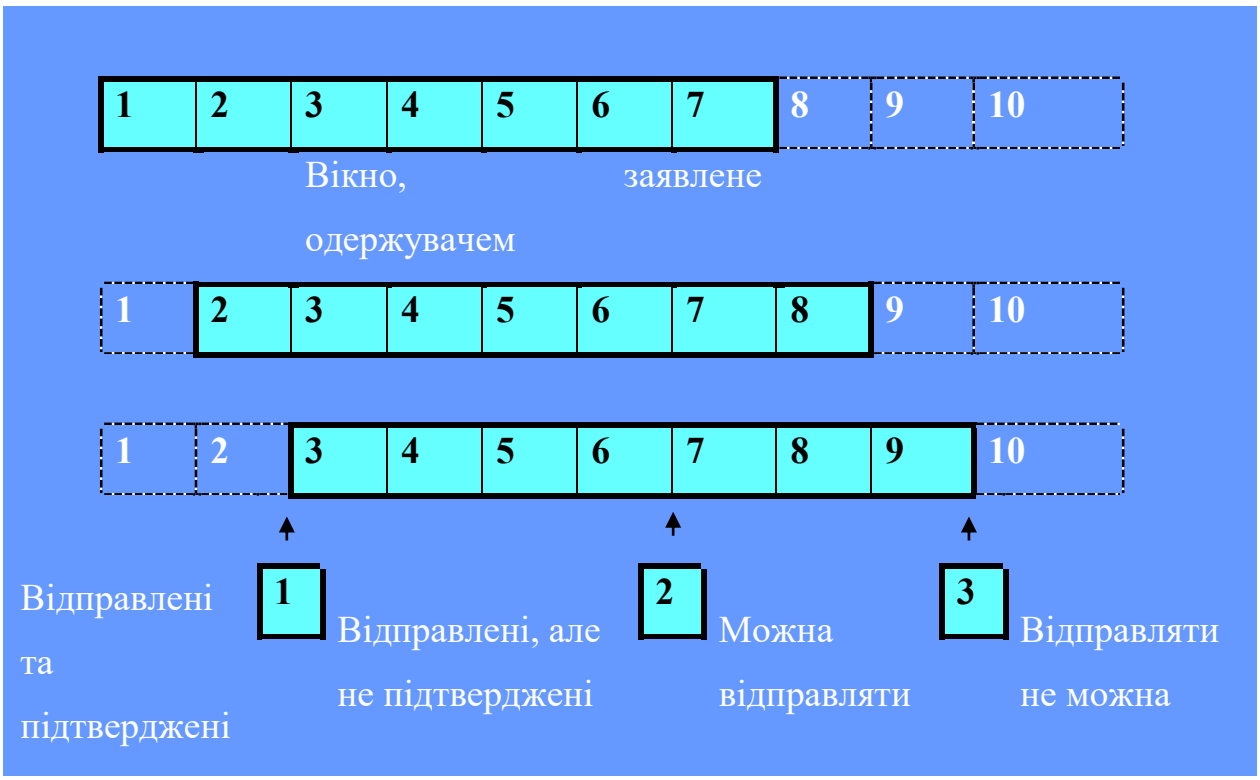


Рисунок 5.12 - Схема використання “ковзаючого вікна” в TCP

Перший покажчик визначає положення лівого краю вікна, відокремлюючи посланий сегмент, що одержав підтвердження, від посланого сегменту, отримання якого не підтверджено. Другий покажчик відзначає правий край вікна і указує на сегмент, який може бути посланий до отримання чергового підтвердження. Третій покажчик позначає межу всередині ковзаючого вікна між тими сегментами, що вже надіслані, і тими, які ще належить надіслати. Одержувач організовує аналогічні вікна для забезпечення контролю потоку даних. Якщо покажчик 3 співпаде з покажчиком 2, відправник повинен перервати подальше відправлення пакетів до отримання хоча б одного підтвердження.

Розмір вікна в сегментах визначається співвідношенням:

window > RTT·B/MSS *(сегментів)***,**

де: ***B*** – смуга пропускання каналу в біт/с,

MSS – максимальний розмір сегменту в бітах,

RTT – час розповсюдження пакету туди і назад.

Максимально допустимий розмір вікна в TCP дорівнює 65535 байта (задається розміром поля).

5.7.3. Регулювання трафіку

Метою регулювання трафіку є встановлення відповідності між темпом передачі і можливостями прийому. Причиною перевантаження може бути не тільки обмеженість розміру буфера, але і недостатня пропускна спроможність якоїсь ділянки каналу.

Регулювання трафіку в TCP передбачає існування двох незалежних процесів: ***контроль доставки***, що управляється одержувачем за допомогою параметра ***window*** (вікно одержувача), і ***контроль перевантаження***, що управляється відправником за допомогою вікна

перевантаження ***cwnd*** (congestion window) і порогу повільного старту ***ssthresh (slow start threshold)***. Перший процес відстежує заповнення вхідного буфера одержувача, другий – реєструє перевантаження каналу, а також пов'язані з цим втрати і знижує рівень трафіку. Процес, що управляє пересилкою, ніколи не відправить більше байт, ніж це задано ***cwnd*** і оголошеним одержувачем значенням ***window***.

При ініціалізації з'єднання вікно перевантаження (***cwnd***) має ширину рівну максимальному сегменту (***MSS***), який може бути використаний в даному каналі. Відправник посилає такий сегмент. Якщо підтвердження надійде до закінчення часу тайм-ауту, розмір вікна перевантаження (***cwnd***) подвоюється і посилається два сегменти максимальної довжини. При отриманні підтвердження доставки кожного з сегментів вікно перевантаження збільшується на один сегмент максимальної довжини. Коли ширина вікна перевантаження стає рівною **X** сегментів і всі **X** послані сегменти одержують підтвердження, вікно перевантаження зростає на число байт, що містяться в цих сегментах. Таким чином, ширина вікна перевантаження (***cwnd***) послідовно подвоюється до тих пір, поки доставка всіх сегментів підтверджується. Зростання ширини вікна перевантаження (***cwnd***) при цьому має експоненціальний характер. Це продовжується до тих пір, поки не наступить тайм-аут, або вікно перевантаження не порівняється з вікном одержувача. Така процедура і називається ***повільним стартом***.

Крім вікон перевантаження і одержувача в TCP використовується третій параметр – *поріг* (іноді він називається порогом повільного старту ***ssthresh***). При встановленні з'єднання ***ssthresh=64*** Кбайт. У разі виникнення тайм-ауту значення ***ssthresh*** робиться рівним **cwnd/2**, а саме значення ***cwnd*** прирівнюється ***MSS***. Далі запускається процедура повільного старту, щоб з'ясувати можливості каналу. При цьому експоненціальне зростання ***cwnd*** здійснюється аж до значення ***ssthresh***. Коли цей рівень ***cwnd*** буде досягнутий, подальше зростання відбувається лінійно з приростом на кожному кроці рівним ***MSS*** (рис. 5.13).

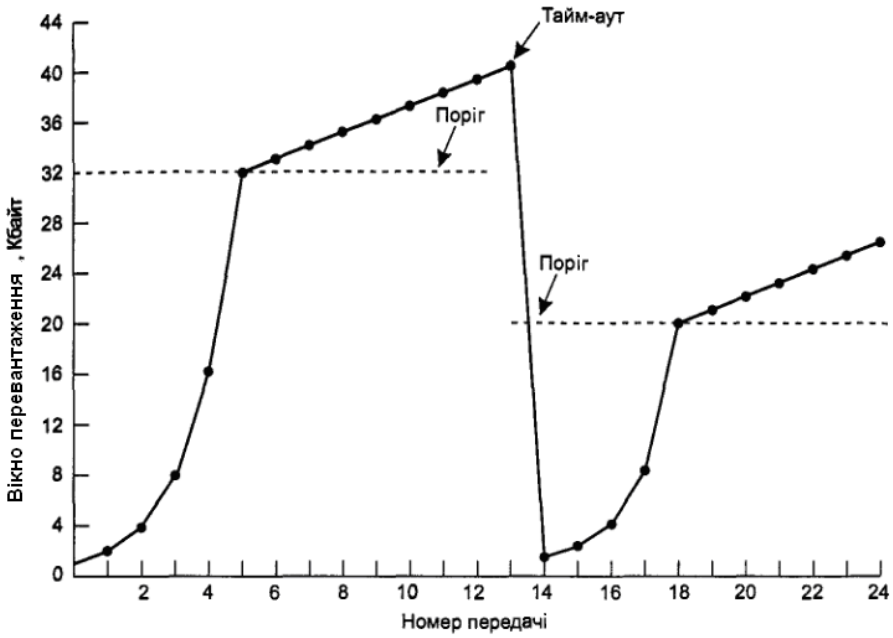


Рисунок 5.13 - Еволюція ширини вікна при повільному старті

В цьому прикладі передбачається, що ***MSS = 1*** Кбайт. Початку діаграми відповідає установка значення ***ssthresh=32*** Кбайт. Дана схема дозволяє точніше вибрати значення ***cwnd***. Після тайм-ауту, який на малюнку відбувся при передачі з номером 13, значення порогу знижується до 20 Кбайт (=***cwnd/2***). Ширина вікна ***cwnd*** знову починає рости від передачі до передачі, починаючи з одного сегменту, аж до нового значення порогу ***ssthresh=20*** Кбайт. Стратегія з експоненціальною і лінійною ділянками зміни ширини вікна перевантаження дозволяє приблизно наблизити середнє його значення до оптимального. Для локальних мереж, де значення ***RTT*** є досить невеликим, а вірогідність втрати пакету мала, оптимізація задавання ***cwnd*** не так істотна, як у разі протяжних зовнішніх (наприклад, супутникових) каналів.

Для взаємного узгодження операцій в рамках TCP-протоколу використовується чотири таймери.

1. ***Таймер повторних передач*** (retransmission; RTO) контролює час приходу підтверджень (ACK). Таймер запускається у момент посилки сегменту. При отриманні відгуку ACK до закінчення часу таймера, він скидається. Якщо

ж час таймера закінчується до приходу ACK, сегмент посилається адресату повторно, а таймер перезапускається.

2. ***Таймер запитів*** (persist timer) контролює час очікування, коли приймальне вікно закрито (якщо вузол-одержувач надіслав повідомлення з *window = 0*, вузол-відправник повинен призупинити передачу). При зміні ситуації одержувач посилає сегмент з ненульовим значенням ширини вікна, що дозволить відправнику відновити свою роботу. Але якщо цей пакет буде втрачено, виникне ситуація, коли кожна із сторін чекатиме сигнал від партнера. Саме у цій ситуації і використовується таймер запитів. Після закінчення часу цього таймера відправник відправить сегмент адресату. Відгук на цей сегмент міститиме нове значення ширини вікна. Таймер запускається кожного разу, коли одержано сегмент з *window = 0*.

3. ***Таймер контролю працездатності*** (keep-alive) реєструє факти виходу з ладу або перезавантаження вузлів, що беруть участь в з'єднанні. Час за умовчанням дорівнює 2 годинам. Keepalive-таймер не є частиною TCP-специфікації. Таймер корисний для виявлення станів сервера "half-open", які виникають за умови, що клієнт відключився (наприклад, користувач вимкнув свій персональний комп'ютер) не виконавши процедуру завершення сеансу. Після закінчення часу таймера клієнту посилається сегмент перевірки стану. Якщо протягом 75 секунд не буде одержаний відгук, сервер повторює запит 10 разів з періодичністю 75 сік, після чого з'єднання розривається. При отриманні будь-якого сегменту від клієнта таймер скидається і запускається знов.

4. ***2MSL-таймер*** (Maximum Segment Lifetime) контролює час перебування каналу в стані очікування (TIME_WAIT). Значення таймера за умовчанням дорівнює 2 хвилинам (FIN_WAIT-таймер). Таймер запускається при виконанні процедури active close у момент посилки останнього ACK.

5.7.4. Формат TCP-пакету

Дані TCP інкапсулюються (вкладаються) в IP-датаграму, як показано на рис. 5.14.

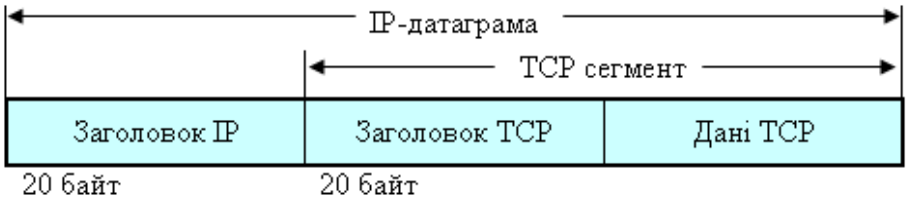


Рисунок 5.14 - Інкапсуляція TCP даних в IP-датаграму.

Поля і повний формат TCP-пакету показані на рис. 5.15.

Поля TCP-пакету.

- ***Порт джерела і порт одержувача.*** Точки, в яких процеси верхнього рівня джерела і одержувача приймають послуги TCP.

- ***Порядковий номер*** – номер першого байта даних в поточному повідомленні. При значенні прапора *SYN=1* в цьому полі лежить код *ISN* (Initial Sequence Number)- початковий номер послідовності, який вибирається для конкретного з'єднання.

Рисунок 5.15 - Формат TCP-пакету

• ***Номер підтвердження.*** Порядковий номер наступного байта даних, який очікує отримати одержувач. Враховується тільки, якщо присутній прапор *ACK*.

• ***Зміщення даних.*** Число 32-розрядних слів в заголовку TCP.

• ***Резерв.*** Область, зарезервована для використання в майбутньому.

• ***Прапори.*** Поле, яке містить управляючу інформацію і складається з наступних бітів (зліва на право).

URG – покажчик важливої інформації (URG =1 – інформація важлива).

ACK – номер октету, який повинен прийти наступним, правильний (ACK=1).

PSH – сегмент вимагає виконання операції push (PSH=1). Одержувач повинен передати ці дані прикладній програмі щонайшвидше.

RST – переривання зв'язку (RST = 1 – одержувач повинен перервати з'єднання).

SYN – прапор для синхронізації номерів сегментів (SYN=1 – одержувач повинен виконати процедуру встановлення з'єднання).

FIN – закінчення передачі (FIN =1 – відправник закінчив посилку байтів).

• ***Вікно.*** Розмір приймального вікна одержувача. Визначає скільки байт може бути послано, після байта, що одержав підтвердження.

• ***Контрольна сума***. Використовується для контролю помилок передачі заголовка.

• ***Покажчик терміновості.*** Є покажчиком останнього байта, що містить інформацію, яка вимагає негайного реагування. Поле має сенс лише при прапорі URG = 1, який відзначає сегмент з першим байтом “важливої інформації”.

• ***Параметри і опції.*** Різні додаткові параметри TCP.

• ***Дані.*** Інформація верхнього рівня.

5.8. Протокол UDP

Протокол передачі датаграм користувача UDP (User Datagram Protocol – UDP) являє собою протокол транспортного рівня, що працює в режимі без встановлення з'єднання і не потребує підтвердження одержання пакетів. По

суті, UDP є інтерфейсом між IP і протоколами верхнього рівня. Порти протоколу UDP вказують на прикладні програми, що ведуть передачу даних.

На рис. 5.16 показана інкапсуляція UDP датаграми в IP датаграму.

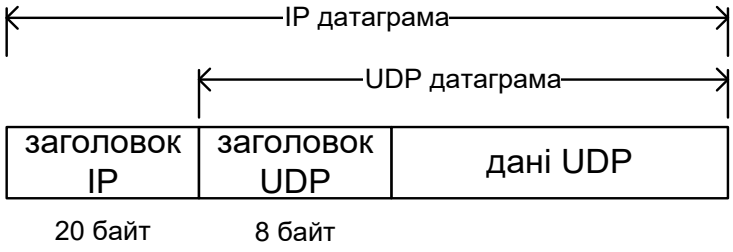


Рисунок 5.16 - UDP інкапсуляція

На відміну від TCP, UDP не додає IP надійності, керування потоком, або функцій виправлення помилок. Через простоту UDP його заголовки коротше й вимагають менше ресурсів мережі, ніж TCP.

UDP корисний у ситуаціях, коли потужні механізми забезпечення надійності протоколу TCP не обов'язкові, наприклад, коли керування потоком і корекцію помилок можна покласти на протокол верхнього рівня.

Формат пакета UDP містить чотири поля: порт джерела, порт одержувача, довжина й контрольна сума (рис. 5.17).

Рисунок 5.17 - Формат пакета UDP

Поля портів відправника й отримувача містять 16-розрядні номери портів протоколу UDP, що вказують на протоколи й служби прикладного рівня, які

використовують протокол UDP у якості транспортного. Поле довжини визначає розмір UDP-заголовка й даних. Поле контрольної суми служить для перевірки цілісності UDP-заголовка й даних.

5.9. Особливості протоколу IPv6

Наприкінці 1992 року співтовариство Інтернет для вирішення проблем адресного простору і ряду суміжних задач розробило три проекти протоколів: “TCP and UDP with Bigger Addresses (TUBA)”; “Common Architecture for the Internet (CatnIP)” й “Simple Internet Protocol Plus (SIPP). Після аналізу всіх цих пропозицій був прийнятий новий протокол IPv6 з IP-адресами, що мають довжину 128 біт замість 32 біт у версії IPv4.

IPv6 являє собою нову версію протоколу Інтернет, що є спадкоємицею версії 4. Відмінності IPv6 від IPv4 можна розділити на наступні групи.

Розширення адресації

В IPv6 довжина адреси розширена до 128 біт (проти 32 в IPv4), що дозволяє забезпечити більше рівнів ієрархії адресації, збільшити число адресованих вузлів, спростити автоконфігурування. Для розширення можливості групової (мультикастинг) маршрутизації в адресне поле введено субполе "scope" (група адрес). Визначено новий тип адреси "anycast address" (енікастний), що використовується для посилки запитів вузла будь-якій групі маршрутизаторів. Енікаст-адресація призначена для використання з набором взаємодіючих маршрутизаторів, чиї адреси невідомі клієнтові заздалегідь.

Специфікація формату заголовків

Деякі поля заголовка IPv4 відкидаються або робляться опціонними, зменшуючи витрати, пов'язані з обробкою заголовків пакетів для того, щоб зменшити вплив збільшення довжини адрес в IPv6.

Покращена підтримка розширень і опцій

Зміна кодування опцій IP-заголовків дозволяє полегшити переадресацію пакетів, послаблює обмеження на довжину опцій і робить більш доступним введення додаткових опцій у майбутньому.

Можливість позначки потоків даних

Введено можливість позначати пакети, що належать певним транспортним потокам, для яких відправник запросив певну процедуру обробки, наприклад, нестандартний тип TOS (вид послуг), або для обробки даних у реальному масштабі часу.

Ідентифікація і захист приватних обмінів

В IPv6 введена специфікація ідентифікації мережних об'єктів або суб'єктів для забезпечення цілісності даних і, при бажанні, захисту приватної інформації.

5.9.1. Особливості адресації в IPv6

Збільшення розрядності поля адреси

Нова, шоста версія протоколу IPv6 внесла істотні зміни в систему адресації IP-мереж (RFC 2373). Адреса IPv6 складається з 128 біт або 16 байт. Обрана довжина IP-адреси повинна надовго зняти проблему дефіциту IP-адрес. Однак таке значне збільшення довжини адреси було зроблено не тільки й навіть не стільки для зняття проблеми дефіциту адрес, скільки для подальшого підвищення ефективності роботи всього стека TCP/IP. Головною метою зміни системи адресації було не механічне збільшення розрядності адреси, а зміна його функціональності за рахунок введення нових полів.

Замість колишніх двох рівнів ієрархії адреси (номер мережі й номер вузла) в IPv6 пропонується використовувати чотири рівні, включаючи трьохрівневу ідентифікацію мереж, і один рівень для ідентифікації вузлів мережі. За рахунок збільшення числа рівнів ієрархії в адресі новий протокол ефективно підтримує технологію агрегування адрес (CIDR). Завдяки цьому, а також удосконаленій системі групової адресації і введенню адрес нового типу “anycast”, нова версія IP дозволяє зменшити витрати на маршрутизацію.

Нова форма запису адреси

Розробники стандарту відмовилися від десяткової форми запису IP-адреси, що дуже незручна при визначенні номера мережі, коли границя маски не збігається із границею байтів адреси. В IPv6 використовується шістнадцяткове представлення – 8 сегментів по 4 шістнадцяткових цифри, причому кожні чотири шістнадцяткові цифри відокремлюються одна від одної двокрапкою. Наприклад:

FEDC:0A98:0:0:0:0:7654:3210.

Якщо в адресі є довга послідовність нулів, то запис адреси можна скоротити. Наприклад, наведену вище адресу можна записати так:

FEDC:0A98::7654:3210.

Скорочення "::" може вживатися в адресі тільки один раз. Можна також опускати незначущі нулі на початку кожного поля адреси, наприклад, замість

FEDC:0A98::7654:3210

можна писати

FEDC:A98::7654:3210.

Для мереж, що підтримують обидві версії протоколу IPv4 й IPv6, дозволяється використовувати для молодших 4 байт традиційний для IPv4 десятковий запис, а для старших 12 байт – визначену для IPv6 шістнадцяткову форму:

0:0:0:0:0:FFFF:129.144.52.38,

або

::FFFF:129.144.52.38.

5.9.2. Типи адрес

У версії IPv6, на відміну від версії IPv4, відсутнє поняття класу мережі (A, B, C й D) і пов'язана з ним фіксована розбивка адреси на номер мережі і номер вузла по границях байт.

В IPv6 визначено 3 основних типи адрес:

- unicast;
- multicast;
- anycast.

Тип адреси задається значенням декількох старших біт адреси, які називаються префіксом формату.

Адреса ”типу “***unicast***” визначає унікальний ідентифікатор окремого інтерфейсу кінцевого вузла або маршрутизатора. Призначення цього типу адреси збігається із призначенням унікальних адрес у версії IPv4 – з їхньою допомогою пакети доставляються певному інтерфейсу вузла призначення.

Адреси типу “unicast” діляться на кілька підтипів для відображення специфіки деяких ситуацій, що часто зустрічаються в сучасній складеній мережі.

Адреса типу “***multicast***” – групова адреса, аналогічна по призначенню груповій адресі IPv4. Вона має префікс формату 1111 1111 й ідентифікує групу інтерфейсів, що відносяться, як правило, до різних вузлів. Пакет з такою адресою доставляється всім інтерфейсам із цією адресою. Адреси типу “multicast” використовуються в IPv6 і для заміни широкомовних адрес. Для цього вводиться особлива адреса групи, що поєднує всі інтерфейси підмережі.

У версії IPv6 групова адреса має ознаку розміру або масштабу (scope), що була відсутня в груповій адресі версії IPv4. Ця ознака дозволяє гнучко задавати область дії групової адреси. Вона може являти собою, наприклад, тільки одну підмережу, або всі підмережі даного підприємства, або весь Internet. Це спрощує роботу маршрутизаторів, яким необхідно виявляти всі вузли, що відносяться до якої-небудь групи. Ще одна ознака задає тип групи – постійна або тимчасова.

Мультикастинг-адреси мають наступний формат (рис. 5.18).
Послідовність 11111111 на початку адреси ідентифікує адресу як мультикастинг-адресу.

Старші 3 прапори зарезервовані й повинні містити нулі.

Якщо четвертий прапор T = 0, це вказує на те, що адреса є стандартною (“well-known”) груповою адресою, офіційно виділеною для глобального використання в Інтернет.

8 біт	4 біта	4 біта	112 біт
11111111	Прапори	Scope	Ідентифікатор групи

Рисунок 5.18 - Формат мультикастинг-адреси

Якщо T = 1, то дана групова адреса призначена тимчасово (“transient”).

Поле “scope” являє собою 4-бітовий код групи, призначений для визначення граничної області дії групи. Допустимі значення поля наведені в таблиці 5.5.

Таблиця 5.5 - Допустимі значення поля “scope”

Поле “scope”	Значення	Поле “scope”	Значення
0	зарезервовано	8	область дії обмежена локальною організацією
1	область дії обмежена локальним вузлом	9	не визначено
2	область дії обмежена локальним каналом	A	не визначено
3	не визначено	B	не визначено
4	не визначено	C	не визначено
5	область дії обмежена локальною мережею	D	не визначено
6	не визначено	E	глобальні межі (global scope)
7	не визначено	F	зарезервовано

Адреса типу ***“anycast”*** – це новий тип адреси, що так само, як і “multicast”, визначає групу інтерфейсів. Але пакет з такою адресою доставляється одному з інтерфейсів групи, як правило, “найближчому” відповідно до метрики,

використовуваної протоколами маршрутизації. Синтаксично anycast-адреса нічим не відрізняється від адреси типу “unicast”. Вона призначається з того ж діапазону адрес, що й unicast-адреси. Адреса типу “anycast” може бути призначена тільки інтерфейсам маршрутизатора. Інтерфейси маршрутизаторів, що входять в одну anycast-группу, мають індивідуальні unicast-адреси і, крім того, загальну anycast-адресу.

Адреси такого типу орієнтовані на застосування маршрутизації від джерела (Source Routing), коли маршрут проходження пакета визначається вузлом-відправником шляхом вказання IP-адрес всіх проміжних маршрутизаторів. Наприклад, провайдер може призначити всім своїм маршрутизаторам одну і ту саму anycast-адресу і повідомити її абонентам. Якщо абонент бажає, щоб його пакети передавалися через мережу цього провайдера, то йому досить вказати anycast-адресу в ланцюжку адрес маршруту від джерела. Пакет буде переданий через найближчий маршрутизатор провайдера.

Енікаст-адреса маршрутизаторів субмережі має формат, наведений на рис. 5.19.

n біт	128-n біт
Префікс субмережі	0000000000000000

Рисунок 5.19 - Формат енікаст-адреси

Префікс субмережі в енікастній адресі є префіксом, що ідентифікує певний канал. Ця енікастова адреса є синтаксично ідентичною унікастовій адресі для інтерфейсу каналу з ідентифікатором інтерфейсу, рівним нулю.

Локальні адреси

У шостій версії протоколу, так само, як й у четвертій, є адреси, призначені для локального використання, тобто в мережах, що не входять в Internet.

Адреси для локального використання представлені в IPv6 двома різновидами. По-перше, це адреси для мереж, не розділених на підмережі (не використовують маршрутизацію). Вони називаються Link-Local і мають 10-бітний префікс формату 1111 1110 10 (FE80::/10). Адреса Link-Local містить тільки 64-розрядне поле ідентифікатора інтерфейсу. Інші розряди, крім префікса формату, повинні бути нульовими, оскільки потреба в номері підмережі тут відсутня.

По-друге, це адреси локального використання для мереж, розділених на підмережі. Такі адреси називають Unique Local Unicast, вони мають префікс формату 1111 110 (FC00::/7) і, у найпростішому випадку – без використання глобального ідентифікатору префіксу, містять у порівнянні з адресами Link-Local додаткове двобайтове поле номера підмережі (16 біт перед ідентифікатором інтерфейсу).

Глобальні агреговані унікальні адреси

Основним підтипом адреси типу “unicast” є глобальна агрегована унікальна адреса, що призначена для ідентифікації вузлів в Internet. Такі адреси можуть агрегуватися для спрощення маршрутизації. На відміну від унікальних адрес вузлів версії IPv4, які складаються із двох полів – номера мережі й номера вузла, глобальні агреговані унікальні адреси IPv6 мають більш складну структуру (рис. 5.20), що включає шість полів.

3	13	8	24	16	64
Префікс формату (FP)	Агрегування верхнього рівня (TLA)		Агрегування наступного рівня (NLA)	Агрегування місцевого рівня (SLA)	Ідентифікатор інтерфейсу (Interface ID)

Рисунок 5.20 - Структура глобальної агрегованої унікальної адреси IPv6

Поле префікса формату FP для цього типу адрес складається із трьох біт і має значення 001.

Наступні три поля TLA, NLA й SLA розглядаються як префікси трьох рівнів – верхнього рівня агрегування адрес (Top-Level Aggregation, TLA), наступного рівня агрегування (Next-Level Aggregation, NLA) і місцевого рівня агрегування (Site-Level Aggregation, SLA).

Префікс верхнього рівня – TLA – призначений для ідентифікації великих провайдерів самого верхнього рівня. Конкретне значення цього префікса являє собою загальну частину адрес, які має даний провайдер. Порівняно невелика кількість розрядів, відведених під це поле (тобто 13), вибрана спеціально для обмеження розміру таблиць маршрутизації в магістральних маршрутизаторах самого верхнього рівня Internet. Це поле дозволяє перенумерувати 8192 мереж провайдерів верхнього рівня. Число записів, що описують маршрути між цими мережами, також буде обмежено значенням 8192, що прискорить роботу магістральних маршрутизаторів. Наступні 8 розрядів зарезервовані для розширення в майбутньому поля TLA, якщо 8192 номерів мереж виявиться недостатнім на верхньому рівні.

Префікс наступного рівня – NLA – призначений для розміщення номерів мереж середніх і дрібних провайдерів. Значний розмір поля NLA дозволяє шляхом агрегування адрес створювати їхню багаторівневу ієрархію, що відображає багаторівневу ієрархію провайдерів.

Префікс місцевого рівня – SLA – призначений для адресації підмереж окремого абонента, наприклад, підмереж однієї корпоративної мережі. Передбачається, що провайдер призначає деякому підприємству номер його мережі, що складається з фіксованого значення полів TLA й NLA, які в сукупності є аналогом номера мережі версії IPv4. Інша частина адреси – поля SLA й ідентифікатор інтерфейсу – надходять у розпорядження адміністратора корпоративної мережі, тобто він повністю управляє процесом його формування і не повинен погоджувати цей процес із провайдером. Причому поле

ідентифікатора інтерфейсу має цілком визначене призначення – воно повинне зберігати фізичну адресу вузла.

На цьому рівні також можливо агрегувати адреси невеликих підмереж у більші підмережі і розмір поля в 16 біт забезпечує достатню свободу і гнучкість побудови внутрішньокорпоративної ієрархії адрес.

Ідентифікатор інтерфейсу (Interface ID) є аналогом номера вузла IPv4. Ідентифікатори інтерфейсів використовуються в адресах типу “unicast” для однозначного визначення інтерфейсів у межах якої-небудь підмережі. Відмінністю версії IPv6 є те, що в загальному випадку ідентифікатор інтерфейсу просто збігається з його фізичною адресою, а не являє собою довільно призначений адміністратором номер вузла. Ідентифікатор інтерфейсу має довжину 64 біта. Це дозволяє помістити туди MAC-адресу Ethernet (48 біт), або адресу X.25 (до 60 біт), або адресу кінцевого вузла ATM (48 біт), або номер віртуального з'єднання ATM (до 28 біт), а також дає можливість використовувати локальні адреси технологій, які можуть з'явитися в майбутньому. Такий підхід робить непотрібним використання протоколу ARP. Процедура відображення IP-адреси на локальну адресу стає тривіальною – вона зводиться до простого відкидання старшої частини адреси. Крім того, у більшості випадків відпадає необхідність ручного конфігурування кінцевих вузлів, тому що молодшу частину адреси (ідентифікатор інтерфейсу) вузол дізнається від апаратури (мережного адаптера й т.п.), а старшу (номер підмережі) йому повідомляє маршрутизатор.

Спеціальні адреси “unicast”

Крім глобальної агрегованої адреси, докладно розглянутої вище, існують і інші різновиди адреси типу “unicast”. Зокрема, адреса зворотної петлі (loopback) і невизначена адреса. Обидві вони мають префікс формату 0000 0000 і відрізняються тільки значенням молодшого біта. Адреса зворотної петлі 0:0:0:0:0:0:0:1 грає у версії IPv6 ту ж роль, що й адреса 127.0.0.1 у версії IPv4.

Невизначена адреса ::, яка складається з одних нулів, є аналогом адреси 0.0.0.0 протоколу версії IPv4. Таке значення говорить про те, що у вузла

відсутня назначена IP-адреса. Така адреса не повинна з'являтися в IP-пакетах як адреса призначення. Якщо ж вона з'являється в полі адреси джерела, то це означає, що пакет посланий до того, як вузол вивчив свою IP-адресу (наприклад, до одержання її від DHCP-сервера).

Ще два різновиди unicast-адрес із префіксом формату 00000000 призначені для забезпечення сумісності версій IPv4 й IPv6.

Для того, щоб вузли, що підтримують версію протоколу IPv6, могли використовувати техніку передачі пакетів IPv6 через мережу IPv4 в автоматичному режимі, розроблено спеціальний підтип адрес, які переносять адресу IPv4 у молодших 4-х байтах адреси IPv6, а в старших 12-ти байтах адреси містяться нулі. Такий тип unicast-адрес значно спрощує процедуру перетворення адрес "IPv6-IPv4" і називається "IPv4-сумісними адресами IPv6".

Є ще один різновид адреси IPv6, що переносить адресу IPv4 – це, так звана, “IPv4-відображена адреса IPv6”. Вона призначена для розв’язання зворотної задачі – передачі пакетів IPv4 через частини Internet, що працюють по протоколу IPv6. Цей тип адреси як і раніше містить в 4-х молодших байтах адресу IPv4, в п'ятому та шостому байтах адреси IPv6 – одиниці, а в старших 10-ти байтах – нулі, Одиниці в 5 та 6 байтах вказують на те, що вузол підтримує тільки четверту версію протоколу IP.

Існує спеціальний підтип unicast-адреси, призначений для відображення адрес IPX на адреси IPv6. Ці адреси відрізняються 7-бітним префіксом формату 0000 010, а інші 121 біт виділяються під адресу IPX і, можливо, ще якусь додаткову інформацію, точне призначення якої стандартом поки ще не визначено.

5.9.3. Агрегування адрес

Розробники стандартів IPv6 вважають агрегування адрес основним способом ефективного використання адресного простору в новій версії протоколу IP. Техніка агрегування використовувалася і до появи IPv6 у

класичній версії IPv4. Ця техніка має назву безкласової міждоменної маршрутизації (Classless Inter-Domain Routing, CIDR).

Суть технології CIDR полягає в наступному. Кожному провайдеру призначається безперервний діапазон у просторі IP-адрес. При такому підході адреси всіх мереж кожного провайдера мають загальну частину в старших розрядах – префікс. В результаті, маршрутизація на магістралях Internet може здійснюватися на основі префіксів, а не повних адрес мереж. Коли клієнт (ним може виявитися й більш дрібний провайдер) звертається до провайдера із проханням про виділення йому деякої кількості адрес, то в наявному пулі адрес "вирізається" безперервна область відповідного розміру. Причому границі цієї області вибираються такими, щоб для нумерації необхідного числа вузлів вистачило деякого числа молодших розрядів, а значення всіх старших розрядів, що залишилися, були однаковими, створюючи префікс адреси даного провайдера-клієнта.

Агрегування адрес дозволяє зменшити обсяг таблиць у маршрутизаторах всіх рівнів, тому що всі мережі з однаковим префіксом представлені в таблиці маршрутизації одним записом. Отже, воно прискорює роботу маршрутизаторів і підвищує пропускну здатність Internet.

В IPv6 зберігається механізм масок, на основі якого маршрутизатор виділяє якесь число, що має значення префікса, номера мережі або номера підмережі. На підставі цього числа він робить перегляд таблиці маршрутизації і приймає рішення щодо проходження пакета.

Існує два типи операцій, пов'язаних з накладенням маски на IP-адресу:

- агрегування (superneting), коли маска зрушується вправо по полю номера мережі; при цьому частина адреси, яка виділяється маскою, називається префіксом;
- розбивка єдиного номера мережі на кілька номерів підмереж за допомогою масок, що використовують частину області номера вузла (subneting).

В IPv4 використовуються і перший (CIDR), і другий (розподіл на підмережі) типи операцій. Агрегування виконують провайдери, правильно

виділяючи пули адрес великим абонентам і більш дрібним провайдерам, налаштовуючи відповідним чином свої маршрутизатори. Мета такої операції – скорочення адресних таблиць маршрутизаторів. Операції другого типу виконуються адміністраторами корпоративних мереж для структуризації мережі (поділу її на підмережі) в умовах дефіциту номерів мереж.

На відміну від IPv4, в IPv6 застосовується тільки агрегування адрес, а операція поділу мережі на підмережі не використовується, тому що в цьому немає необхідності.

Розглянемо приклад. Нехай провайдер верхнього рівня видає провайдеру другого рівня пул адрес IPv6. При цьому він повідомляє провайдеру другого рівня деяке конкретне число – префікс для всіх його мереж, і маску, що визначає довжину префікса. Наприклад, провайдер самого верхнього рівня, що має префікс 1001100100111 в полі TLA (рис. 5.21), може виділити провайдеру другого рівня деякий діапазон адрес із спільним префіксом, утвореним полями FP, TLA, резервним полем, заповненим нулями, а також частиною поля NLA.

Довжина поля NLA, що відводиться під префікс, визначається маскою, яку провайдер верхнього рівня також повинен повідомити своєму клієнтові – провайдеру другого рівня. У даному прикладі маска складається з 29 одиниць у старшій частині. У результаті повний префікс має наступне значення:

001 1001100100111 00000000 01001.

3	13	8	24	16	64
FP = 001	TLA = 1001100100111		NLA = 01001 00...0	SLA = xx...x	Interface ID = xx...x

Рисунок 5.21 - Приклад формування префікса

У розпорядженні провайдера другого рівня залишається 19 розрядів поля NLA для нумерації мереж своїх клієнтів. Як клієнти можуть виступати провайдери третього і нижчих рівнів, а також кінцеві абоненти – підприємства й організації. Для прикладу припустимо, що провайдер другого рівня надає

послуги безпосередньо кінцевим абонентам. У цьому випадку 19 розрядів поля NLA, що залишилися, використовуються для ідентифікації організацій – абонентів (або, що те саме, для нумерації мереж абонентів). Провайдер другого рівня видає клієнтові префікс, що складається із власного префікса цього провайдера, доповненого дев'ятнадцятирозрядним ідентифікатором абонента.

Старша частина IPv6-адреси, що видається кінцевому абонентові (префікс), є прямим аналогом номера мережі IPv4. Частини IPv6-адреси, що залишилися – поле SLA і поле Interface ID – більш віддалена аналогія поля номера вузла IPv4. Відмінності можна пояснити на прикладі використання операцій агрегування адрес (superneting) і розбивки мережі на підмережі (subneting). В IPv4 адміністратор, одержавши від провайдера номер мережі, міг тільки розділяти мережу на підмережі шляхом зсування маски вправо, в область номера вузла. В IPv6 адміністратор відразу ж, одночасно отримує в своє розпорядження фіксоване число (65 535) підмереж однакового розміру, за рахунок того, що частина адреси, що залишилася, розбита на два поля – SLA для номера підмережі й Interface ID для номера вузла. Значення маски для адрес абонента за замовчуванням встановлюється на границі між цими двома полями. Маючи такий величезний діапазон номерів підмереж, адміністратор може використовувати його по-різному. Він може вибрати просту плоску організацію своєї мережі, призначаючи кожній наявній підмережі певне значення з діапазону з 65 535 адрес, не використовуючи ті, що залишилися. У великих мережах більш ефективним способом (скорочуючим розміри таблиць корпоративних маршрутизаторів) може виявитися ієрархічна структуризація мережі на основі агрегування адрес. У цьому випадку використовується та ж технологія CIDR, але вже не провайдером, а адміністратором корпоративної мережі.

5.9.4. Формат заголовка IP-пакета

Однією з основних цілей зміни формату заголовка в IPv6 було зниження накладних витрат, тобто зменшення об'єму службової інформації, переданої з

кожним пакетом. Для цього в новому форматі IPv6 були введені поняття основного й додаткового заголовків. Основний заголовок присутній завжди, а додаткові є опціональними. Додаткові заголовки можуть містити, наприклад, інформацію про фрагментацію вихідного пакета, повний маршрут проходження пакета при використанні техніки маршрутизації від джерела, інформацію, необхідну для захисту переданих даних і т.д.

Основний заголовок має фіксовану довжину 40 байт і наступний формат (рис. 5.22).

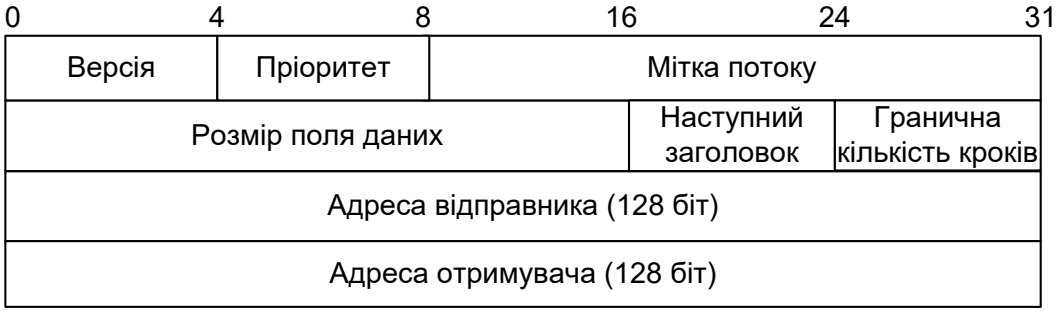


Рисунок 5.22 - Формат основного заголовка IP-пакета в IPv6

Поля заголовка IP-пакета.

Версія – 4-бітний код номера версії Інтернет протоколу (версія Інтернет протоколу для IPv6= 6).

Пріоритет – 4-бітний код пріоритету. У документі RFC-2460, що з'явився через три роки після RFC-1883, поле “пріоритет” замінено на поле “клас трафіка”. Це поле має 8 біт (проти 4 у полі пріоритету). При цьому розмір поля “мітка потоку” скоротився до 20 біт. Це було продиктовано вимогами документа RFC-2474 “Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”, орієнтованого на вирішення завдань керування QoS.

Мітка потоку – 24-бітний код мітки потоку (для мультимедіа).

Розмір поля даних – 16-бітове число без знака. Несе в собі код довжини поля даних в октетах, яке йде відразу після заголовка пакета. Якщо код дорівнює нулю, то довжина поля даних записана в полі даних “jumbo”, що у свою чергу зберігається в зоні опцій.

Наступний заголовок (Next Header) – 8-бітове поле. Ідентифікує тип заголовка, який іде безпосередньо за основним IPv6 заголовком. Кожний наступний додатковий заголовок також може містити поле Next Header. Якщо IP-пакет не має додаткових заголовків, то значення в цьому полі вказує на тип протоколу верхнього рівня, який вклад власне повідомлення в поле даних IP-пакета (TCP, UDP, RIP, OSPF і т.д.), визначений в стандарті IPv4 (аналогічно полю "Protocol" у версії IPv4).

Граничне число кроків – 8-бітове ціле число без знака. Зменшується на 1 у кожному маршрутизаторі, через який проходить пакет. При граничному числі кроків, рівному нулю, пакет видаляється маршрутизатором (аналог поля TTL в IPv4).

Адреса відправника – 128-бітова адреса відправника пакета.

Адреса одержувача – 128-бітова адреса одержувача пакета (може бути не кінцевий одержувач, якщо присутній маршрутний заголовок).

У пропозиціях по IPv6 фігурують наступні типи додаткових заголовків:

- Routing – заголовок для визначення повного маршруту при маршрутизації від джерела (Source Routing);
- Fragmentation – містить інформацію про фрагментацію IP-пакета. Поле обробляється тільки в кінцевих вузлах;
- Authentication – заголовок містить інформацію, необхідну для аутентифікації кінцевих вузлів і забезпечення цілісності вмісту IP-пакетів;
- Encapsulation – заголовок містить інформацію, необхідну для забезпечення конфіденційності переданих даних шляхом виконання шифрування та дешифрування;
- Hop-by-Hop Option – спеціальні параметри, що використовуються при виконанні обробки пакетів по алгоритму Hop-by-Hop;
- Destination Options – заголовок містить додаткову інформацію для вузла призначення.

Таким чином, пакет IPv6 може мати формат, як, наприклад, наведений на рис. 5.23.

Рисунок 5.23 - Структура пакета IPv6

Оскільки маршрутизатори обробляють лише основні заголовки (майже всі додаткові заголовки обробляються тільки в кінцевих вузлах), це збільшує їхню продуктивність і, тим самим, пропускну здатність мережі. Нагадаємо, що в IPv4 всі опції обробляються маршрутизаторами.

З іншого боку, можливість використання великої кількості додаткових параметрів розширює функціональність протоколу IP і робить його відкритим.

5.9.5. Зниження навантаження на маршрутизатори

Для того, щоб підвищити продуктивність маршрутизаторів Internet по виконанню їхньої основної функції – просуванню пакетів, у версії IPv6 вжито ряд заходів по звільненню маршрутизаторів від деяких допоміжних робіт. А саме.

- **Перенесення функцій фрагментації з маршрутизаторів на кінцеві вузли.** Кінцеві вузли у версії IPv6 зобов'язані знайти мінімальний розмір MTU уздовж всього шляху, що з'єднує вихідний вузол з вузлом призначення (ця техніка за

назвою Path MTU Discovery уже використовується в IPv4). Маршрутизатори IPv6 не виконують фрагментацію, а тільки посилають повідомлення по протоколу ICMP "Занадто довгий пакет" кінцевому вузлу, який повинен зменшити розмір пакета.

- **Агрегування адрес**, що веде до зменшення розміру адресних таблиць маршрутизаторів, а отже, до зменшення часу перегляду таблиць і часу, що витрачається на їхнє відновлення При цьому також зменшується службовий трафік, що створюється протоколами маршрутизації.
- **Широке використання маршрутизації від джерела** (Souice Routing), при якій вузол-джерело задає повний маршрут проходження пакета через мережі. Така техніка звільняє маршрутизатори від роботи по перегляду адресних таблиць при виборі наступного маршрутизатора і тим самим підвищує пропускну здатність Internet.
- **Відмова від обробки опціональних параметрів заголовка**.
- **Використання як номеру вузла його MAC-адреси**, що звільняє маршрутизатори від необхідності застосовувати ARP-протокол.

5.10. Особливості системи доменних імен (DNS)

Поняття адрес та імен вузлів

У мережі TCP/IP використовуються наступні типи адрес та імен вузлів.

Машинні адреси (фізичні, MAC-адреси). Це – унікальна адреса, яка «зашита» в мережеве апаратне забезпечення, наприклад, в карту мережного адаптера персонального комп'ютера. Машинна адреса складається з 12 шістнадцяткових цифр (наприклад, 00 04 AC 26 5E 8Б). При написанні для зручності сприйняття цю адресу групується в шість пар по дві цифри. MAC-адреса ідентифікує вузол в одному домені широкомовлення (на одному каналі).

IP-адреси. Логічна адреса, яка ідентифікує вузол в конкретній IP-мережі.

Ім'я NetBIOS (Windows ім'я) - ім'я комп'ютера в локальній Windows мережі. Розраховане на роботу мережі по стеку NetBIOS/NetBEUI. При використанні

стеку TCP/IP у локальній Windows мережі для розпізнавання NetBIOS імен необхідно обов'язково включити опцію «NetBIOS over TCP/IP» в налаштуванні властивостей протоколу TCP/IP. NetBIOS ім'я може мати довжину до 15 символів.

Ім'я хоста. Це ім'я комп'ютера або пристрою в мережі TCP/IP (зазвичай, в Інтернеті). У комбінації з ім'ям Інтернет-домену визначає повністю специфіковане доменне ім'я - FQDN (Fully Qualified Domain Name).

Ім'я домену. Може використовуватись як у локальних Windows мережах, так і у глобальних мережах. У першому випадку воно визначає ім'я домену Active Directory і у комбінації з NetBIOS ім'ям вузла формує повне ім'я вузла у конкретному Windows домені (може розглядатись як аналог FQDN ім'я вузла у Windows домені). В Інтернеті – це ім'я інтернет-домену (наприклад, kpi.ua).

Механізми розпізнавання імен вузлів

Практично в кожній мережі потрібен механізм, що дозволяє перетворювати імена комп'ютерів в IP-адреси і навпаки. Ця вимога обумовлена тим, що користувачі і додатки зазвичай звертаються до комп'ютерів в мережі по іменах, і лише служби нижнього рівня звертаються до мережевих вузлів по IP-адресам.

Існують наступні служби і механізми, які можуть бути використані для вирішення задачі розпізнавання імен:

- WINS (Windows Internet Name Service) - встановлює відповідність NetBIOS імен з IP адресами ;
- DNS (Domain Name System) - встановлює відповідність доменних імен (FQDN) з IP адресами;
- файл Hosts - спрощений аналог системи DNS;
- файл Lmhosts - - спрощений аналог системи WINS;
- відправлення широкомовних запитів.

Найбільш поширеним механізмом є DNS.

Побудова системи імен в Інтернеті

Система іменування DNS являє собою ієрархічну і логічну деревоподібну

структуру, яку називають **простір імен DNS** (DNS namespace), де є один корінь, у якого може бути будь-яке число піддоменів. У окремих піддоменів в свою чергу можуть бути дочірні піддомени. Наприклад, в просторі імен Інтернету корінь "" (порожній рядок) об'єднує безліч доменних імен верхнього рівня, одне з яких - .ua. У домені ua може бути піддомен НТУУ «КПІ»: kpi.ua, який в свою чергу є батьківським для дочірнього домену наступного рівня, наприклад домену факультету електроніки: fel.kpi.ua. Організації мають право створювати приватні мережі та використовувати власні, недоступні з Інтернету, простори DNS-імен.

Кожен вузол в дереві DNS-домену ідентифікується по його повному доменному імені (FQDN), яке однозначно визначає його розташування по відношенню до кореня дерева доменів. Наприклад, FQDN поштового сервера в домені kpi.ua буде mail.kpi.ua. Воно являє собою об'єднання імені вузла (mail) основного суфікса DNS домена (kpi.ua) і замикаючої крапки (.). Замикаюча крапка є стандартним роздільником доменної мітки верхнього рівня і міткою порожнього рядка, відповідного кореню. При повсякденному використанні замикаючу крапку часто опускають, але її додає служба DNS-клієнта при виконанні запитів.

Корінь (самий верхній рівень) простору імен Інтернету управляється міжнародною організацією ICANN (Internet Corporation for Assigned Names and Numbers). Ця організація координує присвоєння ідентифікаторів, які повинні бути унікальними у всьому Інтернеті, в тому числі доменних імен, IP-адрес, параметрів протоколів і номерів портів. Нижче кореневого рівня розташовуються домени верхнього рівня, які також перебувають під управлінням ICANN. Існує два типи таких доменів.

Організаційні домени - в їх імені присутній трибуквений код, який вказує на основний рід діяльності організацій даного DNS-домену (наприклад, com – комерційні організації, edu – освітянські організації, gov – урядові організації і т.і.). Деякі домени організацій мають глобальний характер, інші виділяються тільки організаціям всередині США.

Географічні домени - в їх імені присутній двобуквений код країни або регіону, як визначено Міжнародною організацією зі стандартизації (ISO 3166) (наприклад, ua - Україна, ru - Росія, uk - Великобританія і т.і.). Ці домени виділяються організаціями поза США, хоча ця вимога дотримується не занадто жорстко.

Нижче доменів верхнього рівня ICANN та інші уповноважені органи, які відповідають за присвоєння імен в Інтернеті, передають домени різним організаціям, наприклад Microsoft (microsoft.com) або НТУУ «КПІ» (kpi.ua). Ці організації підключаються до Інтернету і присвоюють імена вузлів в межах своїх доменів (рис. 5.24).

Крім того, організації надають піддомени своїм користувачам або клієнтам. Наприклад, інтернет-провайдери отримують домен від ICANN і можуть передавати піддомени в розпорядження своїх клієнтів. Для перетворення імен в IP-адреси в зоні дії простору імен організації використовуються DNS-сервери.

Організації вправі організовувати приватний простір імен (private namespace), тобто простір DNS-імен, в основі якого кілька кореневих серверів, повністю незалежних від простору доменних імен Інтернету. В рамках приватного простору імен можна призначати імена та створювати власний кореневий домен або домени і будь-які необхідні піддомени. Приватні імена недоступні і не дозволяються в Інтернеті. Приклад приватного доменного імені: mycompany.local.

Принципи функціонування системи DNS

Відповідність між доменними іменами (FQDN) і IP-адресами може встановлюватися як засобами локального вузла, так і засобами централізованої служби. Найпростішим рішенням є створення вручну текстового файлу з ім'ям hosts. Цей файл складається з деякої кількості рядків, кожна з яких містить запис типу «IP-адреса - доменне ім'я», наприклад, 77.47.129.30 – www.kpi.ua.

Файл необхідно розмістити у відповідному системному каталогу (наприклад, у випадку Windows-систем це каталог \WINDOWS\system32\drivers\etc).

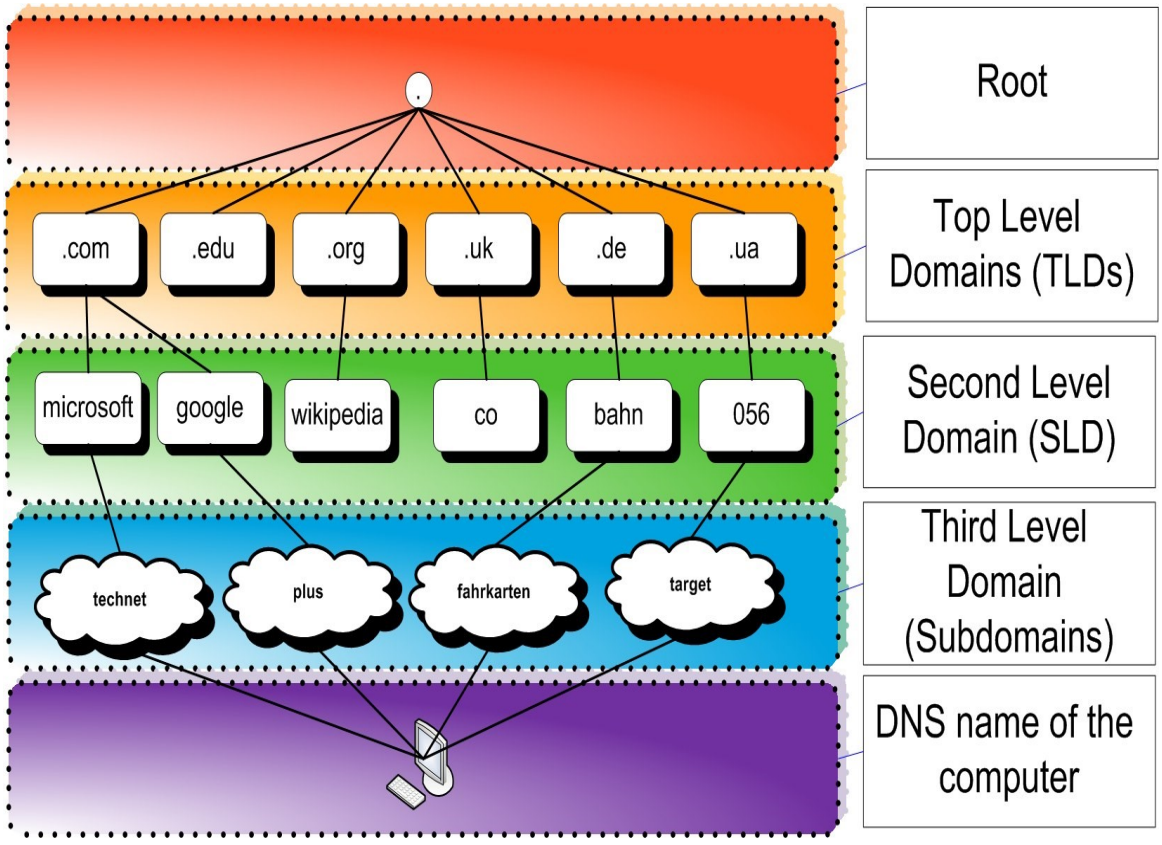


Рисунок 5.24 - Структура простору імен DNS

У загальному випадку для вирішення задачі встановлення відповідності доменних імен і IP-адрес використовується спеціальна служба - *система доменних імен (Domain Name System, DNS).* DNS - це централізована служба, заснована на розподіленій базі відображень «доменне ім'я - IP-адреса». Служба DNS використовує в своїй роботі схему взаємодії типу «клієнт-сервер». У рамках цієї взаємодії визначені DNS-сервери і DNS-клієнти. DNS-сервери підтримують розподілену базу записів, а DNS-клієнти звертаються до серверів із запитами на визначення IP-адреси по конкретному доменному імені вузла або ресурсу. Таким чином, DNS забезпечує механізми як для іменування вузлів, так і для пошуку IP- адрес вузлів по іменах.

Служба DNS використовує текстові файли майже такого ж формату, як і файл hosts, і ці файли адміністратор також може корегувати вручну. Проте, служба DNS спирається на ієрархію доменів, і кожен сервер служби DNS зберігає тільки частину імен мережі, а не всі імена, як це відбувається при використанні файлів hosts. При зростанні кількості вузлів в мережі проблема масштабування вирішується створенням нових доменів і піддоменів імен і додаванням в службу DNS нових серверів.

Для кожного домена імен створюється свій DNS-сервер. Цей сервер може зберігати записи «доменне ім'я - IP-адреса» для всього домена, включаючи всі його піддомени. Частіше сервер домена зберігає тільки імена, які закінчуються на наступному нижче рівні ієрархії в порівнянні з ім'ям домена. Саме при такій організації служби DNS навантаження розподіляється більш-менш рівномірно між всіма DNS-серверами мережі. Наприклад, в першому випадку DNS-сервер домена kpi.ua зберігатиме відображення для всіх імен, що закінчуються на kpi.ua. В другому випадку цей сервер зберігає відображення тільки імен типу fel.kpi.ua, fiot.kpi.ua, а решта всіх записів нижчих рівнів ієрархії повинна зберігатися на DNS-серверах піддоменів fel і fiot.

Кожен DNS-сервер окрім таблиці відображень імен містить посилання на DNS-сервери своїх піддоменів. Ці посилання зв'язують окремі DNS-сервери в єдину службу DNS. Посиланнями є IP-адреси відповідних серверів. Для обслуговування кореневого домена виділено декілька дублюючих один одного DNS-серверів, IP-адреси яких є широко відомими.

Схеми використання системи DNS

Існують дві основні схеми роботи системи DNS. У першому варіанті роботу по пошуку IP-адрес координує DNS-клієнт:

- DNS-клієнт звертається до DNS-серверу, адреса якого явно вказана в налаштуваннях IP-протоколу конкретного вузла (надалі, локальний), із запитом. В запиті він передає повне доменне ім’я вузла, IP-адресу якого необхідно визначити;

- DNS-сервер відповідає, повертаючи клієнту адресу наступного DNS-сервера, обслуговуючого домен верхнього рівня, указаний в старшій частині доменного імені, яке надійшло у запиті;

- DNS-клієнт посилає запит на наступний DNS-сервер, який посилає його до DNS-серверу потрібного піддомена, і т. д., поки не буде знайдений DNS-сервер, в якому зберігається відповідність запитаного імені IP-адресі. Цей сервер дає остаточну відповідь клієнтові.

Така схема взаємодії називається нерекурсивною або ітеративною, коли клієнт сам виконує послідовність запитів до різних серверів імен. Оскільки ця схема завантажує клієнта достатньо складною роботою, то вона застосовується рідко.

У другому варіанті реалізується рекурсивна процедура:

- DNS-клієнт посилає запит на локальний DNS-сервер, аналогічно попередній процедурі;

- якщо локальний DNS-сервер знає відповідь, то він відразу ж повертає його клієнтові; це може відповідати випадку, коли запитане ім'я входить в той же піддомен, що і ім'я клієнта, а також може відповідати випадку, коли сервер вже дізнавався про дану відповідність для іншого клієнта і зберіг її в своєму кеші;

- якщо ж локальний сервер не знає відповідь, то він надсилає запити до кореневого сервера і так далі, як це робив клієнт в попередній процедурі. Отримавши відповідь, він передає його клієнтові, який весь цей час просто чекає її від свого локального DNS-сервера.

У цій схемі клієнт передоручає роботу своєму серверу, тому схема називається непрямою або рекурсивною. Практично всі DNS-клієнти використовують рекурсивну процедуру.

Для прискорення пошуку IP-адрес DNS-сервери широко застосовують процедуру кешування відповідей, що проходять через них. Щоб служба DNS могла оперативно відпрацьовувати зміни, що відбуваються в мережі, відповіді кешуються на певний час - зазвичай від декількох годин до декількох днів.

Порядок визначення імен за механізмом DNS має такий вигляд:

• пошук імені в кеші DNS-клієнта. Імена потрапляють в кеш при більш ранніх запитах;

• пошук імені в файлі Hosts (для Windows - систем розташований в папці Windows \ System32 \ Drivers \ Etc);

• запит DNS-сервера

Основні поняття і записи, які використовуються у системі DNS

Для нормальної роботи DNS необхідно правильно сконфігурувати DNS-сервери, зони і зробити необхідні записи.

DNS-сервер - це комп'ютер з відповідними програмними додатками, наприклад, служба DNS-сервера в Windows, або служба BIND в UNIX-системах. DNS-сервери підтримують базу даних DNS з інформацією про частини структури доменного дерева DNS і обробляють запити на дозвіл імен, що надходять від DNS-клієнтів. У відповідь на запит клієнта DNS-сервер надає запитувану інформацію, дає посилання на інший сервер, який може відповісти на запит, або повідомляє, що інформація недоступна або не існує. DNS-сервери поділяються на основні (повноважні) та резервні (додаткові). Для кожної зони може існувати тільки один основний сервер (на якому можна вносити зміни в зонну інформацію) і будь-яка кількість резервних серверів (які отримують інформацію про зону з основного серверу). Встановлення резервних DNS серверів дозволяє вирішити дві задачі: збільшити надійність роботи системи DNS, розподілити запити клієнтів по різним серверам, збільшуючи таким чином продуктивність роботи системи DNS.

Зона DNS (DNS zone) - це єдина частина простору імен та IP - адрес, що обслуговується повноважним сервером. Сервер може обслуговувати і кілька зон, а зона може містити один або декілька Інтернет - доменів. Наприклад, один сервер може бути повноважним для зон kpi.ua і kpi.edu, кожна з яких містить декілька доменів. Суміжні домени, наприклад, kpi.ua, fel.kpi.ua і keoa.fel.kpi.ua можна перетворити в окремі зони, застосувавши делегування, при якому

відповідальність за піддомен всередині простору імен DNS присвоюється окремому об'єкту (відповідному DNS – серверу).

Файли зон (zone files) містять записи ресурсів зон, в яких сервер є повноважним. У багатьох реалізаціях DNS-сервера дані зон зберігаються в текстових файлах; DNS-сервери на контролерах доменів під керуванням Windows 2000 або Windows Server 2003 можуть також зберігати зонну інформацію в Active Directory.

Існують два види зон: прямого і зворотного перегляду. У перших виконується зіставлення FQDN-імен з IP-адресами, у других навпаки, IP-адреси зіставляються з повними доменними іменами. Таким чином, зони прямого перегляду обслуговують запити по встановленню відповідності між FQDN-іменами і IP-адресами, а зони зворотного перегляду - між IP-адресами і FQDN-іменами.

Якщо ім’я прямої зони співпадає з іменем домену, то ім’я зворотної зони формується з мережної частини IP-адреси, записаної в зворотному порядку, до якої додається стандартний префікс - in-addr.arpa. Наприклад, кафедрі КЕОА виділено блок IP-адрес 10.12.80.0/24. Ім’я зворотної зони – 80.12.10. in-addr.arpa.

Існують поняття основної зони, додаткової зони і зони – заглушки.

Основна зона зберігає базові дані для всіх доменів в зоні. Резервна копія бази даних зони може створюватися в додатковій зоні.

Додаткова зона - повноважна резервна зона для основної зони або інших додаткових зон.

Зона-заглушка (розміщується на сервері) - копія зони, що містить тільки записи ресурсів повноважних DNS-серверів основної зони (master zone).

Записи ресурсів (resource records) - це інформація, що зберігається в базі даних DNS і використовувана для відповіді на запити DNS-клієнтів.

Кожен DNS-сервер містить записи ресурсів, необхідні йому для відповіді на запити, що відносяться до його частини простору імен DNS. Записи ресурсів розрізняються за типами: наприклад, адресний запис (A), канонічне ім'я

(CNAME), сервер імен (NS), поштовий обмінник (MX).

Найбільш важливі типи DNS-записів.

Запис A (address record) або запис адреси - зв'язує ім'я вузла з IP - адресою. Наприклад, запит A-запису на ім'я www.kpi.ua поверне його IP- адресу - 10.7.10.22.

Запис AAAA (IPv6 address record) зв'язує ім'я вузла з адресою протоколу IPv6.

Запис CNAME (canonical name record) або канонічний запис імені (псевдонім) використовується для перенаправлення на інше ім'я. Дозволяє одній IP- адресі поставити у відповідність декілька імен.

Запис MX (mail exchange) або поштовий обмінник - вказує сервер (и) обміну поштою для даного домену.

Запис NS (name server) - вказує на DNS-сервер для даного домену.

Запис PTR (pointer) або запис вказівника - зв'язує IP - адресу вузла з його канонічним ім'ям. Використовується у зворотній зоні і є аналогом A-запису у прямій зоні. Запит PTR запису в зворотній зоні in-addr.arpa на IP - адресу вузла поверне ім'я (FQDN) даного вузла. З метою зменшення обсягу небажаної кореспонденції (спаму) багато серверів-одержувачів електронної пошти можуть перевіряти наявність PTR запису для вузла, з якого відбувається відправлення. У цьому випадку PTR запис для IP - адреси повинен відповідати імені відправляючого поштового сервера, яким він представляється в процесі SMTP сесії.

Запис SOA (Start of Authority) або початковий запис зони – вказує на основний DNS – сервер зони, на якому зберігається еталонна інформація про зону, містить контактну інформацію особи, відповідальну за дану зону, задає параметри (серійний номер та часові параметри), необхідні для оновлення інформації про зону резервними DNS-серверами.

SRV-запис (server selection) вказує на сервери для деяких сервісів; використовується, зокрема, для Jabber і Active Directory.

Запис TXT (Text) - текстовий запис, який використовується для внесення коментаріїв, поміток і т.і.

Питання для самоперевірки та контролю засвоєння знань

1. На які рівні поділяють протоколи стеку TCP/IP?
2. Якому рівню моделі OSI відповідає рівень мережних інтерфейсів стеку TCP/IP?
3. Якому рівню моделі OSI відповідає мережний (Інтернет) рівень стеку TCP/IP?
4. Якому рівню моделі OSI відповідає транспортний (основний) рівень стеку TCP/IP?
5. Які завдання вирішуються на рівні мережних інтерфейсів стеку TCP/IP?
6. Які протоколи стеку TCP/IP працюють на мережному рівні?
7. Який протокол мережного рівня стеку TCP/IP відповідає за доставку пакетів?
8. Які протоколи стеку TCP/IP працюють на транспортному рівні?
9. Який з протоколів транспортного рівня стеку TCP/IP забезпечує надійну доставку даних?
10. Який з протоколів транспортного рівня стеку TCP/IP не забезпечує надійну доставку даних?
11. Який з протоколів транспортного рівня стеку TCP/IP працює у режимі зі встановленням з'єднання?
12. Який з протоколів транспортного рівня стеку TCP/IP працює у дейтаграмному режимі?
13. На які протоколи стеку TCP/IP покладено функції виправлення помилок передачі при використання транспортного протоколу TCP?
14. На які протоколи стеку TCP/IP покладено функції виправлення помилок передачі при використання транспортного протоколу UDP?
15. Які функції забезпечують протоколи прикладного рівня стеку TCP/IP?
16. У якому режимі (зі встановленням з'єднання чи дейтаграмному) працює протокол IP?
17. З якою метою протокол IP проводить фрагментацію дейтаграм?
18. Яке поле в IP - пакеті задає необхідний режим доставки дейтаграми?

19. Яке поле в IP – пакеті використовується для зборки з фрагментів цілісної дейтаграми?
20. Для якої мети використовується поле «Час життя» (TTL - time to live) в IP – пакеті?
21. Коли зменшується значення в полі «Час життя» (TTL - time to live) IP – пакету?
22. Які функції виконує протокол ICMP?
23. Які корегуючи діє по виправленню помилок передачі виконує протокол ICMP?
24. Для якої цілі використовується exo-повідомлення ICMP – протоколу?
25. Про що свідчить повідомлення про «недосяжність вузла призначення» ICMP – протоколу?
26. Про що свідчить повідомлення про «недоступність мережі» ICMP – протоколу?
27. Про що свідчить повідомлення про «недоступність вузла» ICMP – протоколу?
28. Про що свідчить повідомлення про «недоступність протоколу» ICMP – протоколу?
29. Про що свідчить повідомлення про «недоступність порта» ICMP – протоколу?
30. З якою метою маршрутизатор відправляє повідомлення про зміну маршруту ICMP – протоколу?
31. Які функції виконує протокол ARP?
32. Для чого необхідно встановлювати відповідність між IP – адресами вузлів і MAC – адресами?
33. На яку адресу надсилає запит ARP - протокол?
34. Що зробить з пакетом вузол, якщо на ARP – запит не надійде відповідь?
35. Чи прийде відповідь на ARP – запит від вузла, який знаходиться в іншій IP – мережі?

36. Хто видасть відповідь на ARP – запит про вузол, який знаходиться в іншій IP – мережі?

37. Чия MAC- адреса буде вказані в ARP – відповіді про вузол, який знаходиться в іншій IP – мережі?

38. Для якої мети використовуються самозвернені (gratuitous) ARP – запити?

39. Який пристрій в мережі обслуговує RARP – запити?

40. За рахунок чого досягається надійна доставка даних TCP – протоколом?

41. Що розуміють під портом TCP – протоколу?

42. Що розуміють під сокетом TCP – протоколу?

43. Що визначає сонет TCP – протоколу?

44. Які функції виконує процедура трьохетапної синхронізації TCP – протоколу?

45. Які функції виконує алгоритм «козаючого вікна» в TCP – протоколі?

46. Що являє собою «вікно» TCP – протоколу?

47. Про що говорить нульовий розмір вікна TCP – протоколу?

48. В пакет якого протоколу інкапсулюються пакети TCP – протоколу?

49. У якому режимі (зі встановленням з’єднання чи дейтаграмному) працює протокол UDP?

50. В пакет якого протоколу інкапсулюються пакети UDP – протоколу?

51. На протоколи якого рівня покладаються функції виправлення помилок передачі при використання протоколу UDP?

52. Які існують класи IP-адрес?

53. Що визначає маска в IP-адресації ?

54. Як за допомогою маски визначити довжину мережної частини IP –адреси?

55. Як за допомогою маски визначити довжину частини IP –адреси, яка вказує на номер вузла в мережі?

56. Як за допомогою маски визначити конкретний ідентифікатор мережі в IP – адресі?

57. Як за допомогою маски визначити конкретний ідентифікатор вузла в IP – адресі.

58. Які з IP –адрес не можуть належати вузлу?

59. Які з IP –адрес не можуть з’явитися в адресному полі пакета?

60. Пакет з якою IP –адресою в адресному полі одержувача отримають усі вузли конкретної IP-мережі?

61. Пакет з якою IP –адресою в адресному полі одержувача отримають усі вузли IP-мережі, у якій знаходиться вузол відправник пакета?

62. Пакет з якою IP –адресою в адресному полі одержувача пройде через маршрутизатор?

63. Які IP –адреси не можуть з’явитися в адресному полі одержувача пакета?

64. Які IP –адреси не можуть з’явитися в адресному полі відправника пакета?

65. Пакет з якою IP –адресою в адресному полі одержувача отримає група вузлів в різних IP-мережах?

66. Яка IP –адреса вказують на відсутність IP –адреси у вузла?

67. За допомогою маски підмережі розбити IP-мережу 192.168.10.0 на 8 підмереж. Навести маску та діапазон адрес, які можуть бути використані для адресації вузлів, для першої підмережі та останньої.

68. За допомогою маски підмережі розбити IP-мережу 116.0.0.0 на 6 підмереж. Навести маску та діапазон адрес, які можуть бути використані для адресації вузлів, для першої підмережі та останньої.

69. За допомогою маски підмережі розбити IP-мережу 180.218.0.0 на 16 підмереж. Навести маску та діапазон адрес, які можуть бути використані для адресації вузлів, для першої підмережі та останньої.

70. Визначити, до якого класу IP – адрес належить адреса 129.100.100.1 (маска 255.255.255.0). Вказати ознаку належності до класу.

71. Яку довжину має адреса IPv6?

72. Скільки частин ідентифікації мереж та вузлів виділяють у адресі IPv6?

73. Які задачі дозволяє вирішувати багаторівнева схема ідентифікації мереж в IPv6?

74. Яка форма запису адреси використовується в IPv6?

75. Яке скорочення може бути використано для заміни довгої послідовності нулів в адресі IPv6?
76. Скільки разів в адресі IPv6 можна використати таке скорочення?
77. Чи можна опускати незначущі нулі в полях адреси IPv6?
78. Що характерно для адреси, яка може використовуватись у мережах з протоколами IPv4 та IPv6?
79. Яким чином визначені класи адрес в IPv6?
80. Які типи адрес визначені в IPv6?
81. Чим визначається тип адреси в IPv6?
82. Для чого застосовуються адреси типу “unicast” в IPv6?
83. Для чого застосовуються адреси типу “multicast” в IPv6?
84. Який префікс формату має адреса типу “multicast” в IPv6?
85. Що визначає поле “scope” в “multicast” адресі IPv6?
86. Для чого застосовуються адреси типу “broadcast” в IPv6?
87. Для чого застосовуються адреси типу “anycast” в IPv6?
88. Яким вузлам мережі можуть призначатися адреси типу “anycast” в IPv6?
89. Що розуміють під локальними адресами в IPv6?
90. На які типи поділяються локальні адреси в IPv6?
91. Що характерно для локальних адрес типу “Link Local”?
92. Що характерно для локальних адрес типу “Unique Local Unicast”?
93. Для чого застосовуються глобальні агреговані унікальні адреси в IPv6?
94. Скільки полів має формат глобальної агрегованої унікальної адреси в IPv6?
95. Скільки полів в форматі глобальної агрегованої унікальної адреси IPv6 використовується для ідентифікації мереж?
96. Скільки полів в форматі глобальної агрегованої унікальної адреси IPv6 використовується для ідентифікації вузла?
97. Що визначає префікс верхнього рівня – TLA в адресі IPv6?
98. Що визначає префікс наступного рівня – NLA в адресі IPv6?
99. Що визначає префікс місцевого рівня – SLA в адресі IPv6?
100. Що визначає ідентифікатор інтерфейсу в адресі IPv6?

101. Як ARP- протокол встановлює відповідність між IPv6-адресою та MAC-адресою вузла?

102. Які існують типи спеціальних “unicast” адрес в IPv6?

103. Наведіть адресу зворотної петлі (loopback) в IPv6?

104. Наведіть невизначену адресу в IPv6?

105. Для чого застосовують агрегування адрес?

106. Як задається префікс мереж при застосуванні технології CIDR в IPv4?

107. Скільки необхідно записів в таблиці маршрутизації для представлення маршрутів в мережі з однаковим префіксом?

1088. Чи існує в IPv6 поняття маски мережі певного класу?

109. Що визначає маска мережі в IPv6 ?

110. Що розуміють під операцією агрегування (superneting)?

111. Що розуміють під операцією subneting?

112. Яка з операцій (superneting або subneting) використовується в IPv6?

113. Які поля адреси IPv6 можуть використовувати провайдери для агрегування мереж?

114. Які поля адреси IPv6 може використовувати адміністратор корпоративної мережі для агрегування мереж?

115. Чи будуть ідентифікатори мереж клієнтів одного провайдера мати загальну частину при використання техніки агрегування?

116. Де встановлюється значення маски за замовчуванням в адресах IPv6 кінцевого абонента?

117. Чи можна скоротити кількість записів в таблицях маршрутизації в великій корпоративній мережі?

118. Для чого змінено формат заголовку в IPv6 ?

119. Які типі заголовків визначені в IPv6 ?

120. Що визначає значення в полі “Версія” заголовку?

121. Для чого застосовується поле “Пріоритет” заголовку?

122. Що визначає поле “Наступний заголовок”?

123. Що вказується в полі “Наступний заголовок” при використання тільки основного заголовку?

124. Для чого використовується поле “Гранічне число кроків”?

125. Для чого використовується додатковий заголовок “Routing”?

126. Для чого використовується додатковий заголовок “Fragmentation”?

127. Які заголовки обробляються маршрутизаторами IPv6 ?

128. Які механізми, реалізовані в IPv6, дозволяють знизити навантаження на маршрутизатори?

129. Яку функцію виконує система DNS?

130. На які типи поділяють домени в Інтернеті?

131. Що розуміють під зоною DNS?

132. Які типи зон DNS існують?

133. Як формується ім’я прямої зони?

134. Як формується ім’я зворотної зони?

135. На які типи поділяються DNS – сервери, які обслуговують зону?

136. Що визначає запис SOA?

137. Що визначає запис NS?

138. Що визначає запис MX?

139. Що визначає запис A?

140. Що визначає запис TXT?

142. Що визначає запис PTR?

ПРОТОКОЛИ МАРШРУТИЗАЦІЇ

Маршрутизація - це переміщення інформації по об'єднаній мережі від джерела до одержувача. На цьому маршруті зустрічається як мінімум один проміжний вузол. При здійсненні маршрутизації виконуються дві основні дії: визначення маршрутів і транспортування інформаційних груп (пакетів) по об’єднаній мережі. В термінах маршрутизації остання операція називається комутацією пакетів. Комутація пакетів відносно проста дія, тоді як визначення оптимального маршруту може виявитися вельми складним.

Більшість протоколів маршрутизації [О: 2, 5, 7; Д: 11, 12, 13], які застосовуються у сучасних мережах з комутацією пакетів, ведуть своє походження від мережі Internet і її попередниці - мережі ARPANET. Для того щоб зрозуміти їхнє призначення й особливості, корисно спочатку ознайомитись зі структурою мережі Internet, що наклала відбиток на термінологію й типи протоколів.

Мережа Internet будувалася як мережа, що поєднує велику кількість окремих мереж. Із самого початку в її структурі виділяли ***магістральну мережу*** (***core backbone network***), а мережі, приєднані до магістралі, розглядалися як ***автономні системи*** (***autonomous systems, AS***). Магістральна мережа й кожна з автономних систем мали своє власне адміністративне управління й власні протоколи маршрутизації. Такі системи ще називають ***доменом маршрутизації***. Необхідно підкреслити, що автономна система й домен імен Internet - це різні поняття, які служать різним цілям. ***Автономна система*** поєднує мережі, у яких під загальним адміністративним керівництвом однієї організації здійснюється маршрутизація, а домен імен Internet об'єднує комп'ютери (які, можливо, належать різним мережам), у яких під загальним адміністративним керівництвом однієї організації здійснюється призначення унікальних символьних імен. Області дії автономної системи й домена імен можуть в окремому випадку збігатися, якщо одна організація виконує обидві указані функції.

Загальна структура мережі Internet показана на рис. 6.1. В традиційній термінології Internet маршрутизатори називають шлюзами.

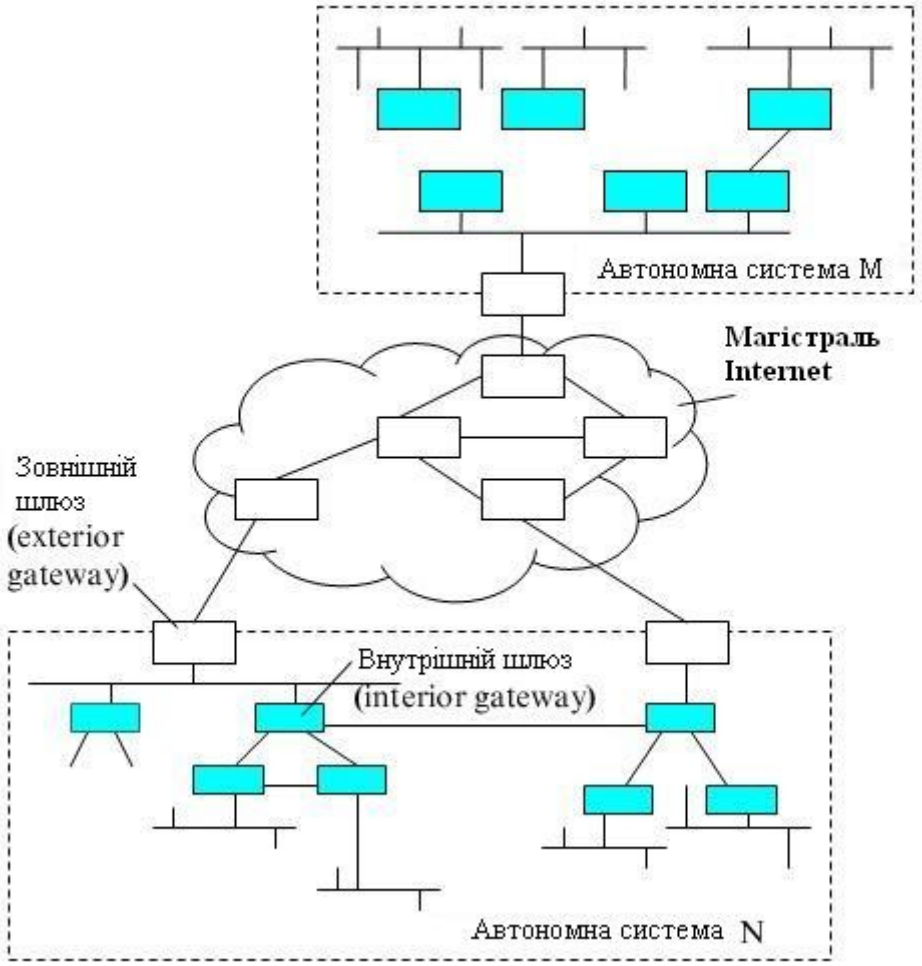


Рисунок 6.1 - Магістраль і автономні системи Internet

Шлюзи, які використовуються для утворення мереж і підмереж усередині автономної системи, називаються ***внутрішніми шлюзами*** (***interior gateways***), а шлюзи, за допомогою яких автономні системи приєднуються до магістралі мережі, називаються ***зовнішніми шлюзами*** (***exterior gateways***). Магістраль мережі також є автономною системою. Всі автономні системи мають унікальний 16-розрядний номер, що виділяється організацією, яка заснувала нову автономну систему - **InterNIC**.

Відповідно, протоколи маршрутизації усередині автономних систем називаються ***протоколами внутрішніх шлюзів*** (***interior gateway protocol, IGP***)

(ще їх називають внутрішньодоменними або внутрішніми), а протоколи, що визначають обмін маршрутною інформацією між зовнішніми шлюзами й шлюзами магістральної мережі — ***протоколами зовнішніх шлюзів*** (***exterior gateway protocol, EGP***) (***ще їх називають міждоменнними або зовнішніми)***. Усередині магістральної мережі також допустимо використовувати будь-який власний внутрішній протокол IGP.

Смисл розподілу всієї мережі Internet на автономні системи - у її багаторівневому модульному представленні, що забезпечує масштабування, необхідне для будь-якої великої системи. Зміна протоколів маршрутизації усередині якої-небудь автономної системи ніяк не повинна впливати на роботу інших автономних систем. Крім того, розподіл Internet на автономні системи повинен сприяти агрегуванню інформації в магістральних і зовнішніх шлюзах. Внутрішні шлюзи можуть використовувати для внутрішньої маршрутизації досить детальні графи зв'язків між собою, щоб вибрати найбільш оптимальний маршрут. Однак, якщо інформація такого ступеня деталізації буде зберігатися у всіх маршрутизаторах мережі, то маршрутні таблиці так розростуться, що потребують наявності пам'яті дуже великих розмірів, а час прийняття рішень по маршрутизації пакетів стане неприйнятно великим.

Тому детальна топологічна інформація залишається усередині автономної системи, а автономну систему як єдине ціле для іншої частини Internet представляють зовнішні шлюзи, які повідомляють про внутрішній склад автономної системи мінімально необхідні відомості - кількість IP-мереж, їхні адреси й внутрішню відстань до цих мереж від даного зовнішнього шлюзу.

Таким чином, дані протоколів верхніх рівнів стеку TCP/IP передаються по об'єднаній мережі з використанням протоколів маршрутизації. У цьому контексті протоколи верхніх рівнів ще називають маршрутизуємими протоколами (routed protocol) або мережними протоколами.

Терміни маршрутизуємий протокол (routed protocol) і протокол маршрутизації (routing protocol) часто помилково сприймають як рівноцінні і взаємозамінні. Маршрутизуємими є протоколи, дані яких передаються по

маршрутах об'єднаної мережі, такі, наприклад, як Internet Protocol (IP), протоколи DECnet, AppleTalk, Novell NetWare і т.і. Протоколи маршрутизації, навпаки, є протоколами, що реалізовують алгоритми маршрутизації. Іншими словами, протоколи маршрутизації використовуються проміжними системами для складання таблиць, по яких визначаються маршрути передачі даних маршрутизуємих протоколів. Протоколами маршрутизації є такі протоколи, як Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), Intermediate System-to-intermediate System (IS-IS) і Routing Information Protocol (RIP).

6.1. Класифікація алгоритмів маршрутизації

Алгоритми маршрутизації розрізняються за декількома ключовими характеристиками. По-перше, на роботу протоколу маршрутизації впливають цілі, які ставилися розробником алгоритму. По-друге, різні види алгоритмів по-різному використовують ресурси мережі і маршрутизаторів. Нарешті, алгоритми маршрутизації застосовують різні метрики, що впливають на вибір оптимальних маршрутів [О: 2, 5, 7; Д: 11, 12, 13].

Алгоритми маршрутизації можна класифікувати по наступних критеріях:

- статична або динамічна маршрутизація;
- наявність одного або декількох маршрутів до одного одержувача;
- лінійна або ієрархічна маршрутизація;
- виконання алгоритму на початковому вузлі або на проміжних маршрутизаторах;
- маршрутизація в рамках автономної системі або між автономними системами;
- маршрутизація за станом каналу або дистанційно-векторна маршрутизація.

Статична і динамічна маршрутизація

Алгоритми статичної маршрутизації представляють собою не стільки алгоритми, скільки таблиці, які складені мережним адміністратором на маршрутизаторах. Вміст цих таблиць може бути змінений тільки мережним адміністратором. Алгоритми, які використовують статичні маршрути, прості і ефективно працюють в порівняно простих мережах з відносно передбаченим характером передачі даних.

Оскільки системи статичної маршрутизації не реагують на зміни в мережі, вони, як правило, не підходять для сучасних великих мереж, що постійно змінюються. Більшість алгоритмів, що використовуються в даний час, є алгоритмами динамічної маршрутизації, які адаптуються до змін мережної обстановки, аналізуючи повідомлення, що поступають, про оновлення маршрутів. Якщо в повідомленні вказується на зміни в мережі, то програмне забезпечення маршрутизації наново обчислює маршрути і розсилає нові повідомлення про оновлення маршрутів. Ці повідомлення розповсюджуються по мережі, примушуючи маршрутизатори наново запускати алгоритми маршрутизації і вносити відповідні зміни в таблиці.

Іноді алгоритми динамічної маршрутизації доцільно доповнити статичними маршрутами.

Єдиний маршрут або декілька маршрутів

Деякі складні протоколи маршрутизації допускають існування декількох маршрутів до одного одержувача. На відміну від алгоритмів, що обчислюють тільки один маршрут, ці протоколи дозволяють розподілити потоки даних по декількох каналах. Переваги таких алгоритмів очевидні: вони значно прискорюють передачу даних і підвищують її надійність. Таку технологію звичайно називають розподілом навантаження (load sharing).

Лінійна та ієрархічна маршрутизація

Одні алгоритми маршрутизації працюють в лінійному просторі, а інші будують ієрархії маршрутів. У системах з лінійною маршрутизацією (flat routing) всі маршрутизатори рівноправні. У системах з ієрархічною

маршрутизацією деякі маршрутизатори утворюють аналог маршрутної магістралі. Пакети поступають від периферійних маршрутизаторів на магістральні маршрутизатори і передаються по магістралі, поки не досягнуть зони, де розташований одержувач. Потім вони з останнього магістрального маршрутизатора передаються одержувачу через один або декілька периферійних маршрутизаторів.

У системах маршрутизації часто створюються логічні групи вузлів, звані доменами, автономними системами або зонами. У системах з ієрархічною маршрутизацією одні маршрутизатори домену можуть обмінюватися даними з маршрутизаторами інших доменів, а інші - тільки з маршрутизаторами свого домену. У дуже крупних мережах іноді створюються додаткові рівні ієрархії, і тоді маршрутна магістраль утворюється маршрутизаторами вищого рівня.

Основна перевага ієрархічної маршрутизації полягає в тому, що вона повторює структуру більшості компаній і тому відповідає структурі передачі їх даних. Найбільш інтенсивний обмін даними відбувається усередині малих груп (доменів). Оскільки внутрішньодоменним маршрутизаторам потрібна інформація тільки про маршрутизатори, що належать до їх домену, їх алгоритми маршрутизації можна спростити і, відповідно, скоротити кількість повідомлень про оновлення маршрутів.

Алгоритми, що виконуються на вузлах-джерелах і на маршрутизаторах

У деяких алгоритмах маршрутизації весь маршрут визначається вузлом-джерелом. Звичайно такий підхід називається маршрутизацією на джерелі (source routing). У системах з маршрутизацією на джерелі маршрутизатори виконують тільки функції запам'ятовування адрес і пересилки пакетів наступному вузлу.

У інших алгоритмах передбачається, що вузлам-джерелам маршрути передачі даних невідомі. У цих алгоритмах шлях проходження по об'єднаній мережі визначається маршрутизаторами, на яких виконується обчислення маршруту. У першій з розглянутих вище систем вузол-джерело повинен бути

здатний визначати маршрут, в другій системі ці функції виконуються проміжними маршрутизаторами.

Маршрутизація в рамках автономної системі або між автономними системами

Одні алгоритми маршрутизації працюють тільки усередині доменів маршрутизації, інші - як усередині доменів маршрутизації, так і між ними. Природа цих двох типів алгоритмів різна, тому оптимальний алгоритм внутрішньодоменної маршрутизації не завжди є оптимальним для міждоменної маршрутизації.

Алгоритми маршрутизації за станом каналу і дистанційно-векторні алгоритми

Алгоритми маршрутизації за стану каналу (link-state), які також називають алгоритмами визначення найкоротшого маршруту, поширюють інформацію про маршрути по всіх вузлах об'єднаної мережі. Проте кожен маршрутизатор посилає тільки ту частину таблиці маршрутизації, яка описує стан його власних каналів. У таких алгоритмах в таблиці маршрутизації кожного маршрутизатора складається картина всієї мережі. Дистанційно-векторні алгоритми маршрутизації (також відомі як алгоритмами Беллмана-Форда) математично порівнюють маршрути, використовуючи який-небудь спосіб виміру відстані. Отримана характеристика називається вектором відстані. Такі протоколи теж вимагають від кожного маршрутизатора відправки всієї таблиці маршрутизації або її части, але тільки своїм сусідам. По суті, алгоритми маршрутизації за станом каналу розсилають невеликі оновлення решті маршрутизаторів, а дистанційно-векторні алгоритми відправляють більше інформації, але тільки сусіднім маршрутизаторам. При використанні дистанційно-векторних алгоритмів (distance vector algorithm) маршрутизатор має інформацію лише про своїх сусідів.

Оскільки алгоритми маршрутизації за станом каналу сходяться швидше, вірогідність утворення петель маршрутизації при їх використанні менша, ніж при використанні дистанційно-векторних протоколів. З іншого боку, алгоритми

маршрутизації за станом каналу вимагають більшої потужності процесора і більшу пам'ять. Тому алгоритми маршрутизації за станом каналу можуть виявитися дорожчими при реалізації і підтримці. Протоколи маршрутизації за станом каналу, зазвичай, більш масштабовані, ніж дистанційно-векторні протоколи.

6.2. Поняття метрики маршрутів

У таблицях маршрутизації міститься інформація, що використовується комутуючим програмним забезпеченням для вибору якнайкращого маршруту. Але як саме будуються ці таблиці? Яка природа інформації, що міститься в них? Як алгоритми маршрутизації визначають, що один маршрут вважається кращим за інші?

Для визначення оптимального маршруту алгоритми маршрутизації використовують безліч різних метрик. У складних алгоритмах маршрутизації вибір маршруту здійснюється за декількома метриками, що створюють складену (гібридну) метрику. Для визначення якнайкращого маршруту використовуються наступні метрики:

- довжина маршруту;
- надійність;
- затримка;
- смуга пропускання;
- навантаження;
- витрати на передачу.

Довжина маршруту є найбільш часто використовуваною метрикою маршрутизації. Деякі протоколи маршрутизації дозволяють мережному адміністратору довільним чином призначати кожному каналу значення, що відображає витрати на передачу. В цьому випадку довжина маршруту представляє собою суму витрат на всіх пройдених ділянках. Інші протоколи маршрутизації обчислюють кількість пройдених вузлів - метрику, яка визначає,

яка кількість переходів між мережними пристроями, такими як маршрутизатори, повинен пройти пакет на шляху від джерела до одержувача.

У контексті маршрутизації ***надійність*** алгоритму маршрутизації визначається надійністю каналу зв'язку (яка, зазвичай, визначається відношенням кількості переданих бітів до кількості помилок). У деяких каналах збої можуть відбуватися частіше, ніж в інших. Після збою одні канали відновлюються швидше і простіше, інші - повільніше. При призначенні рейтингів надійності можуть бути враховані будь-які фактори, що відносяться до цього. Такі рейтинги є числовими оцінками, які, зазвичай, призначаються лініям зв'язку мережними адміністраторами.

Затримка при маршрутизації є часом, потрібним для доставки пакету по мережі від джерела до одержувача. Величина затримки залежить від багатьох чинників, таких як смуга пропускання проміжних ліній зв'язку, довжина черги на порту кожного маршрутизатора, переповнення на проміжних лініях зв'язку, а також фізична відстань, яку необхідно пройти. Оскільки затримка є комбінацією декількох важливих параметрів, ця метрика набула широкого поширення.

Смуга пропускання характеризує пропускну спроможність каналу. За інших рівних умов 100-мегабітовий канал FastEthernet більш бажаніший, ніж виділена лінія із смугою пропускання 2048 Кбіт/с. Хоча смуга пропускання характеризує максимальну пропускну спроможність каналу, маршрути, що проходять по каналах з більшою смугою пропускання, не завжди виявляються кращими за маршрути, що проходять по більш повільних лініях. Наприклад, якщо швидкий канал завантажений більше, то для передачі по ньому пакету, одержувачу може знадобитися більше часу, ніж при використанні повільнішого, але менш завантаженого каналу.

Навантаження характеризує ступінь зайнятості мережного ресурсу, наприклад маршрутизатора. Використовуються різні способи визначення навантаження, зокрема за інтенсивністю, використанням процесора і за

кількістю оброблюваних в секунду пакетів. Проте, сам по собі моніторинг цих параметрів може поглинати значні ресурси.

Ще однією важливою метрикою є ***витрати на передачу даних***, особливо тому, що деякі компанії піклуються не стільки про продуктивність, скільки про експлуатаційні витрати. У багатьох випадках ці компанії вважають за краще передавати дані по своїх власних каналах, хоча в них затримка більше, а не по загальнодоступних каналах, оскільки використання останніх викликає додаткові витрати.

.3. Дистанційно-векторний протокол RIP

Протокол RIP (Routing Information Protocol) є внутрішнім протоколом маршрутизації (протокол внутрішнього шлюзу) дистанційно-векторного типу. Він представляє собою один з найбільш ранніх протоколів обміну маршрутною інформацією і, дотепер, надзвичайно поширений в обчислювальних мережах, зважаючи на простоту реалізації.

Для IP є дві версії протоколу RIP: перша і друга. Протокол RIP v1 не підтримує масок, тобто він поширює між маршрутизаторами тільки інформацію про номери мереж і відстані до них, а інформацію про маски цих мереж не поширює, вважаючи, що всі адреси належать до стандартних класів A, B або C. Протокол RIP v2 передає інформацію про маски мереж, тому він більшою мірою відповідає вимогам сьогодення.

В якості відстані до мережі стандарти протоколу RIP допускають різні види метрик: «хопи», метрики, що враховують пропускну спроможність, затримки і надійність мереж (тобто відповідні ознакам D, T і R в полі «Якість сервісу» IP-пакету), а також будь-які комбінації цих метрик. Метрика повинна володіти властивістю адитивності - метрика складеного шляху повинна бути рівна сумі метрик складових цього шляху. У більшості реалізацій RIP використовується проста метрика - кількість «хопів», тобто кількість проміжних маршрутизаторів, які потрібно подолати пакету до мережі призначення.

6.3.1. Формат пакету RIP v2

Загальний формат пакету протоколу RIP v2 наведено на рис. 6.2.

1 октет	1 октет	2 октети	2 октети	2 октети	4 октети	4 октети	4 октети	4 октети
Команда	Версія	Не використ.	AFI	Мітка маршруту	Адреса мережі	Маска під-мережі	Наступ-ний вузол	Метрика

Рисунок 6.2 - Загальний формат пакету RIP v2

- ***Команда.*** Показує, чи є пакет запитом або відповіддю. Запит вимагає, щоб маршрутизатор відправив маршрутну таблицю - всю або частково. Відповідь може бути регулярним оновленням маршрутної інформації або відповіддю на запит. У відповідях містяться записи маршрутної таблиці. Для передачі інформації з великих маршрутних таблиць використовується декілька RIP-пакетів.
- ***Версія.*** Версія протоколу RIP. У пакетах RIP v2 значення такого поля дорівнює 2.
- Не використовується. Це поле містить нульове значення.
- ***Ідентифікатор AFI.*** Ідентифікатор сімейства адреси (Address-Family Identifier). Ідентифікатор сімейства адреси (Address-Family Identifier) RIP призначений для передачі маршрутної інформації декількох різних протоколів. Кожен запис має ідентифікатор сімейства адреси, яка визначає тип адреси. AFI для IP дорівнює 2. Поле AFI для RIP v2 функціонує аналогічно полю AFI для RIP v1 RFC 1058, з єдиним виключенням: якщо AFI для першого запису повідомлення дорівнює 0xFFFF, то цей запис містить аутентифікаційну інформацію. В даний час єдиним типом аутентифікаційної інформації є пароль.
- ***Мітка маршруту.*** Призначена для розпізнавання внутрішніх маршрутів (що упізнаються RIP) і зовнішніх маршрутів (що упізнаються іншими протоколами). Сюди записуються коди автономних систем. Використовується

як мітка для зовнішніх маршрутів при роботі з протоколами зовнішньої маршрутизації

- ***IP-адреса.*** IP-адреса запису.
- ***Маска підмережі.*** Маска підмережі елементу. Якщо це поле дорівнює нулю, то для даного елементу маска підмережі не визначена.
- ***Наступний вузол.*** IP-адреса наступного вузла, куди прямують пакети.
- ***Метрика.*** Кількість вузлів (маршрутизаторів) між мережами до одержувача. Ця величина знаходиться між 1 і 15 для дійсних маршрутів і дорівнює 16 для недійсних.

У одному пакеті протоколу RIP допускається до 25 полів AFI, адрес і метрик. Таким чином, в одному пакеті RIP може бути перераховане до 25 одержувачів. Якщо AFI визначає аутентифікаційне повідомлення, то в маршрутній таблиці може бути визначено тільки 24 записи.

6.3.2. Алгоритм побудови таблиць маршрутизації

Розглянемо процес побудови таблиці маршрутизації за допомогою протоколу RIP.

Етап 1 - створення мінімальних таблиць.

У початковому стані в кожному маршрутизаторі програмним забезпеченням стека TCP/IP автоматично створюється мінімальна таблиця маршрутизації, в якій враховуються тільки безпосередньо приєднані до інтерфейсів маршрутизатора мережі.

Етап 2 - розсилка мінімальних таблиць сусідам.

Після ініціалізації кожного маршрутизатора він починає посилати своїм сусідам повідомлення протоколу RIP, в яких міститься його мінімальна таблиця. RIP-повідомлення передаються в пакетах протоколу UDP, через порт 520, і включають два параметри для кожної мережі: її IP-адресу і відстань до неї від маршрутизатора, що передає повідомлення.

Сусідами є ті маршрутизатори, яким даний маршрутизатор безпосередньо може передати IP-пакет по будь-якій своїй мережі, не користуючись послугами проміжних маршрутизаторів.

Етап 3 - отримання RIP-повідомлень від сусідів і обробка одержаної інформації.

Після отримання аналогічних повідомлень від сусідніх маршрутизаторів, маршрутизатор нарощує кожне одержане поле метрики на одиницю і запам'ятовує, через який порт і від якого маршрутизатора одержана нова інформація (адреса цього маршрутизатора буде адресою наступного маршрутизатора, якщо цей запис буде внесений в таблицю маршрутизації). Потім маршрутизатор починає порівнювати нову інформацію з тієї, яка зберігається в його таблиці маршрутизації.

Нові записи будуть додані в таблицю. Протокол RIP заміщає запис про яку-небудь мережу тільки в тому випадку, якщо нова інформація має кращу метрику (відстань в «хопах» менша), ніж та що є. В результаті, в таблиці маршрутизації про кожну мережу залишається тільки один запис; якщо ж є декілька рівнозначних відносно відстані шляхів до однієї і тієї ж мережі то. все одно в таблиці залишається один запис, який прийшов в маршрутизатор першим за часом. Для цього правила існує виключення - якщо гірша інформація про яку-небудь мережу прийшла від того ж маршрутизатора, на підставі повідомлення якого був створений даний запис, то гірша інформація заміщає кращу.

Аналогічні операції з новою інформацією виконують усі маршрутизатори мережі.

Етап 4 - розсилка нової таблиці сусідам.

Кожен маршрутизатор посилає нове RIP-повідомлення всім своїм сусідам. У цьому повідомленні він пердає дані про всі відомі йому мережі - як безпосередньо підключені, так і віддалені, про які маршрутизатор дізнався з RIP-повідомлень.

Етап 5 - отримання RIP-повідомлень від сусідів і обробка одержаної інформації.

Етап 5 повторює етап 3 - маршрутизатори приймають RIP-повідомлення, обробляють інформацію, що міститься в них, і на її підставі коректують свої таблиці маршрутизації.

Якщо маршрутизатори періодично повторюють етапи розсилки і обробки RIP-повідомлень, то за кінцевий проміжок часу в мережі встановиться коректний режим маршрутизації. Під коректним режимом маршрутизації, в даному випадку, розуміється такий стан таблиць маршрутизації, коли всі мережі будуть досяжні з будь-якої мережі за допомогою деякого оптимального маршруту. Пакети доходитимуть до адресатів і не зациклюватимуться в петлях.

Очевидно, якщо в мережі всі маршрутизатори, їх інтерфейси і канали зв'язку, що їх сполучають, постійно працездатні, то оголошення по протоколу RIP можна робити досить рідко, наприклад, один раз в день. Проте в мережах постійно відбуваються зміни - змінюється як працездатність маршрутизаторів і каналів, так і самі маршрутизатори і канали можуть додаватися в існуючу мережу або ж виводитися з її складу.

6.3.3. Адаптація RIP-маршрутизаторів до змін стану мережі

Для адаптації до змін в мережі протокол RIP використовує ряд механізмів.

До нових маршрутів RIP-маршрутизатори пристосовуються просто - вони передають нову інформацію в черговому повідомленні своїм сусідам і поступово ця інформація стає відома всім маршрутизаторам мережі. А ось до негативних змін, пов'язаних з втратою якого-небудь маршруту, RIP-маршрутизатори пристосовуються складніше. Це пов'язано з тим, що у форматі повідомлень протоколу RIP немає поля, яке б указувало на те, що шлях до даної мережі більше не існує.

Натомість, використовуються два механізми повідомлення про те, що деякий маршрут більш недійсний:

- закінчення часу життя маршруту;

- вказівка спеціальної відстані (нескінченності) до мережі, що стала недосяжною.

Для відпрацювання першого механізму, кожен запис таблиці маршрутизації, одержаний по протоколу RIP, має час життя (TTL). Під час надходження чергового RIP-повідомлення, яке підтверджує справедливість даного запису, таймер TTL встановлюється в початковий стан, а потім з нього кожну секунду віднімається одиниця. Якщо за час тайм-ауту не прийде нове маршрутне повідомлення про цей маршрут, то він позначається як недійсний.

Час тайм-ауту пов'язаний з періодом розсилки векторів по мережі. У RIP IP період розсилки обраний рівним 30 секундам (зазвичай період розсилки обирається рівним 30 секундам, з додаванням невеликої випадкової кількості часу всякий раз, коли таймер скидається; це робиться щоб уникнути перевантаження, яке може виникнути, якщо всі маршрутизатори одночасно спробують передати оновлену маршрутну інформацію своїм сусідам), а як тайм-аут обрано шестикратне значення періоду розсилки, тобто 180 секунд. Шестикратний запас часу потрібен для впевненості в тому, що мережа дійсно стала недоступна, а не просто відбулися втрати RIP-повідомлень (а це можливо, оскільки RIP використовує транспортний протокол UDP, який не забезпечує надійної доставки повідомлень). Таймер тайм-ауту скидається кожного разу, коли маршрут ініціалізується або коректується. Якщо з часу останньої корекції пройшло 3 хвилини або одержано повідомлення про те, що вектор відстані дорівнює 16, маршрут вважається закритим. Але запис про нього не видаляється, поки не закінчиться час "прибирання сміття" (2 хв.). При появі еквівалентного маршруту, перемикання на нього не відбувається. Таким чином блокується можливість коливань між двома або більше рівноцінними маршрутами.

Якщо який-небудь маршрутизатор відмовляє і перестає слати своїм сусідам повідомлення про мережі, які можна досягти через нього, то через 180 секунд всі записи, які породив цей маршрутизатор, стануть недійсними у його

найближчих сусідів. Після цього процес повториться вже для сусідів найближчих сусідів - вони викреслять подібні записи вже через 360 секунд, оскільки перші 180 секунд найближчі сусіди ще передавали повідомлення про ці записи.

Відомості про недосяжні мережі через маршрутизатор, який відмовив, розповсюджуються по мережі не дуже швидко, час розповсюдження кратний часу життя запису, а коефіцієнт кратності дорівнює кількості хопів між найдальшими маршрутизаторами мережі. У цьому полягає одна з причин вибору в якості періоду розсилки невеликої величини в 30 секунд.

Якщо відмовляє не маршрутизатор, а інтерфейс чи мережа, що зв'язують його з яким-небудь сусідом, то ситуація зводиться до тільки що описаної - знову починає працювати механізм тайм-ауту і маршрути, що стали недійсними, поступово будуть видалені з таблиць всіх маршрутизаторів мережі. Тайм-аут працює в тих випадках, коли маршрутизатор не може послати сусідам повідомлення про маршрут, що відмовив, оскільки або він сам непрацездатний, або непрацездатна лінія зв'язку, по якій можна було б передати повідомлення.

Коли ж повідомлення послати можна, RIP-маршрутизатори не використовують спеціальну ознаку в повідомленні, а вказують нескінченну відстань до мережі, причому в протоколі RIP вона прийнята рівною 16 хопам. Одержавши повідомлення, в якому деяка мережа супроводжується відстанню 16 (або 15, що приводить до того ж результату, оскільки маршрутизатор збільшує отримане значення на 1), маршрутизатор повинен перевірити, чи походить ця «погана» інформація про мережу від того ж маршрутизатора, повідомлення якого послужило свого часу підставою для запису про дану мережу в таблиці маршрутизації. Якщо це той самий маршрутизатор, то інформація вважається достовірною і маршрут позначається як недоступний.

Таке невелике значення «нескінченної» відстані спричинене тим, що в деяких випадках, відмови зв'язків в мережі викликають тривалі періоди некоректної роботи RIP-маршрутизаторів, що виражається в зацикленні пакетів

в петлях мережі. Чим менша відстань, що використовується в якості «нескінченної», тим такі періоди стають коротше.

Розглянемо випадок зациклення пакетів на прикладі мережі, зображеної на рис. 6.3.

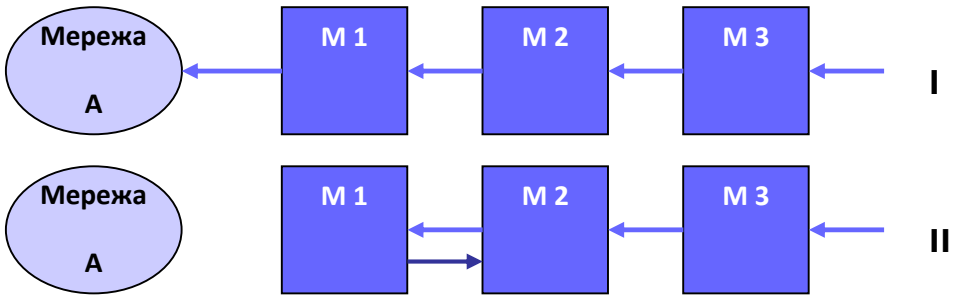


Рисунок 6.3 - Приклад некоректної роботи RIP-маршрутизаторів, що виражається в зацикленні пакетів.

Хай маршрутизатор Ml виявив, що його зв'язок з безпосередньо підключеною до нього мережею А втрачений (наприклад, внаслідок відмови інтерфейсу 1). Ml відзначив в своїй таблиці маршрутизації, що мережа А недоступна. У гіршому випадку він виявить це відразу ж після відправки чергових RIP-повідомлень, так що до початку нового циклу його оголошень, в якому він повинен повідомити сусідів, що відстань до мережі А стала рівною 16, залишається майже 30 секунд.

Кожен маршрутизатор працює на підставі свого внутрішнього таймера, не синхронізуючи роботу по розсилці оголошень з іншими маршрутизаторами. Тому, маршрутизатор М2 випередить маршрутизатор Ml і передасть йому своє повідомлення раніше, ніж Ml встигне передати новину про недосяжність мережі А. В цьому повідомленні будуть дані, породжені наступним записом в таблиці маршрутизації М2 (табл. 6.1).

Таблиця 6.1 - Таблиця маршрутизації маршрутизатора М2

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
A	M1	1	2

Цей запис був одержаний від маршрутизатора Ml і коректний до відмови інтерфейсу М1. Тепер він є застарілим, але маршрутизатор М2 про це ще не дізнався.

Таким чином, маршрутизатор Ml одержав нову інформацію про мережу А - ця мережа досяжна через маршрутизатор М2 з метрикою 2. Раніше Ml також одержував цю інформацію від М2. Але ігнорував її, оскільки його власна метрика для А була кращою. Тепер Ml повинен прийняти дані про мережу А, одержані від М2, і замінити запис в таблиці маршрутизації про недосяжність цієї мережі (табл. 6.2).

Таблиця 6.2 - Таблиця маршрутизації маршрутизатора Ml

Номер мережі	Адреса наступного маршрутизатора	Порт	Відстань
A	M2	2	3

В результаті в мережі утворилася маршрутна петля: пакети, що направляються вузлам мережі А, передаватимуться маршрутизатором М2 маршрутизатору Ml, а маршрутизатор Ml повертатиме їх маршрутизатору М2. IP-пакети будуть циркулювати по цій петлі до тих пір, поки не закінчиться час життя кожного пакету.

Маршрутна петля існуватиме в мережі достатньо довго. Розглянемо періоди часу, кратні часу життя записів в таблицях маршрутизаторів.

- Час 0-180 с. Після відмови інтерфейсу в маршрутизаторах Ml і М2 зберігатимуться некоректні записи, приведені вище. Маршрутизатор М2 як і раніше забезпечує маршрутизатор Ml своїм записом про мережу А з метрикою 2, оскільки її час життя не закінчився. Пакети зациклюються.

- Час 180-360 с. На початку цього періоду у маршрутизатора М2 закінчується час життя запису про мережу А з метрикою 2, оскільки маршрутизатор Ml в попередній період посилав йому повідомлення про мережу А з гіршою метрикою, ніж у М2, і вони не могли підтверджувати цей запис. Тепер маршрутизатор М2 приймає від маршрутизатора Ml запис про мережу А з метрикою 3 і трансформує її в запис з метрикою 4. Маршрутизатор Ml не одержує нових повідомлень від маршрутизатора М2 про мережу А з метрикою 2, тому час життя його запису починає зменшуватися. Пакети продовжують зациклюватися.
- Час 360-540 с. Тепер у маршрутизатора Ml закінчується час життя запису про мережу А з метрикою 3. Маршрутизатори Ml і М2 знову міняються ролями - М2 забезпечує Ml застарілою інформацією про шляхи до мережі А, вже з метрикою 4, яку Ml перетворить в метрику 5. Пакети продовжують зациклюватися.

Якби в протоколі RIP не була вибрана відстань 16 як недосяжна, то описаний процес тривав би до безкінечності (вірніше, поки не була б вичерпана розрядна сітка поля відстані і не було б зафіксовано переповнювання при черговому нарощуванні відстані).

В результаті, маршрутизатор М2 на черговому етапі описаного процесу одержує від маршрутизатора Ml метрику 15, яка після нарощування, перетворюючись на метрику 16, фіксує недосяжність мережі. Період нестабільної роботи мережі тривав 36 хвилин!

Обмеження в 15 хопів звужує область застосування протоколу RIP до мереж, в яких число проміжних маршрутизаторів не може бути більше 15. Для масштабніших мереж потрібно застосовувати інші протоколи маршрутизації, наприклад, OSPF, або розбивати мережу на автономні області.

Приведений приклад добре ілюструє головну причину нестабільної роботи маршрутизаторів, що працюють по протоколу RIP. Ця причина полягає в самому принципі роботи дистанційно-векторних протоколів - використанні інформації, одержаною з інших джерел. Дійсно, маршрутизатор М2 передав

маршрутизатору Ml інформацію про досяжність мережі А, за достовірність якої він сам не відповідає. Викоренити цю причину повністю не можна, адже сам спосіб побудови таблиць маршрутизації пов'язаний з передачею чужої інформації без вказівки джерела її походження.

Не слід думати, що при будь-яких відмовах інтерфейсів і маршрутизаторів в мережах виникають маршрутні петлі. Якби маршрутизатор Ml встиг передати повідомлення про недосяжність мережі А раніше помилкової інформації маршрутизатора М2, то маршрутна петля не утворилася б. Отже маршрутні петлі навіть без додаткових методів боротьби з ними, розглянутими в наступному розділі, виникають в середньому не більше ніж в половині потенційно можливих випадків.

6.3.4. Методи боротьби з помилковими маршрутами в протоколі RIP

Не дивлячись на те що протокол RIP не в змозі повністю виключити перехідні стани в мережі, коли деякі маршрутизатори користуються застарілою інформацією про вже неіснуючі маршрути, є декілька методів, які у багатьох випадках вирішують подібні проблеми.

Ситуація з петлею, що утворюється між сусідніми маршрутизаторами, описана вище, надійно вирішується за допомогою методу, що одержав назву ***розщеплювання горизонту*** (split horizon). Метод полягає в тому, що маршрутна інформація про деяку мережу, що зберігається в таблиці маршрутизації, ніколи не передається тому маршрутизатору, від якого вона одержана (це наступний маршрутизатор в даному маршруті). Якщо маршрутизатор М2, в розглянутому вище прикладі, підтримує техніку розщеплювання горизонту, то він не передасть маршрутизатору Ml застарілу інформацію про мережу А, оскільки одержав її саме від маршрутизатора Ml.

Практично всі сьогоднішні маршрутизатори, що працюють за протоколом RIP, використовують техніку розщеплювання горизонту.

Проте розщеплювання горизонту не допомагає в тих випадках, коли петлі утворюються не двома, а декількома маршрутизаторами.

Для запобігання зациклення пакетів по складених петлях при відмовах зв'язків застосовуються два інших прийоми, так звані ***тригерні оновлення*** (triggered updates) і ***заморожування змін*** (hold down).

Спосіб тригерних оновлень полягає в тому, що маршрутизатор, одержавши дані про зміну метрики до якої-небудь мережі, не чекає закінчення періоду передачі таблиці маршрутизації, а передає дані про маршрут, що змінився, негайно. Цей прийом може у багатьох випадках запобігти передачі застарілих відомостей про маршрут, що відмовив, але він перенавантажує мережу службовими повідомленнями, тому тригерні оголошення також робляться з деякою затримкою (1-5 секунд). Тому можлива ситуація, коли регулярне оновлення в якому-небудь маршрутизаторі трохи випередить за часом прихід тригерного оновлення від попереднього в ланцюгу маршрутизатора і даний маршрутизатор встигне передати по мережі застарілу інформацію про неіснуючий маршрут.

Другий прийом дозволяє виключити подібні ситуації. Він пов'язаний з введенням тайм-ауту на ухвалення нових даних про мережу, яка тільки що стала недоступною. Цей тайм-аут запобігає ухваленню застарілих відомостей про деякий маршрут від тих маршрутизаторів, які знаходяться на деякій відстані від зв'язку, що відмовив, і передають застарілі відомості про його працездатність. Передбачається, що протягом тайм-ауту «заморожування змін» ці маршрутизатори викреслять даний маршрут зі своїх таблиць, оскільки не одержать про нього нових записів і не поширюватимуть застарілі відомості по мережі.

Протокол стану каналів OSPF

Протокол маршрутизації OSPF (Open Shortest Path First) відноситься до протоколів внутрішньої маршрутизації і представляє собою протокол стану каналів, що використовує алгоритм SPF пошуку найкоротшого шляху в графі.

На ***першому етапі*** побудови таблиці маршрутизації, кожен маршрутизатор будує граф зв'язків мережі. Для цього маршрутизатори обмінюються зі своїми сусідами інформацією про граф мережі, за допомогою повідомлень «router links advertisement» - оголошення про зв'язки маршрутизатора. При передачі топологічна інформація не модифікується. В результаті всі маршрутизатори мережі мають в своєму розпорядженні однакові відомості про граф мережі, які зберігаються в топологічній базі даних.

Другий етап - знаходження оптимальних маршрутів за допомогою одержаного графа. Кожен маршрутизатор вважає себе центром мережі і шукає оптимальний маршрут до кожної відомої йому мережі. У кожному знайденому таким чином маршруті запам'ятовується тільки один крок - до наступного маршрутизатора. Цей крок і заноситься в таблицю маршрутизації. У протоколі OSPF на другому етапі використовується ітеративний алгоритм Дійкстри. Якщо декілька маршрутів мають однакову метрику до мережі призначення, то в таблиці маршрутизації запам'ятовуються перші кроки всіх цих маршрутів.

Слідкування за змінами стану мережі і корегування в таблицях маршрутизації проводиться за допомогою повідомлень ***HELLO***. Корегування таблиць проводиться тільки, якщо стан зв'язку змінився. При цьому проводиться розсилка найближчим сусідам нового оголошення тільки щодо даного зв'язку. Одержавши таке повідомлення, маршрутизатор перебудовує граф мережі, наново шукає оптимальні маршрути і корегує свою таблицю маршрутизації. Маршрутизатор ретранслює оголошення кожному зі своїх найближчих сусідів (крім того, від якого він одержав це оголошення).

6.4.1. Ієрархічна маршрутизація (розбиття на області)

Для спрощення обчислення маршрутів і зменшення розміру бази даних стану зв'язків OSPF-система може бути розбита на окремі незалежні області (areas), що об'єднуються за допомогою магістралі (backbone).

Маршрути всередині кожної області обчислюються як в окремій системі: база даних стану зв'язків містить записи тільки про зв'язки маршрутизаторів усередині області, дія протоколу затоплення не розповсюджується за межі області.

Деякі маршрутизатори підключені до магістралі і одній або декільком периферійним областям. Такі маршрутизатори називаються обласними прикордонними маршрутизаторами (area border router, ABR). Кожна область повинна мати як мінімум один ABR.

Обласні прикордонні маршрутизатори підтримують окремі бази даних стану зв'язків для всіх областей.

6.4.2. Побудова маршрутів

Метрика маршруту

Метрика визначає оцінку якості зв'язку в даній мережі: чим менша метрика, тим краща якість з'єднання. Метрика маршруту дорівнює сумі метрик всіх зв'язків, що входять в маршрут.

Протокол OSPF дозволяє визначити для будь-якої мережі різні значення метрик в залежності від типу сервісу, відповідно до значення поля ToS її заголовка. Для кожного типу сервісу обчислюватиметься свій маршрут.

Метрика мережі, що оцінює пропускну спроможність, визначається як кількість секунд, яка потрібна для передачі 100 Мбіт через фізичне середовище даної мережі.

Порядок розрахунку метрик, що оцінюють надійність, затримку і вартість, не визначений.

База даних стану зв'язків (ВДСЗ)

Для роботи алгоритму SPF на кожному маршрутизаторі будується база даних стану зв'язків, що представляє собою повний опис графа OSPF-системи. При цьому вершинами графа є маршрутизатори, а ребрами - зв'язки, що їх сполучають. Бази даних на всіх маршрутизаторах однакові. База даних стану зв'язків представляє собою таблицю, де для кожної пари суміжних вершин графа вказано ребро, що їх сполучає, і метрика цього ребра.

За роботу баз даних відповідають наступні протоколи: протокол Hello, протокол обміну, протокол затоплення (flooding).

Побудова бази даних стану зв'язків

Протокол Hello

Після ініціалізації модуля OSPF через всі інтерфейси, включені в OSPF-систему, починають розсилатися Hello-повідомлення. Завдання Hello-протоколу - виявлення сусідів і встановлення з ними відносин суміжності.

Сусідами називаються OSPF-маршрутизатори, що підключені до однієї мережі (до однієї лінії зв'язку) і обмінюються Hello-повідомленнями.

Суміжними називаються сусідні OSPF-маршрутизатори, які ухвалили рішення обмінюватися один з одним інформацією, необхідною для синхронізації бази даних стану зв'язків і побудови маршрутів. Не всі сусіди стають суміжними.

Hello-пакети продовжують періодично розсилатися і після того, як сусіди були виявлені. Таким чином маршрутизатор контролює стан своїх зв'язків з сусідами і може своєчасно виявити зміну цього стану (наприклад, обрив зв'язку або відключення одного з сусідів). Обрив зв'язку може бути також виявлений і за допомогою протоколу канального рівня, який просигналізує про недоступність каналу.

У мережах з можливістю широкомовної розсилки (broadcast networks) Hello-пакети розсилаються по мультикастинговій адресі 224.0.0.5 ("Всім OSPF-маршрутизаторам"). У інших мережах всі можливі адреси сусідів повинні бути введені адміністратором.

Протокол обміну

Для кожної пари суміжних маршрутизаторів необхідно виконати синхронізацію їх баз даних. Синхронізація баз даних відбувається за допомогою протоколу обміну (Exchange protocol).

Спочатку маршрутизатори обмінюються тільки описами своїх баз даних (Database Description), що містять ідентифікатори записів і номери їх версій. Це дозволяє уникнути пересилки всього вмісту бази даних, якщо потрібно синхронізувати тільки декілька записів.

Під час цього обміну кожен маршрутизатор формує список записів, вміст яких він повинен запитати (тобто ці записи в його базі даних застаріли або відсутні), і відповідно відправляє пакети запитів про стан зв'язків (Link State Request). У відповідь він одержує вміст останніх версій потрібних йому записів в пакетах типу "Оновлення стану зв'язків" (Link State Update).

Після синхронізації баз даних проводиться побудова маршрутів.

Протокол затоплення (flooding)

Кожен маршрутизатор відповідає за ті і лише ті записи в базі даних стану зв'язків, які описують зв'язки, що відходять від даного маршрутизатора. Це означає, що при утворенні нового зв'язку, зміні в стані зв'язку або її зникненні (обриві), маршрутизатор, відповідальний за цей зв'язок, повинен відповідно змінити свою копію бази даних і негайно сповістити решту всіх маршрутизаторів OSPF-системи про зміни, що відбулися, щоб вони також внесли виправлення в свої копії бази даних.

Підпротокол OSPF, що виконує це завдання, називається протоколом затоплення (Flooding protocol). При роботі цього протоколу пересилаються повідомлення типу "Оновлення стану зв'язків" (Link State Update), отримання яких підтверджується повідомленнями типу "Link State Acknowledgment".

Кожен запис про стан зв'язків має свій номер (номер версії), який також зберігається в базі даних. Кожна нова версія запису має більший номер. При розсилці повідомлень про оновлення запису в базі даних номер запису також включається в повідомлення для запобігання випадків потрапляння в базу даних застарілих версій.

Маршрутизатор, відповідальний за запис про зв'язок, що змінився, розсилає повідомлення "Оновлення стану зв'язку" по всіх інтерфейсах. Проте, нові версії стану одного і того ж зв'язку повинні з'являтися не частіше, ніж обумовлено певною константою.

Далі на всіх маршрутизаторах OSPF-системи діє наступний алгоритм.

1. Одержати повідомлення. Знайти відповідний запис в базі даних.

2. Якщо запис не знайдений, додати його в базу даних, передати повідомлення по всіх інтерфейсах.

3. Якщо номер запису в базі даних менше номера повідомлення, що прийшло, замінити запис в базі даних, передати повідомлення по всіх інтерфейсах.

4. Якщо номер запису в базі даних більше номера повідомлення, що прийшло, і цей запис не був нещодавно розісланий, розіслати вміст запису з бази даних через той інтерфейс, звідки прийшло повідомлення. Поняття "нещодавно" визначається значенням константи.

5. У разі рівних номерів повідомлення ігнорувати.

Протокол OSPF встановлює також таку характеристику запису в базі даних, як вік. Вік дорівнює нулю при створенні запису. При затопленні OSPF-системи повідомленнями з даним записом кожен маршрутизатор, який ретранслює повідомлення, збільшує вік запису на певну величину. Окрім цього, вік збільшується на одиницю кожну секунду. Через різницю в часі пересилки, різницю в кількості проміжних маршрутизаторів і з інших причин вік одного і того ж запису в базах даних на різних маршрутизаторах може дещо розрізнятися. Це нормальне явище.

При досягненні віком максимального значення (60 хвилин), відповідний запис розцінюється маршрутизатором як прострочений і непридатний для обчислення маршрутів. Такий запис повинен бути видалений з бази даних.

Оскільки бази даних на всіх маршрутизаторах системи повинні бути ідентичні, прострочений запис повинен бути видалений з усіх копій бази даних та на всіх маршрутизаторах. Це робиться з використанням протоколу

затоплення: маршрутизатор затоплює систему повідомленням з простроченим записом. Відповідно, в описаний вище алгоритм обробки повідомлення вносяться доповнення, пов'язані з отриманням простроченого повідомлення і видаленням відповідного запису з бази даних.

Щоб записи в базі даних не застарівали, маршрутизатори, відповідальні за них, повинні через кожні 30 хвилин затоплювати систему повідомленнями про оновлення записів, навіть якщо стан зв'язків не змінився. Вміст записів в цих повідомленнях незмінний, але номер версії більше, а вік дорівнює нулю.

Для забезпечення надійності передачі даних реалізовано механізм підтвердження прийому повідомлень, також для всіх повідомлень обчислюється контрольна сума.

Підтримка множинних маршрутів

Якщо між двома вузлами мережі існує кілька маршрутів з однаковими або близькими за значенням метриками, протокол OSPF дозволяє направити частини трафіку по цих маршрутах у пропорції, що відповідає значенням метрик. Наприклад, якщо існує два альтернативних маршрути з метриками 1 й 2, то дві третини трафіку буде спрямовано по першому з них, а третина, що залишилася, – по другому.

Позитивний ефект такого механізму:

- зменшення середньої затримки проходження дейтаграм між відправником й одержувачем;
- зменшення коливань значення середньої затримки;
- можливість переходу трафіку на альтернативну лінію.

Зовнішні маршрути

Для досягнення мереж, що не входять в OSPF-систему (в автономну систему), використовуються прикордонні маршрутизатори автономної системи (autonomous system border router, ASBR), які мають зв'язки, що виходять за межі системи.

ASBR вносять у базу даних стану зв'язків дані про мережі за межами системи, що досяжні через той або інший ASBR. Такі мережі, а також маршрути, що ведуть до них, називаються зовнішніми (external).

У найпростішому випадку, якщо в системі є тільки один ASBR, він повідомляє через себе маршрут за замовчуванням (default route) і всі дейтаграми, адресовані в мережі, що не входять у базу даних системи, відправляються через цей маршрутизатор.

Якщо в системі є кілька ASBR, то, можливо, внутрішнім маршрутизаторам системи доведеться вибирати, через який саме граничний маршрутизатор потрібно відправляти дейтаграми в ту або іншу зовнішню мережу. Це робиться на основі спеціальних записів, внесених ASBR у базу даних системи. Ці записи містять адресу й маску зовнішньої мережі й метрику відстані до неї, яка може бути, а може й не бути порівняною з метриками, що використовуються в OSPF-системі. Якщо можливо, адреси декількох зовнішніх мереж агрегуються в загальну адресу з коротшою маскою.

ASBR може одержувати інформацію про зовнішні маршрути від протоколів зовнішньої маршрутизації. Всі або деякі зовнішні маршрути можуть бути сконфігуровані адміністратором (у тому числі єдиний маршрут за замовчуванням).

6.4.3. Алгоритм SPF

Алгоритм SPF був запропонований Е.В. Дійкстрой (E.W.Dijkstra). Алгоритм SPF, ґрунтуючись на базі даних стану зв'язків, обчислює найкоротші шляхи між заданою вершиною S графа і рештою всіх вершин. Результатом роботи алгоритму є таблиця, де для кожної вершини V графа вказаний список ребер, що сполучають задану вершину S з вершиною V найкоротшим шляхом (рис. 6.4).

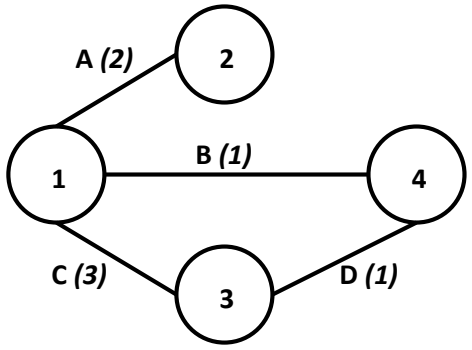
Задамося:

S - задана вершина (джерело шляхів);

E - множина оброблених вершин, тобто вершин, найкоротший шлях до яких вже знайдено;

R - множина вершин графа, що залишилася (тобто множина вершин графа за виключенням множини E);

O - впорядкований список шляхів.



Від→до	Мережа	Метрика
①→②	A	2
①→③	C	3
①→④	B	1
②→①	A	2
③→①	C	3
③→④	D	1
④→①	B	1
④→③	D	1

Рисунок 6.4 - OSPF-система і її база даних стану зв'язків

Принцип роботи алгоритму.

1. Ініціалізувати *E={S}*, *R={всі вершини графа, окрім S}*. Помістити в O всі односегментні (завдовжки в одне ребро) маршрути, що починаються з S, відсортувавши їх у порядку зростання метрик.

2. Якщо O порожній або перший маршрут в O має нескінченну метрику, то відзначити всі вершини в R як недосяжні і закінчити роботу алгоритму.

3. Перший маршрут в множині O оптимальний - P. Видалити P з O. Нехай V - останній вузол в P. Якщо V належить E, перейти до п.2; інакше P є найкоротшим з S в V (записуватимемо як V:P); перенести V з R в E.

4. Побудувати набір нових маршрутів, що підлягають розгляду, шляхом додавання до маршруту P всіх односегментних відрізків, що починаються з V. Метрика кожного нового маршруту дорівнює сумі метрики P і метрики відповідного односегментного відрізка, що починається з V. Додати нові маршрути у впорядкований список O, помістивши їх на місця відповідно до значень метрик. Перейти до п.2.

Всі обчислення проводяться локально по відомій базі даних, а тому швидше в порівнянні з дистанційно-векторними протоколами. При цьому, результати отримуються на основі повної, а не часткової інформації про граф мережі.

6.4.4. Формат пакета

Всі пакети протоколу OSPF починаються з 24-байтового заголовка, як показано на рис. 6.5.

Перше поле в заголовку OSPF – це **номер версії OSPF** (version number). Номер версії позначає конкретну використовувану реалізацію OSPF.

За номером версії йде **поле типу** (type). Існує 5 типів пакетів OSPF.

Hello. Відправляється через регулярні інтервали часу для встановлення й підтримки сусідських взаємовідносин.

Field length,
In bytes

1	1	2	4	4	2	2	8	Variable
Version number	Type	Packet length	Router ID	Area ID	Checksum	Authentication type	Autentication	Data

Рисунок 6.5 - Формат пакета протоколу OSPF

Database Description. Опис бази даних. Описує вміст бази даних. Обмін цими пакетами відбувається при ініціалізації суміжності.

Link-State Request. Запит про стан каналу. Запитує частини топологічної бази даних сусіда. Обмін цими пакетами відбувається після того, як який-

небудь маршрутизатор виявляє (шляхом перевірки пакетів опису бази даних), що частина його топологічної бази даних застаріла.

Link-State Update. Корегування стану каналу. Відповідає на пакети запиту про стан каналу. Ці пакети також використовуються для регулярної розсилки LSA. В один пакет може бути включено кілька LSA.

Link-State Acknowledgement (LSA). Підтвердження стану каналу. Підтверджує пакети корегування стану каналу. Пакети корегування стану каналу повинні бути чітко підтверджені, що є гарантією надійності процесу лавинної пересилки пакетів корегування стану каналу через яку-небудь область.

Кожне LSA в пакеті корегування стану каналу містить тип поля. Існують 6 типів LSA.

Тип 1. **Router Links Advertisement** - маршрутизатор повідомляє про свої зв'язки із сусідніми маршрутизаторами, транзитними й тупиковими мережами; поширюється кожним маршрутизатором всередині області, до якої належать ці зв'язки.

Тип 2. **Network Links Advertisement** - містить список маршрутизаторів, підключених до мережі множинного доступу; поширюється виділеним маршрутизатором усередині області, до якої належить дана мережа. Фактично описує зв'язки, спрямовані в графі системи від вершини типу "транзитна мережа" до маршрутизаторів цієї мережі.

Тип 3. **Summary Link Advertisement** - описує відстань від даного обласного граничного маршрутизатора (ABR) до IP-мережі, що перебуває за межами даної області, але належить даній OSPF-системі; поширюється цим ABR усередині області.

Тип 4. **AS Boundary Router Summary Link Advertisement** - описує відстань від даного ABR до граничного маршрутизатора системи (ASBR); поширюється цим ABR усередині області.

Тип 5. **AS External Link Advertisement** - описує відстань до мережі, що перебуває за межами OSPF-системи; поширюється ASBR і ретранслюється в усі області, крім тупикових, їхніми граничними маршрутизаторами.

Тип 6. **AS External Link Advertisement (NSSA)** - те ж, що тип 5, але поширюється всередині не зовсім тупикових областей (у них поширення LSA типу 5 заборонене); на границі NSSA і магістралі перетворюється в LSA типу 5 для подальшого поширення в системі. Формат ідентичний формату LSA типу 5 за винятком номера типу.

За полем типу заголовка пакета OSPF іде **поле довжини пакета** (packet length). Це поле вказує на довжину пакета разом із заголовком OSPF у байтах.

Поле ідентифікатора маршрутизатора (router ID) ідентифікує джерело пакета.

Поле ідентифікатора області (area ID) ідентифікує область, до якої належить даний пакет. Всі пакети OSPF пов'язані з однією конкретною областю.

Стандартне **поле контрольної суми** (checksum) перевіряє вміст усього пакета для виявлення потенційних пошкоджень, що мали місце при транзиті.

За полем контрольної суми йде **поле типу посвідчення** (authentication type). Прикладом типу посвідчення є "простий пароль". Всі обміни протоколу OSPF проводяться із встановленням правомірності. Тип посвідчення встановлюється за принципом "окремий для кожної області".

За полем типу посвідчення йде **поле посвідчення** (authentication). Це поле має довжину 64 біта і містить інформацію посвідчення.

6.5. Протоколи IGRP і EIGRP

6.5.1. Особливості протоколу IGRP

Протокол маршрутизації внутрішнього шлюзу (Interior Gateway Routing Protocol - IGRP) являє собою протокол маршрутизації, розроблений у середині 1980-х рр. корпорацією Cisco Systems.

Характеристики протоколу IGRP

IGRP є дистанційно-векторним протоколом маршрутизації внутрішнього шлюзу (Interior Gateway Protocol - IGP).

У протоколі IGRP використовується складена метрика, що обчислюється на підставі взятих з певною вагою математичних значень затримки в об'єднаній мережі, смуги пропускання, надійності й навантаження. У кожної з таких величин є свій коефіцієнт (вага), який адміністратор мережі може змінити, хоча робити це потрібно дуже обережно. В протоколі IGRP передбачений широкий діапазон значень метрик. Наприклад, надійність і навантаження можуть змінюватися від 1 до 255, смуга пропускання може приймати значення, що відповідають швидкостям передачі від 1200 біт/с до 10 Гбіт/с, а затримка може змінюватися в межах від 1 до 224. Ці широкі діапазони значень метрик доповнюються рядом констант, які визначаються користувачем, що дозволяє адміністратору мережі впливати на вибір маршруту. Ці константи порівнюються з метриками і одна з одною у відповідності до алгоритму, який і визначає єдину, складену метрику. Така гнучкість дозволяє адміністраторам мережі виконувати тонку настройку автоматичного вибору маршруту по протоколу IGRP.

Для забезпечення додаткової гнучкості IGRP допускає маршрутизацію по декількох маршрутах. Канали з однаковою смугою пропускання можуть циклічно пропускати один потік даних, з автоматичним перемиканням на інший канал, якщо перший вийде з ладу. Маршрути можуть мати різні метрики і, разом з тим, залишаються дійсними множинними маршрутами. Наприклад, якщо один маршрут у три рази кращий за інший (його метрика в три рази менше), то кращий маршрут буде застосовуватися втричі частіше. Для такої маршрутизації можуть використовуватися тільки маршрути з метриками, відхилення яких від метрики найкращого маршруту перебувають у межах певного діапазону або дисперсії. Дисперсія є ще однією характеристикою, яка може бути встановлена адміністратором мережі.

Функції підвищення стабільності

Протокол IGRP має ряд функцій, призначених для підвищення стабільності: утримання, розщеплення горизонтів і зворотні оновлення.

Утримання (holddown) застосовуються щоб уникнути оновлення в таблиці маршруту, на якому, можливо, відбувся збій. Якщо маршрутизатор виходить із ладу, то сусідні маршрутизатори виявляють це по відсутності регулярних повідомлень про оновлення маршрутів. У цьому випадку маршрутизатори визначають нові маршрути і відправляють повідомлення про зміну маршрутизації сусіднім маршрутизаторам. Результатом цього є хвиля корегувань, які передаються через мережу. Такі оновлення надходять на пристрої мережі не одночасно. Пристрій, який ще не одержав повідомлення про збій у мережі, може відправити регулярне оновлення (відповідно до якого маршрут, де щойно відбувся збій, є дійсним) іншому пристрою, який вже одержав повідомлення про збій. У цьому випадку, на вищезгаданому пристрої виявиться (і, можливо, поширіться далі) невірна маршрутна інформація.

Інтервали затримки змін пропонують маршрутизаторам протягом деякого періоду часу не передавати далі будь-які повідомлення про зміни, які можуть вплинути на маршрути. Інтервал затримки змін зазвичай обирається таким чином, щоб він трохи перевищував час проходження оновлення маршрутизації у всій мережі.

Метод розщеплення горизонту (split horizon) опирається на припущення, що недоцільно посилати інформацію про маршрут у тому напрямку, звідки вона надійшла.

Розщеплення горизонту запобігає утворенню маршрутних петель між суміжними маршрутизаторами. Для ліквідації більш великих маршрутних петель застосовуються зворотні оновлення (poison-reverse updates). Збільшення значень маршрутних метрик зазвичай вказує на появу маршрутних петель. У цьому випадку посилають зворотні оновлення , щоб видалити цей маршрут і перевести його в режим утримання. В реалізації IGRP Cisco зворотні оновлення

відправляються в тому випадку, якщо маршрутна метрика збільшується в 1,1 і більше разів.

Таймери

Протокол IGRP передбачає використання ряду таймерів і змінних, які містять тимчасові інтервали: таймер оновлень, таймер недійсних маршрутів, період утримання й таймер виключення. Таймер оновлень (update timer) визначає, з якою частотою повинні відправлятися повідомлення про оновлення маршрутів. Для протоколу IGRP стандартне значення цієї змінної дорівнює 90 сек. Таймер недійсних маршрутів (invalid timer) визначає, протягом якого часу при відсутності повідомлень про оновлення маршрутизатор повинен очікувати, перш ніж оголосити цей маршрут недійсним. Стандартне значення IGRP для такої змінної становить три періоди оновлення . Період утримання (hold-time period) визначає проміжок затримки внесення змін у таблицю маршрутизації. Його стандартне значення в IGRP на 10 секунд більше потрійного періоду таймера оновлення. Нарешті, таймер виключення (flush timer) визначає, скільки часу має пройти до виключення маршрутизатора з таблиці маршрутизації. За замовчуванням для протоколу IGRP цей час у сім разів перевищує період розсилання оновлення маршрутів.

6.5.2. Особливості протоколу EIGRP

Удосконалений протокол маршрутизації внутрішнього шлюзу (Enhanced Internal Gateway Routing Protocol – EIGRP) , являє собою результат еволюції його попередника, протоколу IGRP.

Можливості й атрибути протоколу Enhanced IGRP

Основними властивостями, що відрізняють Enhanced IGRP від інших протоколів маршрутизації, є швидка збіжність, підтримка маски підмережі змінної довжини, часткових оновлень і декількох протоколів мережевого рівня (AppleTalk, IP й Novell NetWare).

Маршрутизатор, на якому виконується протокол Enhanced IGRP, зберігає всі маршрутні таблиці сусідніх маршрутизаторів, що дозволяє йому швидко

адаптуватися до альтернативних маршрутів. Якщо підходящого маршруту немає, то маршрутизатор Enhanced IGRP запитує альтернативний маршрут у сусідніх маршрутизаторів. Ці запити передаються доти, поки альтернативний маршрут не буде знайдено.

Протокол EIGRP підтримує маски підмереж змінної довжини, що дозволяє автоматично узагальнювати маршрути в межах мережі з певним номером. Крім того, EIGRP можна настроїти на узагальнення маршрутів у будь-яких бітових межах на будь-якому інтерфейсі.

Enhanced IGRP не виконує періодичних оновлень. Замість цього він посилає оновлену інформацію частинами й тільки у випадку зміни метрики маршруту. Поширення частково оновленої інформації автоматично обмежується таким чином, що її одержують тільки ті маршрутизатори, яким це необхідно. Завдяки цим двом властивостям протоколу Enhanced IGRP потрібна значно менша смуга пропускання, ніж протоколу IGRP.

Основні процеси і технології

Для підвищення ефективності в протоколі Enhanced IGRP використовуються чотири основні технології, що відрізняють його від інших технологій маршрутизації: виявлення/відновлення сусідніх маршрутизаторів, транспортний протокол з достовірною передачею (reliable transport protocol, RTP), машина з кінцевим числом станів алгоритму DUAL і модулі, залежні від протоколу.

Механізм виявлення і відновлення сусідніх вузлів дозволяє маршрутизаторам динамічно виявляти інші маршрутизатори у своїй мережі. Крім того, маршрутизатори повинні визначати стан сусідніх маршрутизаторів у випадках, коли ті стають недоступними або непрацездатними. Цей процес реалізується з невеликими витратами ресурсів за допомогою періодичної посилки невеликих пакетів вітання (hello packets). Поки маршрутизатор одержує пакети вітання від сусіднього маршрутизатора, він вважає, що сусідній маршрутизатор працездатний і що вони можуть обмінюватися між собою маршрутною інформацією.

Транспортний протокол з достовірною передачею (Reliable Transport Protocol - RTP) забезпечує гарантовану, упорядковану доставку пакетів протоколу EIGRP усім сусіднім маршрутизаторам. Він підтримує змішану передачу багато- і одноадресатних пакетів. Для більшої ефективності EIGRP, з гарантією доставки передаються тільки деякі пакети. У мережах із множинним доступом і можливостями групової передачі, таких як Ethernet, немає необхідності посилати пакети вітання кожному сусідньому маршрутизатору окремо. Протокол EIGRP відправляє декільком абонентам один пакет вітання, що містить вказівник, що інформує одержувачів про те, що пакету не потрібне підтвердження. У пакетах інших типів, таких як пакети оновлення , вказується, що підтвердження необхідне. В протоколі RTP є засоби більш швидкого пересилання багатоадресатних пакетів, у той час як відправка пакетів, не потребуючих підтвердження, затримується. Це дозволяє гарантувати швидку збіжність для швидкісних з'єднань.

Дифузійний алгоритм оновлення (Diffusing Update Algorithm - DUAL) розроблено дозволяє маршрутизаторам EIGRP визначати, чи є маршрут, повідомлений сусіднім вузлом, петлею, і дає можливість маршрутизатору, на якому функціонує протокол EIGRP, знаходити альтернативні маршрути, не чекаючи оновленої інформації від інших маршрутизаторів.

Для вибору ефективних маршрутів без петель DUAL використовує інформацію про відстань і відбирає маршрути для занесення в маршрутні таблиці, ґрунтуючись на допустимих маршрутизаторах. Допустимим маршрутизатором вважається сусідній маршрутизатор, який використовується для пересилання пакетів до одержувача з найменшими витратами і гарантує відсутність маршрутних петель. Якщо в сусіднього маршрутизатора змінюється метрика або топологія мережі, то DUAL шукає в мережі допустимі маршрутизатори. Якщо буде знайдений хоча б один, то DUAL використовує його, щоб уникнути повторного обчислення маршруту. При відсутності допустимих маршрутизаторів і повторних повідомлень про одержувача від сусідніх маршрутизаторів повторне обчислення маршруту (яке називають

дифузійним обчисленням) все-таки виконується, тому що необхідно визначити новий допустимий маршрутизатор. Хоча повторні обчислення не викликають підвищеного навантаження на процесор, вони впливають на швидкість збіжності, тому краще їх уникати.

Концепції маршрутизації

Протокол EIGRP опирається на чотири основні концепції: таблиці сусідніх маршрутизаторів, топологічні таблиці, стани маршрутів і маркування маршрутів.

Коли маршрутизатор виявляє новий сусідній маршрутизатор, він створює запис у **таблиці сусідніх маршрутизаторів** і записує в неї його адресу й інтерфейс. Сусідній маршрутизатор посилає пакет вітання, що сповіщає про час, протягом якого він вважається доступним і працездатним. Якщо пакет вітання не отриманий протягом часу зайнятості, то DUAL сповіщається про зміну топології.

Крім того, у таблиці сусідніх маршрутизаторів міститься інформація для протоколу RTP. Для узгодження пакетів даних і підтвердження їхнього одержання використовуються номери послідовностей. Останній порядковий номер, отриманий від сусіднього маршрутизатора, фіксується, що дозволяє виявляти пакети, що випали з послідовності. Для пересилання на сусідній маршрутизатор використовується черга на основі списку переданих пакетів. Для оцінки оптимального інтервалу повторної передачі використовуються записи в таблицях сусідніх маршрутизаторів, де зберігаються значення таймерів передачі пакетів у прямому й зворотному напрямку.

У **топологічних таблицях** містяться всі адреси одержувачів, про які сповіщають сусідні маршрутизатори. Кожен запис топологічної таблиці містить адресу одержувача й список сусідніх маршрутизаторів, які повинні сповіщати про ці адреси. Для кожного сусіднього маршрутизатора існують записи певної метрики, які зберігаються сусідніми маршрутизаторами в їхніх маршрутних таблицях. Протоколам маршрутизації по вектору відстані необхідно дотримуватися наступного правила: якщо сусідній маршрутизатор повідомляє

про те, що одержувач досяжний, то вони повинні використовувати цей маршрут для передачі пакетів.

Метрика, яка використовується маршрутизатором для звертання до одержувача, асоціюється з одержувачем. Метрика, що використовує маршрутизатор у маршрутних таблицях і про яку він сповіщає інші маршрутизатори, є сумою найкращих метрик і канальних витрат найкращого із сусідніх маршрутизаторів.

Записи топологічних таблиць, що стосуються одержувачів, існують у двох **станах:** активному й пасивному. Одержувач перебуває в пасивному стані, коли маршрутизатор не виконує обчислення маршруту, і в активному, якщо такі обчислення виконуються. Якщо допустимі маршрутизатори завжди доступні, то одержувач ніколи не перейде в активний стан, у такий спосіб уникаючи повторних обчислень.

Повторні обчислення виконуються в тому випадку, коли одержувач не має допустимих маршрутизаторів. Маршрутизатор ініціює повторні обчислення, посилаючи інформаційний пакет із запитом до кожного сусіднього маршрутизатора. У свою чергу, сусідній маршрутизатор може відправити відповідний пакет, що показує, що для одержувача є допустимий маршрутизатор, або підтвердити, що він бере участь у процесі повторних обчислень. Поки одержувач перебуває в активному стані, маршрутизатор не може змінити інформацію в маршрутній таблиці. Після того як маршрутизатор одержить відповідь від всіх сусідніх маршрутизаторів, записи в топологічній таблиці для одержувачів повернуться в пасивний стан і маршрутизатор зможе вибирати допустимий маршрутизатор для одержувача.

Протокол EIGRP підтримує внутрішні й зовнішні маршрути. Внутрішні маршрути породжуються автономною системою з Enhanced IGRP. Таким чином, безпосередньо підключена мережа, що настроєна на використання EIGRP, розрахована на внутрішню маршрутизацію й поширює цю інформацію з автономних систем через протокол EIGRP. Інформація про зовнішні маршрути поширюється іншим протоколом маршрутизації або зберігається в

маршрутній таблиці як статичні маршрути. Ці маршрути **маркуються** індивідуально відповідно до джерела. Зовнішні маршрути маркуються наступною інформацією:

- ідентифікатор (ID) маршрутизатора із протоколом Enhanced IGRP, що поширює маршрут;
- номер AS-одержувача;
- маркер адміністратора;
- ID зовнішнього протоколу;
- метрика зовнішнього протоколу;
- бітові прапори стандартної маршрутизації.

Маркування маршруту надає можливість адміністраторові мережі налаштовувати процес маршрутизації і забезпечує гнучку стратегію керування. Маркування маршрутів особливо корисне для транзитних AS, де Enhanced IGRP взаємодіє з міждоменними протоколами маршрутизації, які застосовують більш глобальні стратегії, що реалізують масштабовану, засновану на стратегії маршрутизацію.

Типи пакетів протоколу Enhanced IGRP

У протоколі Enhanced IGRP використовуються наступні типи пакетів: вітання, підтвердження, оновлення, запити та відповіді.

Пакети вітання (hello packets) є багатоадресатними і призначені для виявлення і відновлення зв'язку із сусідніми вузлами. Ці пакети не вимагають підтвердження.

Пакети підтвердження являють собою пакети вітання, які не містять даних. Ці пакети містять ненульові номери підтвердження і завжди є одноадресатними.

Пакети оновлення використовуються для забезпечення досяжності одержувача. Коли виявляється новий сусідній маршрутизатор, йому відсилаються пакети оновлення для того, щоб він зміг побудувати свою топологічну таблицю. В інших випадках, таких як зміна витрат на з'єднання,

оновлення є багатоадресатними. Пакети оновлення використовують передачу з підтвердженням.

Пакети запитів і відповідей відправляються, коли одержувач не має допустимих маршрутизаторів. Пакети запитів завжди є багатоадресатними. Пакети відповідей посилають у відповідь на пакети запитів для того, щоб повідомити джерелу про відсутність необхідності повторно обчислювати маршрут, оскільки допустимий маршрутизатор існує. Пакети відповідей є одноадресатними й призначені тільки для джерела запиту. Пакети запитів і відповідей використовують передачу з підтвердженням.

6.6. Протоколи EGP і BGP

6.6.1. Особливості протоколу EGP

Протокол зовнішнього шлюзу (Exterior Gateway Protocol - EGP) є протоколом міждоменної маршрутизації.

Основи технології

EGP спочатку призначався для передачі інформації про маршрути між магістральними маршрутизаторами ARPANET. Інформація передавалася з окремих вузлів - джерел, що перебувають у різних адміністративних доменах, (автономних системах - AS), нагору в магістральні маршрутизатори, які передавали цю інформацію через магістральну область доти, поки її можна було передати вниз до мережі пункту призначення, що перебуває в межах іншої AS.

Незважаючи на те, що EGP є динамічним протоколом маршрутизації, він використовує дуже просту схему. Він не використовує додаткові характеристики маршрутів і не може приймати по-справжньому інтелектуальних рішень про маршрутизацію. Корегування маршрутизації EGP містять інформацію про досяжність мереж. Інакше кажучи, вони вказують, що в певні мережі потрапляють через певні маршрутизатори.

EGP має три основних функції. По-перше, маршрутизатори, що працюють із EGP, організують для себе певний набір сусідів. Сусіди - це просто інші маршрутизатори, з якими який-небудь маршрутизатор хоче колективно користуватися інформацією про досяжність мереж; які-небудь вказівки про географічне сусідство не включаються. По-друге, маршрутизатори EGP опитують своїх сусідів для того, щоб переконатися в їхній працездатності. По-третє, маршрутизатори EGP відправляють повідомлення про корегування, що містять інформацію про досяжність мереж у межах своїх AS.

Формат пакета

Формат пакета протоколу EGP представлений на рис. 6.6.

Field length,
In bytes

1	1	1	1	2	2	2	Variable
EGP version number	Type	Code	Status	Checksum	Autonomous system number	Sequence number	Data

Рисунок 6.6 - Формат пакета протоколу EGP

Першим полем у заголовку пакета EGP є **поле номера версії** EGP (EGP version number). Це поле визначає поточну версію EGP і перевіряється приймальними пристроями для визначення відповідності між номерами версій відправника й одержувача.

Наступним полем є **поле типу** (type), що визначає тип повідомлення. В EGP існує 5 окремих типів повідомлення, які будуть розглянуті нижче.

За полем типу йде **поле коду** (code). Це поле визначає різницю між підтипами повідомлень.

Наступне поле - **поле стану** (status), яке містить інформацію про стан, що залежить від повідомлення. У число кодів стану входять коди нестачі ресурсів

(insufficient resources), несправних параметрів (parameter problem), порушень протоколу (protocol violation), та інші.

За полем стану йде **поле контрольної суми** (checksum). Контрольна сума використовується для виявлення можливих проблем, які могли з'явитися в пакеті в результаті транспортування.

За полем контрольної суми йде **поле номера автономної системи** (autonomous system number). Воно визначає AS, до якої належить маршрутизатор-відправник.

Останнім полем заголовка пакета EGP є **поле номера послідовності** (sequence number). Це поле дозволяє двом маршрутизаторам EGP, які обмінюються повідомленнями, погоджувати запити з відповідями. Коли визначений який-небудь новий сусід, номер послідовності встановлюється у вихідне нульове значення й інкрементується на одиницю з кожною новою транзакцією запит-відповідь.

За заголовком EGP ідуть **додаткові поля**. Вміст цих полів розрізняється залежно від типу повідомлення (яке визначається полем типу).

Типи повідомлень

Здобуття сусіда. Повідомлення "здобуття сусіда" містить у собі інтервал вітання (hello interval) і інтервал опитування (poll interval). Поле інтервалу вітання визначає період інтервалу перевірки працездатності сусідів. Поле інтервалу опитування визначає частоту коригування маршрутизації.

Досяжність сусіда. Повідомлення про досяжність сусіда не мають окремих полів у числі полів, що йдуть за заголовком EGP. Ці повідомлення використовують поле коду для визначення різниці між привітальним повідомленням і відповіддю на привітальне повідомлення. Виділення функції оцінки досяжності з функції корегування маршрутизації зменшує трафік в мережі, тому що зміни про досяжність мереж зазвичай з'являються частіше, ніж зміни параметрів маршрутизації. Будь-який вузол EGP заявляє про відмову

одного зі своїх сусідів тільки після того, як від нього не був отриманий певний відсоток повідомлень про досяжність.

Опитування. Щоб забезпечити правильну маршрутизацію між AS, EGP повинен знати про відносне місце розташування віддалених вузлів. Повідомлення опитування дозволяє маршрутизаторам EGP одержувати інформацію про досяжність мереж, у яких перебувають ці машини. Такі повідомлення мають тільки одне поле крім звичайного заголовка – поле мережі джерела IP (source network). Це поле визначає мережу, що повинна використовуватися як контрольна крапка для запиту.

Корегування маршрутизації. Повідомлення про корегування маршрутизації дають маршрутизаторам EGP можливість вказувати місце розташування різних мереж у межах своїх AS. На додаток до звичайного заголовка ці повідомлення включають кілька додаткових полів.

Поле числа внутрішніх маршрутизаторів (number of interior gateways) вказує на число внутрішніх маршрутизаторів, що з'являються в повідомленні.

Поле числа зовнішніх маршрутизаторів (number of exterior gateways) указує на число зовнішніх маршрутизаторів, що з'являються в повідомленні.

Поле мережі джерела IP (IP source network) забезпечує адреси IP тієї мережі, від якої обмірюється досяжність. За цим полем йде послідовність блоків маршрутизаторів (gateway blocks). Кожен блок маршрутизаторів забезпечує адреси IP якого-небудь маршрутизатора й перелік мереж, а також відстаней, пов'язаних з досягненням цих мереж.

У межах одного блоку маршрутизаторів EGP перечислює мережі по відстанях. Наприклад, на відстані три може бути чотири мережі. Ці мережі перераховані по адресах. Наступною групою мереж можуть бути мережі, що перебувають на відстані 4, і т.д.

EGP не розшифровує показники відстані, що містяться в повідомленнях про корегування маршрутів. EGP фактично використовує поле відстані для вказівки існування якого-небудь маршруту; значення відстані може бути використано тільки для порівняння маршрутів, якщо ці маршрути повністю

перебувають у межах однієї конкретної AS. Із цієї причини EGP є скоріше протоколом досяжності, ніж протоколом маршрутизації. Це обмеження призводить також до обмежень у структурі Internet. Характерно, що будь-яка частина EGP мережі Internet повинна являти собою структуру дерева, у якого магістральний маршрутизатор є коренем, і в межах якого відсутні петлі між іншими AS. Це обмеження є основним обмеженням EGP; воно стало причиною його поступового витіснення іншими, більш досконалими протоколами зовнішньої маршрутизації.

Повідомлення про несправності. Повідомлення про несправності вказують на різні збійні ситуації. На додаток до загального заголовка EGP повідомлення про несправності забезпечують поле причини (reason), за яким іде заголовок повідомлення про несправності (message header). У число типових несправностей (причин) EGP входять несправний формат заголовка EGP (bad EGP header format), несправний формат поля даних EGP (bad EGP data field format), надмірна швидкість опитування (excessive polling rate) і неможливість досягнення інформації (unavailability of reachability information). Заголовок повідомлення про несправності складається з перших трьох 32-бітових слів заголовка EGP.

6.6.2. Особливості протоколу BGP

Принциповою відмінністю зовнішньої маршрутизації від внутрішньої є наявність маршрутної політики, тобто при розрахунку маршруту розглядається не стільки метрика, скільки політичні й економічні міркування. Ця обставина не дозволяє адаптувати під завдання зовнішньої маршрутизації готові протоколи внутрішньої маршрутизації, просто застосувавши їх до графа автономних систем, як раніше вони застосовувалися до графа мереж. По тій же причині існуючі підходи - дистанційно-векторний і стану зв'язків - непридатні для вирішення поставленої задачі.

Для вирішення задачі зовнішньої маршрутизації був розроблений протокол BGP (Border Gateway Protocol). Версія цього протоколу, що використовується в даний момент, має номер 4, відповідні стандарти - RFC-1771, 1772.

Загальна схема роботи BGP така. BGP-маршрутизатори сусідніх AS, які вирішили обмінюватися маршрутною інформацією, встановлюють між собою з'єднання по протоколу BGP і стають BGP-сусідами (BGP-peers).

Далі BGP використовує підхід за назвою path vector, що 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 адресу мережі та відстань до неї, а адресу мережі та список атрибутів (path attributes), що описують різні характеристики маршруту від маршрутизатора-відправника в зазначену мережу.

Даних, що містяться в атрибутах шляху, має бути досить, щоб маршрутизатор-одержувач, проаналізувавши їх з погляду політики своєї AS, міг ухвалити рішення щодо прийнятності або неприйнятності отриманого маршруту.

Внутрішній BGP, маршрутні сервери

Очевидно, що BGP-маршрутизатори, що перебувають в одній AS, також повинні обмінюватися між собою маршрутною інформацією. Це необхідно для погодженого відбору зовнішніх маршрутів відповідно до політики даної AS і для передачі транзитних маршрутів через автономну систему. Такий обмін робиться також по протоколу BGP, який у цьому випадку називається IBGP (Internal BGP), (відповідно, протокол обміну маршрутами між маршрутизаторами різних AS називається EBGP – External BGP).

Відмінність IBGP від EBGP полягає в тому, що при оголошенні маршруту BGP-сусідові, що перебуває в тій же самій AS, маршрутизатор не повинен додавати в AS_PATH номер своєї автономної системи. Дійсно, якщо номер AS

буде доданий, і сусід анонсує цей маршрут далі (знову з додаванням номера тієї ж AS), то та сама AS буде додана до AS_PATH двічі, що розцінюється як цикл.

Це правило спричиняє такий наслідок: щоб не виникло циклів, маршрутизатор не може анонсувати по IBGP маршрут, отриманий також по IBGP, оскільки немає способів виявити зациклення при оголошенні BGP-маршрутів усередині однієї AS.

В результаті цього наслідку виникає необхідність повного графа IBGP-з'єднань між прикордонними маршрутизаторами однієї автономної системи: тобто кожна пара маршрутизаторів повинна встановлювати між собою з'єднання по протоколу IBGP. При цьому виникає проблема великої кількості з'єднань (порядку N2, де N-число BGP-маршрутизаторів в AS). Для зменшення числа з'єднань застосовуються різні рішення: поділ AS на конфедерації (підсистеми), застосування серверів маршрутної інформації та ін.

Сервер маршрутної інформації, який обслуговує групу BGP-маршрутизаторів, працює дуже просто: він приймає маршрут від одного учасника групи і розсилає його всім іншим. Таким чином, учасникам групи немає необхідності встановлювати BGP-з'єднання попарно; замість цього кожен учасник встановлює одне з'єднання із сервером.

Слід зазначити, що сервер маршрутної інформації обслуговує тільки анонси маршрутів, а не сам трафік по цих маршрутах.

Атрибути протоколу BGP

Маршрути, отримані з використанням протоколу BGP, мають деякі властивості, які використовуються для визначення найкращого маршруту в тих випадках, коли є кілька маршрутів до пункту призначення. Ці властивості називаються атрибутами протоколу BGP. Існують такі атрибути, які BGP використовує при виборі маршруту:

- Weight;
- Local preference;
- Multi-exit discriminator;
- Origin;

- AS_path;
- Next-hop;
- Community.

Атрибут Weight

Атрибут Weight (вага) являє собою атрибут, введений корпорацією Cisco і є локальним для конкретного маршрутизатора. Він не анонсується сусіднім маршрутизаторам. Якщо маршрутизатор виявляє кілька маршрутів до пункту призначення, то вибирається маршрут з найбільшою вагою.

Атрибут ORIGIN

ORIGIN (тип 1) - обов'язковий атрибут, що вказує на джерело інформації про маршрут:

0 - IGP (інформація про досяжність мережі отримана від протоколу внутрішньої маршрутизації або введена адміністратором),

1 - EGP (інформація про досяжність мережі імпортована із застарілого протоколу EGP),

2 - INCOMPLETE (інформація отримана іншим чином, наприклад, RIP->OSPF->BGP або BGP->OSPF->BGP).

Атрибут ORIGIN вставляється маршрутизатором, що генерує інформацію про маршрут, і при наступному анонсуванні маршруту іншими маршрутизаторами не змінюється. Атрибут фактично визначає надійність джерела інформації про маршрут (найбільш надійний ORIGIN=0).

Атрибут AS_PATH

AS_PATH (тип 2) - обов'язковий атрибут, що містить список автономних систем, через які повинна пройти дейтаграма на шляху в мережу, зазначену в маршруті.

Кожен BGP-вузол при анонсуванні маршруту (за винятком IBGP-з'єднань) додає в AS_PATH номер своєї AS. Можливо (залежно від політики) додатково додаються номери інших AS.

NEXT_HOP

NEXT_HOP (тип 3) - обов'язковий атрибут, що вказує адресу наступного BGP-маршрутизатора на шляху в заявлену мережу; може збігатися або не збігатися з адресою BGP-вузла, що анонсує маршрут. Зазначений в NEXT_HOP маршрутизатор повинен бути досяжний для одержувача даного маршруту. При передачі маршруту по IBGP NEXT_HOP не змінюється.

MULTI_EXIT_DISC

MULTI_EXIT_DISC (тип 4) - необов'язковий атрибут, який являє собою пріоритет використання оголошуючого маршрутизатора, для досягнення через нього мережі, що анонсується. Тобто, фактично це метрика маршруту з погляду маршруту BGP-вузла, що анонсує. Має сенс не саме значення, а різниця значень, коли кілька маршрутизаторів однієї AS повідомляють про досяжність через себе однієї й тієї ж мережі, надаючи в такий спосіб одержувачам кілька варіантів маршрутів в одну мережу. За інших рівних умов дейтаграми в мережі, що оголошується, будуть пересилатися через маршрутизатор, що заявив менше значення MULTI_EXIT_DISC.

Атрибут зберігається при наступних оголошеннях маршруту по IBGP, але не по EBGP.

Атрибут LOCAL_PREF

LOCAL_PREF (тип 5) - необов'язковий атрибут, що встановлює для даної AS пріоритет даного маршруту серед всіх маршрутів до заявленої мережі, відомих усередині AS. Атрибут обчислюється кожним граничним маршрутизатором для кожного присланого йому по EBGP маршруту і потім поширюється разом із цим маршрутом по IBGP у межах даної AS. Спосіб обчислення значення атрибута визначається політикою прийому маршрутів (за замовчуванням береться до уваги тільки довжина AS_PATH). LOCAL_PREF використовується для погодженого між маршрутизаторами однієї AS вибору маршруту з декількох варіантів.

Атрибут Community

Цей атрибут забезпечує спосіб групової адресації одержувачів, які називаються співтовариством (community), до якого можуть відноситися рішення про вибір маршруту (такі, як прийняття, перевага і перерозподіл). Для встановлення даного атрибута використовуються перетворення маршрутів. Стандартні значення атрибута Community:

- **no-export** (не експортується). Такий маршрут не анонсується одноранговим вузлам протоколу EBGP;
- **no-advertise** (не анонсується). Цей маршрут не анонсується ніяким одноранговим вузлам;
- **Internet.** Про цей маршрут оповіщається співтовариство Internet. До цього співтовариства належать всі маршрутизатори мережі.

Атрибути агрегування ATOMIC_AGGREGATE (тип 6) і AGGREGATOR (тип 7) - необов'язкові атрибути, пов'язані з операціями агрегування (об'єднання) декількох маршрутів в один.

Обробка маршрутної інформації (Decision Process) і маршрутні політики

Розглянемо дії BGP-маршрутизатора при отриманні й анонсуванні маршруту. Маршрутизатор використовує три бази даних: Adj-RIBs-In, Loc-RIB і Adj-RIBs-Out, в яких містяться маршрути, відповідно, отримані від сусідів, використовувані самим маршрутизатором і ті, що повідомляються сусідам. Також на маршрутизаторі сконфігуровані дві політики: політика прийому маршрутів (accept policy) і політика анонсування маршрутів (announce policy). Для обробки маршрутів у базах даних відповідно до наявних політик маршрутизатор виконує процедуру, що називають процес відбору (decision process).

Маршрути, отримані від BGP-сусідів, поміщаються в базу даних Adj-RIBsIn. Відповідно до політики прийому для кожного маршруту в Adj-RIBs-In

обчислюється пріоритет (це називається фазою 1 процесу відбору). У результаті цих дій деякі маршрути можуть бути відбраковані (визнані неприйнятними).

Далі (фаза 2) для кожної мережі із всіх наявних (отриманих і невідбракованих) варіантів вибирається маршрут з більшим пріоритетом. Результати заносяться в базу Loc-RIB, звідки менеджер маршрутної таблиці IP-модуля може їх взяти для установки в таблицю маршрутів маршрутизатора й для експорту у внутрішній протокол маршрутизації для того, щоб й інші вузли автономної системи мали маршрути до зовнішніх мереж. І навпаки, щоб інші автономні системи мали маршрути до мереж даної AS, з таблиць протоколу (протоколів) внутрішньої маршрутизації можуть витягатися номери мереж своєї AS і заноситися в Loc-RIB.

Задача третьої фази - відбір маршрутів для анонсування (розсилання сусідам). З LocRIB вибираються маршрути, що відповідають політиці анонсування, і результат поміщається в базу Adj-RIBsOut, вміст якої й розсилається BGP-сусідам. Можливо, що маршрутизатор має різні політики анонсування для кожного сусіда.

Послідовність обробки маршрутної інформації модулем BGP представлена на рис. 6.7.

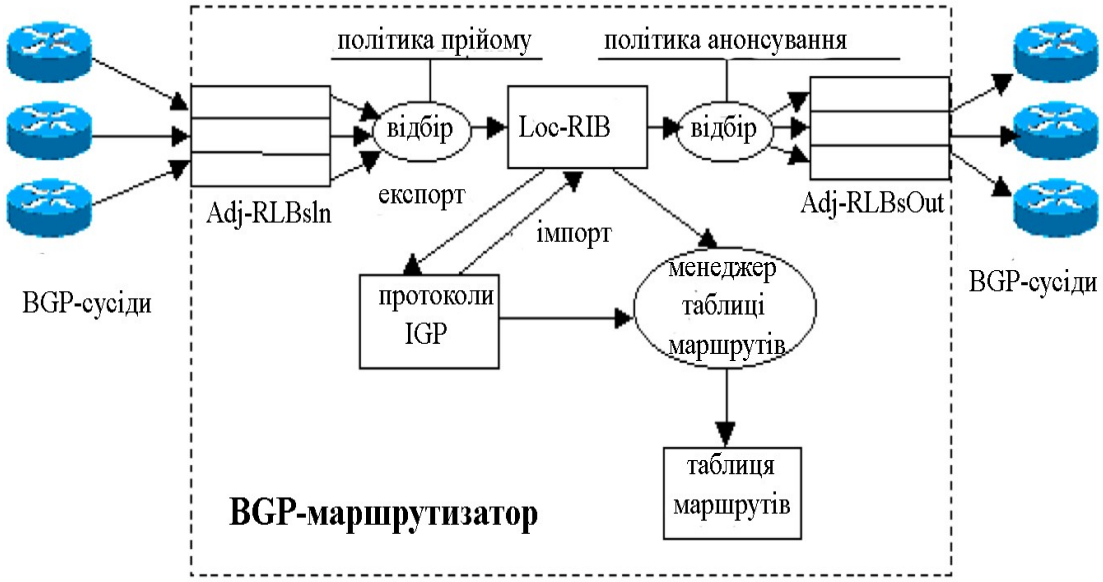


Рисунок 6.7 - Обробка маршрутної інформації модулем BGP

Важливою властивістю процесу відбору є те, що BGP-маршрутизатор повідомляє тільки ті маршрути, які він сам використовує. Ця обставина є наслідком природи IP-маршрутизації: при виборі маршруту для дейтаграми враховується тільки адреса одержувача і ніколи - адреса відправника. Таким чином, якщо маршрутизатор сам використовує один маршрут у мережу X, а сусідові оголосив інший, то дейтаграми від сусіда все одно будуть пересилатися в мережу X по тому маршруту, що використовує сам маршрутизатор, оскільки адреса відправника при виборі маршруту IP-модулем не розглядається.

Формулювання маршрутних політик

Способи опису маршрутних політик не є частиною протоколу BGP і відрізняються в різних реалізаціях BGP. Однак, у кожному випадку політики базуються на критеріях відбору маршрутів і модифікації атрибутів маршрутів, що потрапили під критерії відбору. Модифікація атрибутів маршруту у свою чергу впливає на пріоритет цього маршруту при відборі декількох альтернативних маршрутів під час фази 2.

Для повної заборони прийняття або оголошення маршруту використовується фільтрація, яку можна розглядати як призначення найнижчого пріоритету, що не дозволяє використати маршрут взагалі.

Відбір маршрутів з бази Adj-RIBsIn (для реалізації політики прийому) може відбуватися, наприклад, за наступними критеріями:

- регулярне вираження для значення AS_PATH (окремі випадки: номер кінцевої AS маршруту, AS сусіда, від якого отриманий маршрут);

- адреса мережі, в яку веде маршрут;

- адреса сусіда, що надіслав інформацію про маршрут;

- походження маршруту (атрибут ORIGIN).

До маршруту, що задовольняє встановленому критерію, можна застосувати наступні політики:

- не приймати маршрут - видалити з Adj-RIBsIn (фільтрація);

- встановити адміністративну вагу маршруту,

- встановити значення атрибута LOCAL_PREF,

- встановити маршрут як маршрут за замовчуванням.

Адміністративна вага маршруту не є атрибутом BGP, вона встановлює внутрішній пріоритет маршруту на даному маршрутизаторі (у той час, як LOCAL_PREF встановлює пріоритет маршруту в рамках автономної системи).

Якщо (після виконання фільтрації) у базі Adj-RIBsIn є кілька альтернативних маршрутів, що ведуть в одну мережу призначення, то відбір кращого з них робиться фазою 2 за наведеними нижче критеріями (на прикладі маршрутизаторів Cisco). Критерії послідовно застосовуються в зазначеному порядку, поки не залишиться єдиний маршрут:

- найбільша адміністративна вага;

- найбільше значення LOCAL_PREF;

- перевага віддається шляху, який був ініційований процесом протоколу BGP, що виконується на цьому маршрутизаторі;

- найкоротший AS_PATH (маршрут, породжений у локальній AS, має самий короткий - порожній - AS_PATH);

- найменше значення ORIGIN (IGP<EGP<INCOMPLETE);

- найменше значення MULTI_EXIT_DISC (відсутній MULTI_EXIT_DISC вважається нульовим);

- маршрут, отриманий по EBGP, проти маршруту, отриманого по IBGP;

- якщо всі маршрути отримані по IBGP, то вибирається маршрут через найближчого сусіда;

- маршрут, отриманий від BGP-сусіда з найменшим ідентифікатором.

Принцип роботи протоколу BGP

Пара BGP-сусідів встановлює між собою з'єднання по протоколу TCP, порт 179. Сусіди, що належать різним AS, повинні бути доступні один одному безпосередньо; для сусідів з одної AS 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. Існує 4 типи повідомлень.

Типи BGP-повідомлень

OPEN - посилається після встановлення TCP-з'єднання. Відповіддю на OPEN є повідомлення KEEPALIVE, якщо друга сторона згодна стати BGP-сусідом; інакше посилає повідомлення NOTIFICATION з кодом, що пояснює 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 й пересилання 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 додані або вилучені маршрути в міру їхньої появи (partial update).

NOTIFICATION - повідомлення цього типу використовується для інформування сусіда про причину закриття з'єднання. Після відправлення цього повідомлення BGP-з'єднання закривається.

6.7. Протоколи групової маршрутизації IGMP, DVMPR, MOSPF, PIM

Як було зазначено у розділі 1, в основі групової IP-адресації лежить поняття груп, для ідентифікації яких використовуються спеціальні типи адрес – multicast (наприклад, адреси класу D IP v4).

Побудова складених мереж з підтримкою мультикастинга є набагато складнішим завданням, ніж організація групової розсилки в межах однієї IP-

мережі. Для просування групових дейтаграм від відправника до одержувачів через складену мереж необхідно здійснювати маршрутизацію дейтаграм. Однак по груповій дейтаграмі не можна визначити індивідуальні IP-адреси її одержувачів. В результаті, використання звичайної IP-маршрутизації і навіть її принципів немає сенсу. Тому для маршрутизації групових дейтаграм були розроблені спеціальні методи й протоколи.

Основним припущенням, яке при цьому робиться, є те, що маршрутизатор знає, члени яких груп знаходяться у безпосередньо приєднаних до нього мережах. Механізм реєстрації членів груп на маршрутизаторі, до якого підключена їхня мережа, реалізований у протоколі IGMP.

6.7.1. Особливості протоколу IGMP

Протокол IGMP (Internet Group Memebership Protocol) призначений для реєстрації на маршрутизаторі членів груп, що знаходяться у безпосередньо приєднаних до нього мережах. Маючи цю інформацію, маршрутизатор може повідомляти іншим маршрутизаторам (за допомогою протоколів групової маршрутизації) про необхідність пересилки йому дейтаграм для тих чи інших груп. Сучасна версія протоколу IGMP – версія 2 – документована в RFC-2236.

Формат пакета протоколу IGMP наведений на рис. 6.8.

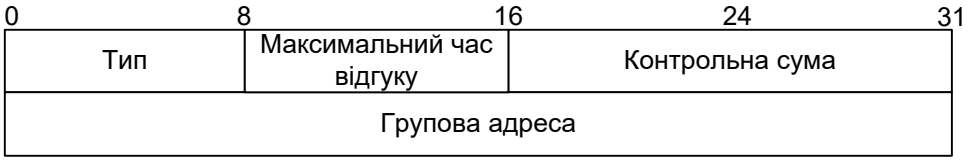


Рисунок 6.8 - Формат пакета протоколу IGMP v2

В IGMP v 2 передбачено чотири типи IGMP-повідомлень:

- запит належності до групи;
- відповідь на запит про належність до групи за версією 1; ′
- відповідь на запит про належність до групи за версією 2;

- повідомлення про вихід із групи.

Вузли відсилають IGMP-відповіді, які відповідають певній multicast групі, для того, щоб повідомити про своє бажання приєднатися до цієї групи. Маршрутизатор періодично відправляє IGMP-запит, щоб переконатися, що хоча б один вузол у підмережі ще зацікавлений в одержанні даних, призначених для даної групи. При підключенні вузла до нової групи він самостійно відправляє повідомлення типу «відповідь на запит про належність до групи», не чекаючи чергового запиту від маршрутизатора.

Для кожної групи, членів якої було виявлено в мережі, маршрутизатор веде відлік часу неактивності. Якщо жодної «відповідь на запит про приналежності до групи» для цієї групи не було отримано за певний період (за замовчуванням - 260 с), то маршрутизатор вважає, що членів цієї групи в мережі більше немає.

Коли вузол від'єднується від групи, він може послати повідомлення про вихід із групи по груповій адресі 224.0.0.2 ("всім маршрутизаторам"); адреса групи міститься в полі "Адреса групи". Вузлу необхідно зробити це, якщо на останній запит про належність до групи від імені даної групи відповідав саме цей вузол. Одержавши повідомлення про вихід із групи, маршрутизатор генерує приватний запит про належність до групи для членів тільки цієї групи. Якщо за час, зазначений у полі "Максимальний час відгуку" запиту (за замовчуванням - 1 с), маршрутизатор не одержав жодного відповіді «відповідь на запит про приналежності до групи», то він вважає, що членів даної групи в мережі більше немає. Для надійності запит посилається 2 рази.

Сполучні дерева групової розсилки

Маршрутизатори групової розсилки створюють сполучні дерева, по яких визначається маршрут, яким повинні пройти по мережі дані групової розсилки протоколу IP, щоб досягти всіх одержувачів. Існує два основних типи групових сполучних дерев: дерева від джерела і дерева спільного доступу.

Дерево від джерела

Найпростішою формою групового зв'язкового дерева є дерево від джерела. Його коренем служить джерело групового дерева, а гілки утворюють сполучне дерево, що з'єднує джерело з одержувачами. Оскільки це дерево використовує найкоротші маршрути, його також називають деревом найкоротших маршрутів (shortest path tree - SPT).

Дерево SPT описується у вигляді пари значень типу (S, G), де S – IP-адреса джерела (Source), а G – групова адреса одержувачів (Group). Зокрема, SPT-дерево на рис. 6.9 описується як (192.1.1.1, 224.1.1.1).

Під записом (S,G) розуміється, що між кожним джерелом і кожною групою існує єдине й коректне SPT-дерево. Наприклад, якщо вузол B також відправляє дані групі 224.1.1.1, а одержувачами є вузли A и C, то повинне існувати окреме дерево (192.2.2.2, 224.1.1.1).

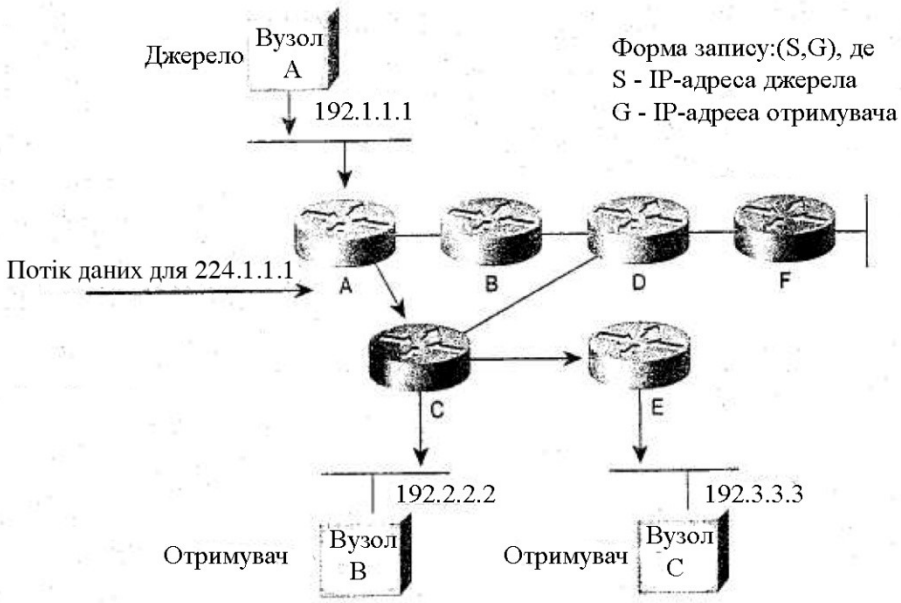


Рисунок 6.9 - Приклад SPT-дерева

Дерево спільного доступу

На відміну від дерева джерела, корінь якого знаходиться в джерелі, дерева спільного доступу мають єдиний, загальний корінь у деякій спеціально призначеній для цього точці мережі. Такий спільний корінь називається точкою рандеву (Rendezvous Point - RP). При використанні дерева спільного доступу джерела відправляють потоки даних кореню, звідки він передається в спадному напрямку по дереву спільного доступу всім одержувачам.

На рис. 6.10 наведено дерево спільного доступу для групи 224.2.2.2, коренем якого є маршрутизатор D.

У цьому прикладі дані групової розсилки від джерел – вузлів A и D – передаються кореню (маршрутизатор D), а звідти по дереву спільного доступу – двом одержувачам, вузлам B и C. Оскільки всі джерела в multicast групі використовують одне дерево спільного доступу, то для його позначення застосовується форма запису із груповим символом *: (*, G). "Зірочка" в цьому випадку означає всі джерела, а G – групу групової розсилки. Відповідно, дерево спільного доступу на рис. 6.10 позначається як (*, 224.2.2.2).

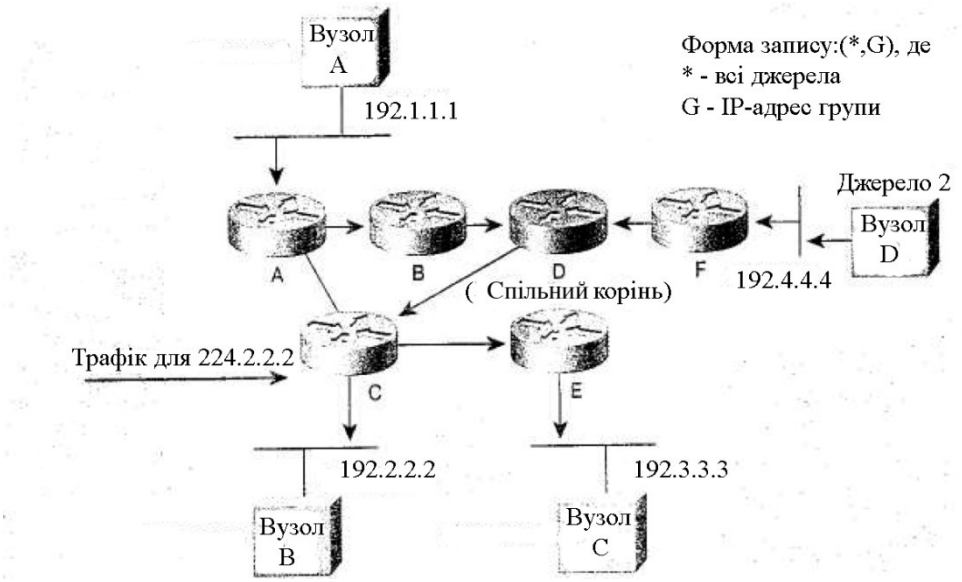


Рисунок 6.10 - Дерево спільного доступу

Дерева SPT і дерева спільного доступу не повинні мати петель. Повідомлення дублюються тільки в точках, де з'являються нові гілки.

Приєднатися до групи групової розсилки або покинути її можна в будь-який момент, тому сполучні дерева мають потребу в динамічному оновленні. Якщо всі активні одержувачі даної гілки перестануть запитувати дані даної групи, то маршрутизатори повинні виключити цю гілку зі сполучного дерева й припинити передачу по ній даних. Якщо один з одержувачів даної гілки знову стане активним і запросить дані групової розсилки, то маршрутизатор динамічно змінить сполучне дерево й відновить передачу даних.

Дерево найкоротших маршрутів має перевагу, що полягає в створенні оптимального маршруту між джерелом й одержувачами. Це забезпечує мінімальну затримку при передачі даних групової розсилки. Однак така оптимізація має свою ціну: маршрутизатори повинні збирати маршрутну інформацію про кожне джерело. Якщо в мережі тисячі джерел і груп, то це вимагатиме від маршрутизаторів значних витрат ресурсів.

Перевага дерев спільного доступу полягає в тому, що кожен маршрутизатор повинен зберігати лише мінімальний обсяг інформації про стан мережі. Якщо в мережі використовуються тільки дерева спільного доступу, то це знижує загальні вимоги до пам'яті. Недоліком дерев спільного доступу є те, що, в певних обставинах, маршрути між джерелом й одержувачами не є оптимальними, що може призвести до затримки при доставці пакетів.

Зворотна передача

При multicast маршрутизації джерело відправляє дані довільній групі одержувачів, представлених груповою адресою. Груповий маршрутизатор повинен визначити, який з напрямків є вхідним (до джерела), а який (які) - вихідним. Якщо вихідних маршрутів багато, то маршрутизатор копіює пакет і направляє його по відповідних маршрутах, причому, необов'язково по всіх. Принцип доставки даних групової розсилки не стільки до одержувача, скільки від джерела, називається зворотною передачею.

Пересилки по зворотному маршруту (Reverse Path Forwarding - RPF) являють собою фундаментальний принцип групової маршрутизації, що дозволяє маршрутизаторам передавати дані групової розсилки по сполучному дереву в правильному напрямку. При використанні RPF сусідні вхідні й вихідні вузли визначаються по таблиці маршрутизації одноадресатного розсилання. Маршрутизатор відправляє груповий пакет тільки в тому випадку, якщо цей пакет надійшов на вхідний інтерфейс. Це гарантує відсутність петель у сполучному дереві.

RPF-перевірка. Коли на вхід маршрутизатора надходить груповий пакет, маршрутизатор виконує його RPF-перевірку. Якщо вона пройшла успішно, то пакет відправляється, в іншому випадку він відкидається.

Для пакета, що направляється по сполучному дереву, RPF-перевірка полягає в наступному.

1. Маршрутизатор визначає по таблиці одноадресатної маршрутизації адресу джерела і перевіряє, чи надійшов пакет на інтерфейс зворотного маршруту й чи не направляється він назад до джерела.
2. Якщо пакет надійшов на інтерфейс, який веде назад до джерела, то RPF- перевірка вважається успішно завершеною і пакет відправляється.
3. Якщо RPF-перевірка завершилася невдало, то пакет відкидається.

6.7.2. Особливості протоколу DVMRP

Протокол DVMRP (Distance Vector Multicast Routing Protocol, RFC-1075) - самий старий протокол групової маршрутизації. Протокол працює за технологією RPF, але для побудови дерев використовується власний дистанційно-векторний протокол, аналогічний протоколу RIP.

При отриманні першого пакета маршрутизатор не має інформації про групу. Він посилає отриманий пакет через всі інтерфейси, крім того, через який цей пакет був отриманий. Якщо пакет прийшов не через інтерфейс, що

використовується маршрутизатором для посилки пакетів відправникові групової інформації, отриманий пакет відкидається. При отриманні пакета маршрутизатором, у зоні відповідальності якого немає членів групи, він посилає повідомлення про видалення (prune-команда). Ці повідомлення використовуються для відсікання від дерева маршрутів гілок, що не містять членів групи. Після закінчення певного часу "відрізані" гілки дерева маршрутів "відростають" знову, й знову можуть бути відсічені. Протокол DVMRP відноситься до внутрішніх протоколів маршрутизації, які призначені для використання в межах автономної системи.

6.7.3. Особливості протоколу MOSPF

Протокол MOSPF (Multicast OSPF, RFC-1584) є розширенням протоколу OSPF. Маршрутизатор, що підтримує це розширення, встановлює біт "M" у полі "Options" повідомлення "Hello". В базу даних стану зв'язків вводиться додатковий тип запису: для зазначеної мережі перераховуються всі групи, члени яких є в цій мережі. Ці записи, як і всі інші записи бази даних стану зв'язків, поширюються по системі мереж за допомогою протоколу затоплення (flooding). Для транзитної мережі запис вноситься в базу даних виділеним маршрутизатором.

Дерева розсилки групових дейтаграм будуються по методу RPF на основі бази даних стану зв'язків. Відзначимо, що розсилка "пробних" групових дейтаграм і наступне відсікання непотрібних гілок дерева в цьому випадку не відбувається, тому що інформація про наявність у мережах членів груп уже міститься в базі даних.

Протокол MOSPF має серйозну проблему, пов'язану з масштабуванням: для кожної пари "джерело-група" проводиться окремий запуск алгоритму SPF для розрахунку дерева розсилки. При великій кількості джерел, а також при нестабільній топології системи мереж, на ці обчислення витрачаються істотні обчислювальні ресурси маршрутизаторів. Крім того, варто врахувати

необхідність застосування протоколу затоплення для розсилки інформації про членство в групах при її зміні.

І, нарешті, очевидно, що MOSPF вимагає використання OSPF як протоколу маршрутизації, тобто, не є незалежним і може застосовуватися тільки в OSPF-системах.

6.7.4. Особливості протоколу PIM

Протокол незалежної від протоколу групової розсилки (Protocol-Independent Multicast - PIM) одержав таку назву внаслідок того, що він не залежить від IP-протоколу маршрутизації. PIM може діяти незалежно від того, який протокол одноадресатної маршрутизації використовується для заповнення таблиць маршрутизації - EIGRP, OSPF, BGP або статичні маршрути. Протокол PIM використовує для групової пересилки цю одноадресну маршрутну інформацію. Незважаючи на те, що PIM називають груповим протоколом маршрутизації, насправді, замість побудови повністю незалежної таблиці групової маршрутизації, він використовує для зворотної передачі таблицю одноадресатної маршрутизації. При використанні PIM, на відміну від інших протоколів, маршрутизатори не посилають і не приймають оновлень групових маршрутів.

Щільний режим протоколу PIM

У щільному режимі PIM (PIM Dense Mode - PIM-DM) доставка даних групової розсилки по всій мережі здійснюється методом виштовхування. Цей метод "грубої сили" по доставці даних одержувачам ефективний для деяких прикладних програм за умови, що активні одержувачі є в кожній підмережі.

Спочатку протокол PIM-DM поширює дані групової розсилки по всій мережі. Маршрутизатори, що не мають сусідів, розташованих у напрямку передачі даних, відсікають ці небажані дані. Такий процес повторюється кожні 3 хвилини.

Механізм поширення й припинення потоків даних є способом нагромадження маршрутизаторами інформації про стан шляхом одержання

потоків даних. Ці потоки даних містять інформацію про джерело і групу, так що маршрутизатори, розташовані в напрямку передачі даних, можуть створювати власні таблиці групової розсилки. Протокол PIM-DM підтримує тільки дерева джерела. Він не може бути використаний для побудови дерев спільного доступу.

Розріджений режим протоколу PIM

У розрідженому режимі PIM (PIM Sparse Mode - PIM-SM) доставка даних групової розсилки здійснюється методом "втягування". Дані передаються тільки в ті мережі, де є активні джерела, що послали явний запит на одержання цих даних.

Для поширення інформації про активні джерела в протоколі PIM-SM використовується дерево спільного доступу. В залежності від конфігурації дані можуть залишатися в межах дерева спільного доступу або перейти на оптимізоване дерево джерела. Дані починають поширюватися по дереву спільного доступу, а потім маршрутизатори, розташовані на його шляху, визначають, чи є кращий маршрут до джерела. Якщо існує кращий, більш короткий маршрут, то виділений (найближчий до одержувача) маршрутизатор відправляє джерелу повідомлення про приєднання, і дані перенаправляються по цьому маршруті.

Оскільки в протоколі PIM-SM, принаймні спочатку, використовується загальне дерево доступу, в ньому використовуються точки рандеву RP. Ці точки рандеву RP настроюються адміністратором мережі. Джерела реєструються в точці рандеву RP, після чого дані передаються одержувачам по дереву спільного доступу. Якщо дерево спільного доступу не є оптимальним маршрутом між джерелом й одержувачем, то маршрутизатори динамічно створюють дерево від джерела й припиняють передачу даних по дереву спільного доступу.

Протокол PIM-SM легко масштабується для мереж будь-якого розміру, у тому числі й тих, де використовуються канали глобальних мереж. Механізм явного приєднання запобігає передачі небажаних даних по глобальних каналах.

Розріджено-щільний режим

Корпорація Cisco розробила новий логічний IP-інтерфейс маршрутизатора, що дозволяє вибирати між щільним і розрідженим режимами. Така необхідність виникла через зміну принципу передачі даних групової розсилки по протоколу PIM, що стало очевидним у процесі розвитку цієї технології. Виявилося, що краще вибирати режим – розріджений або щільний – для кожної групи, а не для кожного маршрутизатора. Таку можливість надає розріджено-щільний режим.

Параметри розріджено-щільного режиму настроюються адміністратором мережі. Він може призначити окремим групам щільний або розріджений режим, залежно від того, чи доступна даній групі інформація про точки рандеву RP. Якщо маршрутизатор має RP-інформацію для групи, то для неї вибирається розріджений режим, у іншому випадку використовується щільний режим.

Питання для самоперевірки та контролю засвоєння знань

1. Що розуміють під маршрутизацією?
2. Що розуміють під автономною системою?
3. Що розуміють під внутрішнім шлюзом?
4. Що розуміють під зовнішнім шлюзом?
5. Де використовують протоколи маршрутизації внутрішнього шлюзу?
6. Де використовують протоколи маршрутизації зовнішнього шлюзу?
7. Чим протокол маршрутизації відрізняється від протоколу, що маршрутизується?
8. За якими критеріями можна класифікувати алгоритми маршрутизації?
9. Що характерно для статичної маршрутизації?
10. Що характерно для динамічної маршрутизації?
11. Що характерно для лінійної маршрутизації?
12. Що характерно для ієрархічної маршрутизації?

13. Що характерно для алгоритмів маршрутизації за станом каналу?
14. Що характерно для дистанційно-векторних алгоритмів маршрутизації?
15. Що розуміють під метрикою маршруту?
16. Які параметри можуть бути використані для формування метрики маршруту?
17. До якого класу відноситься протокол RIP?
18. Що використовує у якості метрики маршруту у протоколі RIP?
19. Наведіть основні етапи алгоритму побудови маршрутних таблиць протоколом RIP.
20. Які механізми використовуються у протоколі RIP для відслідковування змін стану мережі?
21. Які механізми запобігання петлям маршрутизації використовуються у протоколі RIP?
22. До якого класу відноситься протокол OSPF?
23. Наведіть основні етапи алгоритму побудови маршрутних таблиць протоколом OSPF.
24. Що використовує у якості метрики маршруту у протоколі OSPF?
25. Для чого виконується розбиття на області при використання протоколу OSPF?
26. Що розуміють під маршрутизаторами – сусідами в OSPF – процесі?
27. Що розуміють під суміжними маршрутизаторами в OSPF – процесі?
28. Які задачі дозволяє вирішити підтримка множинних маршрутів у протоколі OSPF?
29. До якого класу відноситься протокол IGRP?
30. Що використовує у якості метрики маршруту у протоколі IGRP?
31. Чи підтримує множинні маршрути протокол IGRP?
32. Які функції підтримує протокол IGRP для підвищення стабільності маршрутизації у мережі?
33. Наведіть основні відмінності протоколу EIGRP від IGRP.

34. Які механізми використовуються у протоколі EIGRP для підвищення ефективності?
35. До якого класу відноситься протокол EGP?
36. Наведіть основні етапи побудови маршрутів протоколом EGP.
37. Який основний недолік протоколу EGP?
38. До якого класу відноситься протокол BGP?
39. У чому полягає особливість використання протоколу BGP для маршрутизації в середині автономної системи?
40. Яку функцію виконує сервер маршрутної інформації в BGP – маршрутизації?
41. Які атрибути використовує протокол BGP для вибору оптимального маршруту?
42. Для вирішення яких задач використовують протоколи групової маршрутизації?
43. Для чого призначений протокол IGMP (Internet Group Memebership Protocol)?
44. Що розуміють під сполучними деревами групової розсилки?
45. Які існують типи групових сполучних дерев?
46. Що характерно для дерева від джерела (найкоротших маршрутів)?
47. Що характерно для дерева спільного доступу?
48. Що розуміють під зворотною передачею при груповій розсилці?
49. Для чого використовуються пересилки по зворотному маршруту?
50. Наведіть основні особливості протоколу DVMRP (Distance Vector Multicast Routing Protocol).
51. Наведіть основні особливості протоколу MOSPF (Multicast OSPF).
52. Наведіть основні особливості протоколу PIM (Protocol-Independent Multicast).

БІБЛІОГРАФІЧНИЙ СПИСОК

Основна література

1. Кучернюк, П. В. Основи побудови інформаційних мереж [Електронний ресурс] : навчальний посібник для студентів спеціальності «Радіоелектронні апарати та засоби» / П. В. Кучернюк ; НТУУ «КПІ». –Київ : НТУУ «КПІ», 2014. – 269 с.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. - Спб.: издательство «Питер», 2006. - 958с.
3. Столлиггс В. Современные компьютерные сети – СПб.: Питер, 2003. – 783 с.
4. Кулаков Ю.О., І.А. Жуков Комп'ютерні мережі // навчальний посібник з грифом МОН України Вид-во Нац. Авіа. Ун-ту «НАУ-друк», 2009.—329 с.
5. Матеріали для самостійної роботи студентів по курсу "Комп'ютерні мережі". Розділи: структура стека протоколів TCP/IP, протоколи маршрутизації. Методичні вказівки для студентів спеціальності 7.05090201, 8.05090201 «Радіоелектронні апарати та засоби»/ Уклад.: П.В. Кучернюк. – К.: НТУУ «КПІ», 2012 – 126 с.
6. Новые технологии и оборудование IP- сетей/ В.Г. Олифер, Н.А. Олифер.- СПб: Издательство «Питер», 2001. – 512 с.
7. А. Филимонов. Протоколы Интернета. БХВ-Петербург, 2003. - 516 с.

Додаткова література

1. Гук М. Аппаратные средства локальных сетей. Энциклопедия – СПб: Издательство «Питер», 2000. – 576 с.
2. Технологии передачи данных. 7-е изд./ Г.Хелд.-СПб.: Питер, К.: Издательская группа BHV, 2003. - 720 с.

3. А.Б.Семенов и др. Структурированные кабельные системы. ДМК Пресс; 2006 - 640 с.
4. David Barnett, David Groth, Jim McBee. Cabling: The Complete Guide to Network Wiring, Third Edition, SYBEX Inc San Francisco • London, 2004. - 733 p.
5. Руководство по технологиям объединенных сетей, 4-е издание.: Пер. С англ.. – М.: Издательский дом «Вильямс», 2005. – 1040 с.
6. М. Като. "Построение сетей ЭВМ", М.: Мир, 1988.
7. Ю. Блэк. "Сети ЭВМ: протоколы, стандарты, интерфейсы", М. Мир, 1990.
8. Халсалл. "Передача данных, сети компьютеров и взаимосвязь открытых систем", 1995.
9. TCP/IP КРУПНЫМ ПЛАНОМ. http://www.soslan.ru/tcp/index.html
10. Microsoft TCP/IP. Учебный курс: Офиц. пособие Microsoft для самостоятельной подготовки: Пер. с англ. - 3-е изд., испр. - М.: Издательско-торговый дом "Русская Редакция", 2001. - 366 с.
11. Семенов Ю.А. Telecommunication technologies - телекоммуникационные технологи - http://book.itep.ru/preword.htm
12. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-издание, исправленное, Cisco Systems; – М.: Издательский дом «Вильямс», 2008. - 1168 с.
13. Руководство Cisco по технологиям объединенных сетей, 4-е издание, Cisco Systems; – М.: Издательский дом «Вильямс», 2005. - 1040 с.

ПЕРЕЛІК СКОРОЧЕНЬ

ABR	area border router - прикордонний маршрутизатор області
ACR	відношення загасання сигналу до загасання перехресного наведення на ближньому від передавача кінці лінії
AFI	Address-Family Identifier - ідентифікатор сімейства адреси
ARP	address resolution protocol – протокол перетворення адрес
ARQ	автоматичний запит на повторення
AS	autonomous systems – автономна система
ASBR	autonomous system border router - прикордонний маршрутизатор автономної системи
ATM	асинхронний режим передачі
AWG	американська градація проводів
BGP	Border Gateway Protocol
CIDR	Classless Inter-Domain Routing - безкласова міждоменна маршрутизація
CNAME	canonical name – канонічне ім’я (псевдонім)
CRC	циклічний контроль по надлишковості
CTS	дозвіл передачі
CWDM	розріджене мультиплексування за довжинами хвиль
DA	адреса отримувача
DNS	Domain Name System – система доменних імен
DS	Differentiated Services – диференціальне обслуговування
DSAP	точка доступу до послуги отримувача
DSCP	Differentiated Services Code Point – код точки диференціальної послуги
DSL	цифрова абонентська лінія
DUAL	Diffusing Update Algorithm - дифузійний алгоритм оновлення
DVMRP	Distance Vector Multicast Routing Protocol

DWDM	щільне мультиплексування за довжинами хвиль
EBGP	External BGP
EGP	exterior gateway protocol - протокол зовнішнього шлюзу
EIGRP	Enhanced Interior Gateway Routing Protocol
ELFEXT	еквівалентний коефіцієнт загасання перехресних наведень
FCS	контрольна послідовність кадрів
FDDI	розподілений оптичний інтерфейс даних
FDM	частотне мультиплексування
FEXT	коефіцієнт загасання перехресного наведення на дальньому від передавача кінці
FQDN	Fully Qualified Domain Name – повністю визначене доменне ім’я
FTP	фольгована вита пара
IBGP	Internal BGP
ICMP	Internet Control Message Protocol – міжмережний протокол управляючих повідомлень
IGMP	Internet Group Memebership Protocol
IGP	interior gateway protocol - протокол внутрішнього шлюзу
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol – міжмережний протокол
IPG	міжпакетна щілина
IS-IS	Intermediate System-to-intermediate System
LLC	керування логічним каналом або ланкою
MAC	керування доступом до середовища
MOSPF	Multicast OSPF
MTU	Maximum Transfer Unit - максимальна одиниця передачі даних
MUX	мультиплексор
MX	mail exchange - поштовий обмінник
NEXT	коефіцієнт загасання перехресного наведення на ближньому від

	передавача кінці
NLA	Next-Level Aggregation- агрегування наступного рівня
NRZ	код без повернення до нуля
NRZI	код без повернення до нуля з почерговою інверсією рівнів
NS	name server – сервер імен
NVR	номінальна швидкість поширення сигналу
OSI	взаємодія відкритих систем
OSPF	Open Shortest Path First
OUA	організаційно-унікальна адреса
OUI	організаційно-унікальний ідентифікатор
PCS	керування фізичним сигналом
PDH	плезіохронна цифрова ієрархія
PIM	Protocol-Independent Multicast
PIM-DM	PIM Dense Mode - щільний режим PIM
PIM-SM	PIM Sparse Mode - розріджений режим PIM
PMA	модуль доступу до середовища
PMD	інтерфейс, що залежить від середовища
PTR	Pointer - вказівник
QoS	якість обслуговування
RARP	Address Resolution Protocol – протокол зворотного перетворення адрес
RIP	Routing Information Protocol
RNR	приймач не готовий
RP	Rendezvous Point – точка рандеву
RPF	Reverse Path Forwarding - пересилка по зворотному маршруту
RR	приймач готовий
RTP	Reliable Transport Protocol - транспортний протокол з достовірною передачею

RTS	запит передачі
RZ	код з поверненням до нуля
SA	адреса відправника
SAP	точка доступу до послуги
SDH	синхронна цифрова ієрархія
SLA	Site-Level Aggregation - агрегування місцевого рівня
SM	одномодовий оптичний кабель
SNAP	протокол доступу до підмереж
SOA	Start of Authority – початок авторизації (початковий запис зони)
SPF	Shortest Path First
SPT	shortest path tree
SSAP	точка доступу до послуги відправника
STP	захищена вита пара
TCP	Transmission Control Protocol – протокол управління передачею
TDM	часове мультиплексування
TDMA	множинний доступ з часовим розділенням
TLA	Top-Level Aggregation - агрегування верхнього рівня
TTL	time to live – час життя
ToS	type of service – тип сервісу
UAA	унікально-керована адреса
UDP	User Datagram Protocol – протокол датаграм користувача
UTP	незахищена вита пара
WDM	мультиплексування за довжинами хвиль
АКД(DCE)	апаратура каналу даних
АМ	амплітудна модуляція
ВДСЗ	база даних стану зв'язків
ВОК	волоконно-оптичний кабель

ВП (TP)	вита пара
ГНН	година найбільшого навантаження
ЕОТ	код кінця передачі
ІБД	інтерфейсний блоків даних
ІКМ	імпульсно-кодова модуляція
ІОМ	інформаційно-обчислювальна мережа
КІП	кільцевий інтерфейсний пристрій
КК	коаксіальний кабель
КТМЗК	комутована телефонна мережа загального користування
КУД(DTE)	кінцеве устаткування даних
МДКН/ВК	множинний доступ з контролем несучої і виявленням колізії
ММ	багатомодовий оптичний кабель
ПБД	протокольний блок даних
ПКІ	протокольна керуюча інформація
СБД	сервісний блок даних
СКС	структурована кабельна система
ТК	точка концентрації
ФМ	фазова модуляція
ЦВ	центральний вузол
ЧМ	частотна модуляція