Навчально-методична література

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

Кафедра комп'ютерно-
інтегрованих технологій

# ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

## НАВЧАЛЬНИЙ ПОСІБНИК

для студентів спеціальності 151

«Автоматизація та комп'ютерно-інтегровані технології»

Тернопіль
2017

УДК 621.397
Т31

Укладачі:
*Микитишин А.Г.*, канд. техн. наук, доцент,
*Митник М.М.*, канд. техн. наук, доцент,
*Стухляк П.Д.,* докт. техн. наук, професор.

Рецензенти:
*Лупенко С.А.,* докт. техн. наук, професор.

Методичні вказівки розглянуто й затверджено на засіданні
методичного семінару кафедри комп'ютерно інтегрованих технологій
Тернопільського національного технічного університету імені Івана Пулюя
протокол № 11 від 20 червня 2017 р.

Схвалено та рекомендовано до друку науково-методичною комісією
факультету прикладних інформаційних технологій та електроінженерії
Тернопільського національного технічного університету імені Івана Пулюя
протокол № 11 від 23 червня 2017 р.

Телекомунікаційні системи та мережі : навчальний посібник для
Т31 студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані
технології» / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. –
Тернопіль : Тернопільський національний технічний університет імені
Івана Пулюя, 2017 – 384 с.

УДК 621.397

Відповідальний за випуск: *А.Г. Микитишин, канд. техн. наук, доцент.*

# ЗМІСТ

# 1. Архітектура телекомунікаційних систем та мереж

## 1.1. Історія розвитку телекомунікаційних систем та мереж

Рівень інформатизації будь-якої країни, ступінь її залучення до глобального інформаційного суспільства (ГІС) визначається передусім розвитком інфокомунікацій. Основу інфокомунікацій формують інформаційні мережі, які, у свою чергу, базуються на телекомунікаційних мережах. Це найскладніші й найбільш інтелектуально насичені системи.

На шляху еволюційного розвитку телекомунікаційних систем та мереж прийнято виокремлювати три етапи: аналоговий, цифровий та етап телекомунікаційно-комп'ютерної інтеграції.

Перший етап характеризує епоху аналогової телефонії. Зусиллями багатьох поколінь науковців і виробничників було створено світову мережу телефонного зв'язку, де середовищем передавання переважно були мідні кабелі. Багатоканальні системи передавання будували за принципом частотного розподілу телефонних каналів. Розподіл інформації здійснювався за принципом комутації каналів із використанням електромеханічних (декадно-крокових, координатних) або в кращому випадку квазіелектронних автоматичних телефонних станцій. В Україні до 1991 року також існувала аналогова мережа зв'язку, яка в основному задовольняла потреби населення, народного господарства, громадських інститутів у послугах електричного зв'язку.

Зародження етапу цифрового зв'язку розпочато з моменту формулювання та доведення теореми Котельникова (1933 рік), яка оголосила принцип дискретизації аналогового сигналу та розробки основ теорії потенційної завадостійкості (1946 рік). Цифрове кодування дискретних відліків амплітуд аналогового сигналу та подальше передавання їх каналами зв'язку дали змогу реалізувати принципово інший – цифровий спосіб передавання сигналів.

На початковому етапі теоретичні та експериментальні дослідження в галузі цифрового зв'язку проводилися без будь-якого впровадження, тому що практична реалізація незмінно наштовхувалася на величезні габарити, високу вартість та низьку надійність апаратури цифрового зв'язку. Однак наукові результати були вражаючими: засновано потужну теорію цифрового зв'язку. І коли досягнення мікро-, нано- та оптоелектроніки надали умови для створення апаратури цифрового зв'язку, яка за розмірами стала набагато мініатюрнішою, ніж апаратура аналогового зв'язку, до того ж більш надійною та дешевою, розпочався етап її бурхливого впровадження. Це було яскравим прикладом того,

як наука значніше випередила практику. Досягнення в цих сферах і сьогодні залишаються дуже актуальними та необхідними.

Із появою нових телекомунікаційних технологій, орієнтованих на пакетний спосіб передавання інформації, використання різних середовищ передавання (оптичне волокно, радіочастотний ресурс) та забезпечення мобільності зв'язку, виникла можливість суттєво підвищити продуктивність, ефективність та якість обслуговування телекомунікаційних мереж, а також розширити діапазон послуг, які ними надаються.

Етап телекомунікаційно-комп'ютерної інтеграції ознаменувався успіхами як у галузі електроніки, так і комп'ютерно-інтегрованих технологій. Створення високопродуктивних, малогабаритних і відносно недорогих комп'ютерів, інтеграція їх із телекомунікаціями у якості термінальних і комунікаційних пристроїв, а також досягнення в галузі інформаційних технологій стали підґрунтям створення інформаційних мереж. Це дало змогу накопичувати в електронному вигляді, зберігати й обробляти величезні ресурси інформації та надавати її користувачам за їх запитами у зручний для них час. Бурхливий розвиток і глобалізація інформаційних мереж дали людству Інтернет, без якого ми сьогодні не можемо уявити свого існування.

## 1.2. Основні поняття і визначення

### 1.2.1. Телекомунікаційна мережа

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

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

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

Таким чином, **телекомунікаційна мережа** (Telecommunication Network, TN) – це системоутворююча сукупність засобів телекомунікацій, що надає територіальновіддаленим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (електричними, оптичними або радіо).

Об’єктами при цьому можуть виступати як термінальні пристрої користувачів та кінцеві системи мережі, так і окремі мережі.

Кінцем (інтерфейсною точкою) телекомунікаційної мережі є або телекомунікаційний роз’єм, до якого під’єднано пристрій користувача (мережевий інтерфейс), або кінцеве мережеве обладнання, яке забезпечує з’єднання мереж (міжмережевий інтерфейс) (рис. 1.1).

У англомовній науковій літературі, акцентуючи саме на цьому аспекті, телекомунікаційну мережу називають **Carrier Network** (мережа-переносник).

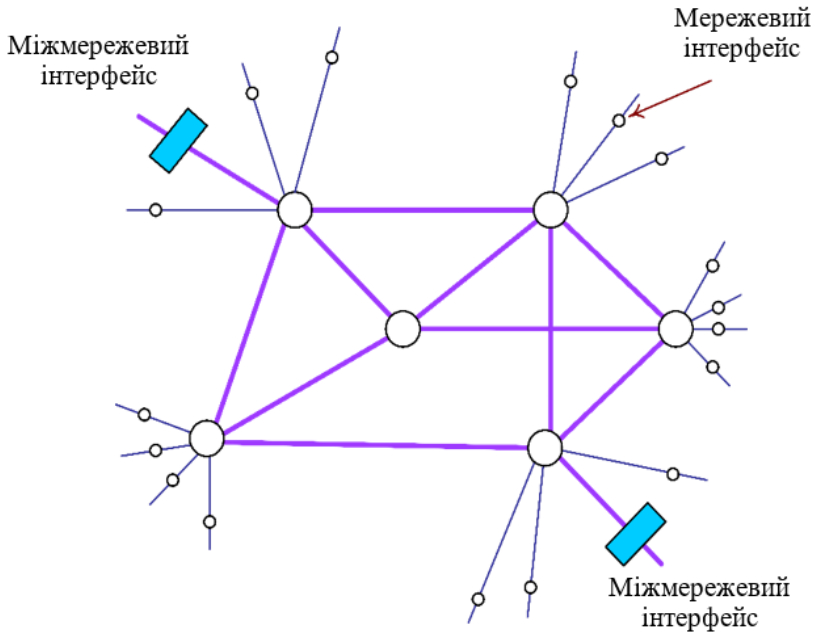



Рис. 1.1. Телекомунікаційна мережа

**Транспортування** (Transfer) інформації в мережевій термінології означає ***перенесення інформації***, перетвореної в сигнал з кінця в кінець, тобто від джерела до одержувача. Його слід відрізняти від терміну **«передача»** (Transmission), під яким розуміється процес ***поширення сигналу*** у фізичному середовищі між двома суміжними пунктами мережі.

Транспортуючи інформацію, необхідно контролювати такі важливі мережеві функції, як якість обслуговування з кінця в кінець, керування потоками з метою запобігання перевантажень у мережі та ін.

Телекомунікаційні мережі можна класифікувати за типом комутації (каналів чи пакетів), режимом перенесення інформації (синхронні, асинхронні) та технологічними характеристиками (середовищем передавання, заданою шириною смуги пропускання, якістю передавання сигналів, швидкістю передавання та ін.).

### 1.2.2. Інформаційна мережа

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

Поняття «інформаційна мережа», на відміну від поняття «телекомунікаційна мережа», є більш містким та узагальненим й відображає різноманіття інформаційних процесів, які протікають в мережі. Ці процеси виникають у результаті взаємодії прикінцевих систем, що під'єднані до телекомунікаційної мережі.

Інформаційні процеси в мережі можна поділити на дві групи: прикладні процеси та процеси взаємодії.

**Прикладні процеси** (Application Processes) ініціюються кінцевими системами під час запуску програм користувача, які ще називаються застосуваннями (Applications).

**Процеси взаємодії** (Interworking Processes) – це процеси в мережі, які призначені для обслуговування прикладних процесів. Наприклад, визначення форматів подання інформації для передавання мережею, встановлення режимів передавання даних, визначення маршрутів просування інформації та ін. Прикладні процеси та процеси взаємодії підтримуються мережевими операційними системами.

Прикінцеві системи інформаційної мережі можуть бути класифіковані наступним чином:

- термінальні системи (Terminal System) – комп'ютери користувачів мережі;
- хостингові системи (Host System) – комп'ютери, на яких розміщені інформаційні та програмні ресурси мережі;
- сервери (Servers) – комп'ютери, на яких встановлено спеціальне програмне забезпечення, яке дозволяє надавати мережеві сервіси. Наприклад, керування доступом для користувачів до інформаційних ресурсів, реєстрація користувачів та контроль за їх правами доступу в мережу та ін. Серверний комп'ютер, залежно від можливості його операційної системи, може бути налаштований як для роботи в режимі хоста (інформаційний сервер), так і в режимі комунікаційного пристрою (наприклад, шлюзу);
- адміністративні системи (Management System) – комп'ютери, які забезпечують роботу додатків керування мережею та окремих її частин.

Оскільки прикінцевими системами інформаційної мережі є комп'ютери, то таку систему ще називають «комп'ютерною мережею». Телекомунікаційна мережа при цьому класифікується як «мережа передавання даних».

Інформаційну мережу доцільно характеризувати за складом ресурсів. Ресурси інформаційної мережі поділяють на інформаційні, ресурси обробки та зберігання даних, програмні та комунікаційні.

**Інформаційні ресурси** – це інформація та знання, накопичені в усіх галузях науки, культури й життєдіяльності суспільства, а також продукція індустрії розваг. Все це систематизується в мережевих банках даних, з якими взаємодіють користувачі мережі. Ці ресурси визначають споживчу цінність інформаційної мережі, тому їх необхідно не лише постійно створювати та поповнювати, але й вчасно архівувати та оновлювати. Користування мережею повинно забезпечувати можливість отримувати актуальну інформацію саме тоді, коли в ній виникає необхідність.

**Ресурси обробки та зберігання даних** – це продуктивність процесорів та обсяги пам'яті комп'ютерів, які працюють у мережі, а також час, протягом якого вони використовуються.

**Програмні ресурси** – мережеве програмне забезпечення (ПЗ): мережеві операційні системи, серверне ПЗ, ПЗ робочих станцій; прикладне ПЗ; інструментальні засоби: утиліти, аналізатори проходження трафіку, засоби мережевого контролю, а також програми додаткових функцій, основними серед яких є навігація (забезпечення пошуку інформації в мережі), обслуговування мережевих електронних поштових скриньок, організація телеконференцій, перетворення форматів переданих інформаційних повідомлень, криптозахист інформації (кодування й шифрування), автентифікація (зокрема, електронний підпис документів, що засвідчує їх справжність).

**Комунікаційні ресурси** – це ресурси, які беруть участь у транспортуванні й перерозподілі потоків інформації в мережі (іншими словами – ресурси телекомунікаційної мережі), основними серед яких є пропускні спроможності ліній зв'язку та обладнання проміжних вузлів, а також час їх використання під час взаємодії користувача з мережею. Вони класифікуються відповідно до типу використаного середовища передачі та телекомунікаційної технології.

Усі перераховані ресурси в інформаційній мережі можуть використовуватися одночасно кількома прикладними процесами, тобто розділятися в часі.

Ресурси інформаційної мережі та інформаційні технології сукупно дозволяють виконувати обробку інформації, забезпечувати ефективний пошук її у будь-якому місці мережі, а також дозволяють здійснювати її накопичення та зберігання. Усі зазначені дії пов'язані з наданням «інформаційних послуг».

Отже, під інформаційною мережею як фізичним об’єктом слід розуміти сукупність територіально розрізнених прикінцевих систем, об’єднаних телекомунікаційною мережею, за допомогою якої забезпечується взаємодія прикладних процесів, активізованих у прикінцевих системах, та їх колективний доступ до ресурсів мережі.

Уся інтелектуальна робота в інформаційній мережі виконується на периферії, тобто в прикінцевих системах мережі, а телекомунікаційна мережа, хоча й займає центральне положення, є лише з’єднувальним компонентом (рис. 1.2). Телекомунікаційна мережа у складі інформаційної мережі виконує функції транспортувальної системи.

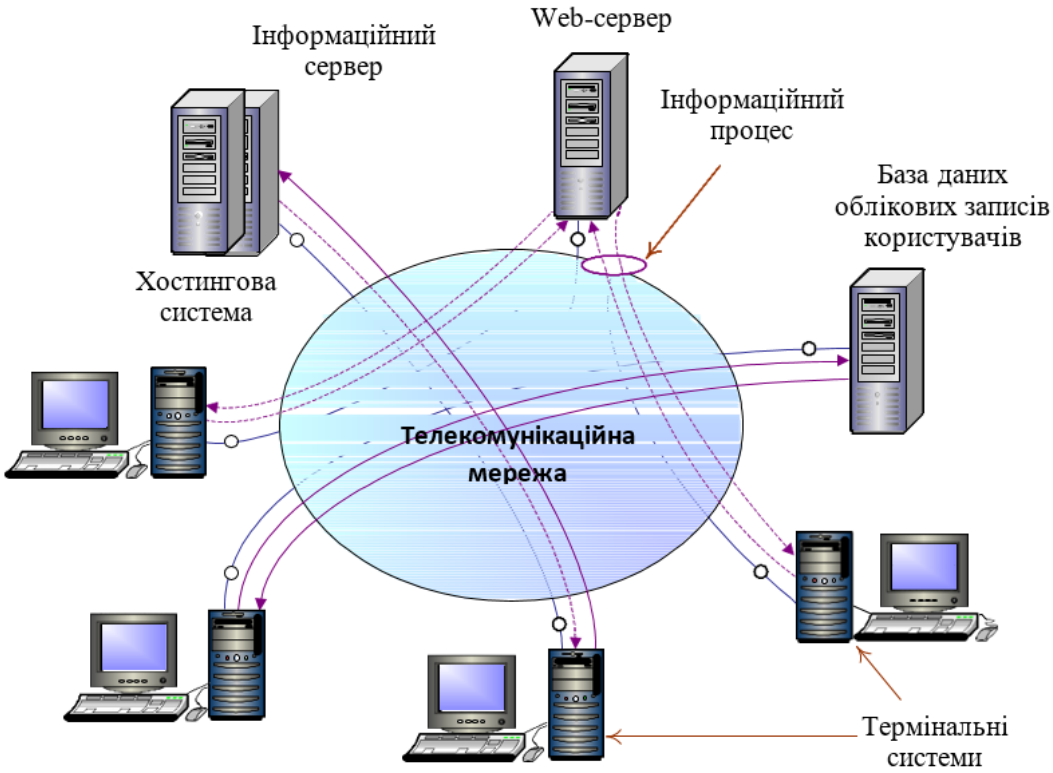



Рис. 1.2. Інформаційна мережа

Отже, поняття «інформаційна мережа» зосереджує увагу на інформаційних процесах, які виникають у мережі під час взаємодії прикінцевих систем через телекомунікаційну мережу. Опис цієї взаємодії демонструє всю складність організації зв’язку в мережі як у режимі «запит-відповідь», так і в реальному масштабі часу.

Основною вимогою, якій має відповідати інформаційна мережа, є забезпечення користувачів ефективним доступом до поділюваних ресурсів. Усі інші вимоги – пропускна спроможність, надійність, живучість – лише забезпечують якісне виконання цієї основної вимоги.

### 1.2.3. Конвергенція мереж, технологій та послуг

Розглянуті вище поняття телекомунікаційної та інформаційної мереж класифікують мережі зв'язку відповідно до категорій наданих послуг, основними серед яких є такі:

- телекомунікаційні або транспортні послуги;
- інформаційні послуги.

Ще в недалекому минулому проблема надання телекомунікаційних послуг вирішувалася шляхом створення окремих мереж електрозв'язку (телефонних, телеграфних, телевізійного мовлення, передачі даних).

Паралельно розвиваючись, комп'ютерні мережі як розподільчі системи обробки даних, забезпечили можливість автоматизованої обробки, накопичення й зберігання в мережі будь-якої інформації, що є продуктом інтелектуальної діяльності суспільства, й надання її на запит користувача в необхідній формі, тим самим розширюючи спектр інформаційних послуг.

У практиці експлуатування існуючих мереж зв'язку вже стало нормою передавати так званий «чужий» трафік. Наприклад, передача комп'ютерних даних засобами телефонних комунікацій, або передача голосового трафіку з використанням пакетного режиму переносу інформації. Внаслідок цього ускладнюється та видозмінюється звична у минулому для зв'язківців класифікація мереж зв'язку за типом переданих інформаційних повідомлень. Відбувається незворотне взаємопроникнення різних за походженням і принципами роботи мереж, таких, наприклад, як мережі передачі комп'ютерних даних і мережі передачі голосового (телефонного) трафіку. Це свідчить про те, що еволюція мереж зв'язку відбувається в напрямі **конвергенції** (convergence – зближення, сходження в одну точку).

Під конвергенцією в телекомунікаціях розуміють забезпечення практично однакових наборів послуг різними за технологічними можливостями мережами, або об'єднання кінцевих пристроїв, таких як телефон, персональний комп'ютер і TV-приймач у єдиний термінал.

Конвергенція передбачає створення конвергентних систем зв'язку на основі злиття мереж, які відрізняються цілим рядом ознак. Це перш за все мережі, які використовують різні телекомунікаційні технології, провідні та безпровідні мережі, стаціонарні та мобільні мережі, мережі доступу та транспортні мережі.

Конвергенція зумовлена прагненням мати однорідну інфраструктуру для тих чи інших послуг, навіть коли ці послуги підтримуються різними технічними рішеннями. Ці рішення можуть бути засновані на телекомунікаційних або інформаційних технологіях. Важливо відзначити, що конвергенція послуг

призводить також до значного збільшення можливостей однієї окремо взятої послуги, як це відбувається, наприклад, у мультимедійних комунікаціях. Закономірно, що конвергенція послуг завжди припускатиме певний рівень конвергенції в технічних системах, які забезпечують ці послуги.

В умовах, коли окремі сегменти телефонної мережі заміщуються мережами передачі даних, які забезпечують також і транспортування голосу, виник новий підхід у телекомунікаційних технологіях – пакетна передача голосу (Voice over Internet Protocol, VoIP).

У сфері конвергенції мереж найбільший інтерес викликає той факт, що Інтернет-послуги можна надавати через лінії доступу телефонної мережі. Отже, можна розглядати конвергенцію як взаємодію між телефонною мережею та Інтернетом на межі телефонної мережі. Забезпечення послугами телефонії між користувачами Інтернету та користувачами телефонної мережі є одним із основних напрямів конвергенції мереж.

Помітними також є фактори зворотного впливу. Необхідність передавання даних на значні відстані призвела до використання існуючих телекомунікацій як транспортного середовища при об’єднанні локальних обчислювальних мереж (LAN) та їх взаємодії з віддаленими комп’ютерами. Комп’ютер, у свою чергу, використовують не тільки як термінальний пристрій, але й як транзитний вузол телекомунікаційної мережі, який поєднує різні сегменти мережі, використовуючи процедури маршрутизації.

Фахівці з комп’ютерних систем дійшли висновку про доцільність використання в LAN телекомунікаційної технології асинхронного режиму перенесення (ATM), що забезпечує передачу різнотипного трафіку необхідної якості. Спеціалісти мають намір використовувати технології синхронної цифрової ієрархії (SDH) для пришвидшення передачі інформації в мережах передачі даних, а зв’язківці на основі таких технологій створюють територіальні мережі, які поєднують локальні мережі підприємств і віддалені «домашні офіси».

Розвиток і зближення технологій різних галузей призвели до появи абсолютно нового класу виробів ІА (Information Appliances). Цей клас охоплює все: починаючи від телевізорів, телефонів з доступом до Web-сервісів до наручних годинників, фотоапаратів, тощо. По суті, ІА визначають декілька нових видів обробки інформації. Усі вони є апаратними засобами з оперативним доступом до мереж.

У цілому еволюція мереж у бік мультисервісної платформи фактично означає необмежені можливості розширення спектру споживчих послуг, особливо завдяки мережевим бізнес-додаткам, які активно розвиваються (наприклад, електронна комерція, дистанційна система навчання, мережеві відеоконференції та ін.)

Підсумовуючи вищезазначене можна констатувати, що конвергенція забезпечила перехід до мереж наступного покоління (**NGN** – Next Generation Network), які мають на меті якісно змінити всі сфери життя й діяльності людини.

### 1.2.4. Інфокомунікаційна мережа

Процеси конвергенції, цифровізації та комп'ютеризації мереж зумовлені прагненням створити єдину мережу, здатну надавати телекомунікаційні та інформаційні послуги інтегровано, а також забезпечувати можливість необмеженого розширення спектру різних послуг. Підкреслюючи нерозривний зв'язок інформаційних і телекомунікаційних компонентів у формуванні та наданні послуг мережею, у технічній літературі часто використовують такі інтегруючі поняття, як «інфокомунікації», «інфокомунікаційна мережа».

Очевидно, що створення інфокомунікаційної мережі вимагає комплексного використання ресурсів мереж, а також істотно відмінних технічних рішень. І саме від складу й можливостей ресурсів такої багатофункціональної мережі залежить спектр послуг, які надаються.

Сукупність ресурсів мережі, задіяних у виробництві та наданні користувачам конкретної послуги або певного набору послуг, прийнято називати **платформою надання послуг.**

**Інфокомунікації** – це сукупність мережевих ресурсів, призначених для спільної участі у виробництві та наданні телекомунікаційних, інформаційних та інших послуг інформаційного співтовариства.

Таким чином, інфокомунікації забезпечують можливість не лише перенесення в просторі інформаційних повідомлень та взаємодію інформаційних систем, а й виробництво нових послуг та інформації.

**Інфокомунікаційна мережа** становить комплекс термінальних пристроїв користувачів, прикінцевих систем мережі та універсальної платформи виробництва та надання послуг, які відповідають різноманітним вимогам користувачів до їх типу та якості.

Інфокомунікаційну мережу як фізичний об’єкт зображено на рис. 1.3. Термінальними пристроями користувачів називають пристрої, призначені для роботи в мережі, якими є як прикінцеві пристрої телекомунікаційних служб: телефонні апарати (стаціонарні, мобільні, IP-телефонії), пристрої телематичних служб (факсимільні апарати, телетекси, відеотермінали тощо), так і багатофункціональні термінали на основі комп’ютерів.

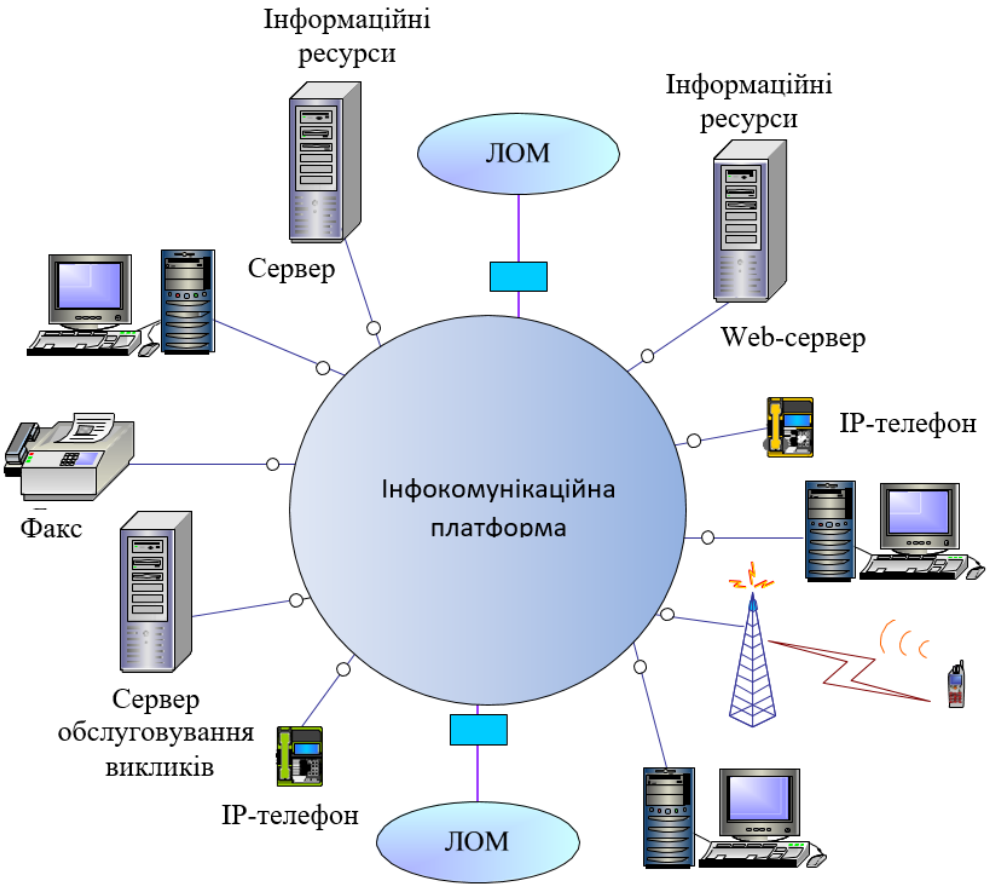



Рис. 1.3. Інфокомунікаційна мережа

Універсальну платформу надання широкого спектру послуг інфокомунікаційної мережі ще називають **«мультисервісною мережею»**. Її відмінною рисою є мережеве закінчення з універсальним відкритим інтерфейсом. Таким чином, інфокомунікаційна мережа дозволяє вирішувати найбільш актуальні завдання інформаційного співтовариства:

- надання користувачам можливості обміну інформаційними повідомленнями різного типу (голос, відео, дані);
- швидке та якісне отримання необхідної інформації з будь-якого віддаленого джерела в мережі;

- автоматизація процесів обробки, накопичення, зберігання великих обсягів інформації в мережі і, зрештою, самого процесу виробництва інформації.

## 1.3. Загальні принципи організації телекомунікаційних мереж

### 1.3.1. Мережі операторів зв'язку

Сьогодні мережі операторів зв'язку є рушійною силою і місцем прикладання практично всіх нових транспортних технологій телекомунікаційних мереж. Корпоративні мережі, як правило, вже не будуються на основі власної інфраструктури глобальних зв'язків – тепер для об'єднання локальних мереж своїх територіально розосереджених підрозділів підприємства звертаються до транспортних послуг телекомунікаційних мереж операторів зв'язку.

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

Кінцевим продуктом діяльності оператора зв'язку є надання послуг з транспортування інформації його мережею. Ці послуги називаються телекомунікаційними послугами (Telecommunication Services) та надаються як кінцевим користувачам мережі, так і іншим мережевим операторам, забезпечуючи їх транзитною можливістю з передачі трафіку через свої мережі. У зв'язку з цим мережі операторів зв'язку прийнято називати телекомунікаційними мережами ("теле" в перекладі з давньогрецької означає "далеко").

До складу телекомунікаційних мереж операторів зв'язку можуть входити глобальні комп'ютерні мережі, телефонні стаціонарні мережі, телефонні мобільні мережі, телевізійні мережі. За допомогою цих мереж оператори зв'язку надають широкий спектр послуг як кінцевим користувачам, так і один одному. Оператори зв'язку відрізняються один від одного:

- набором наданих послуг;
- територією, в межах якої надаються послуги;
- типом клієнтів, на яких орієнтовані їхні послуги;
- наявною у володінні оператора інфраструктурою – лініями зв'язку, комутаційним обладнанням, інформаційними серверами і т. п.

Сучасні оператори зв’язку зазвичай надають послуги кількох типів – як правило, це послуги виділених каналів, телефонії і комп’ютерних мереж. Всі ці послуги можуть бути згруповані і ієрархічно впорядковані. На рис. 1.4 фрагментарно показано взаємозв’язок деяких найбільш популярних сучасних телекомунікаційних послуг.


Рис. 1.4. Взаємозв’язок послуг телекомунікаційної мережі

**Послуги надання каналів зв’язку в оренду** відносяться до самого нижнього рівня, так як користувачу доводиться при цьому самостійно виконувати додаткову роботу – будувати за допомогою наданих каналів власну мережеву інфраструктуру (встановлювати телефонні комутатори або комутатори і маршрутизатори комп’ютерних мереж). Зазвичай, до таких послуг звертаються інші оператори зв’язку (віртуальні оператори), у яких для побудови своєї мережі немає власних каналів зв’язку.

**Віртуальні оператори** (Virtual operators) – це компанії, які не мають власних мережевих ресурсів, займаються в основному маркетингової діяльністю й у вигляді пакетів популярних послуг на основі гнучкої тарифної сітки реалізують їх клієнтам під своєю торговою маркою. Реалізацію ж послуг виконує мережевий оператор, з яким віртуальний оператор вступає у договірні відносини з частковою участю в прибутку від продажу послуг.

Наступний, більш вищий рівень, складають дві великі групи послуг: послуги телефонії і послуги комп’ютерних мереж.

**Послуги телефонії** – це, перш за все, телефонний зв'язок абонентів. Однак з плином часу поряд з цією традиційною послугою оператори зв'язку стали пропонувати абонентам голосову пошту, довідкову службу, переадресацію викликів, блокування певних номерів, обмеження спаму і інші допоміжні сервіси.

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

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

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

**Послуги комп'ютерних мереж** стали пропонуватися набагато пізніше, ніж телефонні, однак зараз переважна більшість операторів зв'язку надають ці послуги. Вони поділяються на:

- ***інформаційні*** – веб-сервіс, електронна пошта, соціальні мережі та ін.;
- ***транспортні*** – доступ в Інтернет, створення віртуальних приватних мереж.

Верхній рівень сьогодні займають **комбіновані послуги**, реалізація яких вимагає спільного використання комп'ютерних і телефонних мереж.

Оператори зв'язку застосовують різні транспортні технології, наприклад IP, Ethernet, OTN, SDH, DWDM, - ці технології працюють на різних рівнях стеку протоколів мережі, мають різні властивості і можуть працювати в різних поєднаннях. Оператор зв'язку використовує ці технології як для створення своїх мереж, так і для надання послуг своїм клієнтам. Співвідношення понять технологія і послуга можна пояснити наступними твердженнями:

- одна і та ж технологія може бути використана для надання різних послуг: наприклад, технологія IP може використовуватись як для доступу в Інтернет, так і для організації віртуальної приватної мережі;
- одна і та ж послуга може бути реалізована на основі різних технологій: наприклад, віртуальну приватну мережу можна побудувати на основі технології IP, Ethernet і MPLS;
- є такі послуги, які можна надавати на основі лише якоїсь однієї специфічної технології: наприклад, послугу виділеної хвилі можна надавати тільки на основі технології DWDM.

### 1.3.2. Інфраструктура мережі операторів зв'язку

На формування набору пропонованих оператором послуг чинить серйозний вплив матеріально-технічний фактор. Так, для надання послуг з оренди каналів оператор повинен мати в своєму розпорядженні первинну мережу SDH/OTN/DWDM, а для надання послуг віртуальних приватних мереж – маршрутизатори з функціональністю MPLS або комутатори Carrier Ethernet.

Типова мережа оператора зв'язку має двошарову структуру, з нижнім рівнем первинної (транспортної) мережі, яка є фундаментом для двох накладених мереж – телефонної мережі та комп'ютерної глобальної мережі. Телефонна та глобальна комп'ютерна мережі найчастіше являють собою паралельні інфраструктури, не пов'язані або слабо пов'язані одна з одною. Недостатня інтеграція цих мереж пояснюється тим, що комбіновані послуги все ще не стали масовим продуктом операторів зв'язку.

У тих випадках, коли у оператора відсутня вся необхідна інфраструктура для надання деякої послуги, він може скористатися можливостями іншого оператора: необхідна послуга може бути сконструйована на базі інфраструктури партнера, а також власних елементів інфраструктури. Наприклад, оператор зв'язку може створити загальнодоступний веб-сайт електронної комерції, не маючи власної IP-мережі, з'єднаної з Інтернетом. Іншим типовим прикладом є оренда оператором фізичних каналів зв'язку для створення власної телефонної або комп'ютерної мережі, з тим щоб на її основі надавати послуги своїм клієнтам. Оператора, який надає послуги іншим операторам зв'язку, часто називають **оператором операторів** (Carrier of Carriers).

### 1.3.3. Взаємовідносини між операторами зв'язку

За ступенем покриття території, на якій надаються послуги, оператори діляться на локальних, регіональних, національних і транснаціональних.

**Локальний оператор** працює на території міста або сільського району. Традиційний локальний оператор володіє усією відповідною транспортною інфраструктурою: фізичними каналами між приміщеннями абонентів і вузлом зв'язку, автоматичними телефонними станціями (АТС) і каналами зв'язку між телефонними станціями. Сьогодні до традиційних локальних операторів добавились альтернативні оператори, які часто є постачальниками послуг нового типу, перш за все послуг Інтернету, але іноді конкурують з традиційними операторами і в секторі телефонії.

**Регіональні** та **національні оператори** надають послуги на великій території, володіючи відповідною транспортною інфраструктурою. Традиційні

оператори цього масштабу виконують транзитну передачу телефонного трафіку між телефонними станціями локальних операторів, маючи в своєму розпорядженні великі транзитні АТС, пов'язані високошвидкісними фізичними каналами зв'язку. Це – оператори операторів, їх клієнтами є, як правило, локальні оператори або великі підприємства, що мають відділення і філії в різних містах регіону або країни. Маючи в своєму розпорядженні розвинену транспортну інфраструктуру, такі оператори, зазвичай, надають послуги телекомунікації, передаючи транзитом великі обсяги інформації без будь-якої обробки.

**Транснаціональні оператори** надають послуги в декількох країнах. Вони мають власні магістральні мережі, що покривають іноді кілька континентів. Часто подібні оператори тісно співпрацюють з національними операторами, використовуючи мережі доступу для доставки інформації клієнтам.

Взаємозв'язки між операторами різного типу (а також їх мережами) ілюструє рис. 1.5. На рисунку показані клієнти двох типів – індивідуальні та корпоративні. Кожен клієнт, зазвичай, потребує послуг двох видів – телефонних і передачі даних. Індивідуальні клієнти мають в своїх будинках або квартирах, як правило, телефон і комп'ютер, а у корпоративних клієнтів є відповідні мережі – телефонна, яка підтримується офісним телефонним комутатором, і локальна мережа передачі даних, побудована на власних комутаторах.

Для під'єднання обладнання клієнтів оператори зв'язку організовують так звані **точки присутності** (Point Of Presents, POP) – будівлі або приміщення, в яких розміщується обладнання доступу, здатне підключити велику кількість каналів зв'язку, що йдуть від клієнтів. Іноді таку точку називають **центральним офісом** (Central Office, CO) – це традиційна назва для операторів телефонних мереж. До POP локальних операторів під'єднуються абоненти, а до POP операторів верхніх рівнів – оператори нижніх рівнів або великі корпоративні клієнти, яким необхідні високі швидкості доступу і велика територія покриття, що об'єднує їх віддалені офіси в різних містах і країнах.

Так як процес конвергенції поки ще не привів до появи єдиної мережі для всіх видів трафіку, то за кожним овалом, що представляє на цьому рисунку мережі операторів, стоять дві мережі – телефонна і комп'ютерна (але спираються на один і той же фундамент – первинну мережу).

Як видно з рисунку, в сучасному конкурентному телекомунікаційному світі немає суворої ієрархії операторів, взаємозв'язки між ними і їхніми мережами можуть бути досить складними і заплутаними. Наприклад, мережа локального оператора 5 має безпосередній зв'язок не лише з мережею регіонального оператора 3, як того вимагає ієрархія, а й безпосередній зв'язок з національним оператором 3 (можливо, цей оператор пропонує дешевші послуги з передачі міжнародного трафіку, ніж це робить регіональний оператор 3). Деякі

оператори можуть не мати власної транспортної інфраструктури (на малюнку це локальний оператор 1). Як це часто буває в таких випадках, локальний оператор 1 надає тільки додаткові інформаційні послуги, наприклад пропонує клієнтам локального оператора 2 відео по запиту або розробку і підтримку їх домашніх сторінок в Інтернеті. Своє обладнання (наприклад, відеосервер) такий оператор часто розміщує в POP іншого оператора, як це і показано в даному випадку.

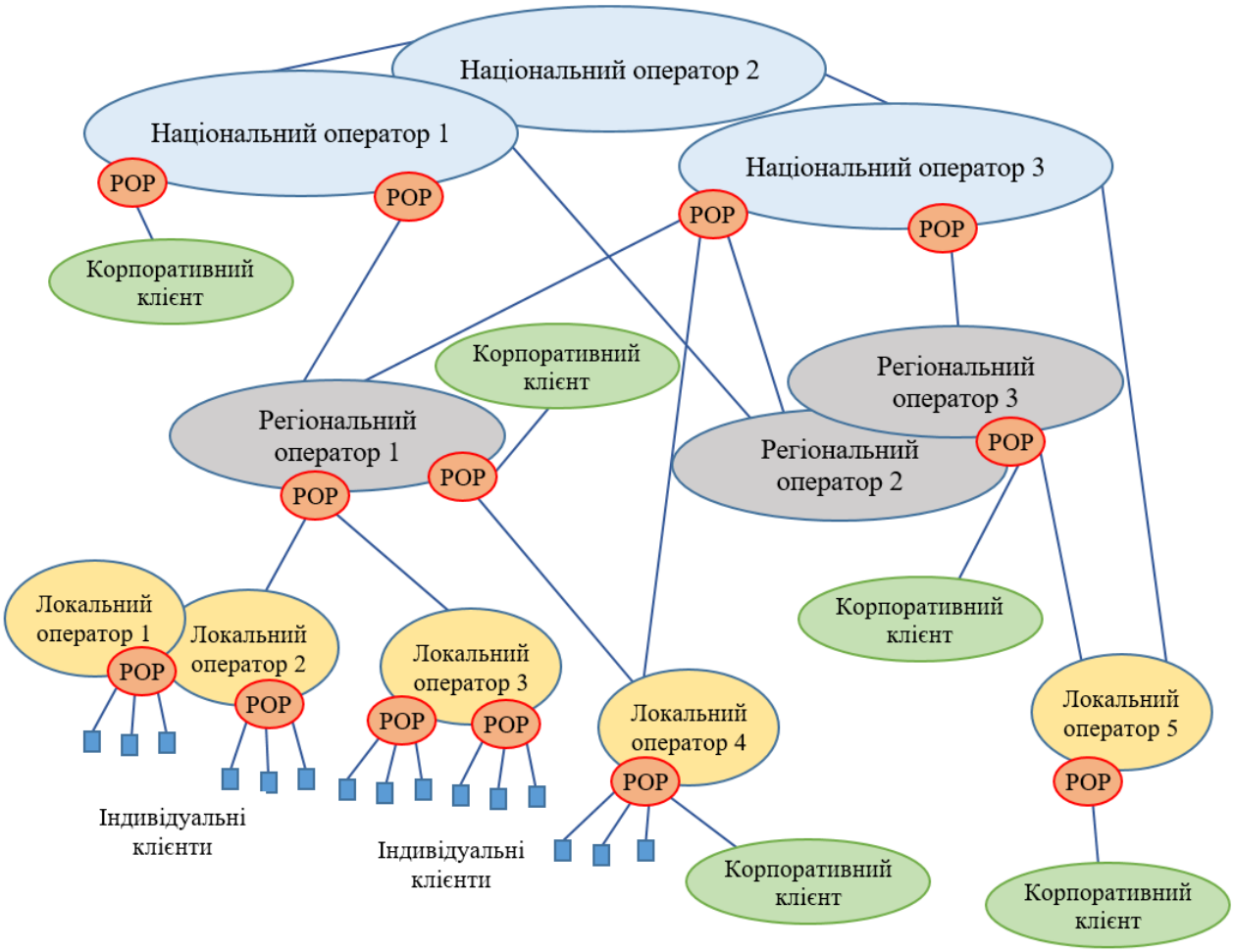



Рис. 1.5. Взаємозв’язок між операторами зв’язку різного рівня

### 1.3.4. Ієрархічна структура телекомунікаційної мережі

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

Мережева активність при транспортуванні інформації різними ділянками телекомунікаційної мережі визначається інтенсивністю створеного в них мережевого трафіку. Принцип розподілу інтенсивності трафіку на різних

ділянках телекомунікаційної мережі може бути основою декомпозиції транспортної функції. Така декомпозиція передбачає ієрархічну структуру телекомунікаційної мережі із виділенням трьох типів сегментів, які вирішують відносно самостійні функціональні підзавдання, а саме: транспортні мережі, мережі доступу і розподільчі мережі.

**Транспортна мережа** (Transport Network) – це сегмент телекомунікаційної мережі з високим ступенем концентрації трафіку, за допомогою якого здійснюється інформаційний обмін між сегментами з більш повільним трафіком і в якому транспортне середовище для передавання будь-якого типу інформації забезпечується використанням єдиних технологічних принципів і встановлених стандартів з надання ширини смуги пропускання (рис. 1.6).

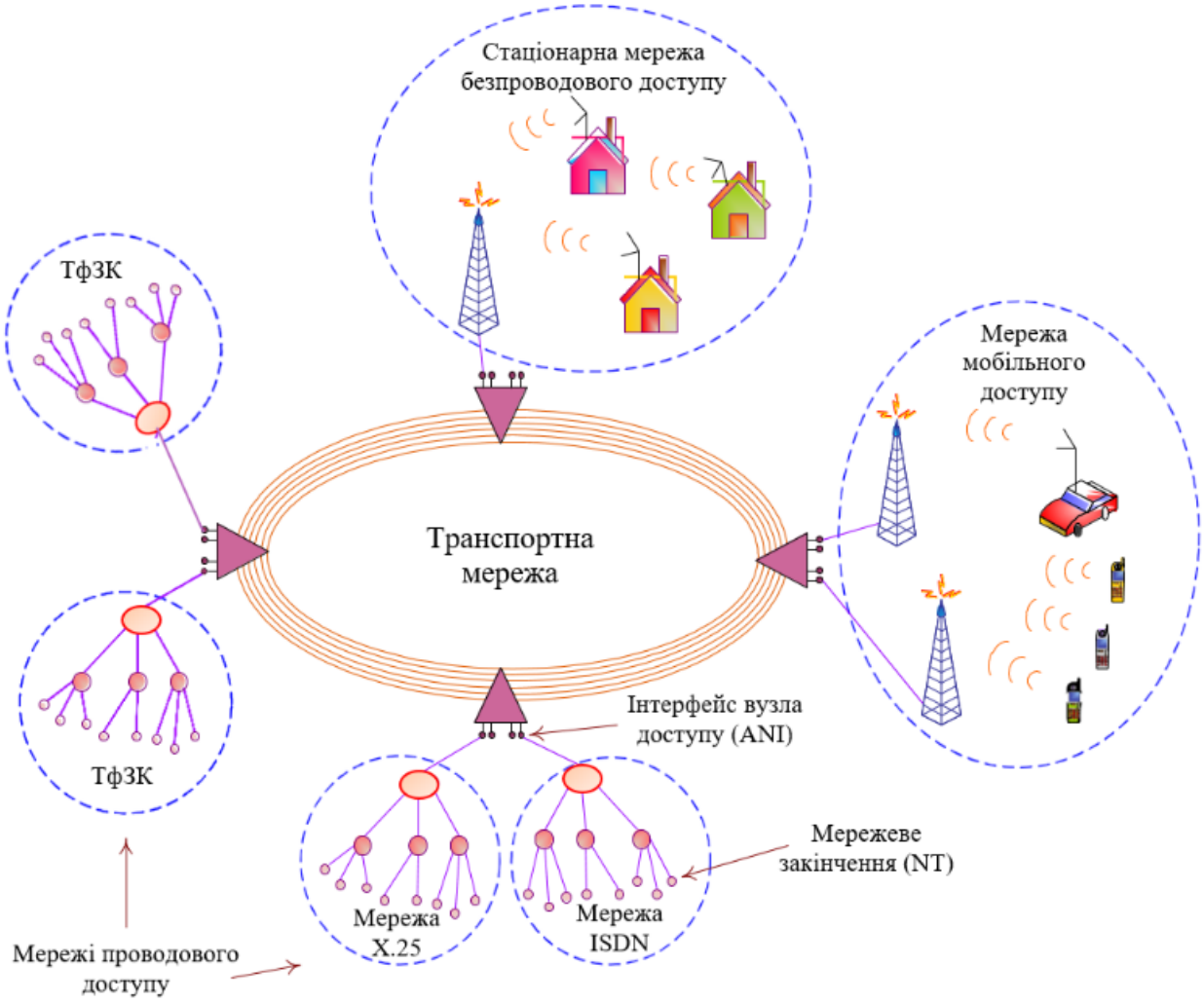



Рис. 1.6. Транспортна мережа та мережі доступу

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

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

Мережі доступу узагальнено поділяються на:

- мережі проводового доступу;
- стаціонарні мережі безпроводового доступу;
- мережі мобільного доступу.

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

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

Мережі доступу, у загальному випадку, мають багаторівневу архітектуру, що включає вузли рівнів доступу, розподілу і ядра (рис. 1.7.).

Пункти мережі підрозділяються на кінцеві і вузлові.

**Кінцеві пункти** (КП) (Endpoints) – це пункти, в яких розміщено термінальне обладнання користувачів і кінцеві системи мережі (сервери, на яких зосереджено інформаційні ресурси й додатки, у тому числі додатки системи керування мережею).

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

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

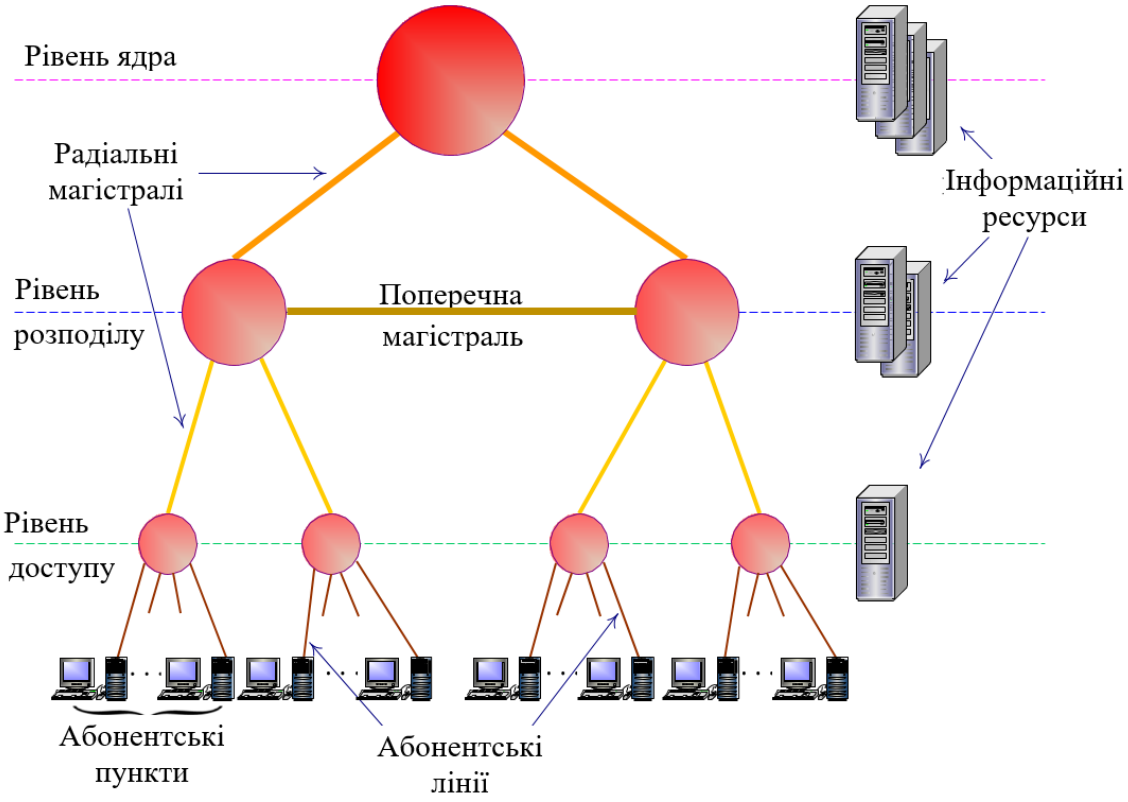



Рис. 1.7. Узагальнена схема організації структури мережі доступу

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

Статус вузлових пунктів визначається відповідно рівнем доступу, розподілу та ядра.

АП зазвичай під'єднуються до вузлових пунктів рівня доступу. Таким чином для них реалізується право доступу в мережу (до її ресурсів).

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

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

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

Лінії зв'язку в моделі організаційної структури також отримують відповідний статус.

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

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

Магістралі, що з'єднують вузлові пункти, які належать різним рівням ієрархії, називаються **радіальними магістралями**, а ті, що з'єднують вузлові пункти одного рівня – **поперечними магістралями.**

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

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

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

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

Опорні вузли мереж абонентського доступу формують рівень доступу.

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

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

**Розподільчою мережею** (Distribution Network) називають сегмент телекомунікаційної мережі, за допомогою якого концентрований потік, який

надходить з транспортної мережі, перерозподіляється та надходить до споживачів.

На практиці функції мережі доступу та розподільчої мережі часто поєднуються в одному сегменті. Класичним прикладом власне розподільчої мережі є тільки мережа оператора кабельного телебачення (рис. 1.8).

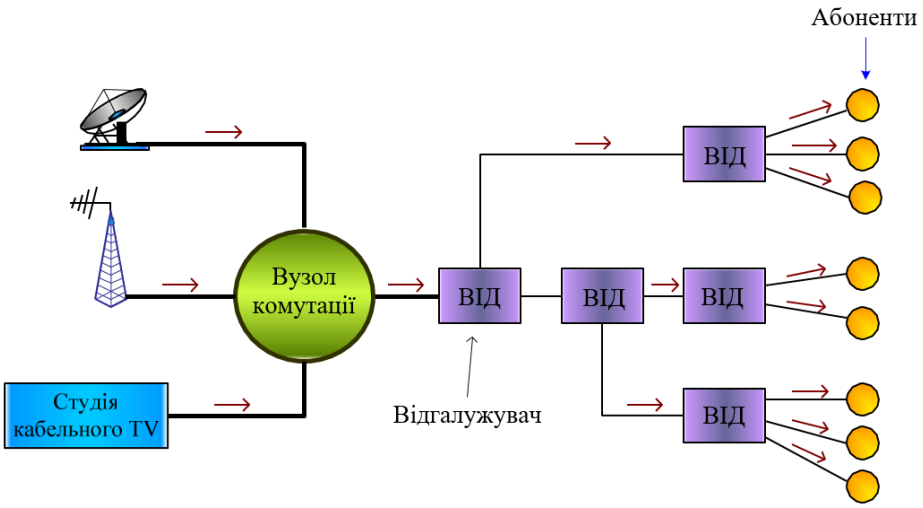



Рис. 1.8. Розподільча мережа

### 1.3.5. Узагальнені характеристики сегментів телекомунікаційної мережі

Узагальненими характеристиками будь-якого сегменту є розмір, масштаб і структура внутрішньосегментного трафіку.

**Розмір** сегмента визначається фізичною відстанню між найбільш віддаленими точками.

**Масштаб** сегмента визначається кількістю об'єднаних у ньому хостів.

**Внутрішньосегментний трафік** в загальному випадку складається з локального трафіку, вихідного, вхідного і транзитного відносно сегменту, який розглядається.

**Локальним** називається трафік, який формується в результаті інформаційного обміну хостів в межах сегменту. Розподіл локального трафіку в сегменті називають замиканням трафіку в сегменті.

**Вихідним** називається трафік, який генерується хостами сегмента і є спрямованим за межі даного сегмента до хостів інших сегментів.

**Вхідним** називається трафік, генерований хостами інших сегментів і призначений хостам даного сегмента.

**Транзитним** відносно сегмента називається трафік, який генерований хостами інших сегментів та адресований хостам, розташованим поза даним сегментом.

Відповідно до перерахованих складових внутрішньосегментного трафіку будемо розрізняти наступні види сегментів.

**Сегмент замикання локального трафіку** (СЗЛТ) – сегмент, у якому циркулює тільки локальний трафік. Це приклад закритої, ізольованої мережі. Існують плоскі і опуклі СЗЛТ.

**Плоский** СЗЛТ відповідає фізичному сегменту зі спільним комунікаційним середовищем, де рівень замикання локального трафіку припадає безпосередньо на фізичне середовище. Прикладом може бути невелика мережа робочої групи з топологією «спільна шина», яка побудована з використанням кабелю, або з топологією «зірка» з використанням комунікаційного обладнання фізичного рівня.

**Опуклий** СЗЛТ відповідає сегменту з комутованою топологією, де трафік замикається через логічний вузол (обладнання канального або мережевого рівня). Такий вузол виконує обов'язки опорного вузла. Наприклад, та ж мережа робочої групи, що має топологію «зірки», але з використанням комутатора в центральному пункті. Опорний вузол, через який хости обмінюються повідомленнями локального трафіку сегмента, визначає **рівень замикання трафіку** в опуклому сегменті.

**Сегмент формування вихідного трафіку** (СФВихТ) – сегмент, хости якого генерують трафік, спрямований за межі сегменту.

**Сегмент розподілення вхідного трафіку** (СРВхТ) – сегмент, у якому є лише трафік, які надходить від зовнішніх відносно нього, хостів.

У СФВихТ і СРВхТ не завершено процес перенесення інформації з кінця в кінець (від джерела до одержувача), і це визначає особливості топологій їх логічних зв'язків. Топологією логічних зв'язків таких сегментів є «дерево з корінням». У разі СФВихТ траєкторії руху трафіку спрямовано від хостів до вузла – «кореня дерева», в якому концентрується вихідний трафік, а в разі СРВхП – навпаки. Вузол, який є «корінням дерева», у зазначених сегментах виступає у ролі транзитного вузла.

Оскільки на практиці всі мережі побудовано як відкриті системи можна припустити, що в багатьох випадках один і той же сегмент виконує відразу декілька функцій з формування трафіку (рис. 1.9).

Структурований СЗЛТ відображено як сукупність вкладених один в одного сегментів з поєднанням функцій СЗЛТ, СФВихТ і СРВхТ (див. рис. 1.10).

У такому сегменті існує декілька рівнів замикання трафіку, кожен з яких визначається статусом відповідного опорного вузла. Прикладом може бути

мережа великого відділу, яка складається з рівня замикання локальних трафіків робочих груп і рівня замикання трафіку відділу.

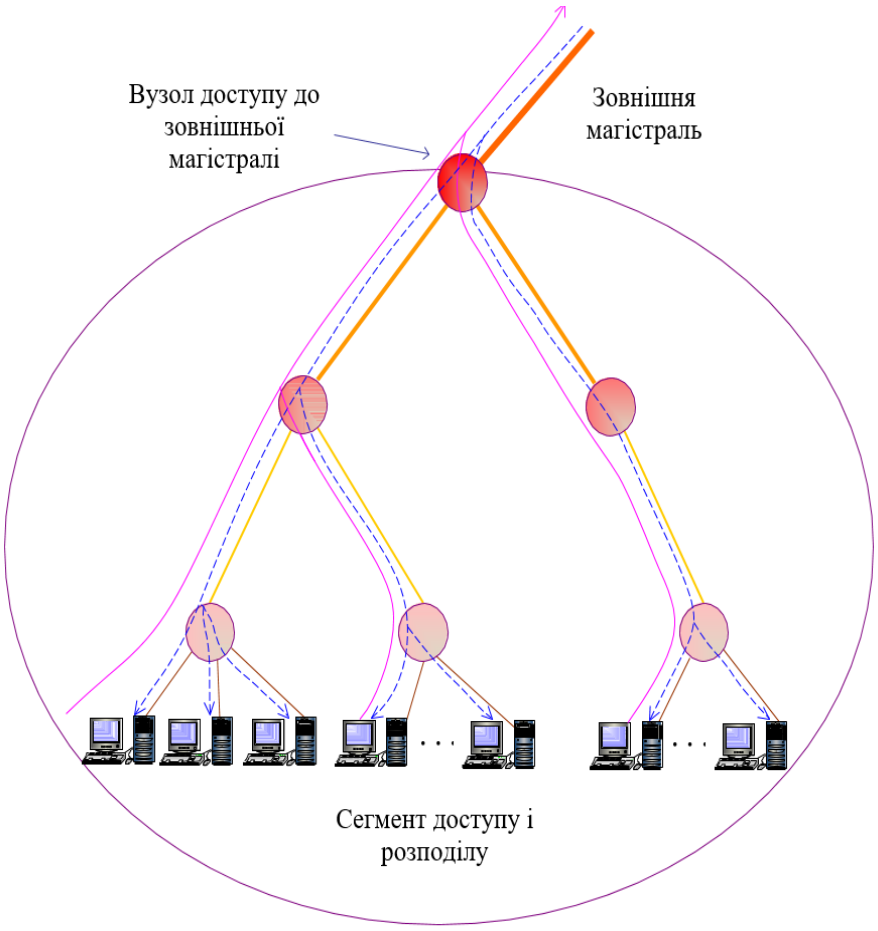



Рис. 1.9. Поєднання функцій СФВихТ і СРВхТ в одному сегменті

**Сегментом формування транзитного трафіку** (СФТТ) називається сегмент, у якому є концентрований трафік від хостів зовнішніх сегментів. СФТТ має особливий статус. Це магістральний сегмент. Він об'єднує опорні, опорно-транзитні або власне транзитні вузли і визначає рівень замикання трафіку, оскільки перерозподіляє трафік між усіма об'єднаними ним сегментами, що мають нижчий статус.

Відмінною особливістю такого сегменту є підвищення вимог до пропускної спроможності магістральних ліній і продуктивності вузлів.

У мережевій термінології такий сегмент називається магістральною мережею (Backbone Network).

## 1.4. Організація Інтернету

Інтернет – це мережа, яка не має єдиного центру управління і в той же час працює за єдиними правилами і надає всім своїм користувачам єдиний набір послуг. Інтернет – це «мережу мереж», але кожна вхідна в Інтернет мережа керується незалежним оператором – **провайдером послуг Інтернету**, або **сервіс-провайдером** (Internet Service Provider, ISP). Деякі центральні органи існують, але вони відповідають лише за єдину технічну політику: за узгоджений набір технічних стандартів, за централізоване призначення таких важливих для гігантської складовою мережі параметрів, як імена та адреси комп'ютерів і мереж, що входять в Інтернет, але не за щоденну підтримку мережі в працездатному стані. Такий високий ступінь децентралізації має свої переваги і недоліки.

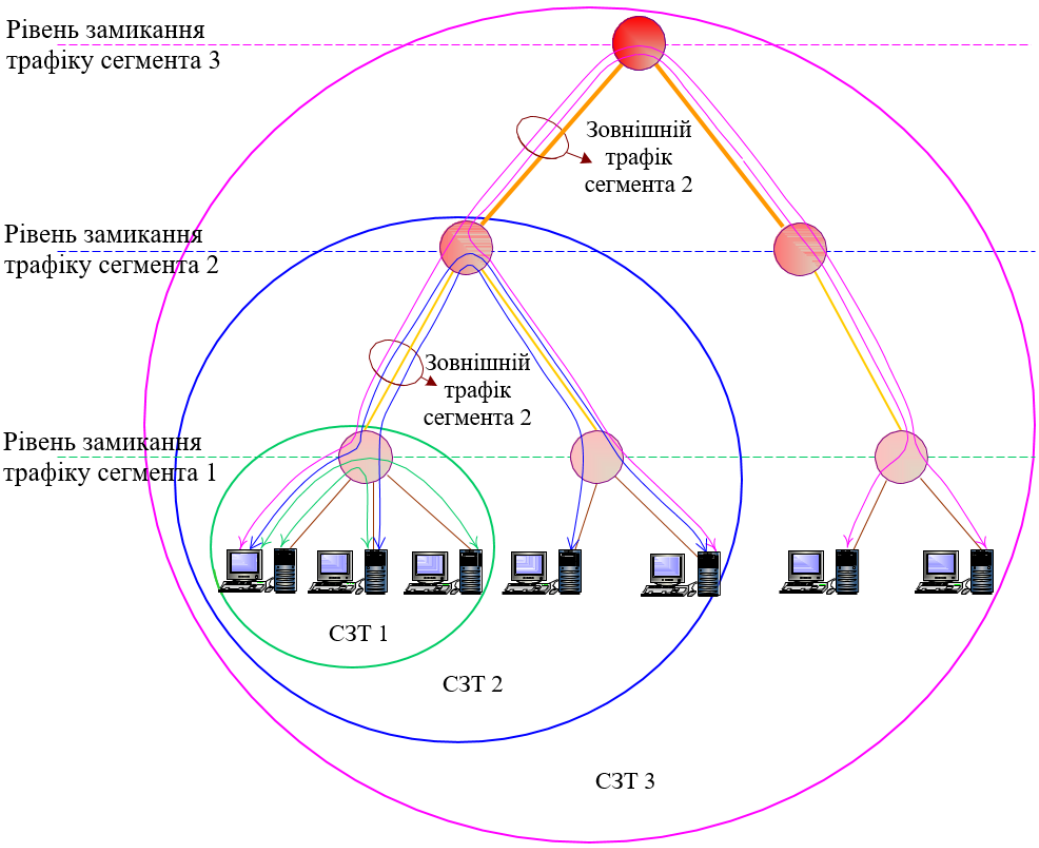



Рис. 1.10. Поєднання функцій СЗЛТ, СФВихТ і СРВхТ в одному сегменті

Переваги виявляються, наприклад, в легкості нарощування Інтернету. Так, новому постачальнику послуг досить укласти угоду принаймні з одним із існуючих провайдерів, після чого користувачі нового провайдера отримують

доступ до всіх ресурсів Інтернету. Негативні наслідки децентралізації полягають в складності модернізації технологій і послуг Інтернету. Будь-які докорінні зміни вимагають узгоджених зусиль всіх провайдерів послуг, в разі «одного власника» вони проходили б набагато легше. Інший недолік – не дуже висока надійність послуг Інтернету, так як ніхто з провайдерів не відповідає за кінцевий результат, наприклад, за доступ клієнта А до сайту В, якщо вони знаходяться в мережах різних постачальників.

Стрімке зростання числа користувачів Інтернету змінив ставлення корпоративних користувачів і операторів зв'язку до цієї мережі. Сьогодні Інтернет підтримується практично всіма традиційними операторами зв'язку. Крім того, до них приєдналася велика кількість нових операторів, що побудували свій бізнес виключно на послуги Інтернету (**інтернет-сервіс-провайдинг**).

Діяльність сервіс-провайдерів зосереджена на організації так званих сервісних вузлів (Service Nodes), за допомогою яких реалізується доступ користувачів до різних мережевих служб та інформаційних ресурсів як даного вузла, так і віддалених вузлів Інтернету. При цьому постачальники послуг (провайдери) також є споживачами телекомунікаційних послуг (послуг з транспортування інформації), які надаються мережевими операторами зв'язку.

Тому, загальна структура Інтернету, показана на рис. 1.11, багато в чому є відображенням загальної структури всесвітньої телекомунікаційної мережі, фрагмент якої зображений на рис. 1.5.

**Магістральні провайдери послуг** є аналогами транснаціональних операторів зв'язку. Вони володіють власними транспортними магістралями, які покривають великі регіони (країна, континент, вся земна куля). Прикладами магістральних провайдерів послуг є такі компанії, як Cable&Wireless, WorldCom, Global One, в Україні – ТОВ «Євротранстелеком», ТОВ «Дабл-Ю-Нет», ПАТ «Датагруп», ТОВ «АйТіСістемз».

**Регіональні провайдери послуг** надають послуги Інтернету в рамках певного регіону (область, штат, графство, округ – в залежності від прийнятого в тій чи іншій країні адміністративного поділу), а **локальні провайдери послуг** працюють, як правило, в межах одного міста.

Зв'язки між постачальниками послуг будуються на основі двосторонніх угод про взаємну передачі трафіку. Такі угоди називають **піринговими. Піринг** (peering – сусідство) – угода інтернет-провайдерів про обмін трафіком між своїми мережами, а також технічну взаємодію, що реалізує дану угоду: з'єднання мереж і обмін інформацією про мережеві маршрути по протоколу BGP.

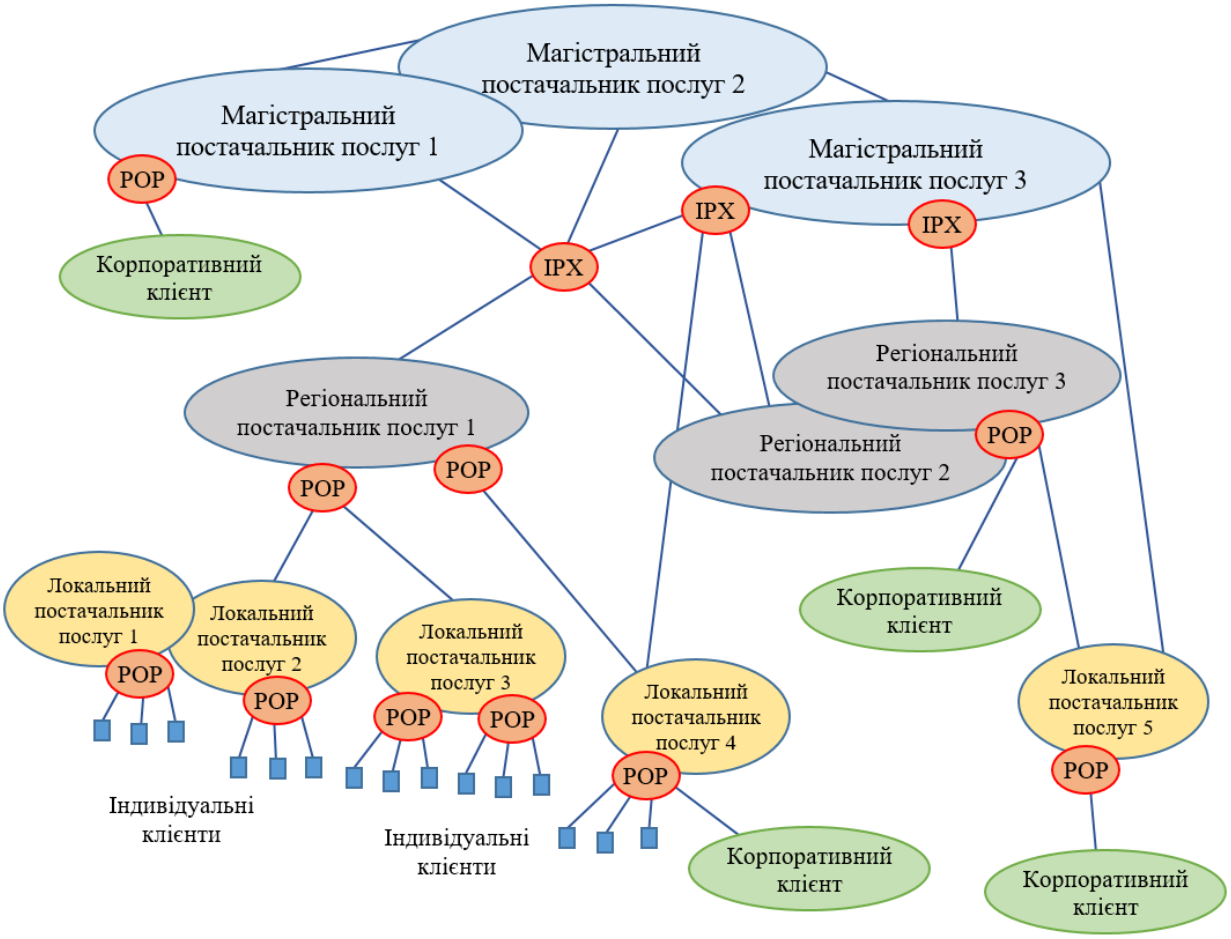



Рис. 1.11. Структура Інтернету

Магістральний оператор, зазвичай, має пірингові угоди з усіма іншими магістральними операторами (так як їх не багато), а регіональні оператори, як правило, укладають такі угоди з одним з магістральних операторів і з декількома іншими регіональними операторами.

Для того щоб провайдерам було простіше організовувати свої пірингові зв’язки, в Інтернеті існують спеціальні центри обміну трафіком, в яких з’єднуються мережі великої кількості провайдерів. Такі центри обміну називаються Internet eXchange Point (IXP), або Network Access Point (NAP).

Центр обміну трафіком є засобом реалізації пірингових зв’язків, для цього він надає постачальникам послуг приміщення і стійки для установки комутаційного обладнання. Всі фізичні і логічні з’єднання між своїм обладнанням провайдери послуг виконують самостійно. Це означає, що не всі мережі провайдерів, які користуються послугами того чи іншого центру обміну даними, автоматично обмінюються трафіком між собою, обмін відбувається між

мережами тільки в тому випадку, коли між провайдерами укладено пірингову угоду і вони його реалізували в даному центрі обміну.

В Інтернеті існує неофіційна градація провайдерів Інтернету за рівнями (tiers) в залежності від того, хто з них і кому платить за передачу транзитного трафіку Інтернету. Провайдери верхнього рівня (**Tier 1** – це, як правило, провайдери міжнародного і національного масштабу) можуть досягти будь-якої частини Інтернету без плати за транзитний трафік: у них у всіх є некомерційні пірингові угоди один з одним. Провайдери другого рівня (**Tier 2**) відносяться до змішаного типу: з одними провайдерами у них є некомерційні пірингові угоди, з іншими – договори про плату за транзит свого трафіку. І нарешті, провайдери третього рівня (**Tier 3**) зовсім не мають безкоштовних пірингових угод і платять іншим провайдерам за транзит свого трафіку.

## 1.5. Споживачі послуг

Усі клієнти – споживачі інфокомунікаційних послуг – можна розділити на два великі класи: масові індивідуальні клієнти і корпоративні клієнти.

У першому випадку місцем споживання послуг виступає квартира або приватний будинок, а клієнтами – мешканці, яким потрібні перш за все базові послуги – телефонний зв'язок, телебачення, радіо, доступ в Інтернет. Для масових індивідуальних клієнтів дуже важлива економічність послуги – низька місячна оплата, можливість використання стандартних термінальних пристроїв, таких як телефонні апарати, телевізійні приймачі, персональні комп'ютери, а також можливість задіяти існуючу кабельну систему між офісом оператора зв'язку і будинком клієнта. Присутня в багатьох місцевостях традиційна телефонна проводка – це серйозне обмеження для надання послуг доступу в Інтернет і нових телекомунікаційних послуг, так як вона не була розрахована на передачу даних, а підведення до кожного дому нового якісного кабелю, наприклад волоконно-оптичного, – справа дорога (хоча цей варіант стає все більш доступним). Тому для надання комп'ютерних послуг таким клієнтам розроблені специфічні технології доступу через існуючі в будинку закінчення телефонної мережі. У цьому випадку нові швидкісні цифрові технології доступу (DSL) використовують телефонну мережу, але тільки на відрізку між будинком клієнта і офісом оператора зв'язку, а далі дані передаються в обхід телефонної мережі по комп'ютерній мережі з комутацією пакетів. Існують також технології доступу, в яких для передачі даних використовується наявна в місті мережа кабельного телебачення.

Корпоративні клієнти – це підприємства і організації різного профілю. **Мережами підприємств** (Enterprise Networks), або **приватними мережами**

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

Відмінною особливістю приватних мереж є те, що всі ресурси мережі використовуються виключно співробітниками підприємства, яке є власником мережі. Крім того під терміном «приватна» мережа розуміють також закриту мережу, призначену для конфіденційного зв'язку. Дрібні підприємства (рис. 1.12) по набору необхідних послуг не надто відрізняються від масових клієнтів – це ті ж базові телефонія і телебачення, а також доступ до інформаційних ресурсів Інтернету.

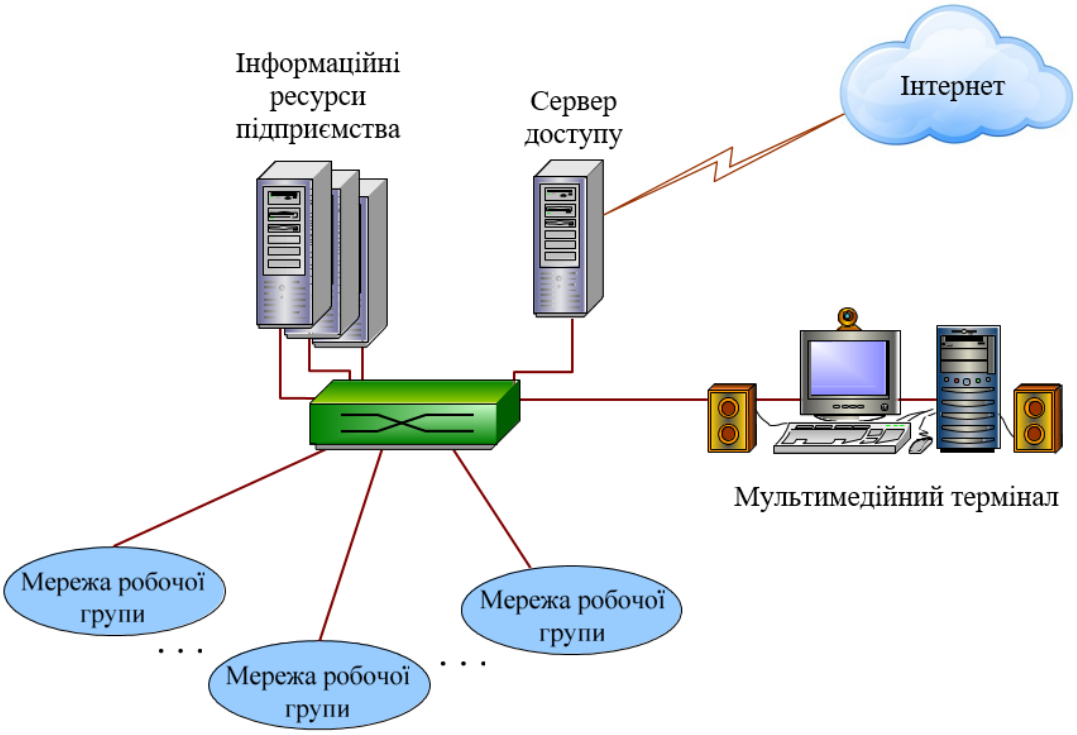



Рис. 1.12. Мережа відділу (невелике підприємства)

Великі підприємства (рис. 1.13), що складаються з декількох територіально розосереджених відділень і філій, а також мають співробітників, які часто працюють вдома, потребують розширені послуг. Перш за все, подібною послугою є така транспортна послуга, як віртуальна приватна мережа (Virtual Private Network, VPN), коли оператор зв'язку створює для підприємства ілюзію того, що все його відділення та філії з'єднані приватною мережею, тобто мережею, яка повністю належить підприємству-клієнту і повністю керується підприємством-клієнтом.

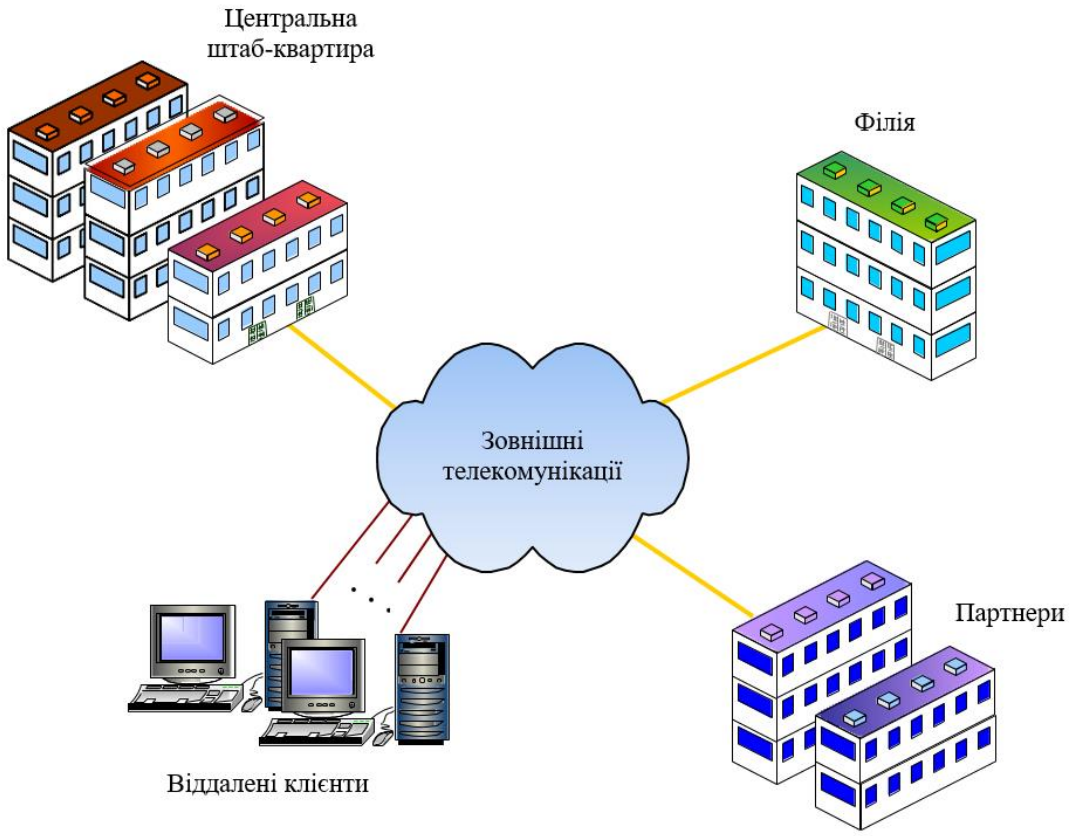



Рис. 1.13. Корпоративна мережа

Насправді ж, для створення цієї ілюзії використовується комп’ютерна мережа оператора, тобто загальнодоступна мережа, яка одночасно передає дані багатьох клієнтів.

Корпоративні користувачі все частіше отримують не тільки транспортні, а й інформаційні послуги операторів зв’язку, наприклад послуги хостингу, переносяться власні сервери, веб-сайти і бази даних на територію оператора, доручаючи останньому підтримувати їх роботу і забезпечувати швидкий доступ до них для співробітників підприємства і, можливо, інших користувачів мережі оператора. Поширені останнім часом хмарні сервіси посилили цю тенденцію, дозволяючи корпоративним користувачам (і індивідуальним теж) отримувати інформаційні послуги прозорим способом, не піклуючись про встановлення, конфігурації і супроводі серверів та програмного забезпечення.

# 2. Технології фізичного рівня. Мультиплексування та комутація

## 2.1. Характеристика ліній зв'язку

### 2.1.1. Класифікація ліній зв'язку

Фізичною основою будь-якої телекомунікаційної технології є лінії зв'язку та комунікаційне (мережеве) обладнання. **Лінія зв'язку** – це узагальнене поняття, яке, залежно від застосування певної телекомунікаційної технології, можна конкретизувати таким чином:

- **ланка** (Link) – це фізичний сегмент, який забезпечує передавання сигналів між суміжними вузлами мережі без використання проміжного комунікаційного обладнання мультиплексування й комутації;
- **канал** (Channel) – це частина пропускної здатності ланки, яка незалежно використовується під час комутації. Канали в ланці можуть бути утворені за допомогою мультиплексора або апаратури ущільнення (наприклад, ланка з 30 каналів, кожен з яких має пропускну здатність 64 Кбіт/с);
- **комутований канал** (Circuit) – це складений канал, який утворюється в сегменті з комутованою топологією з окремих проміжних ланок або каналів та комутаційного обладнання вузлів;
- **тракт передавання** (Highway) – це всі пристрої та споруди, які беруть участь в утворенні шляху проходження інформації з кінця в кінець. Тракт, як правило, утворюють засоби кросової комутації декількох каналів у транзитних вузлах мережі.

### 2.1.2. Фізичні середовища телекомунікаційних систем

Лінії зв'язку відрізняються фізичним середовищем, яке використовується для передавання інформації. В сучасних телекомунікаційних системах інформація передається за допомогою електричного струму або напруги, радіосигналів або світлових сигналів – всі ці фізичні процеси є коливаннями електромагнітного поля різної частоти.

**Провідні (повітряні) лінії** зв'язку являють собою проводи без будь-яких ізолюючих або екрануючих покриттів, що прокладені між стовпами і висять в

повітрі. Ще в недалекому минулому такі лінії зв'язку були основними для передачі телефонних і телеграфних сигналів.

Сьогодні провідні лінії зв'язку швидко витісняються кабельними. Швидкісні якості і завадозахищеність цих ліній залишають бажати багато кращого.

**Кабельні лінії** мають досить складну конструкцію. Кабель складається з провідників, вкладених в кілька шарів ізоляції: електричної, електромагнітної, механічної і, можливо, кліматичної. Крім того, кабель може бути оснащений роз'ємами, які дозволяють швидко виконувати з'єднання з різним обладнанням. У телекомунікаційних мережах застосовуються три основні типи кабелю: **кабелі на основі скручених пар мідних проводів** – неекранована скручена пара (Unshielded Twisted Pair, UTP) і екранована скручена пара (Shielded Twisted Pair, STP), **коаксіальні кабелі** з мідною жилою, **волоконно-оптичні кабелі**. Перші два типи кабелів називають також **мідними кабелями.**

**Радіоканали** наземного і супутникового зв'язку утворюються за допомогою передавача і приймача радіохвиль. Існує велика різноманіття типів радіоканалів, які відрізняються як частотним діапазоном, так і дальністю каналу. Діапазони широкотрансляційного радіо (довгих, середніх і коротких хвиль), відомі як **діапазони амплітудної модуляції** (Amplitude Modulation, AM), забезпечують далекий зв'язок, але при невисокій швидкості передачі даних. Більш швидкісними є канали, які використовують діапазони дуже високих частот (Very High Frequency, VHF), в яких застосовується **частотна модуляція** (Frequency Modulation, FM). Для передачі даних також використовуються діапазони ультрависоких частот (Ultra High Frequency, UHF), звані ще **діапазонами мікрохвиль** (понад 300 МГц). При такій частоті сигнали вже не відображаються іоносферою Землі і для стійкого зв'язку потрібна наявність прямої видимості між передавачем і приймачем. Тому зазначені частоти використовуються в супутникових або радіорелейних каналах або в таких локальних чи мобільних мережах, в яких ця умова виконується.

### 2.1.3. Апаратура ліній зв'язку телекомунікаційних систем

Лінії зв'язку складаються не лише з середовища передавання, але й апаратури. Апаратура, разом з середовищем передавання даних утворює **фізичне мережеве середовище**. Воно відображається моделлю, яка називається фізичною структурою мережі.

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

**Активне мережеве обладнання охоплює** весь парк кінцевого й комунікаційного устаткування мережі, функціонування якого забезпечується за рахунок споживання електроенергії від зовнішніх джерел живлення.

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

У загальному, **апаратура** (Equipment) – це активне обладнання, в якому функції можуть бути реалізовані як у вигляді апаратного забезпечення, так і у вигляді програмного забезпечення (рис. 2.1). Апаратура може мати модульну конструкцію, тобто складатися з певної кількості знімних плат.

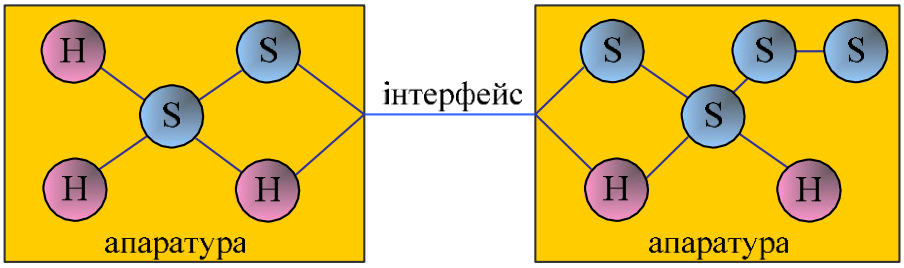



Рис. 2.1. Схема моделі апаратурної реалізації:
H − апаратне забезпечення (Hard ware)
S − програмне забезпечення (Soft ware)

Елементами моделі апаратурної реалізації є такі:

- **апаратне забезпечення** (Hard ware)– обладнання, в якому одна або декілька функцій реалізовано фізично;
- **програмне забезпечення** (Soft ware) – один або декілька програмних модулів, які представляють собою реалізацію одного або декількох об'єктів;
- **фізичний інтерфейс** (Phisical interface) – фізичне середовище (проводи) для передачі сигналів між різної апаратурою.

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

Усі пристрої в мережі, які функціонують як відправники та приймачі даних на фізичному рівні моделі OSI, визначаються як **кінцева апаратура даних,** або

**DTE-пристрої** (Data Terminal Equipment). Разом із функцією формування даних, у реалізації якої в основному бере участь програмне забезпечення, в DTE-пристроях здійснюється також функція керування потоком даних для узгодження роботи відправника та приймача. Ця функція, як правило, виконується апаратно. Відмінною особливістю обладнання класу DTE є те, що воно не належить до складу устаткування ліній зв'язку.

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

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

Поділ обладнання на DCE і DTE є досить умовним. Наприклад, мережевий адаптер можна вважати як складовою комп'ютера (DTE), так і частиною каналу зв'язку (DCE).

Для під'єднання DTE-пристроїв до DCE-пристроїв існує кілька стандартних інтерфейсів. Працюють ці пристрої на коротких відстанях один від одного, як правило, кілька метрів.

**Проміжна апаратура** зазвичай використовується на лініях зв'язку великої протяжності. Вона вирішує два основні завдання:

- поліпшення якості сигналу;
- створення постійного комутованого каналу зв'язку між двома абонентами мережі.

У локальних мережах проміжна апаратура може зовсім не використовуватися, якщо протяжність фізичної середовища – кабелів або радіоефіру – дозволяє одному мережному адаптеру приймати сигнали безпосередньо від іншого мережевого адаптера без додаткового посилення. В іншому випадку застосовується проміжна апаратура, роль якої виконують пристрої типу **повторювачів** і **концентраторів.**

У глобальних мережах необхідно забезпечити якісну передачу сигналів на відстані в сотні і тисячі кілометрів. Тому, для побудови територіальної мережі використовують **підсилювачі** (підвищують потужність сигналів) і **регенератори** (поряд з підвищенням потужності відновлюють форму

імпульсних сигналів, спотворених при передачі на велику відстань), які встановлюють через певні відстані на лінії зв'язку.

У первинних (транспортних) мережах, крім згаданого обладнання, що забезпечує якісну передачу сигналів, необхідна також проміжна комутаційна апаратура – **мультиплексори, демультиплексори, комутатори** і **маршрутизатори**. Ця апаратура створює між двома абонентами мережі постійний комутований (складовий) канал.

Залежно від типу проміжної апаратури всі лінії зв'язку поділяються на аналогові і цифрові. В **аналогових лініях** проміжна апаратура призначена для посилення аналогових сигналів, тобто сигналів, які мають безперервний спектр значень. Такі лінії зв'язку традиційно застосовувалися в телефонних мережах з метою зв'язку телефонних комутаторів між собою.

У **цифрових лініях** зв'язку сигнали мають кінцеве число станів. Як правило, елементарний сигнал, тобто сигнал, який передається за один такт роботи передаючої апаратури, має 2, 3 або 4 стани, які в лініях зв'язку відтворюються імпульсами або потенціалами прямокутної форми. За допомогою таких сигналів передаються як комп'ютерні дані, так і оцифровані голос і зображення (саме завдяки однаковому способу подання інформації сучасними комп'ютерними, телефонними і телевізійними мережами стало можливим поява загальних для всіх первинних мереж). У цифрових лініях зв'язку використовується спеціальна проміжна апаратура – регенератори, які покращують форму імпульсів і відновлюють період їх проходження.

**Пасивне обладнання** використовується для побудови телекомунікаційних кабельних систем мережі. Кабельна система – це складний технічний об'єкт, який будується відповідно до жорстких вимог загальноприйнятих стандартів. До нього належать лінійно-кабельні споруди, кабелі ліній зв'язку, регенераційне обладнання, тощо.

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

### 2.1.4. Спектральний аналіз сигналів на лініях зв'язку

Важливим параметром ліній зв'язку є спектральний аналіз сигналів, що передаються по цій лінії. З теорії гармонійного аналізу відомо, що будь-який періодичний процес можна представити у вигляді суми синусоїдальних коливань різних частот і різних амплітуд (рис. 2.2).

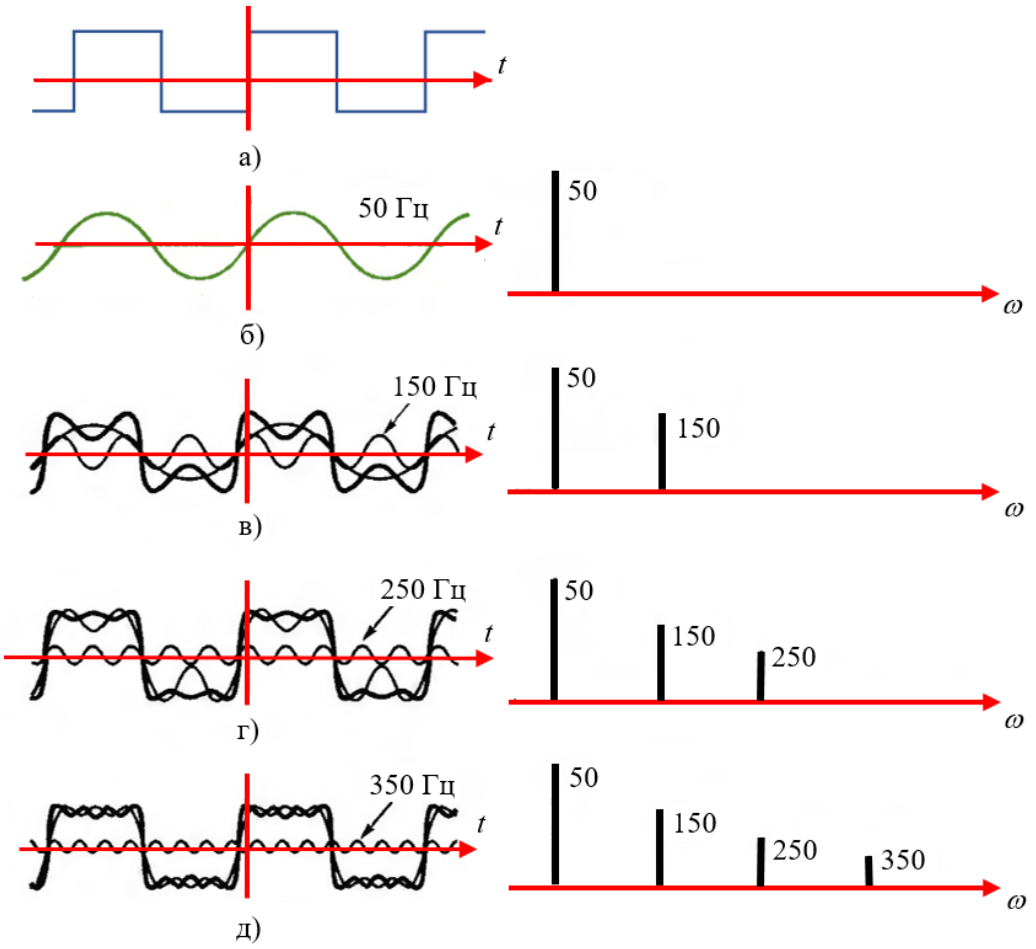



Рис. 2.2. Формування періодичного сигналу сумою синусоїд

Кожна складова синусоїда називається також **гармонікою**, а набір всіх гармонік називають **спектральним розкладанням**, або **спектром,** вихідного сигналу. Під шириною спектра сигналу розуміється різниця між максимальною і мінімальною частотами того набору синусоїд, які в сумі дають вихідний сигнал.

Неперіодичні сигнали можна представити у вигляді інтеграла синусоїдальних сигналів з безперервним спектром частот. Зокрема, спектральне розкладання ідеального імпульсу (одиничної потужності і нульової тривалості) має складові всього спектра частот, від -∞ до +∞ (рис. 2.3).

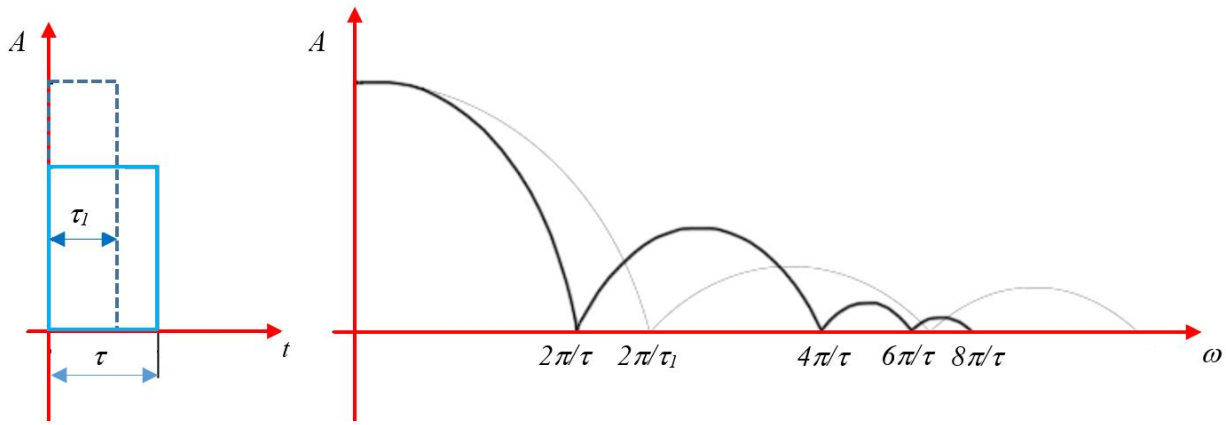



Рис. 2.3. Спектр ідеального імпульсу

Техніка знаходження спектра будь-якого вихідного сигналу добре відома. Для деяких сигналів, які описуються аналітично (наприклад, для послідовності прямокутних імпульсів однакової тривалості і амплітуди), спектр легко обчислюється на підставі формул Фур'є. Для сигналів довільної форми, що зустрічаються на практиці, спектр можна знайти за допомогою спеціальних приладів – спектральних аналізаторів, які вимірюють спектр реального сигналу і відображають амплітуди складових гармонік.

Існує дуже важливе поняття – **практична ширина спектру сигналу.** Зрозуміло, що якщо смуга пропускання якого-небудь пристрою недостатньо широка, щоб пропустити усі гармоніки, які суттєво впливають на форму сигналу, то сигнал на виході цього пристрою спотвориться. Таким чином, можна сказати, що ширина смуги пропускання пристрою не повинна бути вужче ширини спектра сигналу.

Існує декілька критеріїв для визначення практичної ширини спектру сигналу. Наприклад, можна відкидати всі гармоніки з амплітудами меншими 1% максимальної амплітуди в спектрі, тоді частоти гармонік, що залишилися і визначать ширину спектру сигналу. Можна відкидати ті гармоніки, сумарна енергія яких менше 10% загальної енергії сигналу. В цьому випадку ширину спектра також визначатимуть гармоніки, що залишаться в сигналі.

Однак, незалежно від критерію, за яким визначають ширину спектру сигналу, можна виділити такі загальні для всіх сигналів закономірності: чим крутіше фронт сигналу, чим коротші імпульси і чим більші паузи між імпульсами, тим ширший у всіх цих випадках спектр сигналу.

Сигнали, що передаються в телекомунікаційних мережах, спотворюються через недосконаліть ліній зв'язку (рис. 2.4). Спотворення лінією зв'язку синусоїди будь-якої частоти призводить до спотворення амплітуди і форми

сигналу. Спотворення форми проявляються в тому випадку, коли синусоїди різних частот спотворюються неоднаково. Якщо це аналоговий сигнал, що передає мову, то змінюється тембр голосу за рахунок спотворення обертонів – бічних частот. При передачі імпульсних сигналів, характерних для комп'ютерних мереж, спотворюються низькочастотні і високочастотні гармоніки, в результаті фронти імпульсів втрачають свою прямокутну форму і сигнали можуть погано розпізнаватися на приймальному кінці лінії.

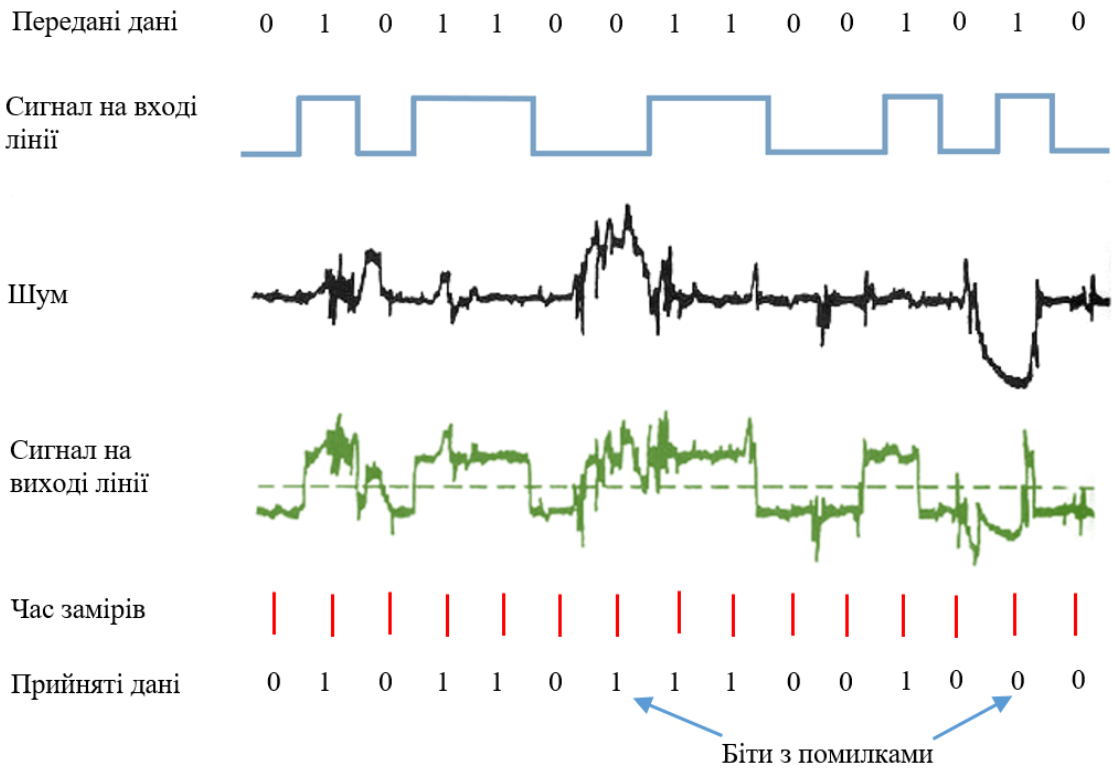



Рис. 2.4. Вплив шуму на цифровий сигнал

Крім спотворень сигналів, що виникають через недосконалість фізичних параметрів лінії зв'язку, існують і зовнішні завади, які вносять свій внесок в спотворення форми сигналів на виході лінії. Ці завади створюються різними електричними двигунами, електронними пристроями, атмосферними явищами і т. д. Не дивлячись на захисні заходи, що вживаються розробниками кабелів, і наявність підсилювальної та комутуючої апаратури, повністю компенсувати вплив зовнішніх перешкод не вдається.

Ступінь спотворення синусоїдальних сигналів лініями зв'язку оцінюється такими характеристиками, як затухання і смуга пропускання. Затухання показує, наскільки зменшується потужність еталонного синусоїдального сигналу на виході лінії зв'язку по відношенню до потужності сигналу на вході цієї лінії.

Затухання (А) зазвичай вимірюється в децибелах (дБ) і обчислюється за формулою:

$$A = 10 \log P_{вих}/P_{вх}$$

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

Так як затухання залежить від довжини лінії зв'язку, то в якості характеристики лінії зв'язку використовується **погонне затухання**, тобто затухання на лінії зв'язку певної довжини. Для кабелів локальних мереж в якості такої довжини, зазвичай використовується 100 м, для територіальних ліній зв'язку погонне затухання вимірюють для відстані в 1 км.

Ступінь затухання потужності синусоїдального сигналу залежить від частоти синусоїди, і ця залежність також характеризує лінію зв'язку (рис. 2.5).

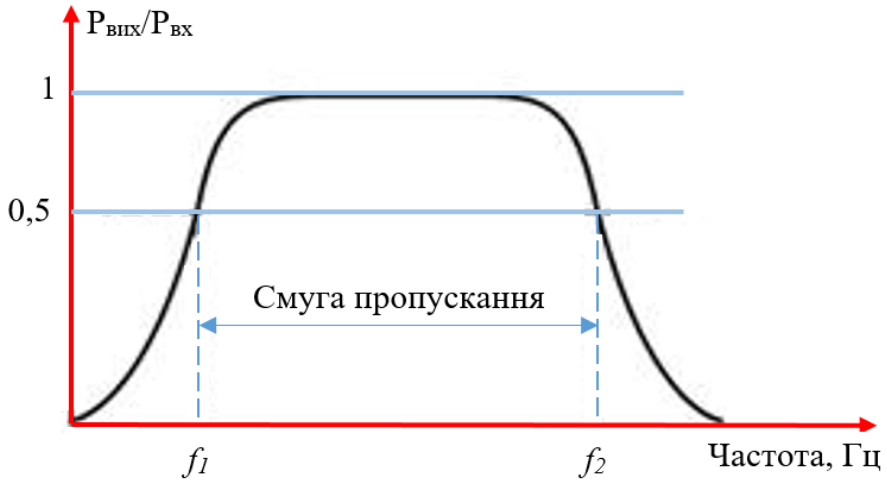



Рис. 2.5. Залежність затухання від частоти

Скручена пара дротів категорії 5 характеризується затуханням сигналу не вище 23,6 дБ для частоти 100 МГц при довжині кабелю 100 м. Оптичний кабель має істотно менші величини затухання, зазвичай в діапазоні від 0,2 до 3 дБ при довжині кабелю в 1000 м. Практично для всіх оптичних волокон типовою є складна залежність затухання від довжини хвилі, яка має три так званих вікна прозорості (рис. 2.6). З рисунку видно, що область ефективного використання сучасних волокон обмежена хвилями довжиною 850 нм, 1300 нм і 1550 нм (відповідно частотами 35 ТГц, 23 ТГц і 19,4 ТГц). Вікно 1550 нм забезпечує найменші втрати, а значить, максимальну дальність при фіксованій потужності передавача і фіксованій чутливості приймача.

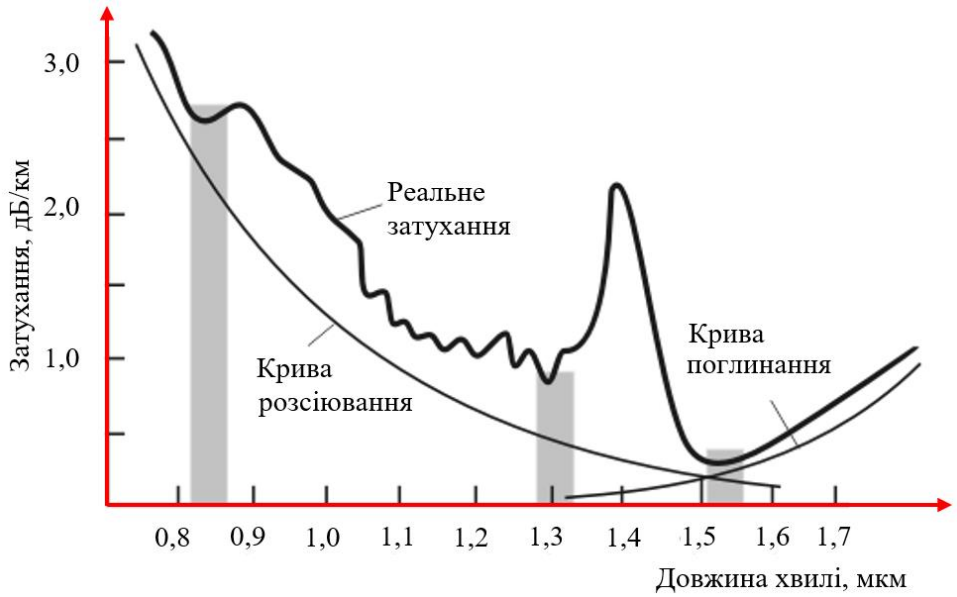



Рис. 2.6. Вікна прозорості оптичного волокна

### 2.1.5. Полоса пропускання та пропускна здатність лінії зв'язку

**Смуга пропускання** – це безперервний діапазон частот, у межах якого забезпечується передавання сигналу без суттєвого викривлення його форми.

Основні параметри, що характеризують смугу пропускання – ширина смуги і нерівномірність амплітудно-частотної характеристики (АЧХ) в межах цього діапазону. Нерівномірність АЧХ вимірюють у белах (для зручності використовують похідну одиницю – децибел). Ширину смуги пропускання, зазвичай визначають як різницю верхньої та нижньої граничних частот, на яких потужність вихідного сигналу зменшується у 2 рази по відношенню до вхідного, що відповідає затуханню – 3 дБ (рис. 2.5). Ширина смуги пропускання виражається в герцах. Вимоги до смуги пропускання різних пристроїв визначаються їх призначенням (наприклад, для телефонного зв'язку потрібна смуга пропускання 300-3400 Гц, для високоякісного відтворення музичних творів 30-16000 Гц, а для телевізійного мовлення – шириною до 8 МГц). Розширення смуги пропускання дозволяє передати більшу кількість інформації, а зменшення нерівномірності АЧХ у смузі пропускання покращує відтворення форми переданого сигналу.

**Пропускна спроможність** мережі характеризує максимально можливу швидкість передавання даних, яка може бути досягнута в цій мережі. Особливістю пропускної спроможності мережі є те, що, з однієї сторони, ця

характеристика залежить від параметрів середовища передавання, а з іншої – визначається методом передавання даних.

Пропускна спроможність, як і швидкість передавання даних, вимірюється в бітах за секунду (біт/с), а також в похідних одиницях (Кбіт/с, Мбіт/с т. д.).

Пропускна спроможність лінії зв’язку залежить не лише від її характеристик, таких як затухання і смуга пропускання, але і від спектру переданих сигналів. Якщо значимі гармоніки сигналу (тобто ті гармоніки, амплітуди яких вносять основний внесок в результуючий сигнал) потрапляють в смугу пропускання лінії, то такий сигнал буде добре передаватися даною лінією зв’язку і приймач зможе правильно розпізнати інформацію, відправлену по лінії передавачем (рис. 2.7, а). Якщо ж значущі гармоніки виходять за межі смуги пропускання лінії зв’язку, то сигнал почне значно спотворюватися і приймач буде помилятися при розпізнаванні інформації (рис. 2.7, б).

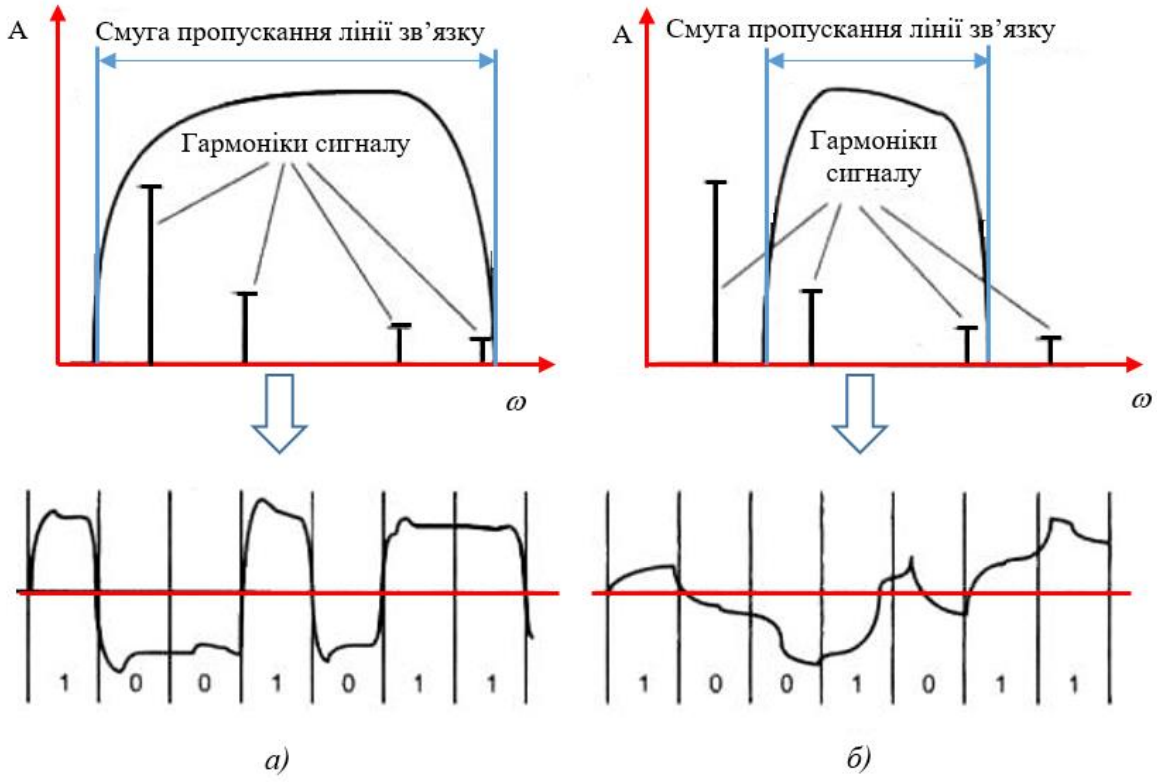



Рис. 2.7. Відповідність між смугою пропускання лінії зв’язку і спектром сигналу

## 2.2. Модуляція сигналів

### 2.2.1. Аналогова модуляція

Історично модуляція почала застосовуватися для аналогової інформації і тільки пізніше для дискретної. Необхідність в **аналоговій модуляції** (аналогова модуляція аналогових сигналів) виникає, коли потрібно передати низькочастотний аналоговий сигнал через аналоговий канал, що знаходиться в високочастотній області спектра.

Перш за все, така потреба виникає при використанні радіоканалів. Якщо передавати звукову інформацію в голосовому діапазоні (300 Гц – 20 кГц), то потрібна буде антена в декілька кілометрів. Очевидно, що безпосередньо голос через таке середовище передати не можна.

Для вирішення даної проблеми здійснюють накладання низькочастотного інформаційного сигналу на високочастотний несучий сигнал (рис. 2.8). Цей процес називається **модуляцією** – зміна одного із параметрів (амплітуди чи частоти) високочастотного несучого сигналу по закону зміни низькочастотного сигналу.

На рис. 2.8 приведена **амплітудна модуляція** (Amplitude Modulation, AM) голосового сигналу. В якості інформаційного параметру використовують також частоту синусоїдального сигналу – **частотна модуляція** (Frequency Modulation, FM) (рис. 2.9).

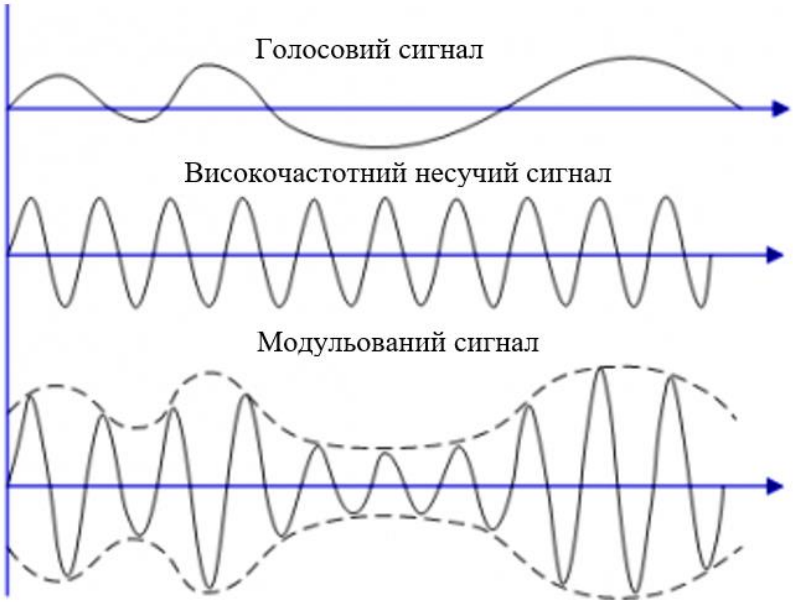



Рис. 2.8. Амплітудна модуляція звукового сигналу

В результаті модуляції сигнали переносяться в область більш високих частот.

Використання модуляції дозволяє:

- узгоджувати параметри сигналу з параметрами лінії;
- підвищити стійкість сигналів;
- збільшити дальність передачі сигналів;
- організовувати багатоканальні системи передачі.

Основні переваги амплітудної модуляції (рис. 2.9):

- вузька ширина спектра АМ сигналу;
- простота отримання модульованих сигналів.

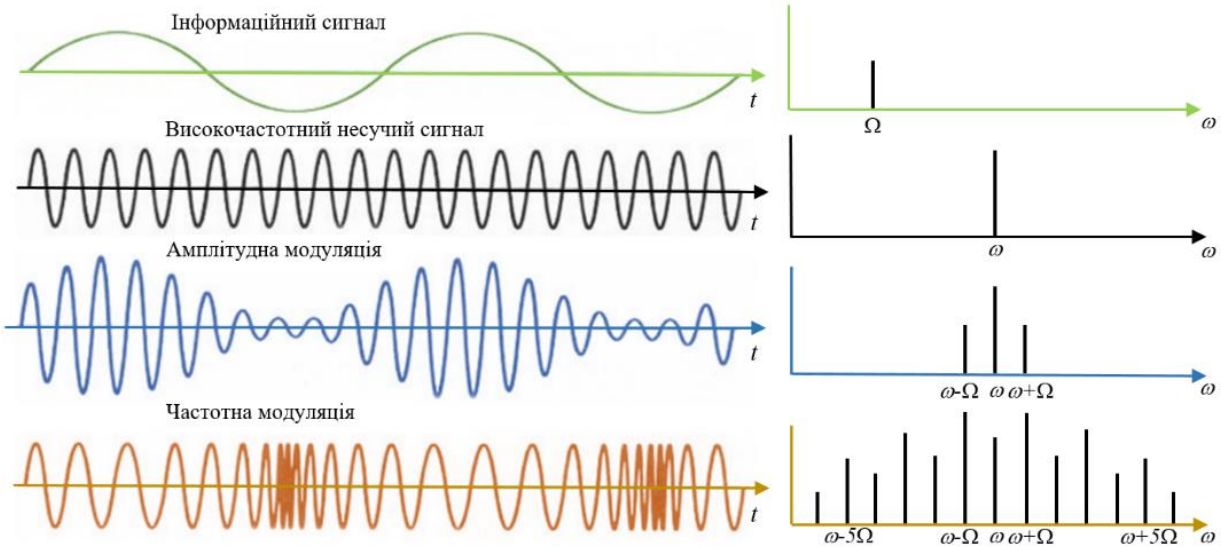



Рис. 2.9. Амплітудна та частотна модуляція аналогового сигналу

Недоліки амплітудної модуляції:

- низька стійкість (при впливі перешкоди на сигнал спотворюється його форма – огинаюча, яка і містить передані дані);
- неефективне використання потужності передавача (найбільша частина енергії модульованого сигналу міститься в складовій несучого сигналу до 64%, а на інформаційні бічні смуги доводиться по 18%).

Амплітудна модуляція знайшла широке застосування:

- в системах телевізійного мовлення (для передачі телевізійних сигналів);
- в системах звукового радіомовлення і радіозв’язку на довгих і середніх хвилях (АМ-діапазон);

Переваги частотної модуляції є:

- висока завадостійкість;
- більш ефективне використання потужності передавача;
- відносно просте отримання модульованих сигналів.

Основним недоліком даної модуляції є велика ширина спектру модульованого сигналу.

Частотна модуляція використовується:

- в системах телевізійного мовлення (для передачі сигналів звукового супроводу);
- в системах супутникового теле- і радіомовлення;
- в системах високоякісного стереофонічного мовлення (FM діапазон);
- в радіорелейних лініях (РРЛ);

При модуляції спектр результуючого сигналу потрапляє в потрібний високочастотний діапазон, що дозволяє використовувати методи мультиплексування або ущільнення.

### 2.2.2. Дискретна модуляція (маніпуляція)

Дискретна модуляція застосовується для передачі дискретних даних по каналах з вузькою смугою частот, наприклад, каналами тональної частоти, що використовується у загальних телефонних мережах. У разі, коли модульовані сигнали передають дискретну інформацію, замість терміну «модуляція» часто використовується термін «маніпуляція»: **амплітудна маніпуляція** (Amplitude Shift Keying, ASK), **частотна маніпуляція** (Frequency Shift Keying, FSK), **фазова маніпуляція** (Phase Shift Keying, PSK ).

Типова амплітудно-частотна характеристика стандартного абонентського каналу тональної частоти, показана на рис. 2.10. Цей комутований канал проходить через комутатори телефонної мережі і з’єднує телефони абонентів. Канал тональної частоти передає частоти в діапазоні від 300 до 3400 Гц, таким чином, його смуга пропускання складає 3100 Гц. Така вузька смуга пропускання цілком достатня для якісної передачі голосу, однак вона недостатньо широка для передачі комп’ютерних даних у вигляді прямокутних імпульсів. Рішення проблеми було знайдено завдяки **дискретній модуляції** (аналогова модуляція дискретних сигналів). Пристрій, що виконує функції модуляції несучої

синусоїди на стороні, яка передає сигнали, і демодуляції на прийомній стороні, називається **модемом** (модулятор-демодулятор).


Рис. 2.10. Амплітудно-частотна характеристика каналу тональної частоти

На рис. 2.11 показані різні типи модуляції, які застосовуються при передачі дискретної інформації.

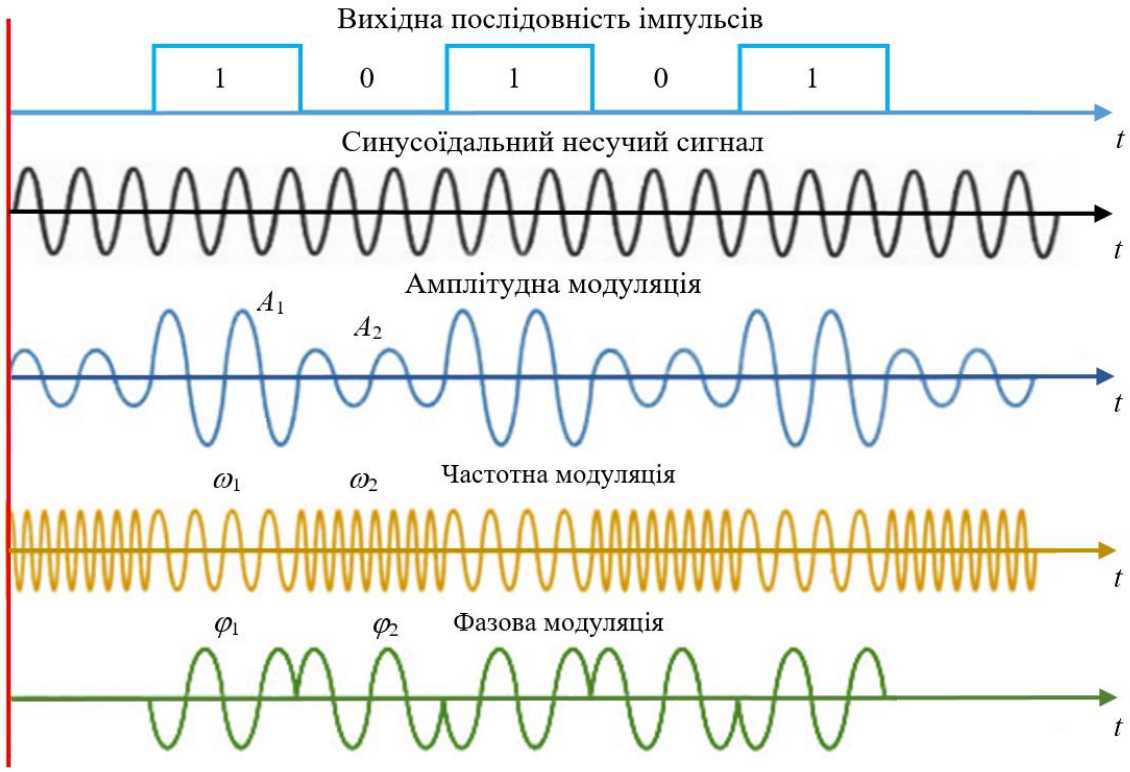



Рис. 2.11. Різні типи дискретної модуляції (маніпуляції)

При **амплітудній модуляції** (маніпуляції) для логічної одиниці вибирається один рівень амплітуди синусоїди несучої частоти, а для логічного нуля – інший ($A_1$ та $A_2$). Цей спосіб в чистому вигляді практично не

використовується через низку завадостійкість, але часто застосовується в поєднанні з фазовою модуляцією.

При **частотній модуляції** (маніпуляції) значення нуля і одиниці вихідних даних передаються синусоїдами з різною частотою ($f_1$ та $f_2$). Цей спосіб модуляції не вимагає складних схем і зазвичай застосовується в низькошвидкісних модемах, які працюють на швидкостях 300 і 1200 біт/с. При використанні тільки двох частот за один такт передається один біт інформації, тому такий спосіб називається **двійковою частотної маніпуляцією** (Binary FSK, BFSK). Можуть також використовуватися чотири різні частоти для кодування двох бітів інформації в одному такті – **чотирирівнева частотна маніпуляція** (four-level FSK). Використовується також назва **багаторівнева частотна маніпуляція** (Multilevel FSK, MFSK).

При **фазовій модуляції** (маніпуляції) значенням даних 0 і 1 відповідають сигнали однакової частоти, але різної фази, наприклад 0 і 180° або 0, 90, 180 і 270°. У першому випадку така модуляція носить назву **двійковій фазової маніпуляції** (Binary PSK, BPSK), а в другому – **квадратурної фазової маніпуляції** (Quadrature PSK, QPSK).

Для підвищення швидкості передачі даних використовують комбіновані методи модуляції. Найбільш поширеними є методи **квадратурної амплітудної модуляції** (Quadrature Amplitude Modulation, QAM). Ці методи засновані на поєднанні фазової і амплітудної модуляції.

Квадратурна амплітудна модуляція – різновид амплітудної модуляції сигналу, яка є сумою двох несучих коливань однієї частоти, але зсунутих по фазі один відносно одного на 90° (тому «квадратурна»), кожне з яких модульоване по амплітуді своїм модулюючим сигналом.

Квадратурна модуляція застосовується для передачі сигналів кольору в телевізійному стандарті PAL і NTSC, в стереофонічному радіомовленні.

### 2.2.3. Імпульсно-кодова модуляція

**Імпульсно-кодова модуляція** (ІКМ або PCM – Pulse Code Modulation) – процес перетворення аналогового сигналу у цифровий сигнал, коли через певні інтервали часу беруться відліки аналогового сигналу і незалежно один від одного квантуються і далі кодуються цифрами. ІКМ використовується для оцифровування аналогових сигналів перед їхньою передачею по телекомунікаційній мережі. Практично всі види аналогових даних (відео, голос, музика, дані телеметрії) допускають застосування ІК-модуляції.

Імпульсно-кодова модуляція заснована на теорії відображення Найквіста-Котельникова. Відповідно до цієї теорії, аналогова неперервна функція, яка

представлена у вигляді послідовності її дискретних за часом значень, може бути точно відтворена, якщо частота дискретизації була в два або більше разів вище, ніж частота найвищої гармоніки спектру вихідної функції. Якщо ця умова не дотримується, то відновлена функція буде істотно відрізнятися від початкової.

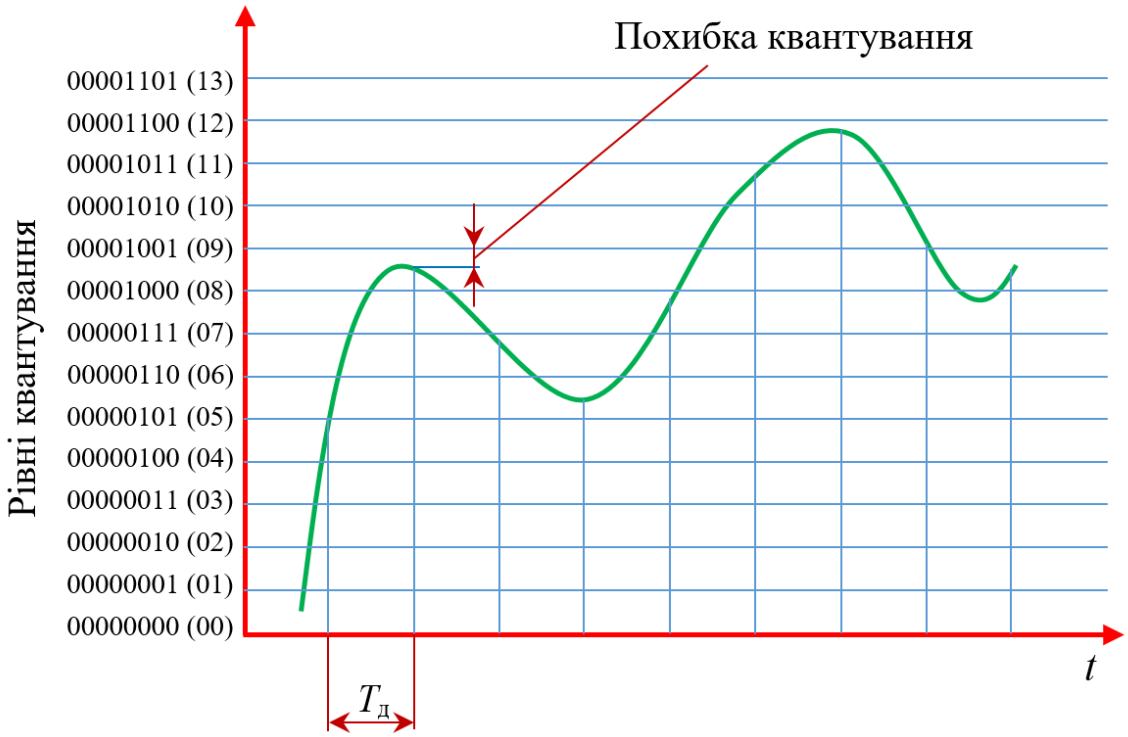



Рис. 2.12. Імпульсно-кодова модуляція

Імпульсно-кодове перетворення складається з наступних етапів:

1. **Дискретизація** аналогового сигналу.

В аналоговій телефонії для передачі голосу був обраний діапазон від 300 до 3400 Гц (рис. 2.10), який досить якісно (рівень чіткості слів 85-90%) передає всі основні гармоніки співрозмовників. Відповідно до теорії Найквіста-Котельникова для якісної передачі голосу досить вибрати частоту дискретизації, яка в два рази перевищує найвищу гармоніку безперервного сигналу, тобто 2 х 3400 = 6800 Гц. Для забезпечення деякого запасу якості обрано частоту дискретизації 8000 Гц, що відповідає періоду дискретизації:

$$T_д = 1/8000 = 0{,}000125 \text{ с} = 125 \text{ мкс}$$

**2. Квантування** амплітуд дискретних відліків сигналу.

Для якісного передавання голосу приймають 256 рівнів квантування (8-бітний код для представлення величини амплітуди одного виміру). Величиною амплітуди дискретного відліку голосового сигналу вибирають

найближчий до її значення рівень квантування. Різницю між значеннями амплітуди сигналу й найближчим рівнем квантування визначає похибка перетворення голосового сигналу в цифрову форму, яку називають **похибкою квантування** $\Delta$.

**3. Кодування** квантованих амплітуд дискретних відліків сигналу.

Якщо номери рівнів квантування подати в двійковому коді, то процес кодування зводиться до вибору номера найближчого до значення дискретної амплітуди сигналу рівня квантування. Номер рівня квантування в двійковому коді передається в лінію.

Кодову комбінацію, яка відповідає одному дискретного відліку амплітуди голосового сигналу, називають **вибіркою.**

Зважаючи на те, що вибірки голосового сигналу надходять у лінію з частотою 8 кГц, послідовно одна за одною, отримуємо цифровий потік зі швидкістю

$$C = 8 \text{ біт} \times 8000 \text{ Гц} = 64 \text{ Кбіт/с}.$$

Швидкість 64 Кбіт/с визначено Міжнародним телекомунікаційним союзом (ITU-T) **швидкістю основного цифрового каналу**, який ще називають **потоком нульового рівня DSO** (Digital Service/Signal of Level 0). Цифровий канал 64 Кбіт/с також називається **елементарним каналом цифрових телефонних мереж.**

## 2.3. Комутація каналів та пакетів

### 3.1. Комутація каналів

Історично комутація каналів з’явилась набагато раніше комутації пакетів і веде свій відлік від перших телефонних мереж. Мережі, що побудовані за принципом комутації каналів, мають багату історію, вони і сьогодні знайшли широке застосування в світі телекомунікацій, будучи основою високошвидкісних магістральних каналів зв’язку.

В якості інформаційних потоків в мережах з комутацією каналів є дані, якими обмінюються пари абонентів. Відповідно глобальною ознакою потоку є пара адрес (телефонних номерів) абонентів, що з’єднуються між собою. Для всіх можливих потоків заздалегідь визначаються маршрути. Маршрути в мережах з комутацією каналів задаються або «вручну» адміністратором мережі, або знаходяться автоматично із залученням спеціальних програмних і апаратних

засобів. Маршрути фіксуються в таблицях, в яких ознакам потоку ставляться у відповідність ідентифікатори вихідних інтерфейсів комутаторів. На підставі цих таблиць відбувається просування і мультиплексування даних.

Однією з особливостей мереж з комутацією каналів є поняття елементарного каналу.

**Елементарний канал** (або просто **канал**) – це базова технічна характеристика мережі з комутацією каналів, що являє собою деяке фіксоване в межах даного типу мереж значення пропускної спроможності. Будь-яка лінія зв'язку в мережі з комутацією каналів має пропускну спроможність, кратну елементарному каналу, прийнятому для даного типу мережі.

Значення елементарного каналу, або, іншими словами, мінімальна одиниця пропускної спроможності лінії зв'язку, вибирається з урахуванням різних факторів. Наприклад, в традиційних телефонних мережах, для якісної цифрової передачі голосу, найбільш поширеним значенням елементарного каналу сьогодні є швидкість 64 Кбіт/с.

Особливістю мереж з комутацією каналів є те, що пропускна спроможність кожної лінії зв'язку повинна дорівнювати цілому числу елементарних каналів. Так, лінії зв'язку, що під'єднують абонентів до телефонної мережі, можуть містити 2, 24 або 30 елементарних каналів, а лінії, що з'єднують комутатори – 480 або 1920 каналів. На рис. 2.13 зображено фрагмент мережі, яка характеризується елементарним каналом *P* біт/с.

У мережі існують лінії зв'язку різної пропускної спроможності, що складаються з 2, 3, 4 та 5 елементарних каналів. На рисунку показані два абонента, A і B, що генерують під час сеансу зв'язку (телефонної розмови) інформаційний потік, для якого в мережі був передбачений маршрут, що проходить через чотири комутатора S1, S2, S3 і S4. Припустимо також, що інтенсивність інформаційного потоку між абонентами не перевищує *2P* біт/с. Тоді, для обміну даними, цим двом абонентам досить мати у своєму розпорядженні по парі елементарних каналів, «виділених» з кожної лінії зв'язку, що лежить на маршруті проходження даних від пункту A до пункту B.

Зв'язок, побудовану шляхом комутації (з'єднання) елементарних каналів, називають **комутованим каналом** або **складовим каналом.**

У розглянутому прикладі для з'єднання абонентів A і B був створений комутований канал з пропускною спроможність в два елементарних канали.

Основні властивості комутованого каналу:

• комутований канал на всьому своєму шляху складається з **однакової** кількості елементарних каналів;

• комутований канал має **постійну і фіксовану пропускну спроможність** на всьому своєму протязі;

• комутований канал створюється тимчасово на період сеансу зв’язку двох абонентів;

• на час сеансу зв’язку всі елементарні канали, що входять в комутований канал, надаються у виключне користування абонентів, для яких був створений цей комутований канал;

• протягом всього сеансу зв’язку абоненти можуть посилати в мережу дані зі швидкістю, що не перевищує пропускну спроможність комутованого каналу;

• дані, що надійшли в комутований канал, гарантовано доставляються абонента без затримок, втрат і з тією ж швидкістю (швидкістю джерела) незалежно від того, чи існують в цей час в мережі інші з’єднання;

• після закінчення сеансу зв’язку елементарні канали, що входили до відповідного комутованого каналу, оголошуються вільними і повертаються в пул розподільчих ресурсів для використання іншими абонентами.


Рис. 2.13. Комутований (складовий) канал в мережі з комутацією каналів

У мережі може одночасно відбуватися декілька сеансів зв’язку. Поділ мережі між сеансами зв’язку відбувається на рівні елементарних каналів за допомогою процесу **мультиплексування**. Мультиплексування дозволяє одночасно передавати через кожен фізичний канал трафік декількох логічних з’єднань.

Можливі ситуації, коли деяка проміжна лінія зв'язку вже вичерпала вільні елементарні канали, тоді новий сеанс зв'язку, маршрут якого пролягає через дану лінію зв'язку, не може відбутися. Для того, щоб розпізнати такі ситуації, обмін даними в мережі з комутацією каналів передує **процедура встановлення з'єднання**. Відповідно до цієї процедури абонент, який є ініціатором сеансу зв'язку (наприклад, абонент А), посилає в комутаційну мережу запит, який представляє собою повідомлення, в якому міститься адреса абонента, наприклад абонента В. Мета запиту – перевірити, чи можна утворити комутований канал між абонентами А і В. А для цього потрібно дотримання двох умов: наявність необхідного числа вільних елементарних каналів в кожній лінії зв'язку, що лежить на шляху від А до В, і незайнятість абонента в іншому з'єднанні.

Запит переміщається по маршруту, визначеному для інформаційного потоку даної пари абонентів. При цьому використовуються глобальні таблиці комутації, що ставлять у відповідність глобальній ознаці потоку (адресу абонента) ідентифікатор вихідного інтерфейсу комутатора (такі таблиці часто називають таблицями маршрутизації). Якщо в результаті проходження запиту від абонента А до абонента В з'ясувалося, що ніщо не перешкоджає встановленню з'єднання, відбувається фіксація комутованого каналу. Для цього у всіх комутаторах уздовж шляху від А до В створюються записи в локальних таблицях комутації, в яких вказується відповідність між локальними ознаками потоку та номерами елементарних каналів, зарезервованих для цього сеансу зв'язку. Тільки після цього комутований канал вважається встановленим, і абоненти А і В можуть почати свій сеанс зв'язку.

Запити на встановлення з'єднання не завжди завершуються успішно. Якщо на шляху між абонентами відсутні вільні елементарні канали або абонент, що викликається зайнятий, то відбувається відмова у встановленні з'єднання. Наприклад, якщо під час сеансу зв'язку абонентів А і В, абонент С відправить запит в мережу на встановлення з'єднання з абонентом D, то він отримає відмову, оскільки обидва необхідних йому елементарних канали, що складають лінію зв'язку комутаторів S3 і S4, вже виділені для з'єднання абонентів А і В. При відмові у встановленні з'єднання мережа інформує абонента спеціальним повідомленням.

Розглянута процедура встановлення з'єднання, що базується на здатності абонентів відправляти в мережу сервісні повідомлення (запити на встановлення з'єднання) і здатності вузлів мережі обробляти такі повідомлення називається **автоматичним динамічним режимом** встановлення з'єднання.

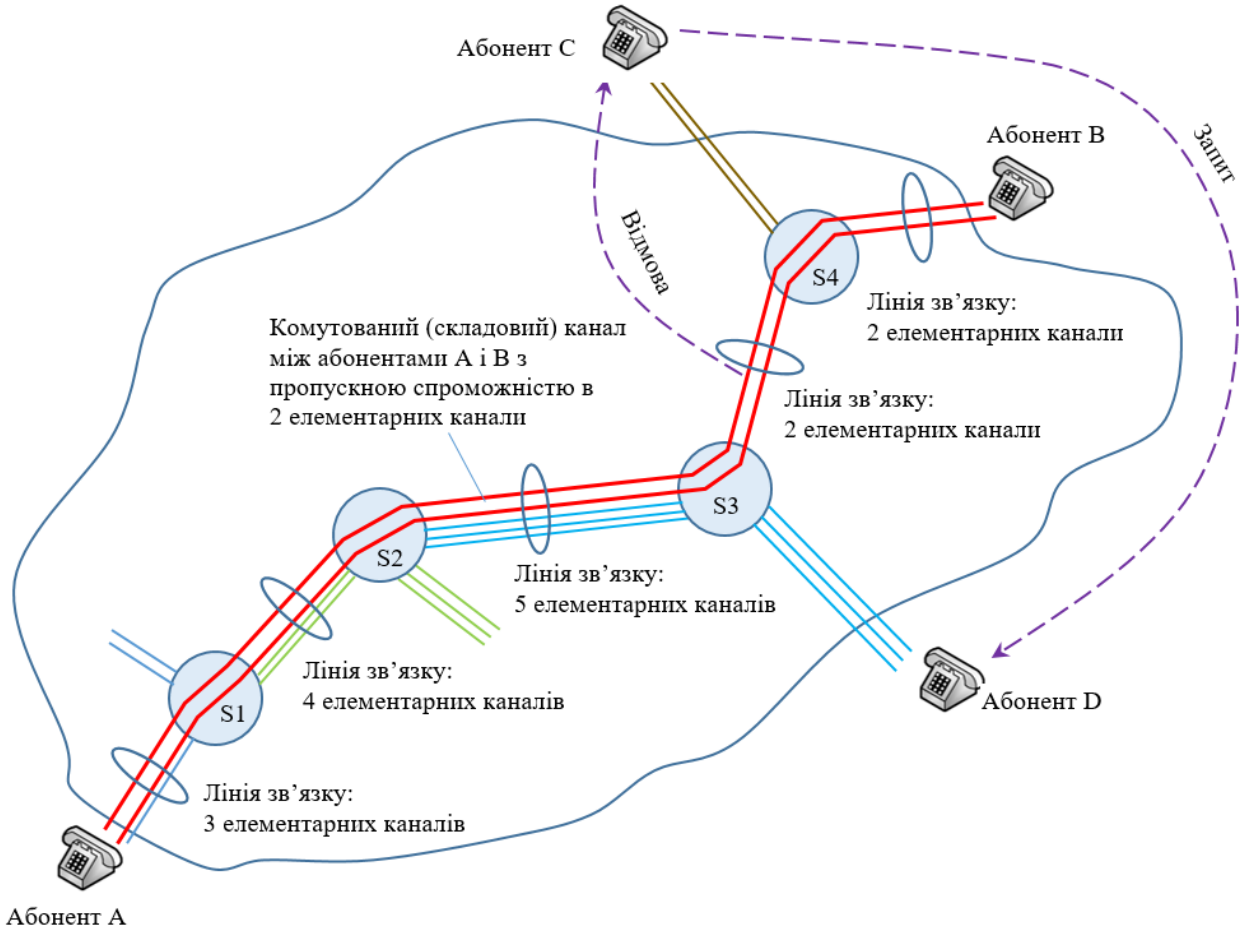



Рис. 2.14. Відмова у встановленні з'єднання в мережі з комутацією каналів

Інший режим – **статичний ручний режим** встановлення з'єднання. Цей режим характерний для випадків, коли необхідно встановити комутований канал не на час одного сеансу зв'язку абонентів, а на більш тривалий термін. Створення такого довготривалого каналу не можуть ініціювати абоненти, він створюється адміністратором мережі. Очевидно, що статичний ручний режим мало придатний для традиційної телефонної мережі з її короткими сеансами зв'язку, однак він добре підходить для створення високошвидкісних телекомунікаційних каналів між містами і країнами.

Мережі з комутацією каналів найбільш ефективно передають користувацький трафік в тому випадку, коли швидкість його постійна протягом усього сеансу зв'язку і максимально відповідає фіксованій пропускної спроможності фізичних ліній зв'язку мережі. Ефективність роботи мережі знижується, коли інформаційні потоки, які генеруються абонентами, набувають пульсуючий характер. Це відбувається при передачі комп'ютерного трафіку, тобто трафіку, що генерується додатками, з якими працює користувач

комп’ютера. Для ефективної передачі нерівномірного комп’ютерного трафіку була спеціально розроблена техніка комутації пакетів.

Техніка комутації каналів має свої переваги і недоліки.

Переваги комутації каналів:

- Постійна і відома швидкість передачі даних по встановленому між кінцевими вузлами каналу.
- Низький і постійний рівень затримки передачі даних через мережу. Це дозволяє якісно передавати дані, чутливі до затримок (трафік реального часу) – голос, відео, різну технологічну інформацію.

Недоліки комутації каналів

- Відмова мережі в обслуговуванні запиту на встановлення з’єднання. Така ситуація може скластися коли на деякій ділянці мережі потрібно встановити з’єднання вздовж каналу, через який вже проходить максимальна можлива кількість елементарних каналів.
- Нераціональне використання пропускної спроможності фізичних каналів. Та частина пропускної спроможності, яка відводиться комутованому каналу після встановлення з’єднання, надається йому на весь час, тобто до тих пір, поки з’єднання не буде розірвано. Неможливість динамічного перерозподілу пропускної спроможності є принциповим обмеженням мережі з комутацією каналів.
- Обов’язкова затримка перед передачею даних через фази встановлення з’єднання.

### 2.3.2. Комутація пакетів

Важливим принципом функціонування мереж з комутацією пакетів є представлення інформації, що передається по мережі, у вигляді структурно відділених один від одного порцій даних, які називаються **пакетами.**

Процедура формування пакету здійснюється за допомогою **інкапсуляції** даних (розглядали в курсі «Комп’ютерні мережі»), при якій дані на певному рівні доповнюються заголовками, закінченнями та іншою інформацію з протоколів вищого рівня OSI моделі.

Кожен пакет забезпечений заголовком (рис. 2.15), який містить адреси відправника та отримувача і іншу допоміжну інформацію (довжина поля даних, контрольна сума і ін.), необхідну для доставки пакету адресату. Наявність адреси в кожному пакеті є однією з найважливіших особливостей техніки комутації пакетів, так як кожен пакет може бути оброблений комутатором незалежно від інших пакетів, що складають мережевий трафік. Крім заголовка у пакета може бути ще одне додаткове поле, яке розміщується в кінці пакета і тому назване

**закінчення**. У закінченні, зазвичай, поміщається контрольна сума, яка дозволяє перевірити, чи була спотворена інформація при передачі через мережу.

Залежно від конкретної реалізації технології комутації пакетів пакети можуть мати фіксовану або змінну довжину, крім того, може змінюватися склад інформації, розміщеної в заголовках пакетів. Наприклад, в технології ATM пакети (звані там комірки) мають фіксовану довжину, а в технології Ethernet встановлені лише мінімально і максимально можливі розміри пакетів (кадрів).

Пакети надходять в мережу **без попереднього резервування ліній зв'язку** і **не з фіксованою заздалегідь заданою швидкістю**, як це робиться в мережах з комутацією каналів, а в тому темпі, в якому їх генерує відправник. Передбачається, що мережа з комутацією пакетів, на відміну від мережі з комутацією каналів, завжди готова прийняти пакет від кінцевого вузла.

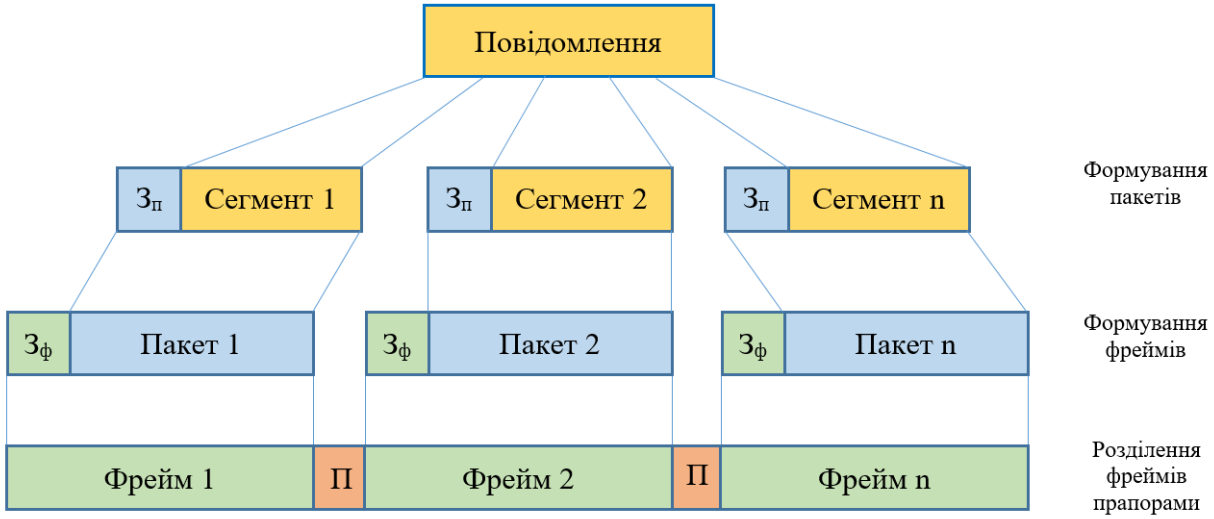



Рис. 2.15. Формування пакетів в мережах з комутацією пакетів

Як і в мережах з комутацією каналів, в мережах з комутацією пакетів для кожного потоку вручну або автоматично визначається маршрут, що зберігається на комутаторах (маршрутизаторах) у таблицях комутації (маршрутизації). Пакети, потрапляючи на комутатор, обробляються і надсилаються з того чи іншого маршруту на підставі інформації, що міститься в їх заголовках, а також в таблиці комутації.

Пакети, що належать одному або різним інформаційним потокам, при переміщенні по мережі можуть «перемішуватися» між собою, утворювати черги і навіть губитися на шляху проходження. На шляху пакетів можуть зустрічатися лінії зв'язку, що мають різну пропускну спроможність. В залежності від часу доби може сильно змінюватися і ступінь завантаженості ліній зв'язку. В таких умовах не виключені ситуації, коли пакети, що належать одному і тому ж потоку,

можуть переміщатися по мережі з різними швидкостями і навіть прийти до місця призначення не в тому порядку, в якому вони були відправлені.

Поділ даних на пакети дозволяє передавати нерівномірний комп'ютерний трафік більш ефективно, ніж в мережах з комутацією каналів. Це пояснюється тим, що пульсації трафіку від окремих комп'ютерів носять випадковий характер і розподіляються в часі так, що їх піки найчастіше не збігаються. Тому коли лінія зв'язку передає трафік великої кількості кінцевих вузлів, в сумарному потоці пульсації згладжуються і пропускна спроможність лінії використовується більш раціонально, без тривалих простоїв.

Невизначеність і асинхронність переміщення даних в мережах з комутацією пакетів висуває особливі вимоги до роботи комутаторів в таких мережах. Головна відмінність пакетних комутаторів від комутаторів в мережах з комутацією каналів полягає в тому, що вони мають внутрішню **буферну пам'ять** для тимчасового зберігання пакетів.

Пакетний комутатор не може прийняти рішення про просування пакета, не маючи в своїй пам'яті всього пакету. Комутатор перевіряє контрольну суму, і лише після того як визначить, що дані пакета не спотворені, починає обробляти пакет і за адресою призначення визначає наступний комутатор. Тому кожен пакет послідовно біт за бітом поміщається у вхідний буфер.

Комутатору потрібні буфери для **узгодження швидкостей передачі даних в лініях зв'язку**, що під'єднанні до його інтерфейсів. Якщо швидкість надходження пакетів з однієї лінії зв'язку протягом деякого періоду перевищує пропускну спроможність тієї лінії зв'язку, в яку ці пакети повинні бути спрямовані, то щоб уникнути втрат пакетів на цільовому інтерфейсі необхідно організувати вихідну чергу. Буферизація необхідна пакетному комутатору також для **узгодження швидкості надходження пакетів зі швидкістю їх комутації.** Якщо комутуючий блок не встигає обробляти пакети (аналізувати заголовки і перекидати пакети на потрібний інтерфейс), то на інтерфейсах комутатора виникають вхідні черги.

Оскільки обсяг буферів пам'яті в комутаторах обмежений, іноді відбувається втрата пакетів через переповнення буферів при тимчасовому перевантаженні частини мережі, коли збігаються періоди пульсації декількох інформаційних потоків. Для мереж з комутацією пакетів втрата пакетів є звичайним явищем, і для компенсації таких втрат в даній технології передбачений ряд спеціальних механізмів.

Пакетний комутатор може працювати на основі одного з трьох методів просування пакетів:

- датаграмна передача;
- передача з встановленням логічного з'єднання;

• передача з встановленням віртуального каналу.

**Датаграмний метод передачі даних** базується на тому, що всі пакети просуваються (передаються від одного вузла мережі до іншого) незалежно один від одного на підставі одних і тих же правил.

Процедура обробки пакета визначається лише значеннями параметрів, які він містить у собі, і поточним станом мережі (наприклад, в залежності від її навантаження пакет може стояти в черзі на обслуговування більший чи менший час). Кожен окремий пакет розглядається мережею як абсолютно незалежна одиниця передачі – **датаграма.**

Рішення про просування пакета приймається на основі таблиці комутації, що ставить у відповідність адресам призначення пакетів інформацію, що однозначно визначає наступний за маршрутом транзитний (або кінцевий) вузол. В якості такої інформації можуть виступати ідентифікатори інтерфейсів даного комутатора або адреси вхідних інтерфейсів комутаторів, наступних за маршрутом.

Датаграмний метод працює швидко, так як ніяких попередніх дій перед відправкою даних проводити не потрібно. Однак, при такому методі важко перевірити факт доставки пакету вузлу призначення. Цей метод не гарантує доставку пакету, він робить це в міру можливості – для опису такої властивості використовується термін **доставка по можливості** (best effort).

**Метод передачі із встановленням логічного з'єднання** ґрунтується на процедурі погодження двома кінцевими вузлами мережі деяких параметрів процесу обміну пакетами. Параметри, про які домовляються два взаємодіючих вузла, називаються **параметрами логічного з'єднання.**

Наявність логічного з'єднання дозволяє більш раціонально в порівнянні з датаграмним методом обробляти пакети. Наприклад, при втраті декількох попередніх пакетів може бути знижена швидкість відправки наступних.

Коли відправник і одержувач фіксують початок нового з'єднання, вони, перш за все, «домовляються» про початкові значення параметрів процедури обміну і тільки після цього починають передачу даних.

Процедура встановлення з'єднання складається з трьох кроків:

1. Вузол-ініціатор з'єднання відправляє вузлу-одержувачу службовий пакет з пропозицією встановити з'єднання.
2. Якщо вузол-одержувач згоден з цим, то він посилає у відповідь інший службовий пакет, який підтверджує встановлення з'єднання і пропонує деякі параметри, які будуть використовуватися в рамках даного логічного з'єднання. Це можуть бути, наприклад, ідентифікатор

з’єднання, кількість кадрів, які можна відправити без отримання підтвердження і т. п.

3. Вузол-ініціатор з’єднання може закінчити процес встановлення з’єднання відправкою третього службового пакета, в якому повідомить, що запропоновані параметри йому підходять.

На відміну від передачі датаграмного типу, в якій підтримується тільки один тип кадру – інформаційний, передача із встановленням з’єднання повинна підтримувати як мінімум два типи кадрів – інформаційні кадри містять дані користувача, а службові призначені для встановлення (розриву) з’єднання.

Після того як з’єднання встановлено і всі параметри погоджені, кінцеві вузли починають передачу даних. Пакети даних обробляються комутаторами так само, як і при датаграмній передачі: з заголовків пакетів зчитуються адреси призначення і порівнюються із записами в таблицях комутації, що містять інформацію про наступні шляхи по маршруту. Так само як датаграми, пакети, що відносяться до одного логічного з’єднання, в деяких випадках (наприклад, при відмові лінії зв’язку) можуть доставлятися адресату за різними маршрутами. Однак передача з встановленням з’єднання має важливу відміну від датаграмної передачі, оскільки в ній крім обробки пакетів на комутаторах має місце додаткова обробка пакетів на кінцевих вузлах.

Після передачі деякого закінченого набору даних, наприклад певного файлу, вузол-відправник ініціює розрив даного логічного з’єднання, посилаючи відповідний службовий кадр.

Передача з встановленням логічного з’єднання надає більше можливостей в плані надійності та безпеки обміну даними, ніж датаграмна передача. Однак цей спосіб більш повільний, так як він використовує додаткові обчислювальні витрати на встановлення і підтримання логічного з’єднання.

**Метод передачі із встановленням віртуального каналу** базується окремому випадку логічного з’єднання, в число параметрів якого входить жорстко визначений для всіх пакетів маршрут. Тобто все пакети, що передаються в рамках даного з’єднання, повинні проходити по одному і тому ж закріпленому за цим з’єднанням маршруту.

Єдиний заздалегідь прокладений фіксований маршрут, який з’єднує кінцеві вузли в мережі з комутацією пакетів, називають **віртуальним каналом** (virtual circuit або virtual channel).

Віртуальні канали прокладаються для стійких інформаційних потоків. З метою виділення потоку даних із загального трафіку кожен пакет цього потоку позначається спеціальною міткою.

Так само як в мережах із встановленням логічних з'єднань, прокладка віртуального каналу починається з відправки з вузла-джерела спеціального пакету-запиту на встановлення з'єднання. У запиті зазначаються адреса призначення і мітка потоку, для якого прокладається цей віртуальний канал. Запит, проходячи по мережі, формує новий запис в кожному з комутаторів, розташованих на шляху від відправника до одержувача. Запис говорить про те, яким чином комутатор повинен обслуговувати пакет, що має задану мітку. Утворений віртуальний канал ідентифікується тієї ж міткою.

Після прокладки віртуального каналу мережа може передавати по ньому відповідний потік даних. У всіх пакетах, які передають дані користувача, адреса призначення вже не вказується, її роль відіграє мітка віртуального каналу. При надходженні пакету на вхідний інтерфейс комутатор читає значення мітки з заголовку пакету і переглядає свою таблицю комутації, по якій визначає, на який вихідний порт передати пакет.

Таблиця комутації в мережах, що використовують віртуальні канали, відрізняється від таблиці комутації в датаграмних мережах. Вона містить записи тільки про віртуальні канали, що проходять через комутатор, а не про всі можливі адреси призначення, як це має місце в мережах з датаграмним алгоритмом просування.

В одній і тій же мережевій технології можуть бути задіяні різні способи просування даних. Так, датаграмний протокол IP використовується для передачі даних між різними мережами, складовими Інтернет. У той же час забезпеченням надійної доставки даних між кінцевими вузлами цієї мережі займається протокол TCP, що встановлює логічні з'єднання без фіксації маршруту. І нарешті, Інтернет – це приклад мережі, яка застосовує техніку віртуальних каналів, так як до складу Інтернету входить чимало мереж ATM і Frame Relay, що підтримують віртуальні канали.

Переваги мереж з комутацією пакетів:

- Висока загальна пропускна здатність мережі при передачі пульсуючого трафіку.
- Можливість динамічно перерозподіляти пропускну спроможність фізичних каналів зв'язку між абонентами відповідно до реальних потреб їх трафіку.

Недоліки мереж з комутацією пакетів:

- Невизначеність швидкості передачі даних між абонентами мережі, обумовлена тим, що затримки в чергах буферів комутаторів мережі залежать від загального завантаження мережі.
- Змінна величина затримки пакетів даних, яка може бути досить тривалою в моменти миттєвих перевантажень мережі.

- Можливі втрати даних через переповнення буферів.

## 2.4. Мультиплексування та комутація

Щоб визначити, на який інтерфейс слід передати дані, комутатор повинен з'ясувати, до якого потоку вони відносяться. Це завдання має вирішуватися незалежно від того, надходить на вхід комутатора тільки один «чистий» потік або «змішаний» потік, який є результатом агрегування декількох потоків. В останньому випадку до завдання розпізнавання потоків додається завдання мультиплексування/демультиплексування.

**Мультиплексування** – утворення з декількох окремих потоків загального агрегованого потоку, який передається по одному фізичному каналу зв'язку. Іншими словами, мультиплексування – це спосіб поділу одного наявного фізичного каналу між декількома одночасно протікають сеансами зв'язку між абонентами мережі.

**Демультиплексування** – поділ сумарного агрегованого потоку на кілька складових його потоків.

В даний час для мультиплексування абонентських каналів використовуються наступні технології:

• **частотне мультиплексування** (Frequency Division Multiplexing, **FDM**);

• **хвильове мультиплексування** (Wave Division Multiplexing, **WDM**);

• **часове мультиплексування** (Time Division Multiplexing, **TDM**);

• **множинний доступ з кодовим поділом** (Code Division Multiple Access, **CDMA**).

Метод TDM використовується при комутації як каналів, так і пакетів. Методи FDM, WDM і CDMA придатні виключно для комутації каналів. Метод CDMA застосовується тільки в техніці розширеного спектру і використовується при бездротовій передачі.

### 2.4.1. Комутація каналів на основі методів FDM і WDM

Технологія **частотного мультиплексування** (FDM) була розроблена для телефонних мереж, але застосовується вона і для інших видів мереж, наприклад первинних мереж (мікрохвильові канали) або мереж кабельного телебачення.

Основна ідея цього методу полягає у виділенні кожному з'єднанню власного діапазону частот в загальній смузі пропускання лінії зв'язку. На основі цього діапазону створюється **канал**. Дані, що передаються в каналі, модулюються за допомогою одного з описаних раніше методів з використанням несучої частоти, що належить діапазону каналу. Мультиплексування

виконується за допомогою зміщення частот, а демультиплексування – за допомогою вузькосмугового фільтру, ширина якого дорівнює ширині діапазону каналу.

Розглянемо особливості цього виду мультиплексування на прикладі телефонної мережі (рис. 2.16). На входи FDM-комутатора 1 надходять вихідні сигнали від абонентів телефонної мережі. Комутатор здійснює перенесення частоти кожного каналу в виділений каналу діапазон частот за рахунок модуляції нової несучої частоти, що належить цій смузі. Щоб низькочастотні складові сигналів різних каналів не змішувалися між собою, смуги роблять шириною в 4 кГц, а не в 3,1 кГц, залишаючи між ними проміжок в 900 Гц. У лінії зв'язку між двома FDM-комутаторами одночасно передаються сигнали всіх абонентських каналів, але кожен з них займає свою смугу частот. Такий канал називають **ущільненим.**

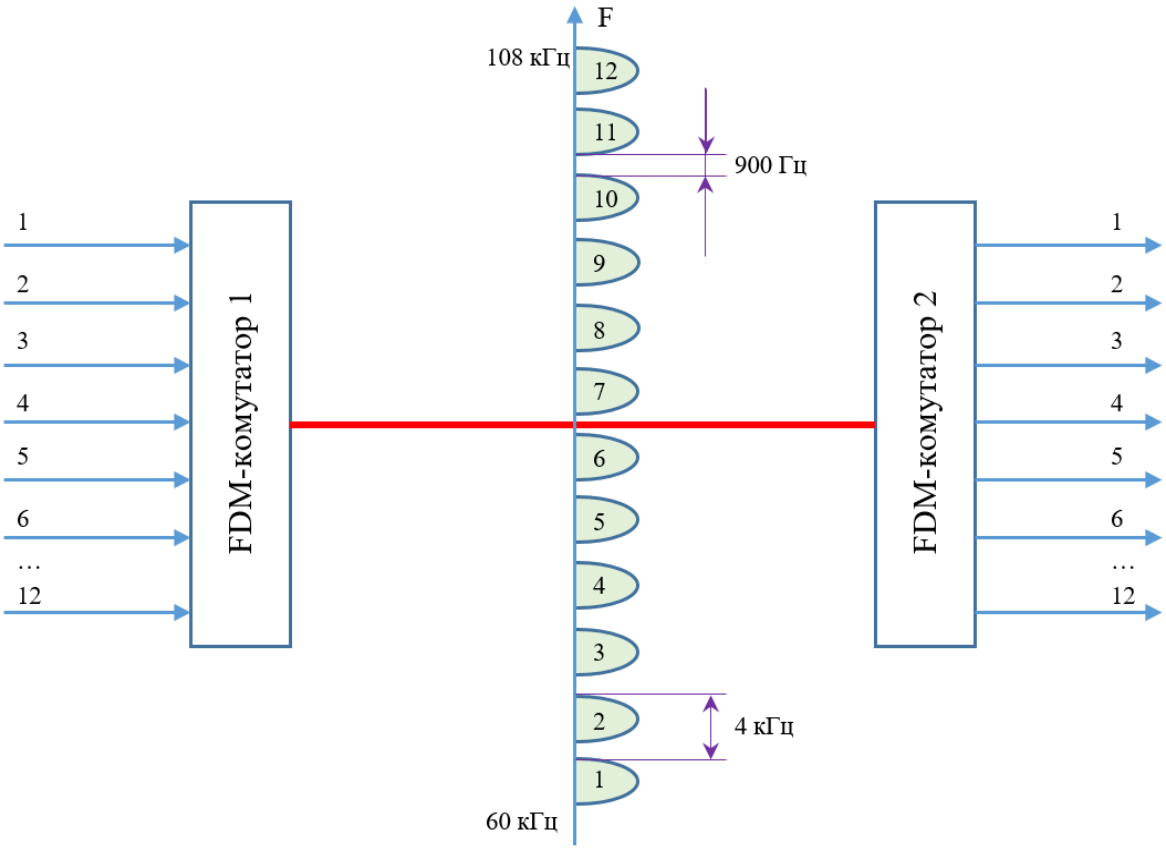



Рис. 2.16. Частотне мультиплексування

Вихідний FDM-комутатор 2 виділяє модульовані сигнали кожної несучої частоти і передає їх на відповідний вихідний канал, до якого безпосередньо підключений абонентський телефон.

У мережах на основі FDM-комутації прийнято кілька рівнів ієрархії ущільнених каналів. Перший рівень ущільнення утворюють 12 абонентських

каналів, що складають **базову групу** каналів, яка займає смугу частот шириною в 48 кГц із границями від 60 до 108 кГц (рис. 2.16). Другий рівень ущільнення утворюють 5 базових груп, що складають **супергрупу**, зі смугою частот шириною в 240 кГц і з границями від 312 до 552 кГц. Супергрупа передає дані 60 абонентських каналів тональної частоти. Десять супергруп утворюють **головну групу**, що використовується для зв'язку між комутаторами на великих відстанях. Головна група передає дані одночасно 600 абонентів і вимагає від каналу зв'язку смугу пропускання шириною 2520 кГц із границями від 564 до 3084 кГц.

FDM-комутатори можуть виконувати як динамічну, так і постійну комутацію. При **динамічної комутації** один абонент ініціює з'єднання з іншим абонентом, посилаючи в мережу номер абонента, що викликається. Комутатор динамічно виділяє даному абоненту одну з вільних смуг свого ущільненого каналу. При постійній комутації за абонентом смуга в 4 кГц закріплюється на тривалий термін шляхом налаштування комутатора адміністратором.

У методі **хвильового мультиплексування** (WDM) використовується той же принцип частотного розділення каналів, але тільки в іншій області електромагнітного спектра. Інформаційним сигналом є не електричний струм і не радіохвилі, а світло. Для організації WDM-каналів в волоконно-оптичному кабелі використовують хвилі інфрачервоного діапазону довжиною від 850 до 1565 нм, що відповідає частотам від 196 до 350 ТГц.

В системах WDM просторово розділені оптичні несучі різних довжин хвиль, які модулюються незалежними інформаційними сигналами за допомогою оптичних мультиплексорів, об'єднуються в один єдиний оптичний потік, який далі подається на оптичне волокно. На приймальній стороні використовується оптичний демультиплексор, який розділяє прийнятий оптичний пучок на спектральні складові, або **оптичні канали.**

У магістральному каналі зазвичай мультиплексується кілька спектральних каналів, причому, починаючи з 16 каналів, така техніка мультиплексування називається **ущільненим хвильовим мультиплексуванням** (Dense Wave Division Multiplexing, DWDM).

Історично першими виникли двохволоконні WDM системи, що працюють на довжинах хвиль другого і третього вікон прозорості (1310 і 1550 нм, рис. 2.6). Головною перевагою таких систем є те, що внаслідок великого спектрального рознесення повністю відсутній вплив каналів один на одного.

Сучасні WDM системи на основі стандартного частотного плану (ITU-T Rec. G.692) можна підрозділити на три групи:

- грубі WDM (Coarse WDM – CWDM) – системи з шириною каналу не менше 200 ГГц, що дають змогу мультиплексувати не більше 16 каналів;

- щільні WDM (Dense WDM – DWDM) – системи з шириною каналу не меншого 100 ГГц, що дають змогу мультиплексувати не більше 32 каналів.
- високощільні WDM (High Dense WDM – HDWDM) – системи з шириною каналів 50 Ггц і менше, що дають змогу мультиплексувати не менше 64 каналів.

По суті WDM – це реалізації ідеї частотного аналогового мультиплексування, але в іншій формі. Відмінність мереж WDM від мереж FDM полягає в граничних швидкостях передачі інформації. Якщо мережі FDM зазвичай забезпечують на магістральних каналах одночасну передачу до 600 розмов, що відповідає сумарній швидкості в 36 Мбіт/с (швидкість перерахована з розрахунку 64 Кбіт/с на одну розмова), то мережі DWDM забезпечують загальну пропускну здатність до сотень Гбіт/с і навіть кількох Тбіт/с.

### 2.4.2. Комутація каналів на основі методу TDM

FDM-комутація розроблялася в розрахунку на передачу голосових аналогових сигналів. Перехід до цифрової форми представлення голосу стимулював розробку нової техніки мультиплексування, орієнтованої на дискретний характер переданих даних – **метод часового мультиплексування** (TDM). Принцип часового мультиплексування полягає у виділенні каналу кожному з'єднанню на певний період часу. Застосовуються два типи часового мультиплексування– асинхронний і синхронний. **Асинхронний режим TDM** використовується в мережах з комутацією пакетів (комп'ютерні мережі). Кожен пакет займає канал певний час, необхідний для його передачі між кінцевими точками каналу. Між різними інформаційними потоками немає синхронізації, кожен користувач намагається зайняти канал тоді, коли у нього виникає потреба в передачі інформації.

В **синхронному режимі TDM** доступ всіх інформаційних потоків до каналу синхронізується таким чином, щоб кожен інформаційний потік періодично отримував канал в своє розпорядження на фіксований проміжок часу.

Принцип комутації каналів на основі техніки TDM при передачі голосу показано на рис. 2.16. Апаратура TDM-мереж – мультиплексори, комутатори, демультиплексори – працює в режимі поділу часу, по черзі обслуговуючи протягом циклу своєї роботи всі абонентські канали. Тривалість цикл $\boldsymbol{T}_{\text{д}}$ становить 125 мкс, що відповідає періоду проходження вимірів голосу в цифровому абонентському каналі. Кожному з'єднанню виділяється один квант часу циклу роботи апаратури, який називають **тайм-слотом**. Тривалість тайм-

слота $\tau$ залежить від числа абонентських каналів $n$, що обслуговуються мультиплексором або комутатором:

$$\tau = T_д / n$$

У мережі, показаній на рис. 2.17, шляхом комутації створено 24 канали, кожен з яких пов'язує пару абонентів. Зокрема, абонент, що під'єднаний до вхідного каналу 1, з'єднаний з абонентом, що під'єднаний до вихідного каналу 24, абонент вхідного каналу 2 з'єднаний з абонентом вихідного каналу 1, аналогічно комутуються між собою абоненти вхідного каналу 24 і вихідного каналу 2.

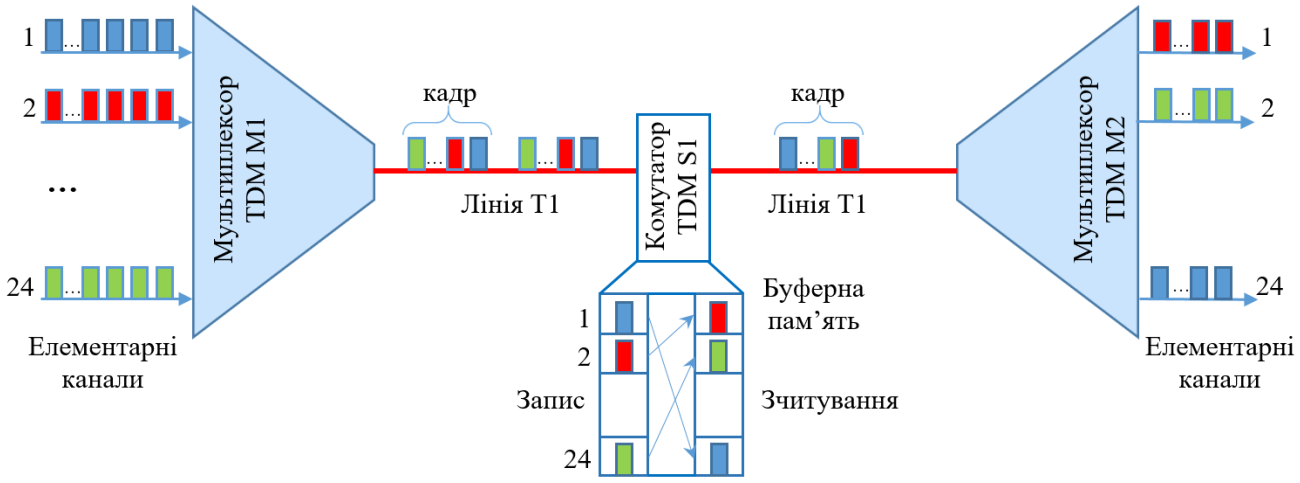



Рис. 2.17. Часове мультиплексування

Мультиплексор M1 приймає інформацію від абонентів по вхідних каналах, кожен з яких передає дані зі швидкістю 1 байт кожні 125 мкс ($T_д$ = 64 Кбіт/с). Для того, щоб упродовж цього часу передати 24 цифрові потоки зі швидкостями 64 Кбіт/с кожен, у лінії зв'язку необхідно забезпечити швидкість:

$$C = 64 \text{ Кбіт/с} \times 24 = 1{,}54 \text{ Мбіт/с}.$$

Тривалість тайм-слоту при цьому становитиме:

$$\tau = 125 \text{ мкс} / 24 = 5{,}2 \text{ мкс}.$$

Упродовж цього часу, послідовно з кожного із 24-х каналів передається 1 байт.

У кожному циклі мультиплексор виконує наступні дії:

1. Прийом від кожного каналу чергового байту даних.

2. Складання з прийнятих байтів кадру.

3. Передача кадру на вихідний канал з бітовою швидкістю, рівній 1,54 Мбіт/с.

Порядок проходження байту в кадрі відповідає номеру вхідного каналу, від якого цей байт отримано. Комутатор S1 приймає кадр зі швидкісного каналу від мультиплексора М1 і записує кожен байт з нього в окрему комірку своєї буферної пам'яті, причому в тому порядку, в якому байти були упаковані в ущільнений кадр. Для виконання комутації байти витягаються з буферної пам'яті не в порядку надходження, а в тому порядку, який відповідає підтримуваним в мережі з'єднанням абонентів. У розглянутому прикладі комутатор S1 комутує вхідні канали 1, 2 і 24 з вихідними каналами 24, 1 і 2 відповідно. Для виконання цієї операції першим з буферної пам'яті повинен бути витягнутий байт 2, другим – байт 24, а останнім – байт 1.

Мультиплексор М2 вирішує зворотну задачу – він демультиплексує байти з ущільненого кадру і комутує їх по своїх вихідних каналах, при цьому він також вважає, що порядковий номер байту в кадрі відповідає номеру вихідного каналу.

Робота TDM-обладнання нагадує роботу мереж з комутацією пакетів, так як кожен байт даних можна вважати деяким елементарним пакетом. Однак на відміну від пакета комп'ютерної мережі «пакет» TDM-мережі не має індивідуальної адреси. Його адресою є порядковий номер в кадрі або номер виділеного тайм-слота в мультиплексорі чи комутаторі. Мережі, що використовують техніку TDM, вимагають синхронної роботи всього обладнання, що і визначило другу назву цієї технології – **синхронний режим передачі** (Synchronous Transfer Mode, STM).

Порушення синхронності руйнує потрібну комутацію абонентів, так як при цьому змінюється відносне положення слота, а значить, втрачається адресна інформація. Тому оперативний перерозподіл тайм-слотів між різними каналами в TDM-обладнанні неможливий. Навіть якщо в якомусь циклі роботи мультиплексора в тайм-слоті одного з каналів в даний момент немає даних для передачі (наприклад, абонент телефонної мережі мовчить), то він передається порожнім.

Існує модифікація техніки TDM – **статистичне тимчасове мультиплексування** (Statistical TDM, STDM). Ця техніка розроблена спеціально для того, щоб за допомогою тимчасово вільних тайм-слотів одного каналу можна було збільшити пропускну здатність інших. Для вирішення цього завдання кожен байт даних доповнюється полем адреси невеликої довжини, наприклад в 4 або 5 біт, що дозволяє адресувати 16 або 32 канали. Фактично STDM є вже технікою комутації пакетів, але тільки з дуже спрощеної адресацією і вузькою областю застосування. Техніка STDM не стала популярною і використовується в

основному в нестандартному обладнанні підключення терміналів до мейнфреймів. Розвитком ідей статистичного мультиплексування стала технологія асинхронного режиму передачі (Asynchronous Transfer Mode, ATM), яка відноситься вже до комутації пакетів.

TDM-мережі можуть підтримувати режим **динамічної** або **постійної** комутації, а іноді і обидва ці режими. Основним режимом цифрових телефонних мереж, що працюють на основі технології TDM, є динамічна комутація, але вони підтримують також і постійну комутацію, надаючи своїм абонентам виділену лінію.

# 3. Первинні мережі

## 3.1. Призначення і типи первинних мереж

**Первинні мережі** займають особливе становище в світі телекомунікаційних мереж, вони призначені для гнучкого створення комутованої інфраструктури, за допомогою якої можна організовувати постійні фізичні канали з топологією «точка-точка» для інших мереж: комп'ютерних та телефонних мереж. Відповідно до семирівневої OSI моделі первинні мережі виконують функції фізичного рівня, однак на відміну від кабелів, такі мережі включають додаткове комунікаційне обладнання, яке шляхом відповідного налаштування дозволяє прокладати нові фізичні канали між кінцевими точками мережі.

Первинні мережі також називають **транспортними мережами**, оскільки вони надають лише транспортні послуги, передаючи інформацію користувача, не змінюючи її. У первинних мережах застосовується техніка комутації каналів.

Мережі, що утворені на базі первинних мереж і використовують їх канали для організації телефонного зв'язку, передавання даних (комп'ютерні мережі) або телепередач, визначені як **вторинні мережі (накладені мережі)**. Таким чином, первинна мережа – це базова телекомунікаційна мережа типових універсальних каналів передачі та мережевих трактів, на основі якої формуються і створюються вторинні мережі. Канали, що надаються первинними мережами, відрізняються високою пропускною спроможністю – зазвичай від 2 Мбіт/с до 100 Гбіт/с.

Існує кілька поколінь технологій первинних мереж:

- **плезіохронна цифрова ієрархія** (Plesiochronous Digital Hierarchy, **PDH**);
- **синхронна цифрова ієрархія** (Synchronous Digital Hierarchy, **SDH**);
- **ущільнене хвильове мультиплексування** (Dense Wave Division Multiplexing, **DWDM**);
- **оптичні транспортні мережі** (Optical Transport Network, **OTN**).

У технологіях PDH, SDH і OTN для поділу високошвидкісного каналу застосовується часове мультиплексування (TDM), а дані передаються в цифровій формі. Кожна з них підтримує ієрархію швидкостей, так що користувач може вибрати потрібну йому швидкість для каналів, за допомогою яких він буде будувати вторинну мережу.

Технології OTN і SDH забезпечують більш високі швидкості, ніж технологія PDH, так що при побудові великої первинної мережі її магістраль будується на технології OTN або SDH, а мережа доступу – на технології PDH.

Мережі DWDM не є власне цифровими мережами, так як пропонують своїм користувачам виділену світлову хвилю для передачі інформації, яку можна застосовувати для передачі інформації як в аналоговій (модулювати), так і в цифровій (кодувати) формі. Техніка мультиплексування DWDM істотно підвищила пропускну спроможність сучасних телекомунікаційних мереж, так як вона дозволяє організувати в одному оптичному волокні кілька десятків хвильових каналів, кожен з яких може переносити цифрову інформацію.

У початковий період розвитку технології DWDM хвильові канали використовувалися в основному для передачі сигналів SDH, тобто мультиплексори DWDM були одночасно і мультиплексорами SDH для кожного зі своїх хвильових каналів.

Згодом, для більш ефективного використання хвильових каналів DWDM була розроблена технологія OTN, яка дозволяє передавати по хвильових каналах сигнали будь-яких технологій, включаючи SDH, Gigabit Ethernet, 10G Ethernet і 100G Ethernet.

## 3.2. Мережі PDH

### 3.2.1. Ієрархія швидкостей

Технологія PDH – **плезіохронної цифрової ієрархії** («плезіо» означає «майже», тобто майже синхронної) – була розроблена в кінці 60-х років компанією AT&T для вирішення проблеми зв’язку великих комутаторів телефонних мереж між собою. Лінії зв’язку FDM, які застосовувалися раніше для вирішення цього завдання, вичерпали свої можливості в плані організації високошвидкісного багатоканального зв’язку по одному кабелю. В технології FDM для одночасної передачі даних 12 абонентських каналів використовувалася вита пара, а для підвищення швидкості зв’язку доводилося прокладати кабелі з великою кількістю пар проводів або дорожчі коаксіальні кабелі.

Початок технології PDH було покладено розробкою мультиплексора **T1**, який дозволяв у цифровому виді мультиплексувати, передавати і комутувати голосовий трафік 24-х абонентів. Оскільки передача голосу йшла в аналоговій формі, то мультиплексори T1 самі здійснювали оцифровування голосу з частотою 8000 Гц і кодували голос методом імпульсно-кодової модуляції. В результаті кожен абонентський канал утворював цифровий потік даних 64 Кбіт/с

(**потік нульового рівня DSO**), а мультиплексор Т1 забезпечував швидкість передавання 1,544 Мбіт/с.

Для об'єднання магістральних автоматичних телефонних станцій (АТС) канали Т1 були занадто повільні і негнучкі, тому була реалізована ідея утворення каналів з **ієрархією швидкостей**. Чотири канали типу Т1 об'єднали в канал наступного рівня цифрової ієрархії – Т2, що передає дані зі швидкістю 6,312 Мбіт/с. Канал Т3, що утворений шляхом об'єднання семи каналів Т2, має швидкість 44,736 Мбіт/с. Канал Т4 об'єднує 6 каналів Т3, в результаті його швидкість дорівнює 274 Мбіт/с. Описана технологія отримала назву **системи Т-каналів**.

З середини 70-х років виділені канали, побудовані на основі систем Т-каналів, стали здаватися телефонними компаніями в оренду на комерційних умовах, перестави бути внутрішньої технологією цих компаній. Системи Т-каналів дозволяють передавати не тільки голос, але і будь-які дані, представлені в цифровій формі: комп'ютерні дані, телевізійне зображення, факси і т. п.

Технологія систем Т-каналів була стандартизована Американським національним інститутом стандартів (ANSI), а пізніше – міжнародним телекомунікаційним союзом (ITU-T). При стандартизації вона отримала назву плезіохронної цифрової ієрархії (PDH). В результаті внесених ITU-T змін виникла несумісність американської і міжнародної версій стандарту PDH. Аналогом систем Т-каналів в міжнародному стандарті є канали типу Е1, Е2, Е3, Е4 та Е5 з відповідними швидкостями (табл. 3.1). Американська версія сьогодні крім США поширена також в Канаді і Японії (з деякими відмінностями), в Європі ж застосовується міжнародний стандарт ITU-T.

Згідно з європейським стандартом для передачі об'єднується 32 канали по 64 Кбіт/с. 30 з цих каналів використовуються для передачі даних, 2 службових канали використовуються для передачі сигналів управління і сигналізації. У Україні цей стандарт також називається ІКМ-30. Швидкість передачі даних в сумарному потоці становить 2048 Кбіт/с (2048000 біт/с).

Наступні рівні ієрархії утворюються мультиплексуванням чотирьох потоків попереднього рівня (рис. 3.1). Таким чином, швидкість передачі на наступних рівнях становить 8 Мбіт/с, 34 Мбіт/с і 140 Мбіт/с, 565 Мбіт/с. На більш високих рівнях агрегація потоків відбувається побітно, а не побайтно, як на першому рівні.

Таблиця 3.1.

Ієрархія цифрових швидкостей PDH

| Позначення швидкості | ANSI (США, Канада) | | | | ITU-T (Європа) | | | |
|---|---|---|---|---|---|---|---|---|
| | Назва каналу | Кількість голосових каналів | Кількість каналів попереднього рівня | Швидкість, Мбіт/с | Назва каналу | Кількість голосових каналів | Кількість каналів попереднього рівня | Швид-кість, Мбіт/с |
| DS0 | | 1 | 1 | 64 Кбіт/с | | 1 | 1 | 64 Кбіт/с |
| DS1 | T1 | 24 | 24 | 1,544 | E1 | 30 | 30 | 2,048 |
| DS2 | T2 | 96 | 4 | 6,312 | E2 | 120 | 4 | 8,488 |
| DS3 | T3 | 672 | 7 | 44,736 | E3 | 480 | 4 | 34,368 |
| DS4 | T4 | 4032 | 6 | 274,176 | E4 | 1920 | 4 | 139,264 |
| DS5 | | | | | E5 | 7680 | 4 | 564,992 |

Незважаючи на відмінності, в американській і міжнародній версіях PDH прийнято використовувати одні і ті ж позначення для ієрархії швидкостей – DSn (Digital Signal n). В табл. 3.1 приведено значення рівнів швидкостей обидвох технологій.

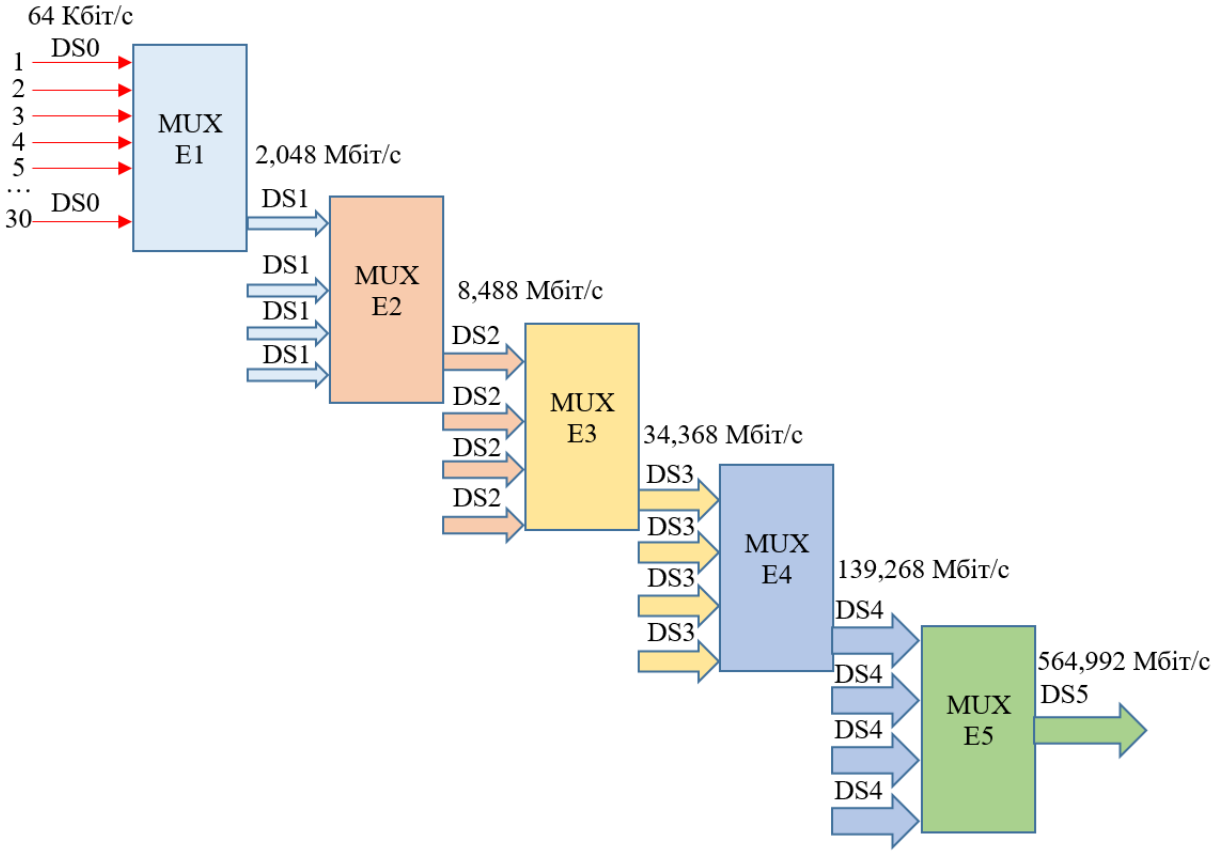



Рис. 3.1. Ієрархія швидкостей PDH

На практиці, в основному використовуються канали T1/E1 та T3/E3.

### 3.2.2. Методи мультиплексування

У кадрі мультиплексора Т1, що забезпечує передачу даних 24-х абонентів зі швидкістю 1,544 Мбіт/с, послідовно передається по одному байту кожного абонента, а після 24 байт вставляється один біт синхронізації. Спочатку пристрої Т1 функціонували лише на внутрішніх тактових генераторах, і кожен кадр за допомогою бітів синхронізації міг передаватися асинхронно. Сьогодні мультиплексори і комутатори первинної мережі PDH працюють на централізованій тактовій частоті, яка розподіляється з однієї або декількох точок мережі. Однак принцип формування кадру не змінився, тому біти синхронізації в кадрі як і раніше присутні. Сумарна швидкість абонентських каналів складає 24 х 64 = 1,536 Мбіт/с, а ще 8 Кбіт/с додають біти синхронізації, разом виходить 1,544 Мбіт/с.

В апаратурі Т1 восьмий біт кожного байту в кадрі має значення, що залежить від типу даних і покоління апаратури. При передачі голосу за допомогою цього біту переноситься службова інформація, до якої відносяться номер абонента, що викликається і інші відомості, необхідні для встановлення з'єднання між абонентами мережі. Протокол, що забезпечує таке з'єднання, називається в телефонії **сигнальним протоколом**. Тому реальна швидкість передачі даних користувача в цьому випадку становить не 64, а 56 Кбіт/с. Техніка застосування восьмого біта для службових цілей отримала назву **«крадіжки біта».**

При передачі комп'ютерних даних канал Т1 надає для передавання даних користувача лише 23 канали, а 24-й канал відводиться для службових цілей, в основному – для відновлення спотворених кадрів. Комп'ютерні дані передаються зі швидкістю 64 Кбіт/с, так як восьмий біт не «крадеться». При одночасній передачі як голосових, так і комп'ютерних даних використовуються всі 24 канали, причому і комп'ютерні, і голосові дані передаються зі швидкістю 56 Кбіт/с.

У європейській версії технології PDH не використовується схема «крадіжки біта». При переході до наступного рівня ієрархії коефіцієнт кратності швидкості має постійне значення 4. Замість восьмого біту в каналі Е1 на службові цілі відводяться 2 байти із 32, а саме нульовий (для цілей синхронізації приймача і передавача) і шістнадцятий (в ньому передається службова сигнальна інформація). Для телефонії чи комп'ютерних даних залишається 30 каналів зі швидкістю передачі 64 Кбіт/с кожен.

При мультиплексуванні декількох потоків в мультиплексорах PDH застосовується біт-стаффінг (stuff – усяка всячина, заповнювач) з побітною синхронізацією. До цієї техніки вдаються, коли швидкість користувацького

потоку виявляється дещо меншою, ніж швидкість об'єднаного потоку – подібні проблеми можуть виникати в мережі, що складається з великої кількості мультиплексорів, незважаючи на всі зусилля з централізованого синхронізації вузлів мережі. В результаті мультиплексор PDH періодично стикається з ситуацією, коли йому «не вистачає» біта для представлення в об'єднаному потоці певного користувацького потоку. В цьому випадку мультиплексор просто вставляє в об'єднаний потік біт-вставку і відзначає цей факт у службових бітах об'єднаного кадру. При демультиплексуванні об'єднаного потоку біт-вставка видаляється з користувацького потоку. Техніка біт-стаффіну застосовується як в європейській, так і в американській версіях PDH.

Відсутність повної синхронності потоків даних при об'єднанні низькошвидкісних каналів в високошвидкісні і дало назву технології PDH («майже синхронний»).

### 3.2.3. Синхронізація мереж PDH

У разі невеликої мережі PDH, наприклад мережі міста, синхронізацію всіх пристроїв мережі з однієї точки здійснити не складно. Однак для більш великих мереж, наприклад мереж масштабу країни, які складаються з певної кількості регіональних мереж, синхронізація всіх пристроїв мережі являє собою складну задачу. Загальний підхід до вирішення цієї проблеми описано в стандарті ITU-T G.810. Він полягає в організації в мережі ієрархії еталонних джерел синхросигналів, а також системи розподілу синхросигналів по всіх вузлах мережі.

Кожна велика мережа повинна мати хоча б один **первинний еталонний генератор синхросигналів** (у варіанті ITU-T називають Primary Reference Clock, **PRC**, а у варіанті ANSI – генератор рівня **Stratum 1**). Це дуже точне джерело синхросигналів, здатне виробляти синхросигнали з відносною точністю частоти не гірше $10^{-11}$. На практиці в якості PRC використовують або автономний атомний (водневий або цезієвий) годинник, або годинник, що синхронізується від супутникових систем точного світового часу, наприклад GPS. Зазвичай точність PRC досягає $10^{-13}$.

Стандартним синхросигналом є сигнал тактової частоти рівня DS1: 2048 кГц – частота для міжнародного варіанту стандарту PDH і 1544 кГц – для американського варіанту стандарту.

Для синхронізації немагістральних вузлів використовується **вторинний генератор синхросигналів** (у варіанті ITU-T називають Secondary Reference Clock, SRC, а у варіанті ANSI – генератор рівня **Stratum 2**). SRC працює в режимі примусової синхронізації, будучи веденим таймером в парі PRC – SRC. Зазвичай

SRC отримує синхросигнали від деякого PRC через проміжні магістральні вузли мережі, при цьому для передачі синхросигналів використовуються біти службових байтів кадру, наприклад нульового байту кадру E1.

Точність SRC менше, ніж точність PRC: ITU-T в стандарті G.812 визначає її як «не гірше $10^{-9}$», а точність генераторів Stratum 2 повинна бути не «гірше $1{,}6 \times 10^{-8}$».

Якщо є необхідність, то ієрархія еталонних генераторів може бути продовжена, при цьому точність кожного нижчого рівня знижується. Генератори нижніх рівнів, починаючи від SRC, можуть використовувати для генерування своїх синхросигналів кілька еталонних генераторів більш високого рівня, але при цьому в кожен момент часу один з них повинен бути основним, а решта – резервними; така побудова системи синхронізації забезпечує її відмовостійкість. Однак в цьому випадку потрібно пріоритезувати сигнали генераторів більш високих рівнів. Крім того, при побудові системи синхронізації потрібно гарантувати відсутність петель синхронізації.

Розглянуті методи синхронізації цифрових мереж можуть бути застосовані не тільки до мереж PDH, а й до інших мереж, що працюють на основі синхронного TDM-мультиплексування, наприклад до мереж SDH, а також до мереж цифрових телефонних комутаторів.

### 3.2.4. Обмеження технології PDH

Технологія PDH володіє рядом недоліків, основним з яких є складність і неефективність операцій мультиплексування і демультиплексування користувацьких даних. Застосування техніки біт-стаффінгу для вирівнювання швидкостей потоків призводить до того, що для вилучення користувацьких даних з об’єднаного каналу необхідно повністю демультиплексувати кадри об’єднаного каналу.

Наприклад, щоб отримати дані одного абонентського каналу 64 Кбіт/с з кадрів каналу E4, потрібно зробити демультиплексування цих кадрів до рівня кадрів E3, потім – до рівня кадрів E2, далі – до E1, а в кінці демультиплексувати і самі кадри E1 (рис. 3.2).

Якщо мережа PDH використовується тільки в якості транзитної магістралі між двома вузлами, то операції мультиплексування і демультиплексування виконуються виключно в кінцевих вузлах, і проблем не виникає. Але якщо необхідно виділити один або кілька абонентських каналів в проміжному вузлі мережі PDH, то це завдання простого рішення не має. Як варіант, пропонується встановлення пари мультиплексорів рівня E1 і вище в кожному вузлі мережі (рис. 3.2). Один забезпечуватиме повне демультиплексування потоку і

відведення частини низькошвидкісних каналів абонентам, інший – знову поєднуватиме в вихідний високошвидкісний потік канали, що залишилися разом з новоутвореними. При цьому значно збільшується кількість працюючого обладнання. Інший варіант – «зворотна доставка». У проміжному вузлі, де потрібно виділити і відвести абонентський потік, встановлюється єдиний високошвидкісний мультиплексор, який просто передає дані транзитом далі по мережі без їх демультиплексування. Цю операцію виконує тільки мультиплексор кінцевого вузла, після чого дані відповідного абонента повертаються по окремій лінії зв'язку в проміжний вузол. Такі складні взаємини комутаторів ускладнюють роботу мережі, вимагають її тонкого конфігурування, що веде до великого обсягу ручної роботи і помилок.

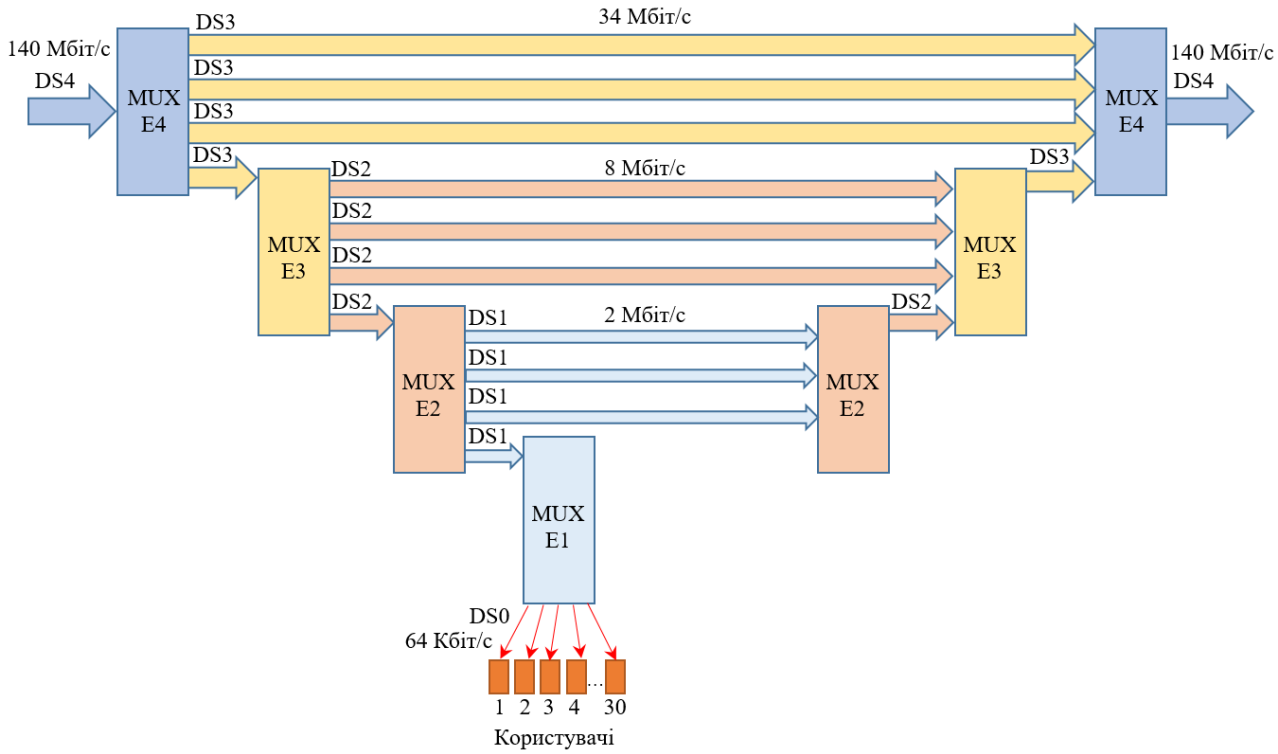



Рис. 3.2. Виділення абонентського каналу в технології PDH

В технології PDH не передбачені вбудовані засоби забезпечення відмовостійкості і адміністрування мережі. І ще одним недоліком PDH є занадто низькі за сучасними поняттями швидкості передавання даних. Волоконно-оптичні кабелі дозволяють передавати дані зі швидкостями в декілька сотень Гбіт/с по одному волокну, що забезпечує консолідацію в одному кабелі десятків тисяч користувацьких каналів, але цю можливість технологія PDH не реалізує – її ієрархія швидкостей закінчується рівнем 560 Мбіт/с.

## 3.3. Мережі SDH

### 3.3.1. Ієрархія швидкостей SDH

Характерні для технології PDH недоліки були враховані і подолані розробниками технології **синхронних оптичних мереж** (Synchronous Optical NET, **SONET**), перший варіант стандарту якої з'явився в 1984 році. Міжнародна стандартизація технології проходила під егідою Європейського інституту телекомунікаційних стандартів (European Telecommunications Standards Institute, ETSI) і сектором телекомунікаційної стандартизації союзу ITU (ITU Telecommunication Standardization Sector, ITU-T) спільно з ANSI. Основною метою розробників міжнародного стандарту було створення технології, здатної передавати трафік всіх існуючих цифрових каналів рівня PDH (як американських Т-каналів, так і європейських Е-каналів) по високошвидкісній магістральній мережі на базі волоконно-оптичних кабелів і забезпечити ієрархію швидкостей, яка продовжує ієрархію технології PDH до швидкостей в десятки Гбіт/с. В результаті вдалося підготувати міжнародний стандарт **SDH** (Synchronous Digital Hierarchy – синхронна цифрова ієрархія). Крім того, стандарт SONET був доопрацьований так, щоб апаратура і мережі SDH і SONET були сумісними і могли мультиплексувати вхідні потоки практично будь-якого стандарту PDH.

Підтримувана технологією SDH/SONET ієрархія швидкостей представлена в табл. 3.2.

Таблиця 3.2.

Ієрархія швидкостей SDH/SONET

| SDH | SONET | Швидкість |
|---|---|---|
| | STS-1, OC-1 | 51,84 Мбіт/с |
| STM-1 | STS-3, OC-3 | 155,520 Мбіт/с |
| STM-3 | OC-9 | 466,560 Мбіт/с |
| STM-4 | OC-12 | 622,080 Мбіт/с |
| STM-6 | OC-18 | 933,120 Мбіт/с |
| STM-8 | OC-24 | 1,244 Гбіт/с |
| STM-12 | OC-36 | 1,866 Гбіт/с |
| STM-16 | OC-48 | 2,488 Гбіт/с |
| STM-64 | OC-192 | 9,953 Гбіт/с |
| STM-256 | OC-768 | 39,81 Гбіт/с |

У стандарті SDH всі рівні швидкостей (і, відповідно, формати кадрів для цих рівнів) мають загальну назву STM-N (Synchronous Transport Module level

N – **синхронний транспортний модуль** рівня N). В технології SONET існує два позначення для рівнів швидкостей: назва STS-N (Synchronous Transport Signal level N – **синхронний транспортний сигнал** рівня N) вживається в разі передачі даних електричним сигналом, а назва OC-N (Optical Carrier level N – **оптоволоконна лінія зв'язку** рівня N) використовують у разі передачі даних по волоконно-оптичному кабелю.

**Модулі STM-N** мають досить складну структуру, що дозволяє агрегувати в загальний магістральний потік потоки SDH і PDH різних швидкостей, а також виконувати операції вводу-виводу без повного демультиплексування магістрального потоку.

### 3.3.2. Структура модулів SDH

Для транспортування цифрового потоку зі швидкістю 155 Мбіт/с створюється синхронний транспортний модуль STM-1. Його спрощена структура показана на рис. 3.3. Модуль являє собою фрейм (рамку) 9 × 270 = 2430 байт. Крім **корисного навантаження** (користувацькі дані), він містить в 4-му рядку **вказівник** (Pointer, **PTR**), який визначає розміщення користувацьких даних.

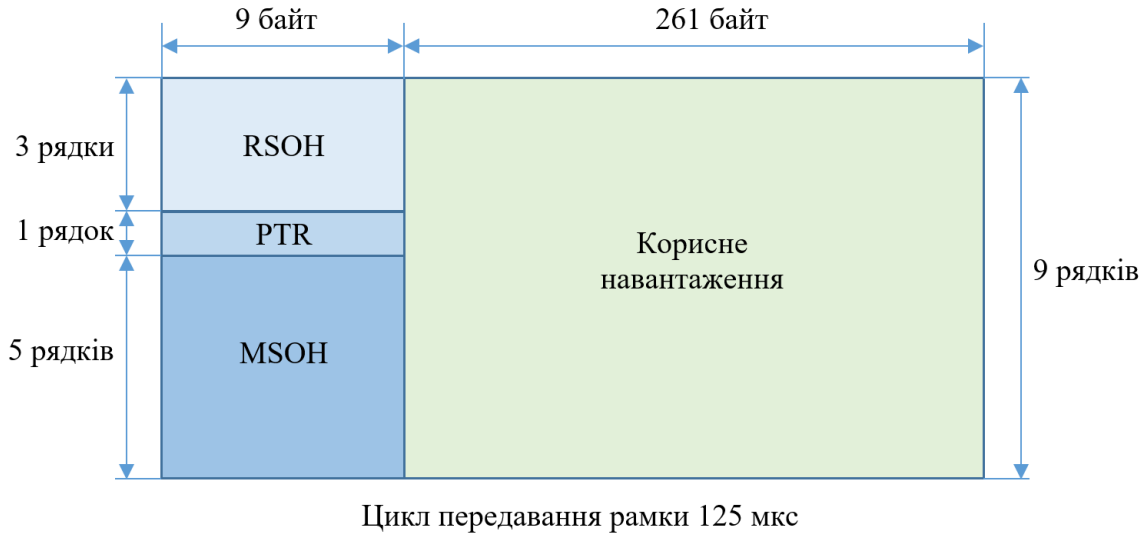



Рис. 3.3. Структура синхронного транспортний модуль STM-1.

Щоб визначити маршрут транспортного модуля, в лівій частині рамки записується секційний заголовок (Section Over Head – **SOH**). Нижні 5×9 = 45 байтів (після вказівника) відповідають за доставку інформації в те місце мережі (до того мультиплексора), де цей транспортний модуль буде переформовуватися. Дана частина заголовка так і називається: заголовок мультиплексної секції (Multiplex SOH, **MSOH**). Верхні 3×9 = 27 байтів (до вказівника) являють собою

заголовок регенераційної секції (Regenerator SOH, **RSOH**), де буде здійснюватися відновлення потоку, «пошкодженого» завадами, і виправлення помилок в ньому.

Один цикл передачі включає в себе зчитування в лінію такого модуля. Порядок передачі байтів – зліва направо, зверху вниз (так само, як при читанні тексту на сторінці). Тривалість циклу передачі STM-1 становить 125 мкс, тобто він повторюється з частотою 8 кГц. Кожна комірка відповідає швидкості передачі 8 біт × 8 кГц = 64 Кбіт/с.

Отже, якщо витрачати на передачу в лінію зв'язку кожного модуля 125 мкс, то за секунду в лінію буде передано 9 × 270 × 64 Кбіт/с = 155520 Кбіт/с, тобто 155 Мбіт/с.

Для створення більш потужних цифрових потоків в формується наступна швидкісна ієрархія (табл. 3.2): 4 модуля STM-1 об'єднуються шляхом побайтового мультиплексування в модуль STM-4, передаючи зі швидкістю 622,080 Мбіт/с; потім 4 модулі STM-4 об'єднуються в модуль STM-16 зі швидкістю передачі 2488,320 Мбіт/с і т. д.

У мережі SDH використовують принцип **контейнерних перевезень.** Цифрові канали (потоки) PDH є вхідними (корисним навантаженням) для транспортної мережі SDH. Усі ці потоки передаються (транспортуються) по трактах транспортної мережі у вигляді інформаційних структур – **віртуальних контейнерів (VC)** відповідного рівня. В технології SDH визначено кілька типів віртуальних контейнерів, призначених для транспортування основних типів блоків даних PDH: VC-11 (1,5 Мбіт/с), VC-12 (2 Мбіт/с), VC-2 (6 Мбіт/с), VC-3 (34/45 Мбіт/с) і VC-4 (140 Мбіт/с).

Дані, які підлягають транспортуванню, попередньо розміщуються в **контейнерах** (Container, **C**). Всі операції з контейнерами здійснюються незалежно від їх змісту, чим і досягається прозорість мережі SDH, тобто здатність транспортувати різні дані, зокрема, потоки PDH.

На рис. 3.4 показана схема формування структур модуля STM-1.

Сигнал PDH «поміщається» в стандартний **контейнер** (Container, **C**). До кожного C додається **трактовий або маршрутний заголовок** (Path Over Head, **POH**) і таким чином, формується **віртуальний контейнер** (Virtual Container, **VC**). Залежно від розміру, віртуальний контейнер може транспортуватися в модулі STM-1 поодиноко або може бути об'єднаний в **трибутарний блок** (Tributary Unit, **TU**). Розрізняють **віртуальні контейнери вищого рівня** (High-order, **HO**) і **віртуальні контейнери нижчого рівня** (Low-order, **LO**). Всі контейнери, що передаються в складі TU відносяться до LO. Контейнерами рівня LO є VC-11, VC-12 і VC-2. VC-3 відносять до рівня LO, якщо цей контейнер передається в складі VC-4. Контейнери, які безпосередньо переносяться в модулі

STM-1, відносяться до рівня HO. VC-4 – контейнер рівня HO. Те саме можна сказати і до VC-3, якщо він передається безпосередньо.

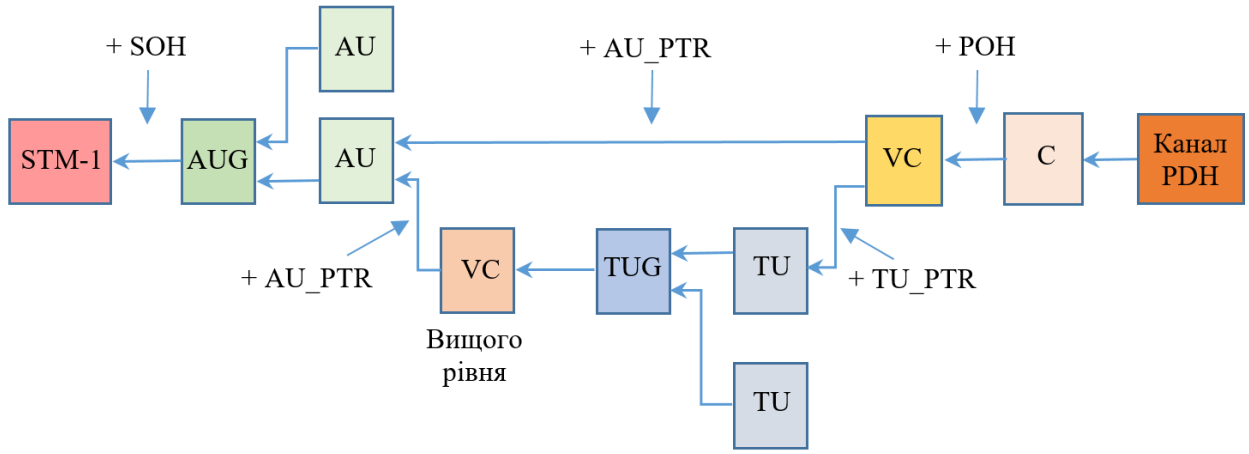



Рис. 3.4 Схема формування структур модуля STM-1

Для відображення розміщення VC в межах TU використовуються **вказівники трибутарного блоку** (Tributary Unit Pointer, **TU_PTR**), що поміщаються в фіксованому місці VC вищого рівня. Перед об'єднанням у віртуальний контейнер вищого рівня (VC-4 або VC-3), кілька TU побайтно об'єднуються в **групи трибутарних блоків** (Tributary Unit Group, **TUG**).

Віртуальні контейнери вищого рівня VC-4 і VC-3, за допомогою **вказівників адміністративного блоку** (Administrative Unit Pointer, **AU_PTR**) трансформуються у **адміністративні блоки** (Administrative Unit, **AU**). Кілька AU можуть бути побайтно об'єднані в **адміністративну групу** (Administrative Unit Group, **AUG**). AUG може складатися з одного AU-4 або трьох AU-3. Для отримання STM-1 до AUG добавляють секційні заголовки SOH.

Найбільш близьким за швидкістю до першого рівня ієрархії SDH (155, 520 Мбіт/с) є цифровий потік E4 (140 Мбіт/с) мережі PDH. Його найпростіше розмістити в модулі STM-1 (рис. 3.5). Для цього вхідний канал E4 спочатку «поміщають» в контейнер (тобто розміщують на певних позиціях його циклу), який позначається C-4. Рамка контейнера C-4 містить 9 рядків і 260 однобайтових стовпців. Додаванням зліва ще одного стовпця – заголовку шляху (POH) – цей контейнер перетвориться у VC-4. Нарешті, щоб помістити віртуальний контейнер VC-4 в модуль STM-1, його доповнюють вказівником AU_PTR, утворюючи таким чином адміністративний блок AU-4, який безпосередньо поміщають в модуль STM-1 разом з секційним заголовком SOH.

Синхронний транспортний модуль STM-1 можна завантажити і плезіохронними потоками E1 (2 Мбіт/с). Для початкової «упаковки» використовується контейнер C-12. Дані розміщуються у певних позиціях цього

контейнера. Шляхом додавання маршрутного або транспортного заголовку (РОН) утворюється віртуальний контейнер VC-12. Віртуальні контейнери формуються і розформовуються в точках закінченнях трактів.

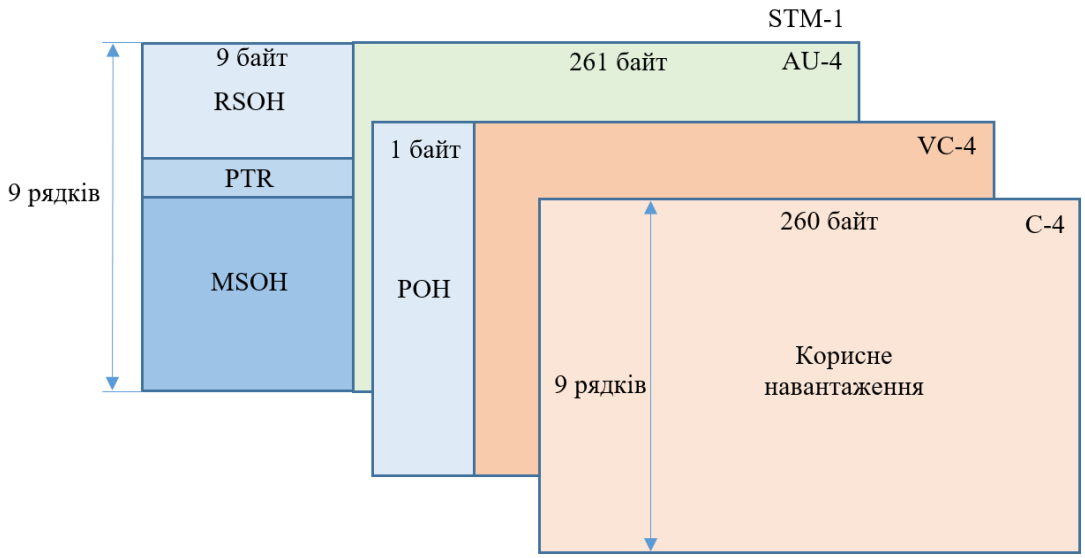



Рис. 3.5. Розміщення контейнера С-4 в модулі STM-1

У модулі STM-1 можна розмістити 63 віртуальних контейнера VC-12 (рис. 3.6). Віртуальний контейнер VC-12 доповнюється вказівником TU_PTR і утворює тим самим трибутарний блок TU-12. Далі цифрові потоки різних трибутарних блоків можна об’єднувати в цифровий потік 155 Мбіт/с. Спочатку три трибутарних блоки TU-12 шляхом мультиплексування об’єднують у групу трибутарних блоків TUG-2, потім сім груп TUG-2 мультиплексують у групу трибутарних блоків TUG-3, а три групи TUG-3 об’єднують разом і поміщають в віртуальний контейнер VC-4. Далі шлях перетворень відомий.

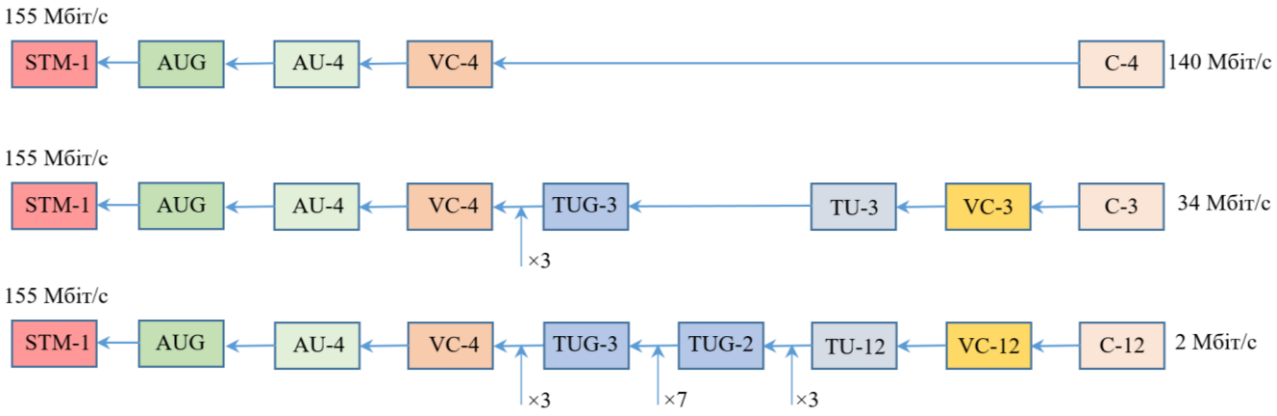



Рис. 3.6. Варіанти введення потоків PDH в модуль STM-1

Схема мультиплексування SDH надає різноманітні можливості по

об’єднанню потоків PDH (рис. 3.7). Наприклад, для кадру STM-1 можна реалізувати такі варіанти:

- 1 потік E4;
- 63 потоки E1;
- 1 потік E3 і 42 потоки E1 і т. д.

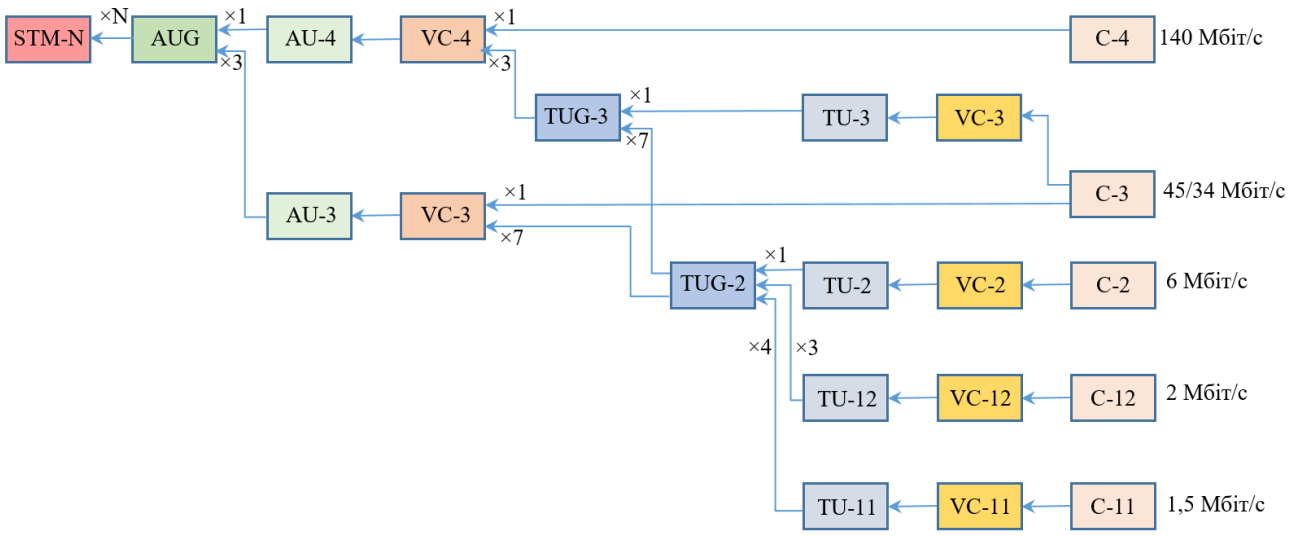



Рис. 3.7. Загальна схема мультиплексування потоків PDH в SDH

### 3.3.3. Апаратура мереж SDH

Основним елементом мережі SDH є мультиплексор (рис. 3.8). Зазвичай, він оснащений деякою кількістю портів PDH і SDH: наприклад, портами PDH на 2 і 34/45 Мбіт/с і портами SDH STM-1 на 155 Мбіт/с і STM-4 на 622 Мбіт/с. Порти мультиплексора SDH діляться на трибутарні та агрегатні.

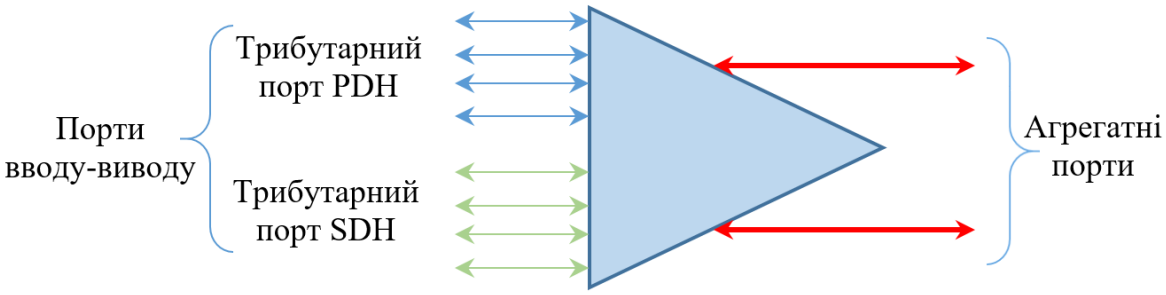



Рис. 3.8. Мультиплексор SDH

**Трибутарні порти** часто називають також портами вводу-виводу, а **агрегатні** – лінійними портами.

Мультиплексори SDH зазвичай поділяють на два типи, різниця між якими визначається положенням мультиплексора в мережі SDH (рис. 3.9).

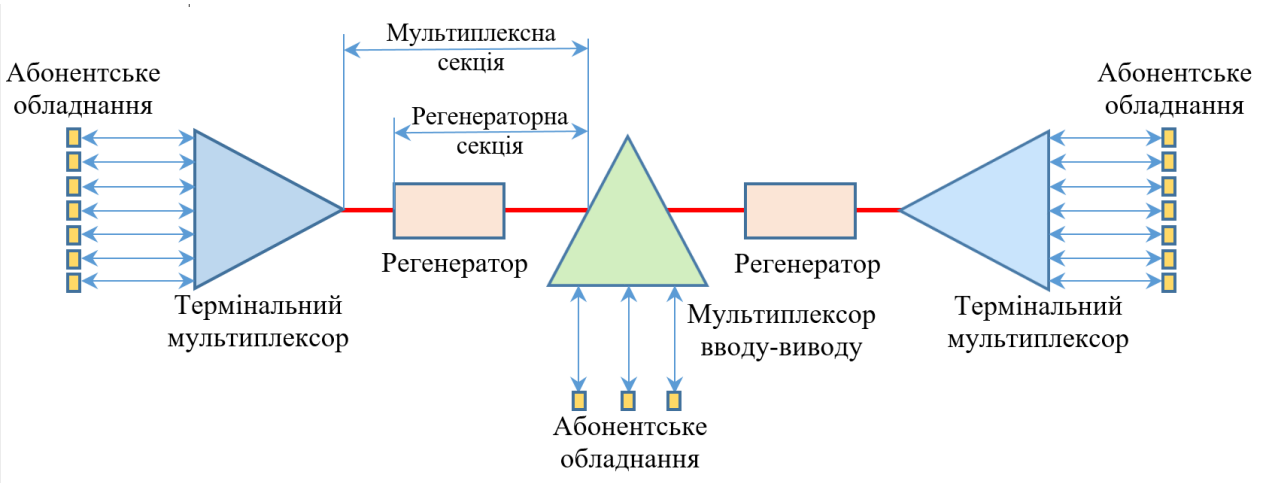



Рис. 3.9. Типи мультиплексорів SDH

**Термінальний мультиплексор** (Terminal Multiplexer, **TM**) завершує агрегатний канал, мультиплексуючи в ньому велику кількість трибутарних каналів, тому він містить один агрегатний і велику кількість трибутарних портів.

**Мультиплексор вводу-виводу** (Add-Drop Multiplexer, **ADM**) займає проміжне положення на магістралі (в кільці, ланцюгу або змішаної топології). Він має два агрегатних порти, через які транзитом передає агрегований потік даних. За допомогою невеликої кількості трибутарних портів такий мультиплексор вводить в агрегатний потік або виводить з нього дані трибутарних каналів.

Іноді також виділяють мультиплексори, які виконують операції комутації над довільними віртуальними контейнерами – **цифрові крос-конектори** (Digital Cross-Connect, **DXC**). У таких мультиплексорах не робиться відмінностей між агрегатними і трибутарних портами, так як вони призначені для роботи в комірчастій топології, де виділити агрегатні потоки неможливо.

Окрім мультиплексорів, до складу мережі SDH можуть входити **регенератори сигналів**, які необхідні для подолання обмежень по відстані між мультиплексорами. Ці обмеження залежать від потужності оптичних передавачів, чутливості приймачів і загасання волоконно-оптичного кабелю. Регенератор перетворює оптичний сигнал в електричний і назад, при цьому відновлюється форма сигналу і його тимчасові характеристики. В даний час регенератори SDH застосовуються досить рідко, так як вартість їх не набагато нижче вартості мультиплексора, а функціональні можливості незрівнянно бідніше.

**Регенераторною секцією** в технології SDH називається кожен

безперервний відрізок волоконно-оптичного кабелю, який з'єднує між собою такі, наприклад, пари пристроїв SDH, як мультиплексор і регенератор, регенератор і регенератор, але не два мультиплексора.

**Мультиплексною секцією** в технології SDH називається відрізок лінії, який відповідає за передачу даних між двома мультиплексорами мережі.

### 3.3.4. Топології мереж SDH

У мережах SDH застосовуються різні топології зв'язків. Найбільш часто використовуються кільця і лінійні ланцюги мультиплексорів, також знаходить все більше застосування комірчаста топологія мережі, яка близька до повнозв'язної.

**Кільце SDH** будується з мультиплексорів вводу-виводу, що мають, принаймні, по два агрегатних порти (рис. 3.10, а). Абонентські потоки вводяться в кільце і виводяться з кільця через трибутарні порти, утворюючи з'єднання «точка-точка. Кільце є класичною регулярною топологією, що володіє потенційною відмовостійкістю – при одноразовому обриві кабелю або виході з ладу мультиплексора з'єднання збережеться, якщо його направити по кільцю в протилежному напрямку. Кільце, зазвичай, будується на основі кабелю з двома оптичними волокнами, але іноді для підвищення надійності та пропускної спроможності застосовують чотири волокна.

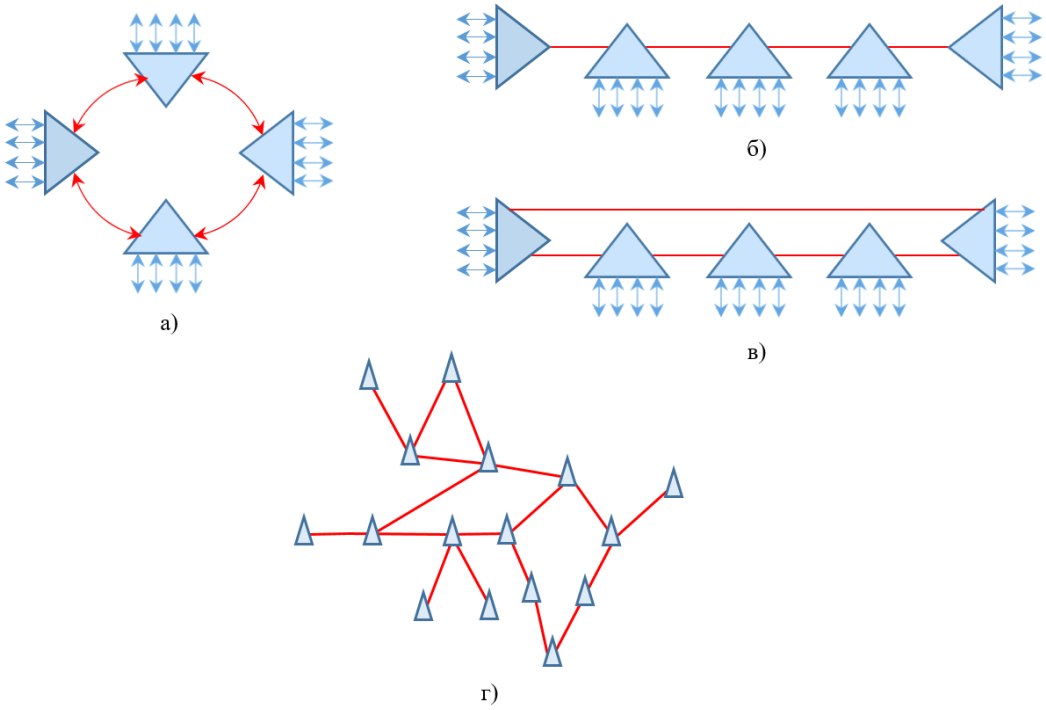



Рис. 3.10. Топології мереж SDH

**Ланцюг** (рис. 3.10, б) – це лінійна послідовність мультиплексорів, з яких два кінцевих відіграють роль термінальних мультиплексорів, інші – мультиплексорів вводу-виводу. Зазвичай, мережу з топологією ланцюга застосовується в тих випадках, коли вузли мають відповідне географічне розташування, наприклад уздовж магістралі залізниці або трубопроводу. Правда, в таких випадках може застосовуватися і **плоске кільце** (рис. 3.10, в), що забезпечує більш високий рівень відмовостійкості за рахунок двох додаткових волокон в магістральному кабелі і по одному додатковому агрегатному порту у термінальних мультиплексорів.

Ці базові топології можуть комбінуватися при побудові складної і розгалуженої мережі SDH, утворюючи ділянки з радіально-кільцевої топологією. Найбільш загальним випадком є повнозв'язна (mesh) топологія (рис. 3.10, г), при якій мультиплексори з'єднуються один з одним великою кількістю зв'язків, за рахунок чого мережа може досягти дуже високого ступеня продуктивності і надійності.

### 3.3.5. Нове покоління протоколів SDH

Спочатку технологія SDH була орієнтована на передачу елементарних потоків голосового трафіку, звідси і її орієнтація на мультиплексування абонентських потоків зі швидкостями, кратними 64 Кбіт/с.

Однак популярність Інтернету змінила ситуацію в телекомунікаційному світі, і сьогодні обсяги комп'ютерного трафіку в первинних мережах перевершують обсяги голосового трафіку. В умовах домінування Ethernet, майже весь комп'ютерний трафік, що надходить на входи мультиплексорів первинних мереж, являє собою кадри Ethernet, а значить, представлений ієрархією швидкостей 10 – 100 Мбіт/с та 1 – 10 -100 Гбіт/с. Користувацькі потоки з такими швидкостями не дуже ефективно вкладаються у віртуальні контейнери SDH, розраховані на вирішення інших завдань.

Для виправлення ситуації організація ITU-T розробила кілька стандартів, які складають так звану **технологію SDH нового покоління** (SDH Next Generation, або **SDH NG**). Ці стандарти роблять технологію SDH більш орієнтовану до комп'ютерних даних.

Стандарти SDH нового покоління описують три нових механізми:

- віртуальна конкатенація (VCAT);
- схема динамічної зміни пропускної спроможності лінії (LCAS);
- загальна процедура інкапсуляції (кадрування) даних (GFP).

**Віртуальна конкатенація** (Virtual Concatenation, **VCAT**) контейнерів

дозволяє більш ефективно використовувати ємність віртуальних контейнерів SDH при передачі трафіку Ethernet. Віртуальна конкатенація дозволяє об'єднати кілька контейнерів в один віртуальний конкатенований контейнер з більш високою швидкістю передачі даних. При цьому об'єднуючі контейнери повинні бути одного типу, наприклад лише VC-3 або лише VC-12.

Коефіцієнт кратності при об'єднанні контейнерів може побути будь-яким, від 1 до максимального числа, що визначається ємністю кадру STM-N, який застосовується для передачі об'єднаного контейнера. При віртуальної конкатенації об'єднаний контейнер позначається як VC-N-Mv, де N – тип віртуального контейнера, а M – кратність його використання.

Наприклад, щоб передавати один потік Fast Ethernet 100 Мбіт/с, в мережі STM-4 можна застосувати віртуальну конкатенацію контейнерів VC-12. Цей тип контейнера забезпечує передачу даних зі швидкістю 2,176 Мбіт/с, тому, об'єднавши 46 таких контейнерів, тобто застосувавши віртуальну конкатенацію VC-12-46v, можна створити канал з пропускною спроможністю 100,096 Мбіт/с. Решта 206 контейнерів VC-12 (кадр STM-4 вміщує 63 × 4 = 252 контейнера VC-12) можна задіяти як для передачі інших потоків Fast Ethernet, так і для передачі голосового трафіку.

Назва «віртуальна конкатенація» відображає той факт, що тільки кінцеві мультиплексори (тобто той мультиплексор, який формує об'єднаний контейнер з абонентських потоків, і той мультиплексор, який його демультиплексує в абонентські потоки) повинні розуміти, що це конкатенований контейнер. Всі проміжні мультиплексори мережі SDH розглядають складові віртуальні контейнери як незалежні і можуть передавати їх до кінцевого мультиплексора за різними маршрутами. Кінцевий мультиплексор витримує деякий тайм-аут перед демультиплексування абонентських потоків, що може бути необхідно для прибуття всіх складових контейнерів, в тому випадку, коли вони передаються по різних маршрутах.

**Схема динамічної зміни пропускної спроможності лінії** (Link Capacity Adjustment Scheme, LCAS) є доповненням до механізму віртуальної конкатенації. Ця схема дозволяє вихідному мультиплексору, тобто тому, який формує об'єднаний контейнер, динамічно змінювати його ємність, приєднуючи до нього або від'єднуючи від нього віртуальні контейнери. Для того, щоб досягнути потрібного ефекту, вихідний мультиплексор посилає кінцевому мультиплексору спеціальне службове повідомлення, що повідомляє про зміну складу об'єднаного контейнера.

**Загальна процедура інкапсуляції даних** (Generic Framing Procedure, GFP) призначена для упаковки кадрів різних протоколів комп'ютерних мереж в кадр єдиного формату і передачі його по мережі SDH. Така процедура корисна,

так як вона вирішує кілька завдань при передачі даних комп'ютерних мереж через мережі SDH. У ці завдання входять вирівнювання швидкості комп'ютерного протоколу зі швидкістю віртуального контейнера SDH, що використовується для передачі комп'ютерних даних, а також розпізнавання початку кадру.

- *Вирівнювання швидкості комп'ютерного протоколу і швидкості віртуального контейнера SDH, використовуваного для передачі комп'ютерних даних*. Наприклад, якщо застосувати об'єднаний контейнер VC-12-46v для передачі кадрів Fast Ethernet, то потрібно вирівняти швидкості 100 і 100,096 Мбіт/с. Процедура GFP підтримує два режими роботи: **GFP-F** (кадровий режим, або Frame Mode) і **GFP-T** (прозорий режим, або Transparent Mode). У режимі GFP-F проблема вирівнювання швидкостей вирішується звичним для комп'ютерних мереж способом – вхідний кадр повністю буферизується, упаковується в формат GFP, а потім зі швидкістю з'єднання SDH передається через мережу. Режим GFP-T призначений для чутливого до затримок трафіку, в цьому режимі кадр повністю не буферизується, а побітно, по мірі надходження передається в мережу SDH (попередньо забезпечений службовими полями GFP). Для вирівнювання швидкостей в режимі GFP-T застосовуються спеціальні службові «порожні» кадри GFP, які надсилаються в ті моменти, коли неузгодженість призводить до відсутності призначених для користувача бітів у вихідного мультиплексора SDH. В розглянутому прикладі в режимі GFP-T такі кадри будуть посилатись, так як швидкість мережі SDH трохи вища, ніж швидкість надходження даних від клієнта Fast Ethernet.
- *Розпізнавання початку кадру*. З'єднання SDH являє для користувача потік бітів, розбитий на кадри SDH, початок яких ніяк не пов'язане з початком кадру користувача. Процедура GFP дозволяє приймаючому мультиплексору SDH розпізнати початок кожного користувцького кадру, що необхідно для його вилучення з потоку бітів, перевірки його коректності та передачі на вихідний інтерфейс в мережу користувача. У процедурі GFP для розпізнавання початку кадру служить його власний заголовок, який складається з поля довжини розміром в два байти і поля контрольної суми поля довжини також розміром в два байти.

## 3.4. Мережі DWDM

### 3.4.1. Принцип роботи

Технологія **ущільненого хвильового мультиплексування** (Dense Wave Division Multiplexing, **DWDM**) призначена для створення оптичних магістралей нового покоління, що працюють на мультигігабітних і терабітних швидкостях.

Сьогодні обладнання DWDM дозволяє передавати по одному оптичному волокну 160 хвиль різної довжини в вікні прозорості 1550 нм, при цьому кожна хвиля являє собою окремий спектральний канал і може передавати власну інформацію зі швидкістю до 100 Гбіт/с. Швидкість передачі залежить від технології дискретного кодування даних на кожній хвилі, наприклад, це може бути кодування технологій SDH або OTN. Зараз ведуться роботи по підвищенню швидкості передачі до 200 Гбіт/с і вище.

Мережі DWDM працюють за принципом комутації каналів. Апаратура DWDM не займається безпосередньо проблемами передачі даних на кожній хвилі – це проблема більше високорівневої технології, яка використовує надану їй хвилю на свій розсуд і може передавати на цій хвилі як дискретну, так і аналогову інформацію. Основними функціями апаратури DWDM є операції мультиплексування і демультиплексування, а саме – об'єднання різних хвиль в одному світловому пучку і виділення інформації кожного спектрального каналу із загального сигналу. Деякі пристрої DWDM можуть також комутувати хвилі.

Технології DWDM передувала **технологія хвильового мультиплексування** (**WDM**), в якій використовується до 8 спектральних каналів в вікнах прозорості 1310 нм і 1550 нм з розносом несучих в 20 нм. Ця технологія також називається **технологією грубого хвильового мультиплексування** (Coarse Wave Division Multiplexing, **CWDM**), через те, що хвилі знаходяться на великій відстані одна від одної, а значить, і сигнал окремої хвилі легше виділити із загального світлового сигналу.

Мультиплексування DWDM називається «ущільненим» через те, що відстань між довжинами хвиль в ньому суттєво менша, ніж в WDM. На сьогодні рекомендацією G.692 сектора ITU-T визначено чотири частотних плани (тобто набору частот, віддалених один від одного на деяку постійну величину) з кроком (тобто рознесенням частот між сусідніми каналами) в 100, 50, 25 і 12,5 ГГц.

Технології з рознесенням частот між сусідніми каналами в 50 ГГц і нижче називаються технологіями з **високощільним хвильовим мультиплексуванням** (High Dense WDM – **HDWDM**), вони дають змогу мультиплексувати не менше 64 каналів.

### 3.4.2. Волоконно-оптичні підсилювачі мереж DWDM

Практичний успіх технології DWDM, обладнання якої вже працює на магістралях багатьох провідних світових операторів зв'язку, багато в чому визначило появу **волоконно-оптичних підсилювачів**. Ці оптичні пристрої безпосередньо посилюють світлові сигнали в діапазоні 1550 нм, виключаючи необхідність проміжного перетворення їх в електричну форму, як це роблять регенератори, що застосовуються в мережах SDH. Системи електричної регенерації сигналів досить дорогі і, крім того, залежать від протоколу, так як вони повинні сприймати певний вид кодування сигналу. Оптичні підсилювачі, «прозоро» передають інформацію, дозволяють нарощувати швидкість магістралі без необхідності модернізації підсилювальних блоків.

Протяжність ділянки між оптичними підсилювачами може досягати 150 км і більше, що забезпечує економічність створюваних магістралей DWDM, в яких довжина мультиплексної секції становить на сьогодні 600-3000 км при застосуванні від 1 до 7 проміжних оптичних підсилювачів.

Хоча оптичний підсилювач відновлює потужність сигналу, він не повністю компенсує ефект хроматичної дисперсії (тобто поширення хвиль різної довжини з різною швидкістю, через що сигнал на приймальному кінці волокна «розмазується»), а також інші нелінійні ефекти. Тому для побудови більш протяжних магістралей необхідно між підсилювальними ділянками встановлювати мультиплексори DWDM, що виконують регенерацію сигналу шляхом його перетворення в електричну форму і назад. Для зменшення нелінійних ефектів в системах DWDM застосовується також обмеження потужності сигналу.

Оптичні підсилювачі використовуються не тільки для збільшення відстані між мультиплексорами, але і встановлюються усередині самих мультиплексорів. Якщо мультиплексування і крос-комутація виконуються суто оптичних засобами без перетворення в електричну форму, то сигнал при пасивних оптичних перетвореннях втрачає потужність і перед передачею в лінію його потрібно посилювати.

Нові дослідження привели до появи підсилювачів, що працюють в так званому L-діапазоні (4-е вікно прозорості), від 1570 до 1605 нм. Використання цього діапазону, а також скорочення відстані між хвилями до 50 і 25 ГГц, дозволяє наростити кількість одночасно передаючих довжин хвиль до 160 і більше, тобто забезпечити передачу трафіку зі швидкостями 800 Гбіт/с-1,6 Тбіт/с в одному напрямку по одному оптичному волокні.

### 3.4.3. Топології мереж DWDM

Хронологічно першою областю застосування технології DWDM (як і технології SDH) стало створення наддалеких високошвидкісних магістралей, що мають топологію **«точка-точка»**. Для організації такої магістралі досить в її кінцевих точках встановити **термінальні мультиплексори DWDM**, а в проміжних точках – оптичні підсилювачі, якщо цього вимагає відстань між кінцевими точками.

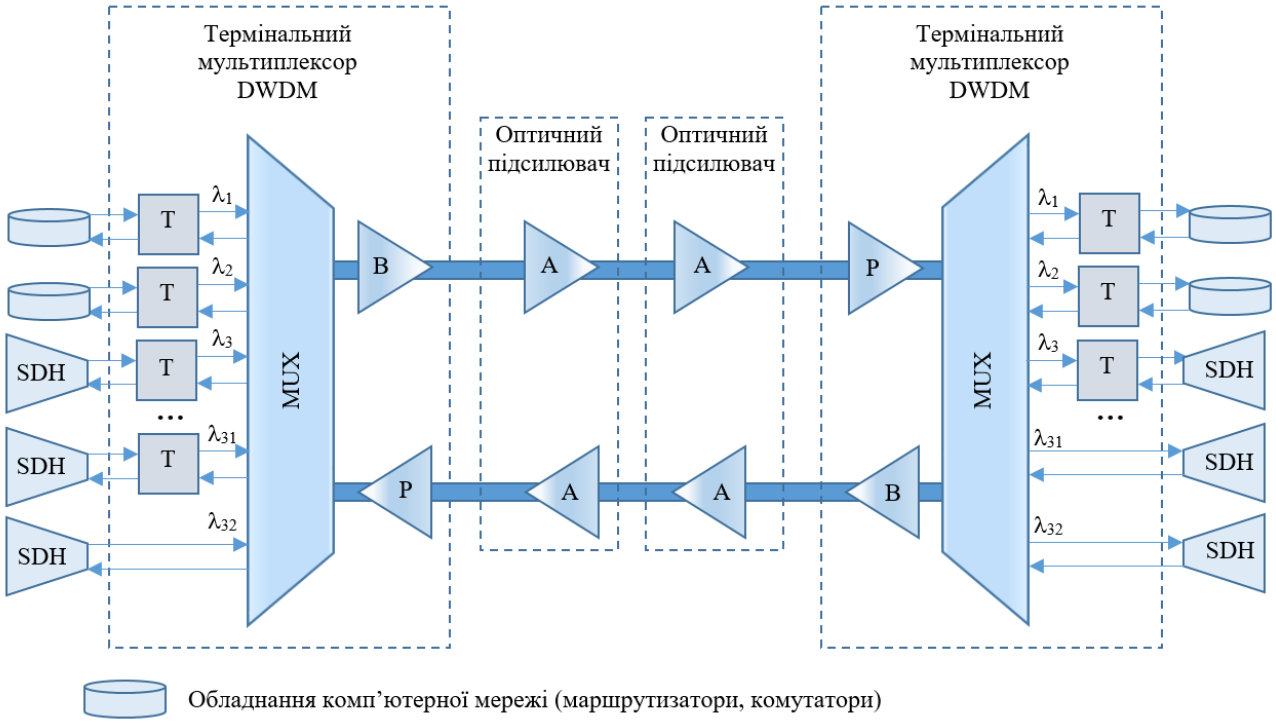



Рис. 3.11. Наддовгий зв'язок «точка-точка» на основі ТМ DWDM

Термінальний мультиплексор включає блок мультиплексування/ демультиплексування, вихідний (Booster, B) і попередній (Pre-amplifier, P) підсилювачі, а також набір транспондерів (**trans**mitter-res**ponder**, Transponder, T), які перетворюють вхідні електричні сигнали, що містять дискретну інформацію, яка поступає від абонентських пристроїв користувачів мережі DWDM, в оптичні сигнали певної довжини хвилі і навпаки.

У наведеній на рисунку схемі дуплексний режим між абонентами мережі відбувається за рахунок однонаправленої передачі всього набору хвиль по двох волокнах. Існує й інший варіант роботи мережі DWDM, коли для зв'язку вузлів мережі використовується одне волокно.

Дуплексний режим досягається шляхом двонаправленої передачі оптичних сигналів по одному волокну – половина хвиль частотного плану

передають інформацію в одному напрямку, половина – в зворотному.

Розвитком топології «точка-точка» є топологія **ланцюга з проміжними під'єднаннями**, в якій проміжні вузли виконують функції оптичних мультиплексорів вводу-виводу (рис. 3.12).

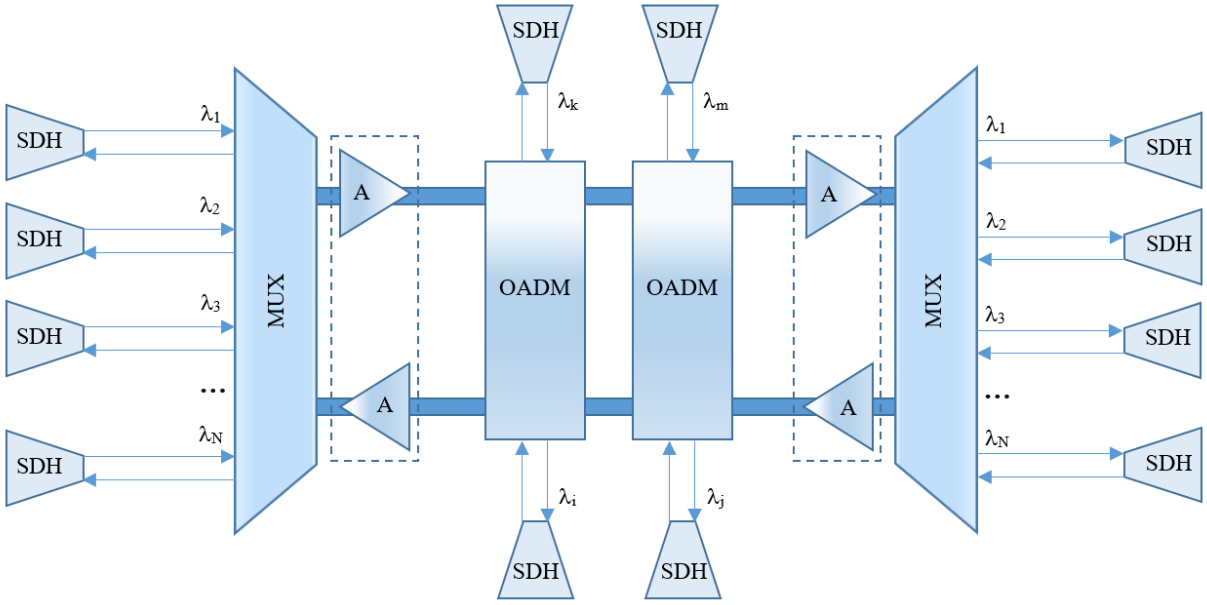



Рис. 3.12. Ланцюг DWDM з вводом-виводом в проміжних вузлах

**Оптичні мультиплексори вводу-виводу** (Optical Add-Drop Multiplexer, **OADM**) можуть вивести із загального оптичного сигналу хвилю певної довжини і ввести туди сигнал цієї ж довжини хвилі, так що спектр транзитного сигналу не зміниться, а з'єднання буде виконано з одним із абонентів, під'єднаних до проміжного мультиплексору. OADM підтримує операції вводу-виводу хвиль суто оптичними засобами або з проміжним перетворенням в електричну форму.

**Кільцева топологія** (рис. 3.13) забезпечує живучість мережі DWDM за рахунок резервних шляхів. Методи захисту трафіку, що застосовуються в DWDM, аналогічні методам в SDH (хоча в DWDM вони поки не стандартизовані). Для того, щоб будь-яке з'єднання було захищене, між його кінцевими точками встановлюються два шляхи: основний і резервний. Мультиплексор кінцевої точки порівнює два сигнали і вибирає сигнал кращої якості (або сигнал, заданий по замовчуванню).

У міру розвитку мереж DWDM в них все частіше буде застосовуватися комірчаста топологія (рис. 3.14), яка забезпечує найкращі показники в плані гнучкості, продуктивності та відмовостійкості, ніж інші топології. Однак для реалізації комірчаста топології необхідна наявність **оптичних крос-конекторів** (Optical Cross-Connector), які не тільки додають хвилі в загальний транзитний сигнал і виводять їх звідти, як це роблять мультиплексори вводу-виводу, а й

підтримують довільну комутацію між оптичними сигналами, що передаються хвилями різної довжини.

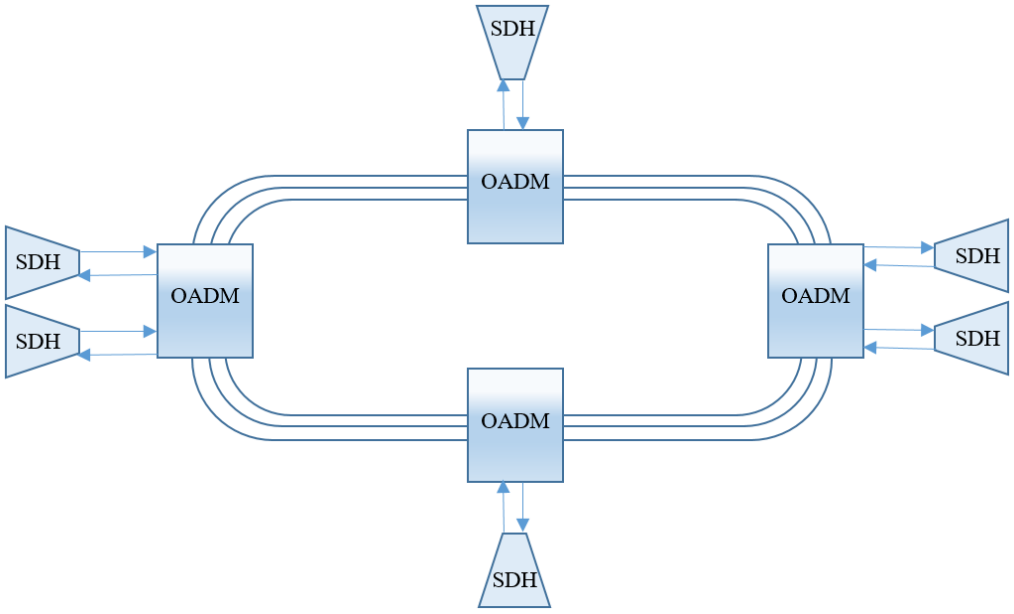



Рис. 3.13. Кільце мультиплексорів DWDM

Можливості оптичних крос-конекторів по створенню комірчастої топології оцінюються кількістю магістральних зв'язків, які вони можуть підтримувати зі своїми безпосередніми сусідами. Ці зв'язки називають **напрямами маршрутизації**. Так, верхній крос-конектор (рис. 3.14) підтримує чотири напрями маршрутизації, а нижній – лише два. Звичайний мультиплексор вводу-виводу завжди підтримує лише два напрями маршрутизації.

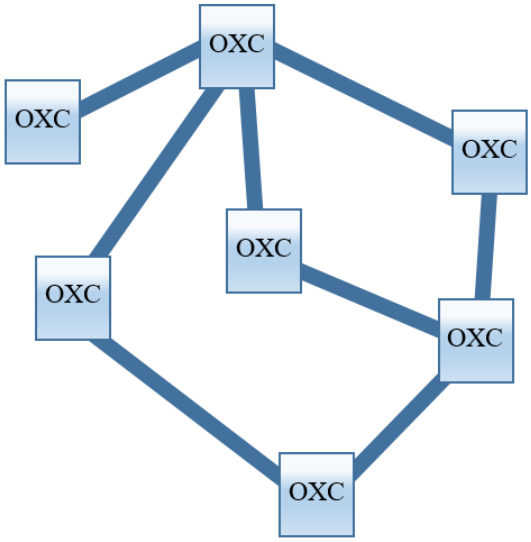



Рис. 3.14. Комірчаста топологія DWDM

З успіхами DWDM пов’язаний ще один перспективний технологічний напрям – **повністю оптичні мережі**. У таких мережах всі операції по мультиплексуванню/ демультиплексування, вводу-виводу і крос-комутації (маршрутизації) даних виконуються без перетворення сигналу з оптичної форми в електричну, що дозволяє істотно здешевити мережу. Однак можливості оптичних технологій поки ще недостатні для створення масштабних повністю оптичних мереж, тому їх практичне застосування обмежене фрагментами, між якими виконується електрична регенерація сигналу.

## 3.5. Мережі OTN

### 3.5.1. Ієрархія швидкостей

Мережі DWDM не є власне цифровими мережами, так як вони лише надають користувачам окремі спектральні канали, які є не більше ніж несучої середовищем. Для того щоб передавати по такому каналу цифрові дані, необхідно якимось чином домовитися про метод модуляції або кодування двійкових даних, а також передбачити такі важливі механізми, як контроль коректності даних, виправлення бітових помилок, забезпечення відмовостійкості, оповіщення користувача про стан з’єднання і т. п.

Історично мультиплексори DWDM були також і мультиплексорами SDH, тобто в кожному з хвильових каналів для вирішення перерахованих завдань вони використовували техніку SDH. Однак, через деякий час експлуатації мереж SDH/DWDM стали помітні певні недоліки, пов’язані із застосуванням технології SDH в якості основної технології передачі цифрових даних по спектральним каналах DWDM. Основні недоліки:

- *Недостатня ефективність кодів FEC, прийнятих в якості стандарту SDH*. Це перешкоджає подальшому підвищенню щільності спектральних каналів в мультиплексорах DWDM. Логіка тут наступна: при збільшенні кількості спектральних каналів в оптичному волокні збільшується взаємний вплив їх сигналів, отже, зростають спотворення сигналів і, як наслідок, бітові помилки при передачі цифрових даних по цих спектральним каналах. Якщо ж процедури FEC настільки ефективні, що дозволяють «на льоту» усунути значну частину цих помилок, то цими помилками можна знехтувати і збільшити кількість спектральних каналів. Або ж не збільшувати кількість каналів, а збільшити довжину нерегенерованих секцій мережі.
- *Занадто «дрібні» одиниці комутації для магістральних мереж*, що працюють на швидкостях 10, 40 і 100 Гбіт/с. Підтримка таких

абонентських каналів, як канали зі швидкостями 1,5, 2 або 34 Мбіт/с, ускладнює апаратуру мереж, тому бажаним є використання одиниць комутації, які більше відповідають бітовим швидкостям сучасного клієнтського обладнання. Механізм віртуальної конкатенації SDH частково вирішує цю проблему, але в цілому вона залишається.

- *Не враховано особливості трафіку різного типу.* Розробниками технології SDH брався до уваги лише голосовий трафік, тоді як зараз переважаючим є комп'ютерний трафік.

На подолання цих недоліків націлена нова технологія – **оптичних транспортних мереж** (Optical Transport Network, **OTN**), яка забезпечує передачу і мультиплексування цифрових даних по хвильових каналах DWDM більш ефективно, ніж SDH. У той же час мережі OTN забезпечують зворотну сумісність з SDH, так як для мультиплексорів OTN трафік SDH є одним з видів користувацького трафіку поряд з такими клієнтами, як Ethernet і GFP.

Потрібно відзначити, що технологія OTN не замінює технологію DWDM, а доповнює її хвильові канали «цифровою оболонкою». Термін «цифрова оболонка» (digital wrapper) інколи навіть використовується в якості назви самої технології OTN.

Архітектура мереж OTN описана в стандарті ITU-T G.872, а найбільш важливі технічні аспекти роботи вузла мережі OTN описані в стандарті G.709.

Технологія OTN багато взяла від технології SDH, в тому числі коефіцієнт кратності швидкостей 4 для побудови своєї ієрархії швидкостей. Однак початкова швидкість ієрархії швидкостей OTN набагато вища, ніж у SDH: 2,5 Гбіт/с замість 155 Мбіт/с. В даний час стандартизовано чотири швидкості технології OTN – **OTU1-OTU4** (Optical channel Transport Unit level k – транспортний блок оптичного каналу рівня k) (табл. 3.3).

Таблиця 3.3.

Ієрархія швидкостей технології OTN

| Назва каналу | Швидкість кадрів OTN (Гбіт/с) | Клієнтський кадр | Швидкість клієнта (Гбіт/с) |
|---|---|---|---|
| OTU1 | 2,666 | STM-16 | 2,488 |
| OTU1 | 10,709 | STM-64 | 9,953 |
| OTU1 | 43,018 | STM-256 | 39,813 |
| OTU1 | 111,8 | 100G Ethernet | 100 |

### 3.5.2. Стек протоколів OTN

Стек протоколів OTN складається з 4-х рівнів. На рис. 3.15 показана узагальнена архітектура мережі OTN і області розповсюдження протоколу кожного рівня, а на рис. 3.16 – ієрархія протоколів OTN.

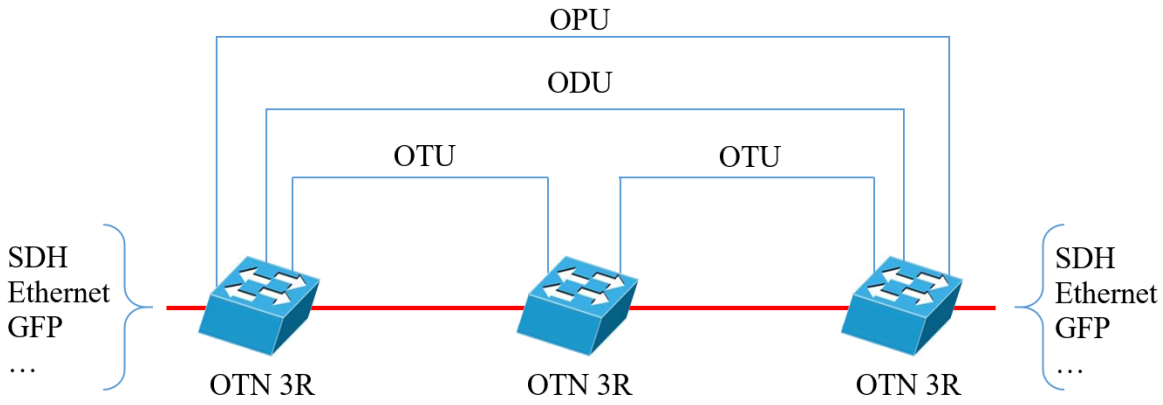



Рис. 3.15. Мережа OTN і розповсюдження протоколів

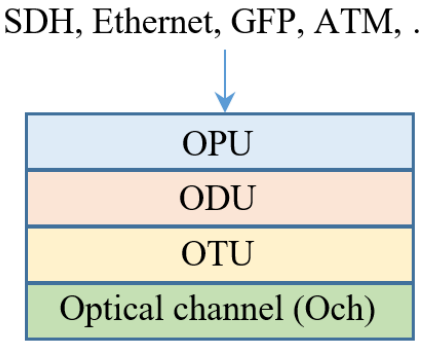



Рис. 3.16. Ієрархія протоколів OTN

**Протокол OPU** (Optical channel Payload Unit – блок користувацьких даних оптичного каналу) відповідає за передачу даних між користувачами мережі. Він займається інкапсуляцією користувацьких даних, таких як кадри SDH або Ethernet, в блоки OPU, вирівнюванням швидкостей передачі користувацьких даних і блоків OPU, а на приймальній стороні вилучає з каналу прийняті дані і передає їх користувачу. В залежності від швидкості передачі даних цьому протоколу відповідають блоки OPU1, OPU2, OPU3 і OPU4. Для виконання своїх функцій протокол OPU додає до користувацьких даних свій заголовок OPU OH (OverHead). Блоки OPU не модифікуються мережею.

**Протокол ODU** (Optical Channel Data Unit – блок даних оптичного каналу), так само, як і протокол OPU, працює між кінцевими вузлами мережі OTN. У його функції входить мультиплексування і демультиплексування блоків OPU,

наприклад, мультиплексування чотирьох блоків OPU1 в один блок OPU2. Крім того, протокол ODU підтримує функції моніторингу якості з'єднань в мережі OTN. Цей протокол формує блоки ODU потрібної швидкості, додаючи до відповідних блоків OPU свій заголовок.

**Протокол OTU** (Optical Channel Transport Unit – транспортний блок оптичного каналу) працює між двома сусідніми вузлами мережі OTN, які підтримують функції електричної регенерації оптичного сигналу, звані також **функціями 3R** (Retiming – відновлення синхронізації, Reshaping – відновлення форми і Regeneration – регенерація). Основне призначення цього протоколу – контроль і виправлення помилок за допомогою кодів FEC (Forward Error Correction – завадостійке кодування). Цей протокол додає до блоку ODU своє **закінчення**, що містить код FEC, утворюючи блок OTU. Блоки OTU поміщаються безпосередньо в оптичний канал.

Нижній рівень протоколів становить **оптичний канал** (Optical Channel, **Och**), зазвичай, це спектральний канал DWDM.

### 3.5.3. Кадр OTN

Кадр OTN складається з 4080 стовпців (байтів) і 4 рядків (рис. 3.17).


Рис. 3.17. Формат кадру OTN

Кадр складається з поля користувацьких даних (Payload) і службових полів блоків OPU, ODU і OTU. Формат кадру не залежить від рівня швидкості OTN, тобто він, наприклад, однаковий для блоків OPU1/ODU1/OTU1 і OPU2/ODU2/OTU2.

Поле користувацьких даних розташовується з 17 по 3824 стовпець і займає всі чотири рядки кадру, а заголовок блоку OPU займає стовпці 15 і 16 також в чотирьох рядках.

Блок ODU представлений тільки заголовком ODU OH (формально він також має поле даних, в яке поміщений блок OPU), а блок OTU складається з заголовка OTU OH і закінчення OTU FEC, що містить код корекції помилок FEC. Починається кадр з невеликого поля вирівнювання кадру, необхідного для

розпізнавання початку кадру.

### 3.5.4. Мультиплексування блоків ODU

При мультиплексуванні блоків ODU поле користувацьких даних блоку OPU розбивається на **трибутарні слоти** (Tributary Slot, TS), в які поміщаються дані блоку OPU-1.

На рис. 3.18 показаний приклад мультиплексування чотирьох блоків ODU1 в один блок ODU2. Як видно з рисунку, поле даних блоку OPU2 розбите на трибутарні слоти TribSlotl, TribSlot2, TribSlot3 і TribSlot4, послідовність яких повторюється. Кожен з цих чотирьох трибутарних слотів призначений для перенесення частини поля даних одного з блоків OPU1. Тут використовується техніка чергування даних швидкості більш низького рівня ієрархії швидкостей в поле даних блоку більш високої швидкості ієрархії швидкостей, яка є типовою для технологій синхронного часового мультиплексування. Ця техніка забезпечує виконання операцій мультиплексування і демультиплексування «на ходу» без проміжної буферизації, так як частота появи порцій даних OPU1 в блоці ODU2 відповідає частоті їх появи в тому випадку, якщо б вони передавалися на швидкості OPU1.

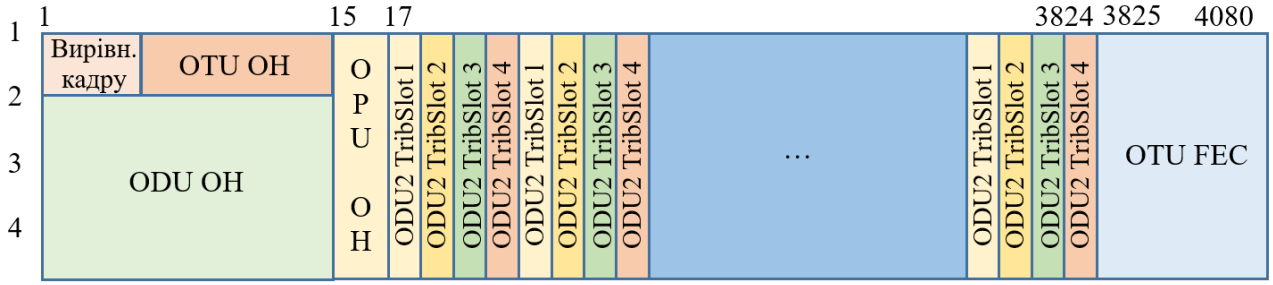



Рис. 3.18. Мультиплексування блоків ODU1 в ODU2

Техніка мультиплексування блоків ODU1 і ODU2 в блок ODU3 аналогічна, якщо не брати до уваги того, що в блоці OPU3 використовується 16 різних трибутарних слотів, що дозволяє помістити в нього 16 блоків ODU1 або 4 блоки ODU2 (в цьому випадку одній порції OPU2 відповідає чотири трибутарних слота ODU3). Існує два типи трибутарних слотів: перший тип відповідає швидкості даних 2,5 Гбіт/с, другий – 1,25 Гбіт/с (він був введений для більш ефективного мультиплексування даних 1G Ethernet).

Інформація про використання трибутарних слотів зберігається в спеціальному розділі поля OPU2 OH або OPU3 OH.

# 4. Транспортні технології телекомунікаційних мереж канального рівня

## 4.1. Класифікація WAN мереж

Протягом всього часу існування телекомунікаційних мереж важливу роль в них відігравали глобальні мережі (Wide Area Network, WAN), побудовані з використанням транспортних технологій канального рівня.

Створення мереж на основі спеціальних стандартів гарантує, що всі пристрої та технології, що використовуються в середовищі WAN, будуть сумісні один з одним.

Стандарти WAN описують характеристики фізичного і канального рівня передачі даних. Стандарти WAN канального рівня включають такі параметри, як фізична адресація, управління потоками і тип інкапсуляції, а також порядок проходження даних по каналу мережі WAN. Тип застосовуваної технології WAN визначає використовувані стандарти канального рівня (рис. 4.1).


Рис. 4.1. Стандарти WAN канального рівня OSI моделі

Нижче представлені приклади протоколів інкапсуляції мережі WAN для канального рівня:

- LAPF (Link Access Procedure for Frame Relay – процедура доступу до каналу Frame Relay);
- HDLC (High-level Data Link Control – високорівневе управління каналом даних)
- PPP (Point-to-Point Protocol – протокол «точка-точка»).

В даний час є багато варіантів реалізації WAN підключень. Вони розрізняються за технологією, швидкістю і вартістю (рис. 4.2). WAN з'єднання

може бути здійснено використовуючи приватну інфраструктуру або ж публічну, таку як Інтернет.

Технологія WAN визначає тип пристроїв, які необхідні для під'єднання до глобальної мережі. Для передачі даних по мережі WAN за допомогою цифрових каналів потрібні **пристрій обслуговування каналу** (Channel Service Unit, **CSU**) і **пристрій обслуговування даних** (Data Service Unit, **DSU**). Ці два пристрої зазвичай об'єднані в один – **пристрій CSU/DSU**. Ці пристрої інтегровані в інтерфейсну плату на маршрутизаторі. При використанні аналогового з'єднання потрібен **модем** (Modem).

Пристрій CSU/DSU або модем управляють швидкістю передачі даних до місцевої лінію. Вони також забезпечують передачу сигналу синхронізації на маршрутизатор. Пристрій CSU/DSU є обладнанням DCE, а маршрутизатор – обладнанням DTE.

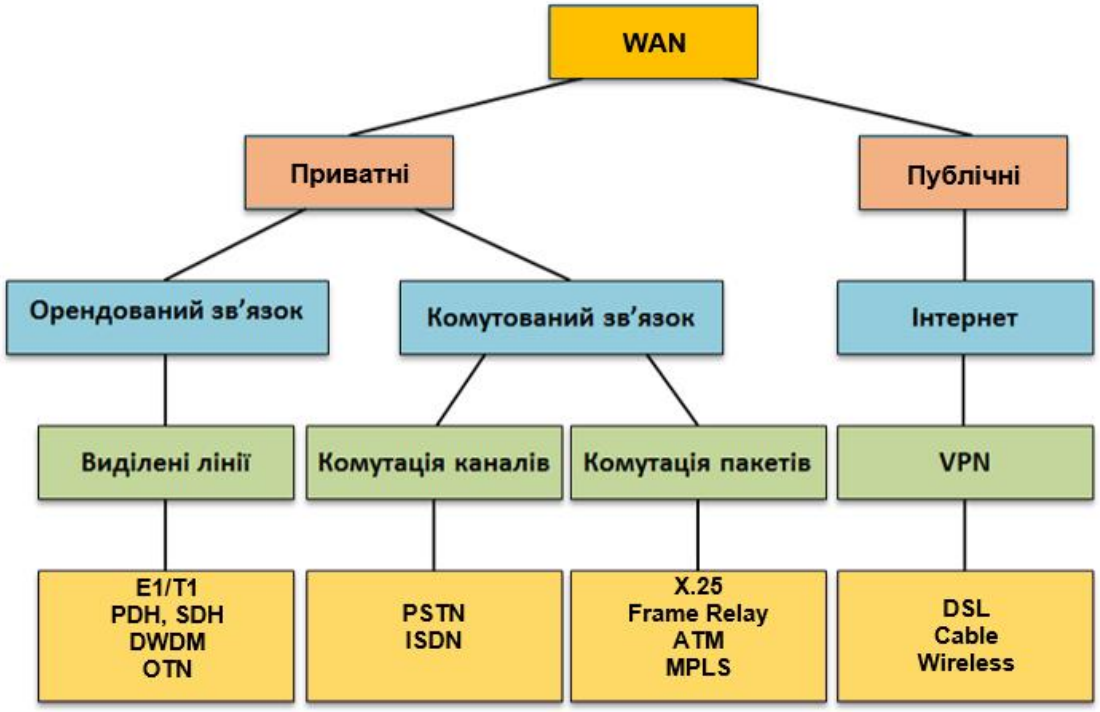



Рис. 4.2. Класифікація WAN мереж

Якщо організація отримує телекомунікаційні послуги мережі WAN за передплатою у провайдера (ISP), то останній надає й обслуговує більшість мережевих пристроїв. У певних місцях користувач може самостійно встановлювати і обслуговувати комунікаційне обладнання. Точка, в якій управління з'єднанням і відповідальність за нього переходить від користувача до постачальника послуг, називається **точкою розмежування** (Demarcation Point). Наприклад, точка розмежування може перебувати між маршрутизатором і

пристроєм перетворення або між пристроєм перетворення і **центральним офісом** (Central Office, CO) постачальника послуг (рис. 4.3).

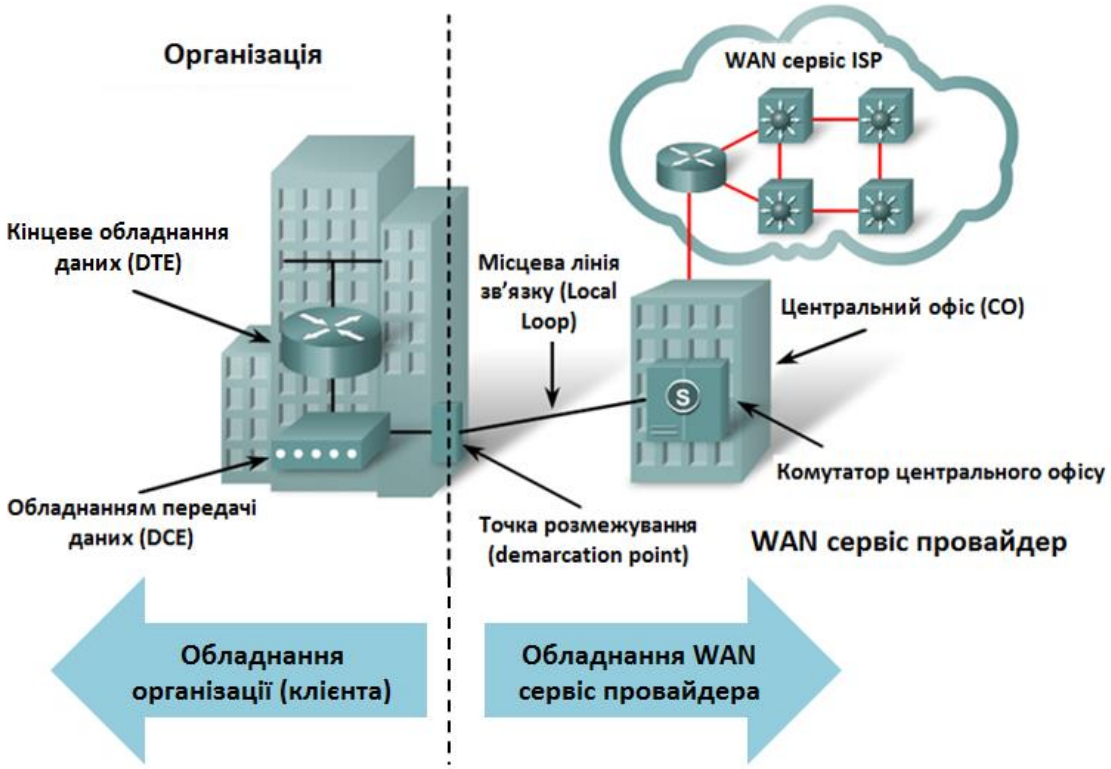



Рис. 4.3. Схема розмежування між пристроями CSU/DSU та CO

Розміщене на стороні користувача обладнання, незалежно від його власника, постачальники послуг називають **телекомунікаційним обладнанням клієнта** (Customer Premise Equipment, **CPE**).

Центральним офісом є місце, в якому знаходиться обладнання постачальника послуг, що забезпечує з'єднання для клієнта. Для фізичного підключення телекомунікаційного обладнання клієнта до маршрутизатора або комутатора мережі WAN в центральному офісі використовується мідний або оптоволоконний кабель. Таке з'єднання називається **місцевої лінією зв'язку** (local loop) або **останньою милею** (last mile). З боку користувача, це з'єднання називається **першою милею** (first mile), так як воно є першою частиною середовища передачі даних, що веде з його місця розташування.

## 4.2. Інкапсуляція кадрів на канальному рівні

Інкапсуляція кадрів відбувається перед проходженням даних по мережі WAN. Тип інкапсуляції відповідає певному формату в залежності від технології, що застосовується в мережі (рис. 4.4).

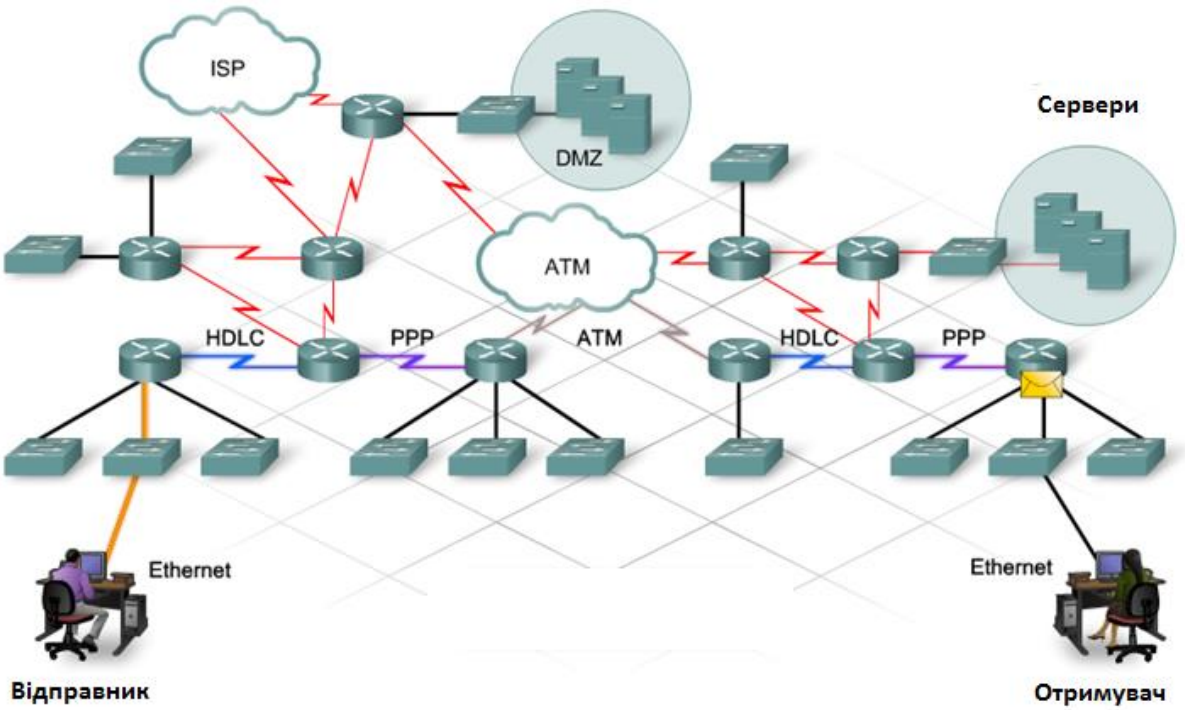



Рис. 4.4. Проходження пакету через WAN з інкапсуляцією кадрів різного типу

Перед перетворенням даних у біти для відправки в середовище передачі інкапсуляція канального рівня додає адресацію і керуючу інформацію.

Канальний рівень додає до кадру вміст заголовка, який відповідає типу фізичної передачі даних по мережі. Всередині середовища локальної мережі (LAN), найбільш поширеною технологією є Ethernet. Канальний рівень інкапсулює пакети в кадри Ethernet. Заголовки кадрів містять відомості про MAC-адресу відправника та отримувача, а також окрему керуючу інформацію Ethernet, таку як розмір кадру і синхронізацію.

При кожному підключення до WAN, дані інкапсулюються в кадри, перед тим як надіслати їх у WAN інтерфейс. В залежності від використовуваного протоколу, необхідно налаштувати відповідний канальний тип інкапсуляції на інтерфейсі. Вибір протоколу залежить від WAN технології та обладнання зв’язку. На рис. 4.5 показані основні типи протоколів інкапсуляції канального рівня:

- **HDLC** – тип інкапсуляції, що встановлений по замовчуванню при використанні з'єднання «точка-точка» (point-to-point) віддалених пристроїв Cisco.
- **PPP** – надає з'єднання «маршрутизатор-маршрутизатор» (router-to-router) та «хост-мережа» (host-to-network) через синхронні і асинхронні канали. PPP підтримує механізми захисту такі як PAP, CHAP.
- **SLIP** – стандартний протокол «точка-точка» для послідовного з'єднання, яке використовує протокол TCP/IP. Даний протокол практично повністю витіснений протоколом PPP.

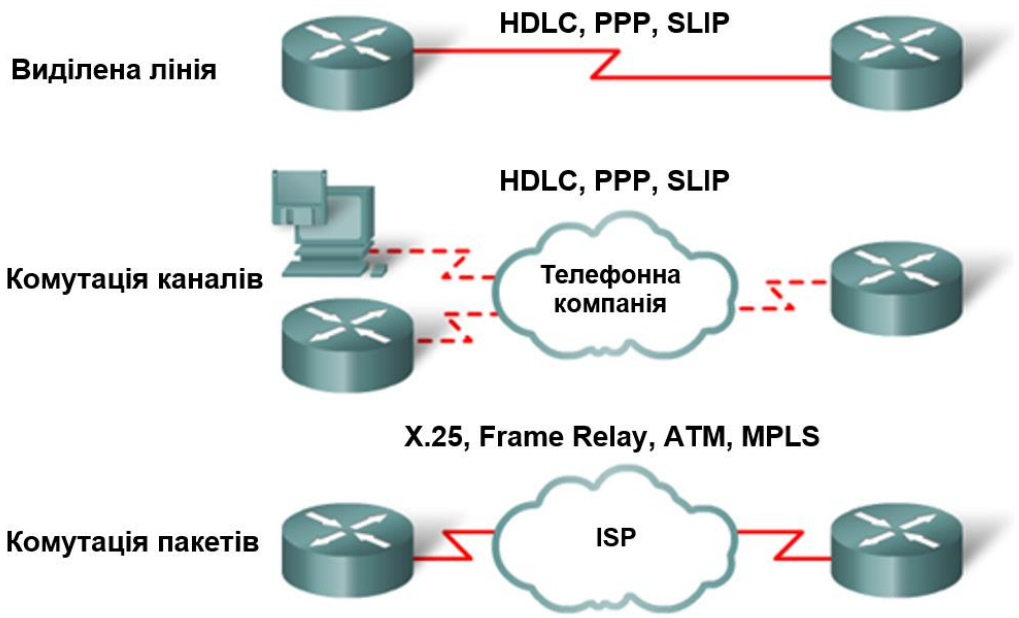



Рис. 4.5. Типи протоколів інкапсуляції

- **X.25/(LAPB)** – стандарт ITU-T, який визначає як буде встановлюватися з'єднання між DCE і DTE для віддалених терміналів при взаємодії комп'ютерів один з одним через загальнодоступні мережі. LAPB використовується в якості протоколу канального рівня X.25.
- **Frame Relay** – промисловий стандарт, протокол канального рівня який підтримує комутовані віртуальні канали. Frame Relay є протоколом наступного покоління після X.25 і виправив деякі його проблемні місця, наприклад, корекцію помилок, контроль потоку (управління потоком).
- **ATM** – міжнародний стандарт, передача даних в якому базується на комутації комірок фіксованої довжини (53 байти). Добре підходить для передачі голосових та відео даних.
- **MPLS** – технологія багатопротокольної комутації по мітках, який поєднує техніку віртуальних каналів з функціональністю стеку TCP/IP.

Тип інкапсуляції канального рівня відрізняється від типу інкапсуляції мережевого рівня. При проходженні даних по мережі інкапсуляція канального рівня може постійно змінюватися, у той час як інкапсуляція мережевого рівня незмінна. Щоб такий пакет пройшов свій шлях по WAN мережі в кінцеву точку, інкапсуляція канального рівня повинна змінитися відповідно до застосовуваної, в даному сегменті мережі, технології.

Пакети виходять з LAN мережі через маршрутизатор шлюзу (рис. 4.6). Маршрутизатор демонтує кадри Ethernet і потім повторно інкапсулює дані до відповідного типу кадрів для мережі WAN. Перетворення кадрів, отриманих в інтерфейсі WAN, в формат кадрів Ethernet відбувається перед їх розподілом в локальній мережі. Маршрутизатор виступає в якості перетворювача даних, налаштовуючи формат кадрів канального рівня до потрібного формату інтерфейсу.

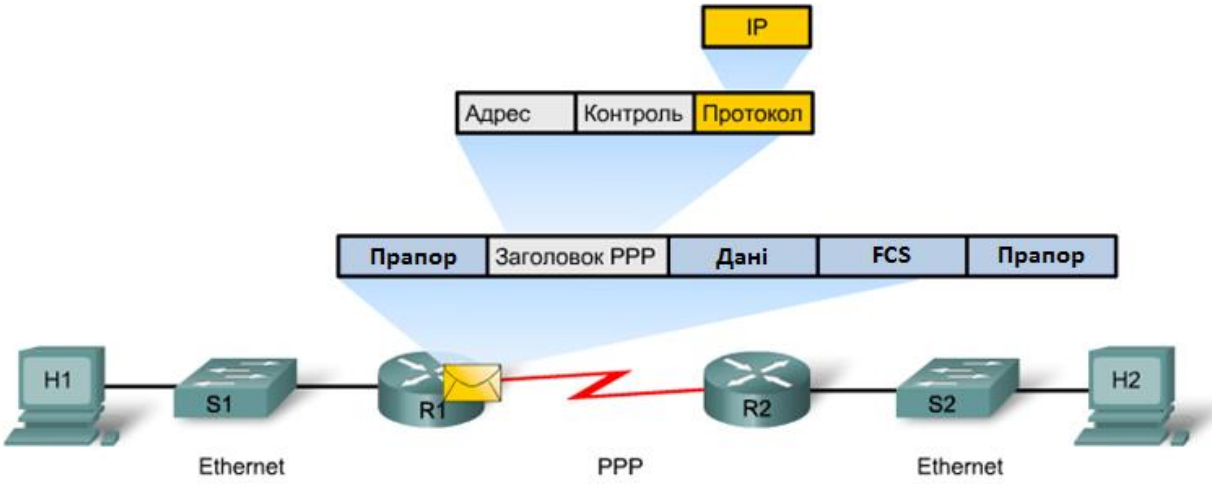



Рис. 4.6. Інкапсуляція кадрів канального рівня

Тип інкапсуляції повинен збігатися в обох кінцевих точках прямого з'єднання. Інкапсуляція канального рівня включає наступні поля:

**Прапор (Flag)** – позначає початок і кінець кожного кадру;

**Адреса (Address)** – залежить від типу інкапсуляції; не вимагається, якщо канал WAN є прямим з'єднанням;

**Контроль (Control)** – використовується для задання типу кадру;

**Протокол (Protocol)** – використовується для визначення типу інкапсульованого протоколу мережевого рівня; представлено не у всіх інкапсуляціях мережі WAN;

**Дані (Data)** – використовується як дані верхнього рівня та датаграма IP-мережі;

**Контрольна послідовність кадру (**Frame Check Sequence, **FCS)** – забезпечує механізм порівняння, що дозволяє переконатися, що кадр не був пошкоджений під час передачі.

Дві найбільш поширені послідовні інкапсуляції канального рівня – це стандарти HDLC і PPP.

## 4.3. Двоточкові технології каналів

У тих випадках, коли IP-маршрутизатори безпосередньо з'єднані лініями зв'язку фізичного рівня (кабелями або каналами технологій первинних мереж, таких як PDH, SDH або OTN), функції протоколу канального рівня скорочуються в порівнянні з випадком, коли на канальному рівні є мережа з комутацією пакетів, наприклад Ethernet або MPLS. Для подібних випадків розроблені спеціальні протоколи канального рівня зі спрощеною функціональністю, які прийнято називати двоточковими, або протоколами «точка-точка», що відображає топологію зв'язків між маршрутизаторами.

### 4.3.1. Протокол HDLC

Протокол **високорівневого управління каналом даних** (High-level Data Link Control, **HDLC**) – це сімейство протоколів, що реалізують функції канального рівня.

Важливою властивістю HDLC є його функціональна різноманітність. Він може працювати в декількох різних режимах, підтримує не тільки двоточкове з'єднання («точка-точка»), але й з'єднання одного джерела з декількома приймачами («точка-багатоточка»).

Складність HDLC пояснюється тим, що це дуже «старий» протокол, розроблений ще в 70-і роки для ненадійних каналів зв'язку. Тому в одному з режимів протокол HDLC, подібно протоколу TCP, підтримує процедуру встановлення логічного з'єднання і процедуру контролю передачі кадрів, а також відновлює втрачені або пошкоджені кадри. Існує і датаграмний режим роботи HDLC, в якому логічне з'єднання не встановлюється і кадри не відновлюються.

В IP-маршрутизаторах найчастіше використовується версія протоколу HDLC, розроблена компанією Cisco. Незважаючи на те, що ця версія є фірмовим протоколом, вона стала стандартом для IP-маршрутизаторів більшості виробників. Версія Cisco HDLC працює тільки в датаграмному режимі, що відповідає сучасній ситуації з надійними каналами зв'язку. У порівнянні зі стандартним протоколом версія Cisco HDLC включає кілька розширень, головним з яких є багатопротокольна підтримка. Це означає, що в заголовок

кадру Cisco HDLC додано поле типу протоколу. Це поле містить код протоколу, дані якого переносить кадр Cisco HDLC. У стандартній версії HDLC таке поле відсутнє (рис. 4.7).

Рис. 4.7 Стандартний і Cisco тип кадрів HDLC


### 4.3.2. Протокол PPP

**Протокол PPP** (Point-to-Point Protocol – протокол двоточкового зв'язку) є стандартним протоколом Інтернету. Протокол PPP так само, як і HDLC, являє собою ціле сімейство протоколів, в яке, зокрема, входять:

- протокол управління лінією зв'язку (Link Control Protocol, LCP);
- протокол управління мережею (Network Control Protocol, NCP);
- багатоканальний протокол PPP (MultiLink PPP, MLPPP);
- протокол автентифікації по паролю (Password Authentication Protocol, PAP);
- протокол автентифікації по «рукостисканню» (Challenge Handshake Authentication Protocol, CHAP).

Особливістю протоколу PPP, що відрізняє його від інших протоколів канального рівня, є складна переговорна процедура прийняття параметрів з'єднання. Сторони обмінюються різними параметрами, такими як якість лінії, розмір кадрів, тип протоколу автентифікації і тип інкапсульованих протоколів мережевого рівня. Протокол, відповідно до якого приймаються параметри з'єднання, називається **протоколом управління лінією зв'язку** (LCP).

При встановленні з'єднання два взаємодіючих пристрої для знаходження взаєморозуміння намагаються спочатку використовувати стандартні параметри, що встановлені по замовчуванню. Кожен кінцевий вузол описує свої можливості

і вимоги. Потім на підставі цієї інформації приймаються параметри з'єднання, що влаштовують обидві сторони.

Одним з важливих параметрів з'єднання PPP є режим автентифікації. Для цілей автентифікації PPP пропонує за замовчуванням **протокол автентифікації по паролю** (PAP), який передає пароль по лінії зв'язку у відкритому вигляді, або **протокол автентифікації по «рукостисканню»** (CHAP), що не передає пароль по лінії зв'язку і тому забезпечує більш високий рівень безпеки мережі.

**Багатопротокольна підтримка** – здатність протоколу PPP підтримувати декілька протоколів мережевого рівня. Всередині одного з'єднання PPP можуть передаватися потоки даних різних мережевих протоколів, включаючи IP, Novell IPX, і інших, а також дані протоколів канального рівня локальної мережі.

Кожен протокол мережевого рівня конфігурується окремо за допомогою відповідного протоколу управління мережею (NCP). Для кожного протоколу, призначеного для конфігурації протоколу верхнього рівня, крім загальної назви NCP використовується спеціальна назва, яка побудована шляхом додавання абревіатури CP (Control Protocol – протокол управління) до імені протоколу верхнього рівня: наприклад, для IP – це протокол IPCP, для протоколу IPX - IPXCP і т. п.

Однією з привабливих здібностей протоколу PPP є здатність використання декількох фізичних ліній зв'язку для створення єдиного логічного каналу, тобто агрегування каналів. Цю можливість реалізує **багатоканальний протокол PPP** (MLPPP).

## 4.4. Технології віртуальних каналів

У мережі з віртуальними каналами два вузла можуть почати обмін даними тільки після того, як між ними буде встановлено логічне з'єднання – **віртуальний канал**. Віртуальний канал краще захищає користувачів від зовнішніх атак, оскільки у зловмисника немає можливості передавати пакети даних між довільними вузлами мережі, що можна зробити в мережах, побудованих на транспортних технологіях датаграмного типу, таких як IP або Ethernet.

Передавання кадрів уздовж віртуального каналу відбувається не на основі адрес кінцевих вузлів, а на основі мітки, яка дозволяє комутатору мережі визначати приналежність кадрів до того чи іншого віртуального каналу. Значення мітки потоку змінюється в кожному комутаторі при передачі кадру з вхідного інтерфейсу на вихідний – в цьому випадку говорять, що відбувається **комутація по мітках**. Комутація по мітках дозволяє позбутися від вимоги

унікальності їх значень в межах мережі, яку забезпечити складно. Для того, щоб кадри різних віртуальних каналів не змішувалися, досить забезпечити унікальність значень міток тільки в межах окремого інтерфейсу.

Технічно встановлення віртуального каналу означає формування записів в **таблицях просування кадрів** на кожному комутаторі уздовж віртуального каналу. Така таблиця включає інформацію про просування: на який вихідний порт потрібно передати кадр з даної міткою, яке нове значення потрібно присвоїти мітці після передачі кадру на вихідний інтерфейс.

На рис. 4.8 показаний фрагмент мережі, що складається з двох комутаторів S1 і S2 і чотирьох кінцевих вузлів C1-C4. Через ці комутатори прокладено три віртуальних канали: C1-C2, C1-C4 і C3-C4.

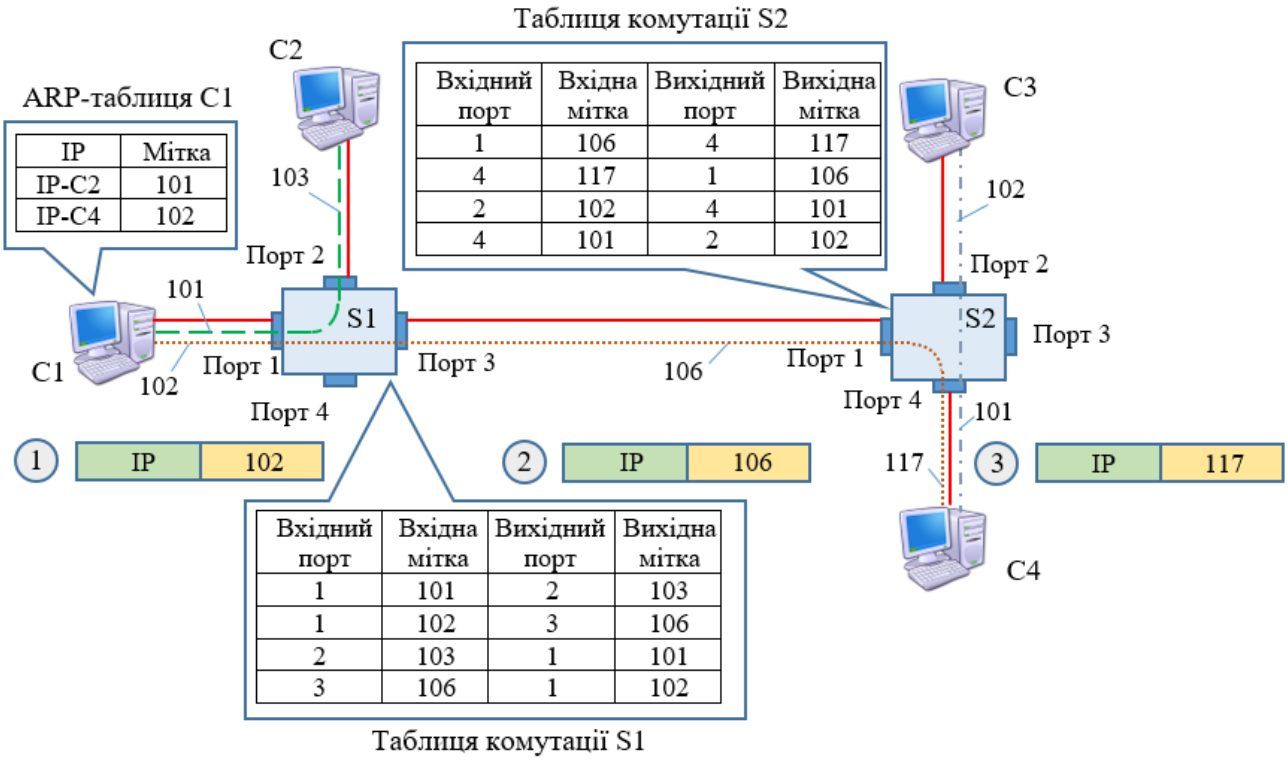



Рис. 4.8. Просування кадрів вздовж віртуальних каналів

Ці канали є двонаправленими, тобто кадри по них можуть передаватися в будь-якому з двох напрямків. Для кожного віртуального каналу в таблиці просування є два записи – по одному для кожного напрямку. Наприклад, перший запис у таблиці комутації комутатора S1 (запис 1-101-2-103) визначає роботу комутатора з просування кадрів віртуального каналу C1-C2 в напрямку від C1 до C2. Даний запис вказує комутатору S1 передати кадр, який прийнятий на порт 1 із значенням мітки 101, на порт 2 і поміняти значення мітки (скомутувати мітку) на 103. Третій запис (2-103-1-101) означає, що всі пакети, які надійдуть на

порт 2 зі значенням мітки 102, будуть скомутовані на порт 3, а значення мітки зміниться на 101.

Існують також однонаправлені віртуальні канали. У разі їх використання для дуплексного обміну інформацією потрібно встановити два незалежних віртуальних канали між кінцевими вузлами – по одному для кожного напрямку.

Віртуальні канали діляться на два класи (рис. 4.9):

- комутовані віртуальні канали (Switched Virtual Circuit, SVC);
- постійні віртуальні канали (Permanent Virtual Circuit, PVC).

Створення **комутованого віртуального каналу** відбувається за ініціативою кінцевого вузла мережі за допомогою спеціального протоколу, що посилає пакет із запитом на встановлення з'єднання в напрямку до вузла призначення віртуального каналу. Назва «комутований» відображає той факт, що канал створюється динамічно на вимогу вузла-відправника аналогічно встановленню комутованого з'єднання в телефонній мережі.

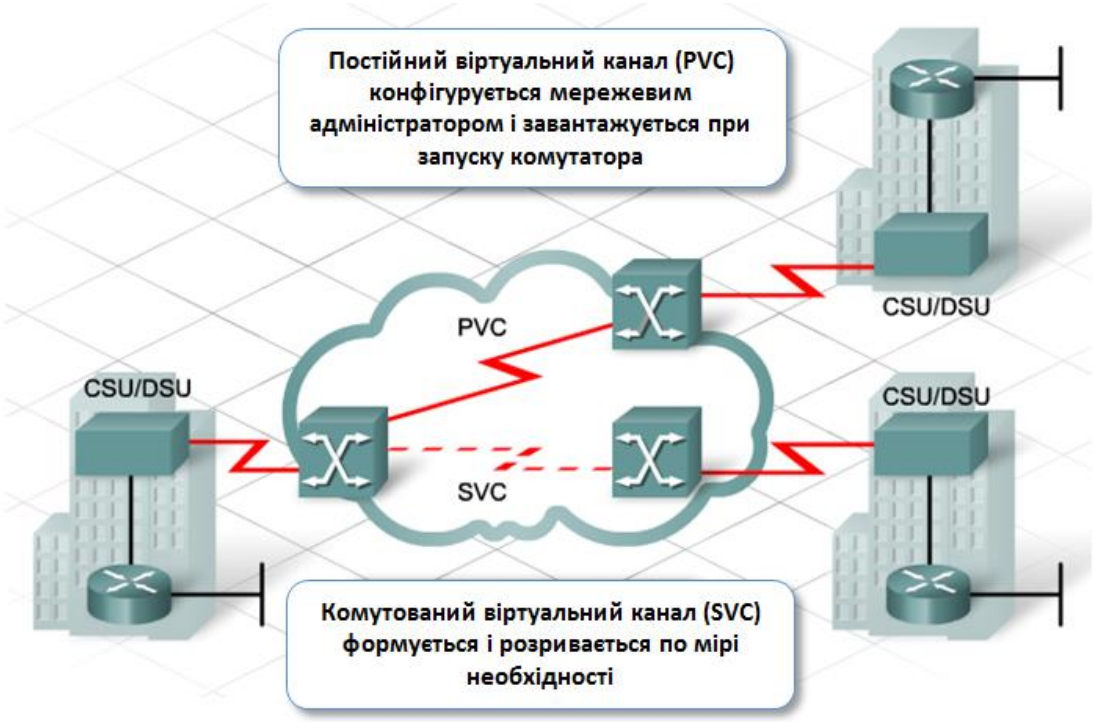
Для підтримки режиму SVC в мережі повинні існувати таблиці маршрутизації, відповідно до яких просувається пакет із запитом з'єднання. По відношенню до **пакету із запитом з'єднання** мережа працює в датаграмному режимі, і такий пакет повинен містити адресу призначення кінцевого вузла, а не мітку.

При встановленні каналу SVC відомості про встановлення з'єднання повинні передаватися до передачі інших даних. **Пакети про завершення зв'язку** розривають з'єднання після того, як воно більше не потрібне. Цей процес викликає затримки в мережі, так як канали SVC створюються і розриваються для кожного сеансу.

**Постійний віртуальний канал** встановлюється вручну. Адміністратор створює його на досить тривалий час (звідси назва), можливо, із залученням централізованої системи управління мережею. Приграничний комутатор мережі приймає пакети від зовнішньої мережі, яка може і не підтримувати техніку віртуальних каналів. Приграничний комутатор повинен якимось чином відображати пакети, що надходять ззовні на один з віртуальних каналів мережі. У найпростішому випадку таке відображення (mapping) виконується на основі вхідного фізичного інтерфейсу, тобто всі кадри, які приходять на деякий вхідний інтерфейс, відображаються на один і той же віртуальний канал. У більш складних випадках необхідно розрізняти кілька потоків, що приходять на вхідний інтерфейс, і відображати їх на різні віртуальні канали. В такому випадку в приграничному комутаторі поряд з таблицею просування повинна існувати таблиця відображення потоків. У прикладі рис. 4.8 така таблиця є у кінцевого

вузла С1. У ній, в якості ознаки потоку використовуються IP-адреси призначення, тому таблиця відображення являє собою ARP-таблицю.

Рис. 4.9. Комутований та постійний віртуальні канали




Мережі, що працюють на основі техніки віртуальних каналів, відносяться до типу **мереж, що не підтримують широкомовлення з множинним доступом** (Non Broadcast Multi-Access Network, **NBMA**). У такій мережі існує довільна кількість кінцевих вузлів, але відсутня можливість передавання кадру відразу всім вузлам. У мережах NBMA протокол IP не може скористатися послугами протоколу ARP для автоматичної побудови ARP-таблиці, так як ці послуги базуються на широкотрансляційних запитах. Так що в тих випадках, коли вхідний потік відображається на віртуальний канал на основі IP-адреси, таблицю відображення, яка являється ARP-таблицею, доводиться будувати вручну або ж за допомогою деякого додаткового протоколу, що не використовує широкомовлення.

**Ефективність віртуальних каналів**

Застосування комутованих віртуальних каналів вимагає попереднього встановлення з’єднання, що вносить додаткову затримку перед передачею даних в порівнянні із застосуванням датаграмних протоколів. Ця затримка особливо позначається при передачі невеликого обсягу даних, коли час встановлення віртуального каналу може бути співрозмірним з часом передачі даних. Крім того,

датаграмний метод швидше адаптується до змін в мережі. При відмові комутатора або лінії зв'язку уздовж віртуального каналу з'єднання розривається, і віртуальний канал потрібно прокладати заново, обходячи проблемні ділянки мережі.

Однак, слід врахувати, що час, витрачений на встановлення віртуального каналу, компенсується подальшою швидкою передачею всього потоку пакетів. Маршрутизація пакетів в мережі з підтримкою віртуальних каналів прискорюється за рахунок двох факторів. Перший полягає в тому, що рішення про просування пакета приймається швидше, так як таблиця комутації, в якій є інформація тільки про встановлені віртуальні канали, найчастіше істотно менша таблиці маршрутизації, в якій число записів визначається кількістю мереж призначення (розмір таблиці маршрутизації магістральних IP-маршрутизаторів провайдерів Інтернету становив навесні 2015 року близько 550 000 записів).

Другим фактором є зменшення частки службової інформації в пакетах. Адреси кінцевих вузлів в глобальних мережах, зазвичай мають досить велику довжину – 4 байти в версії IPv4, 16 байт в версії IPv6, MAC-адреса має довжину 6 байт. Номер ж віртуального каналу зазвичай займає 10-12 біт, так що накладні витрати на адресну частину істотно скорочуються, а значить, корисна швидкість передачі даних зростає.

Постійні віртуальні канали є набагато ефективнішими в плані продуктивності передачі даних, ніж комутовані. Значну частину роботи по маршрутизації пакетів мережі виконує адміністратор, вручну прописуючи постійні віртуальні канали і залишаючи комутаторам лише просування пакетів на основі готових таблиць комутації портів.

Постійний віртуальний канал подібний виділеному фізичному каналу в тому сенсі, що для кожної операції обміну даними не потрібно заново встановлювати або розривати з'єднання. Відмінність же полягає в тому, що користувач PVC не має гарантій щодо дійсної пропускної спроможності каналу. Зате застосування PVC, зазвичай набагато дешевше, ніж оренда виділеної лінії, так як користувач ділить пропускну спроможність мережі з іншими користувачами.

Постійні віртуальні канали вигідно використовувати для передачі **агрегованих потоків трафіку**, що складаються з великої кількості індивідуальних потоків абонентів мережі. У цьому випадку віртуальний канал прокладається не між кінцевими абонентами, а між ділянкою магістралі мережі, на якому даний агрегований потік існує, наприклад від одного прикордонного маршрутизатора мережі оператора зв'язку до іншого.

Таким чином, віртуальні канали більш ефективні при передачі довготривалих, ніж короткочасних, потоків, так як в цьому випадку знижуються витрати на встановлення з'єднань.

## 4.5. Технологія X.25

Технологія віртуальних каналів X.25 з'явилася на початку розвитку комп'ютерних мереж, практично одночасно з мережею ARPANET, що дало початок Інтернету і датаграмному протоколу IP. Довгий час, до середини 1980-х, X.25 була основною технологією для побудови як мереж операторів зв'язку, так і корпоративних мереж.

Технологія X.25 виявилася добре пристосованою для побудови глобальної всесвітньої мережі завдяки тому, що була масштабованою – в ній було визначено протокол міжмережевої взаємодії, що дозволяв об'єднувати мережі різних провайдерів.

X.25 – це типові мережі з налагодженням віртуальних з'єднань та комутацією пакетів (рис. 4.10). Мережі X.25 розробляли для каналів з низькою надійністю зв'язку. Тому, складовою таких мереж є жорсткі процедури виправляння помилок. Зокрема, кожен вузол мережі перевіряє коректність передавання та виконує коригувальні дії. Внаслідок виконання таких дій зменшується швидкість передавання даних.

X.25 визначає характеристики телефонної мережі для передачі даних. Для встановлення зв'язку, один комп'ютер звертається до іншого з запитом про сеанс зв'язку. Комп'ютер, що викликається може прийняти або відхилити зв'язок. Якщо виклик прийнятий, то обидві системи можуть почати передачу інформації з повним дублюванням. Будь-яка сторона може в будь-який момент припинити зв'язок.

Специфікація X.25 визначає двоточкову взаємодію між пристроями DTE і DCE. Пристрої **DTE** (термінали і головні обчислювальні машини в обладнанні користувача) під'єднуються до пристроїв **DCE** (модеми, комутатори пакетів і інші пристрої), що з'єднуються з **комутаторами переключення пакетів** (Packet Switching Exchange, **PSE)** і іншими DCE усередині **мережі передачі даних загального користування** (Public Data Network, **PDN)** і, нарешті, до іншого пристрою DTE. Взаємини між об'єктами мережі X.25 показані на рис. 4.11.

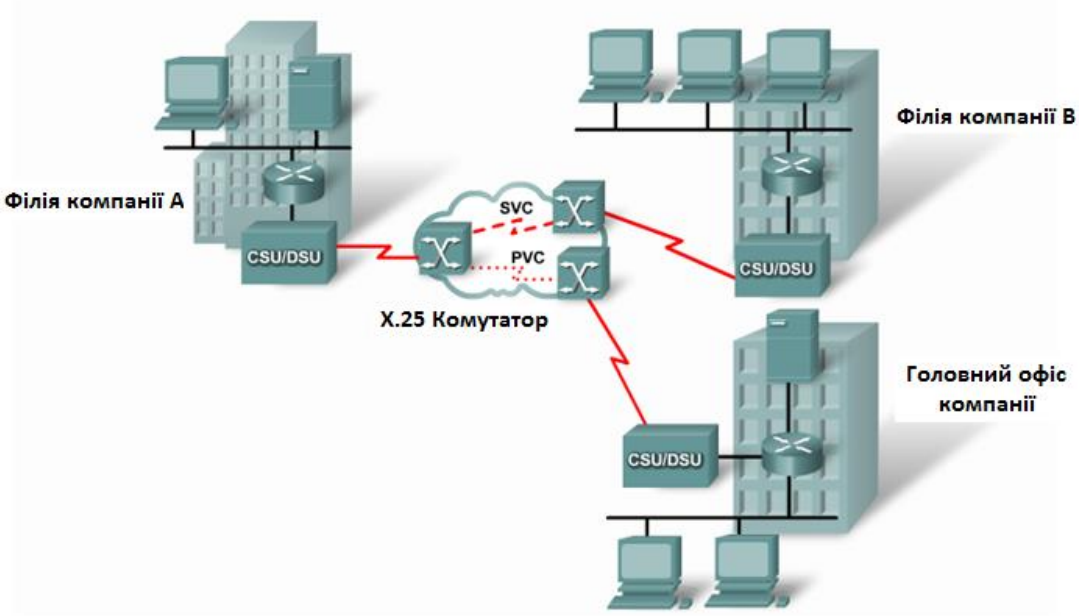



Рис. 4.10. Мережа X.25

Специфікація X.25 описана трьома нижніми рівнями моделі OSI. Мережевий рівень X.25 описує формати пакетів і процедури обміну пакетами між рівноправними об’єктами 3 рівня. Канальний рівень X.25 реалізований протоколом **процедури збалансованого доступу до каналу (**Link Access Procedure, Balanced, **LAPB)**. LAPB визначає кадрування пакетів для ланки DTE/DCE. Фізичний рівень X.25 визначає електричні і механічні процедури активації і дезактивації фізичного середовища, що з’єднує DTE і DCE. Фізичний рівень в той час найчастіше був представлений модемами, які працювали на комутованих і виділених телефонних лініях зі швидкостями 2400-9600 Кбіт/с.

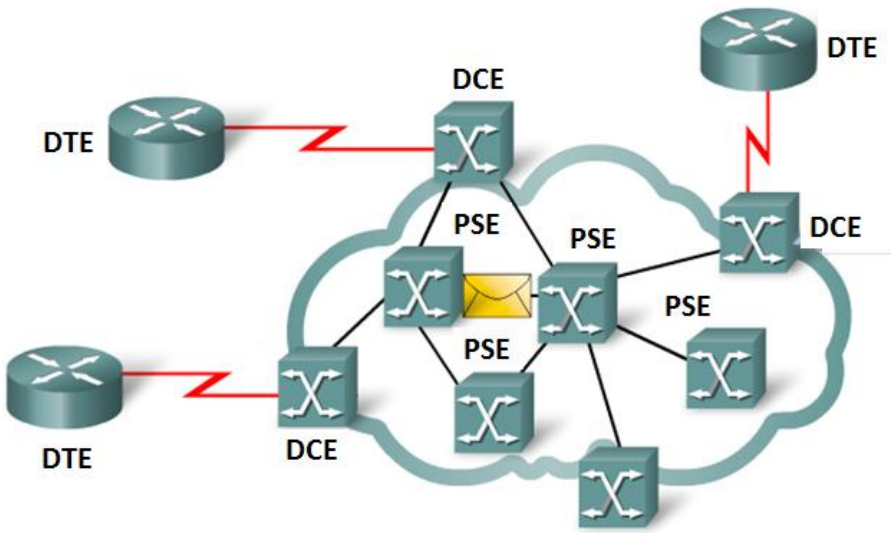



Рис. 4.11. Взаємини між об’єктами мережі X.25

Наскрізна передача між пристроями DTE виконується через віртуальні канали. Віртуальні канали дозволяють здійснювати зв'язок між різними елементами мережі через будь-яке число проміжних вузлів без визначених частин фізичного середовища, що є характерним для фізичних каналів.

Після того, як віртуальний канал створено, DTE надсилає пакет на інший кінець зв'язку шляхом відправлення його в DCE, використовуючи відповідний віртуальний канал. DCE переглядає номер віртуального каналу для визначення маршруту цього пакету через мережу X.25. Протокол мережевого рівня X.25 здійснює широкотрансляційну передачу між усіма DTE, які обслуговує пристрій DCE, що розташований в мережі з боку пункту призначення, у результаті чого пакет буде доставлений до DTE пункту призначення.

Усі термінали, які приєднують до мережі X.25, поділяють на термінали, що виконані з дотриманням вимог стандарту X.25 та інші. В першому випадку порядок приєднання описаний протоколом фізичного рівня X.25 bis, який еквівалентний протоколу RS-232-C. Протокол X.21bis є похідним від CCITT V24 і V.25, які відповідно ідентифікують кола обміну і характеристики електричних сигналів інтерфейсу DTE/DCE. Для приєднання не X.25 терміналів потрібні спеціальні пристрої – **протокольні конвертери**. Кілька терміналів приєднують до одного конвертера **PAD** (Packet Assembler/Disassembler – Пакетний Асемблер/Дисасемблер). PAD збирає символи з кількох терміналів, формує з них пакети X.25 та спрямовує у мережу. Набір протоколів, що описують взаємодію не X.25 терміналів:

• X.3 – дає змогу налагоджувати PAD для різних типів терміналів;

• X.28 – контроль з боку DTE за функціонуванням PAD;

• X.29 – протокол обміну між X.25 DTE та PAD або між двома PAD; зміна параметрів PAD з боку мережі в інтерфейсі PAD-мережа та PAD-віддалене DTE.

• X.32 – дає змогу користувачам одержати доступ до мереж X.25 через стандартні аналогові комутовані телефонні лінії, а не через виділені синхронні лінії, як у випадку X.25.

• X.75 – дає змогу сполучати різні мережі X.25 в одну.

Таким чином, мережі X.25 відносяться до однієї з найбільш старих і відпрацьованих технологій глобальних мереж. Надмірність функцій, спрямованих на забезпечення надійності передачі даних, пояснюється орієнтацією технології на ненадійні аналогові канали. Поширення високошвидкісних і надійних цифрових оптичних каналів в середині 80-х років призвело до того, що функції технології X.25 по забезпеченню надійної передачі даних перетворилися з переваги технології в її недолік, так як лише

сповільнювали швидкість передачі даних. Результатом цієї революції стала поява принципово нової технології глобальних мереж, а саме Frame Relay.

## 4.6. Мережі Frame Relay

Frame Relay (FR) можна розглядати і як спрощений варіант X.25 для надійних мереж та високих швидкостей передавання даних. Головна відмінність цієї мережі від X.25 – це те, що корекцію помилок виконують не проміжні, а кінцеві вузли. Вузол мережі Frame Relay виконує такі дві головні функції:

- перевіряє цілісність кадру; якщо кадр спотворений, його відкидають;
- перевіряє правильність адреси; якщо адреса невідома, кадр відкидають.

Завдяки зменшенню часу опрацювання даних у проміжних вузлах, затримка у вузлі Frame Relay становить близько 3 мс. Аналогічне значення для X.25 – 50 мс. Швидкість передавання Frame Relay становить – від 56 Кбіт/с до 2 Мбіт/с залежно від перепускної спроможності та кількості залучених каналів.

Аналогічно до X.25, технологія FR визначає тільки інтерфейс **UNI (User to Network Interface)** між DTE та DCE, не накладаючи обмеження на протоколи та архітектури магістральної мережі. Для сполучення двох мереж Frame Relay визначено інтерфейс **NNI (Network to Network Interface).**

На відміну від X.25, Frame Relay оперує тільки двома рівнями протоколів. Фізичний рівень подібний до такого ж рівня технології X.25 та відображає аспекти приєднання DTE і DCE. До DTE приєднують мости, маршрутизатори, комутатори та пристрої, функціонально аналогічні до PAD (**FPAD**). Для керування передаванням даних використовують **протокол доступу до каналу D** (Link Access Protocol D, **LAPD**). Базова версія Frame Relay не виконує декількох функцій канального рівня (виявлення та корекції помилок, керування потоком), однак підтримує такі функції мережевого рівня, як маршрутизація та керування логічними каналами. У протоколі Frame Relay використовується технологія комутації пакетів зі змінною довжиною.

Маршрутизатор, або пристрій DTE, підключається до мережі постачальника послуг, зазвичай, по виділеній лінії. При цьому з’єднання проходить через комутатор Frame Relay, або пристрій DCE, до найближчого місцевого постачальника послуг. Таке з’єднання утворює канал доступу (рис. 4.12).

Віддалений маршрутизатор на іншому кінці мережі також є пристроєм DTE. З’єднання між двома кінцевими пристроями DTE здійснюється по віртуальному каналу.

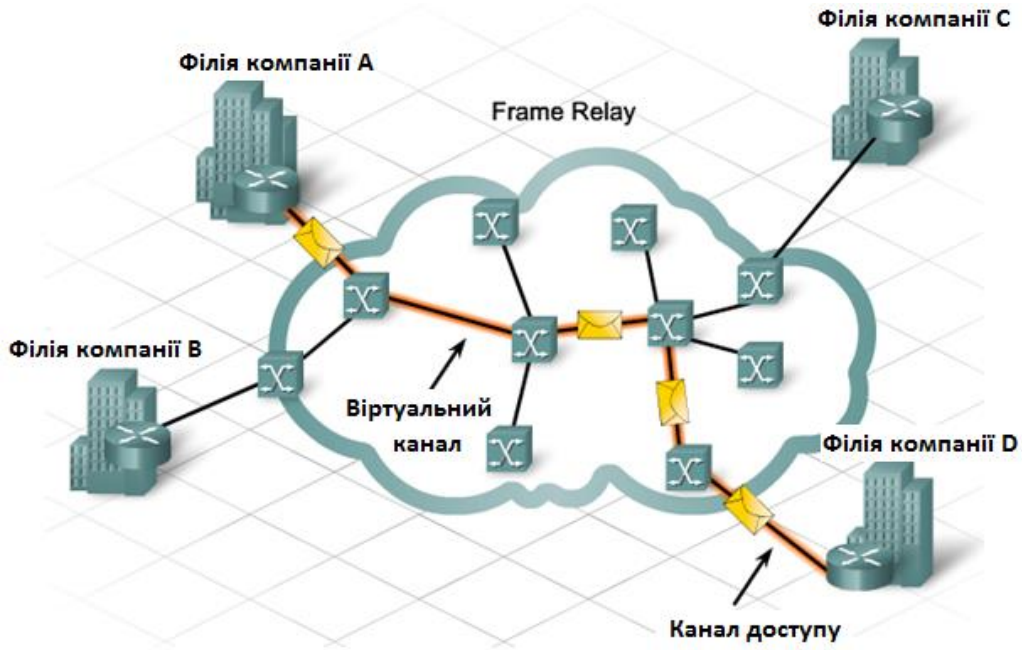



Рис. 4.12. Використання віртуальних каналів в мережі Frame Relay

На відміну від X.25, Frame Relay використовує, в основному, постійні віртуальні канали (PVC). Більшість постачальників послуг не підтримують або навіть забороняють використовувати комутовані віртуальні канали (SVC) в мережі Frame Relay. У випадку розриву зв'язку Frame Relay автоматично перемаршрутизовує з'єднання.

Frame Relay – це мережа, що не підтримує широкомовлення з множинним доступом (NBMA). У мережі NBMA кожному віртуальному каналу для ідентифікації потрібна адреса канального рівня. У мережі Frame Relay такою адресою є **ідентифікатор каналу зв'язку** (Data-Link Connection Identifier, **DLCI)**.

Ідентифікатор DLCI визначає віртуальний канал, по якому будуть передаватись дані в точку призначення. Ідентифікатор DLCI записаний в поле адреси кожного переданого кадру. DLCI, зазвичай, має тільки локальне значення і може відрізнятися в кожній кінцевій точці віртуального каналу.

DLCI канального рівня пов'язаний з адресою мережевого рівня (IP адресою) пристрою, розміщеного на іншому кінці віртуального каналу. Співставлення DLCI та віддаленої IP-адреси можна виконувати вручну або динамічно за допомогою протоколу інверсного ARP (Inverse Address Resolution Protocol, **Inverse ARP** або **InARP**).

Співставлення DLCI та віддаленої IP-адреси виконується за допомогою таких дій (рис. 4.13):

1. Локальний пристрій оголошує про свою присутність за допомогою відправки своєї адреси мережевого рівня по віртуальному каналу.

2. Віддалений пристрій отримує цю інформацію і співставляє IP-адресу мережевого рівня з локальним DLCI канального рівня.

3. Віддалений пристрій оголошує свою IP-адресу по віртуальному каналу.

4. Локальний пристрій співставляє адресу мережевого рівня віддаленого пристрою та локальний DLCI, на який була отримана ця інформація.

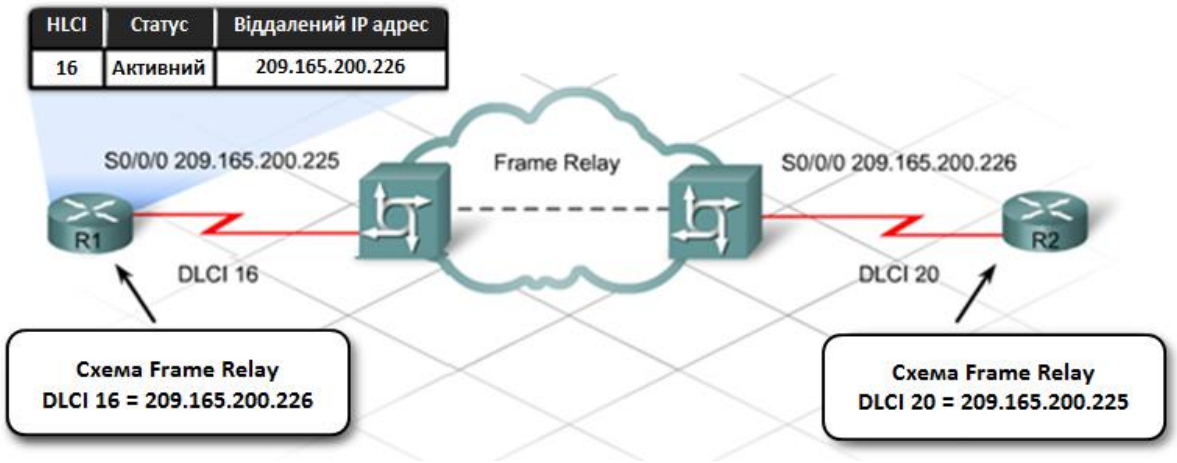



Рис. 4.13. Механізм співставлення DLCI та віддаленої IP-адреси

**Інтерфейс локального управління** (Local Management Interface, **LMI**) є стандартом передачі сигналів між DTE і комутатором Frame Relay. LMI доповідає про стан PVC між пристроями.

Повідомлення LMI забезпечують зв’язок і синхронізацію між мережею і пристроєм користувача. Вони періодично надають звіт про виникнення нових PVC і видалення існуючих. Повідомлення LMI також надають відомості про цілісність постійного віртуального каналу. Повідомлення про стан віртуального каналу запобігають відправці даних через неіснуючі PVC.

Інтерфейс локального управління надає відомості про стан з’єднання по віртуальному каналу, які відображаються в таблиці співставлень Frame Relay (рис. 4.14):

**Активний стан** (Active State) – з’єднання активне, маршрутизатори можуть обмінюватися даними.

**Неактивний стан** (Inactive State) – локальне з’єднання з комутатором Frame Relay виконується, але віддалене з’єднання з комутатором Frame Relay відсутнє.

**Віддалений стан** (Deleted State) – локальне з'єднання не отримує повідомлень інтерфейсу локального управління від комутатора Frame Relay або відсутній зв'язок між маршрутизатором телекомунікаційного обладнання клієнта (CPE) і комутатором Frame Relay.

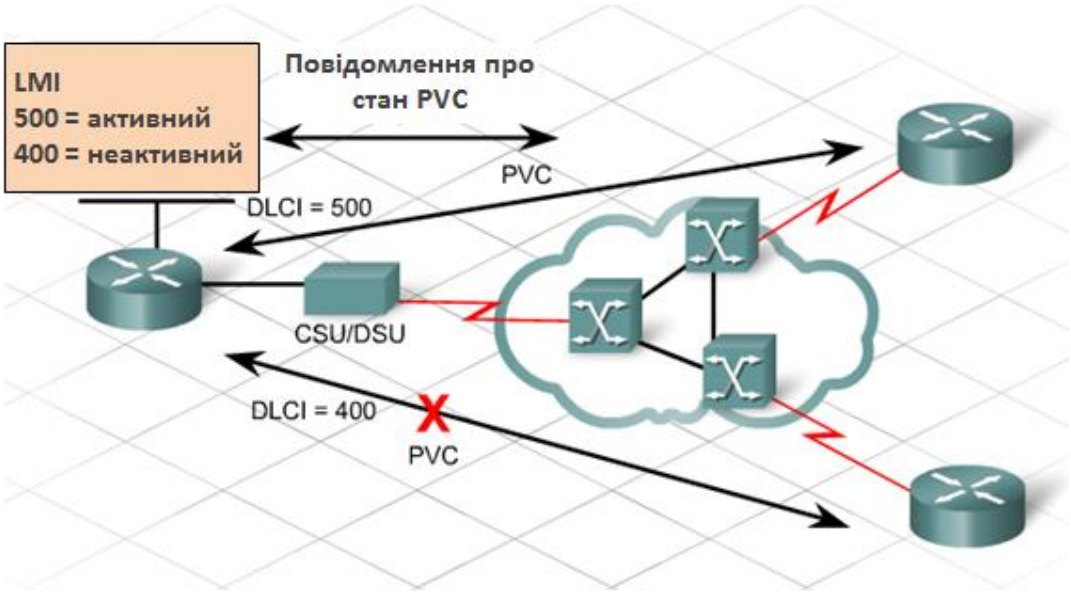



Рис. 4.14. Повідомлення про стан PVC

При підписці кінцевого користувача на послугу Frame Relay він погоджує певні параметри обслуговування з постачальником. Одним з таких параметрів є **гарантована швидкість передачі** (Committed Information Rate, **CIR**). Параметр CIR визначає мінімальну смугу пропускання, гарантовану постачальником для передачі даних по віртуальному каналу (рис. 4.15).


Рис. 4.15. Передача даних в мережі Frame Relay

Параметр CIR визначає мінімальну швидкість передачі даних, проте при відсутності завантаженості каналів постачальник послуг може збільшувати смугу пропускання до узгодженого значення **максимальної швидкості передачі** (Maximum Information Rate, **MIR**).

**Форсована швидкість передачі** (Excess Information Rate**, EIR**) є середнім перевищенням швидкості в порівнянні з CIR, яке може підтримувати віртуальний канал при відсутності перевантаження в мережі. Будь-яке перевищення гарантованої швидкості, аж до максимальної швидкості, **називається форсованим пакетом (**excess burst**, Be).**

Кадри, які одержані в діапазоні швидкостей до CIR, будуть передані. Передача кадрів на швидкості, що перевищує CIR, не гарантується, але підтримується, якщо це допускається можливостями мережі. Такі додаткові кадри позначаються як **кадри, які можуть бути відкинуті (**Discard Eligible**, DE).** У разі перевантаження в мережі, постачальник в першу чергу відкидає кадри, які мають значення DE. Кадри, одержані в діапазоні швидкостей понад MIR будуть відкинуті.

Альтернативою до використання PVC є застосування комутованих віртуальних каналів (SVC). На відміну від постійних, комутовані канали формуються під час передавання.

Відмінність між PVC та SVC полягає в наступному. Користувач PVC повинен перед початком передавання «придбати» певний PVC з визначеним CIR, він оплачує його незалежно від ступеня реального використання каналу. Користувач SVC оплачує реальні параметри потоку. На початку передавання структура каналу PVC відома. Рішення про конфігурування каналу PVC ухвалює адміністратор, а рішення про структуру каналу SVC – інтелектуальні вузли-комутатори.

Мережі Frame Relay набули великого поширення в 1980-і і в першій половині 1990-х років. Їхні послуги з надання гарантійної пропускної спроможності були в той час найбільш якісними послугами VPN, і багато корпоративних мереж їх використовували. Однак, поступово швидкість доступу 2 Мбіт/с, яку надавали ці мережі, стала явно недостатньою для корпоративних користувачів.

До того ж мультимедійний трафік почав все більше цікавити як користувачів, так і провайдерів Інтернету, а мережі Frame Relay були розраховані тільки на передачу комп’ютерного трафіку. В результаті, на початку 1990-х років була почата розробка нової технології глобальних мереж, що отримала назву асинхронного режиму передачі.

## 4.7. Мережі ATM

**Асинхронний режим передачі** (Asynchronous Transfer Mode, **ATM**) – це технологія, що заснована на техніці віртуальних каналів і призначена для використання в якості єдиного універсального транспорту мереж з інтегрованим обслуговуванням (рис. 4.16). Назва цієї технології відображає той факт, що в ній застосовується метод комутації пакетів, який, як відомо, базується на асинхронному часовому мультиплексуванні даних на відміну від синхронного часового мультиплексування, на якому побудовані технології комутації каналів.

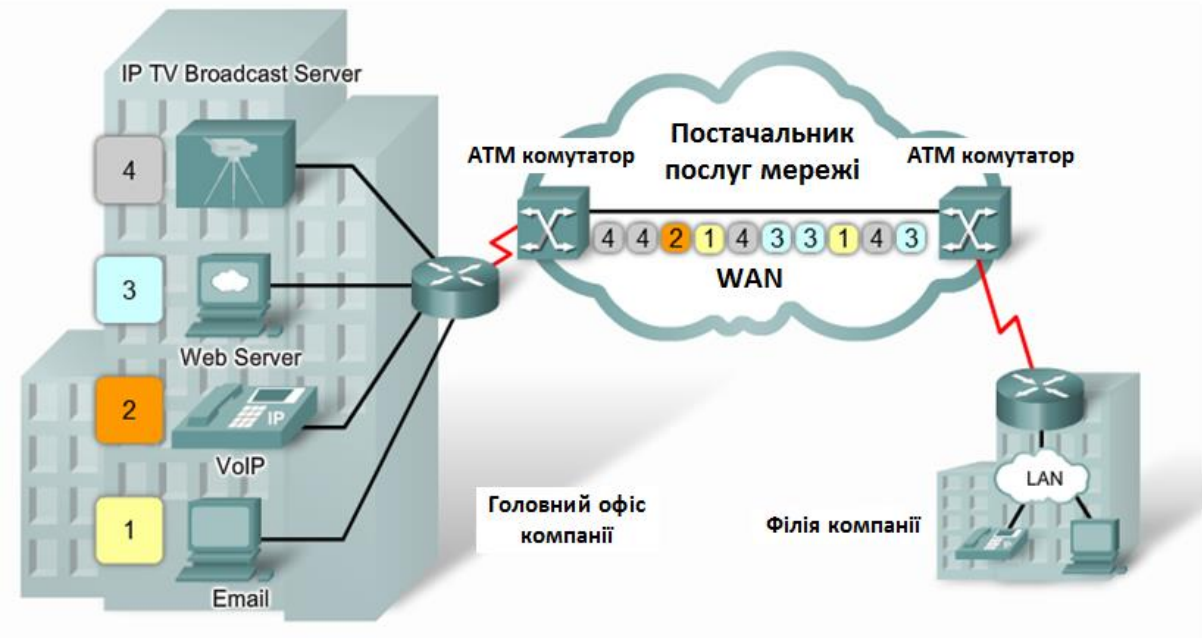



Рис. 4.16. Мережа ATM

Під інтегрованим обслуговуванням розуміється здатність мережі передавати єдиним потоком інформацію з різними вимогами до затримок передавання та достовірності (аудіо-, відеоінформація, дані, інформація електронних систем сигналізації тощо). Під час передавання аудіо- або відеоінформації невелике спотворення даних цілком допустиме і суттєво не впливає на якість сигналу, а під час передавання даних спотворення навіть одного біта недопустиме. Водночас під час передавання аудіо- та відеоінформації потрібна стала швидкість передавання, а під час передавання даних швидкість може бути змінною. Цим технологія ATM принципово відрізняється від технології Frame Relay, яка призначалася тільки для передачі еластичного комп’ютерного трафіку.

Крім того, у цілі розробників технології ATM входило забезпечення багаторівневої ієрархії швидкостей і можливості використання первинних мереж SDH для з'єднання комутаторів ATM.

У технології ATM інформація передається в комірках (cells) фіксованого розміру в 53 байти, з них 48 байт призначені для даних, а 5 байт – для службової інформації (для заголовка комірки ATM). Комірки не містять адресної інформації та контрольної суми даних, що прискорює їх обробку і комутацію.

20-байтовими адресами отримувача та відправника обмінюються тільки в момент встановлення віртуального з'єднання. Основна функція заголовка зводиться до ідентифікації віртуального з'єднання. В процесі передачі інформації комірки пересилаються між вузлами через мережу комутаторів, з'єднаних між собою цифровими лініями зв'язку. ATM комутатори виконують свої функції апаратно, що прискорює читання ідентифікатора в заголовку комірки, після чого комутатор переправляє її з одного порту в інший.

Телекомунікаційна мережа, що використовує технологію ATM, складається з набору комутаторів, що пов'язані між собою. Комутатори ATM підтримують два види інтерфейсів: **UNI (**User-Network Interface – інтерфейс «користувач-мережа») та **NNI (**Network-Network Interface – інтерфейс «мережа-мережа»**).**

Мережа ATM описує тільки інтерфейсні характеристики і для передавання даних може використовувати широкий спектр реальних каналів та комунікаційних мереж. З іншого боку, для зовнішнього користувача вона може надавати сервіс багатьох мереж та протоколів (Frame Relay, X.25, TCP/IP, SPX/IPX та ін.). Магістральними каналами для передавання даних між комутаторами ATM можуть бути канали T1/T3, E1/E3, SDH/SONET і навіть звичайні канали комутованої телефонної мережі.

Для передачі даних в мережі ATM формується віртуальне з'єднання (PVC чи SVC). Віртуальне з'єднання визначається поєднанням ідентифікатора віртуального шляху і ідентифікатора віртуального каналу.

Віртуальний канал є з'єднанням, встановленим між двома кінцевими вузлами на час їх взаємодії, а віртуальний шлях – це шлях між двома комутаторами. При створенні віртуального каналу, комутатори визначають, який віртуальний шлях використовувати для досягнення пункту призначення. По одному і тому ж віртуальному шляху може передаватися одночасно трафік багатьох віртуальних каналів.

Віртуальні з'єднання ATM можуть працювати зі **сталою бітовою швидкістю** (Constant Bit Rate, **CBR**) – для передавання звукових чи відеопотоків, або зі **змінною бітовою швидкістю** (Variable Bit Rate, VBR) для передавання комп'ютерних даних. Кожне віртуальне з'єднання має власний набір параметрів:

- пікова швидкість передавання (Peak Cell Rate, PCR) – максимальна кількість комірок, яку відправнику дозволено передавати за одиницю часу;
- нормальна швидкість передавання (Sustained Cell Rate, **SCR**) – середня кількість комірок, яку відправнику дозволено передавати за одиницю часу;
- мінімальна швидкість передавання (Minimum Cell Rate, **MCR**) – мінімальна кількість комірок, яку відправник повинен передати за одиницю часу.

Наявність окремих категорій послуг для найбільш важливих класів трафіку, таких як чутливий до затримок голосовий трафік з постійною бітовою швидкістю і чутливий до затримок компресований відеотрафік зі змінною бітовою швидкістю, зробило ATM набагато більш ефективною технологією мультисервісних мереж, ніж технологія Frame Relay, яка могла ефективно передавати тільки нечутливий до затримок трафік комп'ютерних даних зі змінною бітовою швидкістю. Технологія ATM усуває відмінності між локальними та глобальними мережами, перетворюючи їх у єдину інтегровану мережу.

Технологія ATM пережила пік своєї популярності в другій половині 1990-х років, але на сьогоднішній час вона практично не використовується. Причин відмови від даної технології декілька. Одна з них – поява мереж DWDM і зростання швидкості мереж Ethernet до 1 Гбіт/с, а потім і до 10 Гбіт/с. Відносно дешева пропускна спроможність простої мережі Ethernet перемогла – операторам мереж виявилося набагато простіше надавати якісні мультимедійні послуги за допомогою недовантаженої мережі IP/Ethernet, ніж керувати складною в налаштуванні і експлуатації мережею IP/ATM.

Крім того, обладнання ATM не змогло перейти поріг швидкості в 622 Мбіт/с. Обмеженням став малий розмір комірок – на високих швидкостях комутатори важко обробляти інтенсивні потоки таких комірок.

# 5. Комутація в телекомунікаційних мережах

## 5.1. Логічна структуризація мереж

### 5.1.1. Міст як попередник і функціональний аналог комутатора

Сучасні **комутатори** (switch) Ethernet є спадкоємцями **мостів** (bridge), які широко використовувалися в мережах Ethernet і Token Ring з поділюваним середовищем. Основна відмінність комутатора від моста полягає в більшій кількості портів (міст, як правило, мав два порти, що і послужило приводом для його назви – міст між двома сегментами) і більш високій продуктивності.

Комутатори поряд з маршрутизаторами сьогодні є основними комунікаційними пристроями, що застосовуються для побудови телекомунікаційних мереж. Комутатори відрізняються внутрішньою архітектурою і конструктивним виконанням. Зараз комутовані локальні мережі витіснили локальні мережі на поділювальному середовищі. Їх успіх вплинув на еволюцію Ethernet – в нових швидкісних версіях Ethernet, таких як 10G і 100G Ethernet, стандарт IEEE 802.3 описує роботу вузлів тільки в комутованому середовищі.

Міст локальної мережі (LAN bridge), або просто міст, з’явився як засіб побудови великих локальних мереж на поділювальному середовищі. Міст об’єднує два або більше поділюваних середовища в єдину мережу, при цьому передача кадрів між вузлами кожного з поділюваних середовищ відбувається за стандартними правилами ізольованого поділюваного середовища. Міст відповідає тільки за передачу кадрів між об’єднаними середовищами, які називаються **сегментами мережі.**

У мережі Ethernet вимога використовувати єдине поділюване середовище призводить до двох обмежень:

- загальний діаметр мережі не може бути більше 2500 м;
- кількість вузлів не може перевищувати 1024 (для мереж Ethernet на коаксіалі це обмеження ще жорсткіше).

На практиці через головну проблему поділюваного середовища – дефіциту пропускної спроможності – кількість вузлів в мережах Ethernet на поділювальному середовищі ніколи не наближається до 1024.

Обмеження, що виникають через використання єдиного поділюваного середовища, можна подолати, виконавши логічну структуризацію мережі. Для цього потрібно сегментувати єдине поділюване середовище на кілька і з’єднати отримані сегменти мережі деяким комунікаційним пристроєм, який не передає

дані побітно, як повторювач, а буферизує кадри і передає їх потім в той чи інший сегмент (або сегменти) залежно від адреси призначення кадру (рис. 9.1).

Потрібно відрізняти логічну структуризацію від фізичної. Наприклад, концентратори стандарту 10Base-T дозволяють побудувати мережу, що складається з декількох сегментів кабелю на скручений парі, але це – фізична структуризація, так як логічно всі ці сегменти являють собою єдине поділюване середовище (рис. 9.1, в). Логічна структуризація мережі за допомогою мостів/комутаторів є першим кроком на шляху віртуалізації мережі, так як користувачам окремого логічного сегмента надається віртуальний ресурс – комунікаційне середовище з певною пропускною спроможністю.

Логічна структуризація локальної мережі дозволяє вирішити кілька завдань, основні з яких – підвищення продуктивності, гнучкості та безпеки, а також поліпшення керованості мережі.

Підвищення продуктивності мережі, розділеної комутатором на сегменти, відбувається через те, що середовище кожного сегмента поділяється тепер між меншим числом кінцевих вузлів. У прикладі на рис. 5.1 при поділі загального середовища на три сегменти максимальна кількість вузлів, що поділяють середовище, знизилась з 8 до 3. Як правило, розбиття на сегменти виконується так, щоб міжсегментний трафік був невеликим, цього можна домогтися, наприклад, якщо кожен сегмент забезпечити власним сервером, обслуговуючим запити комп’ютерів сегмента.

При побудові мережі як сукупності сегментів кожен з них може бути адаптований до специфічних потреб робочої групи або відділу. Це означає підвищення гнучкості мережі. Процес розбиття мережі на логічні сегменти можна розглядати і в зворотному напрямку, як процес створення великої мережі з уже наявних невеликих мереж.

Встановлюючи різні логічні фільтри на мостах/комутаторах, можна контролювати доступ користувачів до ресурсів інших сегментів, чого не дозволяють робити повторювачі. Так досягається підвищення безпеки даних.

### 5.1.2. Алгоритм прозорого моста IEEE 802.1D

Слово «прозорий» в назві алгоритму прозорого моста відображає той факт, що кінцеві вузли мережі функціонують, «не помічаючи» присутності в мережі мостів.

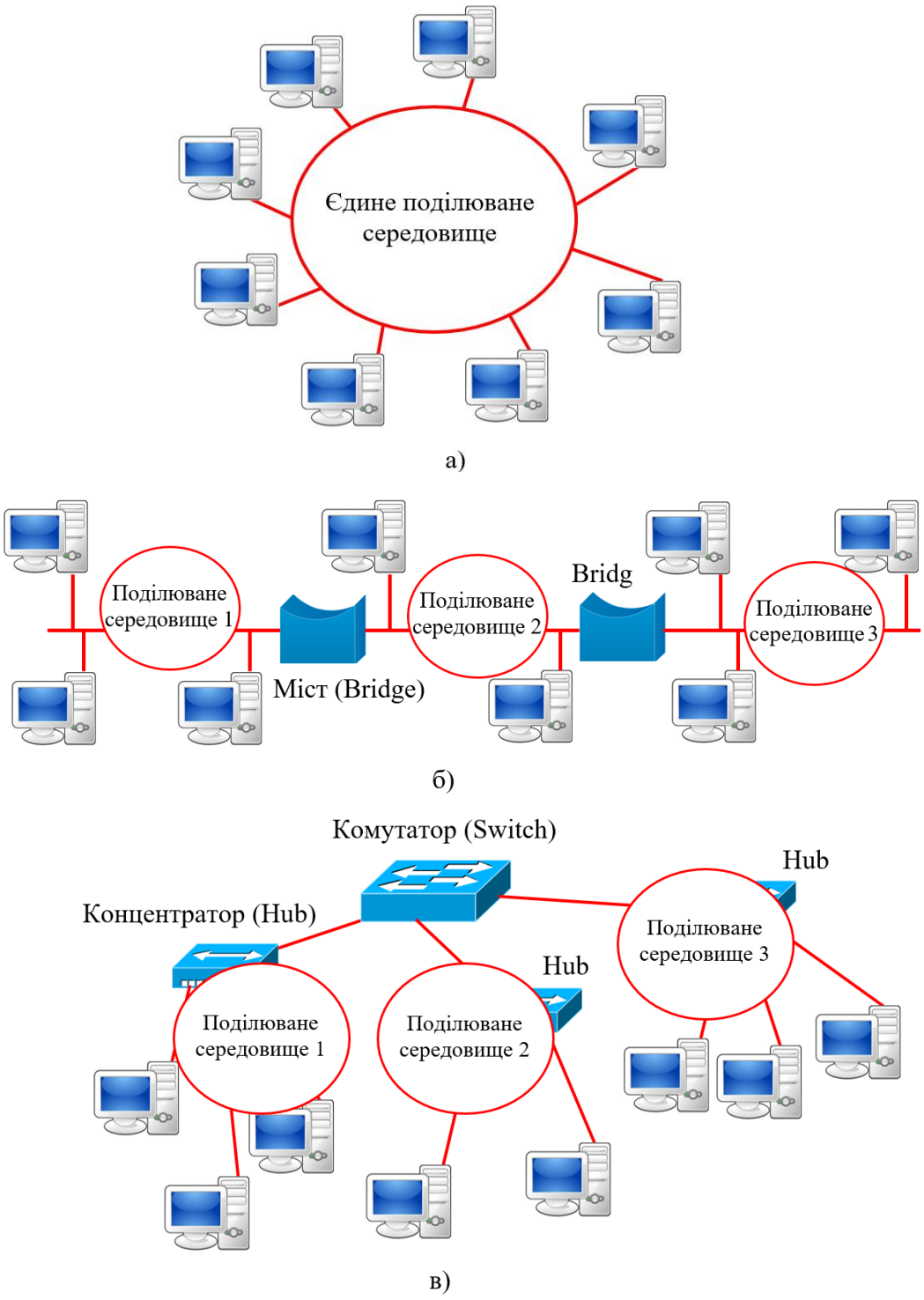



Рис. 5.1. Логічна структуризація мережі: а) єдине поділюване середовище;
б) логічна структуризація за допомогою мостів;
в) логічна структуризація за допомогою комутатора

Міст будує свою таблицю просування (таблицю комутації) на підставі пасивного спостереження за трафіком, що циркулює в підключених до його

портів сегментах. При цьому міст враховує адреси відправників кадрів даних, що надходять на його порти. За адресою відправника кадру міст робить висновок про приналежність цього вузла до того чи іншого сегменту мережі.

Розглянемо процес автоматичного створення таблиці комутації моста і її використання на прикладі простої мережі, представленої на рис. 5.2.

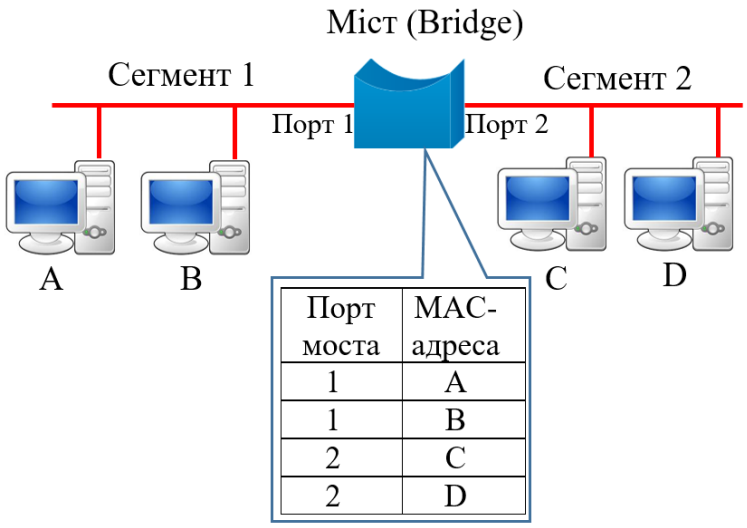



Рис. 5.2. Принцип роботи алгоритму прозорого моста

Міст з'єднує два мережевих сегмента. Сегмент 1 складають комп'ютери, під'єднанні за допомогою відрізка коаксіального кабелю до порту 1 моста, а сегмент 2 – комп'ютери, під'єднанні за допомогою іншого відрізка коаксіального кабелю до порту 2 моста. У початковому стані міст не знає про те, комп'ютери з якими MAC-адресами під'єднанні до кожного з його портів. У цій ситуації міст просто передає будь-який захоплений і буферизований кадр на всі свої порти, за винятком того порту, від якого цей кадр отриманий. У прикладі на рис. 9.2 у моста тільки два порти, тому він передає кадри з порту 1 на порт 2, і навпаки. Відмінність роботи моста від повторювача полягає в тому, що перед передаванням кадру міст його попередньо буферизує, а не здійснює передавання біт за бітом, як це робить повторювач. Буферизація скасовує логіку роботи всіх сегментів як єдиного поділюваного середовища. Коли міст збирається передати кадр з сегмента в сегмент, наприклад з сегмента 1 в сегмент 2, він, як звичайний кінцевий вузол, намагається отримати доступ до середовища сегмента 2 за правилами алгоритму доступу, в даному прикладі – за правилами алгоритму CSMA/CD.

Одночасно з передачею кадру на всі порти міст вивчає адресу відправника кадру і робить запис про його приналежність до того чи іншого сегменту в своїй адресній таблиці. Цю таблицю також називають таблицею комутації, або

просування. Наприклад, отримавши на порт 1 кадр від комп'ютера А, міст робить перший запис у своїй таблиці комутації:

Порт моста 1 – MAC-адреса А

Цей запис означає, що комп'ютер, який має MAC-адресу А, належить сегменту під'єднаному до порту 1 моста. Якщо всі чотири комп'ютери даної мережі проявляють активність і посилають один одному кадри, то скоро міст побудує повну таблицю комутації, що міститиме чотири записи – по одному запису на вузол (див. рис. 5.2).

При кожному надходженні кадру на порт моста він перш за все намагається знайти адресу призначення кадру в таблиці комутації. Алгоритм прозорого моста IEEE 802.1D описує наступні дії моста (див. рис. 5.2):

1. При отриманні кадру, направленого від комп'ютера А до комп'ютера С, міст переглядає таблицю комутації на предмет збігу адреси в будь-якому з її записів з адресою призначення – MAC-адресою С. Запис з шуканою адресою існує в таблиці комутації.
2. Міст виконує другий етап аналізу таблиці – перевіряє, чи знаходяться комп'ютери з адресами відправника і отримувача в одному сегменті. У прикладі комп'ютер А (MAC-адреса А) і комп'ютер С (MAC-адреса С) знаходяться в різних сегментах. Отже, міст виконує операцію **просування** (Forwarding) кадру – передає кадр в порт 2, який з'єднаний із сегментом отримувача.
3. Якби виявилося, що комп'ютери належали одному сегменту, то кадр просто був би видалений з буфера. Така операція називається **фільтрацією** (Filtering).
4. Якби запис про MAC-адресу С був відсутній в таблиці комутації, тобто, адреса призначення була б невідома мосту, то він передав би кадр на всі свої порти, крім порту – відправника кадру, як і на початковій стадії процесу навчання. Такий механізм називається **затопленням мережі** (Flooding).

Процес навчання моста ніколи не закінчується і відбувається одночасно з просуванням і фільтрацією кадрів. Міст постійно стежить за адресами джерела буферизованих кадрів, щоб автоматично пристосовуватися до змін, що відбуваються в мережі, – переміщенням комп'ютерів з одного сегмента мережі в інший, відключенням і появою нових комп'ютерів.

Входи таблиці комутації можуть бути динамічними, що створюються в процесі самонавчання мосту, і статичними, що створюються вручну адміністратором мережі. **Статичні записи** не мають терміну життя, що дає

адміністратору можливість впливати на роботу моста, наприклад обмежуючи передачу кадрів з певними адресами з одного сегмента в інший.

**Динамічні записи** мають термін життя – при створенні або оновленні запису в таблиці комутації з ним пов'язується позначка часу. Після закінчення певного тайм-ауту запис позначається як недійсний, якщо за цей час міст не прийняв жодного кадру з даною адресою в полі адреси відправника. Це дає можливість мосту автоматично реагувати на переміщення комп'ютера з сегмента в сегмент – при його від'єднанні від старого сегмента запис про приналежність комп'ютера до цього сегменту згодом викреслюється з адресної таблиці. Після під'єднання комп'ютера до іншого сегменту його кадри почнуть потрапляти в буфер моста через інший порт і в адресній таблиці з'явиться новий запис, що відповідає поточному стану мережі.

Кадри з **широкотрансляційними** (broadcast) і **груповими** (multicast) MAC-адресами, як і кадри з **невідомими адресами** (unknown unicast) призначення, передаються мостом на всі його порти. Такий режим поширення кадрів називається **затопленням мережі** (Flooding). Наявність мостів в мережі не перешкоджає поширенню широкомовних і групових кадрів по всіх сегментах мережі. Однак це є перевагою лише тоді, коли таку адресу коректно вказано працюючим вузлом.

Нерідко в результаті будь-яких програмних або апаратних збоїв протокол верхнього рівня або мережевий адаптер починає працювати некоректно, а саме постійно з високою інтенсивністю генерувати кадри з широкотрансляційною адресою. Міст у відповідності зі своїм алгоритмом передає помилковий трафік в усі сегменти. Така ситуація називається **широкотрансляційним штормом** (broadcast storm).

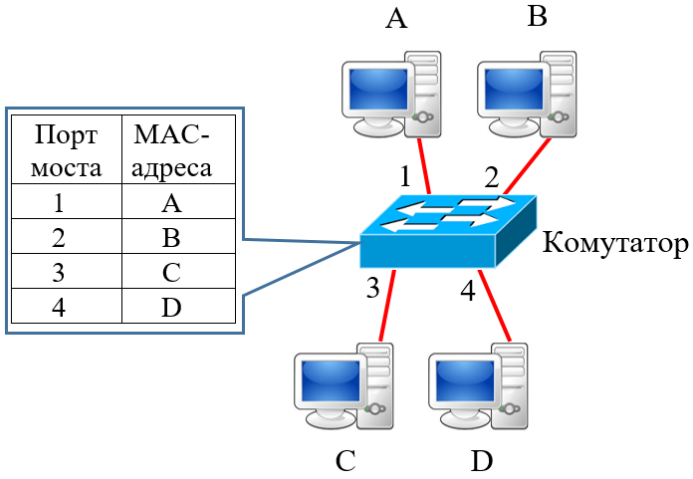
На жаль, мости не захищають мережі від широкотрансляційного шторму, в усякому разі, за замовчуванням, як це роблять маршрутизатори. Максимум, що може зробити адміністратор за допомогою комутатора для боротьби з широкотрансляційним штормом – встановити для кожного порту моста гранично допустиму інтенсивність передачі кадрів з широкотрансляційною адресою. Але при цьому потрібно точно знати, яка інтенсивність є нормальною, а яка – помилковою. При зміні протоколів ситуація в мережі може змінитися, і те, що раніше вважалося помилковим, зараз може виявитися нормою.

## 5.2. Комутатори

### 5.2.1. Принцип роботи комутатора

Принцип роботи комутатора аналогічний роботі моста і базується на алгоритмі прозорого моста IEEE 802.1D. Для того, щоб передавати кадри (фрейми), комутатор використовує таблицю комутації. Спочатку, після включення комутатора, таблиця порожня. Комутатор заповнює її автоматично, при отриманні кадрів від комп'ютерів (хостів). Коли комутатор отримує кадр, він спочатку передає його відповідно до своїх правил, а потім запам'ятовує MAC-адресу відправника, вказану у кадрі і ставить її у відповідність порту на якому він був отриманий.

Наприклад, для зображеної схеми (рис. 5.3), підсумкова таблиця комутації матиме такий вигляд (після того, як усі хости передавали якийсь трафік).




| Порт моста | MAC-адреса |
|---|---|
| 1 | A |
| 2 | B |
| 3 | C |
| 4 | D |

Рис. 5.3. Схема підключення комутатора та таблиця комутації

Коли таблиця заповнена, комутатор знає які хости знаходяться у нього на яких портах і передає кадри на відповідні порти.

Кадр, що **адресований лише одному абоненту** (unicast), для якого у комутатора немає запису в таблиці комутації, називається кадром з **невідомою адресою** (unknown unicast).

#### Механізми передачі кадрів

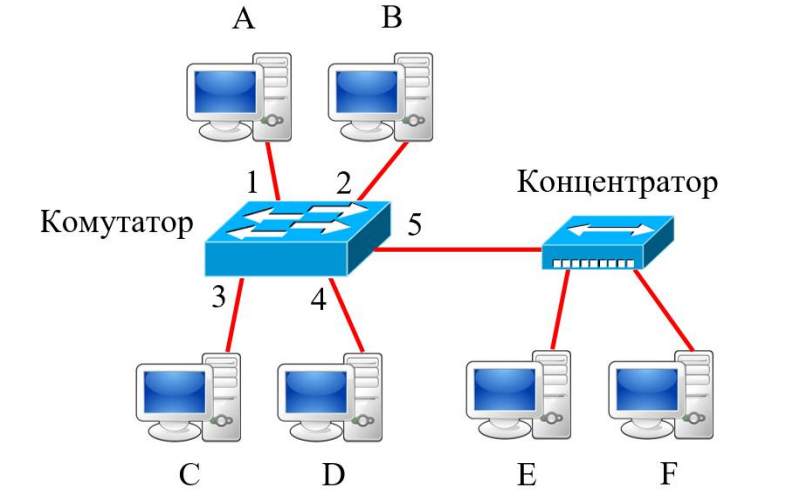
Для того, щоб передавати кадри комутатор використовує ці ж самі, що і міст, три базові механізми:

- **Flooding** (затоплення мережі) – кадр, що надійшов на один з портів передається на інші порти комутатора. Комутатор виконує цю операцію в

двох випадках: при отриманні broadcast або multicast (якщо не налагоджена підтримка multicast) кадру; при отриманні unknown unicast кадру. Це дозволяє комутатору доставити кадр хосту (за умови, що хост досяжний і існує), навіть коли він не знає де знаходиться хост.

- **Forwarding** (просування) – передача кадру, що надійшов на один порт комутатора через інший порт відповідно до запису в таблиці комутації.
- **Filtering** (фільтрація) – якщо комутатор отримує кадр через певний порт і MAC-адреса отримувача доступна через цей же порт (це вказано в таблиці комутації), то комутатор відкидає кадр. Тобто, комутатор вважає, що в цьому випадку хост вже отримав цей кадр і не дублює його.

Приклад мережі для демонстрації використання механізмів передачі кадрів через комутатор (рис. 5.4).




| Порт моста | MAC-адреса |
|---|---|
| 1 | A |
| 2 | B |
| 3 | C |

а)

| Порт моста | MAC-адреса |
|---|---|
| 1 | A |
| 2 | B |
| 3 | C |
| 4 | D |

б)

| Порт моста | MAC-адреса |
|---|---|
| 1 | A |
| 2 | B |
| 3 | C |
| 4 | D |
| 5 | E |
| 5 | F |

в)

Рис. 5.4. Приклад мережі для демонстрації використання механізмів передачі кадрів в комутаторі

Спочатку до комутатора були під’єднані три хости A, B і C. Відповідно у комутатора створилась таблиця комутації, що зображена на рис. 5.4, а.

Коли хост A відправлятиме кадр хосту B, комутатор використає механізм просування (**forwarding**), оскільки йому відомо знаходження обидвох хостів

(згідно таблиці комутації), причому ці хости під'єднані до різних портів комутатора.

Пізніше до комутатора під'єднали хост D. Якщо хост A відправить кадр хосту D, то для комутатора це буде unknown unicast кадр, оскільки в таблиці комутації немає запису про MAC-адресу D. Відповідно до своїх правил комутатор виконає механізм **flooding** і направить кадр на усі порти, окрім 1 (з якого кадр був отриманий). Після того, як комутатор отримає кадр від хоста D, він запам'ятає його адресу і створить відповідний запис в таблиці комутації (рис. 5.4, б).

Далі до комутатора під'єднали концентратор з двома хостами, після чого комутатор вивчив їх адреси. Відповідна таблиця комутації (рис. 5.4, в).

Якщо після цього хост E передаватиме кадр хосту F, то комутатор отримає його, але не передаватиме далі. У цій ситуації комутатор використає механізм **filtering**, оскільки MAC-адреса одержувача надійшла з того ж порту, до якого під'єднаний відправник.

## Методи передачі кадрів

Для просування кадрів комутатори можуть використовувати два методи комутації: комутацію з проміжним зберіганням і наскрізну комутація.

**Комутація з проміжним зберіганням** (Store and Forward) припускає повну буферизацію кадру перш ніж буде прийнято рішення про його просування. Це дозволяє реалізувати безліч функцій, пов'язаних з контролем передачі кадру. Наприклад, можна перевіряти його контрольну суму (Cyclic Redundancy Check, CRC), реалізувати пріоритетну передачу (QoS), контроль доступу по портах (port security) або за списками контролю доступу (Access Control List, ACL).

**Наскрізна комутація** (Cut through) відрізняється тим, що буферизація не відбувається і рішення про просування приймається відразу, після прийому перших 6 байтів кадру, в яких міститься MAC-адреса отримувача. Такий спосіб просування кадрів працює швидше, ніж попередній, але при цьому не можна реалізувати додаткові функції обробки кадрів. Розрізняють два види наскрізної комутації:

1. **Швидке просування** (Fast-forward switching): найшвидший тип, кадр починає передаватися відразу після прийому адреси отримувача. Існує ймовірність появи незавершених кадрів, передача яких може бути перервана колізією.
2. **Просування без фрагментів** (Fragment-free switching): трохи повільніше, оскільки просування кадру починається тільки після того, як будуть прийняті перші 64 байти кадру. Це забезпечить

гарантію того, що при передачі кадру в сегменті відправника не виникало колізій і кадр далі передаватиметься гарантовано повністю.

### Буферизація в пам'яті

Комутатори Ethernet під час прийому кадру зберігають його у буферній пам'яті перш ніж почати пересилку. Також буферна пам'ять використовується, якщо порт призначення зайнятий і кадр поміщається у буфер вже на етапі передачі.

Розрізняють два методи буферизації – буферизація на порту і буферизація із загальною пам'яттю.

У випадку з **буферизацією на порту** (port based), кадри зберігаються в чергах, що пов'язані з конкретними портами на вході і виході.

При **буферизації із загальною пам'яттю** (shared memory), кадри поміщаються в загальну пам'ять, доступну усім портам, звідки і зчитуються для передачі на інший порт. До порту прив'язуються конкретні кадри, а не черги, це дає можливість передавати кадри між портами, уникаючи переписування їх в іншу чергу. Кількість кадрів, що зберігаються обмежує тільки об'єм буферної пам'яті комутатора.

## 5.2.2. Паралельна комутація

При появі в кінці 80-х – початку 90-х років швидких протоколів, продуктивних персональних комп'ютерів, мультимедійної інформації та поділі мережі на велику кількість сегментів класичні мости перестали справлятися з роботою. Обслуговування потоків кадрів між декількома портами за допомогою одного процесорного блоку вимагало значного підвищення швидкодії процесора, а це досить дороге рішення.

Більш ефективним виявилося рішення, яке і «породило» комутатори: для обслуговування потоку, що надходить на кожен порт, в пристрій встановлювався окремий спеціалізований процесор, який реалізовував алгоритм моста. По суті, комутатор – це мультипроцесорний міст, здатний паралельно просувати кадри відразу між усіма парами своїх портів. Але якщо при додаванні процесорних блоків комп'ютер не перестали називати комп'ютером, а додали тільки прикметник «мультипроцесорний», то з мультипроцесорними мостами сталася метаморфоза – багато в чому з маркетингових причин вони перетворилися в комутатори. Окрім процесорів портів комутатор має центральний процесор, який координує роботу портів, відповідаючи за побудову загальної таблиці

просування, а також підтримуючи функції конфігурації і управління комутатором.

Згодом комутатори витіснили з локальних мереж класичні однопроцесорні мости. Основна причина цього – більш висока продуктивність, з якою комутатори передають кадри між сегментами мережі.

Продуктивність комутаторів на кілька порядків вища, ніж мостів – комутатори можуть передавати до декількох десятків, а іноді й сотень мільйонів кадрів в секунду, в той час як мости, зазвичай, обробляли 3-5 тисяч кадрів в секунду.

За час свого існування комутатори увібрали в себе багато додаткових функцій, які утворились в результаті природного розвитку мережевих технологій. До цих функцій належать, наприклад, підтримка віртуальних мереж (VLAN), агрегування ліній зв'язку, пріоритезація трафіку і т. п. Розвиток технології виробництва замовних мікросхем також сприяв успіху комутаторів, в результаті процесори портів сьогодні володіють такою обчислювальною потужністю, яка дозволяє їм швидко реалізовувати досить складні алгоритми обробки трафіку, наприклад виконувати його класифікацію і профілювання.

Основною причиною підвищення продуктивності мережі при використанні комутатора є паралельна обробка декількох кадрів.

Цей ефект ілюструє рис. 5.5, на якому показана ідеальна щодо продуктивності ситуація, коли чотири порти з восьми передають дані з максимальною для протоколу Fast Ethernet швидкістю в 100 Мбіт/с. Причому, вони передають ці дані на інші чотири порти комутатора не конфліктуючи: потоки даних між вузлами мережі розподілилися так, що для кожного приймаючого кадри порту є свій вихідний порт. Якщо комутатор встигає обробляти вхідний трафік при максимальній інтенсивності надходження кадрів на вхідні порти, то загальна продуктивність комутатора в наведеному прикладі складе 4×100 = 400 Мбіт/с, а при узагальненні прикладу для $N$ портів – ($N/2$) × 100 Мбіт/с. У такому випадку говорять, що комутатор надає кожній станції або сегменту, підключеному до його портів, виділену пропускну спроможність протоколу.

Зрозуміло, що в мережі не завжди складається описана ситуація. Якщо двом станціям, наприклад, станціям, під'єднаним до портів 3 і 4, одночасно потрібно записувати дані на сервер, що під'єднаний до порту 8, то комутатор не зможе виділити кожній станції по 100 Мбіт/с, так як порт 8 не в змозі передавати дані зі швидкістю 200 Мбіт/с. Кадри станцій чекатимуть у внутрішніх чергах вхідних портів 3 і 4, коли звільниться порт 8 для передачі чергового кадру. Очевидно, хорошим рішенням для такого розподілу потоків даних було б

під’єднання сервера до більш високошвидкісного порту, наприклад Gigabit Ethernet.

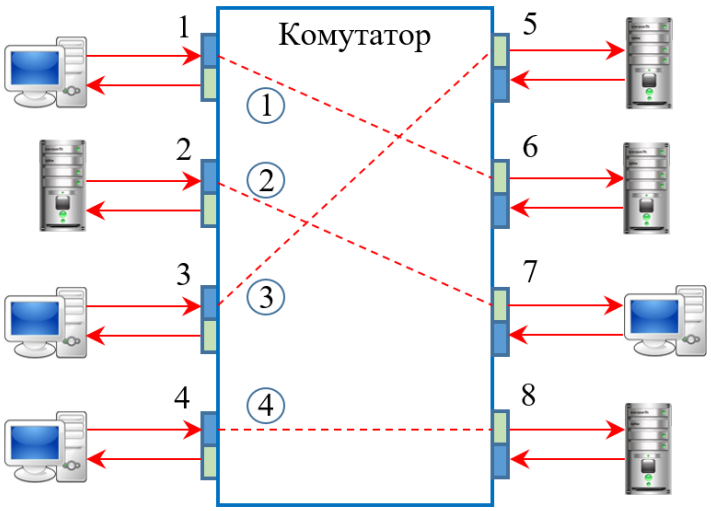



Рис. 5.5. Паралельне передавання кадрів комутатором

### 5.2.3. Дуплексний режим роботи

Технологія комутації сама по собі не має безпосереднього відношення до методу доступу до середовища, який використовується портами комутатора. При підключенні до порту комутатора сегмента, що являє собою поділюване середовище, даний порт, як і всі інші вузли такого сегмента, повинен підтримувати напівдуплексний режим.

Однак коли до кожного порту комутатора під’єднаний не сегмент, а тільки один комп’ютер, причому за двома фізично розділеними каналам, як це відбувається майже у всіх стандартах Ethernet, крім коаксіальних версій Ethernet, ситуація стає не такою однозначною. Порт може працювати як в звичайному напівдуплексному режимі, так і в дуплексному.

В **напівдуплексному режимі** роботи порт комутатора як і раніше розпізнає колізії. Доменом колізії в цьому випадку є ділянка мережі, що включає передавач комутатора, приймач комутатора, передавач мережевого адаптера комп’ютера, приймач мережевого адаптера комп’ютера і дві скручені пари дротів, які з’єднують передавачі з приймачами. Колізія виникає, коли передавачі порту комутатора і мережевого адаптера одночасно або майже одночасно починають передачу своїх кадрів.

У **дуплексному режимі** одночасна передача даних передавачами порту комутатора і мережевого адаптера колізією не вважається. В принципі, це досить

природний режим роботи для окремих дуплексних каналів передачі даних, і він завжди використовувався в протоколах глобальних мереж. При дуплексному зв'язку порти Ethernet стандарту 10 Мбіт/с можуть передавати дані зі швидкістю 20 Мбіт/с – по 10 Мбіт/с у кожному напрямку.

Довгий час комутатори Ethernet співіснували в локальних мережах з концентраторами Ethernet: на концентраторах будувалися нижні рівні мережі будівлі, такі як мережі робочих груп і відділів, а комутатори використовувались для об'єднання цих сегментів в загальну мережу. Поступово комутатори стали застосовуватися і на нижніх поверхах, витісняючи концентратори, так як ціни комутаторів постійно знижувалися, а їх продуктивність росла (за рахунок підтримки більш швидкісних версій технології Ethernet, тобто Fast Ethernet зі швидкістю 100 Мбіт/с, Gigabit Ethernet, 10G Ethernet і 100G Ethernet зі швидкістю 100 Гбіт/с. Цей процес завершився витісненням концентраторів Ethernet і переходом до повністю комутованих мереж, приклад такої мережі показаний на рис. 5.6.

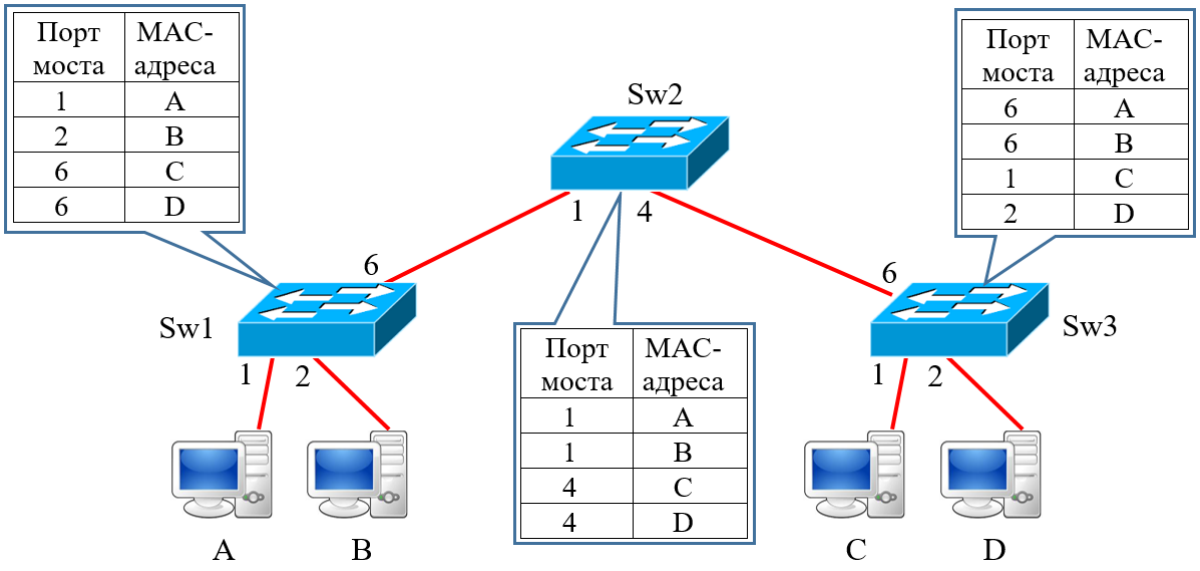



Рис. 5.6. Повністю комутована мережа Ethernet

У повністю комутованою мережі Ethernet всі порти працюють в дуплексному режимі, а просування кадрів здійснюється на основі MAC-адрес. При розробці технологій Fast Ethernet і Gigabit Ethernet дуплексний режим став одним з двох повноправних стандартних режимів роботи вузлів мережі. Однак практика застосування перших комутаторів з портами Gigabit Ethernet показала, що вони практично завжди застосовуються в дуплексному режимі для взаємодії з іншими комутаторами або високошвидкісними мережевими адаптерами. Тому, при розробці версій стандартів 10G і 100G Ethernet його розробники не стали

створювати версію для роботи в напівдуплексному режимі, остаточно закріпивши відхід поділюваного середовища з технології Ethernet.

### 5.2.4. Неблокуючі комутатори

Висока продуктивність є однією з головних переваг комутаторів. З поняттям продуктивності тісно пов'язано поняття неблокуючого комутатора.

Комутатор називають **неблокуючим** (non-blocking switch), якщо він може передавати кадри через свої порти з тією ж швидкістю, з якою вони на них надходять.

Коли говорять, що комутатор може підтримувати стійкий неблокуючий режим роботи, то мають на увазі, що комутатор передає кадри зі швидкістю їх надходження протягом довільного проміжку часу. Для підтримки подібного режиму потрібно таким чином розподілити потоки кадрів у вихідні порти, щоб, по-перше порти справлялися з навантаженням, по-друге, комутатор міг завжди в середньому передати на виходи стільки кадрів, скільки їх надійшло на входи. Якщо ж вхідний потік кадрів (підсумований по всіх портах) в середньому буде перевищувати вихідний потік кадрів (також підсумований по всіх портах), то кадри будуть накопичуватися в буферній пам'яті комутатора і при переповненні – просто відкидатися.

Іноді кажуть, що комутатор підтримує **миттєвий неблокуючий режим.** Це означає, що він може приймати і обробляти кадри від всіх своїх портів на максимальній швидкості протоколу незалежно від того, чи забезпечуються умови стійкої рівноваги між вхідним і вихідним трафіком. Правда, обробка деяких кадрів при цьому може бути неповною – при зайнятості вихідного порту кадр поміщається в буфер комутатора.

Способи, якими здійснюється здатність комутатора підтримувати неблокуючий режим, можуть бути різними. Необхідною вимогою є вміння процесора порту обробляти потоки кадрів з максимальною для фізичного рівня цього порту швидкістю.

Однак тільки адекватної продуктивності процесорів портів недостатньо для того, щоб комутатор був неблокуючим. Необхідно, щоб достатньою продуктивністю володіли всі елементи архітектури комутатора, включаючи центральний процесор, загальну пам'ять, шини, що з'єднують окремі модулі між собою, саму архітектура комутатора. В принципі, завдання створення неблокуючого комутатора аналогічне завданню створення високопродуктивного комп'ютера – в обох випадках вона вирішується комплексно: за рахунок відповідної архітектури об'єднання модулів в єдиному пристрої та адекватної продуктивності кожного окремого модуля пристрою.

### 5.2.5. Усунення проблем, що пов’язані з перевантаженнями

Навіть в тому випадку, коли комутатор є неблокуючим, немає гарантії того, що він у всіх випадках впорається з потоком кадрів, які направляються на його порти. Неблокуючі комутатори теж можуть відчувати перевантаження і втрачати кадри через переповнення внутрішніх буферів.

Основною причиною перевантажень комутатора є обмежена пропускна спроможність конкретного вихідного порту, яка визначається параметрами протоколу. Таким чином, якою б продуктивністю комутатор не володів, завжди знайдеться такий розподіл потоків кадрів, який призведе до перевантаження комутатора через обмеження продуктивності вихідного порту комутатора.

Виникнення таких перевантажень зумовлено відмовою від застосування алгоритму доступу до поділюваного середовища, оскільки в дуплексному режимі роботи портів втрачається контроль над потоками кадрів, які направляються кінцевими вузлами в мережу. У напівдуплексному режимі, властивому технологій з поділюваним середовищем, потік кадрів регулюється самим методом доступу до середовища. При переході на дуплексний режим вузлу дозволяється відправляти кадри до комутатора завжди, коли це йому потрібно, тому в даному режимі комутатори мережі можуть стикатися з перевантаженнями, не маючи при цьому жодних засобів «пригальмовування» потоку кадрів.

Таким чином, якщо вхідний трафік нерівномірно розподіляється між вихідними портами, легко уявити ситуацію, коли на будь-який вихідний порт комутатора прямуватиме трафік з сумарною середньою інтенсивністю більшою, ніж протокольний максимум. На рис. 5.7 показана якраз така ситуація, коли на порт 3 комутатора Ethernet від портів 1, 5, 6 і 8 направляється потік кадрів розміром в 64 байти з сумарною інтенсивністю в 22 100 кадрів в секунду. Відомо, що максимальна швидкість кадрів в секунду для сегмента Ethernet складає 14 880. Таким чином, коли кадри надходять в буфер порту зі швидкістю 22 100 кадрів в секунду, а виходять зі швидкістю 14 880 кадрів в секунду, то внутрішній буфер вихідного порту починає заповнюватися необробленими кадрами.

У наведеному прикладі неважко підрахувати, що при розмірі буфера в 100 Кбайт повне заповнення буфера відбудеться через 0,22 секунди після початку роботи в такому інтенсивному режимі. Збільшення розміру буфера до 1 Мбайт дасть збільшення часу заповнення буфера до 2,2 секунди, що також неприйнятно. Проблему можна вирішити за допомогою засобів контролю перевантаження.

Існують різні засоби контролю перевантаження: управління чергами в комутаторах, зворотний зв'язок, резервування пропускної здатності. На основі цих засобів можна створити ефективну систему підтримки показників QoS для трафіків різних класів.

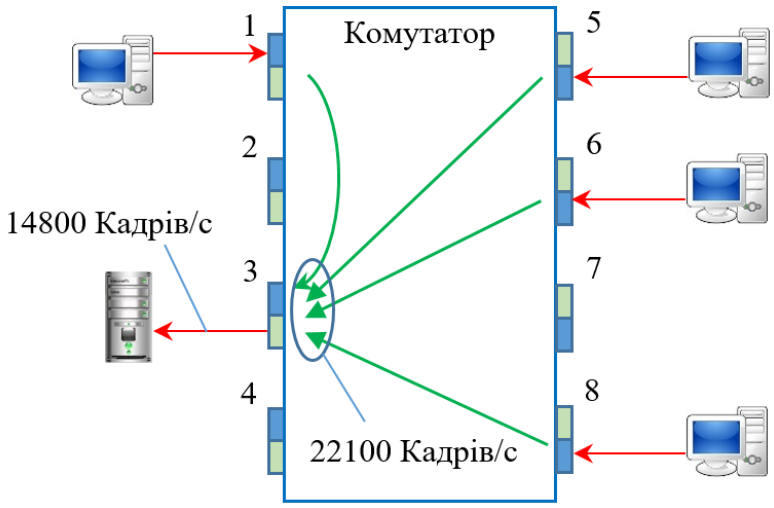



Рис. 5.7. Переповнення буфера порта через незбалансованість трафіку

Проблема, проілюстрована на рис. 7.7, може бути вирішена і іншим способом: застосуванням так званого **магістрального**, або висхідного (uplink), порту. Магістральні порти в комутаторах Ethernet – це, як правило, порти наступного рівня ієрархії швидкості в порівнянні з портами, призначеними для підключення користувачів. Наприклад, якщо комутатор має 12 портів Ethernet стандарту 10 Мбіт/с, то магістральний порт повинен бути портом Fast Ethernet, щоб його швидкість була достатня для передачі до 10 потоків від вхідних портів. Зазвичай низькошвидкісні порти комутатора служать для під'єднання комп'ютерів, а магістральні порти – для під'єднання або сервера, до якого звертаються користувачі, або комутатора більш високого рівня ієрархії.

На рис. 5.8 показаний приклад комутатора, що має 24 порти стандарту Fast Ethernet зі швидкістю 100 Мбіт/с, до яких під'єднані комп'ютери користувачів, і один порт стандарту Gigabit Ethernet зі швидкістю 1000 Мбіт/с, до якого під'єднаний сервер. При такій конфігурації комутатора ймовірність перевантаження портів істотно знижується в порівнянні з варіантом, коли всі порти підтримують однакову швидкість.

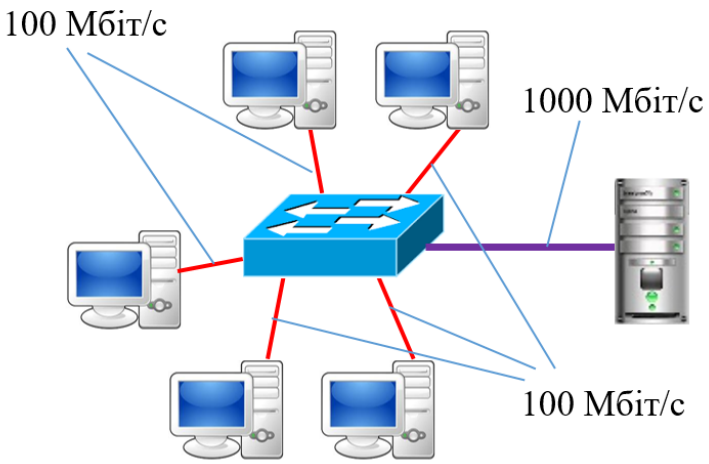



Рис. 5.8. Комутатор робочої групи

## 5.3. Комутована ієрархічна модель мережі

### 5.3.1. Рівні ієрархічної моделі

При розробці телекомунікаційних мереж потрібно враховувати те, що вони застосовуються не лише для передавання даних, але і для передавання голосової і відеоінформації. У такому разі виникає необхідність в структуризації потоків інформації, наприклад, локалізувати трафік між серверами або усередині відділів, виділити окремо голосовий трафік, щоб не виникало затримок, пов'язаних з передачею інформації в загальній мережі. Допомогти в досягненні цих і інших, подібних цілей, може введення ієрархічної структури розподілу використовуваного обладнання і кінцевих вузлів, ґрунтуючись на їх функціональних особливостях.

Типова ієрархічна модель, яка використовується при розробці мережі має три рівні – ядро (core), розподільчий рівень (distribution) і рівень доступу (access). Приклад такої структури наведений на рис. 5.9.

Кожен рівень, у свою чергу, виконує своє коло завдань:

**А. Рівень доступу** (Access Layer) призначений для підключення безпосередньо кінцевих пристроїв мережі – комп'ютерів, IP-телефонів, принтерів.

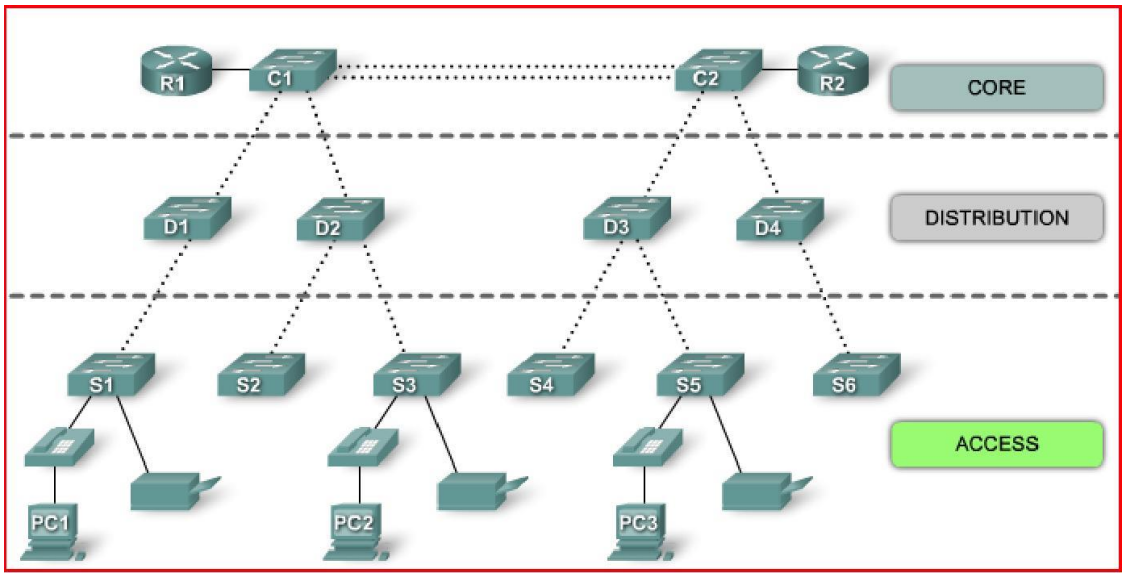



Рис. 5.9. Ієрархічна модель мережі

**В. Розподільчий рівень** (Distribution Layer) збирає потоки даних з комутаторів рівня доступу і направляє їх на рівень ядра. На цьому рівні вже можуть застосуються списки контролю доступу, розподіл по віртуальних локальних мережах, і маршрутизація між ними.

**С. Рівень ядра** (Core Layer) в ієрархічній моделі служить магістраллю, до якої ставляться особливі вимоги по швидкості комутації і надійності. Цей рівень керує потоками даних, що передаються між комутаторами рівня розподілу і також відповідає за з'єднання з мережею Інтернет.

Переваги ієрархічної моделі:

1. Масштабованість.

Модульний дизайн дає можливість легко додавати комутатори на рівень доступу без необхідності часто розширювати рівень розподілу або ядра.

2. Відмовостійкість.

Вихід з ладу будь-якого з компонентів мережі, не позначається на працездатності окремих її частин.

3. Продуктивність.

Використання агрегованих каналів для зв'язку між рівнями дозволяє збільшити пропускну здатність мережі в її вузьких місцях.

4. Безпека.

Комутатори на кожному з рівнів дозволяють виконувати контроль доступу як до самої мережі (port security), так і до різних мережевих служб при допомозі політик доступу (acl).

5. Керованість.

Комутатори на кожному рівні мають схожу функціональність і тому при впровадженні нових комутаторів досить просто копіювати конфігурацію із вже налагоджених пристроїв.

6. Підтримка.

Модульна архітектура дозволяє досить легко розширювати мережу, не вдаючись до глобальної заміни комутаторів у разі нестачі портів, на кожному з рівнів, включаючи ядро.

### 5.3.2. Принципи ієрархічного дизайну

**Діаметр мережі.**

При ієрархічному проектуванні мережі, слід особливу увагу приділити кількості проміжних пристроїв, що знаходяться між кінцевими пристроями, від цього залежатиме затримка, що вноситься мережею в процес передачі інформації. Кількість проміжних комутаторів є діаметром мережі і для збереження низької затримки необхідно, щоб діаметр був якомога меншим.

**Агрегація каналів.**

Пропускна спроможність каналів, що сполучають різні рівні ієрархії, часто є вузьким місцем в загальному потоці даних. Для усунення можливих проблем, пов’язаних з цими каналами, використовується об’єднання (агрегація) декількох портів в один швидкісний канал, така технологія називається EtherChannel.

**Надлишкові зв’язки.**

Наявність надлишкових зв’язків дозволяє підвищити надійність мережі. Причому є декілька шляхів створення таких зв’язків, це може бути або дублювання зв’язків між пристроями, або дублювання самих пристроїв. Слід врахувати, що надлишковість у будь-якому вигляді є досить дорогим впровадженням, тому її слід застосовувати на високих рівнях ієрархії, де це допоможе зберегти працездатність мережі в цілому, а не окремих невеликих її ділянок.

**Конвергенція.**

На сьогодні багато компаній використовують у своїх бізнес-процесах декілька видів мереж, кожна з яких призначена для передачі вузькоспеціалізованого виду інформації - це телефонна мережа, мережа для відео сигналу і мережа для передачі даних. Управління такими мережами, їх впровадження і підтримка є непростим завданням, яке може потребувати застосування декількох різних інфраструктур, не сумісних ні за способом

установки, ні за способом управління. Застосування цифрових мереж для передачі різних видів інформації, дозволяє значно спростити управління такими мережами. Конвергенція (об'єднання) і є таким процесом – це об'єднання декількох видів передаючої інформації в єдину мережу, тобто і голос і відео передаються в одній цифровій мережі.

Звичайно, об'єднання в єдине ціле різних видів мереж, спричиняє за собою і застосування нових видів обладнання. Наприклад, для забезпечення гарантованої затримки при передачі чутливого до неї трафіку, а це і голосові і відеодані, комутатори повинні підтримувати функції пріоритезації трафіку (QoS), підтримувати віртуальні мережі (VLAN).

### 5.3.3. Вибір комутаторів для ієрархічних мереж

Комутатор – це пристрій, який направляє потік повідомлень від одного порту до іншого, обробляючи MAC-адресу одержувача в межах даного кадру. Комутатор не підтримує обмін трафіком між різними локальними мережами. У контексті OSI моделі комутатор працює на канальному рівні.

При виборі комутаторів для кожного з рівнів ієрархічної моделі мережі необхідно детально досліджувати потоки даних, групи користувачів, сервери обробки і зберігання даних. На рис. 5.10 приведено комутатори для різних рівнів ієрархічної моделі.

Для дослідження потоків даних застосовуються різні аналізатори трафіку. Аналізатори трафіку можуть бути комерційними, наприклад ORION NetFlow Traffic Analyzer, або безкоштовними, наприклад MRTG (Multi Router Traffic Grapher).

Дизайн мережі повинен враховувати можливість розширення кількості робочих місць в кожному з відділів, тобто комутатори повинні мати запас портів як для підключення додаткових робочих місць, так і для створення надлишкових зв'язків з комутаторами рівня розподілу.

При дослідженні трафіку, що відноситься до серверів обробки і зберігання даних, необхідно ділити його на трафік клієнт-сервер і на трафік сервер-сервер. Трафік клієнт-сервер, як правило, перетинає декілька комутаторів, і його важливими параметрами є пропускна здатність агрегованих каналів, і швидкість комутації. Сервера, як правило, групуються в одному приміщенні, і трафік між ними має велику інтенсивність, відповідно вимоги до комутаторів, які обирають для рівня доступу всередині центрів обробки даних, ставляться набагато вищі, ніж для комутаторів рівня доступу в відділах.

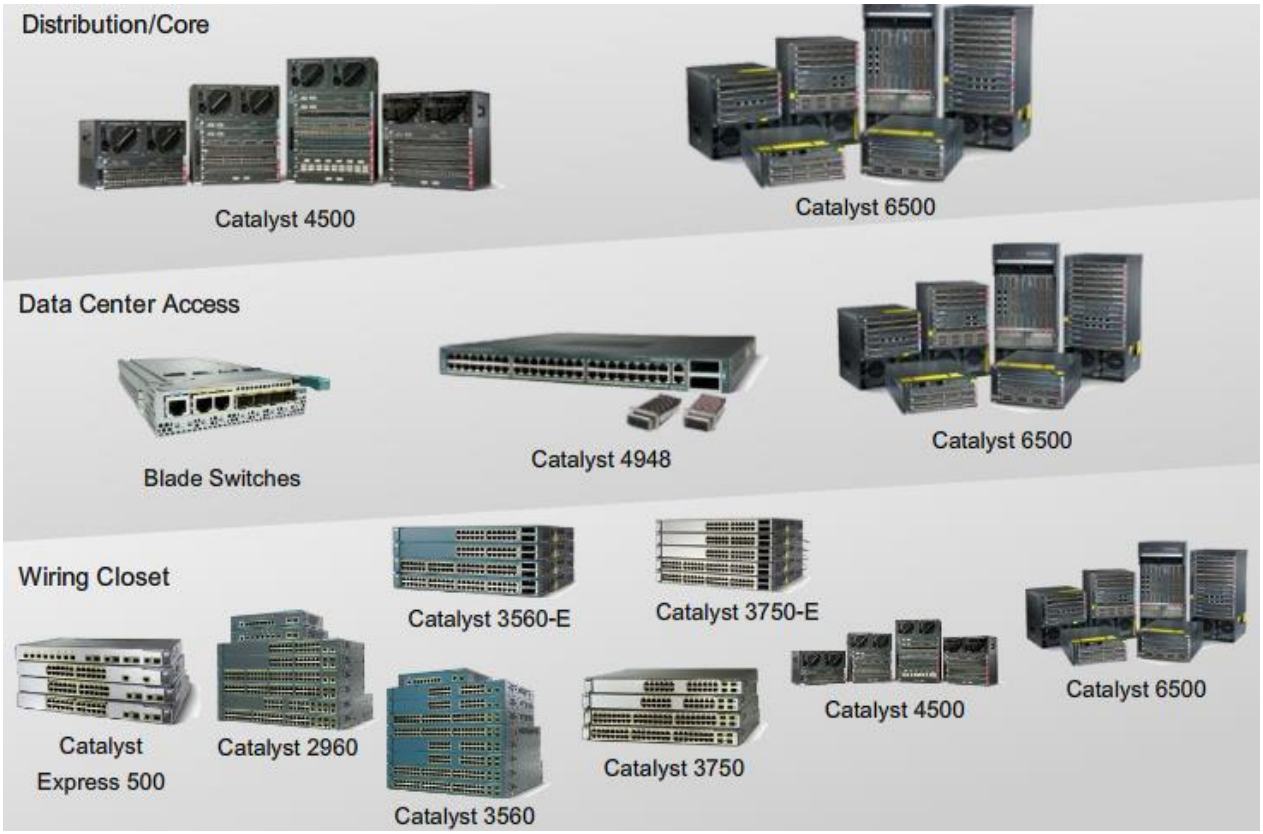



Рис. 5.10. Приклади комутаторів Cisco для рівнів ієрархічної моделі

## Характеристики комутаторів:

**1. Форм-фактор.**

Форм-фактор описує конструктивні особливості комутатора. Розрізняють декілька форм-факторів – з фіксованою конфігурацією, стекові і модульні комутатори.

**Комутатори з фіксованою конфігурацією.** Такі комутатори мають фіксоване число портів – від 8 до 48 і їх кількість не може бути змінена.

Існує кілька моделей комутаторів Cisco Catalyst 2960 з фіксованою конфігурацією, здатних задовольнити різні потреби користувачів (рис. 5.11).

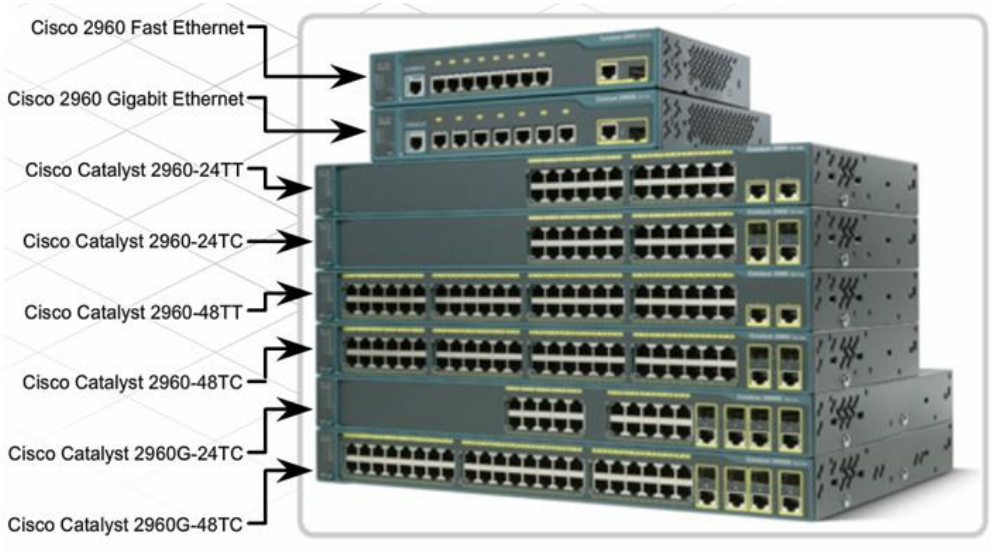



Рис. 5.11. Комутатори Cisco Catalyst 2960 з фіксованою конфігурацією

**Стекові комутатори.** Вони подібні до попередніх, проте мають спеціальну високошвидкісну шину, за допомогою якої можна об’єднати декілька комутаторів в один високопродуктивний відмовостійкий масив. У компанії Cisco така технологія називається StackWise і підтримується, наприклад, комутаторами Catalyst 3750 (рис. 5.12).

Рис. 5.12. Комутатори Cisco Catalyst 3750 з стековою конфігурацією

**Модульні комутатори.** Модульні комутатори – це шасі з високопродуктивною шиною, в яке вставляються плати з портами. Плати можуть бути з різною кількістю і видом портів. Шасі, як правило, містить один або декілька блоків управління (supervisor), які дозволяють реалізувати функції відмовостійкості, гарячої заміни блоків та інше. Прикладами таких комутаторів є Cisco Catalyst 6500 (рис. 5.13).

Рис. 5.13. Модульні комутатори Cisco Catalyst 6500

**2. Продуктивність.**

Продуктивність комутаторів залежить від декількох факторів.

**Щільність портів.** Щільність портів характеризує кількість портів на одному комутаторі. Комутатори з фіксованою конфігурацією мають як правило до 48 портів Fast – або GigabitEthernet і до 4-х GigabitEthernet або оптичних (SFP) портів. При виборі комутатора обов'язково необхідно враховувати можливість підключення не лише кінцевих вузлів, але й підключення до інших комутаторів, причому не одним, а декількома портами, наприклад для агрегації або створення надлишкових зв'язків.

**Пропускна здатність.** Пропускна здатність комутатора характеризує швидкість, з якою комутатор здійснюватиме обробку потоку даних. Ця швидкість ділить комутатори на рівні – від початкового до рівня підприємства. В залежності для якого рівня ієрархії вибирається комутатор, оцінюється його пропускна здатність. Наприклад, для рівня розподілу дуже важливо, щоб швидкість передачі інформації відповідала сумарній пропускній здатності усіх портів. Для комутаторів рівня доступу це не так важливо.

**3. Power over Ethernet (PoE).**

Power over Ethernet (PoE) –технологія передачі електричного живлення в одному дроті разом з мережею Ethernet. Застосовується для живлення таких пристроїв, як IP-телефони, мережеві відеокамери, точки доступу до безпровідної мережі.

**4. Функції 3-го рівня.**

Комутатори є пристроями 2-го рівня OSI моделі – канального, але деякі моделі комутаторів (Cisco Catalyst 3550 і вище) підтримують також функції, типові для пристроїв третього, мережевого рівня, наприклад маршрутизацію. Такі комутатори також називають багаторівневими.

### 5.3.4. Характеристики комутаторів в ієрархічній мережі

**Характеристики комутаторів рівня доступу.**

На рівні доступу підключаються кінцеві користувачі, сервери і різне мережеве обладнання. Тому для цього рівня, окрім швидкості порту (100-1000 Мбіт/с), важливими є такі функції як безпека порту, VLAN, PoE, якість обслуговування (QoS) і агрегація каналів.

Функція безпеки порту, дозволяє контролювати, хто підключається до комутатора. Віртуальні локальні мережі дозволяють розділити трафік різних відділів так, щоб вони не знаходилися в одному канальному рівні, будучи при цьому підключеними до одного комутатора. Трафік IP-телефонії також виділяється в окремі VLAN для забезпечення найкращих характеристик мережі для нього. Підтримка функції якість обслуговування (QoS) дозволить дати телефонному трафіку більший пріоритет перед іншим трафіком.

**Характеристики комутаторів рівня розподілу.**

На цьому рівні для комутаторів важлива підтримка великих швидкостей на портах (1000Мбіт/с, 10Гбіт/с) для зв’язку з комутаторами інших рівнів. Обов’язкова підтримка функцій агрегації каналів, VLAN і якості обслуговування (QoS). Також комутатори рівня розподілу повинні підтримувати функції 3-го рівня і списки контролю доступу (ACL). Списки контролю доступу (ACL – Access Control List) дозволяють або забороняють проходженню певних видів трафіку не лише на мережевому, але і на більш високих рівнях OSI моделі.

**Характеристики комутаторів рівня ядра.**

Рівень ядра пред’являє дуже високі вимоги до швидкості передачі даних. Якщо продуктивності комутатора на цьому рівні не вистачатиме, це може стати проблемою для усієї мережі в цілому. Також важлива наявність функцій 3-го рівня, агрегації каналів і якості обслуговування. Важливими є і можливості забезпечення відмовостійкої роботи, наприклад можливість гарячої заміни компонентів комутатора.

## 5.4. Управління конфігурацією комутатора

### Процес завантаження комутатора

При включенні комутатора в пам’ять завантажується невелика програми, яка зберігається в постійній пам’яті (ROM) – завантажувач (boot loader). Його основні функції:

- Ініціалізація центрального процесора (CPU).
- Виконання процедури самотестування (POST).
- Завантаження в пам’ять образу операційної системи (IOS).

Після завантаження, операційна система зчитує з файлової системи файл конфігурації config.text.

IOS, що використовується в комутаторах Catalyst має два режими – користувацький і привілейований. З привілейованого режиму можна перейти в режим глобального конфігурування комутатора. Перехід між режимами здійснюється за допомогою команд, аналогічних як і для маршрутизаторів Cisco.

### Початкове конфігурування комутатора

Налаштування комутатора Cisco Catalyst виконується на заводі-виробнику. Перед підключенням до мережі необхідно задати тільки основну інформацію про безпеку.

Команди, що служать для задання на комутаторі імені вузла і паролів, є тими ж командами, які використовуються при налаштування маршрутизаторів. Щоб працювати з комутатором Cisco через засоби управління на базі IP або Telnet, потрібно налаштувати для управління IP-адресу.

Для того щоб призначити комутатору адресу, ця адреса має бути призначена інтерфейсу віртуальної локальної мережі VLAN. У мережі VLAN кілька фізичних портів можуть бути об’єднані логічно. За замовчуванням існує тільки одна мережа VLAN, яка заздалегідь налаштована в комутаторі – VLAN1, і вона забезпечує доступ до функцій управління.

Щоб призначити IP-адресу інтерфейсу управління VLAN1, потрібно перейти в режим глобальної конфігурації.

```
Switch> enable
Switch# configure terminal
```

Далі потрібно перейти в режим конфігурації інтерфейсу VLAN1.

Switch (config)# **interface vlan 1**

Потім задати IP-адресу, маску підмережі і шлюз за замовчуванням для інтерфейсу управління. IP-адреса має знаходитися в тій же локальній мережі, що й комутатор.

Switch (config-if)# **ip address** 192.168.1.2 255.255.255.0
Switch (config-if)# exit
Switch (config)# **ip default-gateway** 192.168.1.1

Зберегти конфігурацію потрібно за допомогою команди

Switch (config)# **copy running-config startup-config**

## Налаштування безпеки порту

Комутатори Cisco дозволяють контролювати адреси вузлів, які можуть передавати кадри через їх порти. Ця можливість дозволяє захистити мережу від несанкціонованого підключення пристроїв. Забезпечується такий захист обмеженням кількості дозволених MAC-адрес, які можуть бути в полі source address кадрів, що приймаються на порт. Кадри, в яких джерелом будуть адреси, що не входять в список дозволених, відкидатимуться, або взагалі порт блокуватиметься. Якщо обмежити кількість адрес однією, то відповідно тільки однин вузол зможе підключитися до такого порту.

Існує 3 способи налаштування безпеки порту:

**Статичний**, коли адреси призначаються портам вручну. Виконується це в режимі конфігурації порту командою **switchport port-security mac-address *mac-address***. Щоб можна було активувати функцію безпеки порту, необхідно перевести порт в режим доступу за допомогою команди **switchport mode access**. Статичні MAC-адреси зберігаються в таблиці адрес і додаються в поточну конфігурацію.

Switch# configure terminal
Switch(config)#interface fastEthernet 0/18
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security mac-address [mac-адреса]

**Динамічний**, коли для порту запам’ятовується певна кількість адрес в процесі вивчення комутатора і зберігаються ці адреси тільки в поточній MAC-

таблиці, тобто до перезавантаження комутатора. По замовчуванню, на один порт може бути отримано не більше однієї MAC-адреси. Динамічний спосіб налаштування безпеки порту задається за допомогою команди **switchport port-security**:

```
Switch# configure terminal
Switch(config)#interface fastEthernet 0/18
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

Такий підхід до безпеки порту має недолік – після перезавантаження комутатора прив'язка до портів відбувається наново, і для виправлення цього недоліку використовується наступний режим.

**Зв'язаний (Sticky)**, дозволяє вносити запам'ятовуванні, в результаті вивчення, адреси в конфігураційний файл. Це допоможе уникнути повторного вивчення адрес у разі перезавантаження комутатора. Командою **switchport port-security maximum *число*** можна задати максимальне число захищених адрес, а командою **switchport port-security mac-address sticky** – спосіб зв'язаного налаштування безпеки порту. Налаштування відрізняється від динамічного режиму додатковим параметром:

```
Switch# configure terminal
Switch(config)#interface fastEthernet 0/18
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 50
Switch(config-if)#switchport port-security mac-address sticky
```

Реакція системи на порушення безпеки порту, тобто на спробу передачі через порт кадру з невідомою або закріпленою за іншим портом адресою відправника, має своє налаштування. По замовчуванню порт просто вимикається, в журнал подій пишеться відповідне повідомлення і збільшується лічильник порушень. Такий вид реакції називається **shutdown**. Інша реакція – **restrict**, теж пише повідомлення, збільшує лічильник, але порт при цьому залишається працездатним, тобто він не вимикається. Третій вид реакції на порушення безпеки порту – **protect**, не зачіпає ні журнал повідомлень, ні лічильник порушень, в цьому режимі кадр просто відкидається.

Настроюється реакція на порушення безпеки порту в режимі його конфігурації командою **switchport port-security violation {shutdown | restrict | protect}.**

Для перевірки налаштувань безпеки порту для комутатора або заданого інтерфейсу, використовується команда **show port-security interface interface-*id*.** На екрані з'являться наступні вихідні дані:

- Максимально допустима кількість безпечних MAC-адрес для інтерфейсу
- Кількість безпечних MAC-адрес даного інтерфейсу
- Кількість відбулися порушень безпеки
- Режим порушення безпеки

Крім цього, при введенні команди **show port-security address** відображаються безпечні MAC-адреси для всіх портів, а при введенні команди **show port-security** відображаються налаштування безпеки порту для комутатора.

Порти, які в поточній конфігурації мережі не повинні використовуватися, краще за все відключити, це найпростіший спосіб виключити спроби несанкціонованого підключення до мережі. Виконується це простою командою shutdown в режимі налаштування порту. Для полегшення однакового налаштування декількох портів, можна задавати діапазон портів при переході в режим конфігурації порту. Наприклад:

```
Switch(config)#interface range FastEthernet 0/1-7, FastEthernet 0/9-11
Switch(config-if-range)#
```

Крім включення режиму безпеки порту і відключення невикористовуваних портів, існують інші налаштування безпеки комутатора, які дозволяють встановлювати паролі на порти vty, застосовувати банери входу в систему і зашифровувати паролі за допомогою команди service password-encryption. Для зазначених конфігурацій використовуються ті ж команди інтерфейсу командного рядка Cisco IOS, які застосовуються для налаштування маршрутизатора.

## Перевірка конфігурації комутатора

Перевірка конфігурації комутатора здійснюється за допомогою команди **show** з різними параметрами:

| Команда | Скорочення | Призначення |
|---|---|---|
| **show running-config** | **show run** | Виводить поточну конфігурацію комутатора, що зберігається в RAM. Включає ім’я вузла, паролі, IP-адреси інтерфейсів (якщо вони задані), номери і характеристики портів (режим/швидкість). |
| **show startup-config** | **show star** | Виводить початкову конфігурацію комутатора, що зберігається в NVRAM. Може відрізнятися від поточної, якщо поточна конфігурація не скопійована в початкову. |
| **show version** | **show ver** | Виводить версію IOS, ім’я файлу образу IOS, час роботи комутатора, метод завантаження, кількість і типи встановлених інтерфейсів, обсяг RAM, NVRAM і флеш-пам’яті та значення реєстру конфігурації. |
| **show interfaces** | **show int** | Виводить всі інтерфейси зі статусом каналу (протоколу), смугою пропускання, затримкою, надійністю, інкапсуляцією, параметрами дуплексного режиму і статистикою вводу-виводу. |
| **show ip interface brief** | **show ip int br** | Виводить всі інтерфейси з IP-адресою, статусом інтерфейсу (up/down/admin down) і статусом канального протоколу (up/down). |
| **show port-security** | **show por** | Виводить порти, на яких активований захист, з максимальним числом адрес, поточним числом адрес, лічильником порушень безпеки і діями, які необхідно зробити (як правило, відключення). |
| **show mac-address-table** | **show mac-a** | Перегляд таблиці MAC-адрес. Виводить всі MAC-адреси, вивчені комутатором, спосіб вивчення (статичний або динамічний), номер порту і VLAN, в якій знаходиться порт. |
| **show sessions** | **show ses** | Виводить сеанси Telnet (VTY) з віддаленими вузлами. Показує номер сеансу, ім’я вузла та адресу. |

### Під’єднання комутатора до мережі

Для під’єднання комутатора до маршрутизатора використовується прямий кабель.

Після з’єднання комутатора і маршрутизатора необхідно перевірити, чи можуть ці два пристрої обмінюватися повідомленнями.

Перш за все, необхідно перевірити налаштування IP-адреси. Для цього слід скористатись командою **show running-config**, щоб переконатися в тому, що IP-адреса інтерфейсу управління комутатора мережі VLAN 1 і IP-адреса безпосередньо під’єднаного інтерфейсу маршрутизатора знаходяться в одній локальній мережі. Потім слід перевірити наявність з’єднання за допомогою команди **ping**, надіславши з комутатора команду **ping** на IP-адресу безпосередньо під’єднаного інтерфейсу маршрутизатора. Слід повторити цей процес з маршрутизатора, відправивши команду **ping** на IP-адресу інтерфейсу керування, призначений мережі VLAN 1. Якщо ехо-запит виконати не вдалося, потрібно перевірити підключення та конфігурацію ще раз. Також слід переконатись у тому, що всі кабелі під’єднані правильно і надійно. Коли між комутатором і маршрутизатором встановлений нормальний обмін даними, можна підключати до комутатора за допомогою прямих кабелів окремі комп’ютери.

## 5.5. Уникнення петель комутації. Протокол STP

### 5.5.1. Резервування в комутованих мережах

Відмова одного мережевого каналу, одного пристрою або важливого порту комутатора може стати причиною простою мережі. Щоб виключити критичні точки відмови і забезпечити високу надійність передачі даних в мережеву архітектуру необхідно ввести резервування. Резервування мережі забезпечується дублюванням мережевих пристроїв та впровадженням надлишкових зв’язків в топологію з’єднань між комутаторами. Таке впровадження збільшує кількість можливих шляхів передачі пакетів і у разі відмови будь-якого проміжного комутатора або транкового з’єднання, мережа продовжуватиме функціонувати.

Іноді повне резервування всіх каналів і пристроїв стає невиправдано дорогим. Мережеві інженери часто змушені шукати компроміс між витратами на резервування та вимогами до доступності мережі.

Резервування означає наявність декількох різних шляхів до одного місця призначення. Резервування комутаторів реалізується шляхом створення

декількох каналів між ними. Резервні канали в комутованій мережі знижують перевантаження і підтримують високу доступність і розподіл навантаження.

Однак з'єднання комутаторів може стати причиною проблем. Зокрема, широкотрансляційна природа трафіку Ethernet призводить до утворення **петель комутації** (switching loops). Широкотрансляційні кадри циклічно поширюються у всіх напрямках, викликаючи **широкотрансляційний шторм** (broadcast storm) пакетів (рис. 5.14). Широкотрансляційні шторми займають всю доступну смугу пропускання, блокують створення нових мережевих підключень і розривають існуючі підключення.

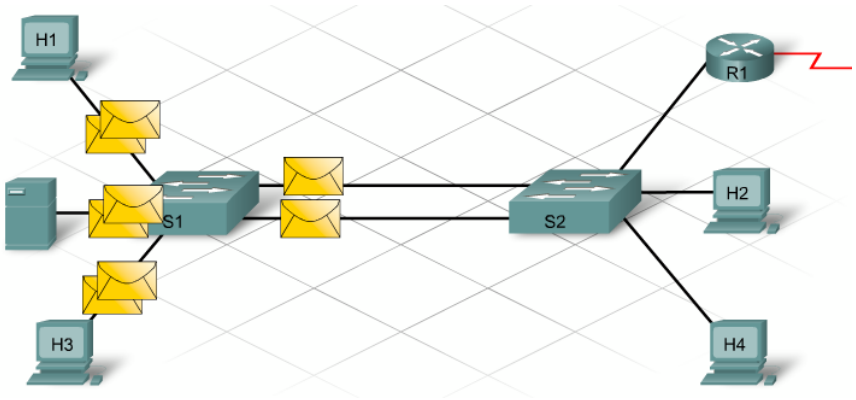



Рис. 5.14. Утворення широкотрансляційного шторму

Широкотрансляційні шторми – не єдина проблема, обумовлена резервними каналами в комутованій мережі**. Одноадресні кадри (Unicast frames)** можуть викликати такі проблеми, як **множинна передача кадрів** та **нестабільність бази даних MAC-адрес**.

Якщо вузол надсилає одноадресний кадр вузлу призначення, MAC-адреса якого не представлена в жодній з таблиць MAC-адрес підключених комутаторів, то всі комутатори виконують лавинну розсилку цього кадру з усіх портів. У мережі з петлями кадр може повернутися до вихідного комутатора. Цей процес повторюється, що призводить до утворення декількох копій кадру в мережі.

Комутатори в резервованій мережі можуть отримувати невірні дані про становище вузла. Якщо в мережі присутня петля, один комутатор може зв'язати MAC-адресу призначення з двома портами. Це може призвести до плутанини і неоптимального пересилання кадрів.

### 5.5.2. Введення в STP

Для боротьби з петлями і для створення надмірних відмовостійких топологій розроблений протокол зв'язуючого дерева – **Spanning Tree Protocol (STP)**, що описаний стандартом IEEE 802.1d.

Протокол STP призначений для забезпечення працездатність мережі при наявності в ній петлевих з'єднань на канальному рівні і використання цих петель для забезпечення відмовостійкої роботи мережі у разі збою будь-якого із зв'язків або проміжного комутатора (рис. 5.15).

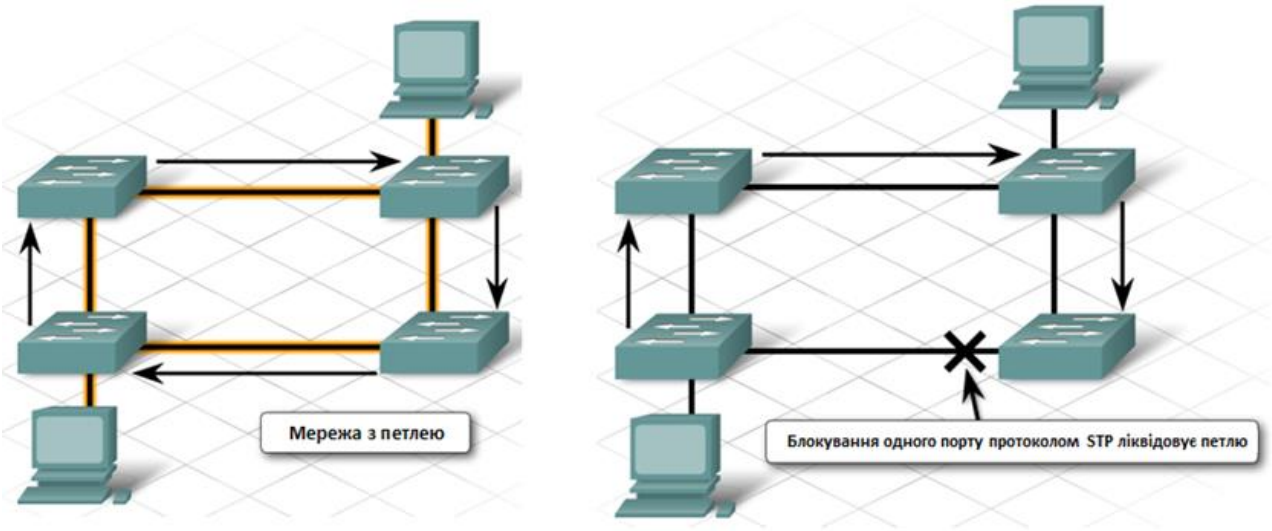



Рис. 5.15. Використання протоколу STP

Протокол STP постійно перевіряє зв'язки між комутаторами в мережі, на предмет появи нових зв'язків або розриву старих і переконфігурує порти комутаторів, щоб уникнути втрати цілісності.

Для обміну інформацією між комутаторами, використовуються кадри, що називаються **модулями даних мостового протоколу** (Bridge Protocol Data Unit, **BPDU**). В процесі роботи протоколу STP порти, які є зайвими в топології зв'язків, блокуються і ніякі дані, окрім BPDU через них не передаються. Таким чином забезпечується логічна топологія без петель в мережі з фізичними петлями.

При роботі протоколу STP для визначення вільного від петель шляху передачі даних застосовується алгоритм покриваючого дерева – **Spanning Tree Algorithm (STA)**. Саме цей алгоритм визначає, які порти комутаторів повинні працювати, а які мають бути заблоковані.

При роботі алгоритму STA в мережі вибирається кореневий комутатор – **root bridge**, від якого потім і буде будуватися дерево з'єднань між комутаторами.

Кореневий комутатор вибирається на основі його ідентифікатора – **bridge ID (BID).** При включенні усі комутатори вважають себе кореневими і розсилають BPDU, в яких вказують свій BID. Перемагає у виборах той комутатор, у якого буде найменше значення BID. Сам ідентифікатор складається з двох частин: 2 байти – пріоритет комутатора, по замовчуванню має значення 32769 і 6 байт – MAC адреса.

Після виборів, алгоритм STA на кожному з комутаторів розраховує найкращий шлях до кореневого і визначає ролі своїх портів.

Найкращий шлях до кореневого комутатора розраховується виходячи з сумарної вартості зв'язків, які повинен пройти кадр на шляху до кореневого комутатора. Кожен комутатор підсумовує вартість усіх можливих шляхів до кореневого і вибирає шлях у якого сума виявилася найменшою. Відповідно порт, через який пролягає такий шлях, призначається кореневим.

Вартість зв'язків описана в стандарті IEEE 802.1D, і в різних редакціях має різні значення. В останній актуальній редакції стандарту IEEE 802.1D, описані наступні значення:

| Швидкість з'єднання | Рекомендоване значення | Рекомендований діапазон | Діапазон |
|---|---|---|---|
| <=100 Кбіт/с | 200 000 000 | 20 000 000 – 200 000 000 | 1 – 200 000 000 |
| 1 Мбіт/с | 20 000 000 | 2 000 000 – 200 000 000 | 1 – 200 000 000 |
| 10 Мбіт/с | 2 000 000 | 200 000 – 20 000 000 | 1 – 200 000 000 |
| 100 Мбіт/с | 200 000 | 20 000 – 2 000 000 | 1 – 200 000 000 |
| 1 Гбіт/с | 20 000 | 2 000 – 200 000 | 1 – 200 000 000 |
| 10 Гбіт/с | 2 000 | 200 – 20 000 | 1 – 200 000 000 |
| 100 Гбіт/с | 200 | 20 – 2 000 | 1 – 200 000 000 |
| 1 Тбіт/с | 20 | 2 – 200 | 1 – 200 000 000 |
| 10 Тбіт/с | 2 | 1 – 20 | 1 – 200 000 000 |

Для комутаторів є можливість вручну настроювати вартість кожного зв'язку. Виконується це в режимі налаштування інтерфейсу командою **spanning-tree cost *value***. Побачити налагоджене значення, або значення за умовчанням можна командою **show spanning-tree detail.**

### 5.5.3. Формат BPDU

Кадр BPDU містить 12 полів (рис. 5.16):

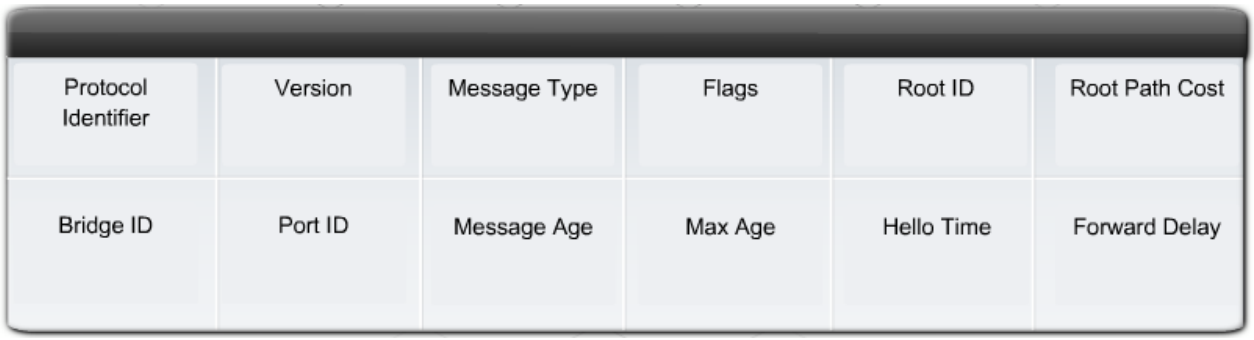



Рис. 5.16. Структура кадру BPDU

1. Ідентифікатор протоколу, 2 октети. Для STP має значення 0.
2. Версія протоколу, 1 октет. Для STP має значення 0.
3. Тип BPDU, 1 октет. Для STP має значення 0.
4. Прапори, 1 октет. Існує 2 значення: **зміна топології** (Topology change, TC) – використовується для позначення того, що змінився шлях до кореневого комутатора; **підтвердження зміни топології** (Topology Change Acknowledgement, TCA) – кадр з цим прапором посилається у відповідь на кадр з прапором TC.
5. Ідентифікатор кореневого комутатора, 8 октетів. У цьому полі вказується BID комутатора, який на думку відправника вважається кореневим. При включенні живлення комутатора, значенні цього поля співпадає з 7-м полем. В процесі виборів, значення цього поля замінюється, якщо від інших комутаторів буде отримано менше значення root BID.
6. Вартість шляху до кореневого комутатора, 4 октети.
7. Ідентифікатор комутатора, що послав кадр, 8 октетів.
8. Ідентифікатор порту, через який кадр був посланий, 2 октети.
9. Вік поточного повідомлення, одиниці відповідає 1/256 сек, 2 октети.
10. Максимальний можливий вік повідомлення (час життя) в секундах, 2 октети.
11. Інтервал посилки Hello-пакетів, по замовчуванню 2 сек, може змінюватися від 1 до 10, розмір – 2 октети.
12. Останнє поле – затримка передачі кадру BPDU, 2 октети.

Розсилаються кадри BPDU за груповою адресою, закріпленою за пристроями, що використовують STP – 01:80:C2:00:00:00.

### 5.5.4. Формат BID

**Ідентифікатор моста** – Bridge ID (**BID**), застосовується для визначення комутатора, що виконуватиме роль кореневого (root) для мережі. Цей ідентифікатор складається з 2-х частин – пріоритет моста (bridge priority) і MAC адреса комутатора (рис. 5.17.).

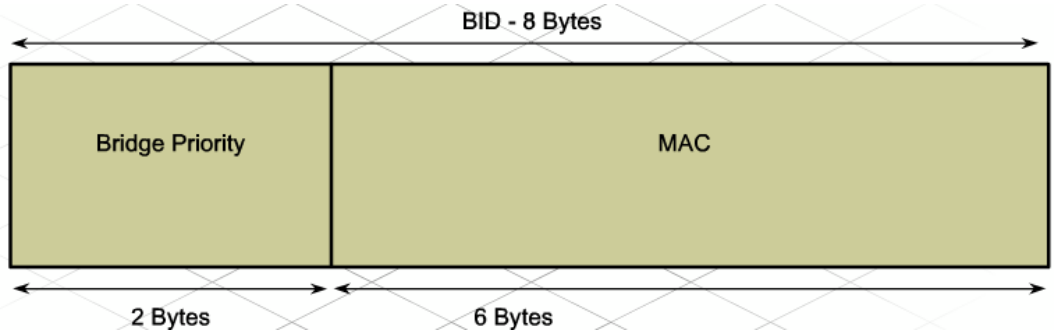



Рис. 5.17. Формат BID

Більш пріоритетним є менше значення bridge priority.

У разі співпадання пріоритетів на усіх комутаторах, порівнюється друга частина BID – MAC адреса, відповідно, вибори виграє той комутатор, у якого опиниться менша адреса. І якщо у випадку з різними пріоритетами можна легко передбачити, який комутатор буде кореневим, а саме на нього покладатиметься основне навантаження при передачі транзитного трафіку, то у випадку з визначенням ролі комутатора по його MAC адресі, результат виборів буде випадковим, і може не співпадати з первинним планом розподілу навантаження.

Для уникнення таких ситуацій рекомендується вручну визначати пріоритети і заздалегідь планувати хто буде коренем дерева і хто буде резервним коренем, на випадок, якщо перший комутатор вийде з ладу. Першому кореневому комутатору слід призначити найнижчий пріоритет, а другому, резервному, трохи вищий, але нижчий інших (рис. 7.18).

Призначення пріоритету комутатору виконується командою режиму глобальної конфігурації **spanning-tree vlan *vlan-id* priority *value*.**

S3(config)#spanning-tree vlan 1 priority 4096

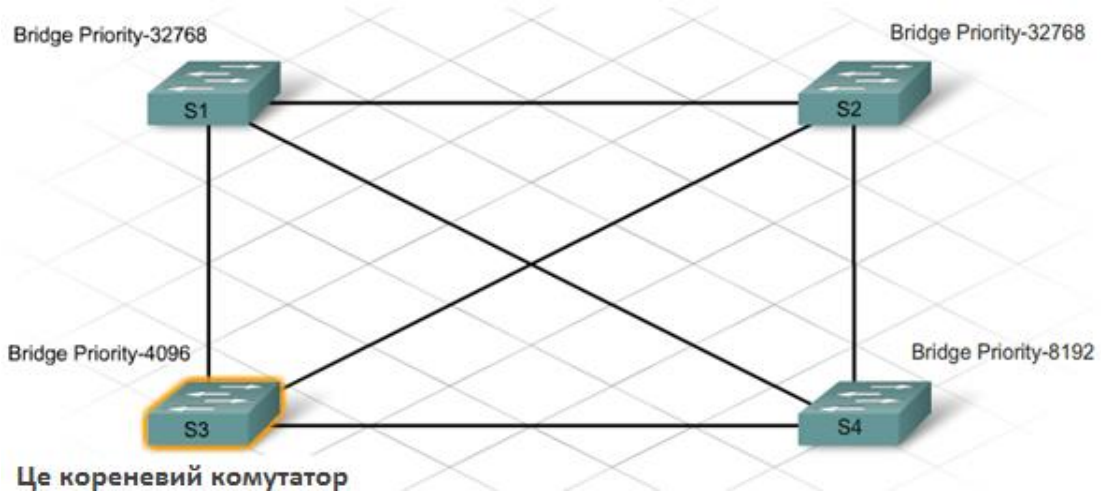



Рис. 5.18. Пріоритети комутаторів

### 5.5.5. Ролі портів

Після виборів кореневого комутатора, необхідно визначити для кожного порту його роль. Розташування кореневого комутатора багато в чому впливатиме на вибір ролі для комутатора. Всього існує чотири типових ролей портів для STP – кореневий порт, призначений порт, непризначений порт і відключений порт (рис. 5.19):

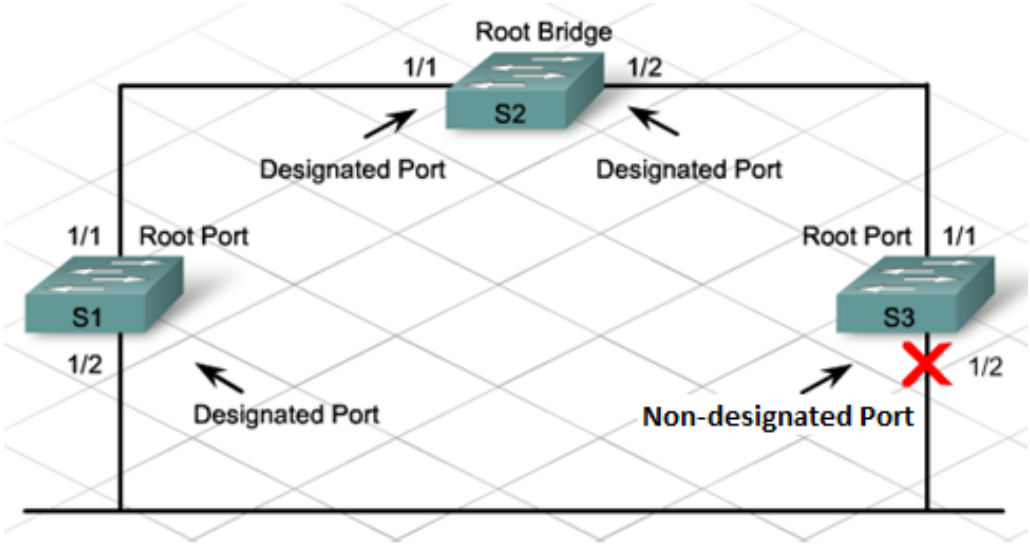



Рис. 7.19. Типи портів комутаторів

- **Кореневий порт (Root Port)** – порт, який знаходиться найближче до кореневого комутатора. Кожен комутатор в мережі, окрім кореневого комутатора, повинен мати один такий порт.
- **Призначений порт (Designated Port**) – через цей порт приймається інформація від сусідніх по дереву комутаторів, що спрямована кореневому. Такі порти є в усіх комутаторів, включаючи і кореневі.
- **Непризначений порт (Non-Designated Port**) – такі порти знаходяться у блокованому стані і ніякі дані окрім BPDU через них не передаються. У деяких варіантах STP такі порти називаються запасними (alternate).
- **Відключений порт (Disabled)** – порт, вимкнений командою shutdown. У процесі STP не бере участь.

Алгоритм STA визначає роль порту на кожному з комутаторів. Для вибору порту, який виконуватиме роль кореневого, комутатор обчислює можливі шляхи до кореневого комутатора і вибирає серед них найменший. Порт, через який пролягатиме цей шлях призначається кореневим. Якщо буде декілька шляхів з однаковою найменшою вартістю, у виборі братиме участь параметр, що називається ідентифікатор порту, port ID. Цей ідентифікатор складається з двох частин – пріоритет порту та його номер. Наприклад 128.1 – значення пріоритету 128 для першого порту комутатора (це значення може змінюватися від 0 до 240 з кроком 16). Менше значення має більший пріоритет.

Налаштовується пріоритет командою режиму конфігурації порту командою **spanning-tree port-priority *value***. У випадку з однаковими вартостями шляхів, буде вибраний порт з меншим значенням port ID, а інші порти будуть переведені в стан non-designated.

Процес вибору ролі порту наступним – кореневий комутатор налаштовує свої порти на роль designated або non-designated залежно від ситуації. Інші комутатори визначають свої порти, що виконують роль кореневих. Для інших портів необхідно вибрати роль designated або non-designated. Якщо у сусіднього по транку комутатора кореневий порт входить до складу цього транка, то порту привласнюється роль designated. Якщо ж у сусідніх комутаторів налагоджені кореневі порти і вони не в одному транку, тоді один з них повинен взяти на себе роль non-designated. Сусідні комутатори вибирають, кому блокувати порт виходячи з більшого значення BID, оскільки комутатор з меншим значенням BID має більше шансів виграти вибори кореневого комутатора. Побачити ролі портів комутатора можна за допомогою команди привілейованого режиму **show spanning-tree**:

```
Switch#sh spanning-tree
VLAN0001
```

```
Spanning tree enabled protocol ieee
Root ID     Priority    32769
         Address     0001.97D9.A619
         Cost        19
         Port        2(FastEthernet0/2)
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID   Priority    32769 (priority 32768 sys-id-ext 1)
         Address     0003.E471.D75C
         Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
         Aging Time 20

---------------------------------------------------------------

____
Interface       Role Sts Cost       Prio.Nbr    Type
Fa0/1           Desg FWD 19         128.1       P2p
Fa0/2           Root FWD 19         128.1       P2p
```

### 5.5.6. Стани портів STP і таймери STP

При включенні комутаторів, потрібний деякий час для формування дерева STP. Якщо комутатори в цей час почнуть передавати дані, то за наявності фізичних петель, мережа утворить тимчасові петлі передачі інформації, що негативно позначиться на продуктивності мережі і пристроїв працюючих в ній. Щоб уникнути можливості утворення таких тимчасових петель в протоколі є декілька проміжних станів для портів:

- **Блокування (blocking)** – в цьому стані порт тільки приймає BPDU для визначення розташування кореневого комутатора і ролі порту. Це первинний стан порту після включення комутатора, також в цей стан порт переходить, якщо в результаті процесу конвергенції він визначений як non-designated або була визначена втрата BPDU сусіднього комутатора.
- **Прослуховування (listening)** – проміжний стан, в якому передаються тільки кадри BPDU, в цьому стані відбувається побудова топології дерева STP. У цей стан порт потрапляє з попереднього і далі переходить або назад до блокування, або до наступного проміжного стану.
- **Вивчення (learning)** – в цьому стані порт вивчає MAC адреси сусідніх пристроїв і передає лише кадри BPDU.
- **Пересилка (forwarding)** – робочий стан порту, в якому передаються усі види кадрів.
- **Відключений (disabled)** – порт вимкнений в конфігурації командою shutdown, і не бере участь в STP.

Таймери STP описують час, за який порти перебувають в кожному із станів. Розрізняють 3 таймери STP:

- **Hello time –** інтервал розсилки повідомлень BPDU. По замовчуванню 2 секунди, може змінюватися від 1 до 10 сек**.**
- **Maximum age –** максимальний вік повідомлень BPDU. По замовчуванню 20 секунд, може змінюватися від 6 до 40 сек.
- **Forward delay –** затримка передачі, визначає час, за який порт знаходиться в стані listening і learning. По замовчуванню 15 секунд, може змінюватися від 4 до 30 сек.

Побачити значення таймерів можна за допомогою команди show spanning-tree detail:

```
Switch#sh spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree Protocol
  Bridge Identifier has priority of 32768, sysid 1, 0003.E471.D75C
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32769
  Root port is 2 (FastEthernet0/2), cost of root path is 19
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 00:00:00 ago
                from FastEthernet0/1
  Times:  hold 1, topology change 35, notification 2
                hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0,
                aging 300
```

Сумарний час, за який порт реагуватиме на зміну топології мережі, складатиметься з суми таймерів, діючих для кожного з проміжних станів.

Блокування (20 сек)→Прослуховування (15 сек)→Навчання (15 сек)→Пересилка

У сумі вийде 50 секунд, досить великий інтервал часу, достатній для збіжності (конвергенції) мережі, що має не більше 7 комутаторів між крайніми вузлами. Цю кількість комутаторів називають діаметром мережі. Не рекомендується міняти значення таймерів довільно, для найбільш оптимальної зміни таймерів рекомендується відразу задавати діаметр мережі при налаштуванні кореневого комутатора в режимі глобальної конфігурації командою **spanning-tree vlan *vlan id* root primary diameter *value***. Значення діаметру можуть змінюватися від 2 до 7.

### 5.5.7. Збіжність STP

Процес формування дерева, проходить через три основні етапи:

1. Вибори кореневого комутатора.
2. Вибори кореневих портів на комутаторах.
3. Вибори призначених і непризначених (блокованих) портів.

**Вибори кореневого комутатора.**

Вибори кореневого комутатора є першим кроком в процесі формування дерева STP. Починаються вибори кореневого комутатора відразу після закінчення процесу завантаження комутатора, або після визначення порушення топології мережі. По замовчуванню, усі порти комутатора знаходяться у блокованому стані 20 секунд, для того, щоб уникати виникнення петель комутації, поки не буде сформовано дерево STP. В цей час через порти кожних 2 секунди передаються BPDU, за допомогою яких комутатори поширюють інформацію про свої BID.

При максимальному діаметрі мережі в 7 комутаторів, інформація про найнижче значення BID (кореневий комутатор) поширеться за 14 секунд і цей час менший, ніж час знаходження у блокованому стані. За цей час кожен комутатор приймає в BPDU від сусіднього комутатора Root ID, порівнює його із збереженим локальним і якщо прийнятий Root ID менший, то локальний замінюється на нього. Якщо ж прийнятий Root ID більший локального, то локальне значення Root ID залишається колишнім. Побачити поточну роль комутатора після виборів можна командою **show spanning-tree**, наприклад для кореневого комутатора виведення цієї команди буде наступним:

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID   Priority   32769
            Address     0002.1655.C0E3
            This bridge is the root
            Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
  Bridge ID   Priority 32769    (priority 32768 sys-id-ext 1)
            Address     0002.1655.C0E3
            Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
            Aging Time    20
Interface        Role Sts Cost      Prio.Nbr Type
---------------  ---- --- -------   ------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

Видно, що Root ID співпадає з Bridge ID, що означає, що він виконує роль кореневого і це позначено відповідним повідомленням. Для комутатора, що не є кореневим, вивід команди буде таким:

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
   Root ID    Priority        32769
              Address     0002.1655.C0E3
              Cost        19
              Port        1(FastEthernet0/1)
              Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
    Bridge ID     Priority         32769    (priority 32768 sys-id-ext 1)
              Address     0090.2171.27ED
              Hello Time    2 sec    Max Age 20 sec    Forward Delay 15 sec
              Aging Time    20
Interface        Role Sts Cost      Prio.Nbr Type
---------------  ---- --- -------   ------- --------------------------------
Fa0/1            Root FWD 19       128.1    P2p
Fa0/2            Altn BLK 19       128.2    P2p
Switch#
```

У цього комутатора Root ID не співпадає з Bridge ID, відповідно він не кореневий.

**Вибори кореневих портів.**

Після виборів кореневого комутатора, починаються вибори кореневих портів. На кожному з комутаторів в дереві STP, окрім кореневого комутатора, має бути вибраний один порт, який виконуватиме функції кореневого порту. Такий порт має найменшу вартість шляху до кореневого комутатора.

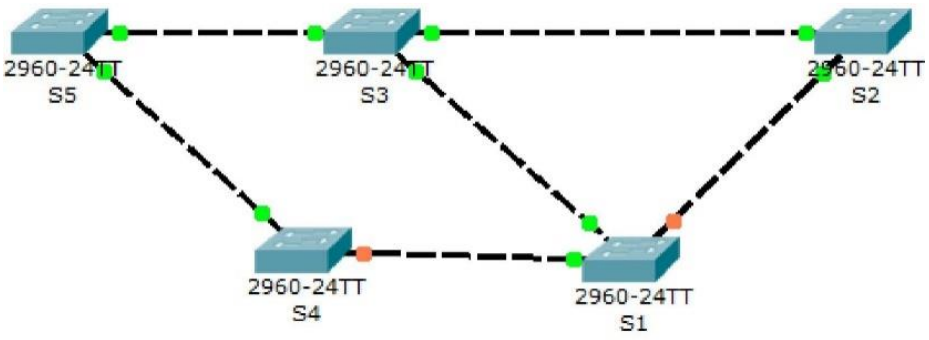
Як правило, комутатор повинен мати тільки один порт для такої ролі, але якщо в результаті підсумовування виявиться декілька портів з однаковою вартістю шляху до кореневого комутатора, це може означати наявність двох і більше зв’язків між двома сусідніми комутаторами. Швидше за все, такий зв’язок між комутаторами призначався для створення агрегованого каналу EtherChannel і залишився ненастроєною. Ця технологія дозволяє об’єднати декілька фізичних каналів Ethernet в один логічний, який матиме пропускну спроможність рівну сумі об’єднаних каналів. Порти, що мають однакову вартість шляху до

кореневого комутатора, використовуватимуть пріоритет порту, для визначення, який із них буде вимкнений, а який продовжуватиме роботу в якості кореневого порту.

Сама ж вартість шляху обчислюється як сума вартості шляху до кореневого, прийнята від сусіднього комутатора в BPDU, і локального значення вартості шляху через порт, на якому був прийнятий BPDU від сусіда. При цьому у кореневого комутатора вартість дорівнюватиме 0, а у інших комутаторів вартість залежатиме від конкретної конфігурації мережі. Розрахунок вартості буде наступним:

1. Кореневий комутатор в BPDU відправляє значення вартості 0.
2. Найближчі до кореневого комутатори додають до отриманого значення вартість порту, який прийняв BPDU від кореневого і передають це значення наступним сусідам по дереву.
3. Комутатори наступного рівня також додають до отриманого значення вартість порту, який прийняв BPDU від сусіда і передають збільшене значення далі.
4. Усі наступні комутатори також збільшують значення вартості і передають його далі.

   Приклад для мережі на рисунку:




```
S3#sh sp
VLAN001
  Spanning tree enabled protocol ieee
    Root ID Priority   32768
            Address     000C.1209.1375
            This bridge is the root
            Hello Time      2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID    Priority 32768
            Address     000C.1209.1375
```

```
        Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300

Interface       Port ID                 Designated              Port ID
Name            Prio.Nbr    Cost Sts    Cost Bridge ID          Prio.Nbr

Fa0/1           32768.1     0 FWD       0 32768 000C.1209.1375 0.1
Fa0/2           32768.2     0 FWD       0 32768 000C.1209.1375 0.2
Fa0/3           32768.3     0 FWD       0 32768 000C.1209.1375 0.3
S1#sh spanning-tree
VLAN001
  Spanning tree enabled protocol ieee
    Root ID Priority   32768
        Address     000C.1209.1375
        Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
    Bridge ID  Priority     32768
        Address     000C.3378.5283
        Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
        Aging Time 300Interface      Port ID       Designated  Port ID

Interface       Port ID                 Designated              Port ID
Name            Prio.Nbr    Cost Sts    Cost Bridge ID          Prio.Nbr

Fa0/1           32768.1     57 FWD      0 32768 000C.1209.1375 57.1
Fa0/2           32768.2     19 FWD      0 32768 000C.1209.1375 19.2
Fa0/3           32768.3     38 BLK      0 32768 000C.1209.1375 38.3

S5#sh sp VLAN001
  Spanning tree enabled protocol ieee
    Root ID     Priority    32768
        Address     000C.1209.1375
        Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

    Bridge ID Priority    32768
        Address     000C.1240.1086
        Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
        Aging Time 300
```

| Interface | Port ID | | Designated | | Port ID |
|---|---|---|---|---|---|
| Name | Prio.Nbr | Cost Sts | Cost Bridge ID | | Prio.Nbr |
| Fa0/1 | 32768.1 | 57 FWD | 0 32768 000C.1209.1375 | | 57.1 |
| Fa0/2 | 32768.2 | 19 FWD | 0 32768 000C.1209.1375 | | 19.2 |

Наприклад, у виводі команди **show spanning-tree** комутатора S5 можна побачити, що значення вартості до кореневого комутатора через порт Fa0/1 складає 57. Шлях до кореневого комутатора через цей порт буде таким S3 → S1 → S4 → S5, відповідно складатимуться значення 0 19 19 19=57, і це значення більше ніж для порту Fa0/2 – 19, тому Fa0/1 при такій вартості не буде кореневим.

**Вибори призначених і непризначених портів.**

По закінченню виборів кореневих портів, комутатори повинні визначитися з роллю інших портів, що являються транками. Для них можливі 2 ролі - призначені порти, designated port (DP), або непризначені порти, non-designated port (non-DP). Спочатку передбачається, що усі порти, які не кореневі, є призначеними, тобто через них приймаються BPDU, які містять великі значення вартості шляху до кореневого комутатора, ніж в BPDU, що приймаються на кореневому порту.

У разі, якщо трапляється ситуація, що одним сегментом сполучені два порти, що не є кореневими, комутатори повинні вибрати чий порт залишиться в стані designated, а чий в стані non-designated. Вибір комутатори роблять, спираючись на BID, якими вони обмінюються за допомогою BPDU в цьому сегменті. Той комутатор, у якого значення BID виявиться менше, залишає свій порт в стані designated, а той у якого більше, переводить свій порт в стан non-designated. Такий вибір обумовлений тим, що комутатор з меншим значенням BID має більше шансів стати кореневим в випадку зміни топології мережі. Перевіряється стан некореневих портів командою show spanning-tree. На цьому конвергенція дерева STP завершується і поточна його конфігурація називається «активною топологією».

### 5.5.8. Зміна топології STP

В протоколі STP застосовується два типи BPDU – конфігураційні і повідомлення про зміни. В процесі роботи активної топології кореневий комутатор розсилає через свої порти конфігураційні BPDU, які передаються на кореневі порти інших комутаторів і далі по дереву. У зворотному напрямі комутатори не передають конфігураційні BPDU. У напрямі кореневого комутатора можуть передаватися BPDU другого типу – повідомлення про зміни.

Вони передаються у разі, якщо будь-який з портів комутатора змінив свій стан – наприклад з блокування в передачу або навпаки.

BPDU, які є повідомленнями про зміни, існує два типи – **повідомлення про зміну топології** (Topology Change Notification, **TCN**) і **підтвердження зміни топології** (Topology Change Acknowledgement, **TCA**). У полі формат кадру BPDU, що означає тип повідомлення, вказується, який конкретно тип повідомлення являє собою BPDU. З восьми біт використовується тільки два (перший і останній), що мають значення TCA і TC.

TCN BPDU посилаються некореневим комутатором наступному комутатору вище за ієрархією у напрямі кореневого, з інтервалом звичайним для BPDU. Комутатор, що приймає повідомлення TCN BPDU, посилає у відповідь конфігураційний BPDU, зі встановленим прапором TCA. Цим він підтверджує, що повідомлення про зміну прийняте, і нижній за ієрархією комутатор повинен припинити посилку TCN BPDU. Далі комутатор, верхній по рівню від того, що послало початковий TCN BPDU, сам формує таке повідомлення для наступного комутатора у напрямі кореневого. Усі дії повторюються до тих пір, поки TCN BPDU не досягне кореневого комутатора.

Як тільки кореневий комутатор приймає TCN BPDU, він відповідає на нього конфігураційним BPDU, зі встановленими прапорами TCA і TC. Після цього, на протязі часу, рівного сумі таймерів Maximum age і Forward delay (20+15=35 сек.) кореневий комутатор розсилатиме конфігураційні BPDU зі встановленим прапором TC. Прийом таких BPDU іншими комутаторами, означає що вони повинні перебудувати топологію зв’язків і дерево STP буде змінено в найкоротші терміни.

### 5.5.9. Пошук і усунення несправностей STP

Проблема, що може виникнути в роботі протоколу STP – це виникнення петлі на 2-му рівні OSI. Для усунення такої несправності, як правило, потрібне консольне підключення до комутатора, оскільки доступ через мережу швидше за все буде неможливий. Такі завдання, пов’язані з пошуком несправностей в роботі протоколу STP виникають нечасто, і перш, ніж приступати до їх вирішення, необхідно зібрати наступну інформацію:

1. Топологію комутованої мережі.
2. Розташування кореневого комутатора.
3. Розташування портів, що знаходяться в стані блокування, і надмірних зв’язків.

Маючи таку інформацію, досить просто визначити джерело проблем, переглядаючи вивід команди show для ключових пристроїв і портів мережі.

Типові помилки, при яких виникають проблеми з функціонуванням протоколу STP, це помилки пов’язані з налаштуванням PortFast і з дотриманням максимального діаметру мережі. Неправильна конфігурація PortFast означає налаштування порту, до якого підключатиметься інший комутатор, в режим, що переводить порт в стан передачі інформації відразу після включення. Підключення, до таким чином налагодженого порту комутатора приведе до того, що утвориться петля. Проте вона виникне ненадовго, оскільки один з комутаторів передасть в такий порт BPDU і петля припиниться. Але при цьому може виникнути і проблема, пов’язана з інтенсивністю трафіку в такому підключенні, адже якщо трафік в петлі буде дуже інтенсивний, то BPDU можуть втрачатися і зрештою може постраждати уся мережа. Також при підключенні до такого порту комутатора, з меншим значенням BID може змінитися місце розташування кореневого комутатора в мережі. Це може призвести до зміни активної топології в неоптимальну і непередбачувану конфігурацію. Захиститися від таких змін допоможе згадувана раніше технологія BPDU guard.

Як відомо, таймери STP розраховані на максимальний діаметр мережі в 7 комутаторів. Пов’язано це з тим, що інформація від кореневого комутатора повинна поширитися до самого крайнього комутатора за час, менший, ніж максимальний вік повідомлення BPDU. Якщо комутатор приймає кадр BPDU з часом життя більшим, ніж максимально можливий, то він повинен відкинути цей BPDU. Таким чином, комутатори, що знаходяться за межами максимального діаметру мережі не зможуть завершити конвергенцію дерева STP. Подібна проблема може виникнути і при меншому діаметрі мережі, якщо необдумано зменшувати таймери STP, намагаючись зменшити час конвергенції дерева. Щоб уникнути подібних проблем, необхідно ретельно обмірковувати встановлювані значення або застосовувати інші способи зменшення часу конвергенції (наприклад застосовуючи комутатори 3-го рівня).

## 5.6. Основні атаки, що пов’язані з комутаторами

Перший тип атак, пов’язаний з переповнюванням CAM-таблиці комутатора, в результаті наповнення мережі неправдивими MAC-адресами відправника. В результаті такої атаки таблиця MAC-адресів комутатора переповнюється, прописані раніше адреси витісняються з неї і комутатор починає поводитися як звичайний концентратор, розсилаючи пакети на усі порти.

Другий вид атак пов’язаний з використанням в мережі протоколу DHCP. Зловмисник може встановити в мережі свій сервер DHCP, який видаватиме клієнтам неправдиві параметри IP. Для боротьби з такими атаками

використовується розроблене Cisco розширення **DHCP snooping**. Ця технологія припускає визначення «довірених портів», які передаватимуть пакети в напрямі від і до DHCP сервера в мережі. Усі відповіді DHCP сервера, що приходять не з «довірених портів» будуть відхилятися.

Наступна атака пов’язана із застосуванням протоколу CDP, який включений по замовчуванню на пристроях Cisco. Цей протокол дуже корисний на етапі початкового налаштування мережі, оскільки дозволяє визначити сусідів по канальному рівню і розпізнати деякі з їх параметрів. Проте згодом цей протокол може бути використаний зловмисниками для дослідження структури мережі і деяких налаштувань проміжних пристроїв. Ця інформація може послужити основою для різних атак на комутатори і маршрутизатори. Для зменшення ймовірності атак, пов’язаних з цим протоколом, рекомендується його відключати, якщо в ньому немає особливої необхідності – в режимі глобальної конфігурації виконати команду **no cdp**.

# 6. Маршрутизація в телекомунікаційних мережах

## 6.1. Будова та завантаження маршрутизаторів Cisco

### 6.1.1. Будова маршрутизаторів Cisco

Маршрутизатори є найінтелектуальнішими пристроями в мережі. Вони можуть проводити фільтрацію пакетів по апаратній (MAC) та по логічній (IP) адресі. Маршрутизатори виконують дві основні функції: вибір шляху та комутацію. Функцію вибору оптимального шляху передачі пакету в маршрутизаторі забезпечують **таблиці маршрутизації**, які можуть формуватися вручну або за допомогою **протоколів маршрутизації.**

Функція комутації дозволяє скомутувати порт, з якого надійшов пакет, з портом, в який його потрібно відправити. Маршрутизатор запобігає виникненню зайвого трафіку в мережевих сегментах за рахунок перевірки логічної адреси отримувача. Маршрутизатор розділяє як **домен колізії** (**Collision Domain)** так і **широкотрансляційний домен** (**Broadcast Domain**), що значно збільшує перепускну здатність мережі та її продуктивність в цілому.

Апаратно маршрутизатор подібний до комп'ютера, до його складу входять наступні компоненти:

- **центральний процесор** (Central Processing Unit, **CPU**), який керує роботою маршрутизатора;
- **оперативна пам'ять** (Random Access Memory, **RAM**), яка зберігає таблиці маршрутизації, ARP-кеш (ARP-cache), кеш швидкої комутації (Fast-Switching Cache), буфери пакетів. В оперативну пам'ять завантажується операційна система (ОС) після включення живлення маршрутизатора. Оскільки цей тип пам'яті енергозалежний, її вміст зникає при перезавантаженні та вимкненні живлення маршрутизатора.
- **енергонезалежна оперативна пам'ять** (Non-Volatile RAM, **NVRAM**). Зберігає файл початкової конфігурації (Startup Configuration).
- **флеш-пам'ять** (Flash). Зберігає файл операційної системи та мікрокод. Використовуючи флеш-пам'ять, можна запустити маршрутизатор і провести модернізацію без зміни мікросхем на системній платі. Може зберігати декілька версій IOS. Вміст флеш-пам'яті зберігається і при виключеному живленні.
- **постійний запам'ятовуючий пристрій (**Read-Only Memory, **ROM)** – використовується маршрутизатором для зберігання програм початкового завантаження, програмного забезпечення операційної системи та програми самотестування після включення живлення (Power-On Self-Test POST).

Мікросхеми ROM встановлюються в гнізда системної плати маршрутизатора і можуть бути замінені при відмові чи при модернізації.

- **інтерфейси** (Interfaces). Розміщаються на системній платі або представляють собою окремі модулі, які можна замінювати. Інтерфейси локальної мережі допускають підключення до мереж Ethernet, FastEthernet і GigabitEthernet. Підключення до глобальних мереж здійснюється через синхронні послідовні порти Serial. Для під'єднання до мереж ISDN можуть бути встановленні додаткові інтерфейсні плати.

На рис. 6.1 показано зовнішній вигляд маршрутизатора з інтегрованими службами (ISR – Integrated Services Router) Cisco 1841.

На передній панелі маршрутизатора міститься 2 світлодіодних індикатора:

1. живлення системи (SYS-PWR) – вказує на функціонування внутрішнього джерела живлення. Світлодіод горить рівним зеленим світлом.
2. робота системи (SYS ACT) – мигання світлодіода вказує на те, що система активно передає пакети.

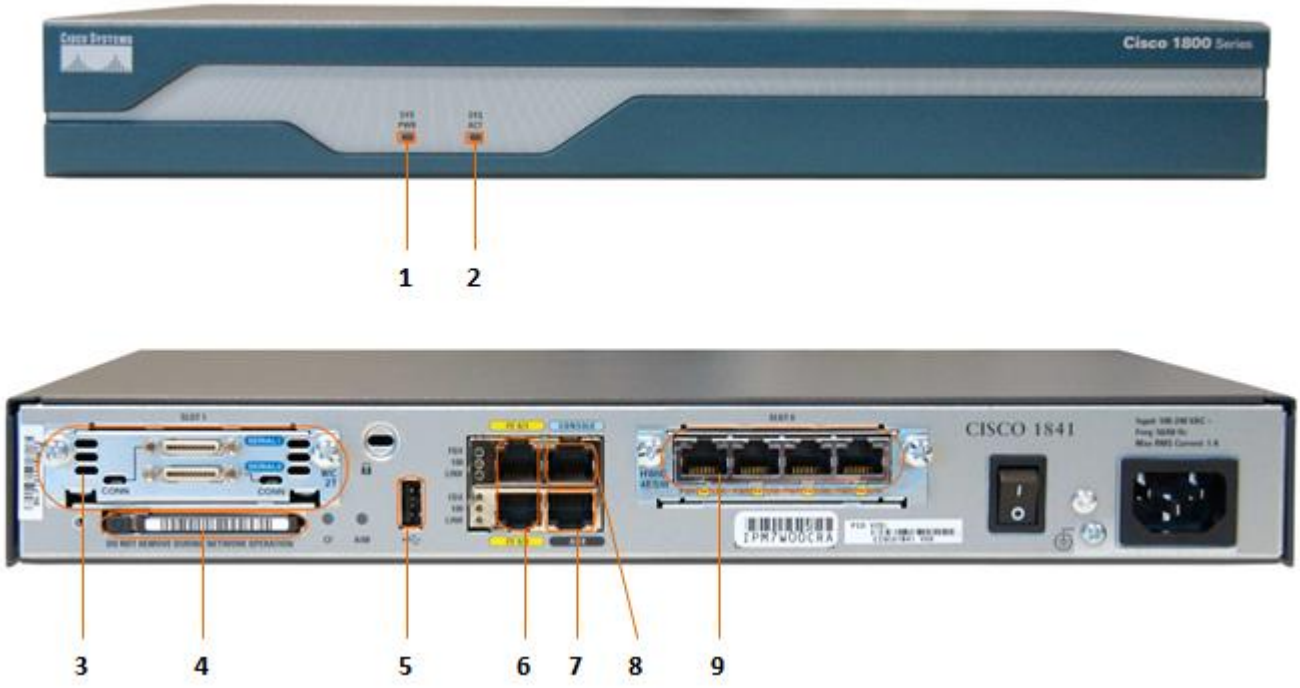



Рис. 6.1. Зовнішній вигляд маршрутизатора Cisco 1841

На зворотній стороні маршрутизатора розміщені порти та слоти для різних модулів:

3. Модульний слот 1 (SLOT 1) з платою високошвидкісного інтерфейсу глобальної мережі (HWIC – High-speed WAN Interface Card), що містить два послідовних порти Serial1/0 та Serial0/0 для підключення

до глобальної мережі. Модульні слоти можуть використовуватися для різних типів інтерфейсів.

4. Модуль для флеш-пам'яті (Compact Flash Module) – цей змінний модуль використовується для зберігання операційної системи Cisco IOS та іншого службового програмного забезпечення маршрутизатора.
5. USB-порт (USB Port) – функція підключення USB флеш-накопичувачів дозволяє користувачам зберігати образи і конфігурації, а також безпосередньо завантажуватися з USB флеш-накопичувачів.
6. Вбудовані порти FastEthernet – забезпечують можливість підключення до локальних мереж на швидкості 10/100 Мбіт/с.
7. Допоміжний порт (Auxiliary Port) – цей порт використовується для налаштування маршрутизатора через модемне з'єднання.
8. Консольний порт (Console Port) – цей порт використовується для налаштування маршрутизатора з безпосередньо підключеного вузла.
9. Модульний слот 0 (SLOT 0) з чотирьохпортовим Ethernet-комутатором – дозволяє підключатися до різних пристроїв по локальній мережі.

Маршрутизатор працює під управлінням міжмережевої операційної системи (IOS – Internetworking Operating Software). Операційна система Cisco IOS дозволяє пристрою Cisco відправляти і приймати мережевий трафік в провідний або бездротової мережі. Програма Cisco IOS пропонується користувачам у вигляді модулів, які називаються образами. Ці образи підтримують різні функції для компаній будь-якого розміру.

Існує багато різних типів і версій образів Cisco IOS. Вони розроблені для конкретних моделей маршрутизаторів, комутаторів і ISR. Перед тим як приступити до конфігурування маршрутизатора, необхідно з'ясувати, який образ і версія IOS завантажені.

### 6.1.2. Завантаження маршрутизатора

Процес завантаження маршрутизатора складається з трьох етапів (рис. 6.2).

**1.** Виконання **самотестування при включенні живлення** (Power-on self-test, **POST**) і запуск програми початкового завантаження (Bootstrap).

Програма POST (зберігається в ROM) служить для тестування апаратного забезпечення маршрутизатора. Після завершення програми POST завантажується програма початкового завантаження, яка зберігається в ROM. Програма призначена для пошуку коректного образу операційної системи IOS.

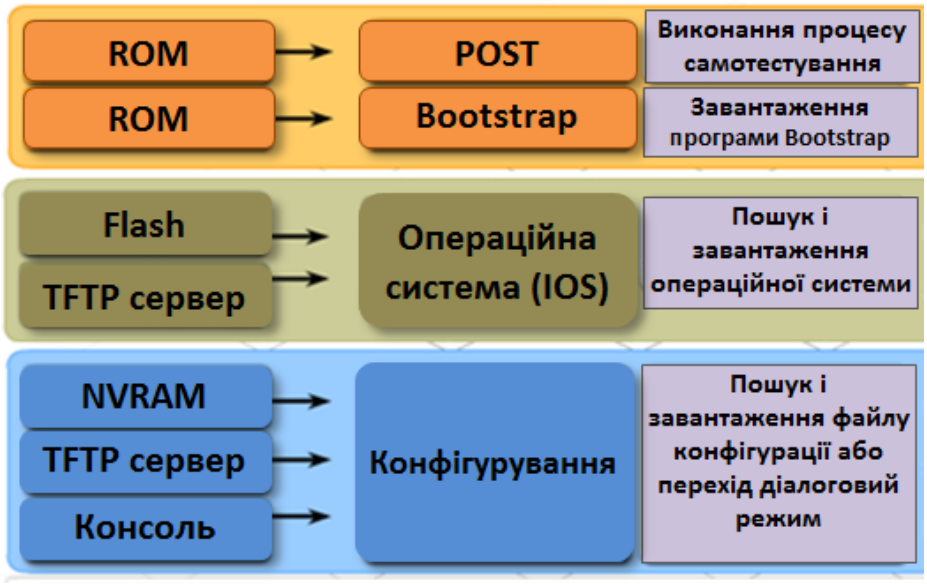



Рис. 6.2. Процес завантаження маршрутизатора

**2.** Пошук та завантаження **операційної системи** Cisco **IOS**.

Програма початкового завантаження знаходить Cisco IOS і завантажує її в RAM. Файли Cisco IOS можуть перебувати в одному з трьох місць: флеш-пам'ять, сервер TFTP, або інше місце, яке вказане у файлі початкової конфігурації. За замовчуванням програма Cisco IOS завантажується з флеш-пам'яті. Для виконання завантаження з інших місць необхідно змінити параметри конфігурації. Точне розміщення образу Cisco IOS, який буде завантажений на маршрутизатор, описується командою **boot system** в файлі конфігурації.

**3.** Пошук і виконання файлу **початкової конфігурації** або перехід в діалоговий режим.

Після завантаження операційної системи Cisco IOS програма початкового завантаження шукає файл початкової конфігурації в енергонезалежній пам'яті (NVRAM). Цей файл містить збережені раніше команди і параметри конфігурації, включаючи адреси інтерфейсів, відомості про маршрутизацію, паролі та інші параметри конфігурації.

Якщо файл конфігурації не буде знайдений, маршрутизатор запропонує користувачеві перейти в діалоговий режим налаштування, щоб приступити до конфігурування. Даний метод не потребує точних знань про конфігурування маршрутизатора. Для конфігурування достатньо відповісти на запитання, які ставить діалог конфігурації. В будь-який момент можна перейти в діалоговий

режим конфігурування за допомогою команди setup.

Якщо файл початковій конфігурації знайдений, він буде скопійований в RAM і на екрані з'явиться ім'я вузла. Поява такого повідомлення означає, що маршрутизатор успішно виконав завантаження програми Cisco IOS і файлу конфігурації.

Після успішного завантаження маршрутизатора можна скористатися командою **show version** для перевірки основних апаратних і програмних компонентів, які використовуються в процесі завантаження, а також для усунення несправностей. Після виконання команди **show version** виводяться наступні дані (рис. 6.3):

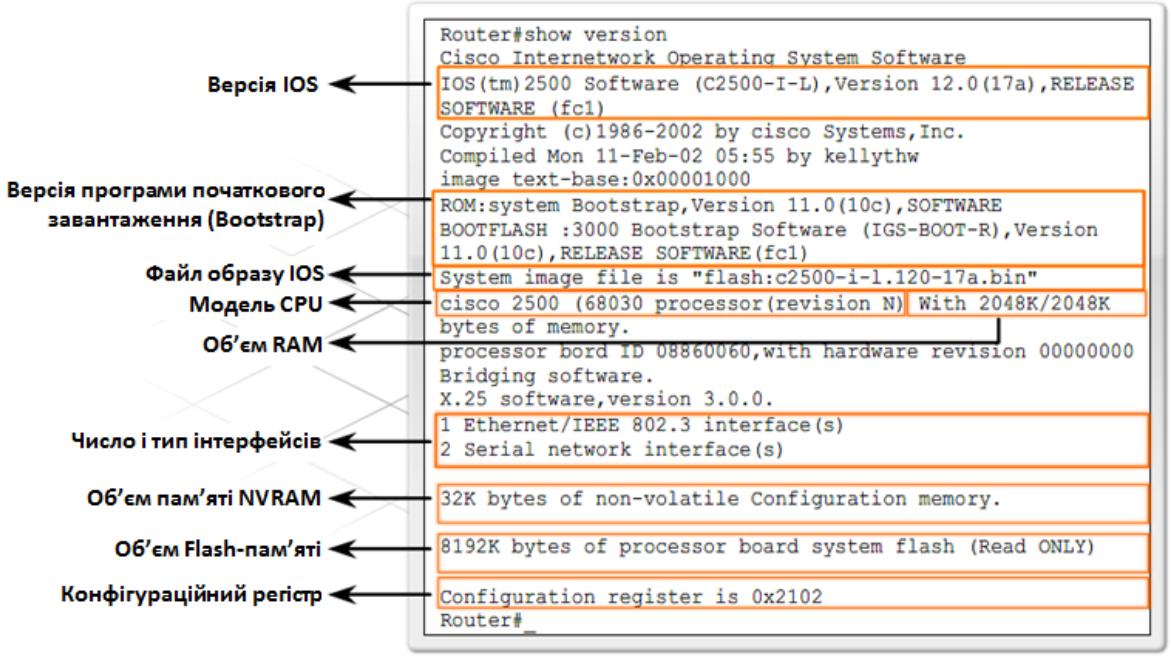



Рис. 6.3. Виконання команди **show version**

- Використовувана версія ОС Cisco IOS.
- Версія програми початкового завантаження системи (Bootstrap), яка зберігається в ROM і використовувалася для первинного завантаження маршрутизатора.
- Повне ім'я файлу образу Cisco IOS і його місцезнаходження.
- Тип центрального процесора маршрутизатора і обсяг RAM. При оновленні програми Cisco IOS може знадобитися збільшення обсягу RAM.
- Кількість і тип фізичних інтерфейсів маршрутизатора.
- Обсяг енергонезалежної пам'яті (NVRAM), в якій зберігається файл початкової конфігурації.

- Обсяг флеш-пам’яті маршрутизатора. Флеш-пам’ять використовується для зберігання образу Cisco IOS. При оновленні Cisco IOS може знадобитися збільшення обсягу флеш-пам’яті.
- Поточне встановлене значення конфігураційного регістра програми – в шістнадцятковому виді.

Конфігураційний регістр визначає процедуру завантаження маршрутизатора. Наприклад, на заводі, за замовчуванням, встановлюється значення конфігураційного регістра 0x2102. Таке значення вказує, що маршрутизатор буде намагатися завантажити програму Cisco IOS з флеш-пам’яті, а файл початкової конфігурації – з NVRAM. Значення конфігураційного регістра можна змінити, змінивши тим самим місце, де маршрутизатор буде шукати образ Cisco IOS і файл початкової конфігурації в процесі завантаження.

### 6.1.3. Конфігураційні файли

Важливо мати чітке розуміння відмінності між файлом початкової конфігурації і файлом поточної конфігурації (рис. 6.4).

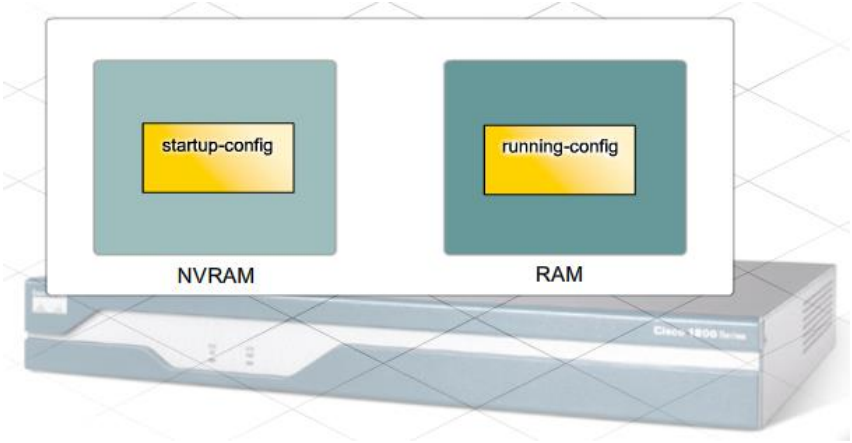



Рис. 6.4. Файли початкової та поточної конфігурації

**Файл початкової конфігурації (startup-config)**

Файл початковій конфігурації являє собою збережений файл конфігурації, що встановлює при кожному включенні маршрутизатора його попередньо налаштовані параметри. Цей файл зберігається в енергонезалежній пам’яті (NVRAM), що забезпечує його збереження навіть при відключенні живлення маршрутизатора.

При включенні маршрутизатора файл початкової конфігурації копіюється з енергонезалежної пам’яті (NVRAM) в оперативну пам’ять (RAM). Коли файл початкової конфігурації завантажується в RAM, він визначає початкову поточну

конфігурацію маршрутизатора, і таким чином, перетворюється в файл поточної конфігурації (running-config).

**Файл поточної конфігурації (running-config)**

Термін «поточна конфігурація» відноситься до поточного файлу конфігурації, що виконується в RAM маршрутизатора. У цьому файлі містяться команди, що визначають принципи роботи пристрою в мережі.

Файл поточної конфігурації зберігається в оперативній пам'яті маршрутизатора. Поки цей файл знаходиться в RAM, можна вносити зміни в конфігурацію і в різні параметри маршрутизатора. Однак, при кожному виключенні маршрутизатора поточна конфігурація втрачається, якщо не зберегти її у файлі початкової конфігурації.

Зміни у конфігурації автоматично не зберігаються у файлі початкової конфігурації. Необхідно вручну скопіювати поточну виконувану конфігурацію в файл початкової конфігурації.

### 6.1.4. Підключення до маршрутизатора

Існує два способи підключення комп'ютера до маршрутизатора для його налаштування і моніторингу: управління поза каналом передачі даних (out-of-band management) та управління через канал передачі даних (in-band management) (рис. 6.5).

**Управління поза каналом передачі даних (out-of-band management)**

Для управління поза каналом передачі даних необхідно, щоб комп'ютер був підключений безпосередньо до консольного порту або до допоміжного порту (AUX) маршрутизатора. Підключення маршрутизатора до локальної мережі при цьому не вимагається. Спосіб управління поза каналом передачі даних використовують при початковому налаштуванні маршрутизатора, оскільки неналаштований мережевий пристрій не бере участь в роботі мережі. Крім того, цей спосіб використовується в тому випадку, якщо зв'язок з мережею поганий і до маршрутизатора неможливо підключитися віддалено. Для здійснення управління поза каналом передачі даних необхідно, щоб на комп'ютері був встановлений клієнт емуляції терміналу (наприклад, HyperTerminal).

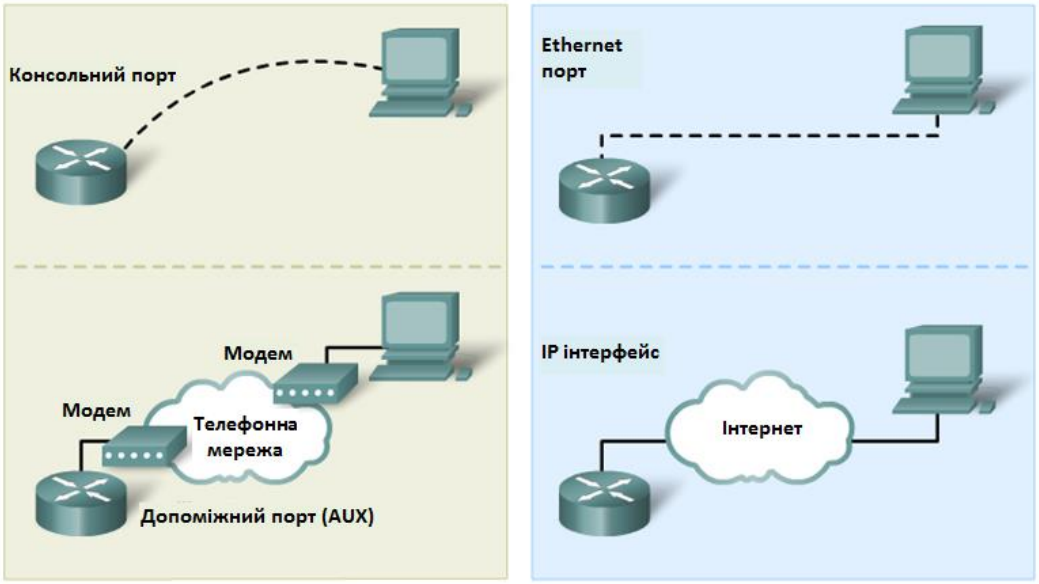



Рис. 6.5. Способи підключення комп'ютера до маршрутизатора

**Управління через канал передачі даних (in-band management)**

Управління через канал передачі даних використовується для моніторингу та внесення змін у конфігурацію маршрутизатора за допомогою мережевих підключень. Щоб встановити зв'язок комп'ютера з маршрутизатором і виконати завдання по налаштуванню чи управлінню, потрібно підключити до мережі хоча б один налаштований мережевий інтерфейс пристрою. Для підключення маршрутизатора в режимі управління через канал передачі даних використовується два протоколи – Telnet або SSH. Відслідковувати роботу маршрутизатора або змінювати його конфігурацію можна через веб-браузер або клієнт Telnet.

Маршрутизатори Cisco можна налаштовувати двома методами: за допомогою інтерфейсу командного рядка **CLI (Command Line Interface**) Cisco IOS та за допомогою веб-інструменту **SDM (Security Device Manager)**.

Інтерфейс командного рядка (CLI) – це текстова програма, що дозволяє вводити і виконувати команди Cisco IOS, і таким чином налаштовувати, відстежувати і обслуговувати пристрої Cisco. В Cisco CLI можна виконувати задачі управління поза каналом передачі даних (out-of-band management) та управління через канал передачі даних (in-band management).

За допомогою команд CLI можна змінювати конфігурацію пристрою і відображати поточний статус процесів в маршрутизаторі. За допомогою CLI досвідчені користувачі можуть заощадити багато часу при створенні різної складності конфігурацій. Майже у всіх мережевих пристроїв Cisco CLI інтерфейс

приблизно однаковий. Після завершення послідовності операцій при включенні маршрутизатора і появі на екрані повідомлення **Router>** можна використовувати CLI для введення команд Cisco IOS (рис. 6.6).

Фахівці, які знають команди CLI і вміють їх використовувати, можуть легко відстежувати і налаштовувати різні мережеві пристрої. Для CLI розроблена велика довідкова система, яка дозволяє настроювати і відстежувати пристрою.

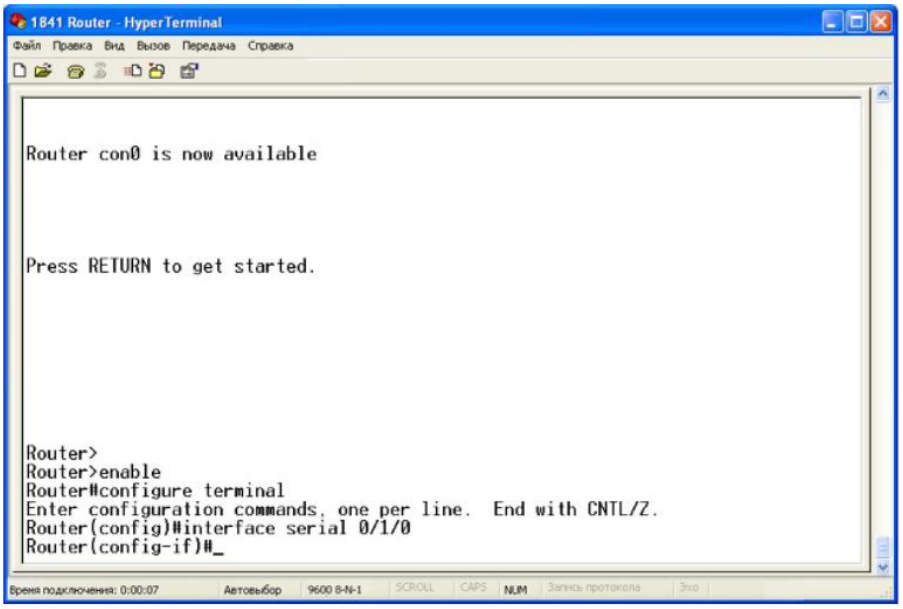



Рис. 6.6. Інтерфейс командного рядка (CLI) Cisco IOS

Засіб SDM – це веб-інструмент управління маршрутизатором. На відміну від командного рядка, SDM можна застосовувати тільки для задач управління через канал передачі даних (in-band management).

SDM Express спрощує завдання початковій конфігурації маршрутизатора. Базова конфігурація маршрутизатора створюється швидко і легко, в покроковому режимі (рис. 6.7).

Повний пакет SDM включає в себе розширені можливості, наприклад:

- налаштування додаткових підключень до мереж LAN і WAN;
- створення міжмережевих екранів;
- налаштування VPN-підключень;
- вирішення завдань, пов’язаних з безпекою.

SDM підтримує широкий діапазон версій Cisco IOS і поставляється безкоштовно разом з багатьма маршрутизаторами Cisco. Якщо в маршрутизаторі встановлено засіб SDM, рекомендується використовувати його для завдання початкової конфігурації маршрутизатора. Це робиться шляхом підключення до

маршрутизатора через наявний на ньому мережевий порт.

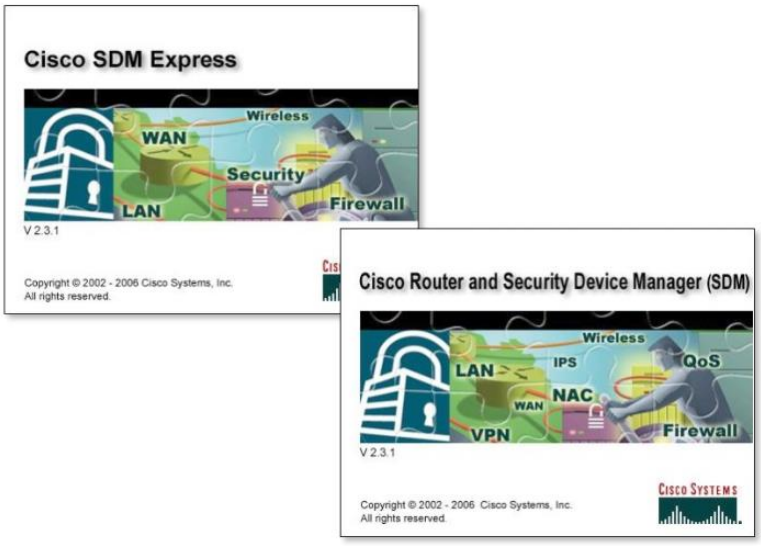



Рис. 6.7. Використання SDM Express

Не всі пристрої підтримують Cisco SDM. Крім того, SDM підтримує не всі команди CLI.

### 6.1.5. Налаштування базової конфігурації маршрутизатора за допомогою Cisco SDM Express

Cisco SDM Express – це засіб з пакету менеджера маршрутизаторів та пристроїв безпеки Cisco, що спрощує створення базової конфігурації маршрутизатора. Перед використанням SDM Express необхідно підключити кабель Ethernet, що йде від плати NIC комп'ютера, до Ethernet порту маршрутизатора.

Графічний інтерфейс SDM Express забезпечує покрокові інструкції для початкової конфігурації маршрутизатора. Після створення конфігурації маршрутизатор буде доступний в локальній мережі. Крім того, у нього може бути налаштоване з'єднання з мережею WAN, міжмережевий екран і до 30 функцій безпеки.

На екрані базової конфігурації SDM Express представлені основні параметри налаштування маршрутизатора (рис. 6.8).

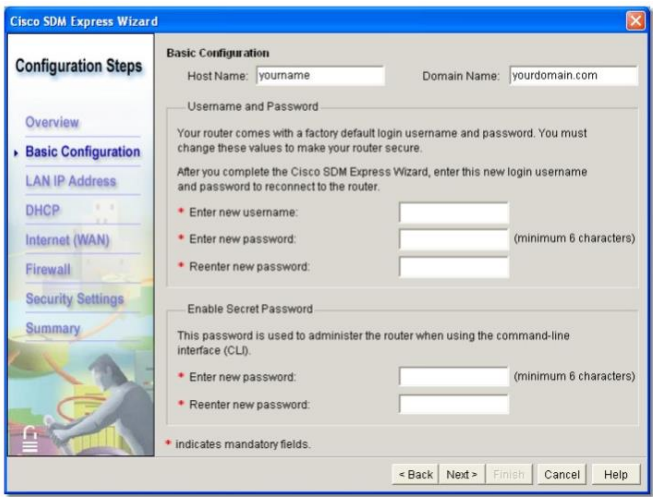



Рис. 6.8. Екран SDM Express для налаштування базової конфігурації маршрутизатора

Необхідна наступна інформація:

- **Host name** (ім’я вузла) – вказується ім’я маршрутизатора.
- **Domain name** (доменне ім’я) – вказується доменне ім’я організації.
- **Username and password** (ім’я користувача і пароль) – задається ім’я користувача та пароль доступу до SDM Express для налаштування маршрутизатора та відстеження його стану. Пароль повинен містити не менше шести символів.
- **Enable secret password** (включення секретного пароля) – задання паролю, що визначає доступ користувача до маршрутизатора для внесення змін у конфігурацію за допомогою інтерфейсу командного рядка, програми Telnet або консольних портів. Пароль повинен містити не менше шести символів.

Параметри конфігурації LAN дають можливість налаштувати IP адреси та під мережеві маски інтерфейсів маршрутизатора (рис. 6.9).

Із списку **Interface** (інтерфейс) вибирається інтерфейс, який потрібно налаштувати.

В полях **IP Address** (IP-адреса) та **Subnet Mask** (маска підмережі) задаються відповідно IP адреса та підмережева маска для обраного інтерфейсу.

За допомогою SDM Express маршрутизатор можна налаштувати як сервер DHCP, який буде динамічно призначати адреси комп’ютерам у внутрішній локальній мережі.

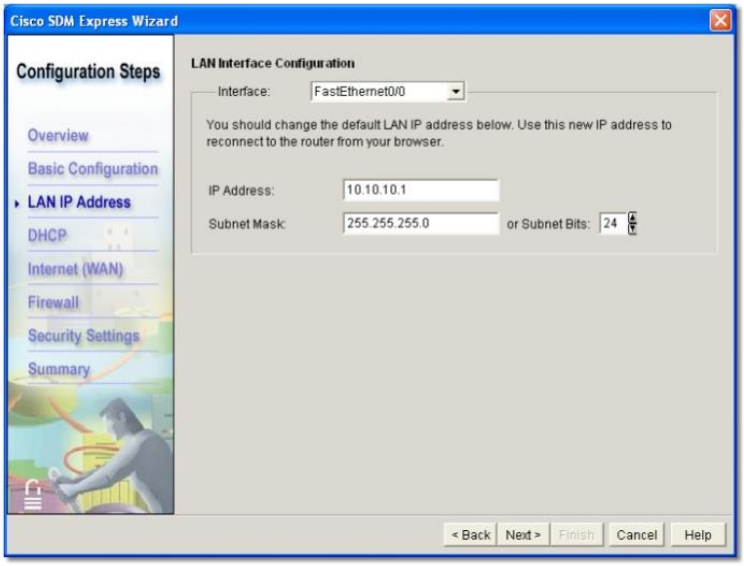



Рис. 6.9. Екран SDM Express для налаштування інтерфейсів маршрутизатора

Щоб використати маршрутизатор в якості сервера DHCP потрібно встановити прапорець **Enable DHCP Server on the LAN interface** (рис. 6.10).

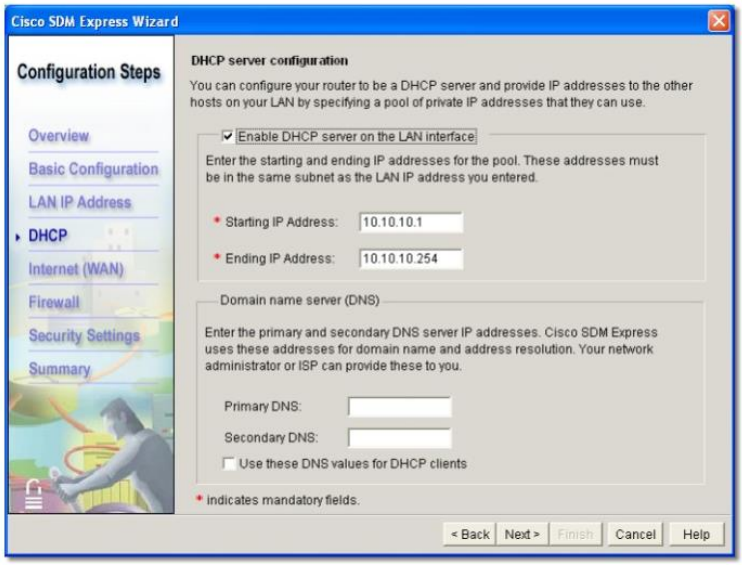



Рис. 6.10. Екран SDM Express для налаштування маршрутизатора в якості сервера DHCP

Встановлення цього прапорця дозволяє маршрутизатору призначати приватні IP-адреси комп'ютерам в локальній мережі. IP-адреси надаються вузлам на один день.

Протокол DHCP використовує діапазон допустимих IP-адрес. За замовчуванням для допустимого діапазону адрес використовується IP-адреса і

маска підмережі, введені для інтерфейсу мережі LAN.

**Початкова адреса (Starting IP Address)** та **кінцева адреса (Ending IP Address)** повинні знаходитись в тій же мережі або підмережі, що й LAN інтерфейс маршрутизатора.

Також у даному вікні можна задати основний **(Primary DNS)** та додатковий **(Secondary DNS)** DNS сервери. Вибір параметра **Use these DNS values for DHCP clients (**використовувати ці значення DNS для клієнтів DHCP) дозволяє серверу DHCP призначати клієнтам DHCP налаштування DNS.

За допомогою засобу Cisco SDM Express здійснюється лише базове налаштування маршрутизаторів Cisco. SDM Express підтримує не всі команди налаштування та відстеження роботи мережевих пристроїв. Для більш точного налаштування потрібно використовувати інтерфейс командного рядка (CLI) маршрутизатора.

## 6.2. Діагностування маршрутизатора за допомогою інтерфейсу командного рядка CLI

### 6.2.1. Рівні доступу до CLI

В Cisco IOS підтримується два рівні доступу до CLI: режим користувача (user EXEC mode) і привілейований режим (privileged EXEC mode) (рис. 6.11).

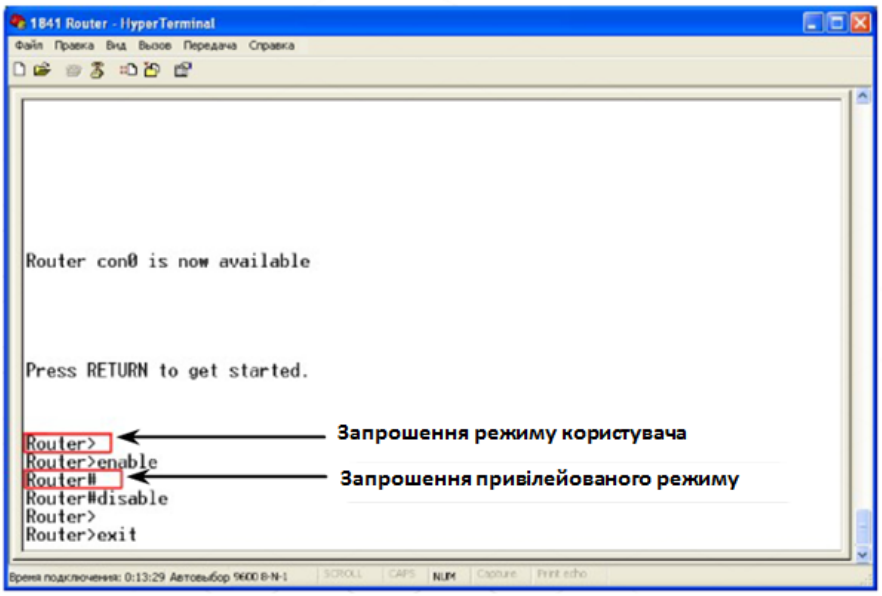



Рис. 6.11. Перехід між режимами роботи маршрутизатора

При включенні маршрутизатора Cisco IOS, за замовчуванням,

встановлюється режим доступу користувача. У цьому режимі запрошення командного рядка буде мати наступний вигляд:

**Router>**

Команди, які можна виконати в режимі користувача (user EXEC mode), зводяться до отримання інформації про роботу маршрутизатора та до діагностики за допомогою команд **show**, а також утиліт **ping** і **traceroute**. В даному режимі обмежені можливості перегляду конфігурації та пошуку неполадок.

Для виходу з режиму користувача в будь-який момент можна скористатися командою **logout**. Якщо на протязі певного періоду часу не вводиться ніяких команд, виникає тайм-аут і маршрутизатор автоматично завершує сеанс роботи з інтерпретатором.

Для введення команд, які змінюють роботу маршрутизатора необхідно мати привілейовані права доступу. Щоб перейти з режиму користувача в привілейований режим, потрібно ввести в командному рядку команду **enable** і натиснути клавішу **Enter**. Якщо налаштовано пароль на вхід в привілейований режим, то появиться рядок із запрошенням для вводу паролю. Командний рядок відповідно зміниться. У цьому режимі запрошення командного рядка буде мати наступний вигляд:

**Router>enable**

**Password:** [не виводиться на екран]

**Router#**

Для виходу з режиму привілейованого доступу та повернення в режим користувача потрібно ввести у командному рядку команду **disable** або **exit.**

Вхід в обидва режими можна захистити паролем або комбінацією імені користувача і пароля.

Лише з привілейованого режиму користувач може перейти режим глобальної конфігурації (global configuration mode) для налаштування маршрутизатора (рис. 6.12).

Щоб увійти в режим глобальної конфігурації, потрібно у привілейованому режимі ввести команду **configure terminal**. У цьому режимі запрошення командного рядка буде мати наступний вигляд:

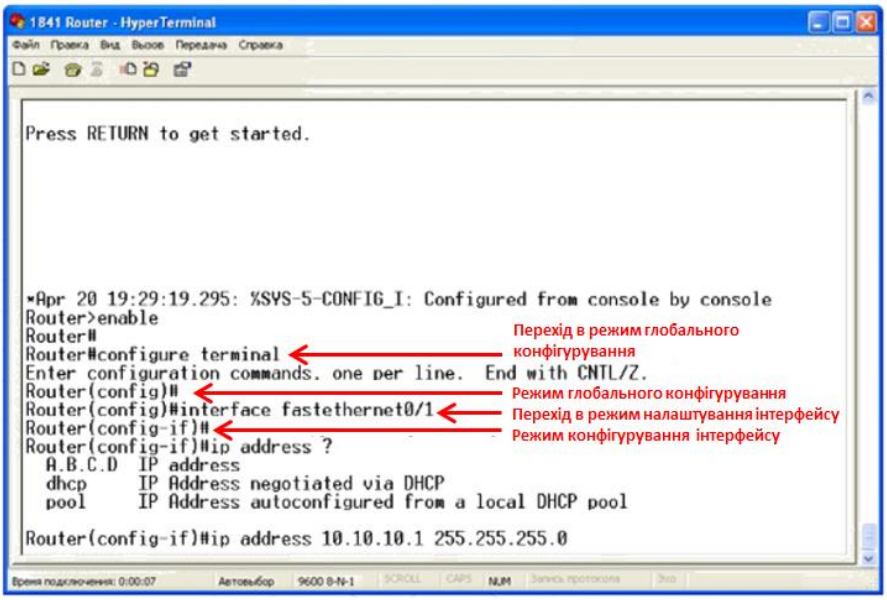



Рис. 6.12. Перехід в режим глобальної конфігурації маршрутизатора

**Router(config)#**

З режиму глобальної конфігурації адміністратор може увійти в інші підрежими.

Для налаштування інтерфейсів використовується режим конфігурування інтерфейсу. Для переходу в режим конфігурування інтерфейсу потрібно ввести в режимі глобальної конфігурації команду **interface [тип] [номер]**. У цьому режимі запрошення командного рядка буде мати наступний вигляд:

**Router(config-if)#**

### 6.2.2. Допомога користувачу

У CLI Cisco IOS є безліч функцій, які допомагають викликати необхідні команди конфігурації. При налаштуванні маршрутизатора особливо корисною є функція виклику контекстної довідки. Якщо ввести в командному рядку команду **help**, то можна отримати короткий опис про користування довідковою системою.

**Router#help**

Якщо ввести в командному рядку команду **?**, то з'явиться список усіх команд, які можна вводити в даному режимі.

```
Router#?
Exec commands:
```

| | |
|---|---|
| **<1-99>** | **Session number to resume** (номер сеансу зв’язку, який було тимчасово припинено) |
| **access-enable** | **Create a temporary Access-List entry** (створення тимчасового ACL входження) |
| **access-profile** | **Apply user-profile to interface** (використовує профілі користувачів на інтерфейсі PPP) |
| **access-template** | **Create a temporary Access-List entry** (створення тимчасового ACL входження) |
| **bfe** | **For manual emergency modes setting** (для задання вручну аварійної зупинки) |
| **cd** | **Change current directory** (зміна поточного каталогу) |
| **clear** | **Reset functions** (функція очищення) |
| **clock** | **Manage the system clock** (управління системним часом) |
| **configure** | **Enter configuration mode** (ввійти в режим конфігурування) |
| **connect** | **Open a terminal connection** (відкрити з’єднання з терміналом) |
| **copy** | **Copy from one file to another** (копіювати конфігурацію чи образ IOS) |
| **debug** | **Debugging functions (see also ‘undebug’)** (функція налаштування (див. також undebug)) |
| **delete** | **Delete a file** (видалити файл) |
| **dir** | **List files on a filesystem** (відображення списку файлів системи) |
| **disable** | **Turn off privileged commands** (вихід з привілейованого режиму) |
| **disconnect** | **Disconnect an existing network connection** (закрити існуюче мережеве з’єднання) |
| **enable** | **Turn on privileged commands** (дозволити використання команд привілейованого режиму) |
| **erase** | **Erase a filesystem** (видалити файл системи) |
| **exit** | **Exit from the EXEC** (завершити роботу інтерпретатора EXEC) |
| **help** | **Description of the interactive help system** (опис діалогової довідкової системи) |
| **lock** | **Lock the terminal** (заблокувати термінал) |
| **login** | **Log in as a particular user** (зареєструватися як конкретний користувач) |
| **logout** | **Exit from the EXEC** (завершити роботу інтерпретатора EXEC) |

| | |
|---|---|
| **more** | **Display the contents of a file** (перегляд вмісту файлу) |
| **mrinfo** | **Request neighbour and version information from a multicast router** (запит до групового маршрутизатора про інформацію щодо сусіда та його версію) |
| **mstat** | **Show statistics after multiple multicast traceroutes** (вивести статистичні дані після багатократного прослідковування групових маршрутів) |
| **mtrace** | **Trace reverse multicast path from destination to source** (прослідкувати груповий маршрут в напрямку від призначення) |
| **name-connection** | **Name an existing network connection** (дати ім’я існуючому мережевому з’єднанню) |
| **no** | **Disable debugging functions** (заборонити використання функцій відналагоджування) |
| **pad** | **Open a X.29 PAD connection** (відкрити з’єднання X.29 PAD) |
| **ping** | **Send echo messages** (послати ехо-повідомлення) |
| **ppp** | **Start IETF Point-to-Point Protocol (PPP)** (запустити протокол PPP IETF) |
| **pwd** | **Display current working directory** (відобразити поточний робочий каталог) |
| **reload** | **Halt and perform a cold restart** (провести холодне перезавантаження системи після зупинки) |
| **resume** | **Resume an active network connection** (відновити активне мережеве з’єднання) |
| **rlogin** | **Open an rlogin connection** (відкрити з’єднання rlogin) |
| **rsh** | **Execute a remote command** (виконати віддалену команду) |
| **send** | **Send a message to other tty lines** (послати повідомлення по іншій tty лінії) |
| **set** | **Set system parameter (not config)** (встановити параметри системи) |
| **setup** | **Run the SETUP command facility** (виконати команду SETUP) |
| **show** | **Show running system information** (вивести поточну інформацію про систему) |
| **Slip** | **Start Serial-line IP (SLIP)** (стартувати протокол SLIP) |
| **start-chat** | **Start a chat-script on a line** (стартувати chat-скрипт по лінії) |
| **systat** | **Display information about terminal lines** (вивести інформацію про лінії) |

| | |
|---|---|
| **telnet** | **Open a telnet connection** (відкрити з'єднання по Telnet) |
| **terminal** | **Set terminal line parameters** (встановити параметри відображення терміналу) |
| **test** | **Test subsystems, memory, and interfaces** (тестування підсистем, пам'яті та інтерфейсів) |
| **traceroute** | **Trace route to destination** (прослідкувати маршрут) |
| **tunnel** | **Open a tunnel connection** (відкрити тунельне з'єднання) |
| **undebug** | **Disable debugging functions (see also 'debug')** (заборонити виконання функцій налаштування (див. також debug)) |
| **undelete** | **Undelete a file** (відновити знищений файл) |
| **verify** | **Verify a file** (перевірити контрольну суму вмісту файлу) |
| **where** | **List active connections** (вивести перелік активних з'єднань) |
| **write** | **Write running configuration to memory, network, or terminal** (записати поточну конфігурацію в пам'ять, передати по мережі або на термінал) |
| **x3** | **Set X.3 parameters on PAD** (встановити параметри X.3 в PAD) |

Повідомлення --More-- вказує, що на екран виведено не всю інформацію. Можна натискати клавішу Enter для перегляду по стрічкам або клавішу пробілу для перегляду наступного екрану.

Для отримання допоміжної інформації про синтаксис певної команди, для її коректного введення потрібно ввести символ **?** після її імені. Причому введення **?** одразу після заданих декількох символів команди дозволить побачити всі команди, що починаються з таких символів (рис. 6.13).

**Router#con?**

configure connect

Якщо вказано достатню кількість символів, щоб команду було розпізнано, наприклад **conf** рівнозначно **configure**, її введення можна завершити і розпочати введення аргументів.

При умові введенні достатньої кількості символів, для розпізнання команди, можна використовувати клавішу Tab для автоматичного її доповнення (робити це необов'язково, оскільки маршрутизатор вже розпізнав команду).

**Router#conf**[Tab]

**Router#configure**

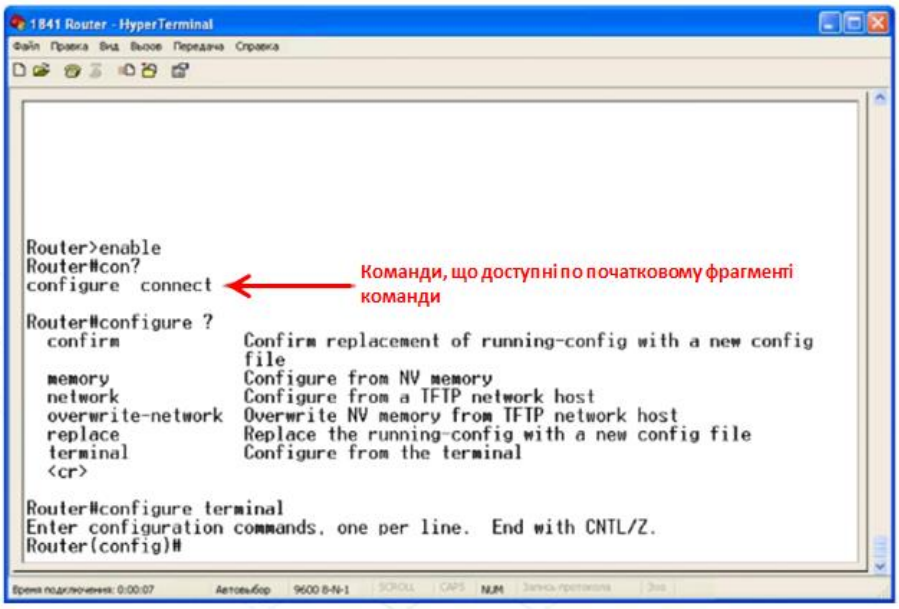



Рис. 6.13. Отримання довідки в CLI Cisco IOS

Як правило, команди мають декілька рівнів вкладеності. Це означає, що потрібно задати декілька аргументів. Для перегляду всіх можливих аргументів потрібно задати **?** після команди та додаткового пробілу. Значення **<cr>** (carrier return – символічне позначення клавіші Enter), означає, що введення команди можна завершити на даному етапі.

**Router#configure ?**

**confirm Confirm replacement of running-config with a new config file**

**memory Configure from NV memory**

**overwrite-network Overwrite NV memory from TFTP network host**

**replace Replace the running-config with a new config file**

**terminal Configure from the terminal**

**<cr>**

**Router#configure t ?**

**<cr>**

Іноді користувачі вводять команди з помилкою. Якщо команда введена не повністю або її не вдається розпізнати, з’явиться відповідне повідомлення CLI. Символом "%", зазначається початок повідомлення про помилку. Наприклад, якщо введена команда **interface** без додаткових параметрів, то з’явиться повідомлення про помилку, яке вказує, що команда введена не повністю (рис. 6.14):

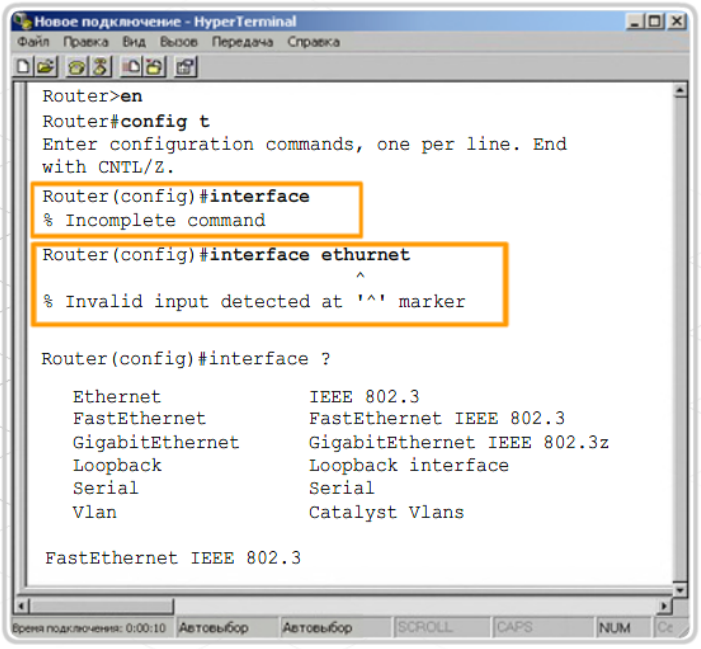



Рис. 6.14. Повідомлення про помилки в CLI Cisco IOS

**% Incomplete command** (Команда не завершена)

Щоб коректно завершити команду, можна скористатись символом **?** для отримання списку доступних параметрів.

Якщо введена невірна команда, з'явиться наступне повідомлення:

**% Invalid input detected** (Неприпустима команда)

Іноді важко помітити помилку в невірно введеній команді. На цей випадок, в CLI є індикатор помилок. У тому місці рядка команди, де знаходиться неправильний або нерозпізнаний символ, з'являється знак вставки **'^'**. Завдяки цьому, користувач може повернутися до потрібного місця і ввести необхідні зміни або ж визначити правильну команду за допомогою функції довідки.

Крім цього, в Cisco IOS CLI є функція виклику раніше введених команд. Ця функція особливо зручна при введенні довгих або складних команд чи записів і викликається за допомогою команди **show history.**

```
Router#show history
     enable
   running-config
   show interface
   configure terminal
   show ip route
   show history
Router#
```

Збереження історії введення команд включається за замовчуванням, і система фіксує 10 записів командних рядків в буфері. Щоб змінити кількість командних рядків, які будуть записуватись системою протягом сеансу, використовується команди **terminal history size** або **history size**. Максимальна кількість командних рядків, що можуть бути записані – 256.

Для виклику з буфера останньої введеної команди використовується комбінація клавіш **Ctrl-P** або клавіша зі стрілкою вгору (↑). Для виклику наступних команд необхідно повторити процедуру.

Для роботи з командною стрічкою використовується декілька комбінацій клавіш, які приведені в табл. 6.1.

Таблиця. 6.1.

Комбінації клавіш для роботи в командному рядку Cisco IOS CLI

| Комбінація клавіш | Виконувана дія |
|---|---|
| Ctrl+A | Переміщенні на початок командної стрічки |
| Ctrl+E | Переміщення вкінець командної стрічки |
| Ctrl+F або → | Переміщення на один символ вперед |
| Ctrl+B або ← | Переміщення на один символ назад |
| Ctrl+P або ↑ | Повторити введення останньої команди |
| Ctrl+N або ↓ | Викликати останню введену команду |
| Esc+F | Перемістится на одне слово вперед |
| Esc+B | Перемістится на одне слово назад |

### 6.2.3. Команди перегляду стану маршрутизатора

Для перевірки стану маршрутизатора є декілька команд, які вводяться в привілейованому режимі. Вони дозволяють переглядати інформацію про конфігурацію та режим роботи пристрою (рис. 6.15).

Фахівці з обслуговування мережі широко користуються командами **show** для перегляду файлів конфігурації, перевірки стану інтерфейсів, а також для контролю робочого стану маршрутизатора.

За допомогою команди **show** можна відобразити стан практично будь-якого процесу або функції маршрутизатора. Найбільш використовуваними командами є наступні:

**show processes –** виводить перелік активних процесів на маршрутизаторі та рівень навантаження CPU: за останні 5 секунд, 1 хвилину та 5 хвилин. До інформації про процеси відносять: **PID** – ідентифікаційний номер кожного

процесу; **QTy** – пріоритет в черзі та стан процесу; **PC** – лічильник програм; **Runtime** – час CPU, відведений під процес; **Invoked** – загальний час активності процесу; **uSecs** – час CPU, відведений під виклик кожного процесу; **Stacks** – нижня межа стека і загальний доступний об'єм стеку в байтах; **TTY** – вказує який термінал керує процесом; **Process** – ім'я процесу.

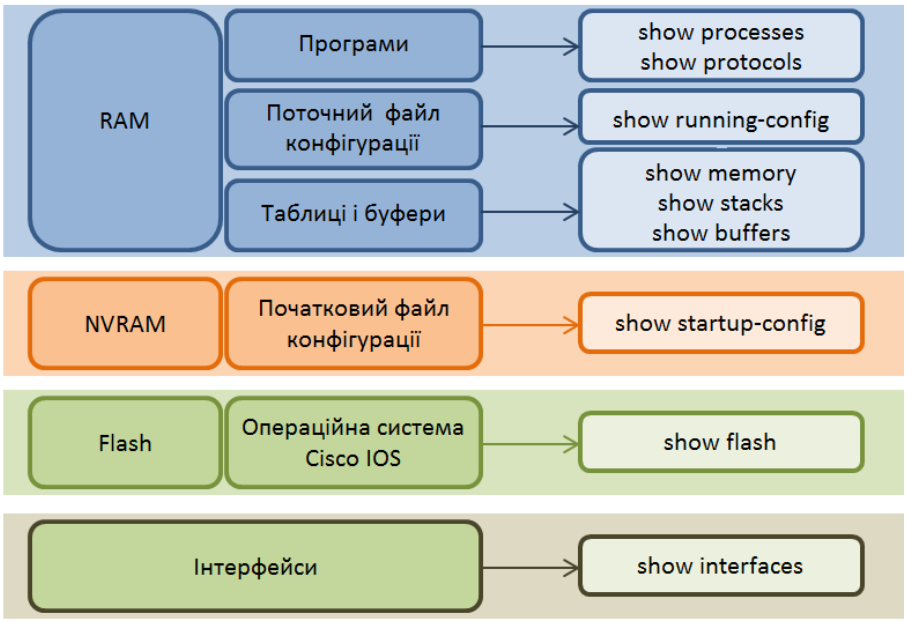



Рис. 6.15. Використання команд **show** для перегляду стану маршрутизатора

**ISPRouter#show processes**

[Виводиться лише фрагмент даних виконання команди]

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

| PID | QTy | PC | Runtime (ms) | Invoked | uSecs | Stacks | TTY | Process |
|---|---|---|---|---|---|---|---|---|
| 1 | Csp | 602F3AF0 | 0 | 1627 | 0 | 2600/3000 | 0 | Load Meter |
| 2 | Lwe | 60C5BE00 | 4 | 136 | 29 | 5572/6000 | 0 | CEF Scanner |
| 3 | Lst | 602D90F8 | 1676 | 837 | 2002 | 5740/6000 | 0 | Check heaps |
| 4 | Cwe | 602D08F8 | 0 | 1 | 0 | 5568/6000 | 0 | Chunk Manager |
| 5 | Cwe | 602DF0E8 | 0 | 1 | 0 | 5592/6000 | 0 | Pool Manager |
| 6 | Mst | 60251E38 | 0 | 2 | 0 | 5560/6000 | 0 | Timers |
| 7 | Mwe | 600D4940 | 0 | 2 | 0 | 5568/6000 | 0 | Serial Backgrou |

--More--

**show protocols –** виводить інформацію про протоколи 3 рівня, що працюють на маршрутизаторі.

**ISPRouter#show protocols**

Global values:

Internet Protocol routing is enabled

```
Ethernet0/0 is up, line protocol is up
  Internet address is 219.17.100.1/24
Serial0/0 is up, line protocol is up
  Internet address is 199.6.13.1/24
Serial0/1 is up, line protocol is up
  Internet address is 201.100.11.2/24
```

**show running-config** – виводить на екран список параметрів поточного файлу конфігурації. Виведення інформації розпочинається словами **Current configuration:** (поточна конфігурація).

```
ISPRouter#sh running-config
Building configuration...

Current configuration : 556 bytes
!
version 12.3
service timestamps log datetime msec
service timestamps debug datetime msec
service password-encryption
!
hostname ISPRouter
!
enable secret 5 $1$qFX0$C84s3OOh9XOIq.XNB63f40!
!
interface FastEthernet0/0
 ip address 209.165.201.1 255.255.255.224
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 209.165.200.226 255.255.255.224
```

```
 clock rate 56000
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
ip classless
!
!
line con 0
 password cisco
 login
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

**show memory** – використовується для отримання загальної інформації про розподіл пам'яті та про її окремі блоки.

**Router#show memory**

| | Head | Total | Used | Free | Lowest | Largest |
|---|---|---|---|---|---|---|
| Processor | 84D10 | 1549040 | 1848 | 1544268 | 0 | 4772 |
| I/O | 200000 | 2097152 | 401000 | 1696152 | 1549596 | 1504464 |

**show stacks** – дозволяє переглядати використання стеків процесами і процедурами переривань, а крім того, у випадку, якщо відбулось перезавантаження після зриву системи, показує причину останнього перезавантаження.

**Router#sh stacks**

**Minimum process stacks:**

Free/Size Name

3528/4000 Router Init

2380/4000 Init
3416/4000 RADIUS INITCONFIG
3392/4000 DHCP Client
2092/4000 Virtual Exec

**Interrupt level stacks:**

| **Level** | **Called** | **Unused/Size** | **Name** |
|---|---|---|---|
| 3 | 9 | 2772/3000 | Serial interface state change interrupt |
| 4 | 160344 | 2496/3000 | Network interfaces |
| 5 | 1012 | 2896/3000 | Console Uart |

**show buffers –** дозволяє переглянути розміри малих (Small), середніх (Middle), великих (Big), дуже великих (Very Big), величезних (Large) та гігантських (Huge) буферів.

**Router#show buffers**
**Buffer elements:**
499 in free list (500 max allowed)
165093 hits, 0 misses, 0 created
**Public buffer pools:**
**Small buffers, 104 bytes (total 50, permanent 50):**
49 in free list (20 min, 150 max allowed)
48921 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)
**Middle buffers, 600 bytes (total 25, permanent 25):**
23 in free list (10 min, 150 max allowed)
41445 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)
**Big buffers, 1524 bytes (total 50, permanent 50):**
50 in free list (5 min, 150 max allowed)
8144 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)
**VeryBig buffers, 4520 bytes (total 10, permanent 10):**
10 in free list (0 min, 100 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)
**Large buffers, 5024 bytes (total 0, permanent 0):**
0 in free list (0 min, 10 max allowed)

0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)
**Huge buffers, 18024 bytes (total 0, permanent 0):**
0 in free list (0 min, 4 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

**show flash –** виводить характеристики флеш-пам'яті, а також розмір файлів в ній та об'єм вільного місця.

**Router#show flash**

System flash directory:
File Length Name/status
1 13832032 c1841-ipbase-mz.123-14.T7.bin
[13832032 bytes used, 18682016 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)

**show startup-config** – виводить на екран детальний список початкового файлу конфігурації, що збережений в NVRAM. При завантаженні маршрутизатора вміст поточного файлу конфігурації (running-config) та файлу початкового конфігурації (startup-config) однаковий. Розрізнити, вміст якого саме файлу виводиться на консоль, можна по заголовку, який виводиться після введення команди. У випадку відображення поточної конфігурації це **Current configuration**, а в іншому випадку відображається розмір зайнятого місця NVRAM.

**ISPRouter#show startup-config**
Using 438 bytes
!
version 12.3
no service password-encryption
!
hostname ISPRouter
interface FastEthernet0/0
ip address 209.165.201.1 255.255.255.224
duplex auto
speed auto
!

```
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 ip address 209.165.200.226 255.255.255.224
 clock rate 56000
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
line con 0
line vty 0 4
 login
!
end
```

**show interfaces** – виводить інформацію про апаратні інтерфейси маршрутизатора та їх стан. Спочатку виводиться інформація про перший інтерфейс, потім про другий і т. д. Для перегляду інформації про конкретний інтерфейс, вказується його ім'я:

```
ISPRouter#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 000c.cfb0.1e01 (bia 000c.cfb0.1e01)
  Internet address is 209.165.201.1/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
```

Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

### 6.2.4. Тестування мережі

В більшості проблеми, що виникають в IP мережах, це проблеми пов'язані з помилками схеми адресування. Кожне тестування, як показано на рис. 6.6, проводиться на відповідному рівні OSI моделі. Тестування мережі проводиться за допомогою команд **telnet, ping, traceroute, show ip route** `та` **show interfaces**.

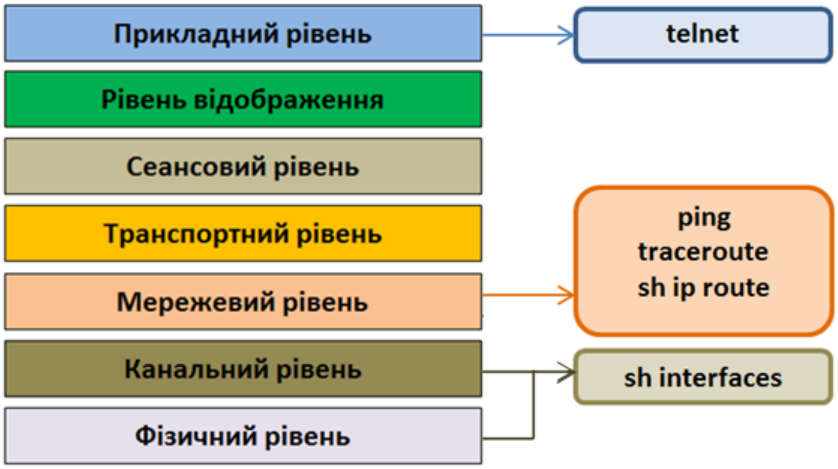



Рис. 6.6. Команди тестування мережі відповідно до рівнів OSI моделі

Протокол **telnet** з набору TCP/IP являє собою протокол віртуального терміналу, що дозволяє зв'язуватися з віддаленими хостами, в тому числі з маршрутизаторами, без фізичного під'єднання до них. Маршрутизатори Cisco можуть підтримувати до п'яти сеансів Telnet одночасно (**`vty 0 4`**). Для

доступу до віддаленого маршрутизатора потрібно ввести команду **telnet** та IP адресу віддаленого хоста. Для маршрутизаторів Cisco це може бути IP адреса будь-якого активного інтерфейсу на маршрутизаторі.

```
ISPRouter>telnet 223.8.151.1
Trying 223.8.151.1 ... Open

User Access Verification

Password:
SPRouter>exit
```

Для завершення сеансу роботи потрібно ввести команду **exit .**

Якщо до того чи іншого хоста не можна під'єднатися по **telnet** або, якщо необхідно протестувати зв'язок між двома або декількома хостами на мережевому рівні, найкраще використовувати ехо-запити **PING (**Packet Inter-Net Groper**). PING** використовується не тільки в мережах IP, але й для будь-якого іншого протоколу мережевого рівня, такі як IPX, AppleTalk, Apollo, VINES і DECnet. В таблиці 6.2 представлено відповіді на ехо-запит.

Таблиця 6.2.

Відповіді на виконання команди **ping**

| **Відповідь** | **Значення** |
|---|---|
| **!** | Успішно отримано відповідь на ехо-запит |
| **.** | Тайм-аут |
| **U** | Хост призначення недосяжний |
| **C** | Пакет Congested Experience |
| **?** | Невідомий тип пакету |
| **&** | Час життя пакету вийшов |

Команда **ping** відправляє ехо-запити (Echo-Request) протоколу ICMP зазначеному вузлу мережі й фіксує відповіді (ICMP Echo-Reply). Час між відправленням запиту й одержанням відповіді (RTT, Round Trip Time) дозволяє визначати двосторонні затримки у маршруті й частоту втрати пакетів, тобто побічно визначати завантаженість каналів передачі даних і проміжних пристроїв.

**ISPRouter#ping 223.8.151.1**
**!!!!!**

Розширений синтаксис команди **ping** надає більше можливостей, але підтримується тільки в привілейованому режимі.

**ISPRouter#**ping
Protocol [ip]:
Target IP address: 219.17.100.1
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 201.100.11.1
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]: y
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: v
Loose, Strict, Record, Timestamp, Verbose[V]:
Sweep range of sizes [n]: y
Sweep min size [36]: 50
Sweep max size [18024]: 2050
Sweep interval [1]: 200
Type escape sequence to abort.
Sending 10, [50..2000]-byte ICMP Echos to 219.17.100.1, timeout is 2 seconds:
Reply to request 0 (4 ms) (size 50)
Reply to request 1 (8 ms) (size 250)
Reply to request 2 (4 ms) (size 450)
Reply to request 3 (8 ms) (size 650)
Reply to request 4 (8 ms) (size 850)
Reply to request 5 (8 ms) (size 1050)
Reply to request 6 (8 ms) (size 1250)
Reply to request 7 (12 ms) (size 1450)
Request 8 timed out (size 1650)
Request 9 timed out (size 1850)
Request 10 timed out (size 2050)
Success rate is 72 percent (8/11), round-trip min/avg/max = 4/7/12 ms

Команду **traceroute** можна використовувати для пошуку маршрутів до віддалених хостів. На відміну від команди ping команда traceroute видає повідомлення про помилку, якщо час життя пакету (TTL – Time To Live) вийшов та тестує кожен вузол на шляху пакету.

Команда **traceroute** розпочинає роботу з відправлення пакету, TTL якого рівне 1. Тому перший маршрутизатор прийме цей пакет і поверне повідомлення про помилку. Далі маршрутизатор буде відправляти пакети з TTL, що постійно зростає, до тих пір, поки маршрутизатор не отримає повну інформацію про відстань, маршрут та час передачі до кожної точки призначення.

```
ISPRouter>traceroute ?
  WORD      Trace route to destination address or hostname
  appletalk AppleTalk Trace
  clns      ISO CLNS Trace
  ip        IP Trace
  ipx       IPX Trace
  oldvines  Vines Trace (Cisco)
  vines     Vines Trace (Banyan)

ISPRouter>traceroute ip 192.5.5.1
  1 Router2 (210.93.105.1) 8 msec 12 msec 4 msec
  2 Router3 (204.204.7.1) 12 msec 4 msec 4 msec
  3 Router4 (199.6.13.1) 8 msec 4 msec 4 msec
  4 Router5 (201.100.11.1) 8 msec *  8 msec
```

Коли пакет команди **traceroute** не досягає точки призначення, на екран виводиться (*), при сукупності повідомлень «порт недосяжний» і тайм-аут. Інші відповіді перераховані в таблиці 6.3.

Команда **sh ip route** дозволяє переглянути таблицю маршрутизації, де можна визначити маршрути, які використовуються ним для передачі даних. Для тестування важливо, щоб шлях до мережі, якій призначається пакет, містився в таблиці маршрутизації. Якщо цей шлях відсутній, то передача даних неможлива.

Таблиця 6.3.

Відповіді на виконання команди **traceroute**

| Відповідь | Значення |
|---|---|
| **!H** | Маршрутизатор отримав пробний пакет, але не переслав його далі внаслідок встановленого списку доступу. |
| **P** | Недосяжний протокол |
| **N** | Недосяжна мережа |
| **U** | Недосяжний порт |
| ***** | Тайм-аут |

**ISPRouter**#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR
T - traffic engineered route

Gateway of last resort is 201.100.11.1 to network 0.0.0.0

R 210.93.105.0/24 [120/2] via 199.6.13.2, 00:00:15, Serial0
R 212.109.59.0/24 [120/1] via 201.100.11.1, 00:00:19, Serial1
R 192.169.15.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
R 192.169.8.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
R 205.7.5.0/24 [120/1] via 201.100.11.1, 00:00:19, Serial1
R 193.192.212.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
C 219.17.100.0/24 is directly connected, Ethernet0
R 192.169.9.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
C 199.6.13.0/24 is directly connected, Serial0
R 192.169.11.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
R 204.204.7.0/24 [120/1] via 199.6.13.2, 00:00:16, Serial0
R 192.168.176.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
R 192.169.4.0/24 [120/3] via 201.100.11.1, 00:00:19, Serial1
--More--

**show interface** команда дозволяє переглянути стан протоколів лінії і канального рівня. Інтерфейс складається з двох частин: фізичної (апаратної) та логічної (програмної). Апаратна частина (кабелі, конектори інтерфейсу) відповідає за реальне з'єднання між мережевими пристроями (фізичний рівень). Програмна частина – це повідомлення про працездатність, передача контрольної інформації, передача даних користувача між з'єднаними пристроями (канальний рівень).

```
ISPRouter#sh int serial 1
```

Опис станів інтерфейсів приведено в таблиці 6.4.

Таблиця 6.4.

Стани інтерфейсів маршрутизатора при виконанні команди **show interface**

| Стан | Значення |
|---|---|
| **Serial is up, line protocol is up** | Інтерфейс працездатний |
| **Serial is up, line protocol is down** | Проблема з'єднання |
| **Serial is down, line protocol is down** | Проблема інтерфейсу |
| **Serial is administratively down, line protocol is down** | Відключено |

Протокол лінії позначає розбиття на фрейми на канальному рівні і вказує, що обрано правильний тип кадру і є зв'язок між кінцевими пунктами. Якщо інтерфейс активний, а протокол лінії – ні, то це означає, що є проблеми із з'єднанням або таймерами. Якщо і протокол і інтерфейс лінії неактивні, то проблема з інтерфейсом. Якщо вказано, що інтерфейс відключено адміністратором і протокол лінії неактивний, то інтерфейс вимкнено.

Скорочену інформацію про стани інтерфейсів можна переглянути командою **sh ip int brief.**

```
ISPRouter#sh ip int b
Interface        IP-Address      OK? Method  Status      Protocol
Ethernet0        219.17.100.1    YES  NVRAM  up          up
Serial0          219.17.100.1    YES  NVRAM  up          up
Serial1          201.100.11.2    YES  NVRAM  up          up
```

## 6.3. Конфігурування маршрутизатора за допомогою інтерфейсу командного рядка CLI

### 6.3.1. Базове конфігурування маршрутизатора за допомогою діалогового режиму

Файл конфігурації містить команди, що визначають конфігурування маршрутизатора і конкретизують функції, які він буде виконувати. Якщо при завантаженні файл конфігурації не був знайденим, то маршрутизатор запропонує користувачеві перейти в діалоговий режим конфігурування, щоб приступити до базового налаштування маршрутизатора.

Перехід в діалоговий режим конфігурування також буде запропоновано після введення команди **erase startup-config** (очистити початковий файл конфігурування startup-config, який зберігається в NVRAM) та перезавантаження маршрутизатора, за допомогою команди **reload**. В будь-який момент можна перейти в діалоговий режим конфігурування за допомогою команди **setup .** Даний метод не потребує точних знань про конфігурування маршрутизатора. Для конфігурування достатньо відповісти на запитання, які ставить діалог конфігурації. Процедура діалогового режиму конфігурування виглядає наступною:

**Notice: NVRAM invalid, possibly due to write erase.**
**--- System Configuration Dialog ---**
**Would you like to enter the initial configuration dialog? [yes/no]: yes**
[Чи ви хочете ввійти в конфігураційний діалог початкового налаштування?]
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
[В будь-який момент можна ввести ? для отримання довідки
Використовуйте CTRL-C для переривання діалогу
Значення по замовчуванню відображаються в квадратних дужках]
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
[Основний режим конфігурування системи дозволить сконфігурувати лише параметри достатні для встановлення зв'язку, режим

розширеної
конфігурації дозволить сконфігурувати кожен інтерфейс системи.]
**Would you like to enter basic management setup? [yes/no]: yes**
[Чи хочете ви ввійти в основний режим конфігурування системи?]

**Configuring global parameters:**
[Конфігурування глобальних параметрів]

**Enter host name [Router]: ISPRouter**
[Введіть ім'я маршрутизатора]

The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
[Секретний пароль на привілейований режим використовується
для заборони доступу до привілейованого та конфігураційного
режимів.
Цей пароль кодується в конфігурації після введення]
**Enter enable secret: class**
[Введіть секретний пароль]

The enable password is used when you do not specify an
enable secret password, with some older software versions.
[Пароль на привілейований режим використовується,
коли не вказано секретний пароль]
**Enter enable password: cisco**
[Введіть привілейований пароль]

The virtual terminal password is used to protect
access to the router over a network interface.
[Пароль на віртуальний термінал використовується для заборони
доступу до маршрутизатора через його інтерфейс]
**Enter virtual terminal password: cisco**
[Введіть пароль на віртуальний термінал]

**Configure SNMP Network Management? [yes]: no**

**Current interface summary**
[Поточний стан інтерфейсів]

| **Interface** | **IP-Address** | **OK?** | **Method** | **Status** | **Protocol** |
|---|---|---|---|---|---|
| FastEthernet0/0 | unassigned | YES | unset | administratively down | down |
| FastEthernet0/1 | unassigned | YES | unset | administratively down | down |
| Serial0/0 | unassigned | YES | unset | administratively down | down |
| Serial0/1 | unassigned | YES | unset | administratively down | down |

**Enter interface name used to connect to the management network from the above interface summary: FastEthernet0/0**
[Введіть назву інтерфейсу, який ви хочете конфігурувати]

**Configuring interface FastEthernet0/0:**
Use the 100 Base-TX (RJ-45) connector? [yes]:
Operate in full-duplex mode? [no]:
Configure IP on this interface? [yes]:
IP address for this interface: 200.200.200.1
Subnet mask for this interface [255.255.255.0] :
Class C network is 200.200.200.0, 24 subnet bits; mask is /24
[Вкінці діалогового режиму конфігурування маршрутизатора потрібно вибрати одну із наступних дій]
**[0] Go to the IOS command prompt without saving this config.**
[Перейти до стрічкового конфігурування без збереження даної конфігурації]
**[1] Return back to the setup without saving this config.**
[Повернутися в setup без збереження даної конфігурації]
**[2] Save this configuration to nvram and exit.**
[Зберегти дану конфігурацію в NVRAM та вийти]
**Enter your selection [2]:**
[введіть вибір]

Building configuration...

Потрібно зауважити, що основний режим конфігурування дозволяє сконфігурувати тільки один інтерфейс для подальшого конфігурування.

### 6.3.2. Початкове конфігурування маршрутизатора за допомогою CLI

У початкове конфігурування маршрутизатора входить задання назви пристрою і паролів, які служать для контролю доступу до різних функцій маршрутизатора.

Однією з перших задач конфігурування є присвоєння маршрутизатору унікального імені. Якщо ім'я невизначено, система використовує ім'я по замовчуванню – **Router.** Для конфігурування імені маршрутизатора використовується команда **hostname *ім'я,*** яку потрібно ввести в режимі глобальної конфігурації.

```
Router(config)#hostname RouterISP
RouterISP(config)#
```

Можна також задати банер, який буде з'являтися при кожній спробі реєстрації на маршрутизаторі.

**Банер** – це текст, який бачить користувач при вході на маршрутизатор. Налаштування відповідного банера є частиною продуманого плану забезпечення безпеки. Банер повинен як мінімум містити попередження щодо несанкціонованого доступу. Не слід встановлювати банер у вигляді привітання для користувача, у якого немає відповідних прав доступу.

Для налаштування банеру використовується команда **banner motd.** Скорочення **motd** означає **message of the day** (повідомлення дня). Введення заголовку розпочинають з вибраного символу – обмежувача, зазвичай – **#.**

```
Router(config)#banner motd # WARNING! Unauthorized Access
Prohibited! #
```

Наступним кроком конфігурування є завдання паролів для запобігання несанкціонованого доступу до маршрутизатора.

Для забезпечення безпеки маршрутизаторів Cisco використовуються п'ять різних паролів: дозволений секрет (enable secret), дозволений пароль (enable password), пароль віртуального терміналу, пароль додаткового порту та пароль консолі.

**enable secret** – пароль на вхід в привілейований режим (рис. 5.7).

Використовується в версіях IOS 10.3 та новіших. Цей пароль використовує спеціальний режим кодування, що розроблений Cisco (не відображається відкритим текстом в файлах конфігурації). Рівень дозволеного секрету (enable secret) вищий від дозволеного паролю (enable password), якщо такий сконфігуровано. Задання секрету виконується або в режимі початкового конфігурування, або по команді **enable secret *пароль* .**

```
Router#conf t
Router(config)#enable secret network
```

**enable password** – пароль на вхід в привілейований режим (рис. 6.7). Використовується при відсутності дозволеного секрету, а також при роботі з старим програмним забезпеченням. Пароль відображається відкритим текстом в файлі конфігурації, тому секрет та пароль повинні не співпадати. В противному випадку, маршрутизатор видасть попередження і не дозволить співпадіння. Задання секрету виконується або в режимі початкового конфігурування, або по команді **enable password *пароль* .**

```
Router#conf t
Router(config)#enable password net
```

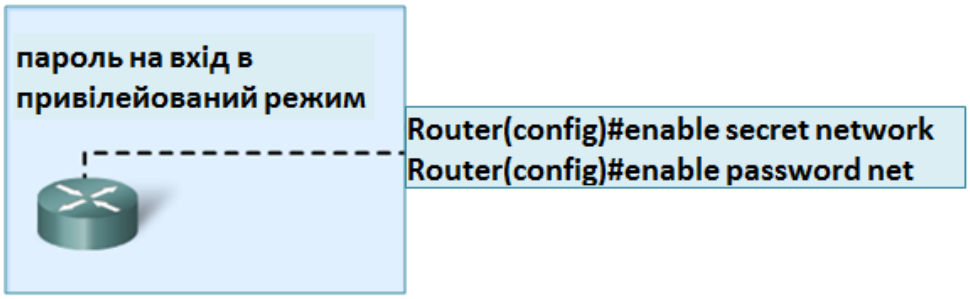



Рис. 6.7. Пароль на вхід в привілейований режим

Пароль віртуального терміналу **(vty)** використовується в сеансах Telnet з маршрутизатором (рис. 6.8). Цей пароль можна змінити в будь-який момент, але він обов’язково повинен бути визначений, оскільки в іншому випадку, спроба зв’язатися по Telnet з маршрутизатором буде невдалою.

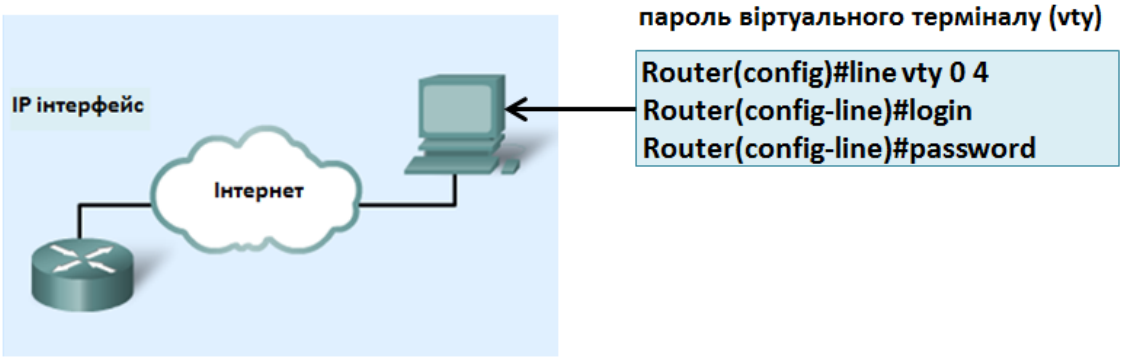



Рис. 6.8. Пароль віртуального терміналу (vty)

Задання паролю виконується в режимі початкового конфігурування або за допомогою конфігурування ліній **vty 0 4 .**

**Router#conf t**
**Router(config)#line vty 0 4**
**Router(config-line)#login**
**Router(config-line)#password network**

Конструкція **line vty 0 4** задає число одночасно можливих сеансів Telnet. Можна встановити паролі для кожного зв'язку, використовуючи команду **line vty [номер лінії] .** Команда **login** дозволяє включити режим перевірки паролю **.**

Пароль допоміжного порту (**aux**) використовується для захисту додаткового порту. Цей порт використовується для підключення модему до маршрутизатора при з'єднанні з віддаленою консоллю (рис. 6.9).

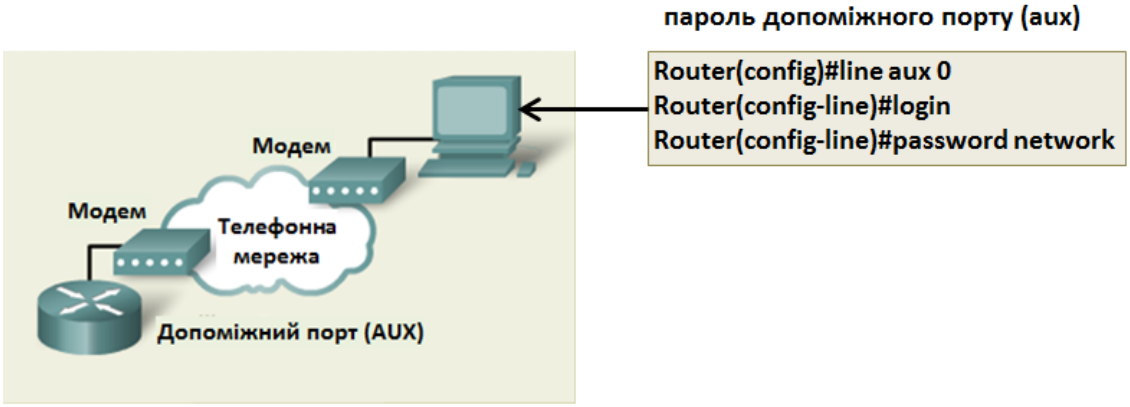



Рис. 6.9. Пароль допоміжного порту (aux)

**Router#conf t**
**Router(config)#line aux 0**

```
Router(config-line)#login
Router(config-line)#password network
```

Пароль консолі використовується для захисту порту консолі (console). Цей порт використовується для початкового налаштування маршрутизатора і задається наступним чином (рис. 6.10).

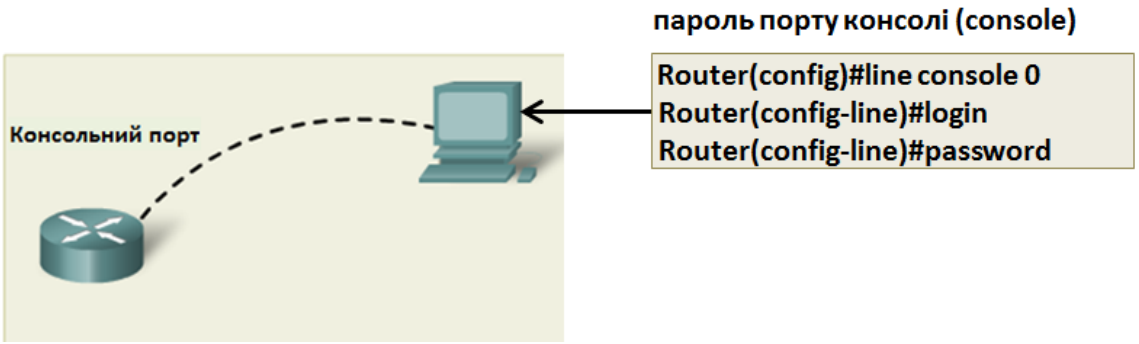



Рис. 6.10. Пароль порту консолі (console)

```
Router#conf t
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password network
```

### 6.3.3. Налаштування інтерфейсів маршрутизатора

Для направлення трафіку з однієї мережі в іншу інтерфейси маршрутизаторів налаштовуються таким чином, щоб вони могли брати участь у передачі даних в обох мережах. Інтерфейс, через який маршрутизатор підключається до мережі, зазвичай має IP-адресу та маску підмережі, призначені з допустимого діапазону адрес для хоста в даній мережі.

Маршрутизатор може мати різні типи інтерфейсів. Найчастіше зустрічаються послідовний інтерфейс (Serial) та інтерфейси Ethernet/FastEthernet. Вони позначаються Serial0/0, Serial0/1, FastEthernet0/0 і т. д., де перше число – це номер модуля, а друге – номер порта в модулі. При підключенні до локальної мережі використовуються інтерфейси Ethernet/FastEthernet.

При підключенні до WAN потрібне послідовне з’єднання, яке забезпечує ISP. На відміну від інтерфейсів Ethernet, послідовному інтерфейсу для контролю часу зв’язку потрібна синхронізація. У більшості середовищ цей сигнал надходить від обладнання для передачі даних (DCE – Data Circuit-Terminating Equipment), наприклад, модему або CSU/DSU.

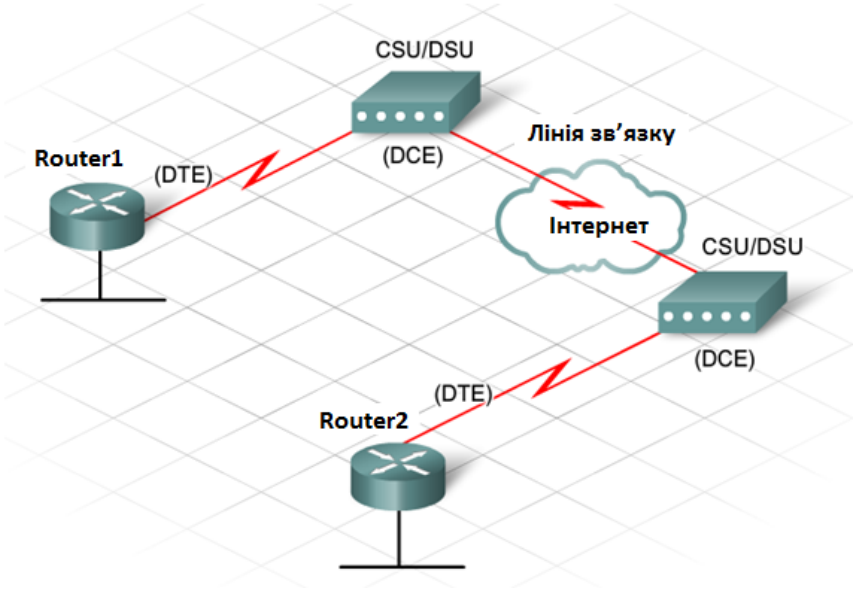



Рис. 6.11. Підключення маршрутизаторів через послідовні порти

Пристрій обслуговування каналу (CSU – channel service unit) – реалізує фактичний інтерфейс між каналом ISP і вузлом замовника. CSU підтримує якість лінії, відстежує з’єднання через інтерфейс «абонент-мережа» і виконує в каналі роль фізичної кінцевої точки.

Модуль обслуговування даних (DSU – data service unit) – відповідає за реальне перетворення сигналів локальної мережі в цифрові сигнали, що передаються по лінії зв’язку. DSU підключається до CSU і до обладнання, що встановлюється в приміщеннях замовника (CPE – customer premises equipment), тобто до мостів і маршрутизаторів, а також до пристроїв мультиплексування.

CSU і DSU зазвичай комбінуються в один пристрій CSU/DSU, що підключається до ISP (з боку CSU) і до клієнта (з боку DSU). Цей пристрій є фізичним втіленням інтерфейсу «користувач-мережа» між вузлом замовника і ISP.

При з’єднанні маршрутизатора з мережею провайдера через послідовне підключення, необхідно обладнання CSU/DSU, якщо мережа WAN є цифровий. Якщо мережа WAN є аналоговою, то необхідний модем. Ці пристрої перетворять дані, отримані від маршрутизатора, у форму, придатну для передачі по глобальній мережі, і навпаки – перетворюють дані, отримані з глобальної мережі,

у формат, допустимий для маршрутизатора. За замовчуванням, маршрутизатори Cisco є пристроями DTE (data terminal equipment), тобто обладнанням обробки даних. Оскільки час зв'язку з маршрутизатором контролюють пристрої DCE, то тактову частоту від пристрою DCE приймають пристрої DTE.

Для того, щоб змоделювати з'єднання глобальної мережі між маршрутизаторами використовується кабель DTE/DCE, за допомогою якого безпосередньо з'єднуються два маршрутизатори. По замовчуванню маршрутизатори є пристроями DTE, але якщо їх з'єднати між собою, для моделювання глобальної мережі, то послідовний інтерфейс можна визначити як пристрій DCE. Оскільки маршрутизатори Cisco використовують синхронну взаємодію, тобто потрібен годинник, в якості якого використовується зовнішній пристрій, то для конфігурації інтерфейсу необхідно задавати команду **clock rate** при конфігуруванні послідовних портів. Налаштування годинника необхідне тому, що в модельованій мережі немає пристрою CSU/DSU, що використовуються для синхронізації ліній. Для моделювання годинника необхідно виконати команду **clock rate** в режимі конфігурування послідовного інтерфейсу DCE.

Щоб перейти в режим інтерфейсу необхідно в режимі глобальної конфігурації ввести команду **interface *назва інтерфейсу*** (рис. 6.12). Наприклад, для переходу в режим конфігурування послідовного інтерфейсу Serial0/0 необхідно ввести команду:

```
Router(config)#interface fastethernet 0/0      <-- Перехід в режим конфігурування інтерфейсу FastEthernet 0/0
Router(config-if)#description connection to Admin LAN      <-- Опис інтерфейсу FastEthernet 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0      <-- Присвоєння IP адреси інтерфейсу FastEthernet 0/0
Router(config-if)#no shutdown      <-- Ввімкнення інтерфейсу FastEthernet 0/0
Router(config-if)#exit
Router(config)#interface serial 0/0/0      <-- Перехід в режим конфігурування інтерфейсу Serial 0/0/0
Router(config-if)#description connection to Router2      <-- Опис інтерфейсу Serial 0/0/0
Router(config-if)#ip address 192.168.1.125 255.255.255.0      <-- Присвоєння IP адреси інтерфейсу Serial 0/0/0
Router(config-if)#clock rate 64000      <-- Задання частоти синхронізації для пристрою DCE
Router(config-if)#no shutdown      <-- Ввімкнення інтерфейсу Serial 0/0/0
```

Рис. 6.12. Налаштування інтерфейсів маршрутизатора

```
Router#conf t
Router(config)#int s0/0
Router(config-if)#clock rate 56000
```

Присвоєння IP – адреси інтерфейсу проводиться за допомогою команди:

**ip address** *ip адрес_підмережева маска_[secondary].*

Параметр **secondary** дозволяє одному фізичному інтерфейсу присвоїти декілька логічних адрес. Це в свою чергу дозволяє використовувати один порт маршрутизатора для під'єднання декількох мереж.

Оскільки в початковому стані всі інтерфейси маршрутизатора знаходяться у неактивному стані, то для їх активування потрібно виконати команду **no shutdown ,** а для вимкнення – **shutdown .**

```
Router#conf t
Router(config)#int fa0/0
Router(config-if)#ip address 219.17.100.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0 secondary
Router(config-if)#no shutdown
```

### 6.3.4. Завантаження та копіювання файлу конфігурації

Налаштувавши маршрутизатор, потрібно зберегти поточну конфігурацію (running-config) в файлі початкової конфігурації (startup-config). Крім того, корисно зберегти копію файлу конфігурації в іншому місці, наприклад, на віддаленому мережевому сервері. Якщо в пам'яті NVRAM виникне збій або пошкодження і маршрутизатор не зможе завантажити файл конфігурації, то можна буде використовувати іншу копію. Існує багато способів збереження файлу конфігурації.

Одним із способів збереження файлів конфігурації на мережевому сервері є використання TFTP. Для роботи з TFTP сервером потрібно впевнитись, що TFTP налаштований та з ним є зв'язок.

Деякі конфігураційні команди для роботи з TFTP сервером:

**copy tftp running-config** – завантажує файл конфігурації з TFTP сервера в RAM.

```
Router#copy tftp run
Address or name of remote host []? 192.5.5.2
Source filename []? lab_b
Destination filename [running-config]?
```

**copy running-config startup-config** – зберігає поточну конфігурацію з RAM

в NVRAM.

**Router#copy run start**
Destination filename [startup-config]?

**copy running-config tftp** – зберігає поточну конфігурацію з RAM на TFTP сервер.

**Router#copy run tftp**
Address or name of remote host []? 192.5.5.2
Destination filename [running-config]?

**copy startup-config running config** – копіювання файлу, що збережений в NVRAM в RAM.

**Router#copy start run**
Destination filename [running-config]?

**erase startup-config** – знищує вміст NVRAM.

**Router#erase start**
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]

## 6.4. Конфігурування маршрутизації на маршрутизаторах Cisco

### 6.4.1. Налаштування статичної маршрутизації

**Статичні маршрути (static route)** настроюються мережевим адміністратором вручну. Для налаштування статичного маршруту в маршрутизаторах Cisco використовується наступна команда, яку потрібно ввести в режимі глобальної конфігурації (рис. 6.13):

**ip route** *адреса мережі_маска підмережі_вихідний інтерфейс_[відстань]*
або
**ip route** *адреса мережі_маска підмережі_адрес наступного переходу_[відстань]*

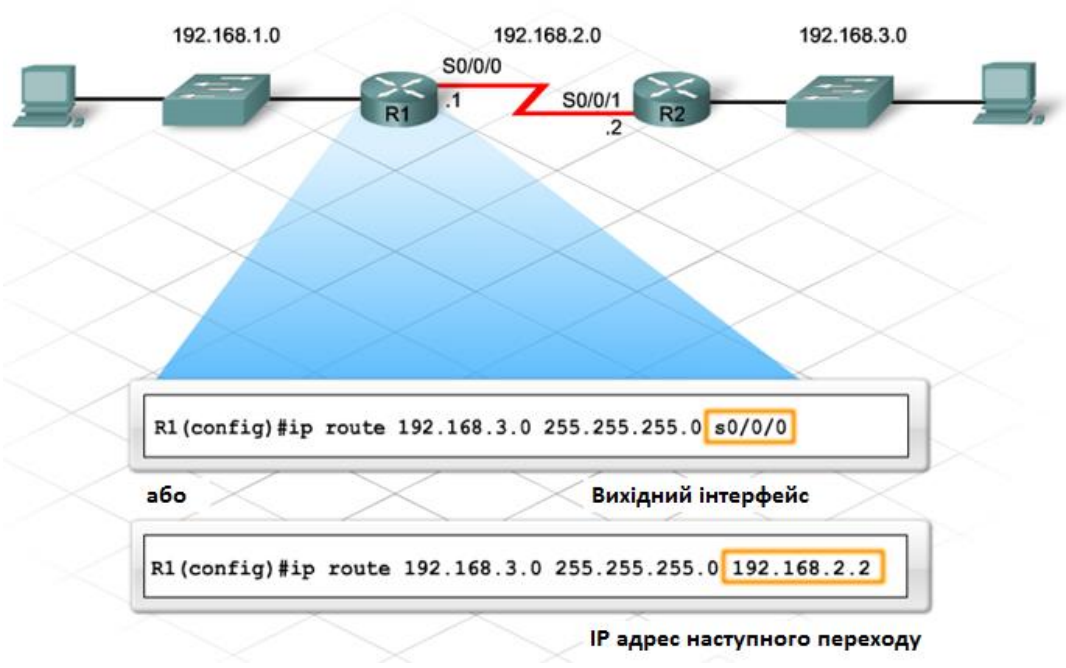



Рис. 6.13. Налаштування статичної маршрутизації

де: адреса мережі – IP адреса мережі або підмережі отримувача;

маска підмережі – маска підмережі отримувача;

вихідний інтерфейс – назва вихідного інтерфейсу, який використовується для доступу в мережу отримувача;

адрес наступного переходу – IP адреса наступного маршрутизатора, який використовується для доступу в мережу отримувача;

відстань – адміністративна відстань.

Згідно рис. 5.13, для встановлення двостороннього зв'язку між мережами 192.168.1.0 та 192.168.3.0, адміністратор також повинен налаштувати статичний маршрут на другому маршрутизаторі (R2):

**R2(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1**

або

**R2(config)#ip route 192.168.1.0 255.255.255.0 S0/0/1**

**Адміністративна відстань (**Administrative Distance**, AD)** відображає рівень довіри або іншими словами оцінку надійності, що присвоюється адміністратором та задається в межах від 0 до 255. Всі протоколи маршрутизації мають адміністративну відстань, що присвоюється по замовчуванню. Чим менше число, тим більша надійність. По замовчуванню рівень довіри в статичній маршрутизації рівний 1, що означає найвищий рівень довіри. Це значення враховується при використанні декількох протоколів маршрутизації на одному маршрутизаторі для вибору оптимального шляху передачі пакету.

При використанні статичної маршрутизації важливо забезпечити всі маршрутизатори інформацією про те, як досягаються різні мережі, оскільки, якщо шлях до отримувача буде невідомим, пакети будуть відкидатися.

Оскільки статичні маршрути настроюються вручну, мережеві адміністратори повинні додавати і видаляти статичні маршрути з урахуванням змін в мережевій топології. У невеликих мережах зі стабільною топологію трудомісткість обслуговування статичних маршрутів невелика. У великій мережі ручне ведення таблиць маршрутизації суттєво підвищує трудомісткість адміністрування, тому динамічні маршрути для них більш доцільні в порівнянні зі статичними.

За допомогою адреси наступного переходу або вихідного інтерфейсу маршрутизатор направляє трафік за потрібною адресою призначення. Однак, ці два параметри діють по-різному.

Перед пересиланням маршрутизатором пакета, процес в таблиці маршрутизації визначає вихідний інтерфейс, який буде для цього використаний. Статичним маршрутам, що налаштовані для роботи з вихідними інтерфейсами, потрібно шукати записи в таблиці маршрутизації лише один раз (рис. 6.14).

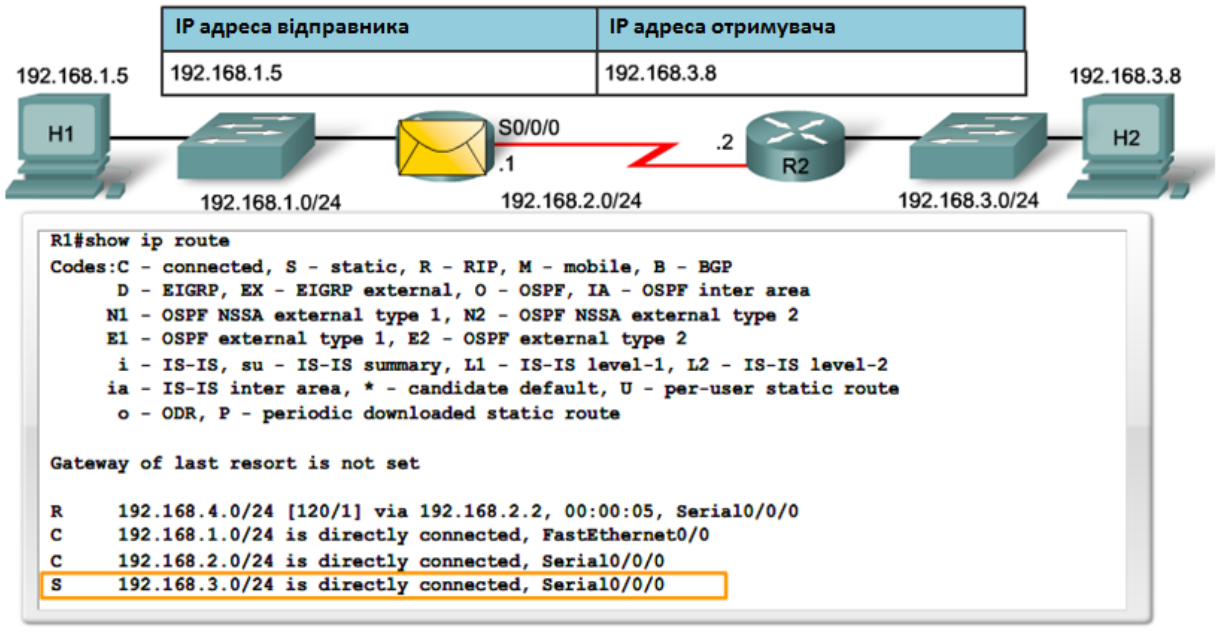



Рис. 6.14. Статичні маршрути, що налаштовані для роботи з вихідними інтерфейсами

У корпоративній мережі статичні маршрути, що налаштовані для роботи з вихідними інтерфейсами, ідеальні для двоточкових з'єднань, наприклад, для з'єднань між прикордонним маршрутизатором і ISP.

Статичним маршрутами, налаштованим для роботи з інтерфейсом

наступного переходу, потрібно два кроки, щоб визначити вихідний інтерфейс (рис. 6.15). Це називається **рекурсивний пошук (recursive lookup)**.

В ході рекурсивного пошуку:

- маршрутизатор зіставляє IP-адресу призначення для пакета зі статичним маршрутом;
- далі він зіставляє IP-адресу наступного переходу статичного маршруту з записами в таблиці маршрутизації, щоб визначити інтерфейс для використання.

Якщо відключений вихідний інтерфейс, статичні маршрути не будуть відображатися в таблиці маршрутизації. Після включення інтерфейсу маршрути будуть в ній переустановлені.

В залежності від топології корпоративних мереж, можна забезпечити резервні канали для статичних маршрутів на випадок відмови основного з'єднання. В цьому випадку, в цілях резервування, використовується функція **плаваючих статичних маршрутів (floating static route)**, яка базується на використанні адміністративної відстані**.**

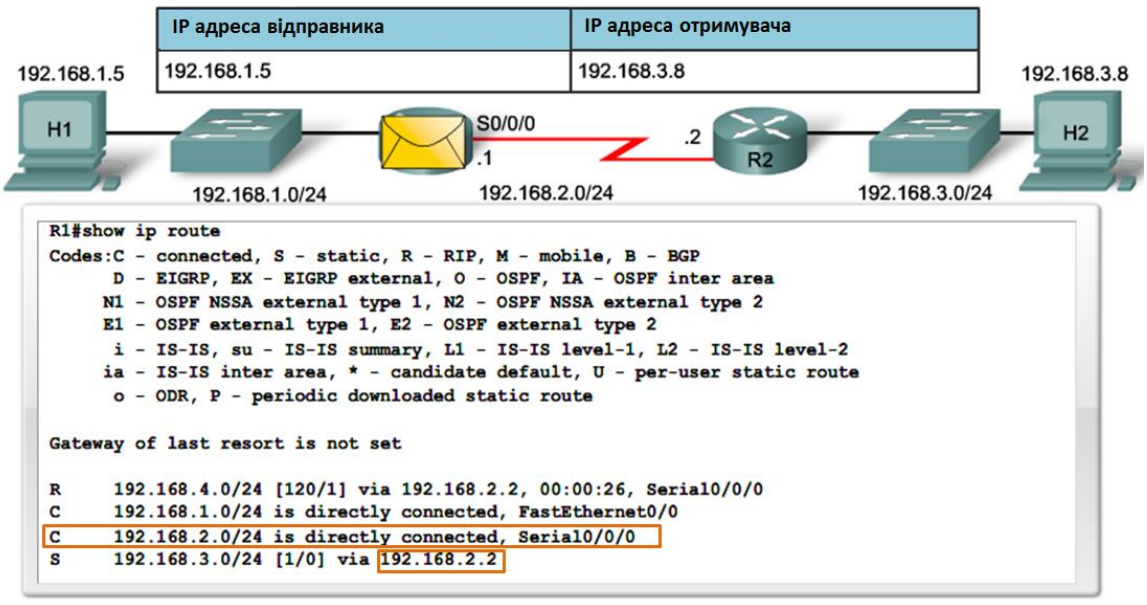



Рис. 6.15. Статичні маршрути, що налаштовані для роботи з інтерфейсом наступного переходу

За замовчуванням адміністративна відстань статичного маршруту менша адміністративної відстані маршруту, отриманого по протоколу динамічної маршрутизації. Адміністративна відстань плаваючого статичного маршруту повинна бути більша адміністративної відстані основного маршруту або маршруту, отриманого по протоколу динамічної маршрутизації. З цієї причини

плаваючий статичний маршрут не відображається в таблиці маршрутизації. Запис плаваючого статичного маршруту буде відображений в таблиці маршрутизації, тільки якщо динамічні відомості втрачені.

Маршрутизатор використовує основний маршрут, поки він активний. Якщо основний маршрут стає неактивним, у таблиці буде встановлено плаваючий статичний маршрут.

Щоб створити плаваючий статичний маршрут, потрібно добавити значення для адміністративної відстані в кінець команди **ip route.**

Нехай, рис. 6.16, доступ з маршрутизатора R1 до мережі 209.165.201.0/27 здійснюється через маршрутизатор R4 по статичному маршруту:

**R1(config)#ip route 209.165.201.0 255.255.255.224 10.20.30.2**


Рис. 6.16. Пакети проходять по основному статичному маршруту

Для створення резервного каналу, на випадок втрати основної лінії зв’язку (наприклад, між маршрутизаторами R1 та R4, необхідно ввести наступну команду в режимі глобальної конфігурації (рис. 6.17):

**R1(config)#ip route 209.165.201.0 255.255.255.224 10.20.10.2 150**

В даному прикладі, для плаваючого статичного маршруту встановлена адміністративна відстань 150, яка менша адміністративної відстані для статичного маршруту (за замовчуванням, рівна 1) і тому, дані будуть проходити по резервному маршруту (через маршрутизатор R3) лише у випадку втрати основного маршруту (через маршрутизатор R4).

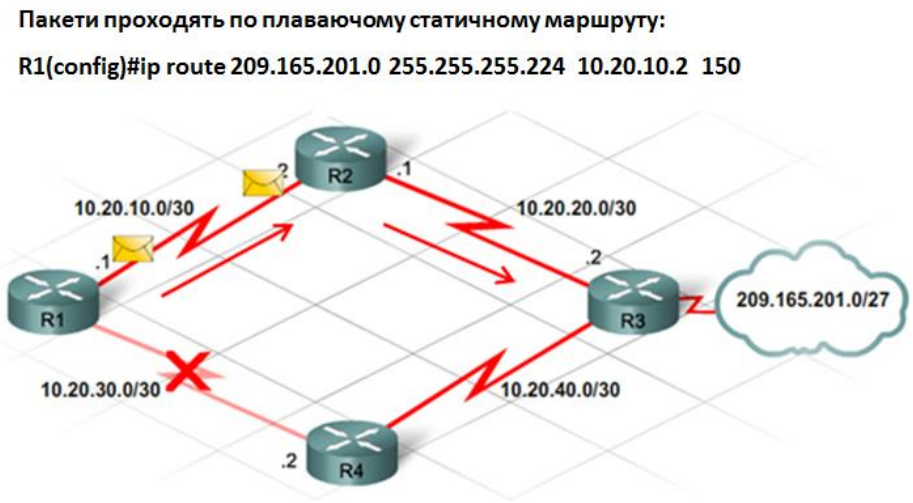
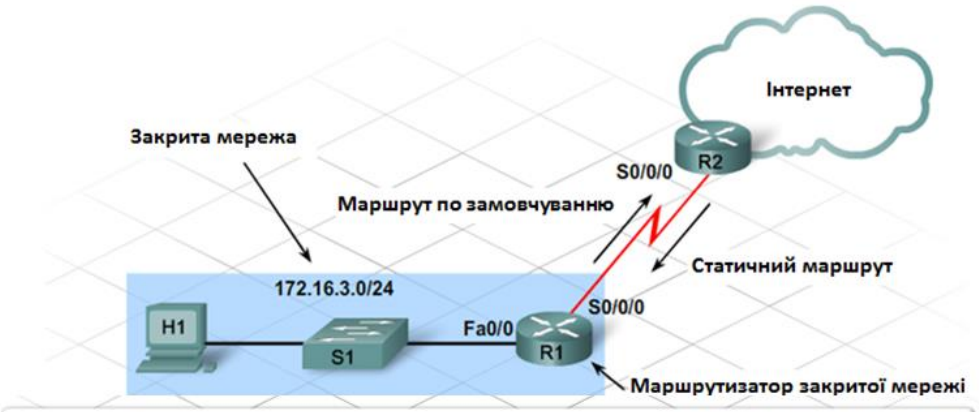



Рис. 6.17. Пакети проходять по плаваючому статичному маршруту

### 6.4.2. Налаштування маршрутизації по замовчуванню




```
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#end

R1#show ip route
<output ommitted>

        Gateway of last resort is 0.0.0.0 to network 0.0.0.0

        172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S       0.0.0.0/0 is directly connected, Serial0/0/0
```

Рис. 6.18. Налаштування маршрутизації по замовчуванню

У таблицях маршрутизації не може бути маршрутів для всіх можливих вузлів мережі Інтернет. У міру зростання розмірів таблиць маршрутизації їм потрібно більше оперативної пам’яті та обчислювальних потужностей.

Спеціальний тип статичного маршруту, званий **маршрутом по замовчуванню (default route)**, вказує адресу **шлюзу (gateway)**, якщо в таблиці маршрутизації немає шляху до адреси призначення. Зазвичай, маршрути за замовчуванням вказують наступний маршрутизатор на шляху до провайдера. У складних корпоративних мережах маршрут за замовчуванням, розташований на прикордонному маршрутизаторі, відправляє трафік до ISP. Цей маршрут позначає останню зупинку в корпоративній мережі як **шлюз останньої інстанції (Gateway of Last Resort)** для пакетів, які не вдається співставити. Ці відомості відображаються в таблицях маршрутизації всіх маршрутизаторів.

Команда для створення маршруту за замовчуванням схожа з командою для створення звичайного або плаваючого статичного маршруту. Мережева адреса і маска підмережі позначаються як **0.0.0.0**, в результаті чого виходить маршрут **чотирьох нулів (quad zero route)**. У команді використовується або адреса наступного переходу, або параметри вихідного інтерфейсу (рис. 6.18).

Нулі вказують маршрутизатору, що для використання цього маршруту біти збігатися не повинні. Якщо не існує більш оптимального збігу, маршрутизатор буде використовувати статичний маршрут за замовчуванням.

Якщо в корпоративній мережі використовується протокол динамічної маршрутизації, прикордонний маршрутизатор може відправляти маршрут за замовчуванням іншим маршрутизаторам у формі поновлення динамічних маршрутів.

### 6.4.3. Налаштування динамічної маршрутизації

#### 6.4.3.1. Налаштування протоколів внутрішньої маршрутизації

RIP (Routing Information Protocol) – поширений протокол на основі вектору відстані, який підтримується більшістю маршрутизаторів. Він найбільш доцільний для невеликих мереж з декількома маршрутизаторами.

На рисунку 5.19 зображено топологію мережі із трьох маршрутизаторів. Перед виконанням налаштування протоколу RIP необхідно вивчити склад мереж, які буде обслуговувати маршрутизатор, і інтерфейсів маршрутизатора, що підключаються до цих мереж.

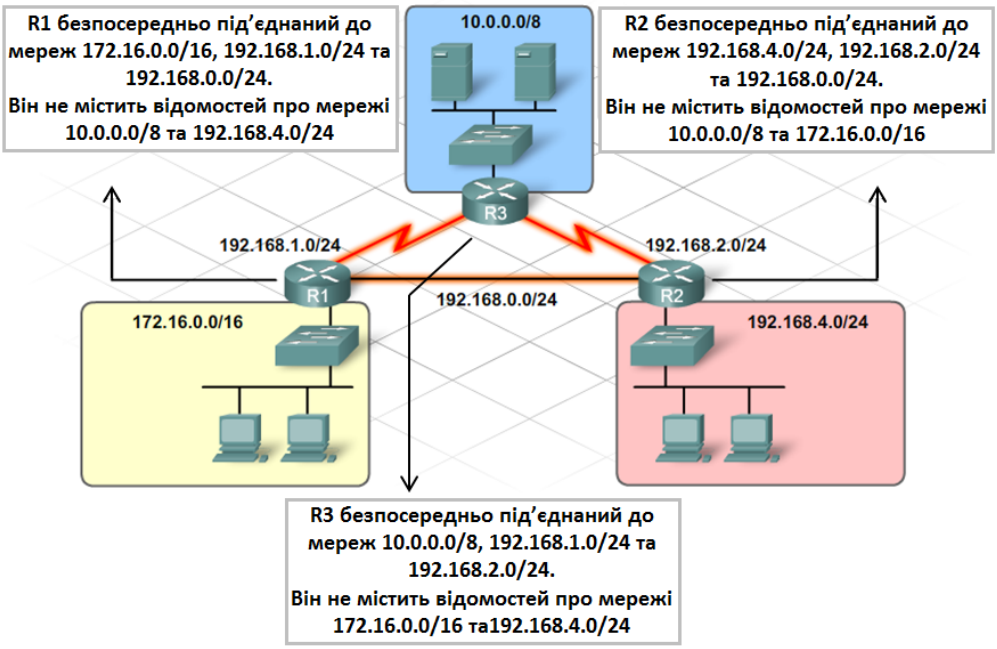



Рис. 6.19. Топології мережі із трьох маршрутизаторів

Кожен з маршрутизаторів обслуговує окрему приватну локальну мережу, таким чином, є три локальні мережі. Оскільки маршрутизатори також з'єднані між собою окремими мережами, то загальне число мереж рівне шести.

У даній топології маршрутизатор R1 має три **безпосередньо під'єднаних (directly connected)** мережі (172.16.0.0/16, 192.168.0.0/24 та і 192.168.1.0/24), маршрутизація між якими здійснюється автоматично. Для маршрутизатора R1 мережі 10.0.0.0/8 і 192.168.4.0/24 будуть доступні після налаштування протоколу динамічної маршрутизації RIP. Після налаштування протоколу RIP маршрутизатори R2 та R3 відправляють оновлення таблиці маршрутизації, які будуть містити відомості про доступність мереж 10.0.0.0/8 та 192.168.4.0/24 для маршрутизатора R1.

На наступному кроці, перед налаштуванням протоколу RIP, необхідно присвоїти IP-адреси та активувати всі фізичні інтерфейси, які братимуть участь в маршрутизації.

Для маршрутизатора R1 необхідно налаштувати три інтерфейси. Serial 0/0/0 під'єднаний до маршрутизатора R3, FastEthernet 0/0 – до маршрутизатора R2, а FastEthernet 0/1 – до локальної мережі 172.16.0.0/16 (рис. 6.20):

```
R1#configure terminal
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.2 255.255.255.0
```

**R1(config-if)#no shutdown**
**R1(config-if)# interface fastethernet 0/0**
**R1(config-if)#ip address 192.168.0.1 255.255.255.0**
**R1(config-if)#no shutdown**
**R1(config-if)# interface fastethernet 0/0**
**R1(config-if)#ip address 172.16.254.254 255.255.255.0**
**R1(config-if)#no shutdown**

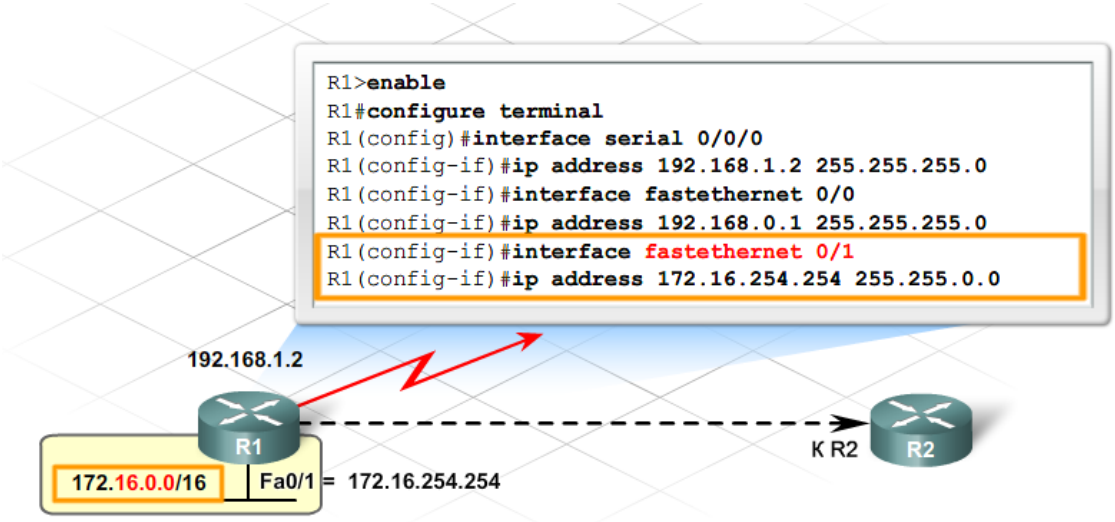



Рис. 6.20. Налаштування інтерфейсів маршрутизатора R1

Для налаштування протоколу RIP на маршрутизаторі необхідно ввести в режимі глобальної конфігурації команду **router rip**. Після введення даної команди, маршрутизатор перейде в режим конфігурування протоколу маршрутизації RIP. Далі потрібно описати всі безпосередньо приєднані мережі за допомогою команди **network**.

Для налаштування RIPv2 після виконання команди **router rip**, в режимі конфігурування протоколу маршрутизації RIP, потрібно ввести команду **version 2** – для задання 2 версії протоколу RIP (RIPv2), а потім потрібно описати всі безпосередньо приєднані мережі за допомогою команди **network** (рис. 6.21):

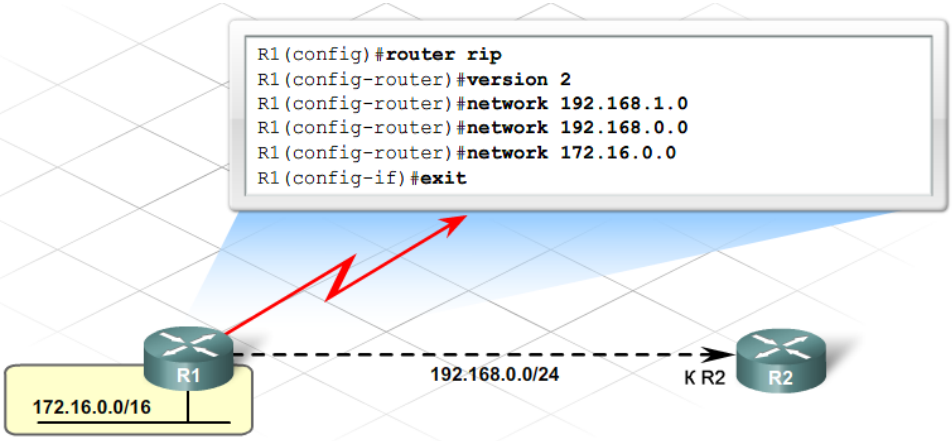



Рис. 6.21. Налаштування протоколу RIPv2 на маршрутизаторі R1

**R1(configf)#router rip**
**R1(config-router)#version 2**
**R1(config-router)#network 192.168.1.0**
**R1(config-router)#network 192.168.0.0**
**R1(config-router)#network 172.16.0.0**

На рис. 6.22 показано налаштування протоколу RIP на маршрутизаторах R2 та R3.

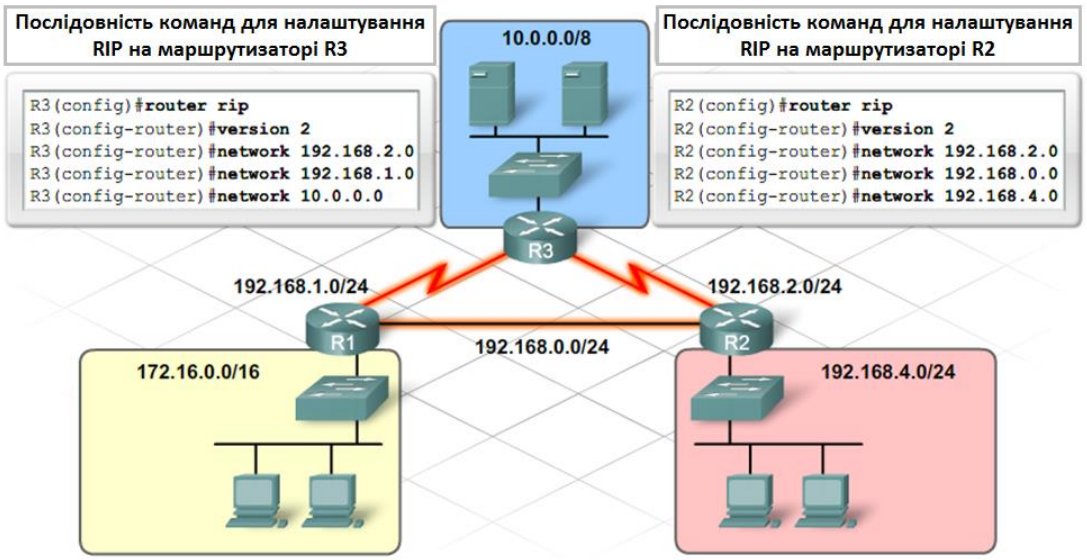



Рис. 6.22. Налаштування протоколу RIPv2 на маршрутизаторах R2 та R3

Протокол RIP – це протокол класової маршрутизації, він завжди працює з узагальненою інформацією про маршрути (не використовує інформацію про

підмережі). На відміну від протоколів класової маршрутизації, в протоколах безкласової маршрутизації інформація про шляхи містить дані про мережі та підмережі, тобто при розсиланні оновлень таблиць маршрутизації розсилається також інформація про маску.

Протокол RIP має значення адміністративної відстані рівне 120.

Перевірити функціонування RIP в мережі можна кількома способами. Якщо конфігурація правильна, то для перевірки працездатності маршрутизації можна відправити ехо-запити командою **ping** на пристрої у віддалених мережах. Успішне виконання команди **ping** буде свідченням працездатності маршрутизації.

Іншим методом перевірки маршрутизації IP є використання команд **show ip protocols** і **show ip route**.

Команда **show ip protocols** призначена для перевірки конфігурації маршрутизації RIP, правильності налаштувань інтерфейсів, які повинні відправляти і отримувати оновлення RIP, а також перевірки мереж, в які відбувається відправка оновлення.

Команда **show ip route** виводить таблицю маршрутизації, за якою можна перевірити присутність маршрутів, отриманих сусідніми маршрутизаторами.

Команда **debug ip rip** дозволяє простежити за повідомленнями про конкретні мережі в оновленнях маршрутів (рис. 6.23). Налагоджувальні повідомлення відображають роботу маршрутизатора в реальному часі. Оскільки налагоджувальний режим створює навантаження на процесорні ресурси і може вплинути на роботу маршрутизатора, його слід використовувати з обережністю.

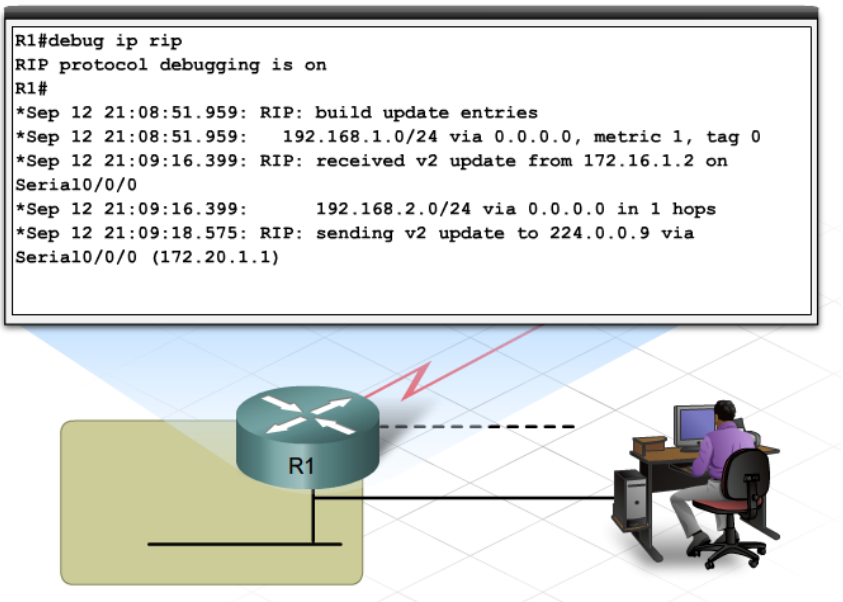



Рис. 6.23. Використання команди **debug ip rip**

### 6.4.3.2. Налаштування протоколів зовнішньої маршрутизації

Протоколи зовнішньої маршрутизації призначені для обміну інформацією між різними автономними системами. Оскільки різні автономні системи знаходяться в компетенції різних адміністраторів і можуть використовувати різні внутрішні протоколи, то протокол, який застосовується на мережевому рівні, повинен забезпечувати взаємодію різнорідних систем. BGP відповідає за перетворення інформації про зовнішні маршрути, роблячи можливою її успішну обробку в кожній мережі автономної системи.

Коли провайдер розміщує маршрутизатор на стороні клієнта, в якості маршруту, зазвичай, налаштовується статична маршрутизація. Однак, іноді провайдеру потрібно включити маршрутизатор в свою автономну систему і зробити його учасником BGP. У цьому випадку необхідно налаштувати маршрутизатор в приміщенні клієнта, ввівши необхідні команди для активації BGP.

Перший крок в активації BGP на маршрутизаторі полягає в налаштуванні номера автономної системи (рис. 6.24). Це робиться в режимі глобальної конфігурації за допомогою наступної команди:

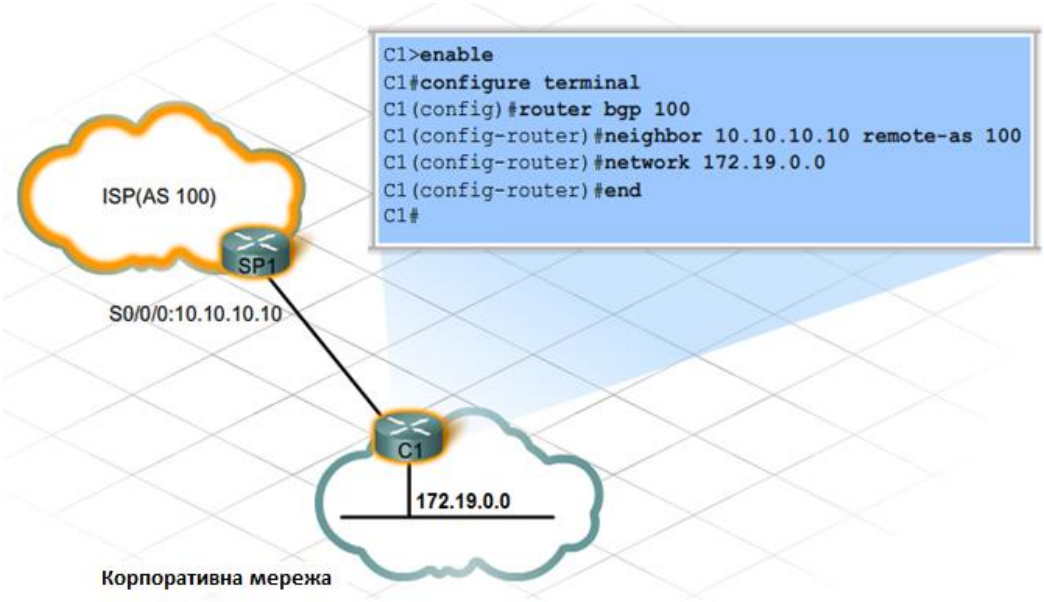



Рис. 5.24. Налаштування протоколу BGP

**router bgp [**номер автономної системи]

Наступний крок – ідентифікація маршрутизатора провайдера, який буде виступати сусіднім вузлом BGP для обміну інформацією з маршрутизатором в приміщенні клієнта (CPE – customer premises equipment). Сусідній

маршрутизатор ідентифікується наступною командою:

**neighbor [**IP адреса] **remote-as** [номер автономної системи]

Клієнтам провайдера, які мають власні зареєстровані блоки IP-адрес, може бути необхідна можливість оголошення маршрутів до своїх внутрішніх мереж в Інтернеті. Для оголошення внутрішніх маршрутів допомогою BGP необхідно задати адресу мережі. Формат команди, яка дозволяє зробити це:

**network** [адреса мережі]

Для BGP зазвичай використовуються зареєстровані IP-адреси, які можуть використовуватися в маршрутизації і однозначно ідентифікувати організацію. У дуже великих організаціях для процесів BGP можуть застосовуватися приватні адреси, як показано на рисунку. В Інтернеті забороняється застосовувати BGP для оголошення адрес приватних мереж.

## 6.5. Технології уникнення петель маршрутизації

### 6.5.1. Утворення петель маршрутизації

Важливо, щоб при зміні топології мережі оновлення в таблиці маршрутизації відбувалися як найшвидше. Але в великих мережах це є проблемою. В мережах, що використовують дистанційно-векторну (distance-vector) маршрутизацію, таблиці маршрутизації можуть оновлюватись як періодично, так і при зміні топології мережі. Кожен маршрутизатор отримує таблицю маршрутизації від сусіднього, збільшує вектор, додає власну інформацію та пересилає далі.

Після включення маршрутизатора, що використовує дистанційно-векторну маршрутизацію, він отримує інформацію про сусідів. Це означає, що він знає відстань (число маршрутизаторів) до інших маршрутизаторів. Після оновлення таблиці маршрутизації, маршрутизатор отримує інформацію про оптимальні шляхи до інших мереж. Інтервал оновлення залежить від протоколу маршрутизації. Шляхи визначаються на основі числа транзитних ділянок між маршрутизатором та кожним з його сусідів. Проте, дистанційно-векторна маршрутизація не дозволяє маршрутизатору знати точну топологію мережі.

При використанні періодичних повідомлень про оновлення таблиць, справжньою проблемою є збіжність мережі. Період збіжності це час, потрібний для того, щоб всі маршрутизатори оновили свої таблиці маршрутизації після зміни конфігурації, обриву лінії або інших змін в мережі. В цей період часу, передача даних ускладнюється та продуктивність мережі в цілому спадає. Тому, в великих мережах, де відбувається багато подій, дистанційно-векторна маршрутизація може працювати незадовільно. Повільний час збіжності може спричиняти поширення через мережу недостовірної інформації та виникнення **петель маршрутизації (Routing loops)**. Приклад виникнення петель показано на рис. 6.25.

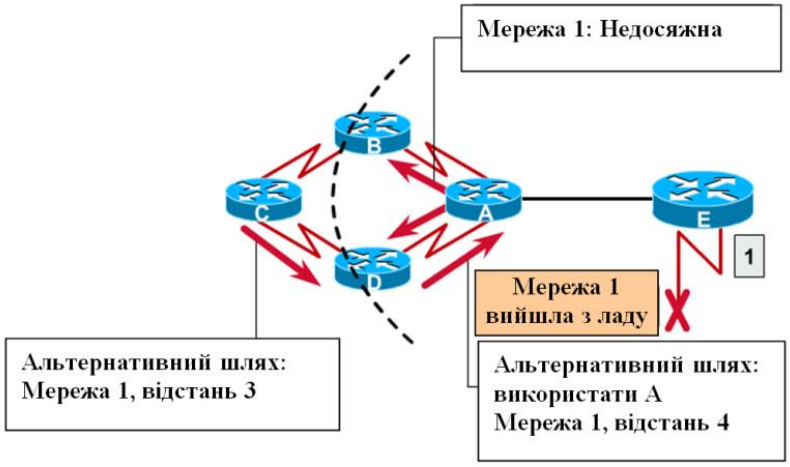



Рис. 6.25. Петлі маршрутизації

1. Перед втратою зв’язку з мережею 1 всі маршрутизатори мали вірну інформацію про маршрутизацію. Мережа є збіжною. Припустимо, що маршрутизатор C використовує шлях через маршрутизатор B для надсилання пакетів в мережу 1. Відстань від маршрутизатора C до мережі 1 рівна трьом переходам.
2. Коли мережа 1 виходить з ладу, то маршрутизатор E посилає повідомлення про оновлення маршрутів маршрутизатору A. Після його отримання маршрутизатор A припиняє відправку пакетів в мережу 1, однак маршрутизатори B, C і D продовжують, оскільки вони ще не інформовані про збій в мережі 1. Коли маршрутизатор A відправляє своє повідомлення про оновлення, маршрутизатори B і D припиняють відправку пакетів в мережу 1. Однак в цей момент маршрутизатор C ще не отримав повідомлення про поновлення. Для нього мережа 1 і надалі вважається досяжною через маршрутизатор B.
3. Тепер маршрутизатор C відправляє періодичні оновлення маршрутів маршрутизатору D, вказуючи маршрут до мережі 1 через маршрутизатор

B. Маршрутизатор D змінює в таблиці маршрутизації стан мережі 1 на досяжний, що є невірно, та поширює цю інформацію до маршрутизатора A. Маршрутизатор A відправляє цю ж інформацію маршрутизаторам B і E, і т. д. Тепер будь-який пакет, що призначений для мережі 1, переміщається по кільцевому маршруту (петлі) від маршрутизатора C до маршрутизатора B, далі до A і D і знову до маршрутизатора C.

### 6.5.2. Проблема підрахунку до нескінченості

Невірні оновлення про стан мережі 1 будуть циркулювати по мережі до тих пір, поки будь-який процес не обірве розсилання. При такому стані мережі, що називається зацикленням (counting to infinity – підрахунком до нескінченості), пакети продовжують безперервно переміщатись по мережі, не зважаючи на те, що мережа-отримувач 1 вийшла з ладу. До тих пір, поки маршрутизатори збільшують кількість переходів, потенційно до нескінченості, невірна інформація, що передається в мережі, буде спричиняти існування петлі (рис. 6.26).

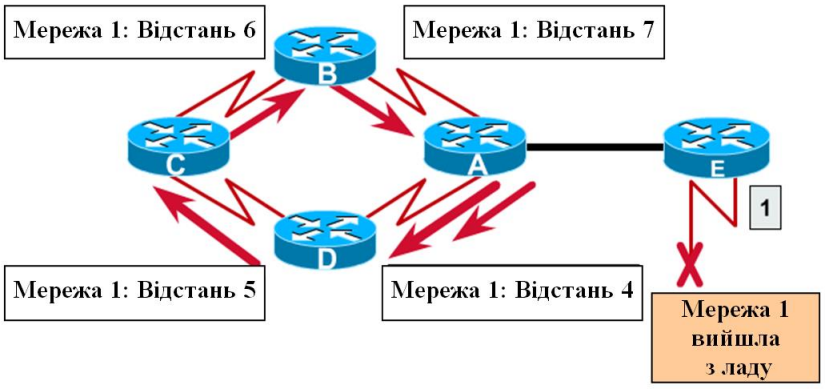



Рис. 6.26. Зациклення

Без засобів протидії цьому, протоколи дистанційно-векторної маршрутизації будуть збільшувати метрику (hop count) на одиницю, кожен раз, коли пакет проходитиме через маршрутизатор.

Одним із методів запобігання цьому є **обмеження верхнього числа маршрутних ділянок (defining a maximum)**, які може пройти пакет. Для запобігання петлям, кожен протокол дистанційно-векторної маршрутизації вважає нескінченість специфічним максимальним числом. Це число, зазвичай

називають **метрикою маршрутизації (routing metric)**. В простих випадках метрика може бути довжиною маршруту (hop count).

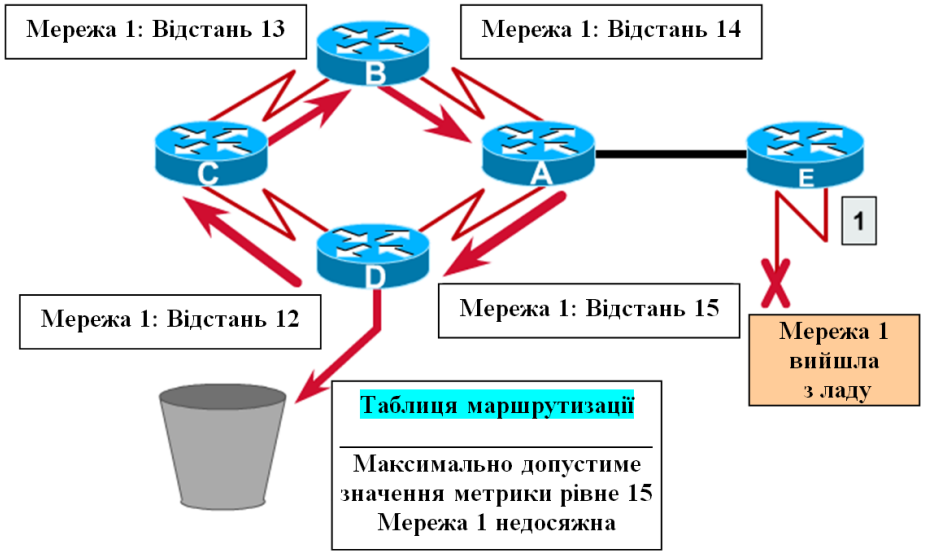



Рис. 6.27. Задання максимального значення метрики

При заміні нескінченності деяким максимальним числом, протокол маршрутизації дозволяє існувати петлі маршрутизації до тих пір, поки метрика не перевищить максимальне допустиме число. Для прикладу, максимальним допустими числом для метрики протоколу RIP є 15. Іншими словами, після того як цикл розростеться до 15 маршрутних ділянок, пакет буде відкидатися маршрутизаторами (рис. 6.27).

Під час виникнення петлі, IP-пакети, які не є повідомленнями протоколів маршрутизації будуть пересилатись від одного маршрутизатора до іншого по кільцю. В протоколі IP існує свій власний механізм запобіганню нескінченній циркуляції пакетів по кільцю – поле TTL (Time-To-Live – час життя пакету). Перед тим як IP-пакет буде переданий вузлом, в це поле, згідно стандарту, може бути встановлено значення між 1 і 255. Це значення не залежить від типу операційної системи і стандартно програмними засобами заноситься число між 32 і 128. Коли такий пакет поступає в маршрутизатор, пристрій зменшує значення в полі (часто його називають просто лічильником TTL) на одиницю. Коли значення TTL досягне нуля, маршрутизатори повинні відкинути такий пакет і переслати відправнику відповідне інформаційне ICMP-повідомлення.

### 6.5.3. Уникнення петель маршрутизації за допомогою розщеплення горизонту

Правило **розщеплення горизонту (split horizon)** не дозволяє маршрутизатору отримувати неправдиву інформацію маршрутизації, що протиречить правильній, яку він попередньо розповсюдив (рис. 6.28).

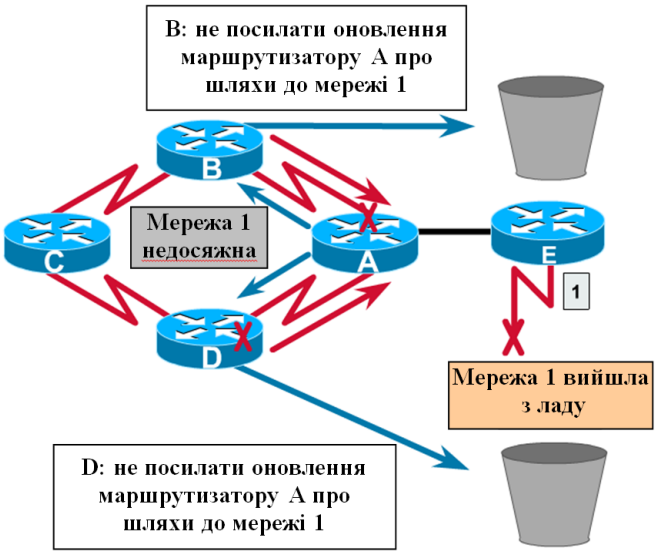



Рис. 5.28. Розщеплення горизонту

1. Маршрутизатор A передає оновлення до маршрутизаторів B і D, повідомляючи, що мережа 1 вийшла з ладу.
2. Маршрутизатор C передає оновлення до маршрутизатора B, повідомляючи, що мережа 1 доступна через маршрутизатор D, з відстанню 4.
3. Маршрутизатор B невірно визначив, що маршрутизатор C має достовірну інформацію про мережу 1, хоча і з гіршою (більшою) метрикою. Маршрутизатор B надсилає оновлення до маршрутизатора A, повідомляючи про новий шлях до мережі 1.
4. Маршрутизатору A тепер відомо, що він може посилати пакети до мережі 1 через маршрутизатор B, який надсилає пакети через маршрутизатори C та D. Будь – який пакет, що передається в такому середовищі буде зациклено між маршрутизаторами.
5. Правило розщеплення горизонту дозволяє запобігти цьому. Згідно цього правила інформація про маршрутизацію не повинна передаватися в тому напрямку звідки вона надійшла. В нашому прикладі маршрутизатори B і D не повинні посилати оновлення про стан мережі 1 назад до

маршрутизатора А. Це правило дозволяє знизити об'єм передачі застарілих даних та загальний об'єм передачі даних про дистанційно-векторну маршрутизацію в мережах.

Правило розщеплення горизонту дозволяє запобігти цьому. Згідно цього правила інформація про маршрутизацію не повинна передаватися в тому напрямку звідки вона надійшла. В нашому прикладі маршрутизатори B і D не повинні посилати оновлення про стан мережі 1 назад до маршрутизатора А. Це правило дозволяє знизити об'єм передачі застарілих даних та загальний об'єм передачі даних про дистанційно-векторну маршрутизацію в мережах.

Розділення горизонту задається в режимі конфігурування інтерфейсу командою **ip split-horizon**. Команду активізовано по замовчуванню. Для відключення механізму використовується команда:

```
Router(config-if)#no ip split-horizon
```

### 6.5.4. Уникнення петель маршрутизації за допомогою таймерів утримання інформації

Для запобігання поширенню невірної інформації при частій зміні маршрутів в мережі використовують також **таймерів блокувань (holddown timer)**. Правильна послідовність дій при цьому описана нижче (рис. 6.29):

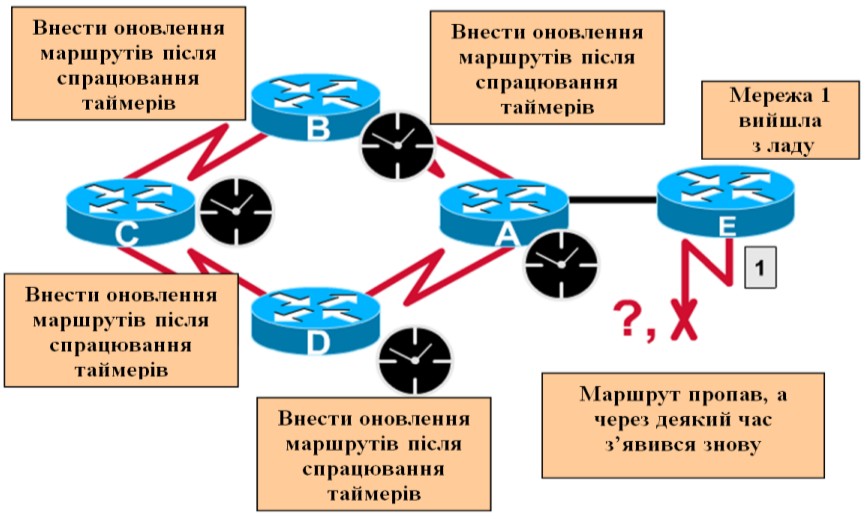



Рис. 6.29. Таймери блокувань

1. Коли маршрутизатор отримує оновлення від сусіднього пристрою, який повідомляє про недоступність мережі, що донедавна була доступною, маршрутизатор позначає шлях до неї як недоступний (inaccessible) і запускає таймер блокувань.

2. Якщо до закінчення часу таймера блокувань від того ж сусіда поступить нове повідомлення-оновлення, з інформацією, що задана мережа знову доступна, то маршрутизатор позначає мережу як доступну і знімає таймер блокувань.
3. Якщо ж нове оновлення надійде від іншого сусіднього маршрутизатора, і вказана в ньому метрика краща від початково зареєстрованої для даної мережі, то маршрутизатор позначає мережу як доступну і знімає таймер блокувань.

Якщо від іншого маршрутизатора надійде оновлення з гіршою метрикою для даної мережі, то воно ігнорується. В такій ситуації, ігнорування повідомлень про оновлення надає більше часу для розповсюдження по всій мережі інформації про зміни в топології мережі.

Для зміни періоду таймера блокувань в RIP використовується команда **timers basic** *update invalid holddown flush*. В даній команді, окрім таймера блокувань задаються також значення наступних таймерів (в секундах):

- Таймер оновлення даних маршрутизації (**update**). Відраховує інтервал між оновленнями інформації про маршрутизацію (для RIP по замовчуванню 30 с). По завершенні цього часу маршрутизатор надсилає всім сусідам повну копію своєї таблиці маршрутизації.
- Таймер застарілого маршруту (**invalid**). Задає інтервал часу (по замовчуванню 180 с), по завершенні якого маршрутизатор помічає маршрут як недійсний. Це використовується в тих випадках, якщо за вказаний проміжок часу маршрутизатор не отримав ніяких даних про оновлення конкретного маршруту. Якщо, по закінченню 31 секунди не отримано ніякої інформації про маршрут, що знаходиться в таблиці маршрутизації, маршрутизатор визначає шлях як недійсний. В період часу від 30 до 180 секунд маршрутизатор не приймає оновлень про заданий шлях з гіршою метрикою в порівнянні з тією, яка відповідала цьому шляху, але розсилає оновлення про цю мережу сусідам. Якщо в цей період часу прийде оновлення про шлях з кращою метрикою або рівноцінною тій, що була на початку, то маршрутизатор оновить запис в таблиці маршрутизації та перезапустить таймер.
- Таймер блокувань (**holddown**). По замовчуванню рівний таймеру застарілого маршруту (180 с). Це дозволяє знизити час збіжності мережі. В стані holddown шлях утримується в таблиці маршрутизації, але оновлення про цей шлях сусідам не розсилаються. В такому стані приймається оновлення з будь-якою метрикою про цей шлях.
- Таймер видалення маршруту (**flush**). Задає інтервал часу (240 с) після

якого маршрут видаляється з таблиці маршрутизації. Перед видаленням маршруту про це повідомляється сусідам.

Інформацію про протокол, що також включає інформацію про таймери, можна переглянути командою **sh ip protocols .**

```
Router>sh ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 4 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version
   Interface       Send  Recv   Key-chain
   Ethernet0       1     1 2
   Serial0         1     1 2
   Serial1         1     1 2
  Routing for Networks:
   199.6.13.0
   201.100.11.0
   219.17.100.0
  Routing Information Sources:
   Gateway         Distance      Last Update
   201.100.11.1         120      00:00:23
   199.6.13.2           120      00:00:15
  Distance: (default is 120)
```

Для зміни таймерів використовується команда **timers basic .**

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#timers basic ?
  <0-4294967295>  Interval between updates

Router(config-router)#timers basic 20 ?
  <1-4294967295>  Invalid
```

**Router(config-router)#timers basic 20 60 ?**

<0-4294967295> Holddown

**Router(config-router)#timers basic 20 60 60 ?**

<1-4294967295> Flush

**Router(config-router)#timers basic 20 60 60 120**

Lab_B(config-router)#^Z

**Lab_B#sh ip prot**

**Routing Protocol is "rip"**

**Sending updates every 20 seconds, next due in 12 seconds**

**Invalid after 60 seconds, hold down 60, flushed after 120**

Outgoing update filter list for all interfaces is

Incoming update filter list for all interfaces is

Redistributing: rip

Default version control: send version 1, receive any version

| Interface | Send | Recv | Key-chain |
|---|---|---|---|
| Ethernet0 | 1 | 1 2 | |
| Serial0 | 1 | 1 2 | |
| Serial1 | 1 | 1 2 | |

……

# 7. Технологія MPLS

## 7.1. Базові принципи і механізми MPLS

### 7.1.1. Суміщення комутації і маршрутизації

У середині 90-х років цілком придатною вважалася багаторівнева структура, в якій на мережевому рівні використовувався протокол IP, на канальному – технології ATM і Frame Relay, а на фізичному рівні – SDH/PDH або DWDM. Застосування такої архітектури, та ще й з двома рівнями передавання пакетів (на канальному з використанням віртуальних каналів і на мережевому, в основному, датаграмним способом) робило глобальну мережу дуже складною і дорогою. Проте вважалося, що ці недоліки є несуттєвими, оскільки перевагами були передавання мультимедійного трафіку та забезпечення необхідної **якості обслуговування** (Quality of Service, **QoS**).

За даними операторів мереж, до 90% інформації, що пересилається в мережах Frame Relay і ATM, становить IP-трафік. Таким чином, абсолютно логічною виглядає ідея об'єднати в одній технології ті переваги, що дає протокол IP, одночасно надаючи гарантію якості і надійність протоколів ATM і Frame Relay.

Проблема передачі короткочасних IP-потоків полягає в тому, що для них немає сенсу створювати постійний віртуальний канал (PVC), так як потік даних між двома конкретними абонентами існує лише короткий час, і створений віртуальний канал переважну частину часу використовується провайдером не за призначенням. Аналогом такої ситуації може бути телефонна мережа, в якій для кожного абонента створено постійне з'єднання з усіма його можливими співрозмовниками. Здавалося б, саме для таких ситуацій в технології ATM були передбачені комутовані віртуальні канали (SVC). Однак в разі, коли час встановлення з'єднання SVC рівний або навіть перевершує час передачі даних, ефективність комутованих віртуальних каналів також виявляється невисокою. Це дуже нагадує ситуацію, коли для того, щоб поговорити 5 хвилин по телефону, потрібно було б щоразу витрачати 5 хвилин на дозвон до потрібного абонента. А в ATM-комутаторах часто спостерігалася саме така ситуація, так як час пульсації комп'ютерного трафіку було співрозмірним з часом встановлення з'єднання SVC.

Для вирішення проблеми компанія Ipsilon запропонувала вбудувати в усі ATM-комутатори блоки IP, які підтримували протокол IP для просування пакетів на основі IP-адрес, і протоколи маршрутизації стека TCP/IP для автоматичної

побудови таблиць маршрутизації. По суті, до АТМ-комутатора був доданий IP-маршрутизатор.

Передача IP-пакета по мережі здійснювалася Ipsilon наступним чином. Пакет надходив від вузла-відправника на комбінований пристрій IP/ATM, який розбивав цей пакет на АТМ-комірки. Кожна комірка короткочасного IP-потоку потім інкапсульовувалась в новий IP-пакет, який передавався від одного пристрою IP/ATM до іншого, і вкінці до отримувача по маршруту, який визначався звичайними таблицями IP-маршрутизації, що зберігалися в цих пристроях.

При цьому стандартне для технології АТМ віртуальне з'єднання між пристроями обмінюватися IP/ATM не встановлювалось, а передача короткочасних IP-потоків істотно прискорювалася за рахунок виключення часу встановлення з'єднання SVC. Довготривалі потоки передавалися пристроями IP/ATM традиційним для АТМ способом – за допомогою віртуальних каналів PVC або SVC. Так як топологія мережі є однаковою як для протоколів IP, так і для протоколів АТМ, з'явилася можливість використовувати один протокол маршрутизації для обох частин комбінованого пристрою.

Компанія Ipsilon розробила власні протоколи, що відповідали за розпізнавання тривалості потоків даних і встановлення віртуальних каналів для довготривалих потоків. Ці протоколи були оформлені у вигляді проектів стандартів Інтернету, але стандартами Інтернету не стали.

Технологія IP-комутації була відразу помічена операторами зв'язку і стала досить популярною. Ініціативу Ipsilon розвинула компанії Cisco, створивши власну технологію **комутації тегів** (tag switching), яка стала значним кроком вперед на шляху об'єднання протоколів IP з технікою віртуальних з'єднань, проте вона, так само як і IP-комутація, не стала стандартною технологією.

На базі цих фірмових технологій робоча група IETF, що складається з фахівців різних компаній, створила в кінці 90-х років технологію **багатопротокольної комутації по мітках** (Multiprotocol Label Switching, **MPLS**).

У MPLS був збережений головний принцип технологій-попередниць.

Технологія MPLS об'єднує в одному комунікаційному пристрої два методи просування пакетів – датаграмний метод і метод комутації віртуальних каналів.

Датаграмне просування реалізується протоколом IP – він працює точно так само, як і в традиційному IP-маршрутизаторі, при цьому таблиця маршрутизації може створюватись як вручну, так і протоколами маршрутизації стеку TCP/IP. Також, в цьому комбінованому комунікаційному пристрої, званому **маршрутизатором з комутацією по мітках** (Label Switch Router, **LSR**), є другий

модуль просування, що працює згідно техніки комутації віртуальних каналів, який називається модулем **комутації по мітках**.

Принцип об'єднання протоколів різних технологій ілюструють рис. 7.1 і 7.2. На першому з них показана спрощена архітектура стандартного IP-маршрутизатора, на другому – архітектура пристрою LSR.

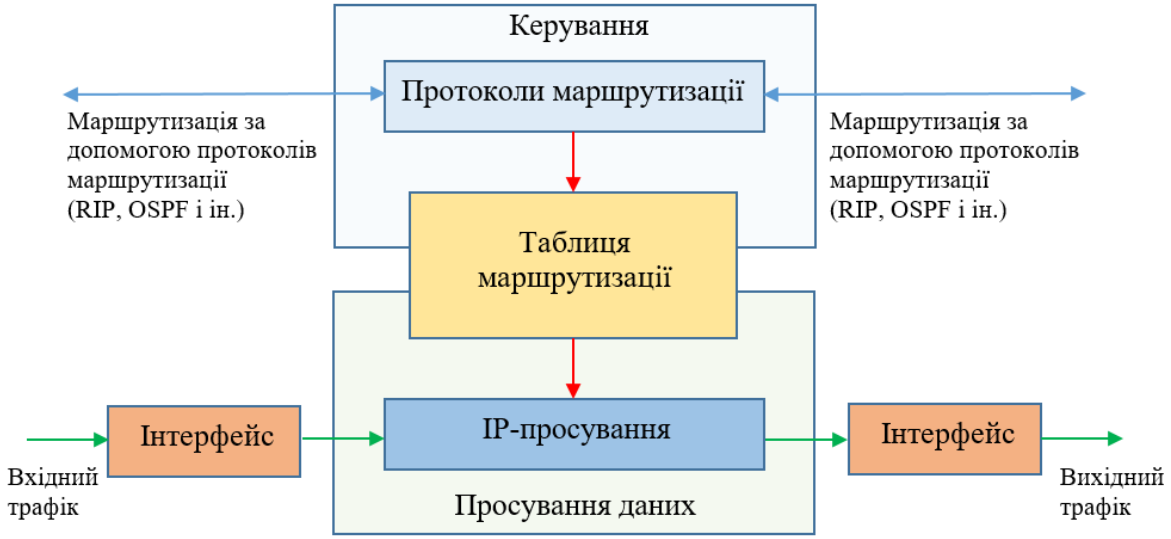



Рис. 7.1. Архітектура IP-маршрутизатора

Обидва модуля просування керуються одним і тим же шаром керування LSR, куди поряд з традиційними протоколами IP-маршрутизації, такими як RIP, OSPF, IS-IS і BGP, входять і нові протоколи, звані сигнальними. **Сигнальні протоколи** потрібні для автоматичного встановлення в мережі віртуального шляху, який називають в технології MPLS **шляхом комутації по мітках** (Label Switching Path, **LSP**). Спільний шар керування дозволяє LSR гнучко використовувати наявність двох модулів просування – одну частину потоків даних він може просувати, застосовуючи техніку IP-просування, а іншу – техніку комутації по мітках. Шар керування має інформацію про топології мережі, необхідну для роботи кожного рівня просування.

Які саме потоки потрібно просувати, тим або іншим методом вирішує адміністратором LSR, який конфігурує його відповідним чином. В залежності від параметрів конфігурації, IP/MPLS-маршрутизатор виконує *відображення* вхідних потоків пакетів на модуль IP-просування або на модуль комутації по мітках. Потік виділяється у відповідності до його ознак, до яких можуть відноситися IP-адреси, MAC-адреси, порти TCP/UDP і інші поля заголовку пакета і кадру, які, зазвичай, використовуються для класифікації потоків даних.

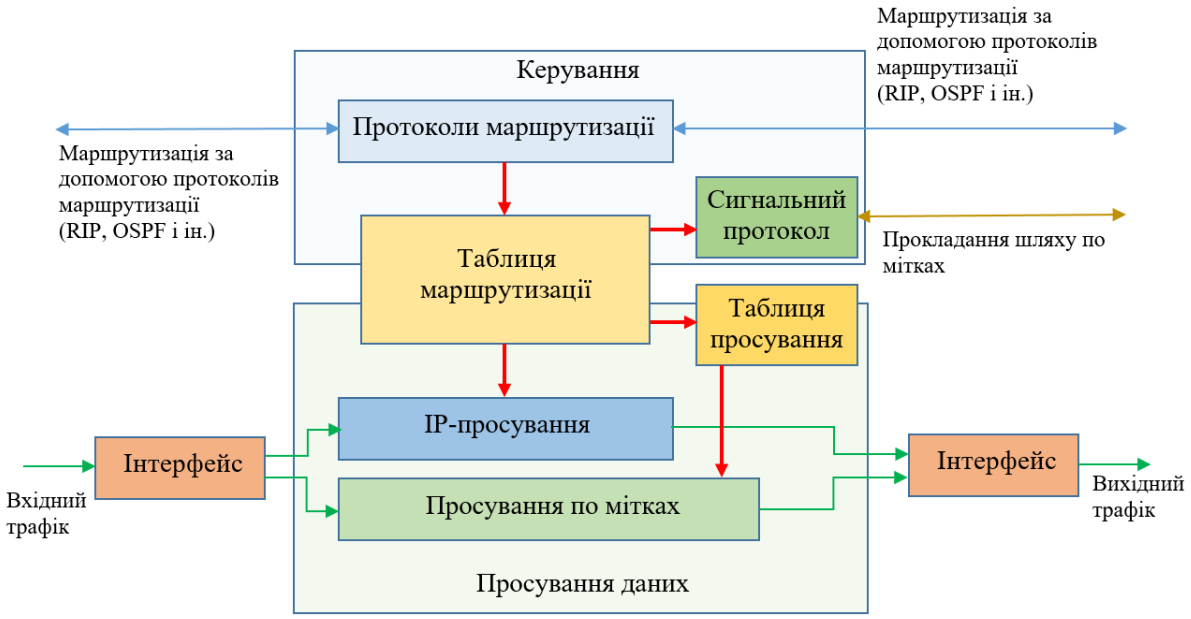



Рис. 7.2. Архітектура IP/MPLS-маршрутизатора

Шляхи комутації по мітках прокладаються в мережі незалежно від того, чи існує потік пакетів в мережі в даний час або тільки є *топологічно можливим*. Остання умова означає, що в мережі є деякі два кінцевих вузла, що визначаються IP-адресами, і між ними є можливість встановити шлях через проміжні IP/MPLS-маршрутизатори. Така властивість шляхів комутації по мітках іноді називають «топологічно веденим» (topology-driven).

### 7.1.2. Шляхи комутації по мітках

Шляхи комутації по мітках в технології MPLS являють собою деякий гібрид комутованих і постійних віртуальних каналів. Їх можна віднести до комутованих, так як вони встановлюються в мережі автоматично за допомогою сигнальних протоколів. У той же час, вони можуть вважатися постійними, так як їх створення ініціюється не динамічним запитом, викликаним необхідністю встановити сеанс зв'язку між кінцевими вузлами і передати деякі дані, а наявною топологією мережі, що мало змінюється в часі.

Шляхи комутації по мітках в технології MPLS підтримують інжиніринг трафіку за рахунок відповідних протоколів маршрутизації і спеціального сигнального протоколу.

Розглянемо роботу шляху LSP на прикладі мережі, показаної на рис. 7.3. Ця MPLS мережа взаємодіє з декількома IP-мережами, які можливо, що не підтримують технологію MPLS. На рисунку показано новий тип пристроїв – це пригранічні пристрої LSR, які в технології MPLS мають спеціальну назву –

**прикордонні комутуючі по мітках маршрутизатори** (Label switch Edge Router, **LER**).

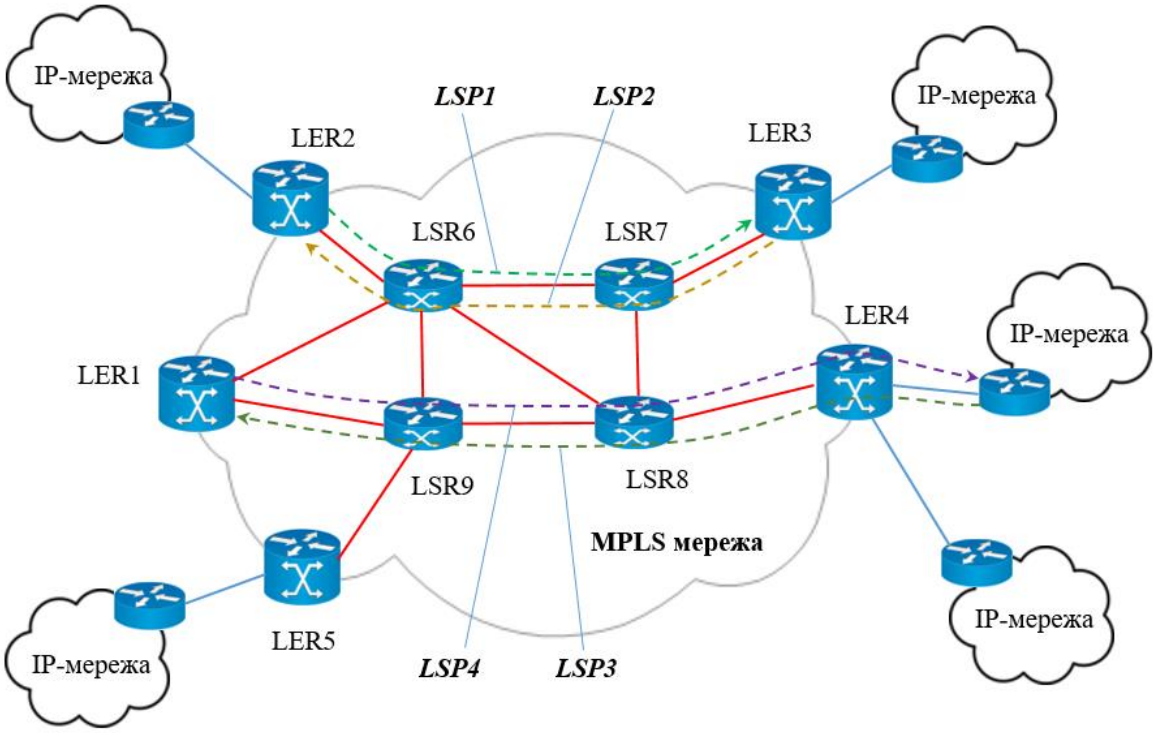



Рис. 7.3. MPLS мережа

Пристрій LER, будучи функціонально більш складним, приймає трафік від інших мереж в формі стандартних IP-пакетів, а потім додає до кожного пакету мітку і направляє уздовж відповідного шляху до вихідного пристрою LER через кілька проміжних пристроїв LSR. При цьому пакет просувається не на основі IP-адреси призначення, а на основі мітки.

Як і в інших технологіях, що використовують техніку віртуальних каналів, мітка має локальне значення в межах кожного пристрою LER або LSR, тобто при передачі пакета з вхідного інтерфейсу на вихідний виконується зміна значення мітки.

При прийнятті рішення про вибір наступного хопа блок просування по мітках використовує таблицю комутації, яка в стандарті MPLS носить назву **таблиці просування**. Таблиця просування в технології MPLS схожа на аналогічні таблиці інших технологій, заснованих на техніці віртуальних каналів (табл. 7.1).

У даній таблиці, в порівнянні з узагальненою таблицею комутації, що була представлена у розділі 4 «Транспортні технології телекомунікаційних мереж канального рівня» (рис. 4.7), замість поля вихідного інтерфейсу – поле наступного хопу, а замість поля вихідний мітки – поле дія. У більшості випадків

обробки MPLS-кадрів ці поля використовуються таким же чином, як відповідні їм поля узагальненої таблиці комутації. Тобто, значення поля наступного хопу є значенням вихідного інтерфейсу, на який потрібно передати кадр, а значення поля дія – новим значенням мітки. Однак в деяких випадках ці поля служать іншим цілям.

Таблиця 7.1.

Приклад таблиці просування в технології MPLS

| **Вхідний інтерфейс** | **Мітка** | **Наступний хоп** | **Дія** |
|---|---|---|---|
| S0 | 245 | S1 | 256 |
| S0 | 27 | S2 | 45 |
| … | … | … | … |

Розглянуті таблиці для кожного пристрою LSR формуються сигнальним протоколом. У MPLS використовується два різних сигнальних протоколи: **протокол розподілу міток** (**Label Distribution Protocol**, **LDP**) і модифікацію **протоколу резервування мережевих ресурсів** (Resource ReSerVation Protocol, **RSVP**).

Формуючи таблиці просування на пристроях LSR, сигнальний протокол прокладає через мережу віртуальні маршрути – **шляхами комутації по мітках** (**LSP**).

У тому випадку, коли мітки встановлюються в таблицях просування за допомогою протоколу LDP, маршрути віртуальних шляхів LSP збігаються з маршрутами IP-трафіку, так як вони вибираються протоколами маршрутизації стека TCP/IP. Модифікація протоколу RSVP, який спочатку був розроблений для резервування параметрів QoS, використовується для прокладки шляхів, вибраних у відповідності до техніки інжинірингу трафіку. Тому ця версія протоколу отримала назву RSVP TE (Traffic Engineering). Можна також формувати таблиці MPLS-просування вручну, створюючи там статичні записи, подібні до статичних записів таблиць маршрутизації.

LSP являє собою однонапрямлений віртуальний канал, тому для передачі трафіку між двома пристроями LER потрібно встановити принаймні два шляхи комутації по мітках – по одному в кожному напрямку. На рис. 5.3 показані дві пари шляхів комутації по мітках, що з’єднують пристрої LER2 і LER3, а також LER1 і LER4.

LER виконує таку важливу функцію, як направлення вхідного трафіку в один із вихідних з LER шляхів LSP. Для реалізації цієї функції в MPLS введено

поняття **класу еквівалентності просування** (Forwarding Equivalence Class, **FEC**).

Клас еквівалентності просування – це група пакетів, які мають одні і ті ж вимоги до умов транспортування (транспортного сервісу). Всі пакети, що належать до даного класу, просуваються через MPLS мережу по одному віртуальному шляху LSR.

Вхідний пакет відносять до того чи іншого класу на підставі деяких ознак. Декілька прикладів класифікації:

- *На підставі IP-адреси призначення*. Це найбільш близький до принципів роботи IP-мереж підхід, який полягає в тому, що для кожного префіксу мережі призначення, наявного в таблиці LER-маршрутизації, створюється окремий клас FEC. Протокол LDP повністю автоматизує процес створення класів FEC за цим способом.
- *У відповідності до вимог інжинірингу трафіку*. Класи вибираються таким чином, щоб домогтися балансу завантаження каналів мережі.
- *У відповідності з вимогами VPN*. Для конкретної віртуальної приватної мережі клієнта створюється окремий клас FEC.
- *За типами додатків*. Наприклад, трафік IP-телефонії (RTP) становить один клас FEC, а веб-трафік – інший.
- *По інтерфейсу, з якого отримано пакет.*
- *За MAC-адресою призначення кадру, якщо це кадр Ethernet.*

Як видно з наведених прикладів, при класифікації трафіку в MPLS можуть використовуватися ознаки, не лише взяті з заголовка IP-пакету, а й багато інших, включаючи інформацію канального (MAC-адреса) і фізичного (інтерфейс) рівнів.

Після прийняття рішення про приналежність пакету до певного класу FEC його потрібно зв’язати з існуючим шляхом LSP. Для цієї операції LER використовує **таблицю FTN** (FEC To Next hop – відображення класу FEC на наступний хоп). Таблиця 7.2 є прикладом FTN.

Таблиця 7.2.

Приклад таблиці FTN

| **Ознаки FEC** | **Мітка** |
|---|---|
| 123.20.0.0/16; 195.14.0.0 | 106 |
| 194.20.0.0; eth1 | 107 |

На підставі таблиці FTN кожному вхідному пакету призначається відповідна мітка, після чого цей пакет в домені MPLS не відрізнятиметься від

інших пакетів того ж класу FEC, всі вони просуватимуться по одному і тому ж шляху всередині домену.

У адміністратора мережі є можливість формувати таблиці FEC або ж корегувати їх, якщо вони формуються автоматично.

Складне налаштування та конфігурування виконуються тільки в LER, а всі проміжні пристрої LSR просто просувають пакет відповідно до техніки віртуального каналу. Вихідний пристрій LER видаляє мітку і передає пакет в наступну мережу вже в стандартній формі IP-пакету. Таким чином, технологія MPLS залишається прозорою для інших IP-мереж.

Зазвичай, в MPLS-мережах використовується вдосконалений, в порівнянні з описаним, алгоритм обробки пакетів. Удосконалення полягає в тому, що видалення мітки виконує не останній на шляху пристрій, а передостанній. Дійсно, після того, як передостанній пристрій визначить на основі значення мітки наступний хоп, мітка в MPLS-кадрі вже не потрібна, оскільки останній пристрій, тобто вихідний пристрій LER, має просувати пакет на основі значення IP-адреси. Ця невелика зміна алгоритму просування кадру дозволяє заощадити одну операцію над MPLS-кадром. В іншому випадку, останній вздовж шляху пристрій мав би видалити мітку, а вже потім виконати перегляд таблиці IP-маршрутизації. Ця техніка отримала назву – **видалення мітки на передостанньому хопі** (Penultimate Hop Popping, PHP).

### 7.1.3. Заголовок MPLS і технології канального рівня

Заголовок MPLS складається з декількох полів (рис 7.4.):

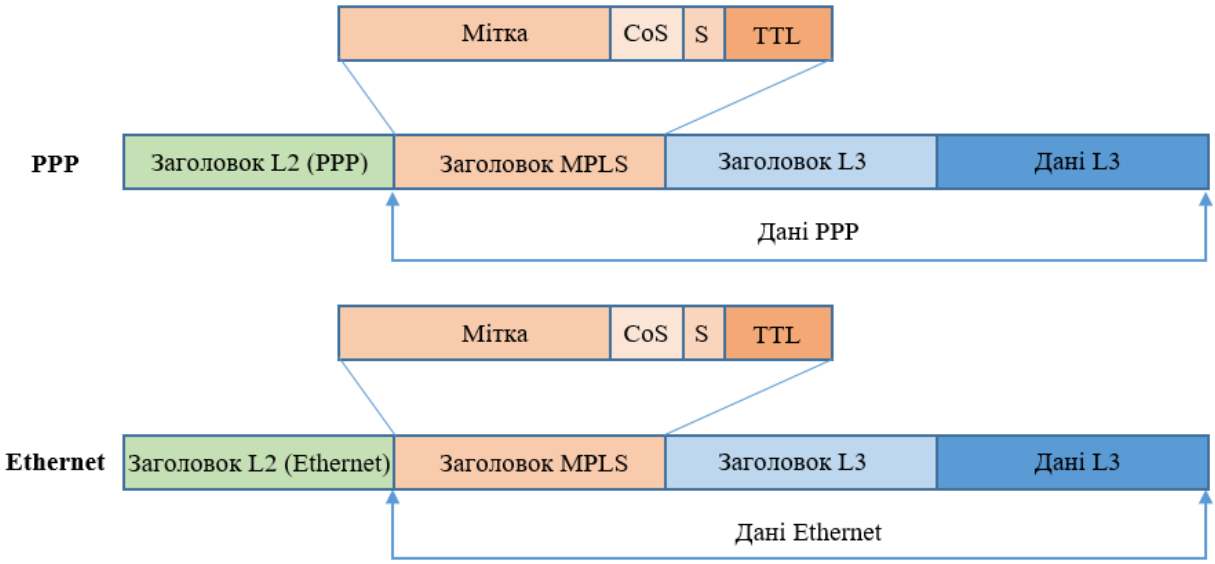



Рис. 7.4. Формат заголовка технології MPLS

- *Мітка* (20 біт). Використовується для вибору відповідного шляху комутації по мітках.
- *Час життя* (TTL – Time to live). Дане поле, що займає 8 біт, дублює аналогічне поле IP-пакета. Це необхідно для того, щоб пристрої LSR могли відкидати «блукаючі» пакети тільки на підставі інформації, що міститься в заголовку MPLS, не звертаючись до заголовку IP.
- *Клас послуги* (Class of Service, CoS). Поле CoS, що займає 3 біти, спочатку було зарезервовано для розвитку технології, але останнім часом використовується, в основному, для вказівки класу трафіку, що вимагає певного рівня QoS.
- *Ознака закінчення стеку міток*. Ця ознака (S) займає 1 біт.

Для пояснення механізму взаємодії MPLS з технологіями канального рівня розглянемо ситуацію, коли заголовок MPLS включає тільки одну мітку. У кадрах канального рівня заголовок MPLS поміщається між оригінальним заголовком і заголовком пакету третього рівня. На рис. 5.4 цей спосіб розміщення мітки показаний для кадрів PPP і Ethernet. Стандарти MPLS визначають також спосіб розміщення мітки в кадрах Frame Relay і комірках ATM.

У зв’язку з тим, що заголовок MPLS поміщається між заголовком канального рівня і заголовком IP, його називають **заголовком-вставкою** (shim header).

Просування кадру в MPLS-мережі відбувається на основі мітки MPLS і техніки LSP, а не на основі адресної інформації і техніки тієї технології, формат кадру якої MPLS використовує. Таким чином, якщо в MPLS застосовується кадр Ethernet, то MAC-адреси відправника і отримувача, хоча і присутні у відповідних полях кадру Ethernet, для просування кадрів в з’єднаннях Ethernet з топологією «точка-точка» не використовуються. Виняток становить випадок, коли між двома сусідніми пристроями LSR знаходиться мережа комутаторів Ethernet, – тоді MAC-адреса призначення MPLS-кадру потрібно для того, щоб кадр дійшов до наступного пристрою LSR, а вже він буде просувати його на підставі мітки. Знаходження MAC-адреси наступного LSR буде в цьому випадку виконано стандартним методом за допомогою протоколу ARP по IP-адресі LSR. Далі для визначеності при розгляді прикладів ми будемо мати на увазі, що використовується формат кадрів MPLS/PPP.

### 7.1.4. Стек міток

Наявність стеку міток є одним з оригінальних властивостей MPLS.

Стек міток дозволяє створювати систему агрегованих шляхів LSP з будь-якою кількістю рівнів ієрархії. Для підтримки цієї функції MPLS-кадр, який

переміщається уздовж ієрархічно організованого шляху, повинен включати стільки заголовків MPLS, скільки рівнів ієрархії має шлях. Заголовок MPLS кожного рівня має власний набір полів: мітка, CoS, TTL і S. Послідовність заголовків організована як стек, так що завжди є мітка, яка перебуває на вершині стека, і мітка, що знаходиться на дні стеку, при цьому остання супроводжується ознакою S = 1.

Над мітками виконуються наступні операції, що задаються в полі дій таблиці просування:

- *Push* – помістити мітку в стек. У разі порожнього стека ця операція означає просте присвоєння мітки пакету. Якщо ж в стеці вже є мітки, в результаті цієї операції нова мітка зсуває «старі» в глибину стеку, а сама опиняється на вершині.
- *Swap* – замінити поточну мітку новою.
- *Pop* – виштовхування (видалення) верхньої мітки, в результаті всі інші мітки стеку піднімаються на один рівень.

Просування MPLS-кадру завжди відбувається на основі мітки, що знаходиться в даний момент на вершині стеку.

Ієрархія міток найчастіше знаходить своє застосування в мережах, розділених на декілька доменів. Всередині домена просування пакетів відбувається на основі міток одного з рівнів стеку, а між доменами – на основі міток іншого рівня. Такий підхід дозволяє незалежно організувати внутрішньодоменну і міждоменну маршрутизацію пакетів. Стек міток також виявляється корисним при організації сервісу VPN.

Розглянемо роботу двох рівнів ієрархії міток на прикладі мережі, зображеної на рис. 7.5.

Мережа складається з трьох MPLS доменів. На рисунку показані шлях LSP1 в домені 1 і шлях LSP2 в домені 2. LSP1 з'єднує пристрої LER1 і LER2, проходячи через пристрої LSR1, LSR2 і LSR3. Нехай початкової міткою шляху LSP1 є мітка 256, яка була привласнена пакету прикордонним пристроєм LER1. На підставі цієї мітки пакет надходить на пристрій LSR1, який по своїй таблиці просування визначає нове значення мітки пакету (272) і переправляє його на вхід LSR2. Пристрій LSR2, діючи аналогічно, привласнює пакету нове значення мітки (132) і передає його на вхід LSR3. Пристрій LSR3, будучи передостаннім

пристроєм на шляху LSP1, виконує операцію *Pop* і видаляє мітку зі стеку. Пристрій LER2 просуває пакет вже на підставі IP-адреси.

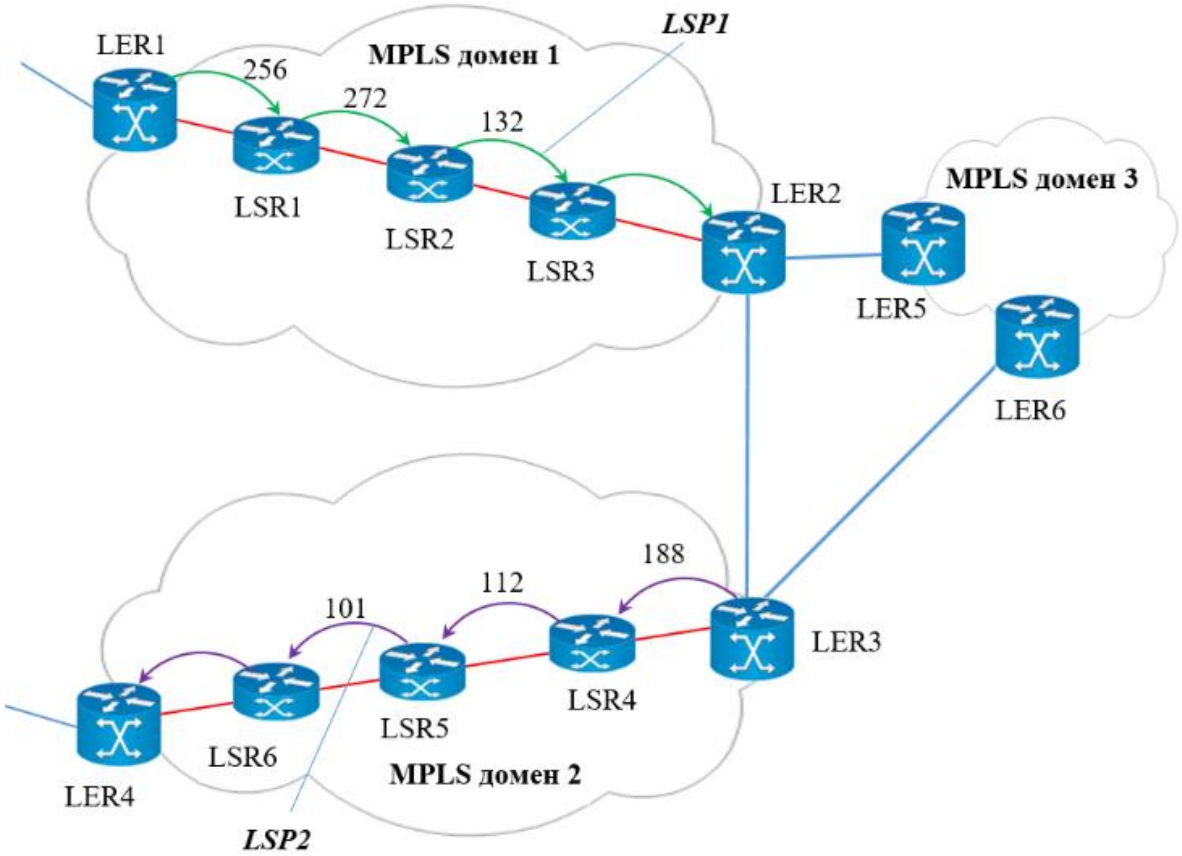



Рис. 7.5 Шляхи LSP1 і LSP2, які прокладені в доменах 1 і 2 MPLS мережі

На рисунку також показано шлях LSP2 в домені 2. Він з'єднує пристрої LER3 і LER4, проходячи через пристрої LSR4, LSR5 і LSR6, і визначається послідовністю міток 188, 112, 101.

Для того, щоб IP-пакети могли передаватися на основі технології MPLS не тільки всередині кожного домена, але і між доменами (наприклад, між пристроями LER1 і LER4), існують два принципово різних рішення.

- Перше рішення полягає в тому, що між LER1 і LER4 встановлюється один однорівневий шлях комутації по мітках, що з'єднує шляхи LSP1 і LSP2 (які в цьому випадку стають одним шляхом). Це просте на перший погляд рішення, назване **зшиванням шляхів** LSP, погано працює в тому випадку, коли MPLS домени належать різним постачальникам послуг, не дозволяючи їм взаємодіяти один з одним, так як шлях повинен бути встановлений «з кінця в кінець» одним з сигнальних протоколів.

- Другим, більш перспективним рішенням є застосування багаторівневого підходу до з'єднання двох MPLS доменів, що належать, можливо, різним постачальникам послуг.

Для реалізації другого підходу, в розглянутому вище прикладі, потрібно створити шлях комутації по мітках другого рівня (LSP3), що з'єднує пристрої LER1 і LER4. Цей шлях визначає послідовність хопів між доменами, а не між внутрішніми пристроями LSR кожного домену. Так, LSP3 складається з хопів LER1-LER2-LER3-LSR4. В цьому відношенні багаторівневий підхід MPLS концептуально дуже близький підходу протоколу BGP, що визначає шлях між автономними системами.

Розглянемо більш детально, як працює технологія MPLS в разі шляхів комутації по мітках двох рівнів (рис. 7.6).

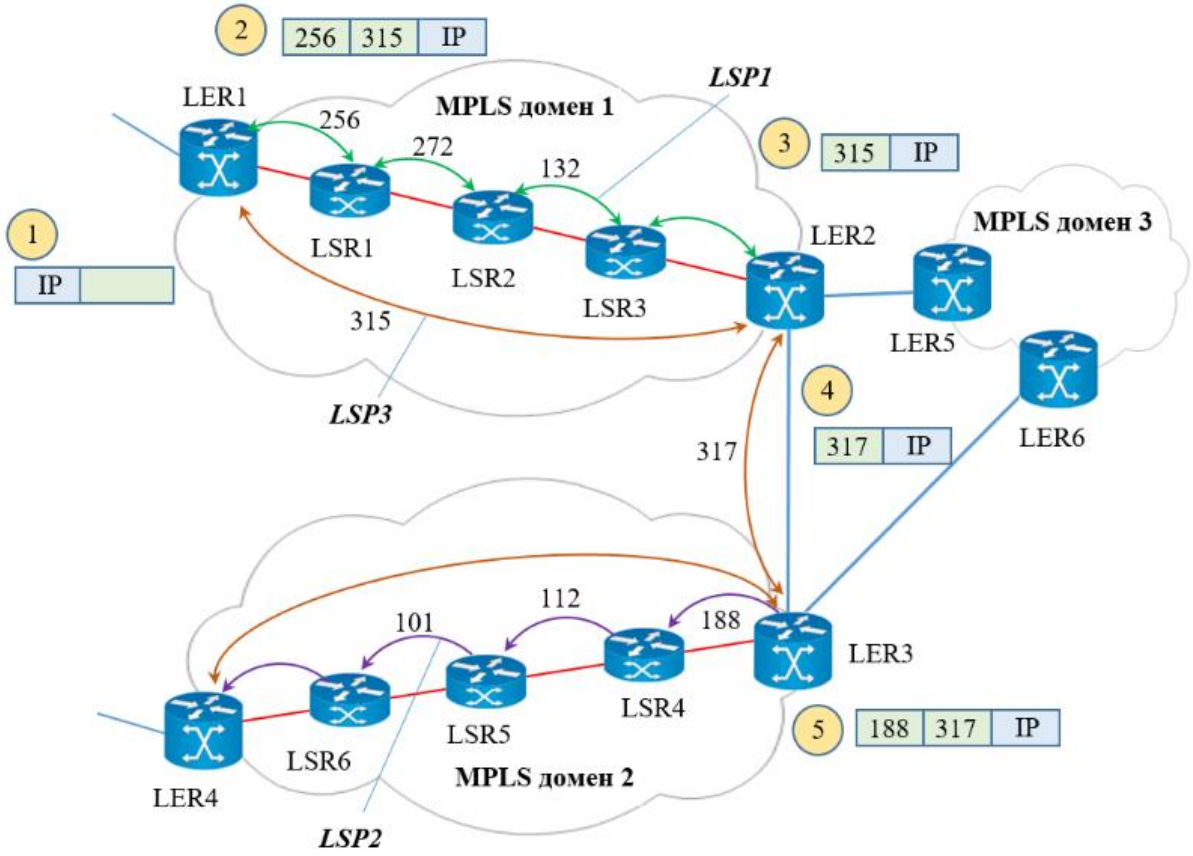



Рис. 7.6. Використання стеку міток в ієрархії шляхів

У пристрої LER1 починаються два шляхи – LSP1 і LSP3, що забезпечується відповідним записом в таблиці просування пристрою LER1 (табл. 7.3).

Таблиця 7.3.

Запис в таблиці просування LER1

| **Вхідний інтерфейс** | **Мітка** | **Наступний хоп** | **Дія** |
|---|---|---|---|
| … | … | … | … |
| S0 | – | S1 | 315<br>Push<br>256 |
| … | … | … | … |

IP-пакети, що надходять на інтерфейс S0, пристрою LER1, просуваються на його вихідний інтерфейс S1, де для них створюється заголовок MPLS, що включає мітку 315 верхнього рівня (LSP3), яка на цей момент знаходиться на верху стеку міток. Потім ця мітка проштовхується на дно стеку (операція Push), а верхньою стає мітка 256, що відноситься до LSP1.

Далі MPLS-кадр з міткою 256 надходить на вихідний інтерфейс S1 прикордонного пристрою LER1 і передається на вхід LSR1. Пристрій LSR1 обробляє кадр відповідно до своєї таблиці просування (табл. 7.4). Мітка 256, що знаходиться на вершині стеку, замінюється міткою 272 (мітка 315, що знаходиться нижче в стеці, пристроєм LSR1 ігнорується).

Таблиця 7.4.

Запис в таблиці просування LSR1

| **Вхідний інтерфейс** | **Мітка** | **Наступний хоп** | **Дія** |
|---|---|---|---|
| … | … | … | … |
| S0 | 256 | S1 | 272 |
| … | … | … | … |

Аналогічні дії виконує пристрій LSR2, який замінює мітку 272 міткою 132 і відправляє кадр наступному на шляху пристрою LSR3.

Робота пристрою LSR3 дещо відрізняється від роботи пристроїв LSR1 і LSR2, так як він є передостаннім пристроєм LSR для шляху LSP1 (табл. 7.5).

Таблиця 7.5.

Запис в таблиці просування LSR3

| **Вхідний інтерфейс** | **Мітка** | **Наступний хоп** | **Дія** |
|---|---|---|---|
| … | … | … | … |
| S0 | 132 | S1 | Pop |
| … | … | … | … |

Пристрій LSR3 виконує виштовхування (*Pop*) з стеку мітки 132, що відноситься до шляху LSP1, виконуючи операцію PHP. В результаті верхньою міткою стеку стає мітка 315, що належить шляху LSP3.

Пристрій LER2 просуває кадр, що надійшов на його вхідний інтерфейс S0, на основі свого запису в таблиці просування (табл. 7.6). Пристрій LER3 спочатку замінює мітку 315 шляху LSP3 значенням 317, потім проштовхує її на дно стеку і поміщає на вершину стеку мітку 188, яка є міткою шляху LSP2, внутрішнього для домену 2. Переміщення кадру уздовж шляху LSP2 відбувається аналогічним чином.

Таблиця 7.6.

Запис в таблиці просування LER3

| **Вхідний інтерфейс** | **Мітка** | **Наступний хоп** | **Дія** |
|---|---|---|---|
| … | … | … | … |
| S0 | 315 | S1 | 317<br>Push<br>188 |
| … | … | … | … |

Значення мітки міждоменного шляху LSP3 на границі між доменами не залежить від значень міток, які використовуються для внутрішньодоменних шляхів LSP1 і LSP2. Це дозволяє операторам доменів змінювати значення міток внутрішньодоменних шляхів незалежно один від одного, наприклад прокладаючи внутрішньодоменні шляхи за іншими маршрутами (це неминуче призведе до перепризначення міток в кожному з пристроїв LSR і LER). Важливо, що при цьому значення міждоменної мітки при передачі пакету між пристроями LER доменів не змінюється, тому пакет правильно обробляється приймаючим пристроєм LER. Наприклад, LER3 отримає пакет від LER6 зі значенням мітки 317 незалежно від того, яке значення мала мітка внутрішньодоменного шляху LSP1. При «зшиванні» однорівневих пристроїв LSP такої незалежності доменів домогтися не можна.

Описана модель дворівневого шляху легко може бути розширена для будь-якої кількості рівнів.

## 7.2. Протокол LDP

**Протокол розподілу міток** (Label Distribution Protocol, LDP) дозволяє автоматично створювати в мережі шляхи LSP відповідно до існуючих в таблицях маршрутизації записами про маршрути в IP-мережі. Протокол LDP є сигнальним протоколом мереж MPLS.

Протокол LDP бере до уваги тільки ті записи таблиці маршрутизації, які створені за допомогою внутрішніх протоколів маршрутизації, тобто протоколів типу IGP, тому режим автоматичної побудови LSP за допомогою протоколу LDP іноді називають режимом MPLS IGP (на відміну від режиму MPLS TE, коли маршрути вибираються з міркувань інжинірингу трафіку і не збігаються з маршрутами, обраними внутрішніми протоколами маршрутизації). Розглянемо роботу протоколу LDP на прикладі мережі, зображеної на рис. 6.7.

Всі пристрої LSR мережі підтримують сигнальний протокол LDP. Від пристрою LSR1 в мережі вже встановлений один шлях LSP1 – по цьому шляху йде трафік до мереж 105.0.0.0 і 192.201.103.0. Таблиця FTN пристрою LSP1 приведена в табл. 7.7.

Таблиця 7.7.

Таблиця FTN пристрою LSP1

| **Ознаки FEC** | **Мітка** |
|---|---|
| 105.0.0.0; 192.201.103.0. | 231 |

Мітка 231 в цій таблиці відповідає шляху LSP1.

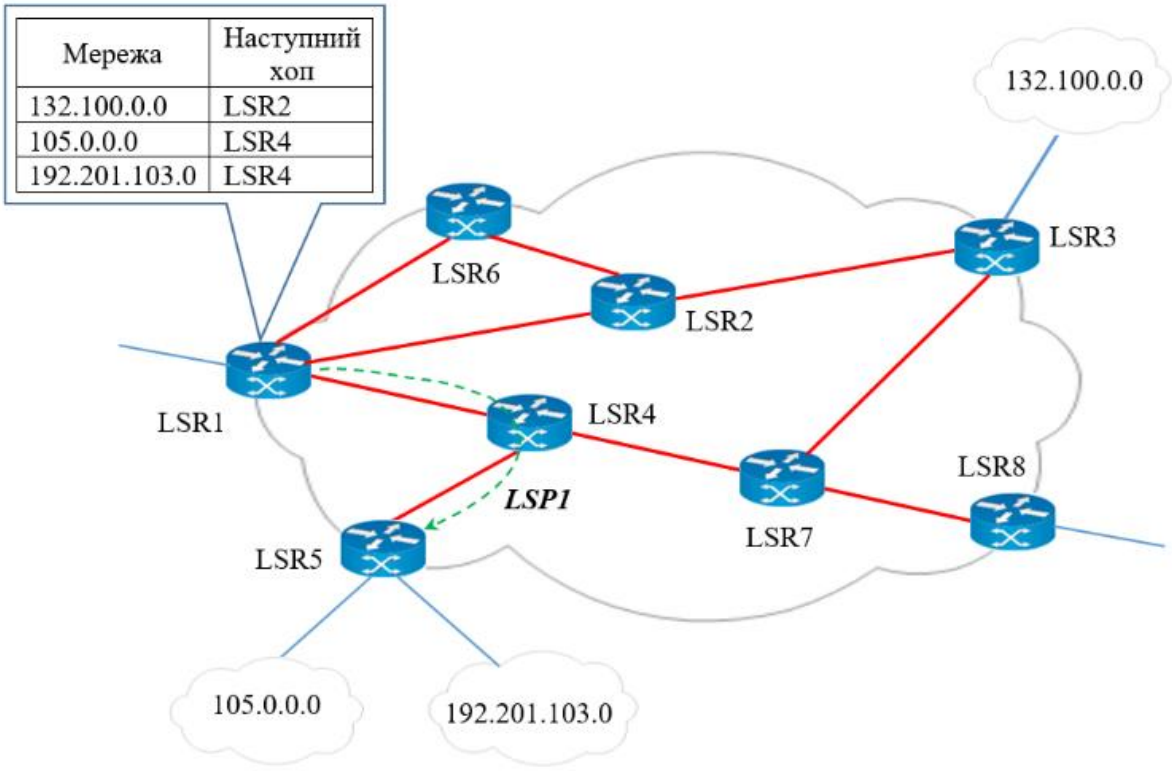



Рис. 7.7. MPLS мережа з пристроями LSR, які підтримують LDP

Розглянемо функціонування протоколу LDP в ситуації, коли в результаті роботи протоколів маршрутизації або ж після ручної модифікації адміністратором мережі в таблиці маршрутизації пристрою LSR1 з'явився запис про нову мережу призначення, для якої в мережі постачальника послуг ще не прокладений шлях комутації по мітках. У нашому випадку це мережа 132.100.0.0 і для неї немає запису в таблиці FTN.

В цьому випадку пристрій LSR1 автоматично ініціює процедуру прокладки нового шляху. Для цього він запитує по протоколу LDP мітку для нової мережі 132.100.0.0 у маршрутизатора, IP-адреса якого в таблиці маршрутизації вказана для даної мережі як адреса наступного хопу. Однак, для того щоб скористатися протоколом LDP, потрібно спочатку встановити між пристроями LSR сеанс LDP, так як цей протокол працює в режимі встановлення з'єднання. Сеанси LDP встановлюються між сусідніми маршрутизаторами автоматично. Для цього кожен пристрій LSR, на якому розгорнуто протокол LDP, починає посилати своїм сусідам повідомлення *Hello*. Ці повідомлення надсилаються по груповій IP-адресі 224.0.0.2, яка є адресою всіх маршрутизаторів підмережі. Якщо сусідній маршрутизатор також підтримує протокол LDP, то він у відповідь встановлює сеанс TCP через порт 646 (цей порт закріплений за протоколом LDP).

В результаті обміну повідомленнями *Hello,* всі пристрої LSR, що підтримують протокол LDP, виявляють своїх сусідів і встановлюють з ними сеанси, як показано на рис. 7.8 (для простоти на рисунку представлені не всі сеанси LDP, існуючі в мережі).

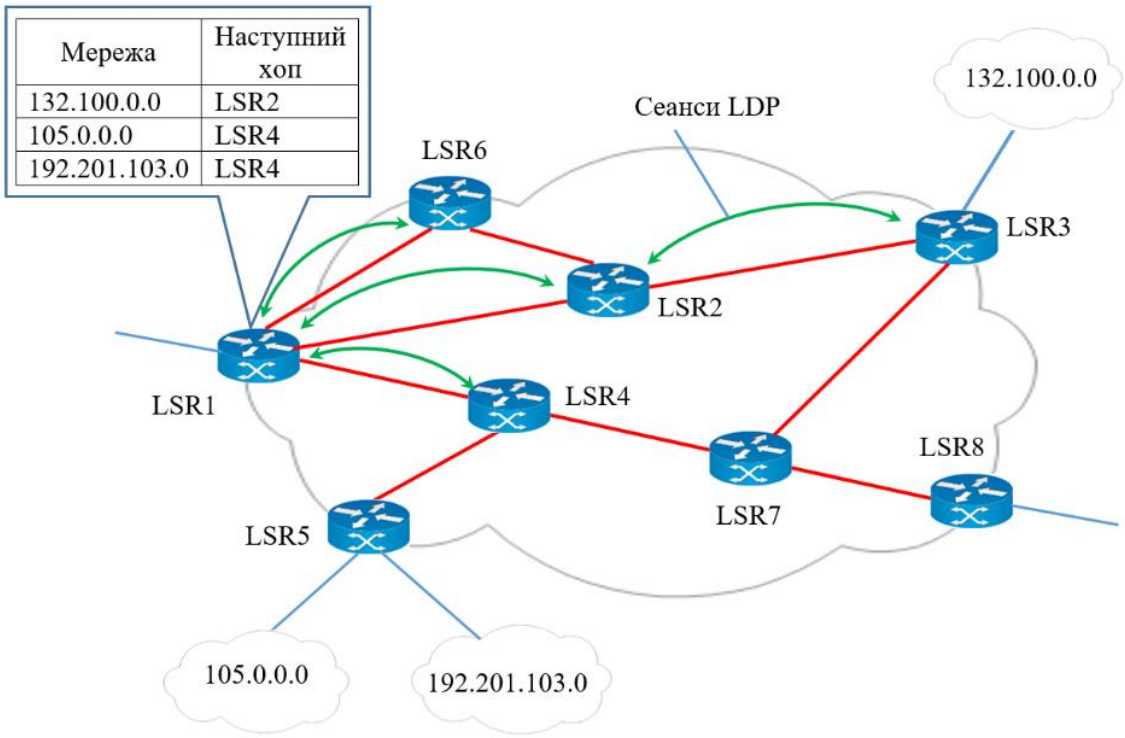



Рис. 7.8. Сеанси LDP, які встановлюються між безпосередніми сусідами

Будемо вважати, що між пристроями LSR1 і LSR2 встановлений сеанс LDP. Тоді, при виявленні нового запису в таблиці маршрутизації, що вказує на пристрій LSR2 в якості наступного хопу, пристрій LSR1 просить пристрій LSR2 призначити мітку для нового шляху до мережі 132.100.0.0. Кажуть, що пристрій LSR2 знаходиться нижче по потоку (downstream) відносно пристрою LSR1 на шляху до мережі 132.100.0.0. Відповідно пристрій LSR1 розташований вище по потоку (upstream) для пристрої LSR2 відносно мережі 132.100.0.0. Зрозуміло, що для інших мереж призначення у пристрою LSR1 є інші сусіди вниз по потоку, а у пристрою LSR2 – інші сусіди вгору по потоку.

Причина, по якій значення мітки для нового шляху вибирається сусідом нижче по потоку, зрозуміла – ця мітка, яка має локальне значення на двоточковому з’єднанні (з’єднання «точка-точка») між сусідніми пристроями, буде використовуватися саме цим пристроєм для того, щоб розуміти, до якого шляху LSP відноситься вхідний MPLS-кадр. Тому пристрій, що знаходиться нижче по потоку, вибирає унікальне значення мітки, виходячи з невикористаних значень міток для свого інтерфейсу, який пов’язує його з сусідом вище по потоку. Для отримання значення мітки пристрій LSR1 виконує запит мітки протоколу LDP.

Пристрій LSR2, прийнявши запит, знаходить, що у нього також немає прокладеного шляху до мережі, тому він передає LDP-запит наступному пристрою LSR, адреса якого вказана в його таблиці маршрутизації в якості наступного хопу для мережі 132.100.00 В прикладі, показаному на рис 5.8, таким пристроєм є LSR3, на якому шлях комутації по мітках повинен закінчитися, так як наступний хоп веде за межі MPLS-мережі даного оператора.

Виникає питання: як пристрій LSR3 дізнається про те, що є останнім в мережі постачальника послуг на шляху до мережі 132.100.0.0? Справа в тому, що сеанси LDP встановлюються тільки між пристроями одного постачальника послуг, тому відсутність сеансу LDP з наступним хопом маршруту і вказує пристрою LSR, що він є останнім у своєму домені для даного шляху LSP.

Пристрій LSR3, виявивши, що на шляху до мережі 132.100.0.0 він є прикордонним, призначає для прокладається шляху мітку, ще не зайняту його вхідним інтерфейсом S0, і повідомляє про цю мітку пристрою LSR2 в LDP-повідомленні. Нехай це буде мітка 231.

У свою чергу пристрій LSR2 призначає не використовувану його інтерфейсом S0 мітку і повідомляє про це в LDP-повідомленні пристрою LSR1 (в прикладі, мітка 199). Після цього новий шлях комутації по мітках, що веде від LSR1 до мережі 132.100.0.0, вважається прокладеним (рис. 7.9), і уздовж нього пакети починають передаватися вже на основі міток і таблиць просування, а не IP-адрес і таблиць маршрутизації.

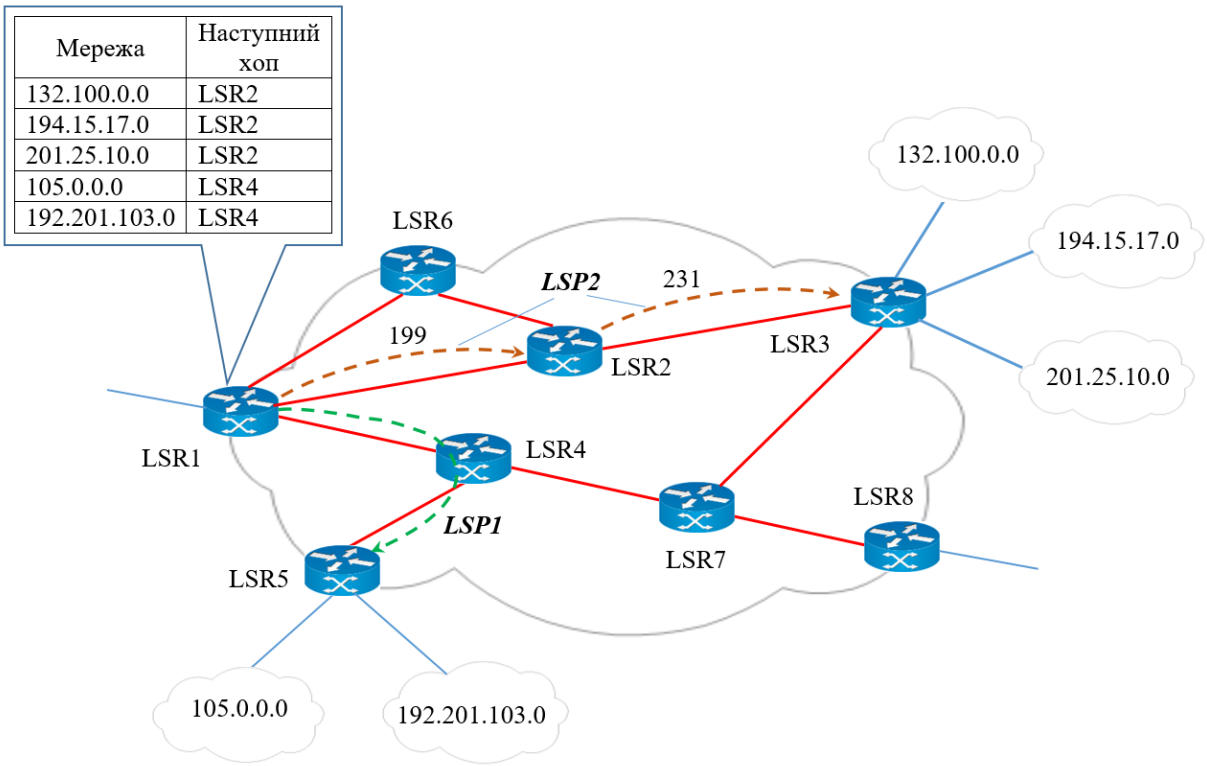



Рис. 7.9. Новий шлях LSP2

Пристрої LSR намагаються будувати агреговані шляху комутації по мітках і передавати уздовж них пакети, які надсилаються до декількох мереж. Так, на рис. 6.9 пристрій LSR1 передає шляхом LSP2 пакети, які направляються не лише до мережі 132.100.0.0, а й до мереж 194.15.17.0 і 201.25.10.0, інформація про яких з'явилася вже після того, як шлях LSP2 був прокладений.

Розглянутий режим управління розподілом міток протоколу LDP носить назву «Впорядкований режим управління розподілом міток із запитом пристрою вниз по потоку». Під упорядкованим режимом розуміється такий режим, коли деякий проміжний пристрій LSR не передає мітку для нового шляху пристрою LSR, який знаходиться вище по потоку, до тих пір поки не отримає мітку для цього шляху від пристрою LSR, по лежачого нижче потоку. У нашому випадку пристрій LSR2 очікував отримання мітки від LSR3 і вже потім передавав мітку пристрою LSR1.

Існує й інший режим управління розподілом міток, який називається незалежним. При незалежному управлінні розподілом міток LSR може призначити і передати мітку, не чекаючи приходу повідомлення від свого сусіда, що знаходиться нижче по потоку. Наприклад, пристрій LSR2 міг би призначити і передати мітку 199 пристрою LSR1, не чекаючи приходу мітки 231 від пристрою LSR3. Оскільки мітки мають локальне значення, результат зміни режиму залишився б незмінним.

Існують також два методи розподілу міток: розподіл по запиту від пристрою, що знаходиться нижче по потоку і без запиту. Для нашого випадку це означає, що якби пристрій LSR2 виявив у своїй таблиці маршрутизації запис про нову мережу 132.100.0.0, він міг би призначити мітку новому шляху і передати її пристрою LSR1 без запиту. Оскільки при цьому пристрій LSR2 не знає свого сусіда вище по потоку (таблиця маршрутизації не вказує про це), він передає цю інформацію всім своїм сусідам по сеансах LDP. У цьому варіанті роботи протоколу LDP пристрої LSR можуть отримувати альтернативні мітки для шляху до деякої мережі. Вибір найкращого шляху здійснюється звичним для IP-маршрутизаторів (якими пристрою LSR є за сумісництвом) способом – на підставі кращої метрики, обраної протоколом маршрутизації.

Як видно з опису, існує два незалежних параметра, які визначають варіант роботи протоколу LDP: режим управління розподілом міток і метод розподілу міток. Оскільки кожен параметр має два значення, то всього існує чотири режими роботи протоколу LDP.

Протокол LDP найчастіше функціонує в режимі незалежного управління розподілом міток без запиту. Впорядковане управління розподілом міток потрібно при прокладанні шляхів LSP, які необхідні для інжинірингу трафіку.

## 7.3. Інжиніринг трафіку в MPLS

Технологія MPLS підтримує техніку **інжинірингу трафіку**, яка вирішує задачу вибору маршрутів для потоків (класів) трафіку з врахуванням дотримання вимог QoS.

У цьому випадку використовуються модифіковані протоколи сигналізації і маршрутизації, які мають приставку TE (Traffic Engineering – інжиніринг трафіку). В цілому такий варіант MPLS отримав назву MPLS TE.

В технології MPLS TE шляхи LSP називають TE-тунелями. TE-тунелі не прокладаються розподіленим методом уздовж шляхів, які визначаються звичайними протоколами маршрутизації незалежно в кожному окремому пристрої LSR. Замість цього TE-тунелі прокладаються згідно з технікою маршрутизації від джерела, коли централізовано задаються проміжні вузли маршруту. В цьому відношенні TE-тунелі подібні до постійних віртуальних каналів технологій ATM і Frame Relay. Ініціатором задання маршруту для TE-тунелю виступає початковий вузол тунелю, а розраховуватися такий маршрут може як цим же початковим вузлом, так і зовнішньою по відношенню до мережі, програмною системою чи адміністратором.

MPLS TE підтримує тунелі двох типів (рис. 7.10):

- **строгий TE-тунель** визначає всі проміжні вузли між двома прикордонними
  пристроями;
- **вільний TE-тунель** визначає тільки частину проміжних вузлів від одного прикордонного пристрою до іншого, а решта проміжних вузлів вибираються пристроєм LSR самостійно.

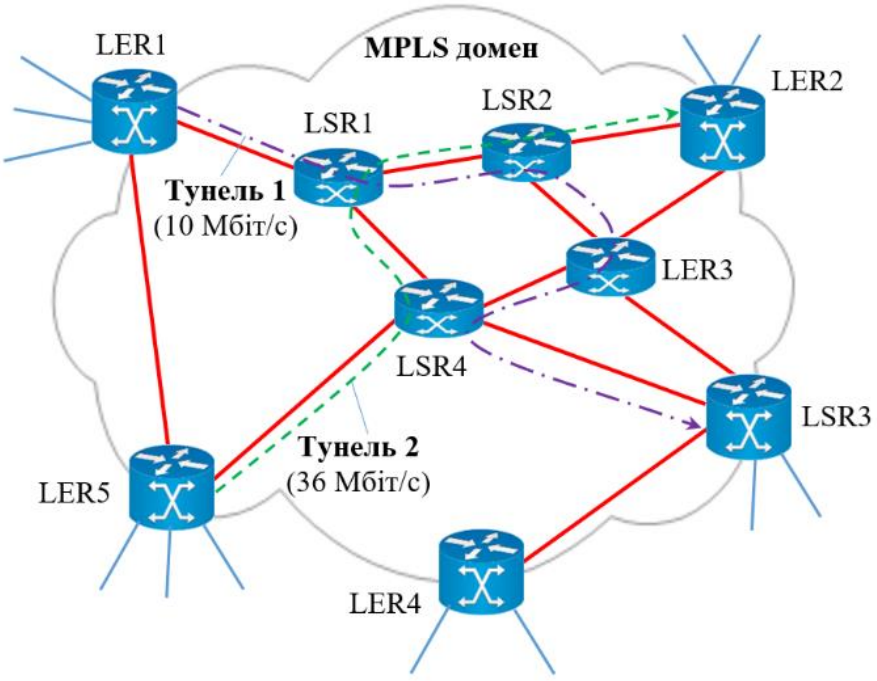



Рис. 7.10. Два типи TE-тунелів в технології MPLS

Тунель 1 є прикладом строгого тунелю, при його заданні зовнішня система (або адміністратор мережі) вказала як початковий і кінцевий вузли тунелю, так і всі проміжні вузли, тобто послідовність IP-адрес для пристроїв LERI, LSR1, LSR2, LSR3, LSR4 , LER3. Таким чином, зовнішня система вирішила завдання інжинірингу трафіку, вибравши шлях з достатньою невикористаною пропускною спроможністю. При встановленні тунелю 1 задається не тільки послідовність LSR, але і необхідна пропускна спроможність шляху. Незважаючи на те, що вибір шляху відбувається в автономному режимі, всі пристрої мережі уздовж тунелю 1 перевіряють, чи дійсно вони володіють необхідною невикористовуваною пропускною спроможністю, і тільки в разі позитивної відповіді тунель прокладається.

При прокладанні тунелю 2 (вільного) адміністратор задає лише початковий і кінцевий вузли тунелю, тобто пристрої LER5 і LER2. Проміжні пристрої LSR4 і LSR2 знаходяться автоматично початковим вузлом тунелю 2, тобто пристроєм LER5, а потім за допомогою сигнального протоколу пристрій LER5 повідомляє цим і кінцевому пристроям про необхідність прокладки тунелю.

Незалежно від типу тунелю він завжди володіє таким параметром, як резервована пропускна спроможність. У даному прикладі тунель 1 резервує для трафіку 10 Мбіт/с, а тунель 2 – 36 Мбіт/с. Ці значення визначаються адміністратором, і технологія MPLS TE ніяк не впливає на їх вибір, вона лише реалізує запрошене резервування.

Однак сама по собі прокладка в MPLS-мережі TE-тунелю ще не означає передачі по ньому трафіку. Вона означає тільки те, що в мережі дійсно існує можливість передачі трафіку по тунелю з середньою швидкістю, що не перевищує зарезервоване значення. Для того, щоб дані були передані по тунелю, адміністратору належить здійснити ще одну ручну процедуру – задання для початкового пристрою тунелю умов, що визначають, які саме пакети повинні передаватися по тунелю. Умови можуть бути різними, так, в якості ознак агрегованого потоку, який повинен передаватися по тунелю, можуть виступати всі традиційні ознаки: IP-адреса відправника і отримувача, тип протоколу, номери TCP і UDP портів, номер інтерфейсу вхідного трафіку, значення пріоритету в протоколі IP і т. д.

Таким чином, пристрій LER має спочатку провести *класифікацію трафіку*, потім виконати *профілювання*, впевнившись, що середня швидкість потоку не перевищує зарезервовану, і, нарешті, почати *маркувати* пакети, використовуючи початкову мітку TE-тунелю, щоб передавати трафік через мережу за допомогою техніки MPLS. У цьому випадку розрахунки, виконані на етапі вибору шляху для тунелю, дадуть потрібний результат – баланс ресурсів мережі при дотриманні середньої швидкості для кожного потоку.

Для вибору та перевірки шляхів через тунелі в технології MPLS TE використовуються розширення протоколів маршрутизації, що працюють на основі алгоритму стану зв'язків. Для вирішення завдання TE в протоколи OSPF і IS-IS включені нові типи оголошень, що забезпечують поширення по мережі інформації про номінальну і незарезервовану (доступну для TE-потоків) величини пропускної спроможності кожного зв'язку.

В технології MPLS TE інформація про знайдений оптимальний шлях використовується повністю – тобто запам'ятовуються IP-адреси відправника, всіх транзитних маршрутизаторів і кінцевого вузла. Тому достатньо, щоб пошуком шляхів займалися лише прикордонні пристрої мережі (LER), а проміжні пристрої (LSR) лише постачали їм інформацію про поточний стан резервування пропускної спроможності каналів.

Після знаходження шляху незалежно від того, знайдений він був пристроєм LER або адміністратором, його необхідно зафіксувати. Для цього в MPLS TE використовується розширення протоколу резервування ресурсів (RSVP), який часто в цьому випадку називають протоколом **RSVP TE**. Повідомлення RSVP TE передаються від одного пристрою LSR до іншого у відповідності з даними про знайдені IP-адреси маршруту. При встановленні нового шляху в сигнальному повідомленні поряд з послідовністю адрес вказується також і резервована пропускна спроможність. Кожен пристрій LSR, отримавши таке повідомлення, віднімає запитувану пропускну спроможність з пулу вільної пропускної спроможність відповідного інтерфейсу, а потім оголошує залишок у повідомленнях протоколу маршрутизації, наприклад OSPF.

Основною метою MPLS TE є використання можливостей MPLS для досягнення власної мети постачальника послуг, а саме збалансованого завантаження всіх ресурсів своєї мережі. Однак при цьому також створюється основа для надання транспортних послуг з гарантованими параметрами QoS, так як трафік по TE-тунелях передається при дотриманні деякого максимального рівня коефіцієнта використання ресурсів. Коефіцієнт використання ресурсів істотно впливає на процес утворення черги, так що потоки, що передаються по TE-тунелях, передаються з деяким гарантованим рівнем QoS. Для того щоб забезпечити різні параметри QoS для різних класів трафіку, постачальнику послуг необхідно для кожного класу трафіку встановити в мережі окрему систему тунелів. При цьому для класів чутливого до затримок трафіку потрібно виконати резервування таким чином, щоб максимальний коефіцієнт використання ресурсів тунелю знаходився в діапазоні 0,2-0,3, інакше затримки пакетів вийдуть за допустимі межі.

## 7.4. Моніторинг стану шляхів LSP

Наявність вбудованих в транспортну технологію засобів моніторингу стану з'єднань і локалізації помилок є необхідною умовою для того, щоб вона претендувала на статус технології операторського класу. В іншому випадку її важко буде використовувати операторам мереж, яким потрібно забезпечувати своїх численних клієнтів транспортним сервісом з високим коефіцієнтом готовності (в межах 0,999-0,99999), як це прийнято в телекомунікаційних мережах.

Спочатку технологія MPLS не мала таких вбудованих засобів, покладаючись на такі засоби стеку TCP/IP, як утиліти *ping* і *traceroute*, що використовують ICMP-повідомлення *Echo Request* (ехо-запит) і *Echo Reply* (ехо-відповідь). Однак класичні утиліти ping і traceroute стеку TCP/IP не дають коректної інформації про стан шляхів LSP, так як вони можуть проходити як уздовж, так і в обхід цих шляхів за допомогою техніки просування пакетів протоколу IP. Тому пізніше був розроблений спеціальний протокол **LSP Ping,** який дозволяє як тестувати працездатність LSP (режим ping), так і локалізувати відмови (режим traceroute).

Крім того, для моніторингу стану LSP можна застосовувати більш економічний, ніж LSP Ping, протокол двонаправленого виявлення помилок просування.

### 7.4.1. Тестування шляхів LSP

У протоколі LSP Ping для тестування стану LSP застосовується техніка, близька до механізму роботи утиліти ping протоколу IP. Вона полягає в тому, що протокол LSP Ping відправляє уздовж тестованого шляху LSP повідомлення Echo Request. Якщо таке повідомлення доходить до пристрою LER, який є кінцевим вузлом тестованого шляху LSP, він відповідає повідомленням Echo Reply . Отримання вихідним вузлом такого повідомлення означає, що шлях LSP працездатний.

Описана схема роботи аналогічна схемі роботи утиліти ping протоколу IP, проте вона має свої особливості (рис. 7.11).

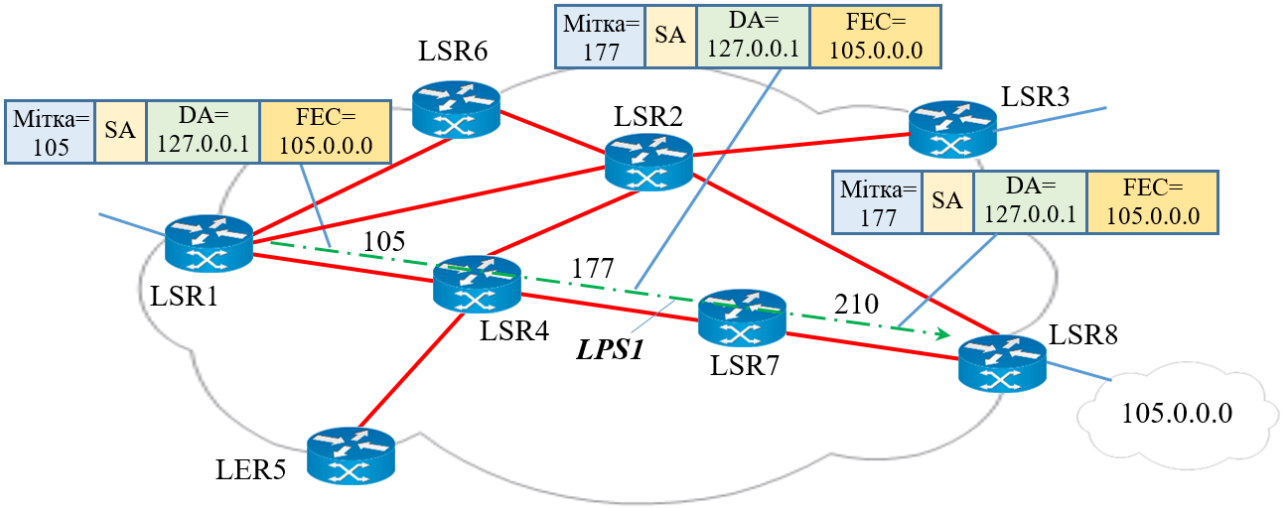



Рис. 7.11. Тестування LSP за допомогою протоколу LSP Ping

У прикладі (рис. 7.11) пристрій LSR1 тестує стан шляху LSP1, який закінчується на пристрої LSR8 (для цього шляху воно є пристроєм LER).

Для тестування шляху LSP1 пристрій LSR1 відправляє MPLS-пакет з міткою 105 – ця мітка відповідає шляху LSP1 на лінії між пристроями LSR1 і LSR4. Повідомлення *Echo Request* вкладається в UDP-повідомлення, яке, в свою чергу, вкладається в IP-пакет. На рисунку показані тільки важливі для вивчення протоколу LSP Ping поля: мітка MPLS-кадру, IP-адреса відправника (SA), IP-адреса отримувача (DA), а також поле FEC, яке ідентифікує тестований шлях LSP. У прикладі це IP-адреса мережі 105.0.0.0, до якої веде шлях LSP1.

Адреса призначення в IP-пакеті, який переносить повідомлення *Echo Request*, рівна 127.0.0.1, тобто є адресою зворотної петлі стеку протоколів TCP/IP кожного вузла. Адреса 127.0.0.1 повинна «працювати правильно», оскільки в процесі передачі запиту по мережі для його просування використовуються MPLS-мітки, а не IP-адреса призначення. При досягненні кінцевого вузла (це також може статися на попередньому хопі, якщо застосовується техніка PHP) IP-пакет звільняється від заголовка MPLS і обробляється на основі IP-адреси. Оскільки адреса 127.0.0.1 вказує на власний вузол, то пакет передається власному стеку TCP/IP, де він розпізнається як UDP-пакет протоколу LSP Ping і обробляється відповідно.

Поле FEC надсилається в запиті Echo Request для того, щоб кінцевий вузол шляху міг порівняти вказане в пакеті значення FEC зі значенням з його власної бази даних для шляху, по якому прийшов кадр запиту. Такий механізм дозволяє відслідковувати ситуації, коли запит, внаслідок деяких помилок, приходить не тим шляхом, який тестується.

У тому випадку, коли запит успішно доходить до кінцевого вузла шляху, і той переконується, що отриманий запит прийшов по потрібному шляху (тобто отримане значення FEC збігається зі значенням FEC з бази даних кінцевого вузла), він відправляє відповідь *Echo Reply* вузлу, який виконав запит. У прикладі на рис. 5.11 вузол LSR8 відправляє відповідь *Echo Reply* вузлу LSR1. Повідомлення *Echo Reply* надсилається вже не по шляху LSP, а як звичайне UDP-повідомлення, вкладене в IP-пакет. Оскільки шляхи LSP є односпрямованими, то це єдине гарантоване рішення, так як зворотного шляху від LSR8 до LSR1 може і не існувати.

На рис. 7.12 представлений випадок, коли з якоїсь причини шлях LSP пошкоджений на останній своїй ділянці (між пристроями LSR7 і LSR8).

У цій ситуації LSR7 не може відправити MPLS-кадр по призначенню, як того вимагає мітка 177, тому відкидає заголовок MPLS і намагається обробити кадр як IP-пакет. Як і в разі справного шляху, адреса 127.0.0.1 вимагає передачі пакета локальному стеку TCP/IP. Саме цього ефекту і домагалися розробники протоколу LSP Ping, вибираючи в якості адреси призначення цю спеціальну адресу. Вузол LSR7 обробляє повідомлення *Echo Request* і відправляє повідомлення *Echo Reply* вузлу LSR1 з інформацією про виявлену помилку.

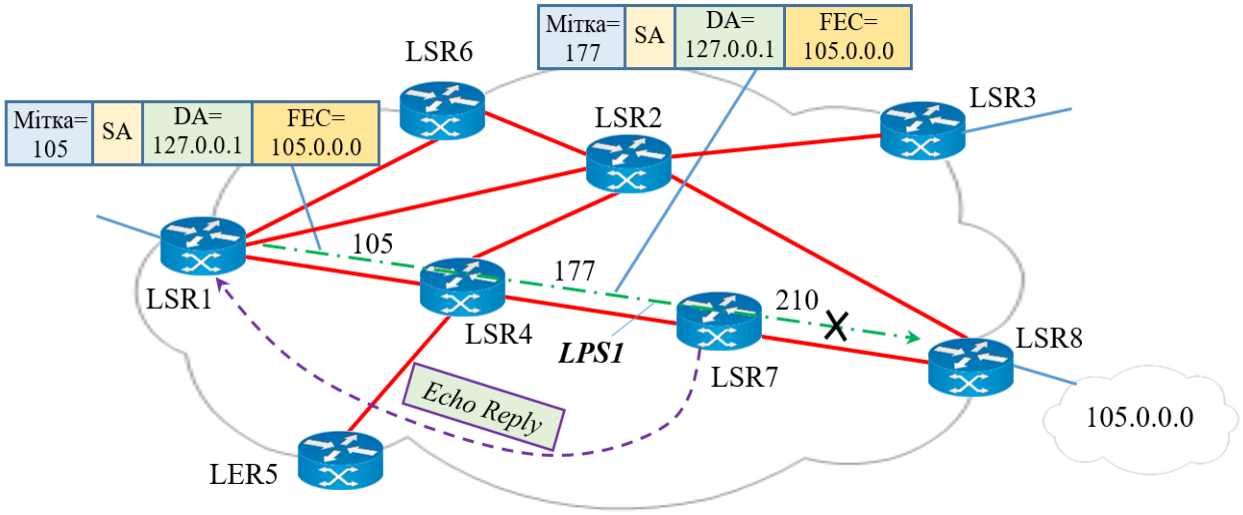



Рис. 7.12. Тестування несправного шляху LSP за допомогою протоколу LSP Ping

### 7.4.2. Трасування шляхів LSP

При несправному стані деякого відрізку шляху LSP повідомлення про помилку не завжди може бути відправлено проміжним пристроєм LSP. Можлива і така ситуація, коли відповідь на запит *Echo Request* просто не приходить – мережа «мовчить», наприклад, тому що відмовив проміжний вузол. Для того,

щоб локалізувати елемент мережі (вузол або з'єднання), який відмовив, протокол LSP Ping може працювати в режимі трасування шляху LSP. Цей режим аналогічний режиму роботи утиліти трасування стека TCP/IP, і в ньому використовується той же механізм, який полягає в надсиланні серії повідомлень *Echo Request* із монотонно зростаючим від 1 значенням поля TTL. Різниця полягає в тому, що це поле вказується не в IP-пакеті, як при використанні IP-утиліти трасування, а в заголовку MPLS (який також має поле TTL).

Подальша поведінка протоколу LSP Ping в режимі трасування – MPLS-кадр з нульовим значенням TTL передається «наверх» LSP Ping протоколу того проміжного вузла, який після вирахування одиниці з значення цього поля отримав нульовий результат. Протокол реагує на таку ситуацію надсиланням повідомлення *Echo Reply* початковому вузлу тестованого шляху.

### 7.4.3. Протокол двонаправленого виявлення помилок просування

Протокол **двонаправленого виявлення помилок просування** (Biderectional Forwarding Detection, **BFD**) розроблений як «полегшена» альтернатива протоколу LSP Ping для постійного моніторингу стану шляху LSP. Такий постійний моніторинг потрібно, наприклад, в тих випадках, коли основний шлях захищений резервним шляхом. Тобто необхідний якийсь механізм, який, з одного боку, може швидко виявити відмову шляху, а з іншого – не перевантажує мережу тестовими повідомленнями і трудомісткими перевірками. Протокол LSP Ping задовольняє першій умові, тобто може використовуватися для постійного тестування стану шляху за допомогою періодичної відправки повідомлень *Echo Request*. Однак обробка цих повідомлень кінцевим вузлом шляху досить трудомістка, тому що вимагає порівняння значення FEC в кожному вхідному запиті зі значенням з власної бази даних. Протокол BFD простіший, ніж LSP Ping. Однак, він не здатний локалізувати елемент мережі, що відмовив, а лише показує, працездатний деякий шлях LSP чи ні.

Протокол перевіряє стан з'єднання між двома вузлами в обох напрямках. Оскільки шляхи MPLS однонаправлені, то для роботи протоколу BFD необхідна пара шляхів LSP, що з'єднують два вузли в обох напрямках. Кожен з двох кінцевих вузлів, на яких для моніторингу певного шляху LSP розгорнуть протокол BFD, періодично посилає цим шляхом повідомлення *Hello*. Отримання повідомлень *Hello* від сусіда означає працездатність шляху в певному напрямку. Неотримання повідомлення *Hello* протягом певного часу означає відмову шляху в цьому напрямі, що і фіксує протокол BFD. Інформацію про відмову шляху можуть негайно використовувати інші протоколи стеку MPLS, наприклад протоколи захисту шляху.

Протокол BFD посилає повідомлення *Hello* в UDP-повідомленнях, які, в свою чергу, упаковуються в IP-пакети і забезпечуються заголовками MPLS. Протокол BFD може використовуватися не тільки для моніторингу шляхів MPLS, він розроблений як універсальний протокол тестування двонапрямлених з'єднань. Зазвичай, для ініціалізації сеансу BFD служить протокол LSP Ping, який переносить по шляху ідентифікатори сеансу BFD.

## 7.5. Відмовостійкість шляхів в MPLS

### 7.5.1. Загальна характеристика

MPLS підтримує кілька механізмів забезпечення відмовостійкості, або, в термінах SDH, механізмів *автоматичного захисного перемикання маршруту*, в разі відмови будь-якого елементу мережі: LSR інтерфейсу, лінії зв'язку або LSR в цілому.

У тому випадку, коли шлях встановлюється за допомогою протоколу LDP, існує єдина можливість захисту шляху – його відновлення за допомогою розподіленого механізму знаходження нового шляху засобами протоколів маршрутизації. Це той же механізм, який використовується в IP-мережах при відмові лінії або маршрутизатора. Час відновлення шляху залежить від протоколу маршрутизації і складності топології мережі, зазвичай це десятки секунд або кілька хвилин.

У тому випадку, коли шлях є TE-тунелем, в технології MPLS розроблено декілька механізмів його відновлення. Ці механізми ілюструє рис. 7.13, на якому показаний основний шлях LSP1, що з'єднує пристрої LSR1 і LSR8. Шлях LSP1 є TE-тунелем.

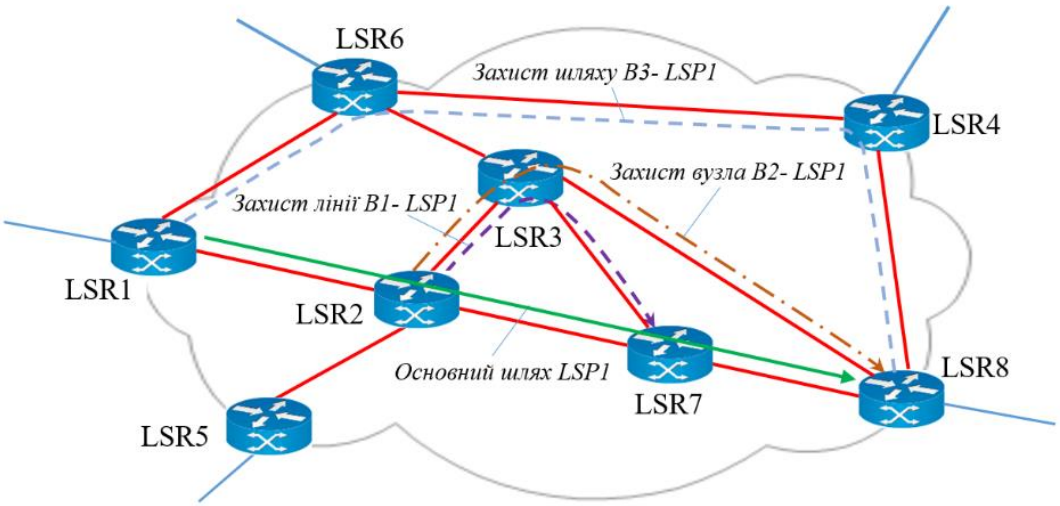



Рис. 7.13. Захисні механізми MPLS

- *Відновлення шляху його початковим вузлом* являє собою традиційне (за допомогою протоколу маршрутизації) повторне знаходження нового шляху, який обходить елемент мережі, що відмовив. Відмінність від відновлення шляху LDP полягає тільки в тому, що прокладанням нового шляху займається лише один вузол мережі, а саме початковий вузол шляху. У прикладі, це вузол LSR1.
- *Захист лінії* організовується між двома пристроями LSR, що безпосередньо з'єднані лінією зв'язку. Обхідний маршрут знаходиться заздалегідь, до відмови лінії, і заздалегідь прокладається між цими пристроями таким чином, щоб обійти лінію зв'язку в разі її відмови. У прикладі, такий варіант захисту встановлений для лінії, що з'єднує вузли LSR2 і LSR7. Обхідний шлях B1-LSP1 прокладений через вузол LSR3. Захист лінії є тимчасовим заходом, так як паралельно з початком використання обхідного шляху, початковий вузол основного шляху починає процедуру його відновлення за допомогою протоколу маршрутизації. Після відновлення основного шляху використання обхідного шляху припиняється. Тимчасовий захист лінії не гарантує TE-тунелю необхідну пропускну спроможність. Механізм захисту лінії працює дуже швидко, зазвичай час перемикання не перевищує 50 мс, тобто співрозмірно з часом перемикання мереж SDH. Тому механізм захисту лінії називають швидкою перемаршрутизацією (fast re-route).
- *Захист вузла* дуже подібний до захисту лінії, відрізняючись тим, що обхідний шлях прокладається таким чином, щоб обійти пристрій LSR, що відмовив (в нашому прикладі це пристрій LSR7). Всі інші характеристики аналогічні характеристикам захисту лінії. Захист вузла теж відноситься до механізмів швидкої перемаршрутизації і теж є тимчасовим заходом.
- *Захист шляху* організовується так, що на додаток до основного шляху в мережі прокладається резервний шлях, що зв'язує ті ж кінцеві пристрої, але проходить, по можливості, через пристрої LSR і лінії зв'язку, що не зустрічаються в основному шляху (на рисунку це резервний шлях B3-LSP1). Даний механізм є найбільш універсальним, але він працює повільніше, ніж механізми захисту лінії і вузла.

Для швидкого виявлення відмови основного шляху або його частини можуть використовуватися різні механізми і протоколи: повідомлення *Hello* протоколу RSVP, протокол LSP Ping або BFD.

### 7.5.2. Використання ієрархії міток для швидкого захисту

Розглянемо роботу швидких механізмів захисту на прикладі захисту лінії, яка представлена на рис. 7.14. Нехай для захисту лінії LSR2-LSR7 в мережі прокладений обхідний шлях B-LSP1. На основному шляху LSP1 для просування кадрів використовується послідовність міток 15, 17 і 21. На першій ділянці обхідного шляху B-LSP1 використовується мітка 7, на другому – мітка 8.

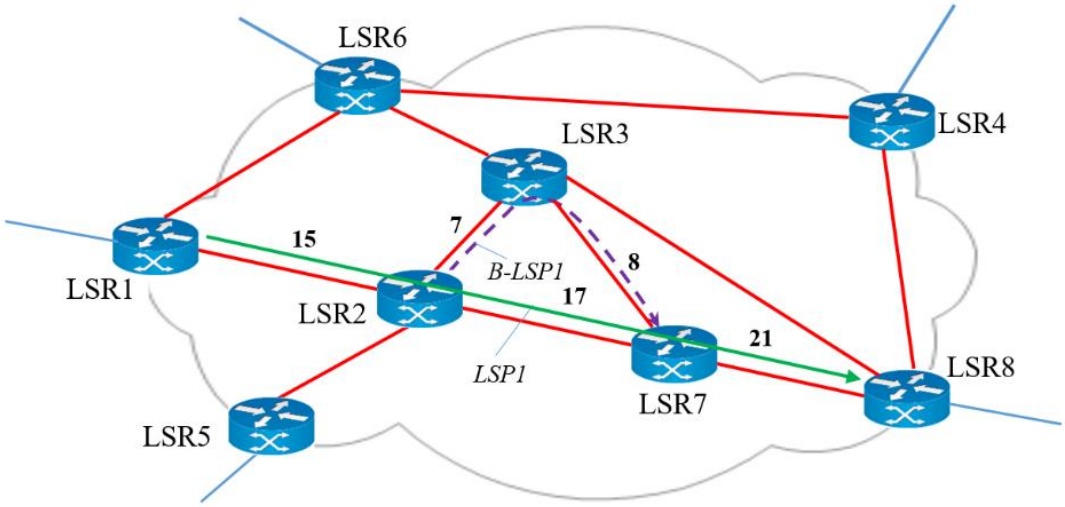



Рис. 7.14. Розподіл міток для основного шляху і обхідного шляху захисту лінії

При відмові лінії LSR2-LSR7 пристрій LSR2 починає спрямовувати в обхідний шлях B- LSP1 кадри, що надходять по шляху LSP1 (рис. 7.15). Однак, якщо при цьому поміняти мітку 15 на мітку 7, як того вимагає звичайна логіка комутації міток, то кадр прийде в пристрій LSR7 з міткою 8 (її встановить пристрій LSR3), що не відповідатиме значенню мітки 17, яка використовується в пристрої LSR7 для передачі кадрів по шляхи LSP1.

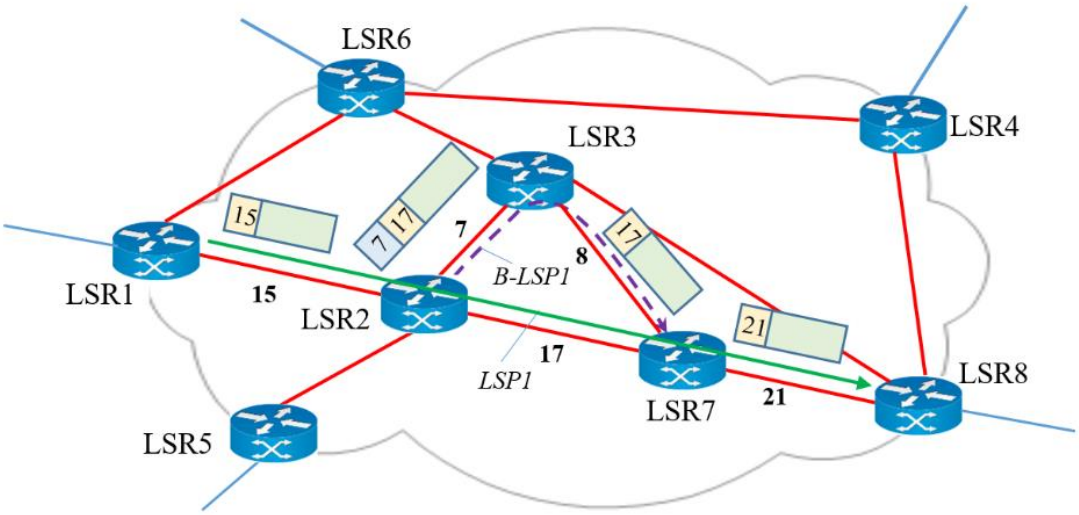



Рис. 7.15. Передача кадрів по обхідному шляху

Для того, щоб пристрій LSR7 працював при переході на обхідний шлях так само, як і при нормальній роботі основного шляху, в техніці швидкого захисту застосовується ієрархія міток. Для цього пристрій LSR2, який реалізує механізм захисту лінії, замінює у вхідному пакеті мітку 15 міткою 17, так ніби лінія LSR2-LSR7 залишалася працездатною. Потім пристрій LSR2 проштовхує мітку першого рівня в стек, а на вершину стеку поміщає мітку 7, яка потрібна для просування кадру по обхідному шляху.

Пристрій LSR3 є передостаннім пристроєм обхідного шляху. Тому він видаляє верхню мітку 7 і виштовхує на вершину стеку мітку 17. В результаті кадр надходить в комутатор LSR7 з міткою 17, що і потрібно для просування його далі по шляху LSP1.

Аналогічним чином працює механізм швидкого захисту вузла, в ньому також використовується ієрархія міток.

Таким чином, технологія MPLS вважається сьогодні багатьма фахівцями однієї з найбільш перспективних транспортних технологій. Головний принцип MPLS: протоколи маршрутизації використовуються для визначення топології мережі, а для просування даних всередині границь мережі одного постачальника послуг застосовується техніка віртуальних каналів. Об'єднання техніки віртуальних каналів з функціональністю стека TCP/IP здійснюється за рахунок того, що один і той же мережевий пристрій, який називається комутуючим по мітках маршрутизатором (LSR), виконує функції як IP-маршрутизатора, так і комутатора віртуальних каналів.

## 7.6. Технологія GMPLS

Технологія **узагальненої мультипротокольної комутації по мітках** (Generalized Multi-Protocol Switching, **GMPLS**) використовує концепцію й протоколи, розроблені для MPLS, однак принцип комутації за мітками тут поширено також на оптичні мережі. Технологію GMPLS розроблено технічною комісією Інтернету (IETF).

У GMPLS, разом з міткою, необхідно передавати інформацію про її тип, тому що у якості міток можуть використовуватися різні компоненти: довжина хвилі, номер оптичного волокна в каналі, номер SDH-контейнера та ін. На даний момент базовими типами міток є:

- *Packet* – мітка, яка ідентифікує Ethernet (1G Ethernet, Fast Ethernet);
- *PDH* – мітка, яка ідентифікує кадри (T1, E1, E3);
- *SONET/SDH* – мітка, яка ідентифікує контейнери SDH (STM-n);
- *Digital Wrapper* – мітка OTN G.709 (2,5, 10, 40, 100 Гбіт/с);
- λ – довжина хвилі при використанні фотонних комутаторів;

- *Fiber* – мітка, яка ідентифікує номер оптичного волокна;
- *Fiber Channel* – мітка, яка ідентифікує оптичний канал.

Технологія GMPLS має ряд переваг:

- можливість налаштовувати та обслуговувати з'єднання, які організовуються скрізь різні технологічні рівні мережі;
- автоматичне розпізнавання мережевих ресурсів;
- автоматична інвентаризація (відстеження зміни та облік) мережевих ресурсів;
- реалізація інтелектуальних захисних механізмів.

GMPLS охоплює весь комплекс комутаційних можливостей – від комутації пакетів до комутації оптичних волокон через IP-маршрутизатори, Ethernet-комутатори, оптичні мультиплексори вводу/виводу, закінчення систем WDM. Дана технологія еволюціонувала від MPLS і базується на тих самих протоколах маршрутизації та сигналізації. Тим самим забезпечується гнучка взаємодія між традиційними та новоствореними магістральними інфраструктурами.

Розширені можливості QoS у GMPLS дають змогу ефективно передавати через єдину мережу повідомлення з різними класами сервісу, такі, як голос, відео та дані з їх специфічними вимогами до затримок. Гнучке та ефективне мережеве управління, запропоноване GMPLS, дозволяє швидке й просте долучення нових транспортних послуг.

# 8. Мережі доступу

## 8.1. Архітектура мереж доступу

Призначення мереж доступу, в загальному випадку, полягає у формуванні агрегованих інформаційних потоків, спрямованих користувачами в транспортну мережу з максимальною концентрацією їх у вузлах доступу, й розподіленні потоку, який надходить з транспортної мережі, між кінцевими користувачами з урахуванням конкретних запитів кожного.

З точки зору користувача, мережі доступу та транспортні мережі є лише засобом отримання телекомунікаційних та інформаційних послуг. При цьому, основні вимоги щодо надання таких видів послуг, як передавання голосу, даних і відеоінформації висувають саме до мереж доступу.

Узагальнену архітектуру та модель мережі доступу визначено ITU-T у Рекомендації G.902. На рисунках 8.1 наведено узагальнену архітектуру мережі доступу, описану в цій рекомендації.

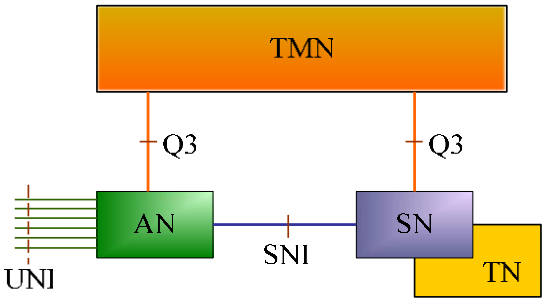



Рис. 8.1. Узагальнена архітектура мережі доступу

Елементами узагальненої архітектури мережі доступу є:

- **TMN** (Telecommunication Management Network) – мережа керування телекомунікаціями;
- **UNI** (User-Network Interface) – інтерфейс «користувач-мережа»;
- **AN** (Access Network) – мережа доступу;
- **SNI** (Service Node Interface) – інтерфейс сервісного вузла;
- **SN** (Service Node) – сервісний вузол;
- **TN** (Transport Network) – транспортна мережа;
- **Q3** – інтерфейс керування.

На мережу керування телекомунікаціями TMN покладено завдання підтримувати функціональність усіх елементів мережі, що здійснюється шляхом

постійного контролювання інтерфейсом Q3 операційних систем, конфігурації та координації ресурсів, контролювання безпеки. Опції повномасштабного керування повинні охоплювати мережі доступу різних операторів на великих територіях (у межах міст, областей).

Мережа доступу AN присутня в даній архітектурі як сегмент телекомунікаційної мережі, що забезпечує доступ користувачів до сервісного вузла SN. Її функціями є концентрація каналів користувачів, мультиплексування сигнальної і пакетної інформації, контролювання та керування.

Транспортна мережа TN забезпечує можливість доступу до різних сервісних вузлів.

Функціями інтерфейсів користувачів UNI є: під'єднання терміналів користувачів; аналогово-цифрове та цифро-аналогове перетворення; перетворення сигналів (інтерфейсів); активація/дезактивація UNI; тестування; контроль, керування та обслуговування.

Прикладами функцій інтерфейсів сервісних вузлів SNI є: під'єднання мереж доступу до сервісних вузлів; концентрація функцій контролю, керування, обслуговування в мережах доступу; тестування, управління, контроль та обслуговування інтерфейсів.

Типами сервісних вузлів SN є: вузли телефонного зв'язку, вузли N-ISDN та B-ISDN, вузли виділених ліній, вузли пакетної комутації, вузли відео- та радіопрограм аналогового мовлення, вузли відео та радіопрограм цифрового мовлення, вузли Інтернет.

На рисунку 8.2 показано узагальнену модель мережі доступу, в якій відображено її основні ділянки, елементи, блоки та системи.

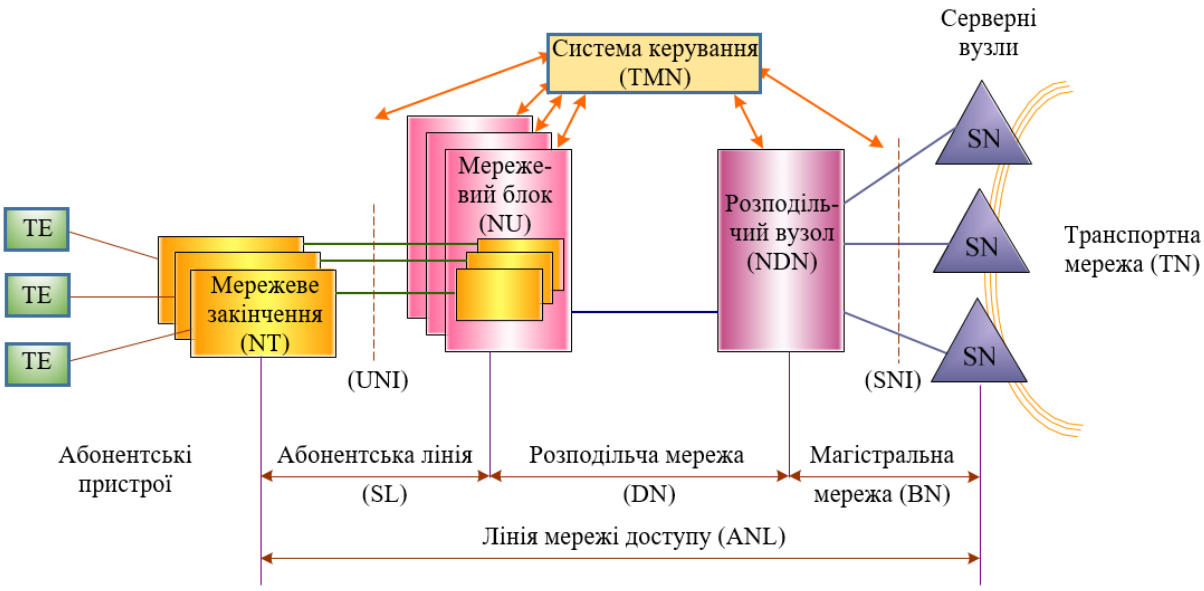



Рис. 8.2. Модель мережі доступу

На цій моделі мережа доступу є сукупністю абонентських ліній та обладнання мережі, які забезпечують доступ абонентських терміналів до транспортної мережі. Мережеве закінчення (Network Termination, **NT**) дає змогу під'єднати один або декілька користувацьких терміналів (Termination Equipment, **TE**).

Доступ абонентських пристроїв TE до **сервісних вузлів** (Service Node, **SN**) здійснюється через **мережевий блок** (Network Unit, **NU**), в якому відбувається мультиплексування і комутація трафіку, та через розподільчий вузол (Distribution Node, **DN**).

**Лінія мережі доступу** (Access Network Line, **ANL**) – це лінія, яка з'єднує мережеве закінчення NT з сервісним вузлом SN і проходить через усю мережу доступу. Вона може бути утворена фізичним каналом (аналоговим або цифровим), комутованим каналом, віртуальним каналом або декількома каналами для надання різних послуг.

ANL проходить через абонентську лінію **SL** (Subscriber Line), розподільчу мережу **DN**, та **магістральну (транспортну) мережу** (Backbone Network, **BN).**

## 8.2. Проблеми «останньої милі»

Організація віддаленого доступу є однією з найбільш гострих проблем комп'ютерних мереж. Вона отримала назву проблеми останньої милі, де під останньою милею мається на увазі відстань від **точки присутності** (Point of Presence, **POP**) оператора зв'язку до приміщень клієнтів. Складність цієї проблеми визначається декількома факторами. З одного боку, сучасним користувачам необхідний доступ, що забезпечує якісну передачу трафіку будь-якого типу, в тому числі даних, голосу, відео. Для цього потрібні швидкості в кілька Мбіт/с, а для якісного прийому телевізійних програм – в кілька десятків Мбіт/с. З іншого боку, переважна більшість будинків у великих і малих містах і особливо в сільській місцевості, як і раніше з'єднані з POP абонентськими закінченнями телефонної мережі, які не були розраховані на передачу комп'ютерного трафіку.

Сьогодні існує ряд технологій, здатних надавати послуги швидкісного віддаленого доступу на основі існуючої інфраструктури абонентських закінчень – телефонних мереж або мереж кабельного телебачення. Ці технології, що забезпечують швидкість від декількох сотень Кбіт/с до декількох десятків Мбіт/с, використовують наступний прийом: після досягнення POP комп'ютерні дані вже не проходять по телефонній мережі або мережі кабельного телебачення, а відгалужуються за допомогою спеціального обладнання в мережу передачі даних. Це дозволяє подолати обмеження на смугу пропускання, що відводиться

абоненту в телефонній мережі або в мережі кабельного телебачення, і підвищити швидкість доступу.

Найбільш популярними технологіями такого типу є технологія ADSL, що використовує телефонні абонентські закінчення, і кабельні модеми, що працюють поверх мережі кабельного телебачення.

Застосовуються також різні бездротові технології доступу, що забезпечують як фіксований, так і мобільний доступ. Набір таких бездротових технологій дуже широкий, в нього входять бездротові мережі Ethernet (802.11), супутникові технології, передача даних по мережі мобільної телефонії, а також технології фіксованого доступу, наприклад стандарту 802.16.

На рис. 8.3 показано методи організації віддаленого доступу в телекомунікаційній мережі. Приміщення клієнтів можуть бути з'єднані з найближчою точкою доступу оператора зв'язку різними способами: за допомогою аналогового або цифрового закінчення телефонної мережі, телевізійного кабелю, бездротового зв'язку. Оператор зв'язку може мати різну спеціалізацію, тобто бути або постачальником телефонних послуг, або постачальником послуг Інтернету, або оператором кабельного телебачення. Або ж він може бути універсальним оператором, що надає весь спектр послуг і володіє власними мережами всіх типів.

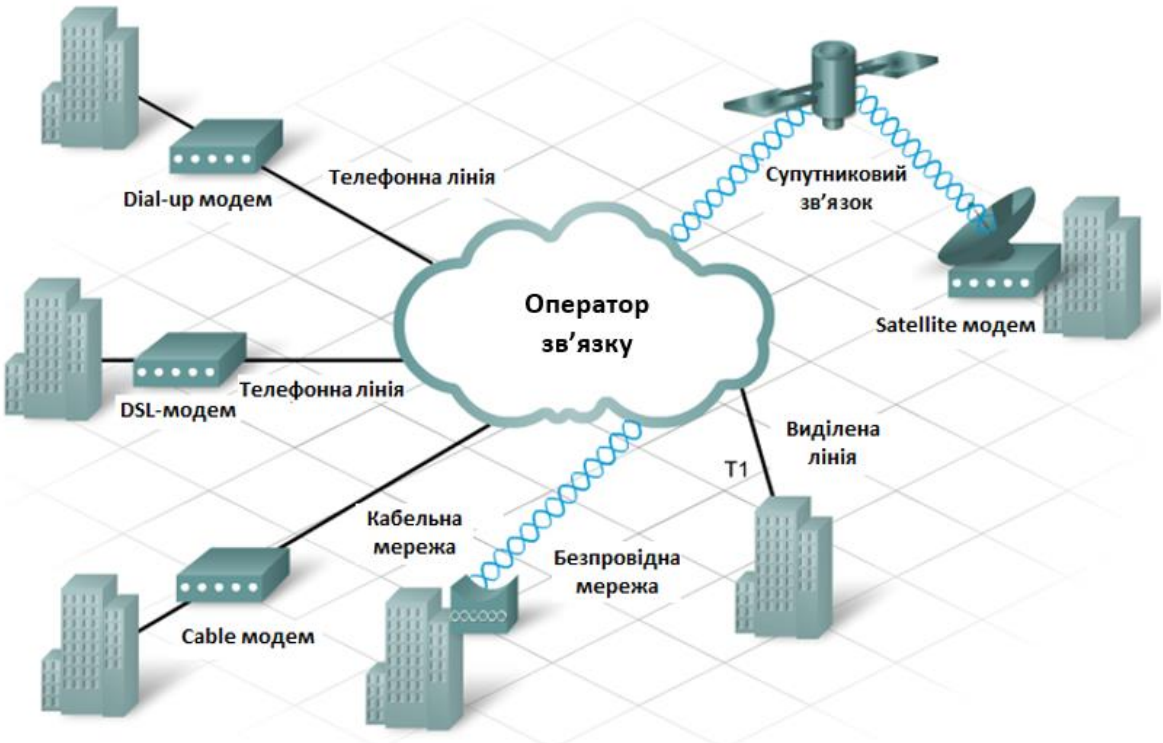



Рис. 8.3. Методи організації віддаленого зв'язку

## 8.3. Комутований аналоговий доступ

Технології з аналоговою комутацією каналів базуються на використанні звичайної телефонної мережі, яка є найбільшою глобальною мережею в світі (рис. 6.4). В англомовній літературі такі мережі іноді називають **традиційними телефонними мережами** (Plain Old Telephone Service, **POTS**), або ж **публічними комутованими телефонними мережами** (Public Switched Telephone Network, **PSTN**).

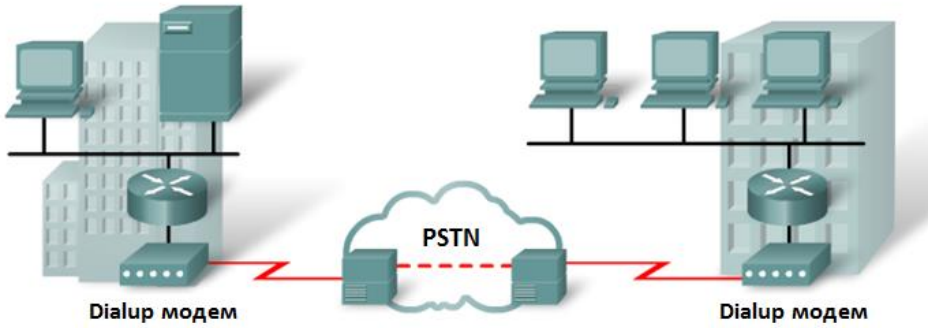



Рис. 8.4. Аналогова мережа з комутацією каналів

Основна ідея комутованого аналогового доступу полягає в тому, щоб задіяти наявну телефонну мережу для комутованого з'єднання між комп'ютером домашнього користувача і **сервером віддаленого доступу** (Remote Access Server, **RAS**), встановленим на кордоні телефонної та комп'ютерної мереж. Комп'ютер користувача підключається до телефонної мережі за допомогою **комутованого модему** (dial-up modem), який підтримує стандартні процедури набору номера і імітує роботу телефонного апарату для підтримання зв'язку з RAS.

Для телефонної мережі модеми є термінальними пристроями, які виконують стандартну процедуру модуляції/демодуляції сигналу (рис. 8.5).

Аналогові мережі можуть використовувати аналогову (FDM) або цифрову (TDM) комутацію, але в них абонент завжди під'єднаний по аналоговому двопровідному закінченню.

Перші телефонні мережі були повністю аналоговими, так як в них абонентський пристрій (телефонний апарат) перетворював звукові коливання, які є аналоговими сигналами, в коливання електричного струму (також аналогові сигнали). Комутатори телефонної мережі теж передавали інформацію користувача в аналоговій формі, переносячи ці сигнали в іншу область частотного спектра за допомогою методів частотного ущільнення (FDM).

Сьогодні в телефонних мережах голос між комутаторами, в основному, передається в цифровій формі по каналах PDH/SDH за допомогою технології TDM.

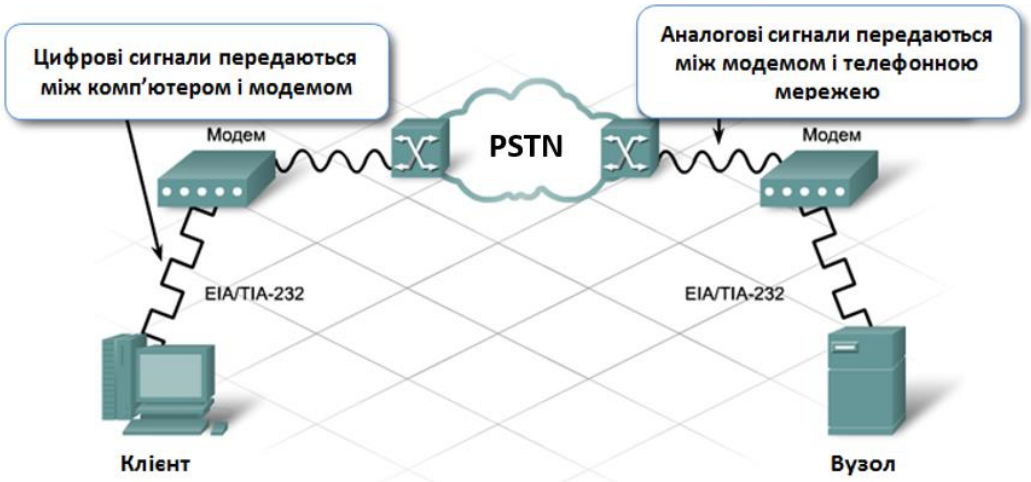



Рис. 8.5. Використання комутованих модемів

Типова схема організації доступу через аналогову телефонну мережу представлена на рис. 8.6. Мережа утворена деякою кількістю телефонних комутаторів, які з'єднані між собою цифровими або, в окремих випадках, аналоговими каналами. Топологія зв'язків між телефонними комутаторами в загальному випадку носить довільний характер, хоча часто має місце багаторівнева ієрархія, коли кілька комутаторів нижнього рівня підключаються до комутатора більш високого рівня і т. п.

До комутаторів нижнього рівня за допомогою мідних пар дротів, під'єднуються телефонні апарати абонентів. Зазвичай довжина абонентського закінчення не перевищує одного-двох кілометрів, проте іноді оператор змушений використовувати і більш протяжні закінчення, до 5-6 км, якщо є кілька віддалених абонентів, для яких будівництво окремої точки присутності економічно невиправдано.

Телефонна мережа, як і будь-яка мережа з комутацією каналів, вимагає обов'язкової процедури попереднього встановлення з'єднання між абонентськими пристроями. У разі успіху цієї процедури в мережі встановлюється канал між абонентами, через який вони можуть вести розмову. Операції підключення реалізується за допомогою сигнального протоколу. В аналогових телефонних мережах кожному абонентському з'єднанню виділяється смуга пропускання шириною в 4 кГц. З цієї смуги 3,1 кГц призначається для передачі голосу, а інші 900 Гц – для передачі сигнальної інформації між аналоговими комутаторами, а також в якості захисної смуги частот між

каналами, що виділені різним користувачам.

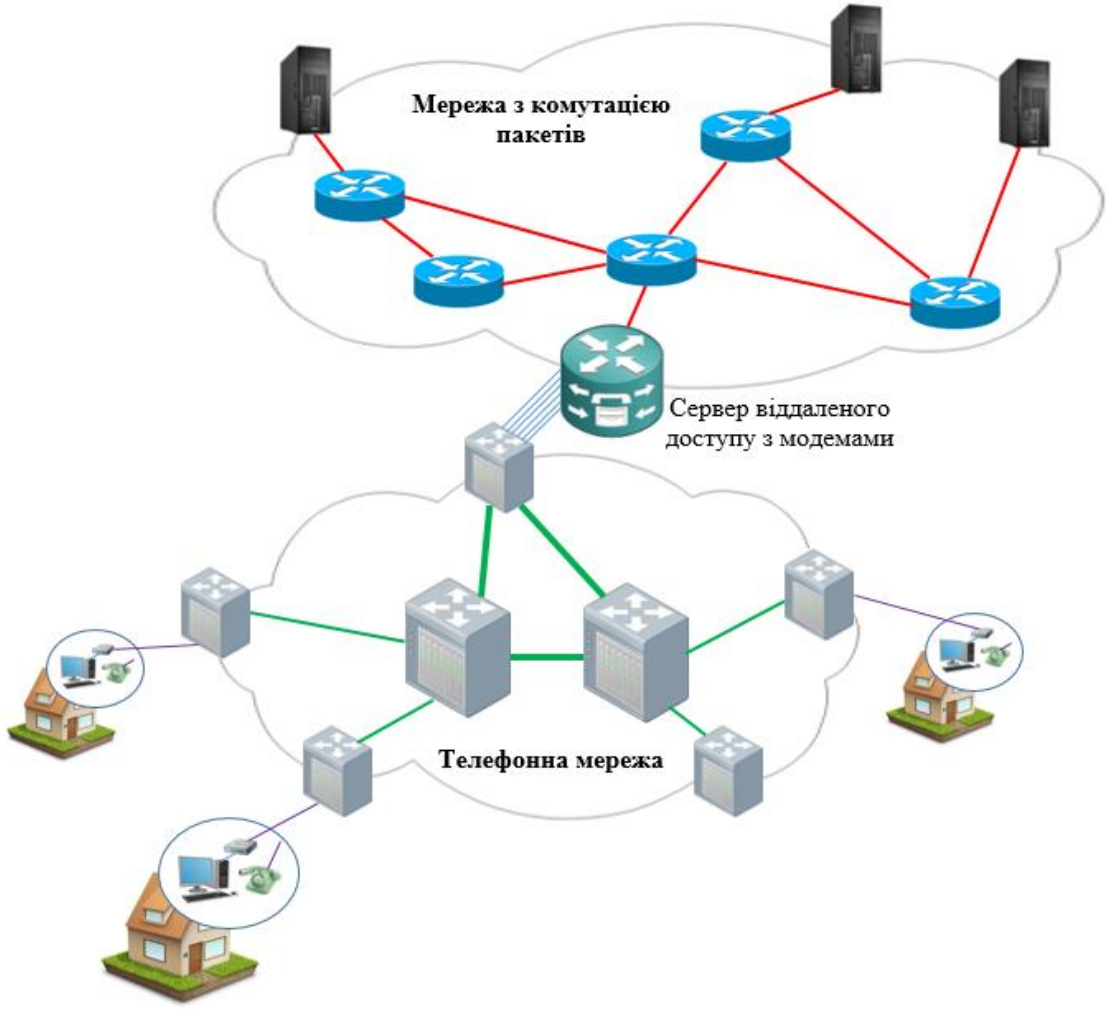



Рис. 8.6. Метод доступу через телефонну мережу з аналоговим закінченням

Існує велика кількість сигнальних протоколів, розроблених за довгі роки існування телефонних мереж. Вони діляться на два класи: сигнальні протоколи UNI працюють між телефоном користувача і першим комутатором мережі, а сигнальні протоколи NNI – між комутаторами мережі. Оскільки модем під'єднується до телефонної мережі в якості абонентського пристрою, то він повинен підтримувати тільки протокол UNI.

Сучасні телефонні комутатори використовують протоколи **сигнальної системи 7** (Signaling System 7, **SS7**), в яких застосовується техніка комутації пакетів. Ці протоколи побудовані відповідно до моделі OSI, описуючи рівні від фізичного до прикладного. Слід зауважити, що користувацькі дані передаються в телефонних мережах за допомогою техніки комутації каналів, а техніка комутації пакетів використовується сигнальними протоколами лише для встановлення з'єднання. Поряд з протоколами SS7 в телефонній мережі може

бути задіяний велика кількість старіших сигнальних протоколів, в тому числі аналогових.

Сервер RAS має два типи з'єднання: з телефонною мережею через пул модемів і з локальною IP-мережею, під'єднаною до Інтернету. Для телефонної мережі RAS і модеми клієнтів є звичайними користувачами. Модеми RAS, зазвичай, встановлюються в точці присутності постачальника послуг.

Для того, щоб отримати доступ в Інтернет або корпоративну мережу через телефонну мережу, модем користувача повинен виконати виклик по одному з номерів, які присвоєнні модемам, що знаходяться на сервері віддаленого доступу RAS. Після встановлення з'єднання між модемами в телефонній мережі утворюється канал з пропускною здатністю близько 4 кГц. Точне значення ширини смуги залежить від типу телефонних комутаторів на шляху від модему користувача до модему RAS і від підтримуваних ними сигнальних протоколів. У будь-якому випадку, ця смуга не перевищує 4 кГц, що принципово обмежує швидкість передачі даних модемом.

Після того, як модем встановить з'єднання з RAS, телефонна лінія стає недоступною для телефону користувача, оскільки модем займаю своїм сигналом всю доступну смугу пропускання лінії.

Найвищою швидкістю сучасних модемів на каналі тональної частоти є швидкість 33,6 Кбіт/с у випадку, коли на шляху проходження інформації необхідно робити хоча б одне аналого-цифрове перетворення, і 56 Кбіт/с у випадку, коли інформація піддається тільки цифро-аналоговому перетворенню. Така асиметрія викликана тим, що аналого-цифрове перетворення більше спотворює дані, ніж цифро-аналогове. Очевидно, що такі швидкості не можна назвати прийнятними для більшості сучасних додатків, які широко використовують мультимедійні форми представлення даних.

Якщо метою користувача є доступ не в Інтернет, а в корпоративну мережу, то він використовує Інтернет як проміжну мережу, що веде до корпоративної мережі (також з підключенням до Інтернету). Оскільки плата за доступ в Інтернет не залежить від відстані до вузла призначення, віддалений доступ до ресурсів корпорації став сьогодні набагато дешевше навіть з урахуванням оплати за локальний телефонний дзвінок і доступ в Інтернет. Однак, при такій двоступеневій схемі доступу користувачу доводиться виконувати автентифікацію двічі – при доступі до RAS постачальника послуг і при доступі до RAS підприємства. Існують протоколи, які виключають подібне дублювання, наприклад **двоточковий протокол тунелювання** (Point-to-Point Tunneling Protocol, **PPTP**). При роботі PPTP сервер віддаленого доступу постачальника послуг передає транзитом запит користувача серверу автентифікації підприємства і, в разі позитивної відповіді з'єднує користувача через Інтернет з

корпоративною мережею.

RAS може під'єднуватись до телефонного комутатора за допомогою як аналогових, так і цифрових закінчень.

## 8.4. Комутований доступ через мережі ISDN

Мережі **ISDN** (Integrated Services Digital Network – **цифрова мережа інтегрованих послуг**) з'явилися в 70-х роках XX ст. Власники провідних телефонних компаній світу дійшли висновку, що подальший розвиток аналогової телефонії безперспективний. Крім того, часто виникали потреби передавання даних з високою швидкістю та надійністю. З цією метою було розроблено концепцію побудови всесвітньої цифрової мережі, яка повинна була прийти на зміну телефонної мережі і, будучи такою ж доступною і поширеною, надавати мільйонам своїх користувачів різноманітні послуги, як телефонні, так і передачі даних. Передача телевізійних програм по мережі ISDN не передбачалась, було вирішено обмежитися пропускною спроможністю абонентського закінчення для масових користувачів в 128 Кбіт/с і 2 Мбіт/с для корпоративних користувачів.

З багатьох причин впровадження ISDN відбувалося дуже повільно. Головною перешкодою на шляху поширення ISDN стала необхідність організації **цифрового абонентського закінчення** (Digital Subscriber Line, **DSL**), що вимагало модернізації мільйонів абонентських закінчень. В результаті процес, який почався в 80-і роки, розтягнувся більше ніж на десять років, так що до моменту появи в будинках користувачів в 90-і роки абонентських закінчень ISDN послуги цієї мережі просто морально застаріли. Швидкість доступу 128 Кбіт/с вже тоді була недостатньою для багатьох користувачів, а послуги зі швидкістю 2 Мбіт/с були дуже дорогими. В результаті інтерес до технології ISDN послабився, оскільки вона виявилася досить дорогою та складною при інсталяції.

Базовою швидкістю мережі ISDN є швидкість каналу DS-0, тобто 64 Кбіт/с.

Однією з оригінальних ідей, покладених в основу ISDN, є спільне використання принципів комутації каналів і пакетів. Однак, мережа з комутацією пакетів, що працює в складі ISDN, виконує тільки службові функції – з її допомогою передаються повідомлення сигнального протоколу. А ось основна інформація, тобто сам голос, як і раніше передається через мережу з комутацією каналів.

Інтерфейс абонента ISDN базується на каналах двох типів: B і D.

**Канали типу B** забезпечують передачу даних користувача (оцифрованого голосу, комп'ютерних даних або поєднання голосу і даних). Канали типу B

можуть мати постійне з'єднання, а також утворювати напівпостійні з'єднання, які еквівалентні з'єднанням каналів звичайної телефонної мережі.

**Канал типу D** є каналом доступу до службової мережі з комутацією пакетів, яка здійснює передавання сигнальної інформації зі швидкістю 16 або 64 Кбіт/с. Передача адресної інформації, на основі якої здійснюється комутація каналів типу B в комутаторах мережі, є основною функцією каналу D. Іншою його функцією є підтримка сервісу низькошвидкісної мережі з комутацією пакетів для користувацьких даних. Зазвичай, цей сервіс виконується мережею в той час, коли канали типу D вільні від виконання основної функції.

Інтерфейс ISDN являє собою набір логічних каналів певного типу і з певними швидкостями. Мережа ISDN підтримує два види інтерфейсу користувача (рис. 8.7):

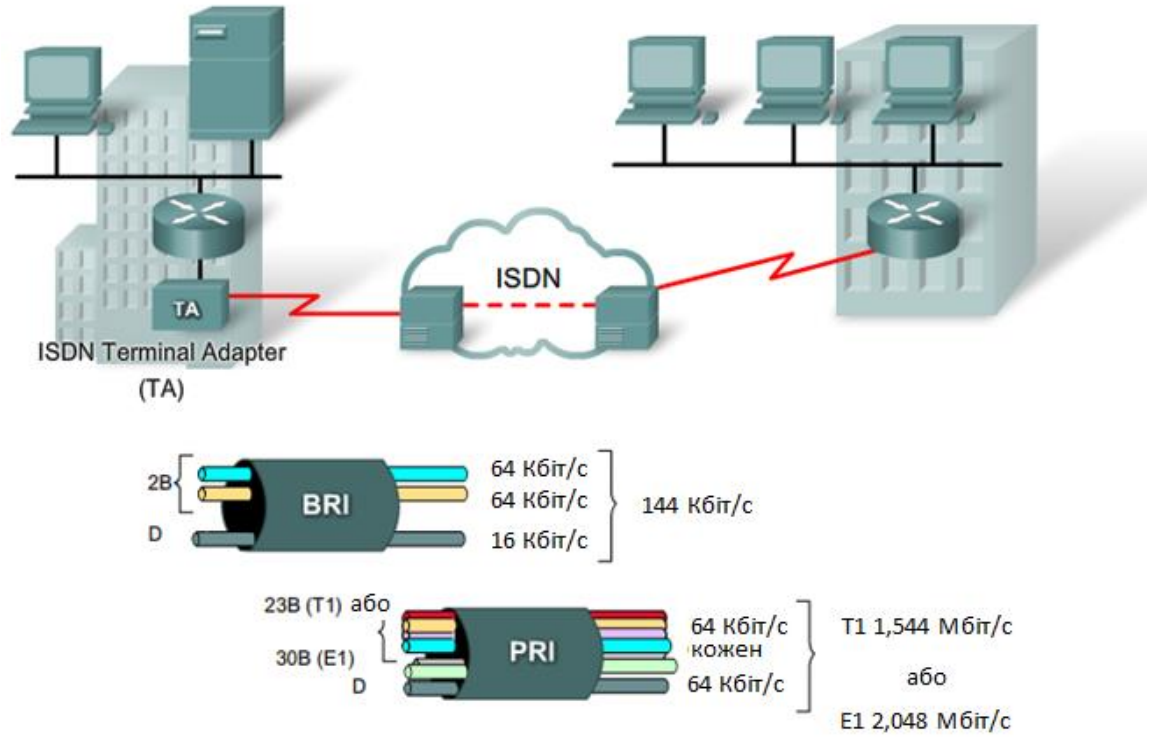



Рис. 8.7. Види інтерфейсів мережі ISDN

**Початковий інтерфейс** (Basic Rate Interface, **BRI**) ISDN надає користувачу два канали по 64 Кбіт/с для передачі даних (канали типу B) і один канал з пропускною спроможністю 16 Кбіт/с для передачі керуючої інформації (канал типу D). За задумом розробників технології ISDN, один канал типу B користувач може задіяти для підключення цифрового телефону, а другий – для підключення комп'ютера.

**Основний інтерфейс** (Primary Rate Interface, **PRI**) ISDN призначений для

користувачів з підвищеними вимогами до пропускної здатності мережі. PRI повністю використовує лінію T1 (в Північній Америці) з 23 B-каналами та одним D-каналом (по 64 Кбіт/с кожен) чи E1 (в Європі) з 30 B-каналами та одним D-каналом (по 64 Кбіт/с кожен). Максимальна сумарна перепускна здатність PRI 2,048 Мбіт/с (європейський варіант) або 1,544 Мбіт/с (американський варіант).

Протоколи ISDN визначаються набором стандартів ITU-T, що належать до фізичного, канального та мережевого рівнів моделі OSI.

Незважаючи на значні відмінності від аналогових телефонних мереж, мережі ISDN використовуються для організації віддаленого доступу в основному так само, як аналогові телефонні мережі, тобто як мережі з комутацією каналів, але тільки більш швидкісні. Якість цифрових каналів набагато вище, ніж аналогових, а отже, істотно нижчий відсоток спотворених кадрів і значно вища корисна швидкість обміну даними.

Зазвичай інтерфейс BRI використовується для під'єднання окремих комп'ютерів або невеликих локальних мереж домашніх користувачів, а інтерфейс PRI – для під'єднання мережі середніх розмірів.

Схема віддаленого доступу через ISDN показана на рис. 8.8.

Для віддаленого доступу необхідно оснастити комп'ютери користувачів **термінальними адаптерами** (Terminal Adapter, **TA**), а в POP встановити маршрутизатор, який має один або кілька інтерфейсів PRI. В цьому випадку максимальна швидкість доступу для окремого користувача буде дорівнює швидкості передачі двох каналів типу B, тобто 128 то Кбіт/с. Драйвери TA ISDN вміють об'єднувати два окремих фізичних каналу типу B в один логічний канал. Для цього служить розширення протоколу PPP – **багатоканальний протокол PPP** (Multilink PPP, **MLPPP**). Якщо користувач віддаленого доступу згоден обмежитися швидкістю 64 Кбіт/с, він може задіяти другий канал типу B свого інтерфейсу BRI для паралельної роботи телефону ISDN, що неможливо зробити при застосуванні аналогового комутованого модему.

## 8.5. Технології DSL

Технологія **асиметричного цифрового абонентського закінчення** (Asymmetric Digital Subscriber Line, **ADSL**) була розроблена для забезпечення швидкісного доступу в Інтернет масових індивідуальних користувачів, квартири яких оснащені звичайними абонентськими телефонними закінченнями. Поява технології ADSL можна вважати революційною подією для масових користувачів Інтернету, тому що для них це означало підвищення швидкості доступу в десятки разів без зміни кабельної проводки в квартирі та будинку.

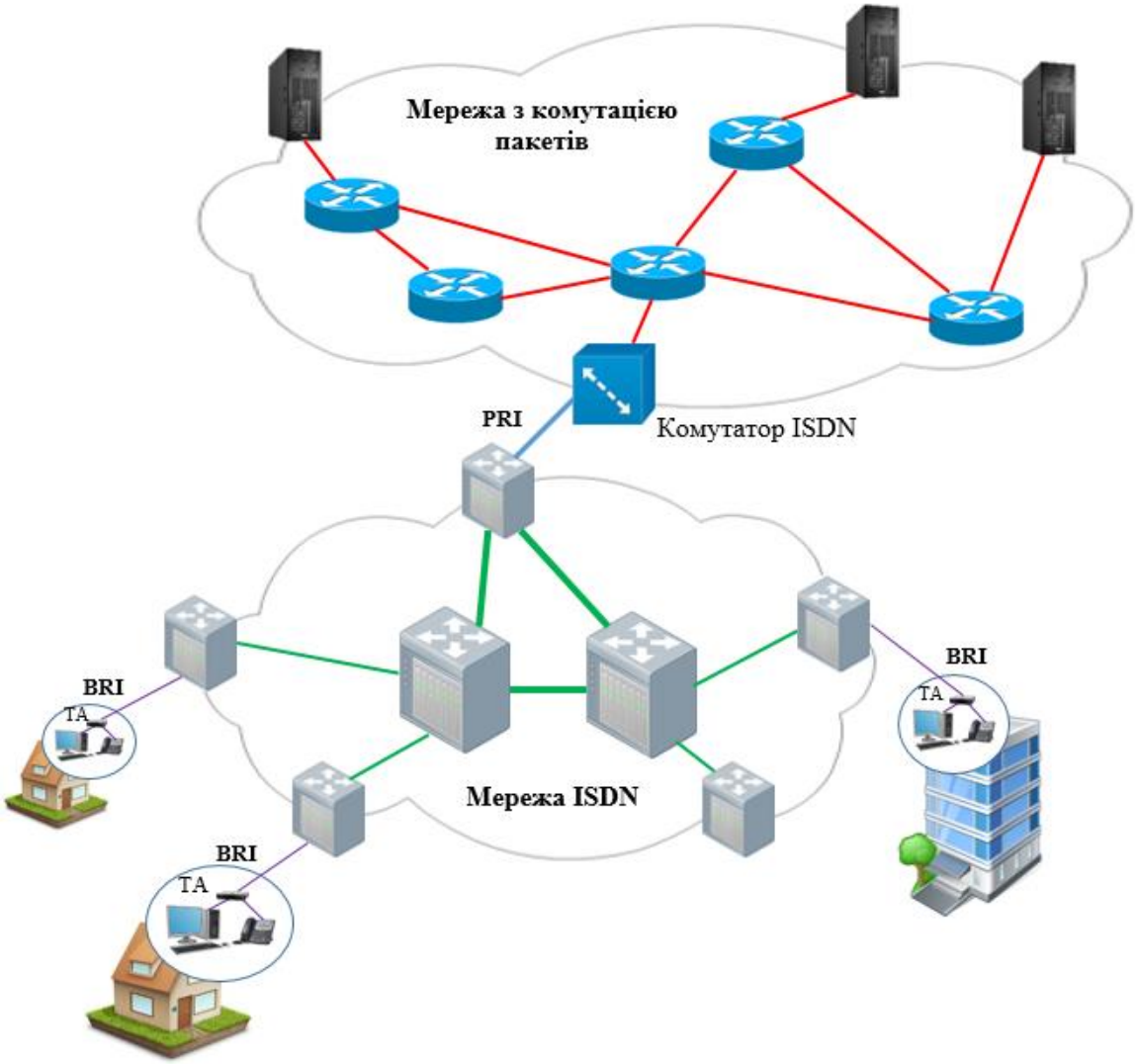



Рис. 8.8. Метод доступу через мережу ISDN

Для підключення абонентів до WAN постачальники послуг Інтернету повинні співпрацювати з постачальниками послуг телефонних мереж (часто це один оператор). Для доступу через ADSL, так само як і для аналогового комутованого доступу, потрібні телефонні абонентські закінчення і модеми. З'єднання абонентів з глобальною мережею здійснюється через **мультиплексор доступу до цифрового абонентського закінчення** (Digital Subscriber Line Access Multiplexer, **DSLAM**) (рис. 8.9). Для підключення до глобальної мережі у нього використовуються WAN-порти, а для підключення клієнтів – **DSL-модеми** (DSL modems), до яких підключається абонентська лінія.

Принциповою відмінністю доступу через ADSL від комутованого доступу є те, що ADSL-модеми працюють тільки в межах абонентського закінчення, в той час як комутовані модеми використовують можливості телефонної мережі, встановлюючи в ній з'єднання «з кінця в кінець», яке проходить через кілька транзитних комутаторів.

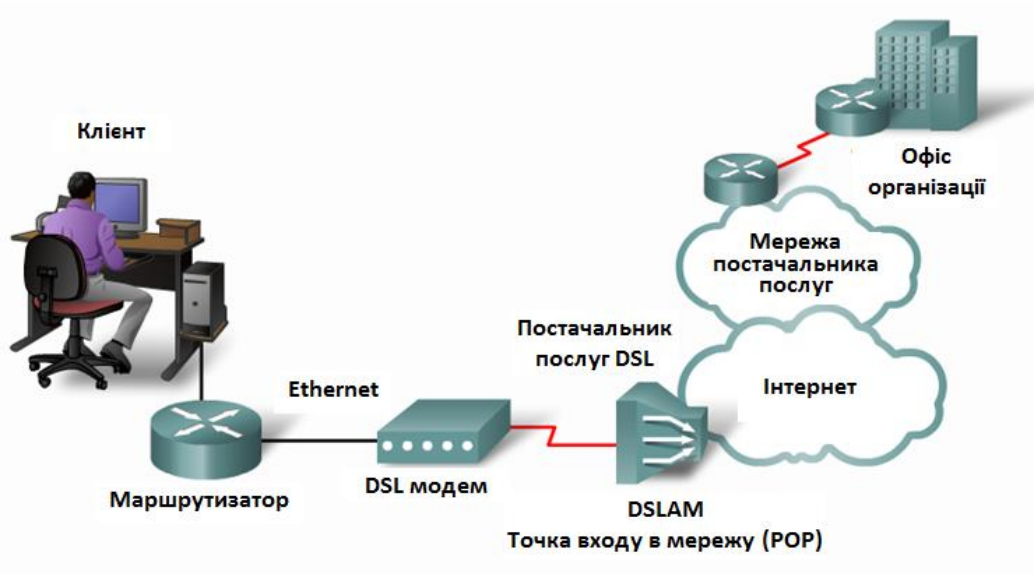



Рис. 8.9. Технологія DSL

Тому, якщо традиційні телефонні модеми (наприклад, V.34, V.90) повинні забезпечувати передачу даних на каналі з пропускною здатністю 3100 Гц, то ADSL-модеми отримують в своє розпорядження смугу пропускання близько 1 МГц – ця величина залежить від довжини кабелю, прокладеного між приміщенням користувача і POP, і січення проводів цього кабелю.

Схема доступу через ADSL показана на рис. 8.10. Ця схема близька до загальної схеми використання універсального абонентського закінчення за виключення того, що при доступі через ADSL факт наявності телевізорів у користувачів ігнорується, а доступ для телефонів і комп'ютерів є спільним.

ADSL-модеми, що підключаються до обох кінців короткої лінії між абонентом і POP, утворюють три канали: високошвидкісний спадний канал передачі даних з мережі в комп'ютер, менш швидкісний висхідний канал передачі даних з комп'ютера в мережу і канал телефонного зв'язку, по якому передаються звичайні телефонні розмови.

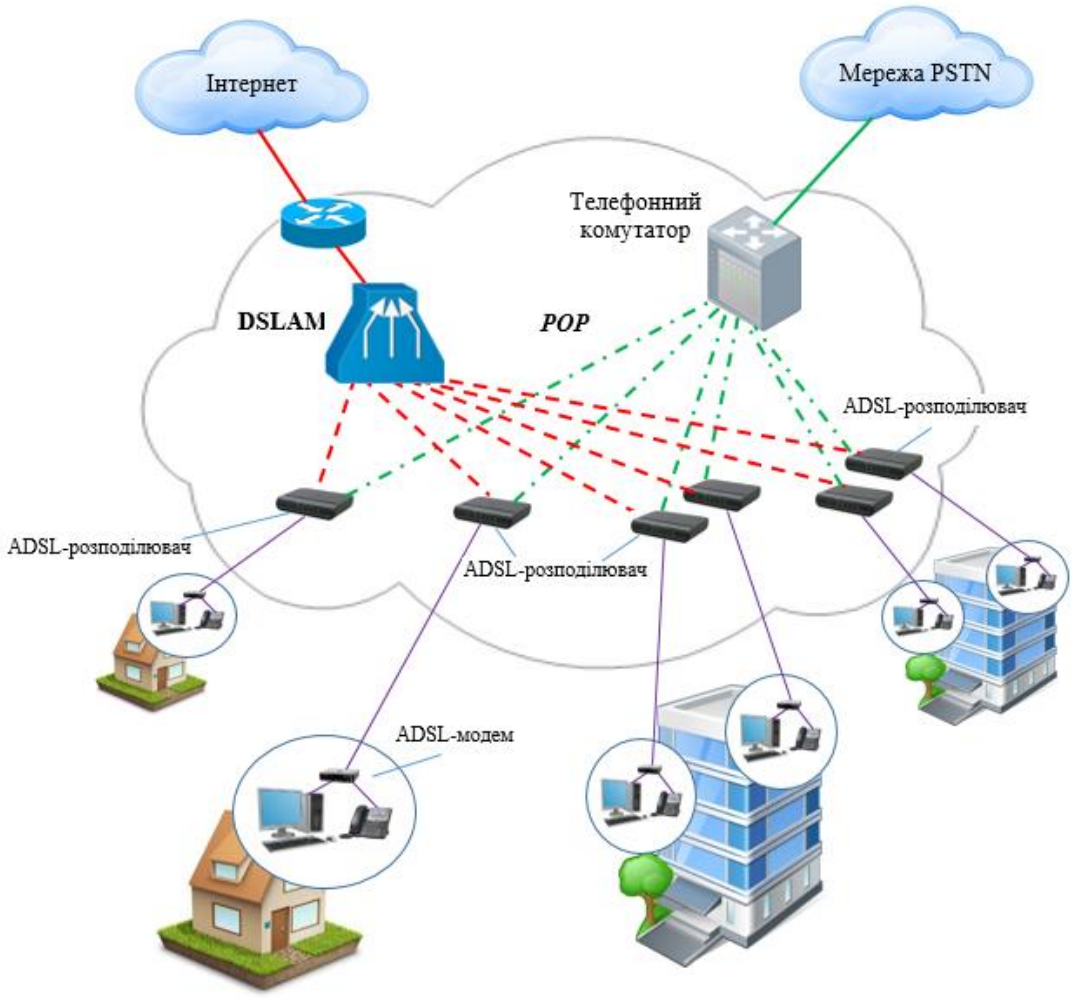



Рис. 8.10. Відмінності в роботі ADSL-модемів від комутованих модемів

Передача даних в каналі від мережі до абонента відбувається зі швидкістю до 24 Мбіт/с, а в каналі від абонента до мережі – до 3,5 Мбіт/с; для телефону залишена традиційна смуга в 4 кГц (рис. 8.11).


Рис. 8.11. Розподіл смуги пропускання абонентського закінчення між каналами ADSL

Для асиметрії низхідної і висхідної швидкостей смуга пропускання

абонентського закінчення ділиться між каналами також асиметрично. На рис. 8.11 показано розподіл смуги між каналами, при цьому наведені значення для висхідної і низхідної лінії є максимальними, які модем в кожному конкретному сеансі може використовувати повністю або ж частково.

Невизначеність використовуваних смуг частот пояснюється тим, що модем постійно тестує якість сигналу і вибирає тільки ті частини виділеного для передачі спектра, в яких співвідношення сигнал/шум є прийнятним для стійкої передачі дискретних даних. ADSL-модеми вміють адаптуватися до якості абонентського закінчення і вибирати максимально можливу на даний момент швидкість передачі даних.

У приміщенні клієнта встановлюється розподільник, який виконує поділ частот між ADSL-модемом і звичайним аналоговим телефоном, забезпечуючи їх спільне співіснування.

У POP встановлюється мультиплексор DSLAM, який приймає комп'ютерні дані, що відокремлені ADSL-розподілювачами від голосових сигналів. DSLAM-мультиплексор повинен мати стільки ADSL-модемів, скільки користувачів віддаленого доступу обслуговує постачальник послуг за допомогою телефонних абонентських закінчень.

Після перетворення модульованих сигналів в дискретну форму DSLAM відправляє дані на IP-маршрутизатор, який також, зазвичай, знаходиться в приміщенні POP. Далі дані надходять в магістраль передачі даних постачальника послуг і доставляються відповідно до IP-адрес призначення на публічний сайт Інтернету або в корпоративну мережу користувача. Відокремлені ADSL-розподілювачем голосові сигнали передаються на телефонний комутатор.

Відомо, що на сигнали, які передають телефонною лінією, впливають сильні завади. DSL модеми усувають цей вплив за допомогою спеціальних алгоритмів кодування, які опрацьовують сигнал на сигнальних процесорах та адаптивно узгоджують параметри сигналу і лінії. Пристрої DSL мають схеми кодування 2B1Q, CAP, DMT з невеликою шириною смуги перепускання та небагатьма кодовими станами. Ці методи кодування дають змогу збільшити ступінь стиснення даних і завдяки цьому збільшити швидкість їх передавання.

Окрім технології ADSL існують інші типи технологій DSL, які розрізняються за методом модуляції, що використовується для кодування даних, та швидкістю передачі даних.

**RADSL** (Rate-Adaptive Digital Subscriber Line-цифрова абонентська лінія із адаптацією швидкості з'єднання): дозволяє автоматично адаптувати швидкість передачі до протяжності та якості лінії зв'язку. При використанні технології RADSL зв'язок на різних телефонних лініях буде мати різну швидкість передачі даних. Швидкості передавання в інтервалах від 600 Кбіт/с до 8 Мбіт/с для одної

лінії, та від 128 Кбіт/с до 1 Мбіт/с – для іншої.

**HDSL** (High bit-rate Digital Subscriber Line – високошвидкісна цифрова абонентська лінія). В таких лініях дані передаються з швидкістю від 1,544 Мбіт/с (швидкість каналу T1) до 2,048 Мбіт/с (швидкість каналу E1) в довільному напрямку по двопарному мідному кабелю. HDSL лінії в першу чергу використовуються для з'єднання з офісною АТС, для обміну даними між точками присутності (POP) і приватними мережами передачі даних.

**SDSL** (Symmetric Digital Subscriber Line – симетрична цифрова абонентська лінія) – є варіантом HDSL, в якому використовується тільки одна пара кабелю. SDSL забезпечує однакову швидкість передачі даних як в сторону користувача, так і від нього. Відомі дві модифікації цієї технології: MSDSL (Multi-rate Symmetric DSL – багатошвидкісні SDSL) і HDSL2, що мають вбудований механізм адаптації швидкості передачі до параметрів фізичної лінії.

**VDSL** (Very high bit rate DSL – надвисокошвидкісна цифрова абонентська лінія). Дані передаються з швидкістю від 13 до 52 Мбіт/с до абонента (Downstream) і з швидкістю до 11 Мбіт/с від абонента (Upstream) при роботі в асиметричному режимі. Максимальна пропускна здатність лінії VDSL при роботі в симетричному режимі становить приблизно 26 Мбіт/с у кожному напрямку передачі. Залежно від необхідної пропускної здатності і типу кабелю довжина лінії VDSL лежить в межах від 300 метрів до 1,3 км.

**IDSL** (ISDN Digital Subscriber Line – цифрова абонентська лінія ISDN) – недорога технологія, що дозволяє забезпечити канал зв'язку для передачі даних по існуючих телефонних лініях на швидкості 144 Кбіт/с (трохи більшій, ніж при використанні подвійного каналу ISDN зі швидкістю 128 Кбіт/с). Технологія IDSL доступна не у всіх країнах. IDSL це щось середнє між ISDN і XDSL.

**Reach DSL** (протяжна DSL) – належить до групи симетричних технологій і була спеціально розроблена для використання на довгих й неякісних абонентських лініях. Швидкість в обох напрямках до 2,2 Мбіт/с на відстані не менше 9 км без обладнання ретрансляції.

## 8.6. Використання мереж кабельного телебачення

**Кабельне телебачення** (Cable TV, **CATV**) є однією з телекомунікаційних послуг, для якої була створена власна розгалужена інфраструктура абонентських закінчень. Хоча кабельне телебачення і поступається за поширеністю телефонній мережі, проте кількість коаксіальних абонентських закінчень, що з'єднують будинку і квартири з точками присутності постачальників послуг, в деяких країнах стало наближатися до кількості абонентських телефонних закінчень. З огляду на те, що коаксіальний кабель має більш ширшу смугу пропускання (як

мінімум, 700-800 МГц), абонентське закінчення кабельного телебачення може виконувати одночасну передачу телефонного, комп'ютерного та телевізійного трафіків.

Початковою метою мереж кабельного телебачення було широкотрансляційне поширення телевізійних програм до телевізійних приймачів абонентів кабельного телебачення з джерела інформації, розташованого в точці присутності постачальника послуг. Для цього займається діапазон частот від 50 до 550-868 МГц (точне значення залежить від національної політики виділення частот). Кожній програмі CATV виділяється в цьому діапазоні смуга в 6 або 8 МГц, сигнал якої шифрується і може бути розшифрований приймачами тих абонентів, які підписалися на прийом певної програми.

Апаратна структура мереж кабельного телебачення забезпечує однонапрямлене передавання (від головного вузла до абонента). Зі збільшенням попиту на передавання даних та послуг Інтернету виникла потреба надавати такі послуги абонентам з високою швидкістю та в обох напрямах. Водночас сучасні кабельні мережі потребують деякої технічної перебудови для передавання даних. Модернізація мереж кабельного телебачення полягає, головним чином, у заміні магістральних мідних коаксіальних кабелів волоконно-оптичними. Таким чином, мережі стають **гібридними волоконно-коаксіальними** (Hybrid Fiber Coaxial, **HFC**).

Смугу частот 750 МГц цих мереж зазвичай поділяють на три діапазони:

- діапазон від 5 до 42 МГц застосовують для передавання у висхідному напрямі;
- діапазон 550-750 МГц використовують для передавання у низхідному напрямі;
- решта діапазону призначено для передавання сигналів телебачення.

Діапазон низьких частот використовується для менш швидкісного висхідного каналу, а діапазон високих частот – для високошвидкісного низхідного каналу. Швидкість передавання даних в висхідному напрямку може доходити до 10 Мбіт/с, а в низхідному – до 30-40 Мбіт/с.

Оскільки висхідний і низхідний канали розділені по частотах, абонентське закінчення кабельного телебачення утворює два колективні середовища.

Для передавання даних через мережу Інтернет, абоненти кабельного телебачення використовують спеціальні **кабельні модеми (cable modems)**. Дані модеми мають вбудований концентратор Ethernet для підключення комп'ютера і інших мережевих пристроїв. Послуги доступу через кабельні модеми можливі в будь-якому місці, де є інфраструктура кабельного телебачення.

На рис. 8.12 показана деревовидна топологія мережі кабельного телебачення.

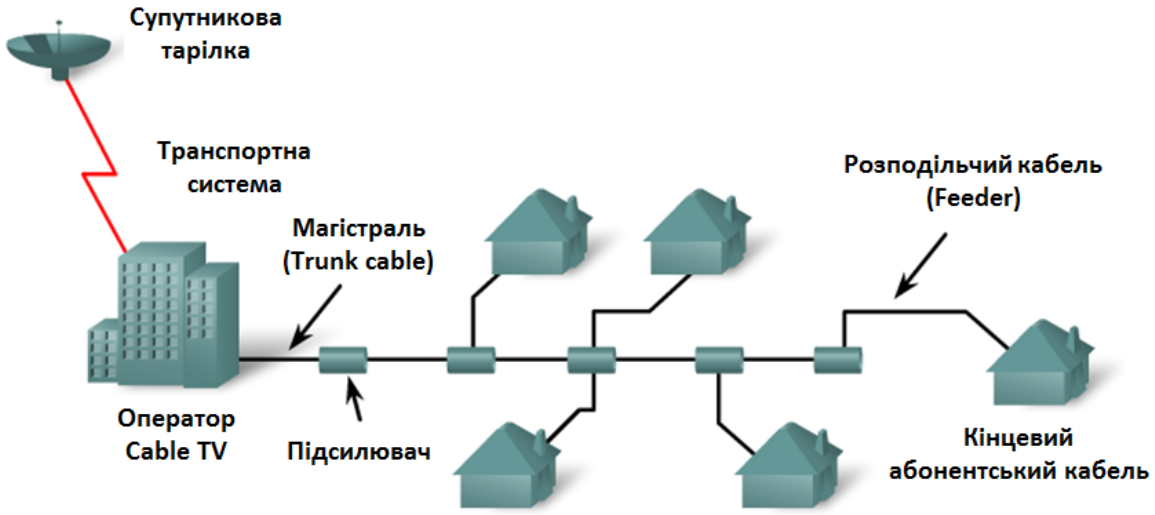



Рис. 8.12. Деревовидна топологія мережі кабельного телебачення

Кабельні оператори використовують супутникові тарілки для збору телевізійних сигналів. Від головного вузла постачальника послуг розходяться **магістральні кабелі** (Trunk cable), зазвичай, волоконно-оптичні, також можуть використовуватись коаксіальні кабелі. З метою поновлення аналогового сигналу та збільшення відстані передавання, у мережу вмонтовані **підсилювачі** (Amplifiers), які можуть бути одно- або двонапрямленими. До коаксіального кабелю за схемою монтажного АБО під'єднується одночасно кілька абонентів. Це може бути кілька десятків будинків або ж сотень квартир багатоквартирного будинку. Таким чином, мережі кабельного телебачення створюють **поділюване середовище (shared media)**, яке використовується, наприклад, в мережах Ethernet на коаксіальному кабелі, не допускаючи комутації.

До користувачів, через **розподільчі кабелі** (Distribution cable) або **високочастотні кабелі** (Feeders), заходить **кінцевий абонентський кабель** (Subscriber Drop cable).

На рис. 8.13 показана схема підключення абонента мережі кабельного телебачення до Інтернет.

В головному вузлі постачальника послуг розміщена термінальна система кабельних модемів (Cable Modem Termination System, **CMTS**), яка забезпечує передачу даних у напрямку з мережі до користувача – низхідному (Downstream) і від користувача у мережу – висхідному (Upstream) по існуючій інфраструктурі кабельного телебачення. Для організації доступу в Інтернет по мережах кабельного телебачення найчастіше використовуються **універсальні**

**широкосмугові маршрутизатори** (Universal Broadband Router, **UBR**), наприклад, Cisco uBR7200**.** Дані пристрої мають вбудований високошвидкісний маршрутизатор і модемну карту з інтегрованим частотним конвертором.

Для низхідного каналу CMTS є єдиним передавачем інформації, тому тут не виникає конкуренції за доступ до середовища. Станція CMTS використовує нисхідний канал для передачі по ньому кадрів даних всім абонентам за рахунок адресації Ethernet і поділу каналу в часі.

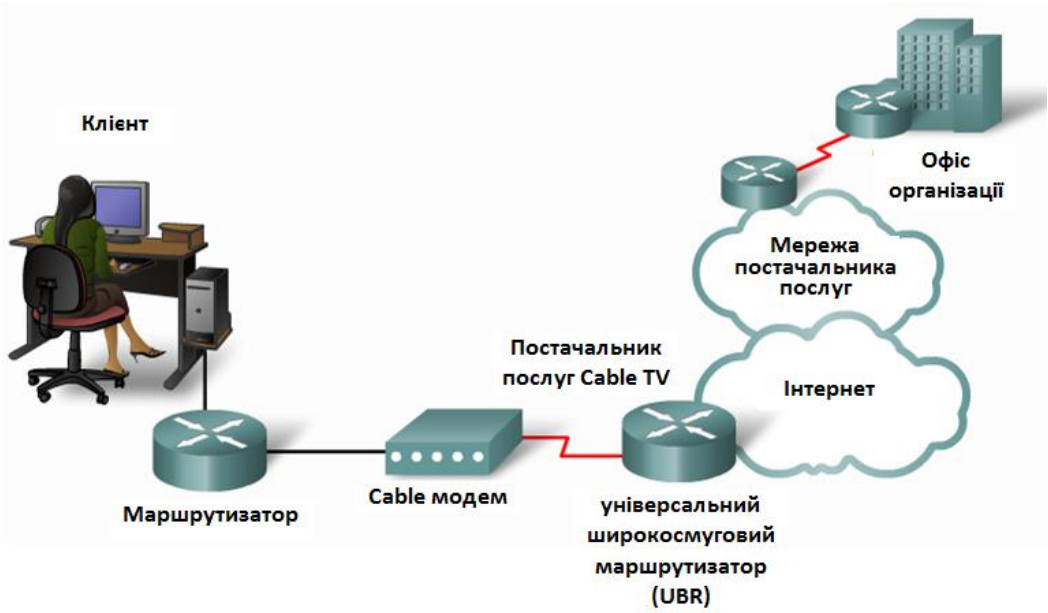



Рис. 8.13. Схема підключення абонента мережі кабельного телебачення до Інтернет

Висхідний канал задіюється в режимі множинного доступу усіма кабельними модемами, що під'єднанні до даного абонентського закінчення. У цьому поділюваному середовищі CMTS відіграє роль арбітра. Кожен абонентський модем починає передачу тільки після того, як отримає дозвіл на це від CMTS по прямому каналу. Для того, щоб один абонентський модем не займав канал надовго, CMTS призначає кожному абонентському модему тайм-слот обмеженого розміру. Тайм-слоти розподіляються тільки між активними модемами – це дозволяє витрачати обмежену пропускну спроможність максимально ефективно. При включенні абонентський модем використовує певний тайм-слот, щоб оповістити CMTS про свою присутність в мережі. Далі він очікує, коли йому буде виділений тайм-слот на рівних підставах з іншими модемами.

Кабельний модем абонента може мати роз'єм для під'єднання телефону, для якого також виділяється смуга в 4 КГц в нижньому діапазоні частот. В цьому випадку абонент отримує від одного постачальника послуг доступ трьох типів:

телефонний, комп'ютерний і телевізійний.

У 1998 р. на сесії робочої групи ITU в Женеві був схвалений стандарт J.112, що визначає методи передачі даних по мережах кабельного телебачення. Базуючись на основі стандартів ITU J.112 і J.83, консорціумом CableLabs, в співпраці з широким колом виробників обладнання, був розроблений єдиний міжнародний стандарт, відомий під назвою «Специфікація інтерфейсу служби передачі даних по кабелю» (Data Over Cable Service Interface Specification, **DOCSIS**).

Цей стандарт передбачає передачу даних абонентові у мережі кабельного телебачення з максимальною швидкістю до 42 Мбіт/с (при ширині смуги пропускання 6 МГц і використанні багатопозиційної амплітудної модуляції) та отримання даних від абонента зі швидкістю до 10,24 Мбіт/с. Він покликаний змінити поширені раніше рішення на основі фірмових протоколів передачі даних і методів модуляції, несумісних один з одним, і повинен гарантувати сумісність апаратури різних виробників.

Прийняті ITU документи містять також рішення, що враховують специфічні особливості американського, європейського і японського ринків послуг CATV і поширені в цих регіонах стандарти (NTSC, PAL, SECAM).

Існує декілька версій специфікації DOCSIS: DOCSIS 1.0, DOCSIS 1.1, DOCSIS 2.0, DOCSIS 3.0, EURODOCSIS. EURODOCSIS регламентує прийнятий для Європи розподіл частот прямого і зворотного каналу, обумовлює роботу із смугою 8 МГц.

В таблиці 8.1 приведені швидкості передачі для кожного із стандартів.

Таблиця 8.1. Швидкості передачі протоколів DOCSIS

| Версія | **DOCSIS** | | **EuroDOCSIS** | |
|---|---|---|---|---|
| | **Downstream** | **Upstream** | **Downstream** | **Upstream** |
| 1.x | 42,88 Мбіт/с | 10,24 Мбіт/с | 55,62 Мбіт/с | 10,24 Мбіт/с |
| 2.0 | 42,88 Мбіт/с | 30,72 Мбіт/с | 55,62 Мбіт/с | 30,72 Мбіт/с |
| 3.0 4channel | 171,52 Мбіт/с | 122,88 Мбіт/с | 222,48 Мбіт/с | 122,88 Мбіт/с |
| 3.0 8channel | 343,04 Мбіт/с | 122,88 Мбіт/с | 444,96 Мбіт/с | 122,88 Мбіт/с |

## 8.7. Пасивні оптичні мережі

Проведення оптичного волокна від точки присутності оператора до будівлі користувача є найякіснішим вирішенням проблеми організації віддаленого доступу, так як дозволяє забезпечити високі швидкості обміну даними і хорошу захищеність даних. Для під'єднання численних будівель індивідуальних і корпоративних користувачів, що займають значну територію, оператор повинен

створити деяку мережу доступу. Для її організації оператор може задіяти технології PDH, SDH або OTN. Оптична мережа, побудована на цих технологіях, повинна включати такі пристрої, як підсилювачі, повторювачі і мультиплексори. Всі ці пристрої є активними, тобто включають електричні схеми, які потребують електроживлення. Таке рішення цілком допустиме, і багато операторів його застосовують для побудови мереж доступу, що вимагають прокладки оптичного волокна до приміщень користувачів. Однак це рішення є досить дорогим.

Для здешевлення оптичної мережі доступу ще в середині 90-х років була запропонована технологія, що отримала назву **пасивна оптична мережа** (Passive Optical Network, **PON**).

Назва «пасивна» походить від застосування в мережі пасивних оптичних пристроїв – **розгалужувачів** (splitter), які не потребують електроживлення. За допомогою розгалужувачів організовується деревовидна оптоволоконна структура, що з'єднує точку присутності оператора з приміщеннями користувачів (рис. 8.14).

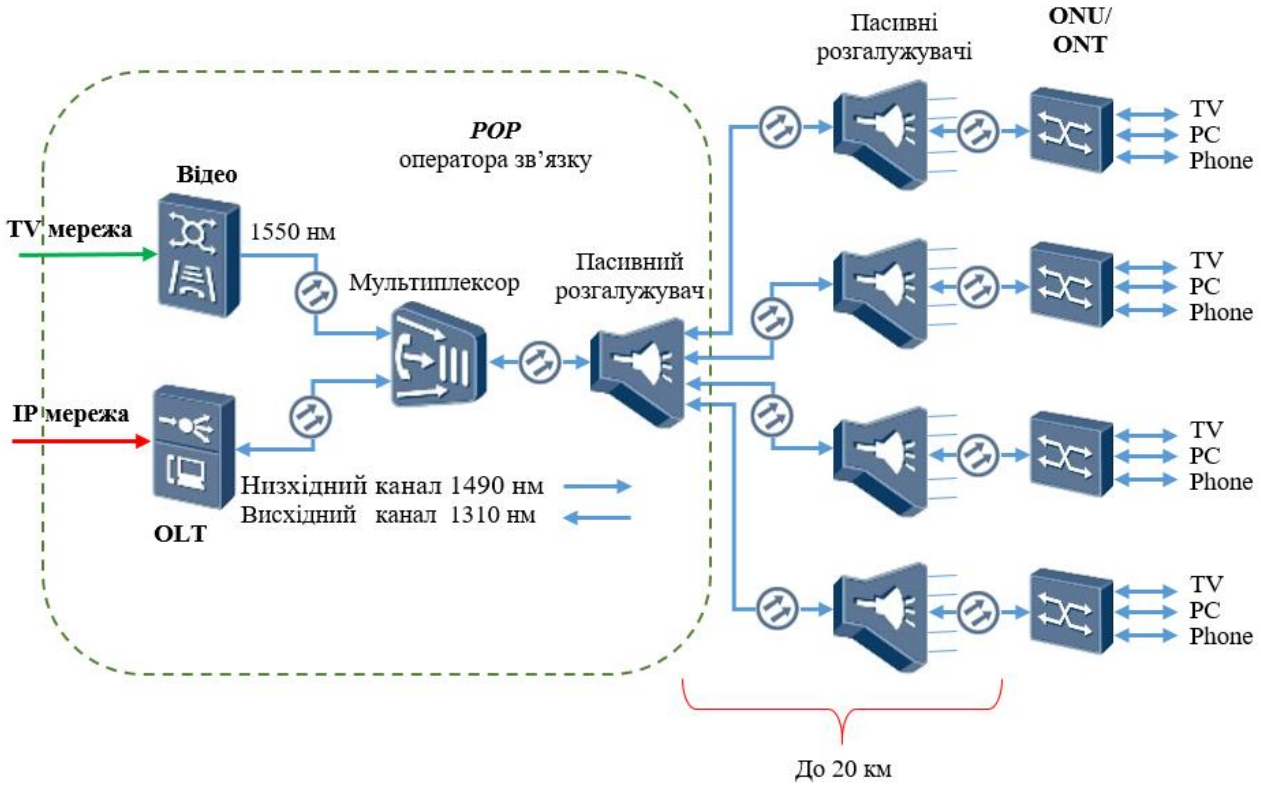



Рис. 8.14. Структура PON доступу

Розгалужувач виконує просту операцію – він направляє світловий сигнал з одного вхідного волокна в кілька вихідних, що йдуть в напрямку до користувачів. Розгалужувач виконує також зворотну операцію мультиплексування сигналів користувачів в одне волокно, що йде до POP.

Коефіцієнт розгалуження цих пасивних пристроїв може досягати значень

1:16 або 1:32, а максимальна відстань від них до активних пристроїв, що знаходяться в точці присутності оператора, дорівнює 20 км (застосовується одномодове волокно). Оскільки розгалужувачі не вимагають електроживлення, їх можна розміщувати в близьких до будівель користувачів точках міської інфраструктури, де активні пристрої не змогли б працювати, тим самим скорочується сумарна довжина оптичного волокна. Економія досягається за рахунок того, що замість N індивідуальних волокон на відрізку між центральним офісом оператора і розгалужувачем потрібно лише одне загальне волокно. Крім того, пасивні розгалужувачі дешевші активних мультиплексорів. Оператор може застосовувати не один, а два рівня розгалуження. На рис. 8.14 показаний саме такий варіант, перший розгалужувач розподіляє сигнал між чотирма волокнами, а розгалужувачі другого рівня розподіляють його між кінцевими користувачами.

До вершини дерева підключається центральний **термінал оптичної лінії** (Optical Line Terminal, **OLT**). До кожного оптичного волокна на стороні користувача підключається **модуль оптичної мережі** (Optical Network Unit, **ONU**), який спільно з OLT організовує прийом і передачу даних між користувачем і мережею оператора зв'язку. Крім ONU на стороні користувача повинен працювати **термінал оптичної мережі** (Optical Network Terminal, **ONT**), який забезпечує інтерфейси для термінальних пристроїв користувача – телевізора (TV), комп'ютера (PC) і телефону (Phone). Часто функції ONU і ONT суміщені в одному і тому ж пристрої (як це і показано на рисунку).

Для передачі цифрової інформації в низхідному (від OLT до модулів ONU) і визхідному (від модулів ONU до OLT) напрямках використовується дві хвилі, що поширюються в одному волокні: 1490 нм для низхідного напрямку і 1310 нм – для висхідного. Для передачі відеосигналу зазвичай виділяється окрема хвиля в 1550 нм, що йде в низхідному напрямку. Хвилі мультиплексуються в OLT і ONU за технологією WDM.

За своєю природою деревовидна мережа доступу, побудована на пасивних розгалужувачах і відрізках оптичного волокна, є **поділюваним середовищем.** Світловий сигнал певної хвилі, відправлений OLT, одночасно поширюється по всіх відрізках оптичного волокна і досягає всіх користувачів мережі. При передачі в зворотному напрямку поділюваним середовищем є відрізки волокна від розгалужувачів, встановлених на стороні користувачів, а також від розгалужувача, встановленого в POP (на рисунку є чотири поділюваних середовища для зворотного напрямку).

Очевидно, що для роботи в поділюваному середовищі необхідний якийсь метод доступу, який би регулював його використання таким чином, щоб сигнали, що передаються різними вузлами, не змішувалися. Проблема скоординованого застосування поділюваного середовища існує тільки для висхідного напрямку.

Для низхідного напрямку в мережі є тільки один передавач – OLT. Тому передавач OLT передає кадри даних (наприклад, Ethernet кадри), спрямовані деякому кінцевому вузлу мережі PON, тоді, коли йому це потрібно (тобто тоді, коли такий кадр надходить в OLT з локальної мережі оператора, до якої під'єднаний передавач). Кадр надходить по пасивній деревовидній оптичній мережі на всі кінцеві вузли мережі, але приймає його тільки той вузол, який розпізнає власну адресу в заголовку кадру, інші вузли просто ігнорують чужий кадр.

Для висхідного напрямку, зазвичай, застосовується схема з центральним арбітром в поєднанні з мультиплексуванням з поділом часу (TDM). Арбітром є центральний пристрій OLT, він керує розподілом тайм-слотів між модулями ONU. Модуль ONU передає в висхідному напрямку кадри даних тільки в межах свого тайм-слота, весь інший час він простоює, накопичуючи кадри для передачі в своєму буфері. Алгоритм розподілу тайм-слотів між модулями ONU може бути адаптивним, підлаштовуватися під наявні потреби модулів ONU в передачі кадрів.

Для телевізійного сигналу проблеми поділу середовища не існує, так як він передається тільки в низхідному напрямку, причому всім приймачів потрібен один і той же сигнал.

Існує дві групи стандартів PON: від міжнародного союзу електрозв'язку (ITU-T) і від інституту інженерів з електротехніки та електроніки (IEEE). Останні версії цих стандартів підтримують швидкості передачі даних 1 і 10 Гбіт/с.

Стандарти ITU-T GPON (Gigabit PON) та XG-PON (10 Gigabit PON) забезпечують сумісність з технологією SDH. Ці стандарти пропонують власний формат кадрів, який може ефективно переносити кілька користувацьких кадрів, наприклад кадрів Ethernet. Кадри GPON і XG-PON також можуть переносити дані SDH із зберіганням їх синхронності, що важливо при передачі голосу і відео. Стандарти ITU-T забезпечують несиметричні швидкості передачі даних: 2,488/1,244 Гбіт/с і 9,953/2,488 Гбіт/с.

Стандарти IEEE EPON (Ethernet PON, 802.3ah) і 10G-EPON (10G Ethernet PON, 802.3av) підтримують кадри Ethernet безпосередньо. У цих стандартах канал передачі даних є симетричним, тобто дані передаються як в низхідному, так і в висхідному напрямку з однаковою швидкістю 1 і 10 Гбіт/с відповідно.

## 8.8. Бездротовий доступ

Бездротова передача даних останнім часом широко використовується також для організації зв'язку з телекомунікаційними мережами, особливо в тих випадках, коли постачальник послуг з певних причини не може забезпечити

своїм клієнтам дротовий доступ. Найчастіше це трапляється з альтернативними постачальниками послуг, які не мають в своєму розпорядженні провідних абонентських закінчень до будинків клієнтів. Іншим типовим прикладом є організація тимчасового високошвидкісного доступу для певної будівлі, наприклад при проведенні конференції в приміщенні готелю, не оснащеному засобами проводового доступу необхідної пропускної спроможності.

Доступ може бути як фіксованим, так і мобільним.

**Фіксований бездротовий доступ** організовується для абонентів, комп'ютери яких знаходяться в межах обмеженій території, найчастіше в межах будівлі. В такому випадку постачальник послуг може використовувати направлену антену і передавач відомої потужності, щоб забезпечити стійкий прийом високочастотних сигналів в такій вузькій області покриття, як будівля. Якщо у постачальника послуг є досить велика кількість абонентів фіксованого бездротового доступу, то він зазвичай використовує кілька спрямованих антен, щоб покрити всі сектори, в яких знаходяться його абоненти.

Для бездротового фіксованого доступу вживається також термін **бездротове абонентське закінчення** (Local Loop Wireless, **WLL**). Цей термін добре відображає той факт, що, незважаючи на відсутність кабелів, абоненти «прив'язані» до певної географічної точки, як і в разі проводового абонентського закінчення.

Існують вузькосмугові і широкосмугові бездротові абонентські закінчення. Перший тип не забезпечує передачу телевізійного сигналу, а лише низькошвидкісний комп'ютерний трафік (64-128 Кбіт/с) і телефонний сигнал. Другий тип, зазвичай, базується на системах поширення телевізійного сигналу, тому використовує високочастотні діапазони і забезпечує всі три види доступу, причому комп'ютерні дані передаються зі швидкостями від декілька сотень Кбіт/с до кілька Мбіт/с. До систем останнього типу відносяться **багатоканальна багатоточкова служба розподілу** (Multichannel Multipoint Service Distribution, **MMDS**) і **локальна багатоточкова служба розподілу** (Local Multipoint Distribution Service, **LMDS**). MMDS працює в діапазоні 2,1 ГГц, а LMDS – 30 ГГц в Америці і 40 ГГц в Європі. Обидві системи забезпечують двосторонню передачу сигналів для абонентів телевізійних, телефонних та комп'ютерних послуг. Так як система MMDS працює на більш низьких частотах, ніж LMDS, вона забезпечує більш ширшу область покриття. Одна щогла з направленими антенами MMDS, зазвичай, може обслуговувати територію радіусом в 50 км, в той час як радіус покриття передавачів LMDS, зазвичай, не перевищує 5 км, а в міських умовах ще менше. Зате LMDS може забезпечити для своїх абонентів вищі швидкості доступу (до 155 Мбіт/с).

Як у вузькосмугових, так і в широкосмугових бездротових абонентських

закінченнях використовуються різні методи мультиплексування сигналів для одночасної роботи своїх абонентів в одному секторі направленості антени, а також для поділу телевізійного, телефонного та комп'ютерного трафіків. Зазвичай, тут застосовується комбінація прийомів FDM і TDM. Наприклад, для кожного типу трафіку може бути виділено певний діапазон частот відповідно до принципів частотного мультиплексування. Потім всередині діапазону частот, виділеного для комп'ютерного трафіку, може застосовуватися асинхронне часове мультиплексування з певним алгоритмом доступу до загального середовища, наприклад з центральним арбітром. Для деяких абонентів, яким необхідна гарантована смуга пропускання, може застосовуватися синхронне часове мультиплексування з утворенням бездротових каналів PDH/SDH.

На жаль, технології WLL досі багато в чому є фірмовими з несумісними обладнанням доступу та центральними станціями. Для усунення цього недоліку був розроблений стандарт IEEE 802.16 (відомий під назвою **WiMAX**), який визначає деякі загальні принципи використання частотного діапазону, методів мультиплексування і наданих послуг. Цей стандарт передбачає застосування різних методів мультиплексування, як частотного, так і часового синхронного і асинхронного, щоб врахувати інтереси різних виробників обладнання WLL і забезпечити максимальну гнучкість таких систем.

Технологія 802.11 також може використовуватися для фіксованого бездротового доступу. Однак вона застосовується в цій якості не так часто, тому що орієнтована виключно на комп'ютерний трафік і ігнорує особливості телефонного і телевізійного трафіків, а саме – доступ з постійною бітовою швидкістю. Метод доступу **CDMA/CA** (Carrier Sense Multiple Access/with Collision Avoidance – множинний доступ з прослуховуванням несучої та уникненням колізій), що описаний в 802.11, не може забезпечити необхідного рівня QoS для чутливого до затримок трафіку. Проте, деякі постачальники послуг застосовують технологію стандарту 802.11 для фіксованого доступу в Інтернет тих абонентів, яких задовольняє невизначена пропускна спроможність. Ця технологія також популярна для «кочового» доступу в зонах тимчасового перебування абонентів, наприклад в аеропортах або на залізничних вокзалах.

**Мобільний бездротовий доступ** в Інтернет надається сьогодні в основному операторами мобільних телефонних мереж.

Протягом відносно недовгого періоду свого існування мобільний Інтернет пережив кілька основних етапів свого розвитку, які були пов'язані як з вдосконаленням стільникових мереж, так і самих телефонних апаратів, які поступово еволюціонували в смартфони і комунікатори.

Мережі першого покоління (**1G** – Generation) призначалися, в основному, для голосового зв'язку. Передавання даних відбувалось за допомогою технології

**CSD** (Circuit Switched Data – стандартна технологія передачі даних з комутацією каналів в мережі GSM) з використанням спеціально розробленого протоколу **WAP** (Wireless Application Protocol – бездротовий протокол передачі даних, що використовується для запуску Інтернет-додатків на мобільних терміналах). По суті, протокол WAP являв собою аналог HTTP протоколу, але адаптований під мізерні можливості тодішніх мобільних пристроїв. Швидкість обміну даними в WAP не перевищувала 9600 біт/с, а для перегляду контенту мобільної версії сайту був потрібний спеціальний WAP-браузер, побудований на мові WML (Wireless Markup Language – мова розмітки та форматування наповнення для пристроїв чи програм, що підтримують WAP протокол для обміну мережевою інформацією).

Другим поколінням розвитку (**2G**) стала поява технології пакетної передачі даних **GPRS** (General Packet Radio Service – загальний сервіс пакетної радіопередачі). Теоретично, швидкість обміну даними в мережах GPRS може становити 171 Кбіт/с, хоча на практиці вона набагато нижча. Це пов'язано з тим, що пріоритет в GSM-мережах віддається голосовому трафіку, а отже, чим більше завантажена мережа в даний момент, тим меншою буде швидкість передачі даних.

Проміжною віхою **(2,5G)** на шляху до мереж третього покоління стала технологія **EDGE** (Enhanced Data rates for GSM Evolution) – технологія передачі даних, що забезпечує передачу великих обсягів інформації в мережі мобільного зв'язку. Технологія EDGE підтримує у середньому в три рази вищу швидкість передачі даних, ніж GPRS, крім того, забезпечується ефективніше використання частотних ресурсів і поліпшення покриття мережі. Максимально досяжна, теоретична, швидкість передачі інформації в мережі EDGE – 474,6 Кбіт/с.

Головна перевага стандарту EDGE – це здатність адаптувати передачу даних відповідно до умов завантаженості в мережі. Стандарт починає працювати тільки в той момент, коли дійсно виникає необхідність в прийомі або передачі даних, тому тарифікація в мережах EDGE відбувається за обсягом трафіку.

На даний момент технологія EDGE підтримується всіма мобільними операторами України, які працюють в мережах GSM.

Наступним великим кроком у розвитку мобільних мереж доступу стало створення стандарту мобільних мереж третього покоління – **3G.**

Всі перераховані вище цифрові системи другого покоління засновані на методі **множинного доступу з часовим поділом каналів** (Time Division Multiple Access, **TDMA**). Принципова відмінність мереж 3G полягає в використанні технології **множинного доступу з кодовим поділом каналів** (Code Division Multiple Access, **CDMA**).

Найбільшого поширення набули стандарти **UMTS** (Universal Mobile

Telecommunications System – універсальна мобільна телекомунікаційна система) в Європі і **CDMA2000** в США.

Стандарт UMTS дає теоретичну можливість обмінюватися даними на швидкостях до 2 Мбіт/с. Технологія використовує метод доступу CDMA. Також спільно з UMTS використовується надбудова **HSDPA** (High-Speed Downlink Packet Access – високошвидкісний пакетний доступ у низхідному напрямку) – технологія **3,5G** зі швидкістю передавання даних 7,2 Мбіт/с.

Технологія **HSPA+** (Evolved High-Speed Packet Access – розвинутий високошвидкісний пакетний доступ) – стандарт мобільного зв'язку (**3,75G**), що дозволяє досягти швидкості завантаження до 43,2 Мбіт/с та віддачі до 5,76 Мбіт/с.

Стандарт UMTS також ще називається **3GSM**, щоб підкреслити причетність до мереж GSM і до третього покоління мобільних мереж.

1 листопада 2007-го року державне підприємство Укртелеком запустило мережу мобільного зв'язку 3G під брендом «Utel». Мережа «Utel» працювала в стандарті UMTS 2100 з надбудовою HSDPA (3,5G). З 2012 р. її правонаступником стала компанія «ТриМоб», яка теж працює з цією надбудовою. Після приєднання у 2013-му році CDMA Ukraine до Інтертелекому в Україні діяли такі оператори мобільного 3G зв'язку: ТриМоб, Інтертелеком та PEOPLEnet.

З лютого 2015 року ліцензії 3G отримали три найбільших оператори мобільного зв'язку України: МТС Україна (зараз Vodafone Україна), Київстар та Life:) Україна (зараз Lifecell). Вартість кожної ліцензії становила близько 2,7 млрд. грн. За умовами тендеру оператори зобов'язуються протягом 18 місяців після проведення конкурсу запустити мережу третього покоління на території всіх обласних центрів України, а протягом 6 років — на території всіх районних центрів і всіх населених пунктів з населенням понад 10 тисяч осіб.

Мережі **4G** – четверте покоління мобільних мереж, які стали продовженням розвитку мереж третього покоління. Основною перевагою мереж 4G є швидкість, що перевищує показники 3G в 200-500 разів. Очікуваний перехід до 4G принесе All-IP із комутацією пакетів, мобільний широкосмуговий доступ із швидкостями до Гбіт/с при передаванні із використанням декількох несучих.

Міжнародний телекомунікаційний союз (ITU) до стандартів четвертого покоління відносить стандарти мобільної передачі, затверджені у специфікації **ITM-Advanced** у жовтні 2010 року. Кандидатами у четверте покоління були визначені дві технології: **LTE-Advanced** (3GPP LTE Release 10) та **WiMax Release 2** (IEEE802.16m). Це дозволяє їх кваліфікувати у якості справжніх технологій 4G.

Незважаючи на використання деякими операторами позначень «4G» та

«четверте покоління» у рекламі послуг, що надаються у стандартах Mobile WiMax та LTE, такі мережі не відносяться до мереж IMT-Advanced, і не є кандидатами у четверте покоління.

На відміну від попередника, мережі четвертого покоління не використовують канал для передачі голосу, а працюють тільки з цифровими даними. Це означає, що дзвінки перейдуть у формат **VoIP** і в майбутньому може привести до зникнення класичного стільникового зв'язку на користь Інтернет-телефонії.

У липні 2015 р. президент України Петро Порошенко підписав указ про запровадження технології **4G в Україні**. Очікується, що ліцензії на технологію 4G LTE отримають у 2018 р.

# 9. Бездротові мережі

## 9.1. Класифікація бездротових мереж

Бездротові технології призначені для організації якісних магістральних каналів зв'язку та ефективної «останньої милі» незалежно від наявності існуючих каналів зв'язку.

У порівнянні з традиційними дротовими мережами бездротова технологія має цілий ряд переваг.

Однією з головних переваг є можливість встановлення зв'язку в будь-який час і з будь-якої точки. Широке поширення бездротових мереж в громадських місцях, таких як інтернет-кафе, дозволяє встановлювати зв'язок з мережею Інтернет, завантажувати інформацію, обмінюватися електронною поштою і файлами.

Бездротова технологія досить проста і недорога з точки зору монтажу. Вартість домашніх і комерційних бездротових пристроїв продовжує знижуватися. При цьому, незважаючи на зниження вартості, швидкість передачі даних збільшується, а функціональність цих пристроїв стає більш досконалою, що забезпечує більш високу швидкість і надійність зв'язку.

Бездротова технологія розширює межі мереж без обмежень, що властиві кабельним з'єднанням. Вона дозволяє швидко і зручно встановлювати мережеві з'єднання постійно зростаючої кількості користувачів.

Незважаючи на гнучкість і значні переваги бездротових мереж, їм також властиві деякі обмеження і ризики.

По-перше, в технологіях бездротових мереж використовуються неліцензовані області радіочастотного спектру. Оскільки ці області діапазону не регламентуються, в них використовується безліч різних пристроїв. Це призводить до переповнення областей спектру і перешкод від різних пристроїв. Крім того, ці частоти використовуються багатьма пристроями, наприклад, мікрохвильовими печами та бездротовими телефонами, які можуть створювати перешкоди роботі бездротових локальних мереж.

Інша проблема бездротового зв'язку – безпека. Доступ в бездротові мережі відкритий. Кожен може отримати доступ до даних, що передаються в сеансі широкотрансляційного розсилання. При цьому рівень захисту даних в бездротовій мережі також обмежений. Кожен може перехоплювати потоки даних навіть ненавмисно. Для забезпечення безпеки даних в бездротових мережах було розроблено ряд методів, таких як шифрування і автентифікація.

Бездротові мережі поділяються на три основні категорії: **бездротові персональні мережі** (Wireless Personal Area Network, **WPAN**), **бездротові локальні мережі** (Wireless Local Area Network, **WLAN**), **бездротові міські мережі** (Wireless Metropolitan Area Networks, **WMAN**) і **бездротові глобальні мережі** (Wireless Wide Area Network, **WWAN**) (рис. 9.1).

Незважаючи на подібні чіткі категорії, важко розмежувати рамки реалізації бездротових технологій. Це пов'язано з тим, що на відміну від кабельних мереж для бездротових мереж не потрібні чітко визначені межі. Діапазон передавання даних в бездротових мережах може змінюватися під впливом різних факторів. Бездротові мережі чутливі до зовнішніх джерел перешкод – природних або штучних. Перепади температури і вологості можуть значно впливати на зону покриття бездротових мереж. Перешкоди в середовищі бездротових мереж також впливають на діапазон їх дії.

Бездротові мережі **WPAN** застосовуються для підключення різних периферійних пристроїв, таких як миші, клавіатури, PDA (Personal Digital Assistant – персональний кишеньковий секретар) і т. п. до комп'ютера і мають найменший діапазон дії. Всі ці пристрої підключаються до одного вузла з використанням технологій інфрачервоного зв'язку або Bluetooth.

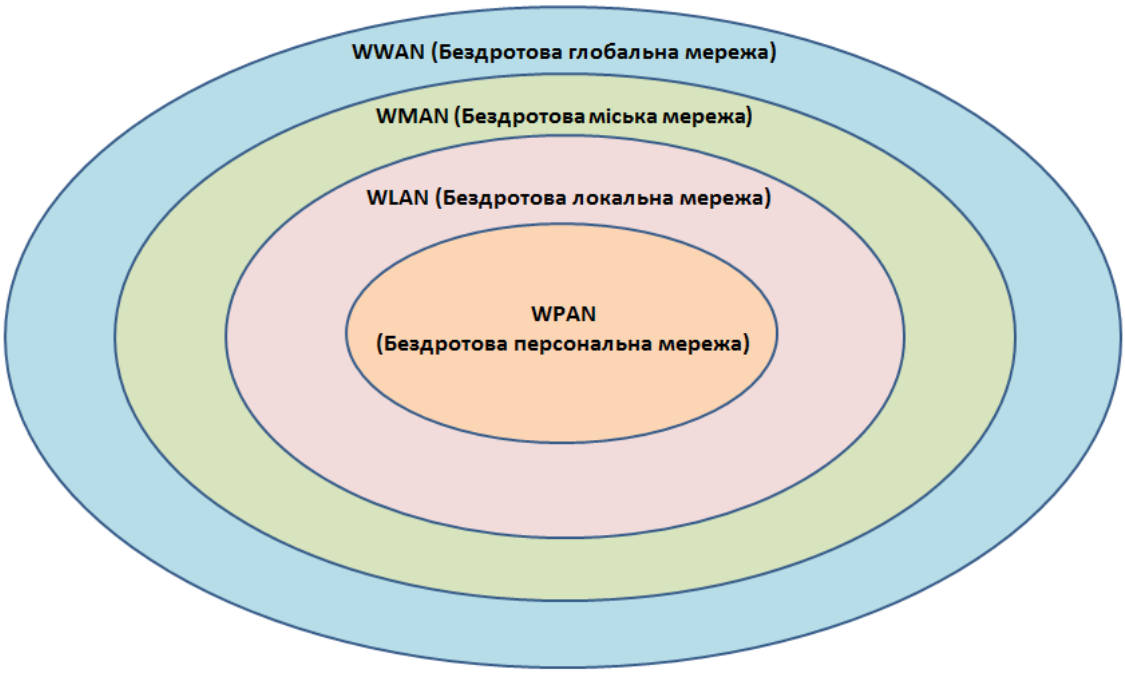



Рис. 9.1. Класифікація бездротових мереж

Мережі **WLAN** розширюють межі локальних кабельних мереж (LAN). Мережі WLAN використовують радіочастотну технологію і відповідають вимогам стандартів IEEE 802.11 (Wi-Fi). В таких мережах користувачі можуть

підключатися до дротової мережі за допомогою **точок доступу (Access Point, AP)**. Точка доступу забезпечує зв'язок між бездротовими вузлами і вузлами в кабельній мережі Ethernet.

Мережі **WMAN** надають широкосмуговий доступ до мережі через радіоканал в межах міста. Мережі WMAN відповідають стандарту IEEE 802.16 (WiMAX), який описує wireless MAN Air Interface. 802.16 – це так звана технологія «останньої милі», яка використовує діапазон частот від 10 до 66 ГГц. Стандарт підтримує топологію «точка-багатоточка» (Point-to-Multipoint), технології **дуплексного режиму з частотним розподілом** (Frequency Division Duplex, **FDD**) та **дуплексного режиму з часовим розподілом** (Time-Division Duplex, **TDD**), з підтримкою QoS. Можлива передача звуку і відео.

Мережі **WWAN** забезпечують покриття дуже великих територій. Найбільш наочним прикладом мережі WWAN є мережа стільникового зв'язку. У цих мережах використовуються такі технології, як **багатостанційний доступ з кодовим поділом каналів** (Code Division Multiple Access, **CDMA**) і **глобальна система мобільного зв'язку** (Global System for Mobile Communication, GSM), а їх діяльність зазвичай регламентується урядовими організаціями. Також прикладами WWAN можуть бути мережі на базі супутникового та радіорелейного зв'язку.

## 9.2. Бездротові персональні мережі (WPAN)

### 9.2.1. Технологія IrDA

Передача даних на базі інфрачервоних (ІЧ) каналів реалізована відповідно до стандартів **IrDA (Infrared Data Association – ІЧ-порт)**. IrDA визначає стандарти фізичних параметрів та протоколів інтерфейсу передачі даних із використанням інфрачервоного випромінювання (довжина хвилі від 850 до 900 нм) на малі відстані, наприклад, для застосування в WPAN. IrDA було розроблено HP.

IrDA являє собою напівдуплексну технологію передачі даних з обмеженим радіусом дії (стандартом визначається межа в 100 см). Шляхом обмеження дальності досягається безпека від прослуховування. Завдяки цьому, також, зменшується вартість приладів, однак, передача даних мусить відбуватись за умов прямої видимості між портами.

Протоколи IrDA задають процедури, що підтримують ініціалізацію зв'язку, визначення адреси пристрою, установку з'єднання і узгодження швидкості передавання даних, обмін даними, розрив з'єднання, припинення зв'язку та вирішення конфліктів адрес пристроїв.

Апаратна реалізація, як правило, являє собою пару з передавача, у вигляді світлодіода, і приймача, у вигляді фотодіода розташованих на кожній зі сторін лінії зв'язку. Наявність і передавача і приймача на кожній зі сторін є необхідним для використання протоколів гарантованої доставки даних.

У ряді випадків, наприклад при використанні в пультах дистанційного керування побутовою технікою, одна зі сторін може бути оснащена тільки передавачем а інша тільки приймачем. Іноді пристрої оснащують кількома приймачами, що дозволяє одночасно підтримувати зв'язок з кількома пристроями. Використання при цьому одного передавача можливо завдяки тому, що протоколи логічного рівня вимагають лише незначного зворотного трафіку для забезпечення гарантованої доставки даних. Наявність декількох передавачів зустрічається набагато рідше.

Більшість переносних комп'ютерів і кишенькових пристроїв в даний час містять інфрачервоний приймач, що підтримує асинхронне послідовне передавання даних з максимальною швидкістю 115,2 Кбіт/с або 4 Мбіт/с, в деяких випадках – 16 Мбіт/с.

Реалізація ІЧ-зв'язку **Serial IrDA (SIR)** підтримує максимальну швидкість передавання даних 115,2 Кбіт/с. Основною перевагою цього стандарту є можливість використання існуючих послідовних портів без додаткових витрат.

Стандарт ІЧ-зв'язку **Fast IrDA (FIR)** підтримує максимальну швидкість передавання даних 4 Мбіт/с, яку легко переналаштувати на більш повільні пристрої. Підтримується також стандарт **Very Fast IrDA (VFIR)**, який забезпечує напівдуплексне передавання даних зі швидкістю 16 Мбіт/с. Пристрої стандартів FIR і VFIR можуть використовуватися для зв'язку з пристроями стандарту SIR.

Протокол **IrLMP** (Infrared Link Management Protocol – протокол управління інфрачервоним каналом) – відповідає мережевому рівню OSIмоделі. Він складається з двох підрівнів – LM-MUX (Link Management Multiplexer – канал управління мультиплексором) і LM-IAS (Link Management Information Access Service – канал управління доступом до інформації служби).

LM-MUX відповідає за:

- поділ потоку даних на різні канали зв'язку;
- зміну Первинних / Вторинних пристроїв.

LM-IAS відповідає за:

- публікацію списку доступних сервісів;
- доступ клієнтських пристроїв до опублікованих сервісів.

Протокол **IrCOMM** (Infrared Communications Protocol – протокол інфрачервоного зв'язку) – протокол, який дозволяє використовувати мобільний телефон як бездротовий модем.

Протокол **TinyTP** (Tiny Transport Protocol – крихітний транспортний протокол) – дозволяє передавати великі масиви даних і керувати потоком даних, розставляючи пріоритети кожному логічному каналу.

Протокол **IrOBEX** (Infrared Object Exchange – інфрачервоний обмін об'єктами) – протокол, заснований на базі TinyTP. Забезпечує можливість обміну довільними об'єктами даних: контактами, подіями календаря, програмами і т.п.

Протокол **IrLAN** (Infrared Local Area Network – інфрачервона локальна мережа) – протокол, що дозволяє підключитися до локальної мережі через ІЧ-з'єднання одним з трьох способів: як точка доступу, одноранговий зв'язок («peer-to-peer»), або як хост.

На відміну від радіоканалу інфрачервоний канал нечутливий до електромагнітних перешкод, і це дозволяє використовувати його у виробничих умовах. До недоліків інфрачервоного каналу відносяться низькі швидкості передачі та необхідність прямої видимості. Крім того, дана технологія не дозволяє забезпечити захист переданої інформації.

Маючи такі недоліки, інфрачервоний канал не зміг отримати широкого розповсюдження. В останній час, IrDA витісняється технологією Bluetooth.

### 9.2.2. Технологія Bluetooth

Bluetooth («синій зуб», походить від прізвища середньовічного короля Данії Гаральда I Синьозубого) – це технологія бездротового зв'язку, створена у 1998 році групою компаній: Ericsson, IBM, Intel, Nokia, Toshiba.

В даний час розробки в області Bluetooth ведуться групою Bluetooth SIG (Special Interest Group), до якої входять також Lucent, Microsoft та інші компанії, чия діяльність пов'язана з мережевими технологіями. Згодом Bluetooth SIG і IEEE досягли угоди, на основі якої специфікація Bluetooth стала частиною стандарту IEEE 802.15.1 (дата опублікування – 14 червня 2002 року).

Основне призначення Bluetooth — забезпечення дешевого радіозв'язку між різноманітними типами електронних пристроїв, такими як мобільні телефони та аксесуари до них, портативні та настільні комп'ютери, принтери та інші. Причому, велике значення приділяється компактності електронних компонентів, що дає можливість застосовувати Bluetooth у малогабаритних пристроях.

Інтерфейс Bluetooth дозволяє передавати як голос (зі швидкістю 64 Кбіт/с), так і дані. Для передачі даних можуть бути використані асиметричний (721 Кбіт/с в одному напрямку і 57,6 Кбіт/с в іншому) та симетричний (432,6 Кбіт/с в обох напрямках) методи. Працюючи на частоті 2,4 ГГц, прийомопередавач Bluetooth дозволяє встановлювати зв'язок у межах 10 або 100 метрів. У стандарті Bluetooth передбачене шифрування даних, що

передаються з використанням ключа ефективної довжини від 8 до 128 біт і можливістю вибору односторонньої або двосторонньої аутентифікації. Додатково, до шифрування на рівні протоколу, може бути використано шифрування на програмному рівні. В Bluetooth застосовується метод розширення спектра зі стрибкоподібною перебудовою частоти (Frequency Hopping Spread Spectrum, FHSS). Метод FHSS простий в реалізації, забезпечує стійкість до широкосмугових перешкод, а обладнання недорого.

Протокол Bluetooth підтримує не тільки з'єднання «точка-точка», а й з'єднання «точка-багатоточка».

Робоча група з розробки стандарту бездротової передачі даних Bluetooth в квітні 2009 року випустила специфікацію Bluetooth 3.0. Модулі з підтримкою нової специфікації поєднуватимуть в собі дві радіосистеми. Перша, з низьким енергоспоживанням, забезпечує передачу даних на звичайній для другої версії Bluetooth швидкості в 3 Мбіт/с. Інша, високошвидкісна і сумісна із стандартом IEEE 802.11, забезпечує швидкості мереж Wi-Fi.

В Bluetooth 3.0 з'явилась технологія під назвою «розширений контроль живлення» (Enhanced Power Control). Вона дозволяє уникнути розриву з'єднання, якщо пристрій поклали в сумку або в кишеню.

В грудні 2009 року консорціум Bluetooth SIG анонсував стандарт Bluetooth 4.0 для електронних давачів. Новий стандарт призначений для передачі коротких пакетів даних обсягом по 8-27 байт зі швидкістю 1 Мбіт/с. Для порівняння, Bluetooth 3.0 дозволяє передавати дані зі швидкістю до 24 Мбіт/с, але і призначений він для іншої сфери застосування.

Bluetooth 4.0 призначений для використання в мініатюрних сенсорах, що розміщуються на тілі пацієнтів, в спортивному взутті, тренажерах тощо. Сенсори на базі нового стандарту зможуть передавати різну інформацію з навколишнього світу – температуру, тиск, вологість, швидкість пересування і так далі – на різні пристрої контролю, включаючи мобільні телефони. За словами представників консорціуму, окремий стандарт був розроблений у зв'язку з тим, що Bluetooth 3.0 і більш ранні версії не в змозі забезпечити необхідний низький рівень енергоспоживання.

### 9.2.3. Інші технології WPAN

Нові технології бездротового передавання пропонують швидкості передавання та потребують мінімальних витрат енергії.

**UWB** (Ultra-Wide Band – надширока полоса) – це бездротова технологія високошвидкісного зв'язку на малі відстані при дуже низьких витратах енергії. Використання широкої смуги частот (не менше 500 МГц) дозволяє UWB досягти

швидкість до 480 Мбіт/с на відстані до 3 м. На відстаннях до 10 м технологія дозволяє досягти лише 110 Мбіт/с. Вони не використовують складних систем чи схем модуляції сигналу. Розглядають також варіанти роботи взагалі без окремого джерела живлення та отримання потрібної невеликої енергії з середовища, подібно до годинників, що заводяться від рухів їх власників.

**ZigBee** – бездротовий стандарт передачі даних. Підтримується і розвивається однойменним альянсом ZigBeeTM, який був створений в 2002 році з метою об'єднання зусиль по розробці найбільш ефективних протоколів та забезпечення сумісності пристроїв різних виробників.

Мережі ZigBee є мережами з самоорганізовуванням та самовідновленням, оскільки ZigBee пристрої при вмиканні живлення, завдяки вбудованому програмному забезпеченню, вміють самі знаходити один одного і формувати мережу, а у разі виходу з ладу будь-якого з вузлів можуть встановлювати нові маршрути для передавання повідомлень.

## 9.3. Бездротові локальні мережі (WLAN)

### 9.3.1. Огляд стандартів Wi-Fi

**Wi-Fi** – торгова марка, що належить Wi-Fi Alliance. Загальновживана назва для стандарту бездротового зв'язку передачі даних, який об'єднує декілька протоколів та ґрунтується на сімействі стандартів IEEE 802.11. Термін «Wi-Fi» спочатку був придуманий як гра слів для залучення уваги споживача натяком на Hi-Fi (High Fidelity, висока точність). Незважаючи на те, що спочатку в деяких прес-релізах WECA (Wireless Ethernet Compatibility Alliance) фігурувало словосполучення «Wireless Fidelity» («бездротова точність»), на даний момент від такого формулювання відмовилися, і термін «Wi-Fi» ніяк не розшифровується.

Стандарт IEEE 802.11 регламентує роботу пристроїв в мережах WLAN. З урахуванням різних характеристик бездротового зв'язку в стандарт IEEE 802.11 були внесено чотири поправки. На сьогоднішній день діють наступні поправки – 802.11a, 802.11b, 802.11g і 802.11n. Всі ці технології віднесені до категорії Wi-Fi:

1. IEEE 802.11a:
   - використовує радіочастотний спектр 5 ГГц;
   - несумісний зі спектром 2,4 ГГц, тобто пристроями 802.11b/g/n;
   - максимальна швидкість передавання даних – 54 Мбіт/с;
   - радіус дії – 50 м;
   - дорігий в реалізації в порівнянні з іншими технологіями;

- обладнання, яке відповідає стандарту 802.11a, стає все більш рідкісним.

2. IEEE 802.11b:
   - перша технологія, яка використовує радіочастотний спектр 2,4 ГГц;
   - максимальна швидкість передавання даних – 11 Мбіт/с;
   - радіус дії – приблизно 46 м в приміщенні і 96 м на відкритому повітрі.
3. IEEE 802.11g:
   - використовує радіочастотний спектр 2,4 ГГц;
   - максимальна швидкість передавання даних – 54 Мбіт/с;
   - радіус дії – такий же, як у 802.11b;
   - є зворотна сумісність з 802.11b.
4. IEEE 802.11n:
   - використовує радіочастотний спектр 2,4-2,5 ГГц або 5 ГГц;
   - максимальна швидкість передавання даних – до 300 Мбіт/с (в перспективі до 600 Мбіт/с);
   - радіус дії – до 250 м на відкритому повітрі;
   - зворотна сумісність з існуючим обладнанням 802.11g і 802.11b (у проекті стандарту передбачена підтримка 802.11a).

Висока швидкість стандарту 802.11n досягається завдяки технології багатопотокової передачі даних (MIMO – multiple-input multiple-output). Приймачі і передавачі оснащуються кількома антенами. Бездротова мережа 802.11n може працювати в двох частотних діапазонах і забезпечує розширену зону прийому в порівнянні з попередньою версією.

Організація Wi-Fi Alliance відповідає за тестування пристроїв для бездротових LAN, випущених різними виробниками. Логотип Wi-Fi на корпусі пристрою означає, що це обладнання може взаємодіяти з іншими пристроями того ж стандарту.

Після вибору стандарту необхідно переконатися в тому, що всі компоненти в мережі WLAN відповідають його вимогам або сумісні з ним. В мережі WLAN має бути декілька обов’язкових компонентів: бездротовий клієнт (wireless client) або STA (скорочення від STAtion), точка доступу (Access Point), бездротовий міст (Wireless Bridge) (рис. 9.2).

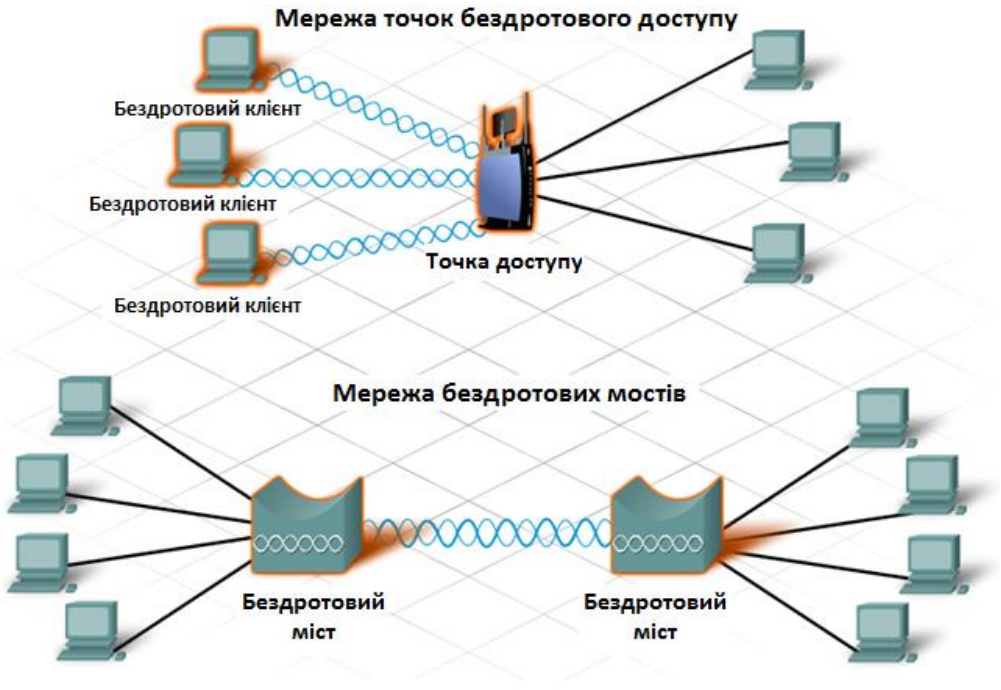



Рис. 9.2. Приклади мереж Wi-Fi

При побудові бездротової мережі важливо, щоб бездротові компоненти були підключені до відповідної мережі WLAN. Для цього використовується ідентифікатор набору послуг (SSID – Service Set Identifier).

SSID – це ідентифікатор бездротової мережі, що являє собою алфавітно-цифровий рядок довжиною до 32 символів. Цей ідентифікатор пересилається в заголовку всіх кадрів, що передаються по мережі WLAN. Ідентифікатор SSID повідомляє бездротові пристрої, до якої WLAN вони належать і з якими пристроями вони взаємодіють.

Для забезпечення зв’язку всі бездротові пристрої в мережі WLAN повинні мати загальний ідентифікатор SSID, незалежно від типу побудови мережі WLAN.

### 9.3.2. Методи побудови мереж WLAN

Використовується два основних методи побудови мереж WLAN: режим ad-hoc (децентралізований або «точка-точка») та інфраструктурний режим (рис. 9.3).

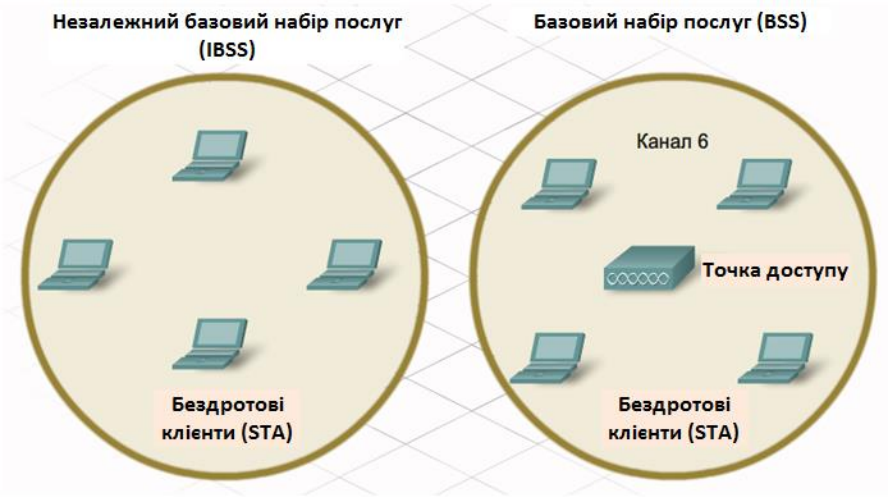



Рис. 9.3. Два основних види побудови мереж WLAN

**Режим ad-hoc**

Найпростіша бездротова мережа створюється за допомогою об'єднання двох або більше бездротових клієнтів в одноранговій мережі. В такій бездротовій мережі немає жодної точки доступу, а клієнти з'єднуються за участю мережевих адаптерів «напряму». Всі клієнти усередині мережі ad-hoc рівноправні. Зона покриття цієї мережі називається незалежним базовим набором послуг (IBSS – Independent Basic Service Set). Мережа ad-hoc дозволяє організувати обмін файлами та інформацією між пристроями без витрат і труднощів, пов'язаних з придбанням і налаштуванням точки доступу.

**Інфраструктурний режим**

Незважаючи на те, що режим ad-hoc може бути достатнім для невеликих мереж, у більш великих мережах потрібен пристрій, який би керував обміном даних в межах бездротової соти. Якщо в мережі використовується точка доступу, то вона бере ці функції на себе: визначає, які вузли і в який час можуть встановлювати зв'язок. Такий режим називається інфраструктурним режимом бездротового зв'язку. При такій формі організації мереж WLAN окремі STA-пристрої не можуть взаємодіяти між собою безпосередньо. Щоб ці пристрої могли взаємодіяти між собою, їм необхідний дозвіл від точки доступу. Точка доступу управляє всіма взаємодіями і забезпечує рівний доступ в середовище усім STA-пристроям. Зона покриття однієї точки доступу називається **базовим набором послуг** (Basic Service Set, **BSS**) або сотою.

Базовий набір послуг (BSS) – це найменший блок мережі WLAN. Точка доступу має обмежену зону покриття. Для розширення зони покриття можна об'єднати декілька BSS через **систему розподілу** (Distribution System, **DS**).

Таким чином створюється **розширений набір послуг** (Extended Service Set, **ESS**). В ESS використовується декілька точок доступу. Кожна точка доступу функціонує як окремий BSS.

Щоб перехід між сотами було можливий без втрати сигналу, базові набори послуг повинні перетинатися між собою приблизно на 10%. Це дозволяє клієнту підключатися до другої точки доступу перед тим, як відключитися від першої точки доступу (рис. 9.4).

У більшості домашніх і комерційних мереж є лише один базовий набір послуг. Тим не менше, при необхідності збільшення зони покриття та кількості вузлів, може знадобитися створення розширеного набору послуг.

Незалежно від того, як взаємодіють бездротові клієнти всередині IBSS, BSS або ESS, необхідно управляти зв’язком між відправником та одержувачем. Одне з рішень цієї задачі полягає у використанні каналів (Channels).

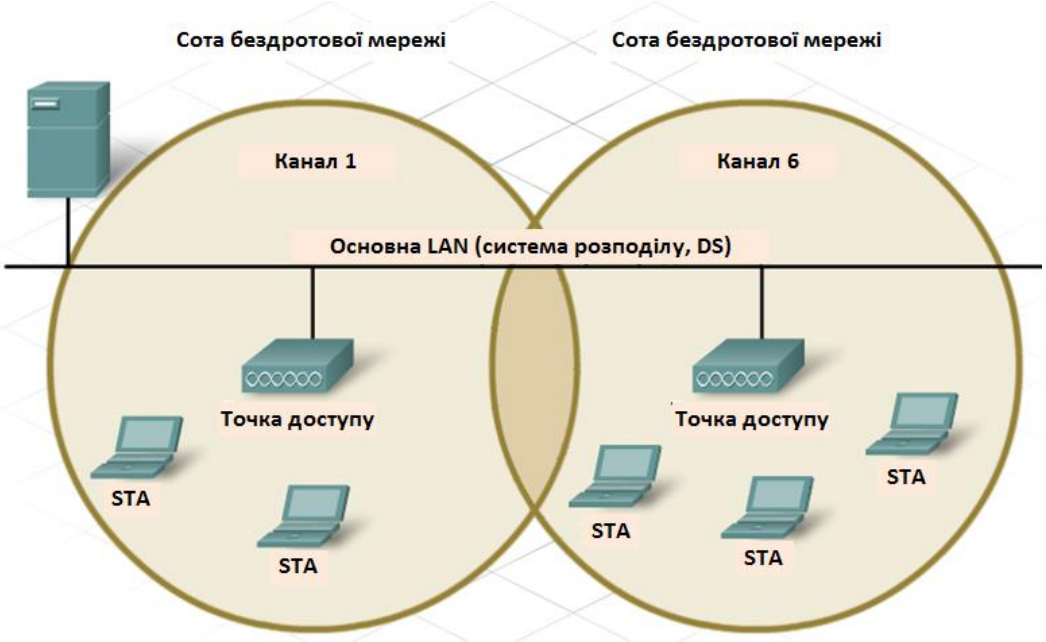



Рис. 9.4. Розширений набір послуг (ESS)

Канали створюються шляхом поділу доступного радіочастотного спектру. Кожен канал може використовуватися в якості несучої для іншого сеансу зв’язку. Це можна порівняти з передачею кількох телевізійних каналів по одному тракту. Кілька точок доступу можуть працювати в безпосередній близькості одна до одної, якщо вони використовують різні канали зв’язку.

На жаль, частоти, вибрані для деяких каналів, можуть перетинатися з каналами, зайнятими іншими пристроями. Різні сеанси зв’язку повинні використовуватися на непересічних каналах. Кількість і розподіл каналів залежить від регіону і вибору технологій. Канал для окремого сеансу зв’язку

можна налаштовувати вручну або автоматично, враховуючи його завантаженість і пропускну здатність.

Зазвичай для кожного сеансу бездротового зв'язку виділяється окремий канал. У деяких сучасних технологіях передбачено об'єднання каналів в єдиний канал з підвищеною смугою пропускання і більш високою швидкістю передавання даних.

Відсутність чітких кордонів в мережі WLAN не дозволяє виявляти колізії в процесі передачі даних. Тому необхідно використовувати такий метод доступу, який би гарантував відсутність колізій.

Для цього в бездротових технологіях застосовується **множинний доступ з контролем несучої та запобіганням колізій** (Carrier Sense Multiple Access with Collision Avoidance, **CSMA/CA**). CSMA/CA резервує канал для окремого сеансу зв'язку. Якщо канал зарезервований, жоден інший пристрій не зможе передавати по ньому дані, що дозволить уникнути можливих колізій.

Процес резервування працює наступним чином (рис. 9.5). Якщо пристрою потрібен спеціальний канал зв'язку в BSS, він звертається до точки доступу за дозволом. Цей етап називається **готовністю до передавання** (Request to Send**, RTS**). Якщо канал вільний, точка доступу відправить пристрою повідомлення про **готовність до прийому** (Clear To Send, **CTS**), яке показує, що пристрою дозволена передача з даного каналу. Повідомлення CTS передається усім пристроям в базовому наборі послуг (BSS). Тому усі пристрої в BSS знають, що канал в даний момент зайнятий. Після цього починається передача даних по каналу.

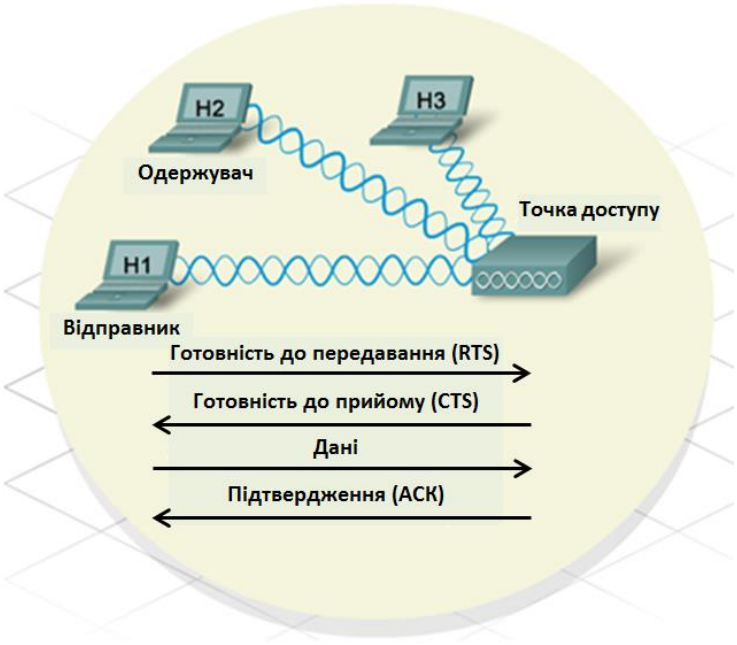



Рис. 9.5. Процес резервування

Після завершення сеансу зв’язку пристрій, який використовув канал, відправляє в точку доступу ще одне повідомлення – **підтвердження (ACK – Acknowledgement)**. Повідомлення ACK повідомляє точці доступу, що канал може бути звільнений. Це повідомлення також розсилається всім пристроям в мережі WLAN. Всі пристрої в базовому наборі послуг отримують повідомлення ACK і, таким чином, сповіщаються про те, що даний канал знову вільний.

### 9.3.3. Забезпечення безпеки WLAN

Одним із основних недоліків WLAN є легкий доступ зловмисників до мережі з будь-якої точки в межах дії бездротового зв’язку. Є декілька методів обмеження доступу в бездротову мережу.

#### Фільтрація по MAC-адресах

При використанні фільтрації по MAC-адресах рішення про допуск конкретного пристрою в бездротову мережу приймається на підставі MAC-адреси. При кожній спробі бездротового клієнта встановити з’єднання або асоціюватися з точкою доступу він повинен передати свою MAC-адресу. Якщо включена функція фільтрації по MAC-адресах, то бездротовий маршрутизатор або точка доступу виконає пошук MAC-адреси цього пристрою у своєму попередньо створеному списку. Підключення до мережі буде дозволено лише тим пристроям, чиї MAC-адреси внесені в базу даних маршрутизатора.

Якщо MAC-адреса в базі даних відсутня, то пристрою буде відмовлено у підключенні до бездротової мережі.

Такий спосіб забезпечення безпеки має один суттєвий недолік. Зловмисник може створити клон MAC-адреси пристрою, який внесений в базу даних «дозволених пристроїв», і таким чином, отримати доступ до мережі.

#### Автентифікація

Автентифікація – це надання дозволу на вхід в мережу за результатами перевірки автентичності набору облікових даних. Її мета – з’ясувати, чи є пристрій, що намагається встановити з’єднання, є довіреним пристроєм.

Найбільш поширена автентифікація по імені користувача та паролю. Існує три методи автентифікації в бездротових мережах: відкрита автентифікація, PSK і EAP.

**Відкрита автентифікація**

За замовчуванням, автентифікація бездротових пристроїв не вимагається. Усім пристроям дозволено встановлювати з'єднання незалежно від їх типу. Це називається **відкритою автентифікацією** (Open Authentication). Відкрита автентифікація повинна використовуватися тільки в **загальнодоступних бездротових мережах** (Public Wireless Networks), наприклад, в школах, інтернет-кафе, вокзалах і т. п. Вона може використовуватися в мережах, де автентифікація буде виконуватися іншими засобами після підключення до мережі.

**Попередньо погоджений ключ (PSK)**

При використанні режиму PSK (Pre-shared keys) точка доступу і клієнт повинні використовувати загальний ключ або кодове слово. Точка доступу відправляє клієнту випадковий рядок байтів. Клієнт приймає цей рядок, шифрує його, використовуючи ключ, і відправляє назад в точку доступу. Точка доступу отримує зашифрований рядок і для його розшифрування використовує свій ключ. Якщо розшифрований рядок, отриманий від клієнта, збігається з вихідним рядком, то клієнту дається дозвіл встановити з'єднання.

В цьому випадку виконується одностороння автентифікація, тобто точка доступу перевіряє реквізити вузла, що під'єднується. PSK не здійснює перевірки вузлом справжності точки доступу, а також не перевіряє достовірності користувача, що під'єднується до мережі.

**Розширюваний протокол автентифікації (EAP)**

**Розширюваний протокол автентифікації** (Extensible Authentication Protocol, **EAP**) забезпечує взаємну або двосторонню автентифікацію, а також автентифікацію користувача. Якщо на стороні клієнта встановлено програмне забезпечення EAP, клієнт взаємодіє з внутрішнім сервером автентифікації, таким, наприклад, як **служба віддаленої автентифікації користувачів з комутованим доступом** (Remote Authentication Dial-in User Service, **RADIUS**). Цей внутрішній сервер працює незалежно від точки доступу і веде базу даних користувачів, які мають дозвіл на доступ в мережу. При застосуванні EAP користувач, а не тільки вузол, повинен пред'явити ім'я та пароль, які потім перевіряються по базі даних сервера RADIUS. Якщо пред'явлені облікові дані є допустимими, вважається, що користувач пройшов автентифікацію.

Якщо функція автентифікації включена, то незалежно від застосовуваного методу клієнт повинен успішно пройти автентифікацію до того, як йому буде надано дозвіл на з'єднання з точкою доступу. Якщо включені функції автентифікації і фільтрації по MAC-адресах, то в першу чергу виконується автентифікація.

## Шифрування

Автентифікація і фільтрація по MAC-адресах можуть блокувати зловмиснику доступ в бездротову мережу, але не зможуть запобігти перехопленню переданих даних. Оскільки не існує чітких меж бездротових мереж і весь трафік передається без дротів, то зломщик може легко перехопити або прочитати кадри даних бездротової мережі. Шифрування – це процес перетворення даних, з метою приховання інформації.

### Протокол WEP

Протокол для **забезпечення конфіденційності бездротових мереж** (Wired Equivalency Protocol, **WEP**) – це вдосконалений механізм безпеки, що дозволяє шифрувати мережевий трафік в процесі передачі. У протоколі WEP для шифрування і розшифрування даних використовуються попередньо налаштовані ключі.

WEP-ключ вводиться як рядок чисел і букв довжиною 64 або 128 біт. В деяких випадках протокол WEP підтримує 256-бітові ключі. Для спрощення створення і введення цих ключів в багатьох пристроях використовуються фрази-паролі (passphrase). Фраза-пароль – це простий засіб запам'ятовування слова або фрази, які використовуються при автоматичній генерації ключа.

Для ефективної роботи протоколу WEP точка доступу, а також кожен бездротовий пристрій повинні використовувати загальний WEP-ключ. Без цього ключа пристрої не зможуть розпізнати дані, які передаються по бездротовій мережі.

Протокол WEP – це ефективний засіб захисту даних від перехоплення. Тим не менш, протокол WEP також має свої слабкі сторони, одна з яких полягає у використанні статичного ключа для всіх пристроїв з підтримкою WEP. Існують програми, що дозволяють зловмиснику визначити WEP-ключ. Ці програми можна знайти в мережі Інтернет.

Одним із засобів захисту від такої вразливості є часта зміна ключів. Існує удосконалений і безпечний засіб шифрування – **протокол захищеного доступу до Wi-Fi** (Wi-Fi Protected Access, **WPA**).

### Протокол WPA

У протоколі WPA використовуються ключі шифрування довжиною від 64 до 256 біт. При цьому WPA, на відміну від WEP, генерує нові динамічні ключі при кожній спробі клієнта встановити з'єднання з точкою доступу. З цієї причини WPA вважається більш безпечним, ніж WEP, так як його значно важче зламати.

В Україні використання Wi-Fi без дозволу ДП «Український державний центр радіочастот» можливе лише у разі використання точки доступу зі стандартною всенаправленной антеною (<6 дБ, потужність сигналу ≤ 100 мВт на 2,4 ГГц і ≤ 200 мВт на 5 ГГц) для внутрішніх (використання усередині приміщення) потреб організації (Рішення НКРЗІ (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації) № 914 від 06.09.2007 «Про видачу ліцензій на здійснення діяльності у сфері телекомунікацій та на користування радіочастотним ресурсом України»). У випадку використання зовнішньої антени необхідно реєструвати передавач і отримати дозвіл на експлуатацію радіоелектронного засобу від ДП УДЦР. Крім того, для діяльності з надання телекомунікаційних послуг із застосуванням Wi-Fi необхідно отримати ліцензію від НКРЗІ (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації).

## 9.4. Бездротові міські мережі (WMAN)

### 9.4.1. Технологія WiMAX

**WiMAX** (Worldwide Interoperability for Microwave Access) – телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв'язку на великих відстанях для широкого спектру пристроїв (від робочих станцій і портативних комп'ютерів до мобільних телефонів). WiMAX заснований на стандарті IEEE 802.16, який також називають Wireless MAN.

Назву «WiMAX» було створено WiMAX Forum – організацією, яка була заснована в червні 2001 року з метою просування і розвитку технології WiMAX. Форум описує WiMAX як «засновану на стандарті технологію, яка надає високошвидкісний бездротовий доступ до мережі, альтернативний виділеним лініям і DSL».

WiMAX підходить для вирішення наступних завдань:

- З'єднання точок доступу Wi-Fi між собою та з іншими сегментами Інтернет.
- Забезпечення бездротового широкосмугового доступу як альтернативи виділеним лініям і DSL.
- Надання високошвидкісних сервісів передачі даних і телекомунікаційних послуг.
- Створення точок доступу, що не прив'язані до географічного положення.

WiMAX дозволяє здійснювати доступ в Інтернет на високих швидкостях, з набагато більшим покриттям, ніж у Wi-Fi мережі. Це дозволяє використовувати технологію в якості «магістральних каналів», продовженням яких виступають традиційні DSL-і виділені лінії, а також локальні мережі. В результаті подібний підхід дозволяє створювати високошвидкісні мережі в масштабах цілих міст.

Розробники стандарту WiMAX шукали оптимальні рішення як для фіксованого, так і для мобільного використання, але поєднати всі вимоги в рамках одного стандарту не вдалося. Хоча ряд базових вимог збігається, націленість технологій на різні ринкові ніші призвела до створення двох окремих стандартів. Кожна із специфікацій WiMAX визначає свої робочі діапазони частот, ширину смуги пропускання, потужність випромінювання, методи передавання і доступу, способи кодування і модуляції сигналу, принципи повторного використання радіочастот та інші показники. А тому WiMAX-системи, засновані на версіях стандарту IEEE 802.16 e і d, практично несумісні. Короткі характеристики кожної з версій наведені нижче.

**802.16d** (або фіксований WiMAX). Специфікація затверджена в 2004 році. Використовується ортогональне частотне мультиплексування (OFDM – Orthogonal Frequency Division Multiplexing), підтримується фіксований доступ в зонах з наявністю або відсутністю прямої видимості. Пристрої користувачів являють собою стаціонарні модеми для встановлення поза і всередині приміщень, а також PCMCIA-карти для ноутбуків. У більшості країн під цю технологію відведені діапазони 3,5 і 5 ГГц. Багато аналітиків бачать в ній конкурентну або взаємодоповнюючу технологію кабельного широкосмугового доступу DSL.

**802.16e** (або мобільний WiMAX). Специфікація затверджена в 2005 році. Це новий виток розвитку технології фіксованого доступу (802.16d). Дана версія оптимізована для мобільних користувачів і підтримує ряд специфічних функцій, таких як хендовер (handover – процес переходу абонента від однієї базової станції до іншої), режим очікування (idle mode) та роумінг (roaming – процедура надання послуг зв'язку абоненту поза зоною покриття «домашньої» мережі (або базової станції) шляхом використання ресурсів базової станції іншого оператора зв'язку). Застосовується масштабований OFDM-доступ (SOFDMA – Scalable Orthogonal Frequency Division Multiplexing Access), можлива робота при наявності або відсутності прямої видимості. Плановані частотні діапазони для мереж Mobile WiMAX такі: 2,3; 2,5; 3,4-3,8 ГГц. Конкурентами 802.16e є мобільні технології третього покоління.

Основна відмінність двох технологій полягає в тому, що фіксований WiMAX дозволяє обслуговувати тільки «статичних» абонентів, а мобільний

орієнтований на роботу з користувачами, що пересуваються зі швидкістю до 120 км/год. Мобільність означає наявність функцій роумінгу і «безшовного» перемикання між базовими станціями при пересуванні абонента (як і в мережах стільникового зв'язку). У окремих випадках мобільний WiMAX може застосовуватися і для обслуговування фіксованих користувачів.

У загальному вигляді WiMAX мережі складаються з наступних основних частин – базових і абонентських станцій, а також обладнання, що зв'язує базові станції між собою та з постачальником послуг Інтернет.

Для з'єднання базової станції з абонентською використовується високочастотний діапазон радіохвиль від 1,5 до 11 ГГц. В ідеальних умовах швидкість обміну даними може досягати 70 Мбіт/с, при цьому не вимагається забезпечення прямої видимості між базовою станцією і приймачем.

Між базовими станціями встановлюються з'єднання (прямої видимості), що використовують діапазон частот від 10 до 66 ГГц, швидкість обміну даними може досягати 120 Мбіт/с. При цьому, принаймні одна базова станція підключається до мережі провайдера з використанням класичних кабельних з'єднань. Однак, чим більше число базових станцій підключено до мереж провайдера, тим вища швидкість передачі даних і надійність мережі в цілому.

Структура мереж стандартів IEEE 802.16 схожа із традиційними GSM мережами (базові станції діють на відстанях до десятків кілометрів, для їх встановлення не обов'язково будувати вежі – допускається установка на дахах будинків при дотриманні умови прямої видимості між станціями).

Обладнання для використання мереж WiMAX поставляється кількома виробниками і може бути встановлено як у приміщенні, так і поза ним.

### 9.4.2 Порівняння стандартів бездротового зв'язку

Дуже часто порівнюють технології WiMAX та Wi-Fi. Дані технології хоча і однаково використовують бездротове з'єднання та застосовуються для підключення до Інтернет (каналу обміну даними), але незважаючи на це, вони спрямовані на вирішення абсолютно різних завдань.

WiMAX – це система далекої дії, що покриває великі відстаней (десятки кілометрів), яка зазвичай використовує ліцензовані спектри частот (хоча можливо і використання неліцензованих частот) для надання ISP з'єднання із Інтернет типу «точка-точка» кінцевому користувачу. Різні стандарти сімейства 802.16 забезпечують різні види доступу: мобільний (схожий з передачею даних із мобільних телефонів) та фіксований (альтернатива кабельного доступу, при якому бездротове обладнання користувача прив'язане до місця розташування).

Wi-Fi – це система більш короткої дії, що зазвичай покриває сотні метрів, яка використовує неліцензовані діапазони частот для забезпечення доступу до мережі. Зазвичай Wi-Fi використовується користувачами для доступу до їх власної локальної мережі, яка може бути не підключена до Інтернет.

WiMAX і Wi-Fi мають зовсім різний механізм QoS (Quality of Service). WiMAX використовує механізм, що базується на встановленні з'єднання між базовою станцією та пристроєм користувача. Кожне з'єднання використовує спеціальний алгоритм планування, який може гарантувати йому однаковий параметр QoS. Wi-Fi, в свою чергу, використовує механізм QoS подібний тому, що використовується в Ethernet, при якому пакети отримують різний пріоритет. Такий підхід не гарантує однаковий QoS для кожного з'єднання.

Для тестування, стандартизації, сертифікації та маркетингу продуктів WiMAX створений індустріальний альянс WiMAX Forum. Саме він видає висновки WiMAX Forum Certified. Одним з найбільш активних членів альянсу WiMAX Forum є компанія Intel, яка бере участь у всіх його починаннях – від постановки завдання, закінчуючи ратифікацією стандартів і розробкою кінцевого обладнання.

У жовтні 2010 року Інститут інженерів електроніки та електротехніки (IEEE) затвердив стандарт IEEE 802.16m, відомий як **WiMAX 2**. Він дозволить підвищити пропускну здатність бездротових мереж у кілька разів. Так, стаціонарне обладнання в мережах нового покоління зможе приймати дані на швидкості до 1 Гбіт/с, а мобільні гаджети та портативні комп'ютери – до 100 Мбіт/с. При цьому збережеться зворотна сумісність з існуючим обладнанням WiMAX.

Стандарт WiMAX 2 повинен прийти на зміну нинішньому WiMAX (802.16e) і стати гідним конкурентом LTE. Його підтримує альянс комп'ютерних фірм, у числі яких Intel, Motorola та Samsung. Поява більш швидкісних стандартів бездротового зв'язку цілком затребувані ринком. За оцінкою аналітиків компанії Cisco, мобільний інтернет-трафік у світі буде щорічно подвоюватися і до 2018 року зросте до 7 млн. терабайт на місяць, в основному, за рахунок збільшення частки відео. За п'ять років відеотрафік для мобільних пристроїв зросте більш ніж у 100 разів.

Відразу після прийняття стандарту IEEE 802.16m (WiMAX-2) ініціативна група під назвою PAR (Project Authorization) почала роботу над новою версією цього стандарту IEEE 802.16n (**WiMAX 3.0**), який повинен забезпечити користувачам абсолютно неймовірні швидкості доступу до мереж – 10 Гбіт/с для каналів фіксованого зв'язку і до 1 Гбіт/с для мобільного зв'язку.

Перший WiMAX-оператор в Україні – Альтернет. Альтернет – це торгова марка, що належить ТОВ «Українські новітні технології». Мережа Альтернет почала роботу в листопаді 2005 року. На сьогодні в зону покриття мережі компанії входять міста: Київ, Харків, Донецьк, Дніпропетровськ, Одеса, Львів, Хмельницький та деякі інші.

У березні 2008 року про намір будувати національну мережу WiMAX оголосила компанія «ММДС-Україна», асоційована з СКМ Ріната Ахметова і Turkcell (торгова марка life:).

У вересні 2009 року було запущено мережу мобільного WiMAX Freshtel – проект компанії «Українські новітні технології». На момент запуску мережа функціонувала лише в центрі Києва.

У травні 2010 року почала функціонувати нова WiMAX-мережа у Києві від оператора Intellecom. Після запуску мережі в Києві Intellecom планує запустити WiMAX також в 10 інших великих містах України.

В таблиці 9.1 представлено порівняння стандартів бездротового зв'язку.

Таблиця 9.1. Порівняння стандартів бездротового зв'язку

| Технологія | Стандарт | Використання | Пропускна здатність | Радіус дії | Несучі частоти |
|---|---|---|---|---|---|
| Wi-Fi | 802.11a | WLAN | до 54 Мбіт/с | до 300 м | 5,0 ГГц |
| Wi-Fi | 802.11b | WLAN | до 11 Мбіт/с | до 300 м | 2,4 ГГц |
| Wi-Fi | 802.11g | WLAN | до 54 Мбіт/с | до 300 м | 2,4 ГГц |
| Wi-Fi | 802.11n | WLAN | до 450 Мбіт/с (в перспективі до 600 Мбіт/с) | до 300 м | 2,4 — 2,5 або 5,0 ГГц |
| WiMax | 802.16d | WMAN | до 75 Мбіт/с | 25-80 км | 1,5-11 ГГц |
| WiMax | 802.16e | Mobile WMAN | до 40 Мбіт/с | 1-5 км | 2,3-13,6 ГГц |
| WiMax 2 | 802.16m | WMAN, Mobile WMAN | до 1 Гбіт/с (WMAN), до 100 Мбіт/с (Mobile MAN) | до 100 км | 10-66 ГГц |
| WiMax 3 | 802.16n | WMAN, Mobile WMAN | до 10 Гбіт/с (WMAN), до 1 Гбіт/с (Mobile MAN) | н/д (стандарт в розробці) | н/д (стандарт в розробці) |

| | | | | | |
|---|---|---|---|---|---|
| Bluetooth v. 1.1 | 802.15.1 | WPAN | до 1 Мбіт/с | до 10 м | 2,4 ГГц |
| Bluetooth v. 2.0 | 802.15.3 | WPAN | до 2,1 Мбіт/с | до 100 м | 2,4 ГГц |
| Bluetooth v. 3.0 | 802.11 | WPAN | от 3 Мбіт/с до 24 Мбіт/с | до 100 м | 2,4 ГГц |
| UWB | 802.15.3a | WPAN | 110-480 Мбіт/с | до 10 м | 7,5 ГГц |
| ZigBee | 802.15.4 | WPAN | от 20 до 250 Кбит/с | 1-100 м | 2,4 ГГц (16 каналов), 915 МГц (10 каналов), 868 МГц (один канал) |
| Інфрачервоний порт | IrDa | WPAN | до 16 Мбит/с | до 10 м | |

## 9.5. Бездротові глобальні мережі (WWAN)

### 9.5.1. Радіорелейний зв’язок

Радіорелейні станції (РРС) використовують для передавання аналогового сигналу в телебаченні та цифрового послідовного коду згідно стандарту ITU G.703 в телефонії.

Радіорелейну лінію зв’язку утворюють декілька веж, на яких встановлені параболічні спрямовані антени. Кожна така лінія працює в мікрохвильовому діапазоні на частотах в декілька гігагерц. Спрямована антена концентрує енергію у вузькому пучку, що дозволяє передавати інформацію на значні відстань, зазвичай до 60-80 км. Високі вежі забезпечують пряму видимість антен.

Це можуть бути як магістральні лінії, так і лінії доступу. Оператори зв’язку часто використовують подібні лінії, коли прокладка оптичного волокна або неможлива (через природні умови), або економічно невигідна.

Пропускна здатність лінії може бути досить високою – до 155 Мбіт/с (потік STM-1 синхронної цифрової ієрархії, SDH) або до 140 Мбіт/с (потік E4 плезіохронної цифрової ієрархії, PDH). Для наземного радіорелейного зв’язку використовують частотні діапазони від 0,39 ГГц до 40,5 ГГц.

Граничним випадком радіорелейного зв’язку є супутниковий зв’язок – у ньому ретранслятор винесений на максимально можливу висоту (десятки тисяч кілометрів), і в зоні його видимості – майже половина земної кулі.

Глобальна мережа радіорелейного зв’язку активно розгорталась в СРСР в 70-х роках минуло століння. Це було набагато дешевше, ніж прокладати кабельні лінії, особливо в умовах величезних просторів з нерозвиненою інфраструктурою, та й високі ж швидкості передавання інформації тоді ще не були потрібні. Пізніше на її основі будувалася мережа стільникового зв’язку, особливо в регіонах.

### 9.5.2. Супутникові технології

Супутниковий зв’язок – один з видів радіозв’язку, що базується на використанні штучних супутників Землі, на яких змонтовані ретранслятори. Супутниковий зв’язок здійснюється між земними станціями, які можуть бути як стаціонарними, так і мобільними.

Для супутникового зв’язку союз МСЕ виділив кілька частотних діапазонів (табл. 9.2).

Таблиця 9.2. Частотні діапазони супутникового зв’язку

| Діапазон | Низхідна частота, ГГц | Висхідна частота, ГГц |
|---|---|---|
| L | 1,5 | 1,6 |
| S | 1,9 | 2,2 |
| C | 3,7–4,2 | 5,925–6,425 |
| Ku | 11,7–12,2 | 14,0–14,5 |
| Ka | 17,7–21,7 | 27,5–30,5 |

Історично першим використовувався діапазон С, в якому для кожного з дуплексних потоків Земля-супутник (висхідна частота) і супутник-Земля (низхідна частота) виділяється по 500 МГц – цього достатньо для великого числа каналів. Діапазони L і S призначаються для організації мобільних послуг за допомогою супутників. Вони також часто використовуються наземними системами. Діапазони Ku і Ka поки мало «населені», їх застосуванню перешкоджає висока вартість обладнання, особливо для Ka діапазону.

Орбіта обертання супутника навколо Землі, в загальному випадку, є еліптичною, але для збереження постійної висоти над Землею супутники можуть переходити на майже кругову орбіту.

Сьогодні використовують три групи кругових орбіт, що відрізняються висотою над Землею:

- геостаціонарна орбіта (Geostationary Orbit, GEO) – 35 863 км;
- середньовисотна орбіта (Medium Earth Orbit, MEO) – 5000-15 000 км;

- маловисотних орбіта (Low Earth Orbit, LEO) – 100-1000 км.

Найпопулярнішими супутниковими технологіями є:

- технологія VSAT;
- технології на базі низькоорбітальних супутників LEO.

**Технологія VSAT** (Very Small Aperture Terminal – термінал з дуже малою апертурою) використовує для передавання даних геостаціонарні супутники. Системи VSAT надають послуги супутникового зв'язку клієнтам (як правило, невеликим організаціям), яким не потрібна висока пропускна здатність каналу. Швидкість передавання даних для VSAT-терміналу, зазвичай, не перевищує 2048 Кбіт/с.

Слова «дуже мала апертура» відносяться до розмірів антен терміналів в порівнянні з розмірами більш старих антен магістральних систем зв'язку. VSAT-термінали, що працюють в С-діапазоні, зазвичай використовують антени діаметром 1,8-2,4 м, в Ku-діапазоні – 0,75-1,8 м.

Водночас технологія VSAT відрізняється значними затримками передавання даних, зумовленими великою відстанню до супутника (затримка становить приблизно 250 мкс, тоді як для кабельних мереж – 15 мкс). Тому канал VSAT не можна використовувати у системах реального часу та оперативного зв'язку.

Окрім того, місце на орбіті геостаціонарного супутника регулюється союзом ITU. Сьогодні спостерігається певний дефіцит таких місць, так як геостаціонарні супутники не можуть розташовуватися на орбіті ближче, ніж 2° один до одного. З цього випливає, що на орбіті може перебувати не більше 180 геостаціонарних супутників.

**Технології на базі низькоорбітальних супутників LEO**, як і системи VSAT, для передавання використовують супутник. Супутник розміщено на висоті близько 100 км на звичайній, а не геостаціонарній орбіті. У цьому випадку зменшується затримка в передаванні даних. Крім того, вивести такий супутник на орбіту значно дешевше, ніж геостаціонарний. Водночас для підтримування постійного зв'язку необхідно використовувати велику кількість таких низькоорбітальних супутників. Серед наявних проектів LEO можна виділити системи Iridium та Globalstar.

**Iridium (Іридій)** – всесвітній оператор супутникового телефонного зв'язку. Покриття становить 100% поверхні Землі, включаючи обидва полюси. Система Iridium налічує 66 супутників, що розташовані на низьких орбітах з нахилом 86,5° на висоті 780 км.

Свою назву система отримала в зв'язку з тим, що спочатку планувалося створити систему з 77 супутників. Це число дорівнює атомному номеру іридію.

На кінець 2009 року мережа Iridium налічувала близько 400 000 абонентів, в число яких увійшли співробітники великих світових корпорацій, що працюють у сфері видобутку корисних копалин, морського, наземного та повітряного транспорту, будівництва, туризму, інших галузях і службах порятунку та екстреної допомоги. Одним з найбільших користувачів мережі є уряд США.

**Globalstar (Глобалстар)** – це система із групи супутників низької навколоземної орбіти, що призначена для супутникових телефонів і низькошвидкісного передавання даних.

Система Globalstar налічує 48 супутників та 4 запасних частини, що розташовані на низьких орбітах з нахилом 52°. Таким чином, Globalstar не поширюється на полярні райони.

Висота орбіти Globalstar близько 1400 км, час затримки відносно низький (близько 60 мс).

У 2005 році, деякі з супутників стали доходити до межі їх терміну експлуатації – 7,5 років. У грудні 2005 року Globalstar почав переміщати деякі з його супутників на орбіту поховання вище навколоземної орбіти.

Маючи більш ніж 315 000 абонентів (за даними на 2008 р.), Globalstar є найбільшим в світі постачальником мобільного супутникового зв'язку і передачі даних. Globalstar пропонує свої послуги для рекламних та розважальних користувачів в більш ніж 120 країнах світу. Продукти компанії включають мобільні та фіксовані супутникові телефони, пакети супутникового ефірного часу.

### 9.5.3. Технології передавання даних в стільникових мережах

Мережі на стільникових модемах використовують наявну інфраструктуру стільникової телефонії. На фізичному та канальному рівнях розрізняють аналогові та цифрові методи доступу, які відображені у різноманітних технологіях.

Класичними методами доступу, які використовують для передавання аналоговий сигнал є:

1. **FDMA** (Frequency Division Multiple Access – множинний доступ з поділом по частоті**)**
2. **TACS** (Total Access Communications System – система зв'язку повного доступу**).**

Аналогові методи доступу виділяють для кожного передавання окремий канал – смугу частот у призначеному для мережі діапазоні. У цьому випадку сусідні стільникові комірки не можуть працювати в одному й тому ж діапазоні частот (інакше передавання в сусідніх комірках заважали б одне одному).

Основними методами доступу для цифрового передавання є:

**1. TDMA** (Time Division Multiple Access – множинний доступ з часовим поділом) – використовує принцип розподілу часу передавання на окремі часові слоти.

Даний метод дозволяє кільком користувачам використовувати одну частоту (радіо канал), але лише в певні інтервали часу. Ці інтервали (кадри) надаються почергово кожному користувачу каналу, через які він може передавати чи приймати інформацію.

**2. CDMA** (Code Division Multiple Access – множинний доступ з кодовим поділом).

В основі CDMA лежить технологія передавання **DSSS** (Direct Sequence Spread Sequence – розширення спектру методом прямої послідовності). Послідовність інформаційних бітів множать на псевдовипадкову послідовність коротких імпульсів. Одержують сигнал, що є в ширшому частотному спектрі й має значно меншу інтенсивність. Для декодування такої послідовності необхідно знати псевдовипадкову послідовність, яку використовували під час передавання. Цей механізм кодування забезпечує сигнал захищений від підслуховування.

Особливістю, що поліпшує якість передавання у CDMA-мережах, є механізм відпрацювання переходу абонента з однієї комірки в іншу. В інших технологіях під час такого переходу спочатку розривається зв’язок з однією базовою станцією, а потім налагоджується з іншою. Це знижує якість передавання. У технології CDMA завдяки збереженню однієї частоти-носія у сусідніх комірках можна спочатку налагодити з’єднання з новою станцією, а вже потім розірвати з попередньою. Це поліпшує якість переходу і дає змогу коректно опрацювати передавання у «прикордонній зоні», коли передавач може багато разів переходити зі сфери обслуговування однієї базової станції у сферу обслуговування іншої та навпаки.

**3. CDPD** (Cellular Digital Packet Data – цифрова стільникова пакетна передача даних). Стандарт CDPD розроблений у 1992 році IBM і Pacific Communications Sciences для бездротового широкосмугового асинхронного передавання даних. Дані передаються в інтервалах між звичайними голосовими дзвінками, коли стільникова мережа зв’зку вільна.

Мережа CDPD може взаємодіяти з існуючими мережами стільникового телефонного зв’язку. Забезпечує передачу даних зі швидкістю до 19,2 Кбіт/с, вихід у Internet і міжмережевий роумінг.

Технологія CDPD реалізує як пакетне передавання (протокол TCP/IP), так і модемний інтерфейс (AT-команди). На відміну від радіомодемів, стільникові модеми використовують не спеціальні антени та приймачі-передавачі, а наявні пристрої стільникового телефону.

Сьогодні важко собі уявити стільниковий зв’язок без передавання даних. За останні 30 років було розроблено 4 покоління (Generation) мобільного зв’язку, у яких швидкості передавання інформації по стільникових мережах збільшились в сотні тисяч раз.

В технологіях стільникового зв’язку першого покоління (1 Generation, 1G), коли стільниковий телефон використовувався в першу чергу для здійснення дзвінків, для стандарту NMT (Nordic Mobile Telephone – аналоговий стандарт стільникового зв’язку в діапазоні частот від 453 до 468 МГц) у 1981 році була запропонована нова послуга – передача даних. Максимальна швидкість була обмежена 1,2 Кбіт/с. У ті часи ще не було мережі Інтернет, і основне призначення даної послуги було передача тексту. Однак у той час ця послуга не знайшла особливого інтересу і лише кілька операторів вирішили реалізувати її на практиці.

Стандарт GSM (Global System for Mobile Communications – глобальна система мобільного зв’язку) – це стандарт другого покоління (2G) стільникового зв’язку, в якому вперше передбачалася послуга передачі даних ще до початку розробки. Вона реалізовувалася на основі технології CSD (Circuit Switched Data – передавання даних з комутацією каналів) з максимальною швидкістю 9,6 Кбіт/с. Дані передавалися всередині розмовних каналів. Відповідно, швидкість була обмежена пропускною здатністю одного таймслота. За допомогою технології HSCSD (High Speed CSD – високошвидкісне передавання даних з комутацією каналів) швидкість передачі даних була збільшена до 57,6 Кбіт/с. Це було досягнуто за рахунок можливості об’єднання кількох вільних таймслотів для передачі даних одного абонента.

Дані, у випадку з комутованим з’єднанням, передаються по розмовних каналах аж до MSC (Mobile Switching Centre – центр комутації) і комутуються через нього в напрямку до інших мереж передавання даних. При цьому максимальна сумарна швидкість обмежена швидкістю передавання по окремим таймслотах. Щоб ще збільшити максимально-можливу швидкість необхідно відокремити дані від голосу ще до передавання центральному комутатору. Крім того, потрібно змінити спосіб кодування інформації на радіоінтерфейс між базовою станцією та телефоном абонента.

З урахуванням цього була розроблена технологія GPRS (General Packet Radio Service – загальний сервіс пакетного радіопередавання). Передані дані відділялися від решти трафіку в контролері базових станцій, який зазнавав заміну програмного забезпечення і деякі апаратні доопрацювання. Також для мережі GPRS додавалися два нових елементи: GGSN (Gateway GPRS Support Node – шлюз обслуговування абонентів GPRS) та SGSN (Serving GPRS Support Node –

вузол обслуговування абонентів GPRS). Швидкість передавання даних в мережах GPRS може досягати 171,2 Кбіт/с.

Наступним кроком збільшення швидкості передавання даних стала зміна способу модуляції переданих даних на радіоінтерфейсі. Завдяки цьому швидкість була збільшена до 326 Кбіт/с. Ця технологія отримала назву EDGE (Enhanced Data rates for GSM Evolution – розвиток GSM з підвищенням швидкості передавання даних) – найбільш швидкісна технологія передавання даних в мережах GSM (2,75G).

GSM є найпоширенішим стандартом у світі. За 10 років кількість користувачів мереж GSM досягло 500 мільйонів, причому їхній щоденний приріст складає 1 мільйон. Станом на 2011 у світі працює 838 GSM-мереж в 234 країнах.

Технологію EDGE підтримують всі мобільні оператори України (окрім Goldentelecom), які надають послуги зв'язку GSM: Beeline, Life:), Київстар, МТС Україна. EDGE працює майже скрізь, де є покриття мережі мобільного зв'язку. Незважаючи на це, завантаження мереж мобільного зв'язку поки що не дозволяє повністю використовувати швидкісний потенціал цієї технології.

Експлуатація систем стільникового зв'язку другого покоління показала зацікавленість абонентів у високошвидкісному передаванні даних, що створило передумову для появи стандарту третього покоління (3G) – UMTS (Universal Mobile Telecommunications System – універсальна мобільна телекомунікаційна система). Дана технологія була розроблена ETSI (European Telecommunications Standards Institute). UMTS для передавання даних через повітряний простір використовує технологію W-CDMA (Wideband Code Division Multiple Access – широкосмуговий множинний доступ із кодовим розподілом каналів).

Максимальна швидкість передавання даних для даного стандарту обмежується 2 Мбіт/с. Таке збільшення швидкості обумовлено змінами в способі передавання даних між базовою станцією і терміналом абонента. Наступним кроком стала поява технології HSDPA (High Speed Downlink Packet Access – високошвидкісний пакетний доступ у зворотньому напрямку), яка надає швидкості передавання даних до 14,4 Мбіт/с. Зміні, в даному випадку, піддався спосіб модуляції даних на шляху від базової станції до телефону. HSDPA прийнято відносити до мереж покоління «3,5G».

Обсяги переданої інформації з телекомунікаційних мережах збільшується щорічно і навіть технологія HSDPA перестане задовольняти потреби користувачів. З метою вирішення проблеми пропускної здатності був розроблений стандарт четвертого покоління (4G), який отримав назву LTE (Long Term Evolution – довготерміновий розвиток). Окрім збільшення швидкості передавання даних даний стандарт дозволяє збільшити ємність мережі і

підсилити безпеку. Максимальна швидкість передавання теоретично може досягати 326,4 Мбіт/с. У грудні 2009 року була запущена в комерційну експлуатацію перша система стільникового зв'язку цього стандарту.

Таким чином, за неповні три десятиліття швидкості передавання інформації по стільникових мереж зв'язку збільшилися в сотні тисяч разів (табл. 9.3).

Таблиця 9.3. Технології стільникових мереж для передавання даних

| Покоління | Назва технології | Максимальна швидкість передавання даних |
|---|---|---|
| 1G | NMT (Nordic Mobile Telephone – аналоговий стандарт стільникового зв'язку) | 1,2 Кбіт/с |
| 2G | GSM (Global System for Mobile Communications – глобальна система мобільного зв'язку) | 9,6 Кбіт/с |
| 2G | CSD (Circuit Switched Data – передавання даних з комутацією каналів) | 9,6 Кбіт/с |
| 2G | HSCSD (High Speed CSD – високошвидкісна передача даних з комутацією каналів) | 57,6 Кбіт/с |
| 2G | GPRS (General Packet Radio Service – загальний сервіс пакетного радіопередавання) | 171,2 Кбіт/с |
| 2,75G | EDGE (Enhanced Data rates for GSM Evolution – розвиток GSM з підвищенням швидкості передавання даних) | 326 Кбіт/с |
| 3G | UMTS (Universal Mobile Telecommunications System – універсальна мобільна телекомунікаційна система) | 2 Мбіт/с |
| 3,5G | HSDPA (High Speed Downlink Packet Access – високошвидкісний пакетний доступ у зворотньому напрямку) | 14,4 Мбіт/с |
| 4G | LTE (Long Term Evolution – довготерміновий розвиток) | 326,4 Мбіт/с |

# 10. Ethernet операторського класу

## 10.1. Області покращення технології Ethernet

Класична технологія Ethernet розроблялась виключно як технологія локальних мереж, і до недавнього часу мережі цього класу були єдиною областю застосування цієї технології. Однак безперечний успіх Ethernet в локальних мережах, де вона витіснила всі інші технології, привів до ідеї про використання цієї технології і в глобальних мережах (які здебільшого є операторськими).

Потенційних переваг від експансії Ethernet за межі локальних мереж декілька.

Для користувачів технологія Ethernet важлива в якості послуги глобальних мереж. Ця послуга може у різних провайдерів називатися по-різному – Carrier Ethernet, Ethernet VPN, VPLS, ELINE або ELAN – суть від цього не змінюється: користувачі отримують можливість з'єднати свої територіально розосереджені мережі, під'єднуючи їх до інтерфейсу Ethernet, що надає провайдер. При цьому мережі об'єднуються на рівні Ethernet, без залучення протоколу IP. Це означає, що мережа провайдера враховує лише MAC-адреси, ідентифікатори VLAN і фізичний інтерфейс користувача для того, щоб належним чином забезпечити об'єднання мереж користувача.

При цьому користувачі мають справу з добре вивченою технологією на інтерфейсах доступу до мережі провайдера, тобто **мережевих інтерфейсах користувача** (User Network Interface, **UNI**). Крім того, при з'єднанні мереж на канальному рівні користувачі вільні в IP-адресації своїх мереж, так як при передачі трафіку між мережами користувачів послуги Ethernet операторського класу провайдер не застосовує IP-адреси. Таким чином, можна, наприклад, призначити адреси однієї і тієї ж IP-підмережі для всіх мереж користувачів або ж задіяти приватні IP-адреси. Це загальна властивість послуг VPN канального рівня, але сьогодні така послуга практично завжди виглядає як послуга з інтерфейсом Ethernet.

Для провайдерів технологія Ethernet операторського класу важлива не лише як популярна послуга, а й як внутрішня транспортна технологія канального рівня – **Carrier Ethernet Transport** (**CET**), що може використовуватись для реалізації глобальних послуг Ethernet або ж створення надійних, швидкісних і контрольованих з'єднань між маршрутизаторами. Привабливість Ethernet як внутрішньої транспортної технології для операторів зв'язку пояснюється відносно низькою вартістю обладнання Ethernet. Порти Ethernet завжди мали найнижчу вартістю в порівнянні з портами будь-який інший технології (з урахуванням швидкості передачі даних портом). Низька вартість є результатом

простоти технології Ethernet, яка пропонує тільки мінімальний набір функцій з передачі кадрів в режимі доставки по можливості (з максимальними зусиллями), не підтримуючи ні контроль над маршрутами трафіку, ні моніторинг працездатності з'єднання між вузлами.

Прагнення до уніфікації також приводить до експансії Ethernet в глобальні мережі. Мережевий рівень вже давно демонструє однорідність завдяки домінуванню протоколу IP, і перспектива отримати однорідний канальний рівень у вигляді Ethernet виглядає дуже привабливою.

Однак, в своєму класичному вигляді технології локальної мережі, Ethernet не готова використовуватись в глобальних мережах. Для того, щоб успішно працювати в мережах операторів зв'язку, технологія і обладнання Ethernet повинні володіти певним набором характеристик, серед яких в першу чергу потрібно відзначити надійність, відмовостійкість, масштабованість і керованість. Еталоном такої технології може служити технологія SDH, яка довгі роки використовується в мережах операторів зв'язку, поєднуючи своїми каналами маршрутизатори, телефонні станції і будь-яке інше обладнання провайдера. Технологія MPLS також може виступати в якості такого еталона.

Для того, щоб перетворити класичний варіант технології Ethernet, що використовується в LAN, в транспортну технологію операторського класу (тобто CET), здатну працювати в мережі провайдера в якості основного транспортного механізму, необхідно до даної технології додати ряд нових функцій та властивостей.

### 1. Функції експлуатації, адміністрування і обслуговування

Функції експлуатації, адміністрування і обслуговування (Operation, Administration, Maintenance**,** OAM) завжди були слабкою ланкою Ethernet, і це одна з головних причин, по якій оператори зв'язку не хотіли застосовувати цю технологію в своїх мережах. Нові стандарти, пропоновані IEEE і MCE-T, покликані виправити цю ситуацію, вводячи засоби, за допомогою яких можна виконувати моніторинг досяжності вузлів, локалізувати несправні сегменти мережі і вимірювати рівень затримок і втрат кадрів між вузлами мережі.

### 2. Розподіл адресних просторів користувачів і провайдера

Адресний простір сучасної комутованої мережі Ethernet складається з двох частин: значень MAC-адрес кінцевих вузлів і значень ідентифікаторів **локальних віртуальних мереж** (Virtual Local Network, **VLAN**), на які логічно розділена мережа. Комутатори Ethernet при ухваленні рішення про просування кадру враховують обидва адресних параметра. Якщо мережа провайдера становитиме з мережами користувачів єдине ціле на рівні Ethernet, то така

мережа виявиться практично непрацездатною, так як всі комутатори провайдера повинні будуть в своїх таблицях комутації містити MAC-адреси всіх кінцевих вузлів всіх користувачів, а також підтримувати прийняте кожним користувачем розбиття мережі на локальні віртуальні мережі. Крім очевидної проблеми кількості MAC-адрес (для великого провайдера це значення може доходити до декількох мільйонів), є ще проблема їх унікальності – хоча система призначення адрес і покликана запобігти дублюванню «апаратних» MAC-адрес, існують ще й програмовані адреси, та й помилки в прошивці апаратних адрес теж трапляються.

Застосування в мережі провайдера для користувача ідентифікаторів VLAN також призводить до проблем. По-перше, користувачам потрібно домовлятися про узгоджене застосування ідентифікаторів VLAN, для того, щоб вони були унікальними для кожного користувача, оскільки лише тоді мережа провайдера зможе доставляти кадри потрібним мережам користувача. Крім того, стандарт VLAN спочатку не був розрахований на глобальне застосування і тому в ньому передбачено лише 4092 значення мітки, що вкрай мало для великого провайдера.

### 3. Маршрутизація, інжиніринг трафіку і відмовостійкість

Оператори зв’язку звикли до ситуації повного контролю над шляхами проходження трафіку в своїх мережах, що забезпечує, наприклад, технологія SDH. В IP-мережах ступінь контролю оператора над маршрутами трафіку дуже низька, і однією з причин популярності технології MPLS є те, що вона привнесла в IP-мережі можливості інжинірингу трафіку. Іншою бажаною для операторів характеристикою мережі є відмовостійкість маршрутів, тобто можливість швидкого переходу на новий маршрут при відмовах вузлів або ліній зв’язку мережі. Технологія SDH завжди була в цьому плані еталоном, так як забезпечує перехід з основного на заздалегідь прокладений резервний шлях за десятки мілісекунд. Подібною властивістю володіє також технологія MPLS.

У мережах Ethernet маршрутизація трафіку і відмовостійкість забезпечуються **протоколом покриваючого дерева** (Spanning Tree Protocol, **STP**). Цей протокол дає адміністратору мережі обмежений контроль над вибором маршруту (це справедливо і для нових варіантів STP, таких як RSTP і MSTP). Крім того, STP є загальним для всіх потоків незалежно від їх адреси призначення. Зважаючи на ці особливості протокол STP є поганим рішенням щодо інжинірингу трафіку. І хоча STP забезпечує відмовостійкість маршрутів, але час перемикання на новий маршрут складає декілька десятків секунд, що дуже далеко до мілісекундного діапазону SDH. Все це вимагає нового підходу до маршрутизації потоків в мережах CET, і IEEE працює над цією проблемою.

## 10.2. Функції OAM в Ethernet операторського класу

До теперішнього часу розроблено декілька стандартів, що відносяться до функцій експлуатації, адміністрування та обслуговування, необхідних для перетворення технології Ethernet в Ethernet операторського класу:

- IEEE 802.1ag. **Connectivity Fault Management** (Управління несправностями з'єднань, **CFM**). Стандарт описує протокол моніторингу стану з'єднань.
- MCE-T Y.1731. Стандарт комітету ITU-T відтворює функції стандарту IEEE 802.1ag CFM і розширює їх за рахунок групи функцій моніторингу параметрів QoS.
- IEEE 802.3ah. Стандарт тестування фізичного з'єднання Ethernet.
- MEF E-LMI. Інтерфейс локального управління Ethernet.

### Протокол CFM

Протокол CFM забезпечує моніторинг логічних з'єднань Ethernet. Цей протокол орієнтується на техніку віртуальних локальних мереж (VLAN). Під логічним з'єднанням в ньому розуміється з'єднання вузлів, що належать одній мережі VLAN. Протокол CFM розрахований на тестування з'єднань будь-якої топології: «точка-точка», зірка, повнозв'язної.

Протокол CFM може виконувати моніторинг як в мережі, що належить одному провайдеру (однодоменний сценарій), так і в тих випадках, коли з'єднання проходить через мережі кількох провайдерів (багатодоменний сценарій).

Моніторинг виконується між так званими **кінцевими точками обслуговування** (Maintenance End Point, **MEP**), що являють собою кінцеві точки з'єднання, стан якого потрібно спостерігати.

Кожна з точок MEP періодично посилає **повідомлення перевірки безперервності з'єднання** (Continuity Check Message, CCM), що оформлені як кадри мережі VLAN, з'єднання якої тестується. Наприклад, якщо спостерігається з'єднання VLAN5, то повідомлення CCM оформляються як кадри Ethernet з ідентифікатором VLAN, рівним 5. З'єднання між точками MEP тестується окремо в кожному напрямку.

Моніторинг CFM здійснюється шляхом **активних вимірювань**, так як для його реалізації генеруються службові повідомлення CCM, а не використовуються кадри користувацького трафіку.

Пристрої, які не мають точок MEP, передають повідомлення CCM транзитом.

У тому випадку, коли деяка точка MEP не приймає повідомлення CCM від іншої точки MEP протягом заданого тайм-ауту, з'єднання вважається **непрацездатним**.

У проміжних пристроях, через які проходить з'єднання, можна конфігурувати **проміжні точки обслуговування** (Maintenance Intermediate Point, MIP). Ці точки допомагають локалізувати проблему, збираючи статистику про повідомлення CCM, що проходять через них транзитом, самі вони такі повідомлення не генерують. Допомога MIP полягає в тому, що при наявності проблеми (тобто в тому випадку, коли повідомлення CCM не проходять від однієї точки MEP до іншої) факт проходження повідомлень CCM через деяку точку MIP говорить про те, що даний сегмент мережі працездатний і причину проблеми потрібно шукати в іншому сегменті.

На рис. 10.1 показаний приклад моніторингу стану з'єднання локальної віртуальної мережі VLAN 5. Ця мережа має повнозв'язну топологію, тому комп'ютери C1, C2 і C3 можуть взаємодіяти між собою за принципом «кожен з кожним». Для моніторингу мережі VLAN5 створені три точки, MEP1, MEP2 і MEP3, які розташовуються на інтерфейсах комутаторів S1, S2 і S5 відповідно.

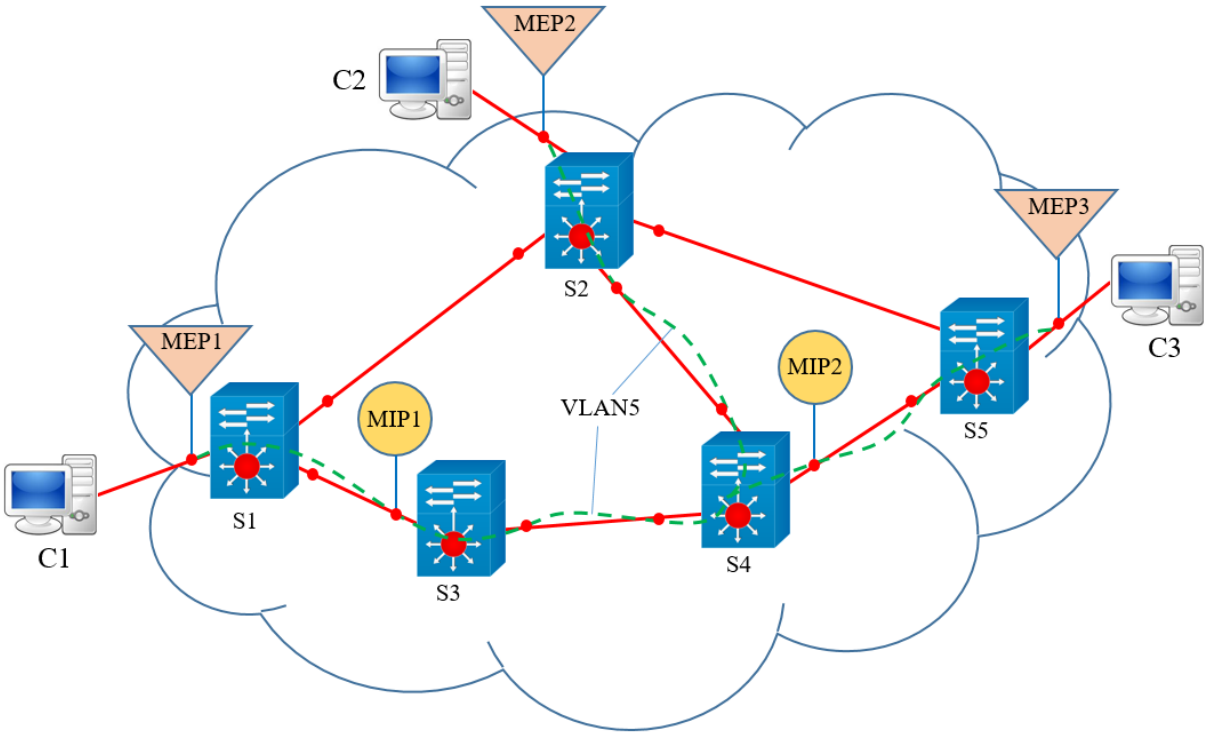



Рис. 10.1. Моніторинг стану VLAN за допомогою протоколу CFM

Для того, щоб здійснювати моніторинг з'єднань повнозв'язної топології, яку має VLAN5, повідомлення CCM надсилаються з груповою MAC-адресою.

Для моніторингу двоточкових з'єднань можуть використовуватися як індивідуальні, так і групові MAC-адреси.

У прикладі на рис. 10.1 точка MEP1 періодично посилає в мережу VLAN5 повідомлення CCM з груповою адресою. Якщо мережа VLAN5 працездатна, то точки MEP2 і MEP3 регулярно отримують повідомлення CCM, що відправляються точкою MEP1. Також регулярно передаються і приймаються повідомлення CCM, які генеруються точками MEP2 і MEP3. В результаті протокол CFM визначає статус мережі VLAN5 як працездатної.

Припустимо тепер, що в мережі відбулася відмова фізичного з'єднання між комутаторами S4 і S5. Внаслідок цього точка MEP3 перестає приймати повідомлення CCM від точок MEP1 і MEP2, а вони, в свою чергу, – повідомлення CCM від точки MEP3. У той же час точки MEP1 і MEP2 як і раніше продовжують обмінюватися повідомленнями CCM. Результатом моніторингу буде перехід з'єднання VLAN5 в стан часткової працездатності, коли лише частина вузлів виявляється досяжною.

Припустимо, що зв'язок між комутаторами S4 і S5 відновлений, але з якоїсь причини втрачено зв'язок між комутаторами. Точка MEP1 при цьому перестає приймати повідомлення від точки MEP3, а точка MEP3 – від точки MEP1 (для спрощення аналізу проігноруємо точку MEP2 і контрольовану нею частина мережі). Точки MEP1 і MEP3 фіксують порушення зв'язку між собою, але їх інформація не дозволяє судити про те, де конкретно в мережі виникла проблема, – відмова могла статися в будь-якому з трьох сегментів мережі між комутаторами S1 і S5. Оскільки в мережі є точки MIP, то адміністратор може проаналізувати їх статистику. Статистика MIP1 покаже, що через цю точку і раніше проходять повідомлення CCM від MEP1, але не проходять повідомлення MEP3. Статистика MIP2 покаже зворотне –наявність повідомлень від MEP3, але не від MEP1. Ці дані свідчать про те, що зв'язок втрачено між комутаторами S3 і S4.

Важливою є здатність протоколу CFM працювати в багатодоменному середовищі, коли з'єднання проходить через кілька мереж, що належать різним адміністративним доменам. Кожен з адміністраторів домену потребує моніторингу з'єднання, але тільки в межах своєї мережі. Для підтримки моніторингу стану з'єднань в багатодоменній мережі для протоколу CFM конфігурується окремий домен моніторингу, при цьому домени моніторингу утворюють ієрархію доменів різного рівня моніторингу. У кожному домені створюються точки обслуговування MEP і MIP, але точки кожного домена працюють тільки з повідомленнями CCM свого рівня, а повідомлення більш високих рівнів просто прозоро передають.

На рис. 10.2 показана мережа, що складається з доменів різних типів: домена користувача, домену провайдера послуги віртуальної приватної мережі та домену оператора зв’язку, через який працює мережа провайдера послуги. У мережі є три домену операторів: оператора А, оператора В і оператора С. Домени операторів вкладені в домен провайдера послуг, який надає користувачеві послуги віртуальної локальної мережі «з кінця в кінець». На верхньому рівні знаходиться домен користувача, в який входить домен провайдера послуги.

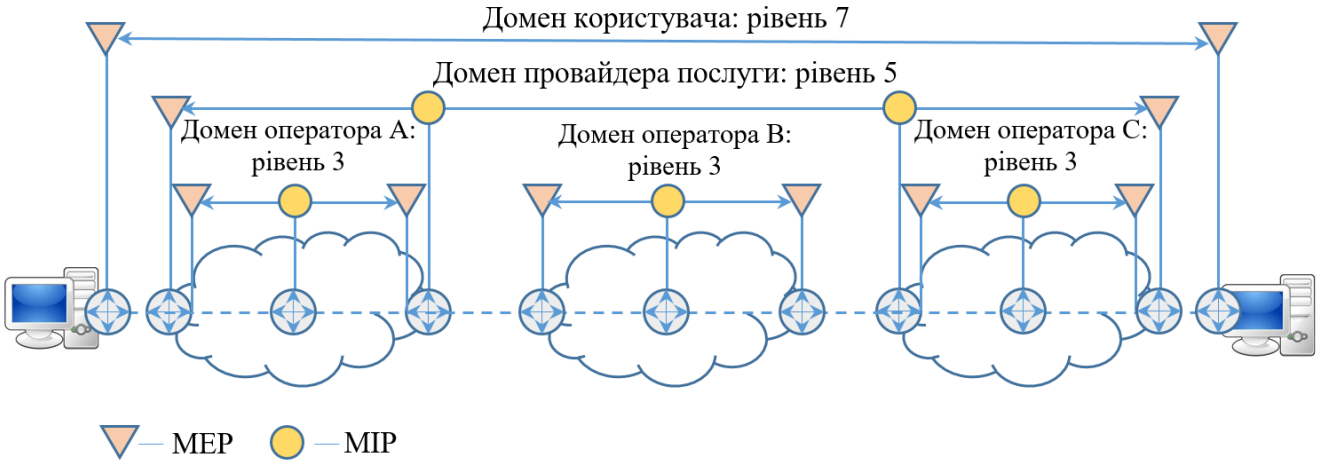



Рис. 10.2. Багатодоменне застосування протоколу CFM

Домену користувача привласнений рівень 7, домену провайдера – 5 рівень, домену оператора зв’язку – рівень 3. Точки MEP на інтерфейсах обладнання оператора зв’язку працюють з повідомленнями CCM рівня 3, а повідомлення точок обслуговування мережі користувача рівня 7 і мережі провайдера послуги рівня 5 вони передають прозоро. Аналогічно, точки провайдера послуги працюють на інтерфейсах його обладнання на рівні 5, вони прозоро передають повідомлення CCM рівня домену користувача 7. Повідомлення рівня 3 до точок MEP рівня 5 не доходять, тому що завершуються в точках MEP рівня 3.

В результаті кожен оператор зв’язку отримує інформацію про стан з’єднання в межах своєї мережі, провайдер. Такий ієрархічний спосіб організації сеансів між точками MEP дає можливість проводити незалежний моніторинг одного і того ж з’єднання різними організаціями без необхідності координувати конфігурацію точок моніторингу – досить узгодити рівні точок MEP, що використовуються кожною організацією. Обов’язковою умовою є вкладеність доменів кожного рівня в домен вищого рівня ієрархії.

## Протокол моніторингу якості з'єднань Y.1731

Стандарт Y.1731, розроблений MCE-T, додає до стандарту CFM можливість вимірювати деякі додаткові параметри між точками моніторингу мережі.

- *Одностороння затримка кадру.* Для вимірювання цієї затримки точки обслуговування мережі MEP генерують повідомлення вимірювання затримки і відповіді на вимір затримки. У цих повідомленнях переносяться тимчасові позначки, що дозволяють виміряти затримку.
- *Варіація затримки*. Ця затримка вимірюється на основі тих же повідомлень, що і одностороння затримка.
- *Втрати кадрів*. Для вимірювання цієї величини служать повідомлення виміру втрат і відповіді на вимір втрат. Лічильники повідомлень двох точок обслуговування порівнюються, і на основі цього порівняння розраховуються втрати кадрів в кожному з напрямків.

## Стандарт тестування фізичного з'єднання Ethernet

Стандарт тестування фізичного з'єднання Ethernet IEEE 802.3ah призначений для виявлення помилок з'єднання між двома безпосередньо фізично пов'язаними інтерфейсами Ethernet. Він підтримує такі функції, як віддалене виявлення несправностей і віддалений контроль зворотного зв'язку.

Остання функція є найбільш цікавою для фахівців, що займаються експлуатацією мереж Ethernet так як вона дозволяє віддалено (через мережу) видати запит деякому інтерфейсу Ethernet на перехід в режим зворотного зв'язку. У цьому режимі всі кадри, що надсилаються на цей інтерфейс сусідом по лінії зв'язку, повертаються ним назад. Отримані кадри потім можна проаналізувати, щоб встановити якість фізичної лінії.

Необхідно відзначити, що процедура тестування лінії в режимі зворотного зв'язку порушує нормальну роботу з'єднання, тому тестування потрібно проводити в спеціальний час, відведений для обслуговування мережі.

## Інтерфейс локального управління Ethernet

Стандарт E-LMI дозволяє прикордонному пристрою користувача запитувати інформацію про стан і параметри послуги, що надається мережею провайдера з даного інтерфейсу. Наприклад, прикордонний комутатор Ethernet, що розташований в мережі користувача, може вимагати від прикордонного комутатора провайдера інформацію про стан послуги (працездатності

з’єднання), що надається даним інтерфейсом. Крім того, згідно стандарту E-LMI, по запиту можна отримати таку інформацію про послугу, як ідентифікатор VLAN користувача на дане з’єднання, величину пропускної спроможності, що гарантована для даного з’єднання.

## 10.3. Розподіл адресних просторів користувачів і провайдера

### 10.3.1. Мости провайдера

Стандарт IEEE 802.1ad на **мости провайдера** (Provider Bridge, **PB**) був першим стандартом, який вирішував проблему ізоляції адресного простору мережі провайдера від адресного простору його користувачів. Цей стандарт був прийнятий IEEE в 2005 році і сьогодні реалізований в комутаторах Ethernet багатьох виробників. Проблема ізоляції адресних просторів вирішується в цьому стандарті лише частково, так як MAC-адреси користувачів, як і раніше присутні в комутаторах мережі провайдера, поділяються тільки простору ідентифікаторів VLAN.

Стандарт PB вводить дворівневу ієрархію ідентифікаторів VLAN (рис. 10.3). На зовнішньому (верхньому) рівні розташовується ідентифікатор VLAN провайдера – **S-VID** (Service VLAN ID – ідентифікатор сервісу VLAN), а на нижньому (внутрішньому) рівні – ідентифікатор VLAN користувача – **C-VID** (Customer VLAN ID – ідентифікатор VLAN користувача).

Ідентифікатор S-VID поміщається в кадр користувача прикордонним комутатором (Edge Bridges, EB) провайдера – він проштовхує C-VID в стек і додає новий ідентифікатор S-VID, який буде потрібен комутаторам мережі провайдера для поділу трафіку на віртуальні локальні мережі провайдера. Оскільки S-VID являє собою нове поле кадру Ethernet, то йому передує нове поле типу Ether Type, яке на рис. 10.3 позначено як S-VID-Ether Type (на відміну від оригінального поля C-VID-Ether Type). Цей спосіб інкапсуляції часто неформально називають інкапсуляцією **Q-in-Q** за назвою стандарту 802.1Q, що описує техніку VLAN.

Після того як прикордонний комутатор мережі провайдера виконує інкапсуляцію Q-in-Q, кадр обробляється магістральними комутаторами (Core Bridges, CB) провайдера як звичайний кадр, тобто відповідно до зовнішнього ідентифікатора VLAN в полі S-VID.

Коли кадр прибуває на вихідний прикордонний комутатор провайдера, над ним виконується зворотна операція – ідентифікатор S-VID видаляється. Після цього кадр відправляється в мережу користувача в початковому вигляді, маючи

в своєму заголовку тільки ідентифікатор C-VID. Таким чином, провайдеру немає необхідності погоджувати логічну структуру своєї мережі з користувачами.

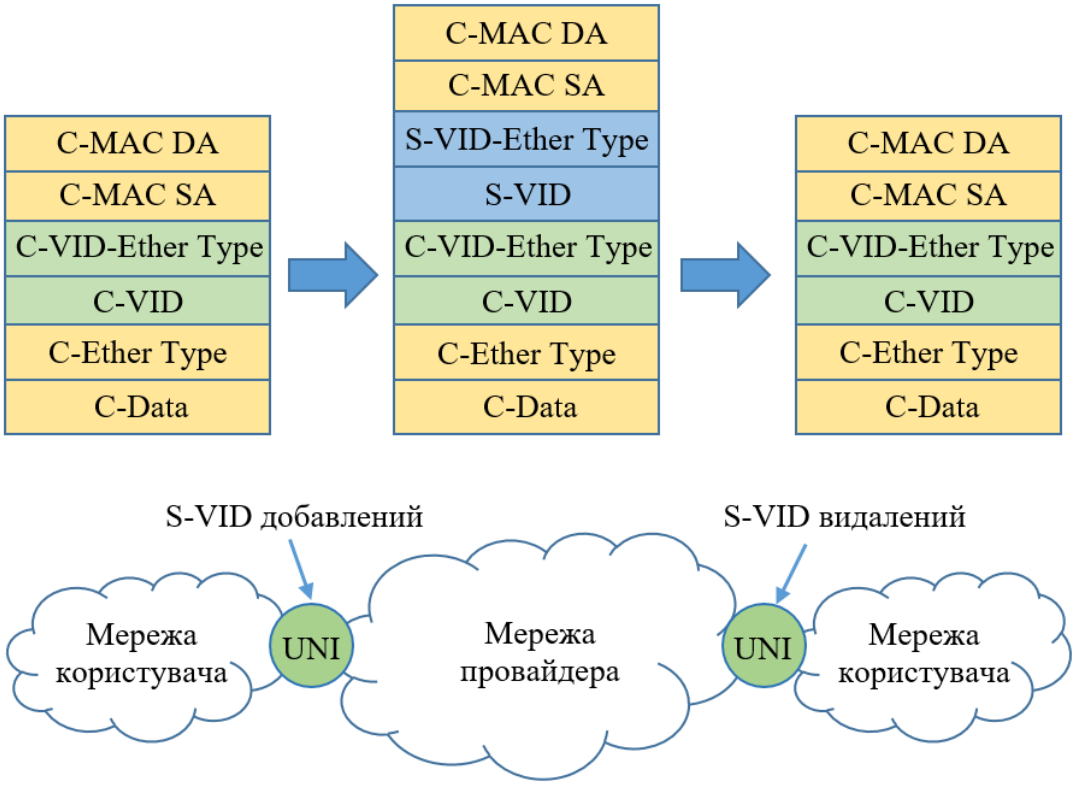



Рис. 10.3. Інкапсуляція ідентифікаторів VLAN

На рис. 10.4 показана мережа провайдера, яка з'єднує VPN мережі двох користувачів. Мережі N1, N3 і N5 є мережами користувача A, вони об'єднуються в мережу з ідентифікатором S-VID, рівним 156, а мережі N2, N4 і N6 є мережами користувача B, вони об'єднуються в мережу з ідентифікатором S-VID = 505.

Конфігурація послуг мереж 156 і 505 виконано без урахування значень користувацьких ідентифікаторів VLAN на підставі під'єднання мережі користувача до певного фізичного інтерфейсу комутатора провайдера. Так, наприклад, весь користувацький трафік, що надходить від мережі N1, класифікується прикордонним комутатором EB1 як трафік, що належить віртуальній приватній мережі з ідентифікатором S-VID = 156.

Стандарт PB дозволяє провайдеру надавати послуги і з урахуванням значень користувацьких ідентифікаторів VLAN. Наприклад, якщо всередині мережі N1 виконана логічна структуризація і існують дві мережі VLAN, трафік яких не можна змішувати, провайдер може організувати для цього дві мережі S-VLAN і відображати на них вхідні кадри в залежності від значень C-VID.

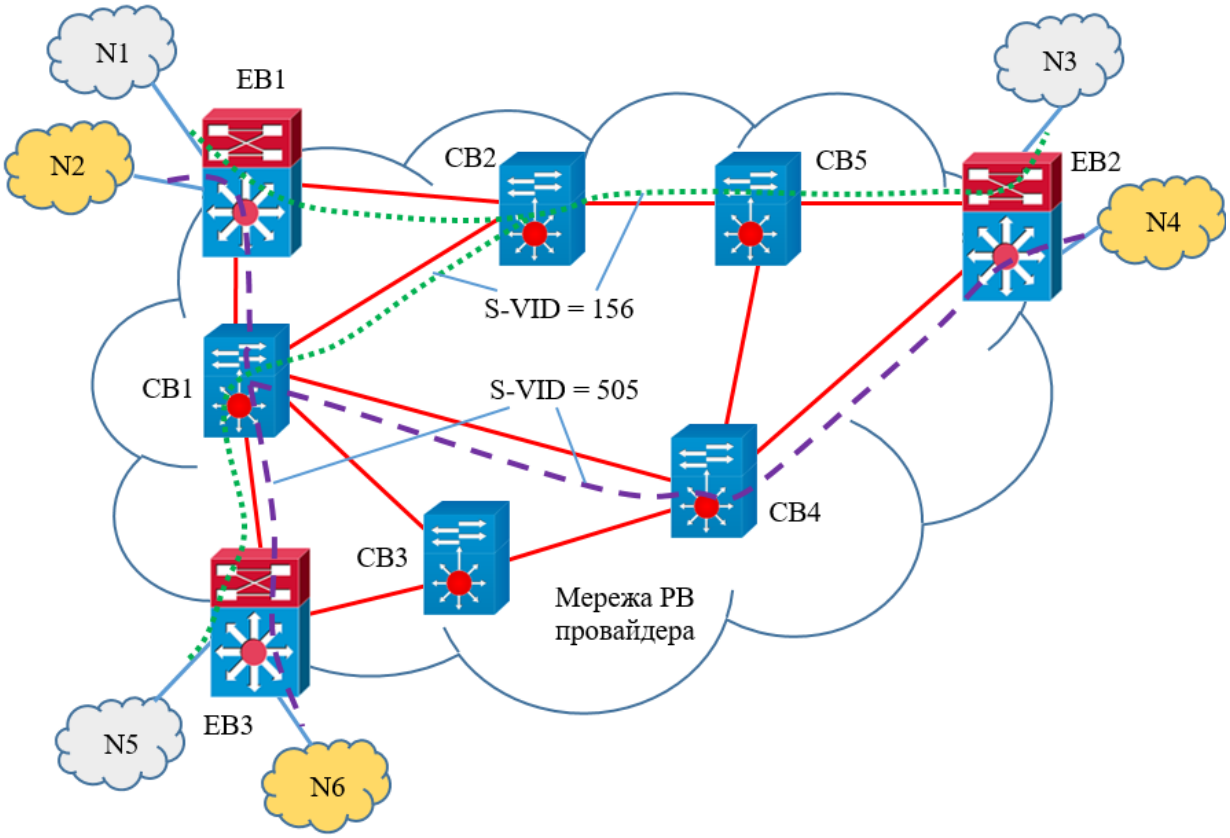



Рис. 10.4. Мережа стандарту PB, що надає послуги створення приватних мереж двох користувачів

Стандарт PB має декілька недоліків.

- Комутатори мережі провайдера, як прикордонні, так і магістральні, повинні вивчати MAC-адреси вузлів мереж користувачів. Це не є масштабованим рішенням.
- Максимальна кількість послуг, що надаються провайдером, обмежена числом 4096 (так як поле S-VID має стандартний розмір 12 біт).
- Інжиніринг трафіку обмежений протоколом STP.
- Для розмежування дерев STP, що створюються в мережах провайдера і користувачів, в стандарті 802.lad довелося ввести нову групову адресу для комутаторів провайдера. Ця обставина не дозволяє задіяти в якості магістральних комутаторів провайдера ті комутатори, які не підтримують стандарт 802.lad.

Деякі з цих недоліків були усунуті в стандарті на магістральні мости провайдера IEEE 802.1ah, який був прийнятий влітку 2008 року.

### 10.3.2. Магістральні мости провайдера

У стандарті IEEE 802.1ah на **магістральні мости провайдера** (Provider Backbone Bridges, **PBB**) адресні простори користувачів і провайдера поділяються за рахунок того, що прикордонні комутатори провайдера повністю інкапсулюють користувацькі Ethernet кадри в нові кадри Ethernet, які потім застосовуються в межах мережі провайдера для доставки користувацьких кадрів до вихідного прикордонного комутатора.

**Формат кадру PBB**

При передачі кадрів Ethernet через мережу PBB в якості адрес відправника та отримувача використовуються MAC-адреси прикордонних комутаторів (Backbone Edge Bridges, BEB) провайдера. По суті, в мережі провайдера працює незалежна ієрархія Ethernet зі своїми MAC-адресами і розподілом мережі на віртуальні локальні мережі (VLAN) так, як це зручно провайдеру Через два рівня MAC-адрес в кадрах провайдера стандарт PBB отримав також назву **MAC-in-MAC**.

Формат кадру при такій інкапсуляції показаний на рис. 10.5. Тут передбачається, що мережа PBB провайдера приймає кадри від мереж PB (можливо, іншого провайдера), які в свою чергу з'єднані з мережами користувача. У цьому випадку в кадрах, що надходять на прикордонні комутатори мережі PBB, є ідентифікатор S-VID, який доданий вхідним прикордонним комутатором мережі PB. Наявність ідентифікатора S-VID у вхідних кадрах не є необхідною умовою роботи мережі PBB, це тільки можливий варіант; якщо мережа PBB безпосередньо з'єднує мережі користувачів, то вхідні кадри поля S-VID не мають. Поле S-VID не використовується при просуванні кадрів в мережі PBB.

Вхідний прикордонний комутатор мережі PBB додає до приймаючого кадру шість нових полів, з яких чотири поля являють собою стандартний заголовок нового кадру, в поле даних якого упакований прийнятий кадр. У цьому заголовку MAC-адресами отримувача та відправника є адреси вихідного і вхідного прикордонних комутаторів мережі, які на рис. 10.5 позначені як B-MAC DA і B-MAC SA відповідно (буква «B» від слова «backbone» – магістральний). Адреси B-MAC ідентифікують комутатор провайдера в цілому як вузол, будучи аналогом IP-адреси зворотного зв'язку маршрутизатора.

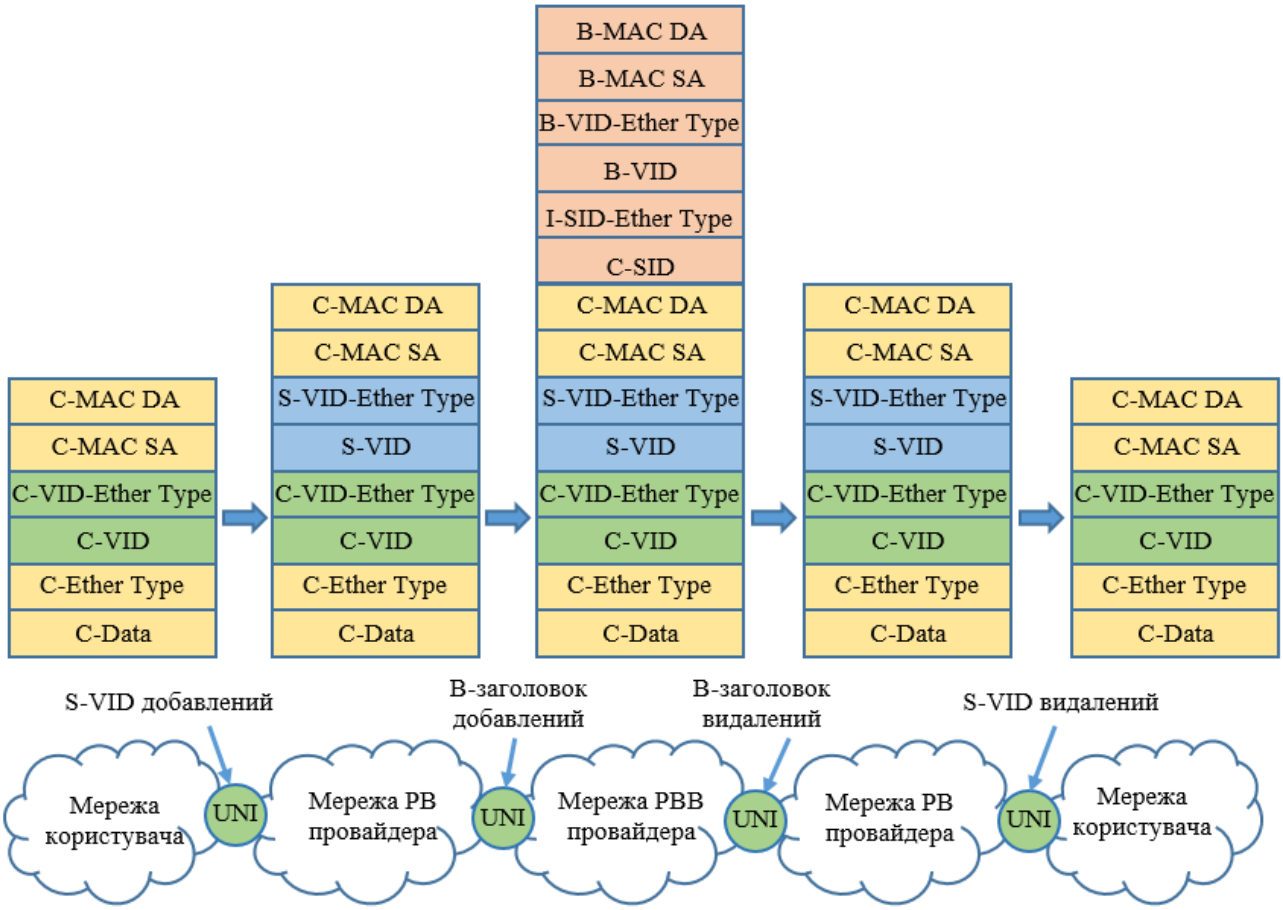



Рис. 10.5. Формат кадрів при інкапсуляції MAC-in-MAC

Адреси B-MAC використовуються в межах мережі PBB разом з ідентифікатором віртуальної локальної мережі B-VID для передачі кадрів відповідно до правил локальної мережі, розділеної на сегменти VLAN, і при цьому абсолютно незалежно від адресної інформації мереж користувача. Користувацькі MAC-адреси, а також ідентифікатори S-VID і C-VID знаходяться в полі даних нового кадру і при передачі між магістральними комутаторами мережі PBB ніяк не використовуються.

**Дворівнева ієрархія з'єднань**

Повна інкапсуляція вхідних кадрів не є єдиним нововведенням стандарту на PBB. Іншим удосконаленням цього стандарту є введення дворівневої ієрархії з'єднань між прикордонними комутаторами. Це забезпечує масштабованість технології при обслуговуванні великої кількості користувацьких з'єднань.

Для цього в кадр PBB введено поле I-SID з попереднім йому полем I-SID Ether Type. Значення ідентифікатора I-SID (Information Service Identification – ідентифікатор інформаційного сервісу) вказує на користувацьке з'єднання

(віртуальну приватну мережу користувача) в мережі PBB. Так як мережа PBB ділиться на сегменти B-VLAN, то з'єднання I-SID є логічними з'єднаннями всередині цих сегментів. Роль сегментів B-VLAN полягає в наданні транспортних послуг з'єднанням I-SID, вони є свого роду тунелями. У кожній мережі B-VLAN може налічуватися до 16 мільйонів з'єднань I-SID (це значення визначається форматом поля I-SID, що складається з 24 розрядів).

Призначення ідентифікатора I-SID в мережі PBB аналогічно призначенню ідентифікатора S-VID в мережі PB – обидва визначають віртуальну мережу користувача в мережі провайдера. Цей факт пояснює також необов'язковість поля S-VID в кадрах користувача, що надходять на вхідні інтерфейси мережі PBB, – це поле є тільки однією з ознак, що враховуються при відображенні кадрів користувача на деяку віртуальну мережу користувача, існуючу в мережі провайдера. Якщо поле S-VID в кадрах користувача відсутнє, то для відображення використовуються інші ознаки: MAC-адреси, значення поля C-VID або номер інтерфейсу, з якого надходять кадри користувача.

На рис. 10.6 показана мережа провайдера, що надає послуги Ethernet своїм клієнтам на основі стандарту на PBB. Вона складається з прикордонних комутаторів (Backbone Edge Bridge, BEB) і магістральних комутаторів (Backbone Core Bridge, BCB).

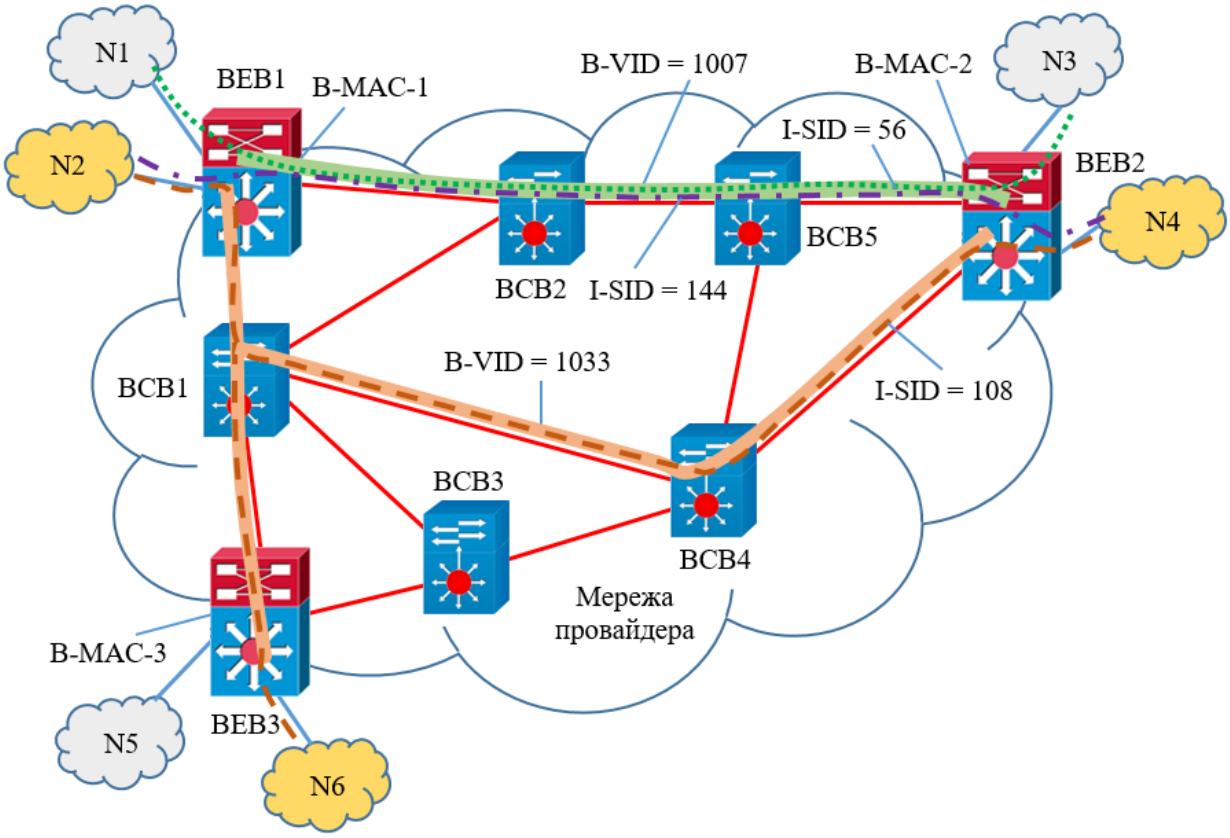



Рис. 10.6. Організація послуг в мережі PBB

Провайдер в цьому прикладі надає послуги трьох віртуальних мереж:

- LAN1 – передає голосовий трафік між мережами N1 і N3 (двоточкова топологія);
- LAN2 – передає голосовий трафік між мережами N2 і N4 (двоточкова топологія);
- LAN3 – передає еластичний трафік даних між мережами N2, N4 і N6 (повнозв'язна топологія).

Користувацькі мережі безпосередньо під'єднанні до мережі PBB, проміжних мереж PB в цьому прикладі немає.

На верхньому рівні структуризації мережі провайдера в ній сконфігуровані дві магістральні віртуальні локальні мережі (B-VLAN) з ідентифікаторами 1007 і 1033. Різні мережі B-VLAN покликані підтримувати трафік різного типу: B-VLAN 1007 підтримує більш вимогливий голосовий трафік, а B-VLAN 1033 – менш вимогливий еластичний трафік даних.

На рівні користувача послуг в мережі організовано три користувацьких з'єднання, позначені як I-SID 56, 144 і 108. Ці з'єднання призначені для реалізації послуг LAN1, LAN2 і LAN3 відповідно.

З'єднання I-SID 56 і 144 відображаються прикордонними комутаторами BEB1 і BEB2 на мережу B-VLAN 1007, так як ці з'єднання переносять користувацький голосовий трафік, а дана мережа B-VLAN створена для цього типу трафіку. У той же час з'єднання I-SID 108 відображається прикордонними комутаторами BEB1, BEB2 і BEB3 на мережу B-VLAN 1033, так як сервіс 108 переносить еластичний користувацький трафік даних. Задає ці відображення адміністратор при конфігуруванні прикордонних комутаторів.

Завершує процес конфігурації послуг LAN1, LAN2 і LAN3 відображення користувацького трафіку на відповідні з'єднання I-SID. Це відображення також задає адміністратор мережі при конфігуруванні прикордонних комутаторів BEB. При відображенні користувацького трафіку адміністратор може враховувати тільки інтерфейс, за яким трафік надходить в мережу провайдера. У прикладі таким способом поставлено відображення для сервісу з I-SID 56, який монопольно використовує інтерфейси комутаторів BEB1 і BEB2, не розділяючи їх з іншими сервісами.

У тому випадку, коли на один і той же інтерфейс надходить трафік більш ніж одного сервісу, при відображенні потрібно також враховувати значення C-VID (в прикладі поле S-VID в користувацьких кадрах відсутнє, так як користувацькі мережі з'єднані з мережею PBB безпосередньо, без проміжної мережі типу PB). Цей випадок має місце для сервісів з I-SID 144 і 108, так як вони поділяють один і той же інтерфейс комутаторів BEB1 і BEB2. Тому такі

відображення потрібно конфігурувати з урахуванням значень C-VID: C-VID 305 відображається на I-SID 144, а C-VID 500 – на I-SID 108.

**Користувацькі MAC-адреси**

Магістральним комутаторам мережі PBB знання користувацьких адрес не потрібне, так як вони передають кадри тільки на підставі комбінації B-MAC/B-VID. Поведінка прикордонних комутаторів щодо користувацьких MAC-адрес залежить від топології сервісу, що надається мережею PBB своїм користувачам.

При відображенні кадрів сервісу з топологією «точка-точка» на певне з'єднання I-SID прикордонні комутатори не застосовують користувацькі MAC-адреси, так як всі кадри, незалежно від їх адрес призначення, передаються одному і тому ж вихідному прикордонному комутатору. Наприклад, для сервісів з I-SID 56 і 144 комутатор BEB1 завжди використовує MAC-адресу комутатора BEB2 в якості B-MAC DA при формуванні кадру, який переносить інкапсульований користувацький кадр через мережу PBB.

Однак, при відображенні кадрів сервісу із зіркоподібною або повнозв'язною топологією у вхідного комутатора завжди існує кілька вихідних прикордонних комутаторів, що підтримують цей сервіс. Наприклад, у вхідного комутатора BEB1 при обслуговуванні кадрів сервісу I-SID 108 є альтернатива – відправити вхідний кадр комутатору BEB2 або BEB3. Для прийняття рішення в таких випадках використовується інформація, що знаходиться в користувацьких MAC-адресах. Прикордонні комутатори BEB, що підтримують сервіси із зіркоподібною та повнозв'язною топологіями, вивчають користувацькі MAC-адреси і передають кадр вихідному комутатору, що зв'язаний з тією мережею користувача, в якій знаходиться MAC-адреса отримувача C-MAC DA. Так, в прикладі на рис. 10.6 комутатор BEB1 вивчає адреси C-MAC DA кадрів, що надходять через сервіс I-SID 108, щоб знати, чи підключені вузли з цими адресами до BEB2 або BEB3. В результаті BEB1 створює таблицю просування (табл. 10.1).

Таблиця 10.1. Таблиця просування для сервісу I-SID 108

| C-MAC | I-SID | B-MAC | B-VID |
|---|---|---|---|
| C-MAC-1 | 108 | B-MAC-2 | 1033 |
| C-MAC-2 | 108 | B-MAC-2 | 1033 |
| C-MAC-3 | 108 | B-MAC-3 | 1033 |
| C-MAC-4 | 108 | B-MAC-3 | 1033 |
| … | 108 | … | 1033 |

На підставі цієї таблиці комутатор BEB1 за адресою призначення C-MAC вибирає відповідну адресу вихідного прикордонного комутатора і поміщає його

в формований кадр: наприклад, для кадру з адресою призначення C-MAC-2 це буде B-MAC-2. У тому випадку, коли користувацька адреса отримувача ще не вивчена, комутатор BEB1 поміщає в поле B-MAC широкотрансляційну адресу.

Маршрутизація і відмовостійкість в мережах PBB.

Для нормального функціонування мережі PBB її активна топологія повинна бути вільна від петель, при цьому мережа повинна забезпечувати відмовостійкість, тобто топологія мережі повинна автоматично змінюватися в разі відмов ліній зв'язку або комутаторів мережі.

У мережах Ethernet для цієї мети застосовується протокол STP, він же може бути застосований і в мережах PBB в його версії MSTP (Multiple STP), яка будує окреме дерево для кожної магістральної мережі VLAN (яка визначається значенням B-VID). Відомо, що у протоколу STP є кілька принципових недоліків, таких як неоптимальність маршрутів і занадто тривалий час встановлення нової активної топології.

Для подолання недоліків протоколу STP робочою групою IEEE 802.laq був створений протокол маршрутизації з **комутацією по найкоротшому шляху** (Shortest Path Bridging, **SPB**). SPB створений на основі **протоколу маршрутизації проміжних систем (IS-IS)**, що стандартизований ISO і використовується в основному у великих мережах провайдерів послуг. IS-IS який являє собою протокол маршрутизації, що враховує стан зв'язків.

Вибір протоколу IS-IS для застосування в мережах Ethernet пояснюється тим, що він створювався як гнучкий протокол маршрутизації, здатний працювати в різних стеках протоколів. Протокол IS-IS може передавати свої повідомлення безпосередньо в кадрах канального рівня, не використовуючи пакети IP і повідомлення TCP або UDP. Крім того, для ідентифікації зв'язків мережі він може використовувати адресну інформацію різного типу. У тому випадку, коли IS-IS працює в мережі IP, він застосовує для ідентифікації зв'язку IP-адреси її кінцевих точок. При роботі в мережі Ethernet IS-IS (точніше SPB, що працює на основі IS-IS) використовує для цієї мети MAC-адреси.

При роботі протоколу SPB кожен прикордонний комутатор BEB будує дерево оптимальних маршрутів до решти прикордонних комутаторів окремо для кожної магістральної мережі VLAN, тобто окремо для кожного значення B-VID. Наприклад, на рис. 10.6 прикордонний комутатор BEB1 будує для сервісу 1033 дерево маршрутів до прикордонних комутаторів BEB2 і BEB3, а для сервісу 1007 – дерево маршрутів тільки до BEB2, оскільки лише цей комутатор входить в магістральну віртуальну локальну мережу 1007 крім BEB1.

Знаходження оптимальних маршрутів виконується стандартним для протоколів маршрутизації, що враховують стан зв'язків, способом: кожен комутатор (як типу BEB, так і типу BCB) розсилає оголошення про стан зв'язків

{B-MAC1, B-MAC2}, де B-MAC-адреси відносяться до комутаторів, що є кінцевими точками даного зв'язку. Прикордонні комутатори BEB поширюють також інформацію про номери магістральних віртуальних мереж B-VID, для яких ці комутатори є кінцевими. Наприклад, комутатор BEB1 поширює інформацію про два зв'язки: {B-MAC1, B-MAC-BCB1} і {B-MAC1, B-MAC-BCB2} (другі адреси в парах належать магістральним комутаторам BCB1 і BCB2). Крім того, він оголошує про те, що є прикордонним комутатором для B-VID 1033 і B-VID 1007.

Після отримання інформації про топологію мережі кожен комутатор мережі будує дерево оптимальних маршрутів від себе до кожного кінцевого комутатора BEB в кожній магістральній віртуальній мережі B-VID. У прикладі BEB1 будує два дерева: для B-VID 1033 до комутаторів BEB2 і BEB3, а також для B-VID 1007 до комутатора BEB2. Далі ці дерева служать для побудови таблиці просування, тобто знаходження наступного хопу передачі кадру. Таблиця будується аналогічно як і таблиця маршрутизації в протоколах OSPF і IS-IS, тобто вибирається наступний комутатор уздовж шляху до комутатора призначення.

## 10.4. Магістральні мости провайдера з підтримкою інжинірингу трафіку

Технологія **PBB TE** (Provider Backbone Bridge Traffic Engineering – магістральні мости провайдера з підтримкою інжинірингу трафіку) базується на технології PBB, але додає до неї можливість інжинірингу трафіку. У PBB-TE застосовується та ж сама схема інкапсуляції кадрів, створення магістральних мереж VLAN (B-VID) і користувацьких з'єднань I-SID. На відміну від PBB, технологія PBB-TE працює лише з топологією з'єднань «точка-точка».

Головними цілями розробників технології PBB TI були:

- підтримка функцій інжинірингу трафіку;
- забезпечення «швидкої» відмовостійкості зі швидкістю, співрозмірною зі швидкістю захисту з'єднань в технології SDH.

Поставлені цілі досягаються в технології PBB TE за рахунок наступних змін технології PBB і класичної технології локального моста:

- Заборона на роботу протоколу STP.
- Відключення механізму автоматичного вивчення магістральних MAC-адрес.
- Використання пари «B-VID/B-MAC-DA» в якості мітки тунелю між двома прикордонними комутаторами. В принципі, будь-який комутатор,

який підтримує VLAN техніку (стандарт IEEE 802.1Q), просуває кадри на вихідний порт, аналізуючи два вказаних в кадрі значення: MAC-адрес призначення і ідентифікатор VLAN. Тому дана властивість просто передбачає, що комутатор поводиться у відповідності з алгоритмом просування, описаним у стандарті 802.1Q, але тільки для магістральних адрес і магістральних віртуальних локальних мереж.

- Попередня прокладка первинного (основного) і резервного тунелів для тих випадків, коли потрібно забезпечити відмовостійкість тунелю.

Перші три перерахованих властивості технології PBB TE дозволяють адміністратору або системі управління мережею формувати шляхи проходження через мережу довільним чином, незалежно від того, чи забезпечують вони найкоротшу відстань до деякого комутатора (кореневого комутатора), чи ні, тобто чи забезпечують підтримку функцій інжинірингу трафіку. Пара «B-VID/B-MAC-DA» є аналогом мітки шляху LSP в технології MPLS, проте на відміну від мітки MPLS значення цієї мішки залишається незмінним в процесі переміщення кадру по мережі провайдера, тобто комутації мітки не відбувається.

Розглянемо як працює технологія PBB TE, на прикладі мережі, що зображена на рис. 10.7. У цій мережі налаштовано два тунелі:

- Основний тунель з B-VID 1007 між BEB1 і BEB2, який проходить через BCB2 BCB5. На відміну від тунелів MPLS, тунелі PBB TE є двонаправленими.
- Резервний тунель з B-VID 1033, що з’єднує ті ж кінцеві точки BEB1 і BEB2, але проходить через інші проміжні комутатори BCB1 і BCB4, що дозволяє забезпечити працездатність резервного тунелю при відмові будь-якого елемента (комутатора або лінії зв’язку) основного тунелю.

Організація обох тунелів досягається шляхом ручного конфігурування таблиць просування на всіх комутаторах мережі, через які проходять тунелі. Наприклад, таблиця просування комутатора BEB1 після такого конфігурування виглядає як табл. 10.2.

Таблиця 10.2. Таблиця просування комутатора BEB1

| MAC-адреса призначення | VLAN ID (B-VID) | Вихідний порт |
|---|---|---|
| B-MAC-2 | 1007 | Порт 1 |
| B-MAC-2 | 1033 | Порт 2 |

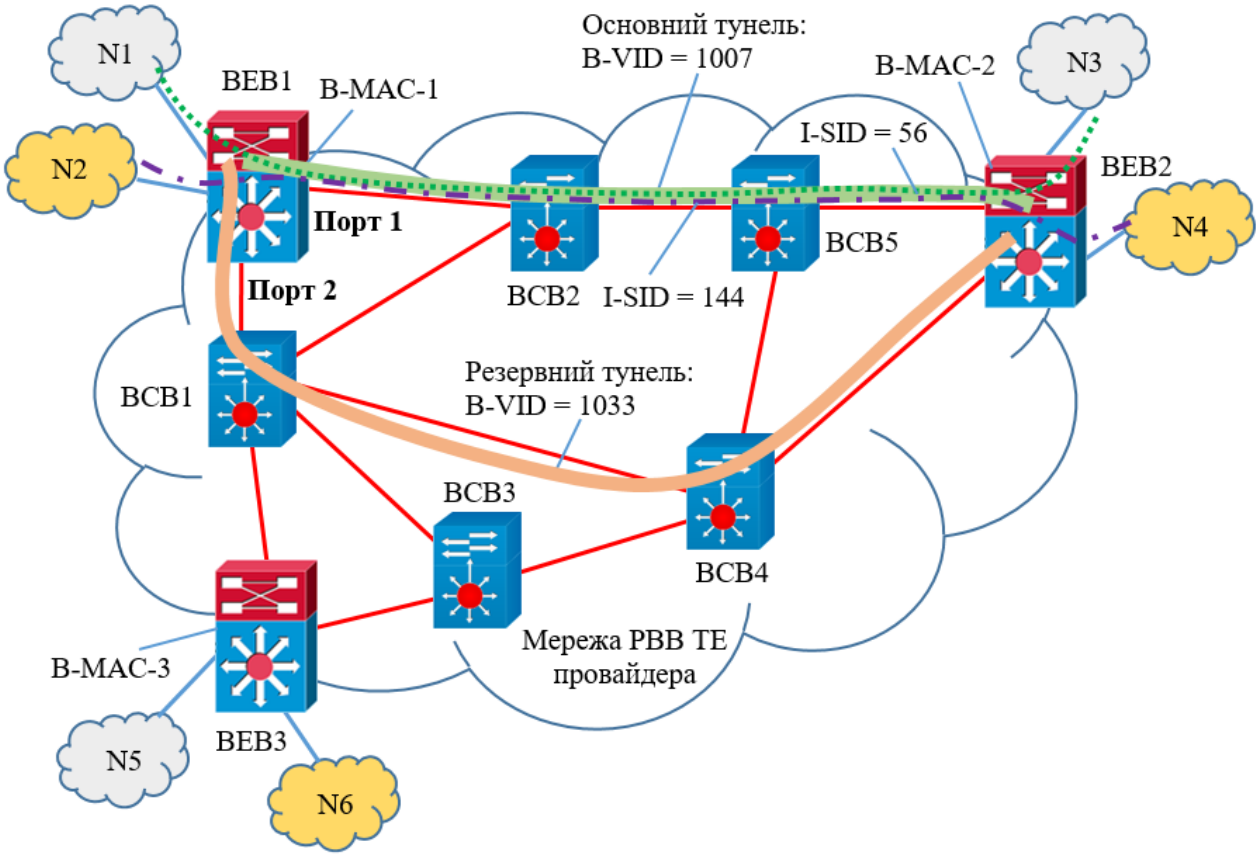



Рис. 10.7. Організація послуг в мережі PBB TE

Для стійкої роботи мережі PBB TE необхідно, щоб комбінація B-VID/B-MAC-DA була унікальною в межах цієї мережі.

Як і в технології PBB, для ідентифікації магістральних комутаторів BEB і BCB в технології PBB TE використовуються MAC-адреси зворотного зв'язку, які відносяться не до окремого фізичному інтерфейсу, а до комутатора в цілому.

Додавання значення B-VID до адреси B-MAC-DA дозволяє організувати до одного і того ж прикордонного комутатора до 1024 тунелів з різними шляхами проходження через мережу. Це дає адміністратору або системі управління широкі можливості щодо інжинірингу трафіку в мережах PBB TE.

Таблиці просування в мережі PBB TE мають стандартний вигляд для комутаторів, що підтримують техніку VLAN. Змінюється лише спосіб побудови цих таблиць – замість автоматичної побудови на основі вивчення адрес переданих кадрів має місце їх зовнішнє формування. Відображення користувацького трафіку на з'єднання I-SID і зв'язування цих з'єднань з тунелями B-VID відбувається в технології PBB TE аналогічно, як і в технології PBB.

Оскільки мережі PBB TE підтримують тільки двоточкові з'єднання, прикордонним комутаторам не потрібно вивчати користувацькі MAC-адреси.

Відмовостійкість тунелів PBB TE забезпечується механізмом, аналогічним механізму захисту шляху в технології MPLS. Якщо адміністратор мережі хоче захистити деякий тунель, він повинен сконфігурувати для нього резервний тунель і постаратися прокласти його через елементи мережі, що не лежать на шляху основного тунелю. У разі відмови основного тунелю його трафік автоматично направляється прикордонним комутатором в резервний тунель. У прикладі, наведеному на рис. 10.6, для основного тунелю з ідентифікатором B-VID = 1007, налаштований резервний тунель з ідентифікатором B-VID = 1033. При відмову тунелю 1007 трафік з'єднань з ідентифікаторами I-SID, рівними 56 і 144, буде спрямований комутатором BEB1 в тунель 1033.

Для моніторингу стану основного та резервного тунелів в технології PBB TE застосовується протокол CFM. Моніторинг виконується шляхом періодичної відправки повідомлень CCM кожним прикордонним комутатором тунелю. Час реакції механізму захисту тунелів PBB TE визначається періодом проходження повідомлень CCM. При апаратній реалізації цього протоколу портами комутатора час реакції може знаходитися в межах десятка мілісекунд, тобто співрозмірно з реакцією мереж SDH.

# 11. Мережеві інформаційні сервіси телекомунікаційних систем

## 11.1. Загальні принципи організації мережевих сервісів

### 11.1.1. Загальні поняття та визначення

Англомовний термін «**Service**» у технічній літературі часто трактують синонімічно до понять «послуга», «служба», «обслуговування» та «сервіс». Однак, рекомендовано все ж таки розрізняти ці поняття.

**Послуга** – це сукупний результат дій мережі, спрямований на задоволення запиту користувача щодо його телекомунікаційної та/або інформаційної потреби.

Послуга є продуктом мережі, який має вартість, що залежить від її типу й якості, і який споживає користувач мережі.

**Телекомунікаційні послуги** призначені для якісного транспортування інформації, яку створюють користувачі мережі у вигляді інформаційних повідомлень. Мережа приймає інформацію, перетворену у сигнал, в пункті, де знаходиться мережевий інтерфейс, передає її через транзитні пункти, та видає в пункт призначення також через інтерфейс. Надаючи телекомунікаційні послуги, мережа не вносить жодних змін у зміст інформації, яку передає, видаючи її одержувачу в тому вигляді, в якому вона надійшла в мережу від відправника. У зв'язку з цим телекомунікаційні послуги ще називають **послугами транспорту.**

Надання транспортних ресурсів здійснюють мережеві оператори (оператори зв'язку).

**Інформаційні послуги** забезпечують користувачів можливістю отримати необхідну інформацію, створену в мережі без посередництва користувача. Користувач отримує інформацію з мережі у вигляді **контенту** (content) – деякого обсягу інформації, що забезпечує сприйняття його смислового змісту. У цьому контексті інформаційні послуги ще називають **контент-послугами.**

Виробництво й надання інформаційної послуги завжди пов'язано з операціями обробляння інформації (перетворенням та впорядкованим її зберіганням у файлах, базах даних, веб-сторінках), а також пошуку її в мережі. Для цього застосовують різні інформаційні технології: програмування, створення файлів і баз даних, копіювання, архівування файлів та ін.

Створюють, накопичують і обробляють інформацію спеціальні інформаційні служби мережі. Підготовлену інформацію розміщують у Web-порталах на Web-серверах постачальників послуг.

**Службою мережі** називають комплекс апаратних, програмних ресурсів мережі, а також організаційних засобів, задіяних для виробництва і надання конкретної послуги або виду послуг. Таким чином, на відміну від послуги, служба є мережевою компонентою, а не продуктом мережі.

Існує специфікація мережевих служб, яка не залежить від загальної концепції побудови мережі зв'язку й функцій кінцевих пристроїв, але яка конкретизує режим обслуговування користувачів. У зв'язку з цим виокремлюють три категорії служб: діалогові, інтерактивні та дистрибутивні служби.

**Діалогові служби** (On-Line Service) забезпечують двобічний обмін інформацією в реальному масштабі часу (без проміжного накопичення) між користувачами або між користувачем і комп'ютером. Діалогові служби можна застосовувати для передавання голосових повідомлень, відео-повідомлень, даних.

**Інтерактивні служби** (Off-Line Service) містять служби з накопиченням та служби за запитом.

**Служби з накопиченням** призначені для непрямого зв'язку між користувачами за допомогою проміжного зберігання інформаційних повідомлень. Проміжне зберігання здійснюється в центральних пристроях мережі, так званих електронних поштових скриньках, з яких повідомлення можуть бути забрані адресатами самотужки або автоматично переправлятися мережею відповідно до заздалегідь визначених умов абонентів, наприклад, під час дії пільгових тарифів. Служби з накопиченням можна використовувати для передавання голосових, аудіо-, відео-повідомлень, тексту, даних. У зв'язку з цим виникли поняття «голосова пошта», «відеопошта» та ін.

**Служби за запитом** (Service On Demand) дають можливість користувачу отримувати інформацію (контент) з різних центрів накопичення інформації в мережі. Прикладом отримання контенту є «скачування» аудіо-, відео- та мультимедійних файлів з подальшим їх відтворенням на термінальному пристрої користувача, який ініціалізує запит. У даному випадку за запитом користувача фактично реалізується режим мовлення на одну адресу за схемою «точка – точка». Такий режим мовлення має назву «**режим негрупового розсилання**» (Unicast).

**Дистрибутивні служби** (Distribution Service) забезпечують розподілення повідомлень від одного джерела інформації до будь-якої кількості абонентів, які мають право на прийом. У цьому випадку реалізується режим мовлення. За допомогою дистрибутивних служб, наприклад, реалізують роботу засоби масової інформації (ЗМІ). Користувач може приймати потік повідомлень у будь-який момент часу, але він не може впливати ні на час його проходження, ні на

його зміст. Такий режим мовлення називають **режимом групового розсилання** (Multicast), він реалізований за схемою «точка – багатоточка». Класичними прикладами надання таких послуг є звукове та телевізійне мовлення в мережі. Однак можливим є застосування цього режиму також для інших видів повідомлень, наприклад розсилання рекламних роликів, факсимільних повідомлень, даних.

Інтерактивні й дистрибутивні служби оператори мережі.

Під термінами «**сервіс**» і «**обслуговування**» розуміють специфікацію (Specification) послуг, які надає мережа, а саме:

- спектр додаткових видів обслуговування;
- функціональну повноту (специфічних особливостей послуги);
- клас обслуговування (рівень комфортності послуг);
- якість обслуговування QoS (Quality of Service).

**Прикладний додаток** або просто **додаток** (Application) – це програма користувача прикладного рівня, яку підтримує мережа.

Додаток може бути автономним (наприклад, навчальний курс, скачаний з Інтернету). Такий додаток користувач отримує аналогічно як і послугу, але у вигляді кінцевого програмного продукту, який можна потім багаторазово використовувати.

Окрім того, в мережі можуть виконуватися й розподілені додатки. Розподілений додаток містить декілька частин, кожна з яких виконує певну закінчену роботу для розв’язання прикладної задачі (наприклад, система дистанційного навчання, система електронної комерції та ін.). Розподілені додатки в повному обсязі використовують можливості мережі для організації взаємодії своїх компонентів, а тому їх називають **мережевими додатками.**

Індустрія телекомунікацій історично розвивалася у напрямку розширення спектру послуг зв’язку, водночас індустрія інформаційних технологій з самого початку була спрямована надавати послуги у формі додатків.

**Користувачів** (Users) мережі поділяють на клієнтів та абонентів, що визначається порядком їх взаємодії з мережею.

**Клієнт** звертається до мережі за одноразовим споживанням послуги та сплачує лише за спожиту послугу. **Абонент** взаємодіє з мережею на контрактній основі з передоплатою споживаних послуг.

Залежно від виду та набору споживаних послуг усіх користувачів (клієнтів та абонентів) умовно поділяють на три категорії:

- користувачі в діловому секторі;
- користувачі в домашньому секторі;
- користувачі в дорозі.

У діловому секторі (в установах, офісах) з усіх видів послуг найбільш

споживаними є послуги телефонії, доповнені секретарськими послугами (наприклад, накопичення інформації про дзвінки, повідомлення про номер абонента та ін.), послуги аудіо- та відео- конференційного зв'язку, голосової пошти, а також послуги, пов'язані з передаванням даних.

Вимоги до послуг зв'язку в домашньому секторі висувають не в такому обсязі, як у діловому, однак і вони є досить чіткими і зумовлені різними факторами. Збільшується кількість приватних ділових заходів (взаємодія з банком, страховою компанією, придбання товарів), зростає вільний час, зростає потреба в безпеці. Найбільш споживаними в побуті є такі послуги, як: відео за запитом, послуги індустрії розваг (ігри, музичні шоу), освіти, телефонії, електронної пошти, дистанційне керування та контроль комунальних систем і домашньої апаратури, оповіщення про небезпеку, аварійні виклики. Останнім часом виник також інтерес до послуг мультимедіа (одночасного передавання зображення, звуку та даних).

Рухливі користувачі споживають в основному послуги телефонії, однак, важливе значення має й одержання контент-послуг (наприклад, про стан дорожнього руху, карти і плану міста для орієнтації під час руху, можливих місць паркування транспорту та ін.).

### 11.1.2. Хронологія розвитку мережевого сервісу

На ранньому періоді розвитку зв'язку, у рамках концепції **єдиної автоматизованої мережі зв'язку** (ЄАМЗ), для надання конкретного виду послуг на базі первинної мережі будували окремі, спеціально для цього призначені вторинні мережі. Прикладами таких мереж є комутована телефонна мережа загального користування (ТфЗК), телеграфна мережа загального користування (ТлгЗК), загальнодержавна мережа передавання даних, мережа факсимільного зв'язку, мережа передавання програм телевізійного мовлення та ін. На цьому етапі поняття служби ідентифікували з призначенням і типом мережі.

З появою телематичних служб поняття служби набуло більш конкретного й самостійного значення. Телематичні служби є прикладом розширення спектру послуг на основі наявних мереж. Такими службами були телефакс (використання каналів телефонної мережі для факсимільного способу передавання повідомлення), датафакс (використання каналів мережі передавання даних факсимільним способом), телекс (поєднання можливостей друкарської машинки з передаванням текстових повідомлень каналами мереж електрозв'язку), відеотекст (інформаційно-довідкова служба, що обслуговує запити користувачів), телетекст (доповнення TV-програм додатковою інформацією). Організація телематичних служб передбачала створення деяких конкретних

технічних платформ надання послуг, які б забезпечували передавання «чужого» (відносно до використовуваної мережі) трафіку.

На етапі оцифровування мереж електрозв'язку виникла можливість надання різних послуг на основі єдиної інтегрованої мережі – загального телекомунікаційного середовища для передавання будь-яких інформаційних повідомлень, поданих у цифровому коді. Це зумовило інтеграцію й самих служб, що визначено в концепції цифрових мереж інтегрального обслуговування ISDN.

Поява інтегральної мережі ISDN спонукала до проведення значних робіт зі стандартизації та міжнародних угод. Міжнародні рекомендації в цій сфері розробляв Сектор зі стандартизації телекомунікацій ITU-T. Зокрема, відповідно до положень Рекомендації I.112, служби в інтегрованій мережі розділено на дві групи, які не залежать від форм зв'язку. Це служби передавання й телеслужби.

**Служби передавання** (Bearer Service) забезпечують прозоре транспортування інформації між інтерфейсами точок мережі, в яких забезпечується під'єднання абонентів, і не несуть відповідальність за сумісність функцій зв'язку кінцевих пристроїв користувачів. Цю відповідальність у даному випадку цілком покладають на користувачів.

**Телеслужби** (Teleservice) призначені для надання зв'язку «користувач-користувач» з підтримкою функцій зв'язку користувацьких терміналів, забезпечуючи їх сумісність.

Служби передавання, таким чином, реалізують функції трьох нижніх рівнів OSI моделі, а телеслужби, в загальному випадку, – всіх семи рівнів цієї моделі.

ITU-T ввів термін «**телекомунікаційний сервіс**». Під цим терміном розуміють задоволення мережею специфічних вимог користувачів до зв'язку, поєднуючи як різні послуги, так і забезпечення різних видів зв'язку з наданням каналів, різних за швидкостями, за середовищем передавання і принципом надання послуг користувачеві (на час передавання або оренди на тривалий час) та ін.

Інтеграція обчислювальної техніки в мережеве середовище, впровадження електронних комутаційних систем дало змогу розширити функціональність послуг, а саме: надавати користувачам послуги не лише із стандартним набором функцій, але й з розширеним набором функцій, що забезпечує підвищення їх якості та зручність зв'язку. Наприклад, скорочений набір номера для викликаючого абонента, повідомлення про надходження виклику з індикацією, переадресація виклику, оплачування послуги абонента, зазначення дати й часу налаштування з'єднання, виявлення абонентів, які здійснюють зловмисні виклики та ін. Розширений набір функції наданих послуг використовують тільки за відповідною заявою користувача й для різних груп абонентів вони можуть бути різними.

Розподіливши види обслуговування на основні та додаткові, було організовано новий принцип надання послуг користувачам, при якому послуга основного виду могла бути доповнена однією або кількома додатковими видами обслуговування, в залежності від запиту користувача.

Виокремлення механізму формування послуг у нову функціональну підсистему стало початком інтелектуалізації мереж. Реалізація концепції **інтелектуальної мережі** (Intelligent Network, **IN**) передбачала широке використання елементів штучного інтелекту, синтезаторів і розпізнавачів мови та ін. Слід зазначити, що технологію IN можна реалізувати на основі будь-якої мережі, але найбільш ефективною вона є при використанні технологічної інфраструктури цифрових мереж (зокрема, ISDN).

Концепція інтелектуальної мережі передбачає динамізм спектру послуг, коли доцільно вже класифікувати окремі складові послуг та додатків, які дають змогу компонувати будь-який вид послуги на запит користувача із зазначених складових як незалежних від виду обслуговування й один від одного функціональних блоків **SIB** (Service Independent Block).

Широкосмугова інтегрована мережа, яка підтримує всі класи сервісу отримала назву «**мультисервісна мережа**». Вона розробляється в рамках концепції **мереж наступного покоління** (Next Generation Network, **NGN**).

Мультисервісна мережа (Multiservice Network) – це мережа з гнучкими можливостями для організації різних служб, які забезпечують надання необмеженого набору послуг. Мережеві служби в мультисервісній мережі є системними розподіленими програмами і невід'ємними компонентами мережевої операційної системи. Забезпечення користувачів спільним доступом до певного мережного ресурсу називають **наданням сервісу**. Мережеві сервіси, які реалізовані програмно, є об'єктами прикладного рівня моделі OSI/ISO. Мережева операційна система, зазвичай, підтримує декілька видів мережевих сервісів для користувачів, такі, наприклад, як: файловий сервіс, сервіс електронної пошти, сервіс віддаленого доступу та ін.

### 11.1.3. Класифікація мережевих служб

Служби прийнято ділити на декілька груп за типами адресатів надаваних ними послуг:

- Служби, що орієнтовані на кінцевих користувачів і їх додатки. Це такі служби як файловий сервіс, пошта, веб-сервіс, довідкова служба, IP-телефонія, служба хмарних обчислень.
- Служби, що забезпечують безпеку мережі. До них відносяться мережева автентифікація, авторизація та контроль доступу. Послуги цих служб

потрібні як кінцевим користувачам, наприклад при інтерактивному вході в мережу, так і іншим службам, яким необхідно захистити свою інформацію і автентифікувати своїх користувачів – прикладом може бути служба баз даних, яка автентифікує своїх користувачів за допомогою служби мережевої автентифікації.

- Служби, орієнтовані на мережевих адміністраторів, які вирішують завдання конфігурації і управління мережевими пристроями. В цю категорію входять служби управління мережею на основі протоколів Telnet і SNMP, служба моніторингу та аудиту.
- Служби, які допомагають комп'ютерам і мережевим пристроям надавати свої транспортні послуги. Це такі служби як служба відображення символьних імен вузлів на IP-адреси (DNS) і служба динамічного призначення IP-адрес (DHCP).
- Служби підтримки розподілених обчислень. Наприклад, служба реплікації, служба виклику віддалених процедур (Remote Procedure Call, RPC), що є допоміжними по відношенню до інших служб.

Клієнтами мережевих служб можуть бути інші мережеві служби: наприклад, в число клієнтів довідкової служби входять служба автентифікації і поштова служба. У той же час служба крім основних послуг, що дають ім'я цьому типу служби, може надавати і допоміжні послуги. Наприклад, веб-служба може виконувати автентифікацію самостійно, не звертаючись до централізованої службі мережевий автентифікації.

Велика частина прикладних мережевих служб оформляються як додатки, тобто у вигляді виконавчих модулів стандартного для ОС формату. Оскільки такий же формат мають і багато модулі ОС, то часто буває складно провести чітку межу між операційною системою і мережевими службами. Рішення про те, повинна чи ні певна служба стати частиною ОС приймає виробник даної ОС.

У деяких випадках для підвищення продуктивності сервісу служба або її певні компоненти включаються в ядро. Прикладом є клієнтська і серверна частини файлової служби, які часто вбудовують в ядро з тим, щоб вони могли отримувати швидкий прямий доступ до всіх модулів ОС без витрат часу на перемикання з режиму користувача в привілейований режим.

Мережеві служби найчастіше являють собою «клієнт-серверні» розподілені додатки. Принциповою різницею між клієнтом і сервером є те, що ініціатором виконання мережевої службою певної роботи завжди виступає клієнт, а сервер завжди знаходиться в режимі пасивного очікування запитів. Наприклад, поштовий сервер здійснює доставку пошти на комп'ютер користувача тільки при надходженні запиту від поштового клієнта.

Основними питаннями розробки розподілених додатків є розподіл функцій

між клієнтом і сервером та визначення протоколу взаємодії між ними.

**Розподіл функцій** між клієнтом і сервером мережевої служби може виконуватися різними способами. Наприклад, клієнт може бути наділений тільки функціями підтримки інтерфейсу з користувачем сервісу і підтриманням протоколу взаємодії, а вся логіка роботи служби покладена на серверну частину. Можлива й інша ситуація, коли клієнт несе значне навантаження на підтримку роботи мережевої служби. Наприклад, при реалізації поштової служби на диску клієнта може зберігатися локальна копія бази даних, що містить його велике листування. У цьому випадку клієнт робить основну роботу при формуванні повідомлень в різних форматах, в тому числі і складному мультимедійному, підтримує ведення адресної книги і виконує ще багато різних допоміжних функцій.

**Протоколи обміну повідомленнями**, що лежать в основі мережевих служб, відносяться до прикладного рівня. Служби, які мають одне і те ж призначення, можуть використовувати різні протоколи. Наприклад, існує два типи поштової служби, в одній з них клієнт і сервер взаємодіють по протоколу SMTP, а в іншій – X.400. Вірно і зворотне твердження: служби, розроблені для надання різних сервісів, можуть використовувати один і той же протокол взаємодії клієнтської і серверної частин. Наприклад, протокол HTTP, розроблений для веб-служби, використовується в інших службах і мережевих програмах, таких як служба управління мережею, поштова служба й багатьох інших.

## 11.2. Веб-служба

Винахід в 1989 році Тімом Бернерс-Лі і Робертом Кайо **Всесвітньої павутини** (World Wide Web, **WWW**) стоїть в одному ряду з винаходами телефону, радіо і телебачення. Завдяки цьому винаходу Інтернет став таким, яким він є сьогодні. Використовуючи **службу WWW** (або **Веб-службу**), люди отримали можливість доступу до потрібної їм інформації в будь-який зручний для них час.

Веб-служба являє собою розподілену програму, побудовану за архітектурою «клієнт-сервер». Клієнт і сервер веб-служби взаємодіють один з одним по протоколу **HTTP** (HyperText Transfer Protocol – протокол передачі гіпертексту).

**Веб-клієнт**, або **браузер**, являє собою додаток, який встановлюється на комп'ютері кінцевого користувача і призначений для перегляду веб-сторінок.

**Веб-сторінка**, або **веб-документ**, як правило, складається з основного HTML-файлу і деякої кількості посилань на інші об'єкти різного типу: GIF і JPEG-зображення, інші HTML-файли, аудіо- та відеофайли.

**HTML-файлом**, **HTML-сторінкою** або **гіпертекстової сторінкою** називають файл, який містить текст, написаний на мові **HTML** (HyperText Markup Language – мова розмітки гіпертексту).

Однією з важливих функцій браузера є підтримка графічного інтерфейсу користувача. Через цей інтерфейс користувач отримує доступ до широкого набору послуг, головними з яких є пошук і перегляд сторінок, навігація між переглянутими сторінками, перехід по закладках і зберігання історії відвідувань. Крім засобів перегляду і навігації, веб-браузер надає користувачеві можливість маніпулювання сторінками: зберігання їх на диску комп'ютера, друк, передача по електронній пошті, контекстний пошук, зміна кодування і формату тексту, а також безліч інших функцій, пов'язаних з поданням інформації на екрані і конфігуруванням браузера.

До числа найбільш популярних зараз браузерів можна віднести Microsoft Internet Explorer, Mozilla Firefox, Google Chrome і Apple Safari. Веб-браузер не єдиний вид клієнта, який може звертатися до веб-сервера. Цю роль можуть виконувати будь-які програми та пристрої, що підтримують протокол HTTP.

Значну частину своїх функцій браузер виконує в поєднанні з веб-сервером. Клієнт і сервер веб-служби зв'язуються через мережу по протоколу HTTP. Це означає, що в клієнтській частині веб-служби присутня клієнтська частина HTTP, а в серверній – серверна частина HTTP.

**Веб-сервер** – це програма, що зберігає об'єкти локально в каталогах комп'ютера, на якому вона запущена, і забезпечує доступ до цих об'єктів з URL-адресами. Найбільш популярними веб-серверами зараз є Apache і Microsoft Internet Information Server.

Браузер знаходить веб-сторінки і окремі об'єкти за адресами спеціального формату, званими **URL** (Uniform Resource Locator – уніфікований покажчик ресурсу). URL-адреса може виглядати, наприклад, так: http://kaf-kt.tntu.edu.ua/books/books.htm.

В URL-адресу можна виділити три частини:

- *Тип протоколу доступу*. Початкова частина URL-адреси (http://) вказує на те, який протокол використовується для доступу до даних. Крім HTTP, тут можуть бути зазначені й інші протоколи, такі як FTP, Telnet, HTTPS, які також дозволяють здійснювати віддалений доступ до файлів або комп'ютерів.
- *DNS-ім'я сервера*. Ім'я сервера, на якому зберігається потрібна сторінка. У нашому випадку – це ім'я сайту http://kaf-kt.tntu.edu.ua.
- *Шлях до об'єкту*. Зазвичай це повне ім'я файлу (об'єкта) відносно головного каталогу веб-сервера. У нашому випадку шляхом до об'єкта є /books/books.htm.

Як і будь-який інший сервер, веб-сервер повинен бути постійно в активному стані, прослуховуючи TCP-порт 80, який є призначеним портом протоколу HTTP. Як тільки сервер отримує запит від клієнта, він встановлює TCP-з'єднання і отримує від клієнта ім'я об'єкта, наприклад, у вигляді /books/books.htm, після чого знаходить в своєму каталозі цей файл, а також інші пов'язані з ним об'єкти (текст, зображення, мультимедіа) і передає по TCP-з'єднанню клієнту. Отримавши об'єкти від сервера, веб-браузер відображає їх на екрані (рис. 11.1). Після відправки всіх об'єктів сторінки клієнту сервер розриває з ним TCP-з'єднання. У додаткові функції сервера входять також автентифікація клієнта і перевірка прав доступу даного клієнта до даної сторінки.

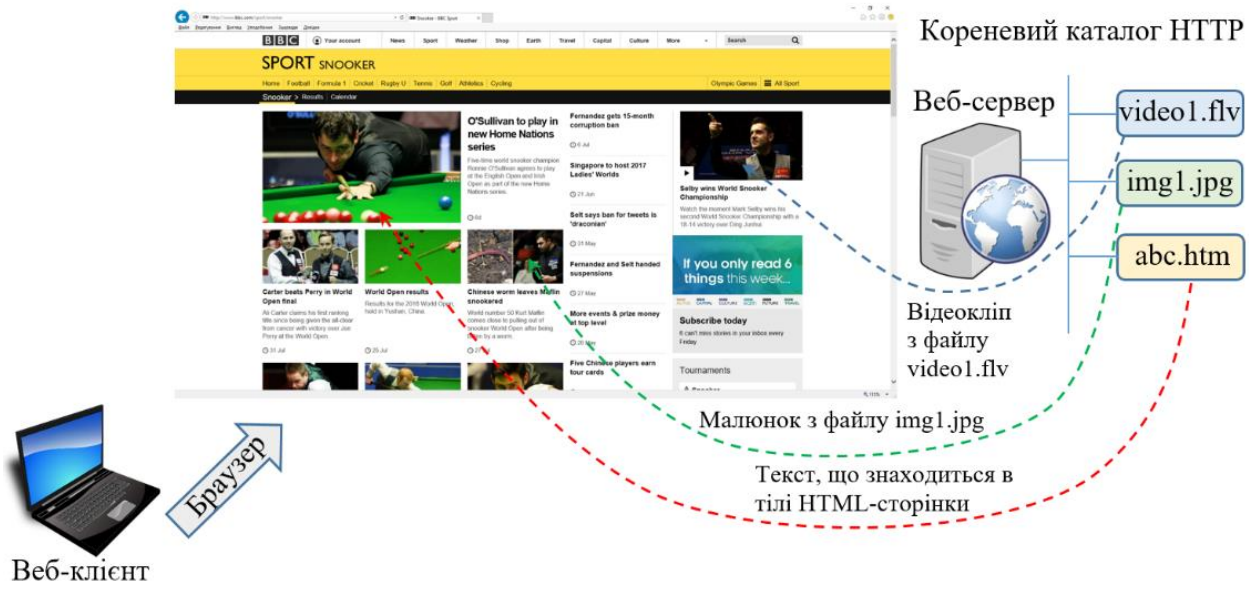



Рис. 11.1. Вивід веб-сторінки на екран

Веб-сервер по відношенню до сеансу з веб-браузером є **сервером без збереження стану** (stateless). Це означає, що на сервері не зберігається інформація, що стосується стану сеансу: які сторінки користувач вже відвідав і які дані йому були передані. Такий режим спілкування з клієнтом спрощує організацію сервера, якому необхідно відповідати на великий потік запитів різних користувачів, так що запам'ятовування стану сеансів сильно збільшило б навантаження на веб-сервер. Замість цього веб-сервер розглядає кожен запит ізольовано, відповідаючи на нього і забуваючи про даного користувача відразу після відповіді. Недоліком даного режиму є уповільнення роботи клієнта і збільшення трафіку в мережі через часте виконання процедури встановлення TCP-з'єднань.

Для підвищення продуктивності деякі веб-сервери вдаються до кешування найбільш часто використовуваних останнім часом сторінок в своїй пам'яті. Коли

приходить запит на будь-яку сторінку, сервер, перш ніж зчитувати її з диска, перевіряє, чи не перебуває вона в буферах більш «швидкої» оперативної пам'яті. Кешування сторінок здійснюється і на стороні клієнта, а також на проміжних серверах (проксі-серверах). Крім того, ефективність обміну даними з клієнтом іноді підвищують шляхом компресії (стиснення) переданих сторінок. Обсяг інформації, що передається зменшують також за рахунок того, що клієнту передається не весь документ, а лише та частина, яка була змінена. Всі ці прийоми підвищення продуктивності веб-служби реалізуються засобами протоколу HTTP.

Веб-сторінки, в яких зміст не змінюється в залежності від дій користувача називаються **статичними**. Тобто, коли користувач клацає на гіперпосиланнях, то він переходить на нову сторінку, а якщо виконує команду повернення назад, то на екрані знову з'являється попередня сторінка в незмінному вигляді.

Однак в деяких випадках було б бажано, щоб зміст сторінки змінювалося в залежності від дій користувача, наприклад при наведенні вказівника миші на певну область сторінки там з'являвся б малюнок замість тексту або значка. Динамічне відтворення стану бази даних також є типовим прикладом ситуації, коли статична сторінка не може вирішити задачу. Наприклад, багато інтернет-магазинів підтримують базу даних товарів, що продаються, і вивід кількості товарів, що є в наявності вимагає динамічного оновлення відповідного поля веб-сторінки.

Веб-сторінки, які можуть генерувати виведений на екран вміст, який змінюється в залежності від деяких зовнішніх умов, називаються **динамічними.** Динаміка сторінки досягається шляхом її програмування, зазвичай для цього використовуються програмні мови сценаріїв, такі як Perl, PHP або JavaScript.

## 11.3. Поштова служба

### 11.3.1. Електронні повідомлення

**Мережева поштова служба**, або **електронна пошта**, – це розподілений додаток, головною функцією якого є надання користувачам мережі можливості обмінюватися електронними повідомленнями.

Як і всі мережеві служби, електронна пошта побудована за архітектурою «клієнт-сервер». Поштовий клієнт завжди розташовується на комп'ютері користувача, а поштовий сервер, як правило, працює на виділеному комп'ютері.

**Поштовий клієнт** (званий також **агентом користувача**) – це програма, яка призначена для підтримки інтерфейсу користувача (зазвичай графічного), а також для надання користувачу широкого набору послуг з підготовки

електронних повідомлень. У число таких послуг входить створення тексту в різних форматах і кодуваннях, збереження, знищення, переадресація, сортування листів за різними критеріями, перегляд переліку вхідних і відправлених листів, граматична і синтаксична перевірка тексту повідомлень, ведення адресних баз даних, автовідповіді, утворення груп розсилки та інше. Крім того, поштовий клієнт підтримує взаємодію з серверної частиною поштової служби.

**Поштовий сервер** виконує прийом повідомлень від клієнтів, для чого він постійно знаходиться в активному стані. Крім того, сервер виконує буферизацію повідомлень, розподіл вхідних повідомлень по індивідуальним буферам (поштових скриньках) клієнтів, виконує реєстрацію клієнтів і регламентує їх права доступу до повідомлень, а також вирішує багато інших завдань.

Поштова служба оперує **електронними повідомленнями** – інформаційними структурами певного стандартного формату. Спрощено електронне повідомлення може бути представлено у вигляді двох частин, одна з яких (заголовок) містить допоміжну інформацію для поштової служби, інша частина (тіло повідомлення) – це власне той «лист», який призначається для читання, прослуховування або перегляду адресатом ( RFC 822).

Головними елементами заголовка є адреси відправника і одержувача у вигляді Polina@ domen.com, де Polina – ідентифікатор користувача поштової служби, а domen.com – ім’я домену, до якого відноситься цей користувач. Крім цього, поштова служба включає в заголовок дату і тему листа, робить відмітки про застосування шифрування, терміновості доставки, необхідності підтвердження факту прочитання цього повідомлення адресатом і ін.

При транспортуванні через Інтернет поштове повідомлення поміщається в конверт (envelope), який також має кілька службових полів, наприклад поле відправника і поля одержувачів (рис. 11.2). Інформація конверта використовується тільки при транспортуванні поштового повідомлення, а інформація заголовка повідомлення – поштовим клієнтом одержувача.

Важливу роль в розширенні можливостей електронної пошти з передачі мультимедійної інформації зіграв стандарт MIME (Multipurpose Internet Mail Extensions – багатоцільові розширення пошти Інтернету). Цей стандарт описує структуру повідомлення, яке складається з декількох частин, кожна з яких має свої заголовок і тіло. Заголовок описує тип даних, які містяться в тілі: це можуть бути як звичайні текстові дані в форматі ASCII, так і дані іншого типу, наприклад:

- текст в 8-бітному форматі (така можливість стала стандартною зовсім недавно, вона описана в документі RFC 6152, прийнятому в березні 2011 року);
- текст не в форматі ASCII, перетворений в ASCII-код (наприклад, за

допомогою алгоритму base64);

- гіпертекст (HTML);
- зображення;
- відеокліп;
- звуковий файл.

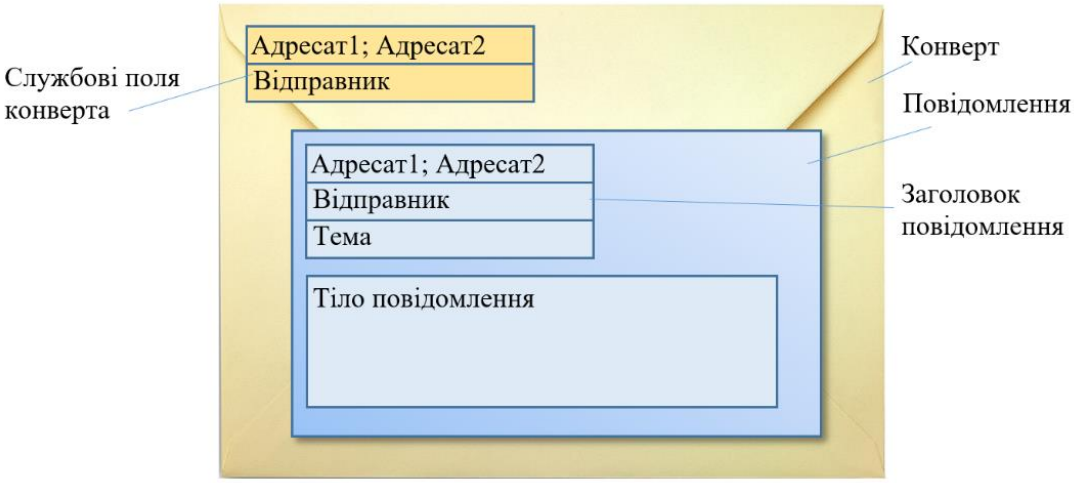



Рис. 11.2. Конверт і повідомлення електронної пошти

У заголовку кожної частини повідомлення є також інформація про те, яким чином поштовий клієнт повинен обробляти тіло частини: відображати її негайно при відкритті повідомлення (наприклад, вставляють зображення в текст) або вважати це тіло вкладенням (додаток), яке користувач буде обробляти сам.

Одна зі специфікацій стандарту MIME (кожна специфікація MIME описує одне або кілька розширень оригінальної специфікації RFC 822), а саме RFC 1847, відноситься до розширень безпеки, тому цей документ називають специфікацією S/MIME (Security MIME). У S/MIME описані два нових типи частин MIME:

- цифровий підпис (Multipart/Signed);
- шифрування тіло (Multipart/Encrypted).

Ці два типи частин повідомлення можуть використовуватися разом з метою забезпечення автентичності, цілісності і конфіденційності електронного листа.

### 11.3.2. Протокол SMTP

В якості засобу передачі повідомлення поштова служба Інтернету використовує стандартний, розроблений спеціально для поштових систем протокол SMTP (Simple Mail Transfer Protocol – простий протокол передачі пошти). Як і більшість протоколів прикладного рівня, SMTP реалізований

несиметричними взаємодіючими частинами: SMTP-клієнтом, що працює на стороні відправника, і SMTP-сервером, що працює на стороні одержувача. SMTP-сервер повинен постійно бути в режимі під'єднання, чекаючи запитів з боку SMTP-клієнта.

Логіка протоколу SMTP є досить простою, як це і випливає з його назви.

- Після того як, застосовуючи графічний інтерфейс свого поштового клієнта, користувач клацає на значку відправки повідомлення, SMTP-клієнт надсилає запит на встановлення TCP-з'єднання на порт 25 SMTP-сервера (це призначений порт).
- Якщо сервер готовий, то він передає свої ідентифікаційні дані, зокрема своє DNS-ім'я. Якщо SMTP-сервер виявився не готовий, то він передає відповідне повідомлення клієнту і той знову надсилає запит, намагаючись заново встановити з'єднання.
- Потім клієнт передає серверу поштові адреси (імена) відправника і одержувача.
- Якщо ім'я одержувача відповідає очікуваному, то після отримання адрес сервер дає згоду на встановлення SMTP-з'єднання і в рамках цього логічного каналу відбувається передача повідомлення.
- Якщо після прийому тіла повідомлення сервер відповідає командою OK, це означає, що сервер прийняв на себе відповідальність за подальшу передачу повідомлення одержувачу.
- Використовуючи одне TCP-з'єднання, клієнт може передати кілька повідомлень, вказуючи в кожному з них поштові адреси відправника і одержувача.
- Після завершення передачі повідомлення TCP- і SMTP-з'єднання розриваються, і надіслане повідомлення буде зберігатись в буфері на сервері.

Хоча в будь-якому протоколі передбачається обмін даними між взаємодіючими частинами, тобто дані передаються в обидві сторони, розрізняють протоколи, орієнтовані на передачу (push protocols), і протоколи, орієнтовані на прийом даних (pull protocols). У протоколах, орієнтованих на передачу, до яких, зокрема, відноситься протокол SMTP, клієнт є ініціатором передачі даних на сервер, а в протоколах, орієнтованих на прийом, до яких відносяться, наприклад, протоколи HTTP, POP3 і IMAP, клієнт є ініціатором отримання даних від сервера.

### 11.3.3. Методи взаємодії клієнта і сервера

**Безпосередня взаємодія клієнта і сервера**

Розглянемо декілька основних схем організації поштової служби. Почнемо з найпростішого, практично не використовуваного зараз варіанту, коли відправник безпосередньо взаємодіє з одержувачем. Як показано на рис. 11.3, у кожного користувача на комп'ютері встановлюються поштові клієнт і сервер.

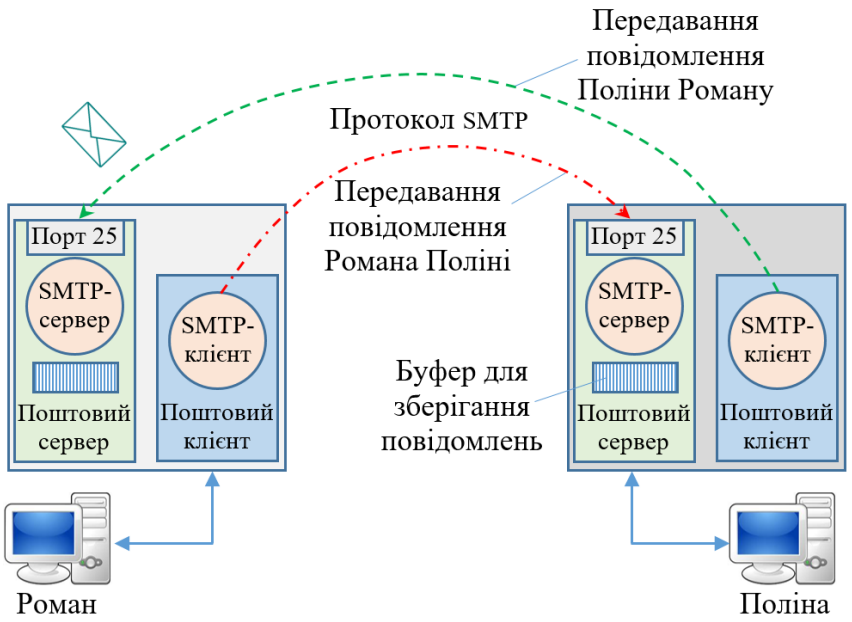



Рис. 11.3. Схема безпосередньої взаємодії клієнта і сервера

Роман, використовуючи графічний інтерфейс свого поштового клієнта, викликає функцію створення повідомлення, в результаті на екрані з'являється стандартна незаповнена форма повідомлення, в поля якої Роман вписує свою адресу, адресу Поліни і тему листи, а потім набирає текст листа. Коли лист готовий, Роман викликає функцію відправки повідомлення, і вбудований SMTP-клієнт надсилає запит на встановлення зв'язку SMTP-серверу на комп'ютері Поліни. В результаті встановлюються SMTP- і TCP-з'єднання, і повідомлення передається через мережу. Поштовий сервер Поліни зберігає лист в пам'яті її комп'ютера, а поштовий клієнт по команді Поліни виводить його на екран, при необхідності виконуючи перетворення формату. Поліна може зберегти, переадресувати або видалити цей лист. Зрозуміло, що в тому випадку, коли Поліна вирішить направити електронне повідомлення Роману, схема роботи поштової служби буде симетричною.

**Схема з виділеним поштовим сервером**

Розглянута вище найпростіша схема поштового зв'язку має серйозний і

очевидний недолік – для обміну повідомленнями необхідно, щоб SMTP-сервер постійно знаходився в очікуванні запиту від SMTP-клієнта. Це означає, що для того, щоб листи, спрямовані Поліні, доходили до неї, її комп'ютер повинен постійно перебувати в режимі онлайн. Зрозуміло, що така вимога для багатьох користувачів є неприйнятною.

Природним вирішенням цієї проблеми є розміщення SMTP-сервера на спеціально виділеному для цієї мети комп'ютері-посереднику. Зазвичай, поштові сервери підтримуються великими організаціями для своїх співробітників або провайдерами для своїх клієнтів. Для кожного домена імен система DNS створює записи типу MX (Mail Exchanger), в яких зберігаються DNS-імена поштових серверів, які обслуговують користувачів, що відносяться до цього домену.

На рис. 11.4 представлена схема з виділеним поштовим сервером. На рисунку показані лише ті компоненти, які беруть участь у передачі повідомлення від Романа до Поліни. Для зворотного випадку схема повинна бути симетрично доповнена.

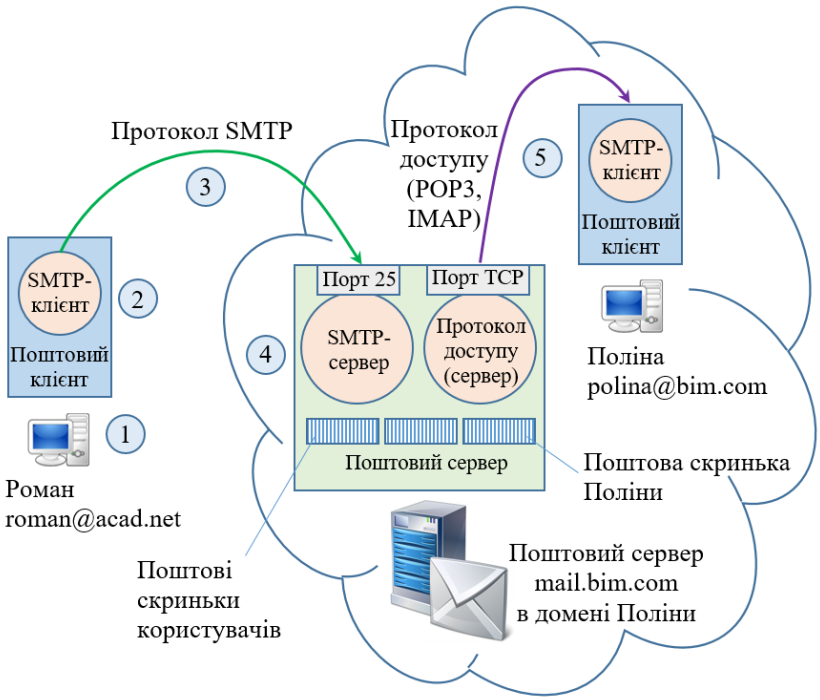



Рис. 11.4. Схема з виділеним поштовим сервером

1. Отже, нехай Роман вирішує надіслати лист Поліні на адресу polina@bim.com. Оскільки готове повідомлення повинно бути направлено конкретному поштовому серверу, клієнт звертається до системи DNS, щоб визначити ім'я поштового сервера, який обслуговує домен Поліни bim.com. Отримавши від DNS-сервера, в якості відповіді, ім'я mail.bim.com, SMTP-клієнт ще раз звертається до DNS, на цей раз, щоб дізнатися IP-адресу поштового сервера mail.bim.com.

2. SMTP-клієнт надсилає по даній IP-адресі запит на встановлення TCP-з'єднання через порт 25 (SMTP-сервер).

3. З цього моменту починається діалог між клієнтом і сервером по протоколу SMTP, який був розглянутий вище. Тут, як і у всіх протоколів, орієнтованих на передачу, напрямок передачі запиту від клієнта на встановлення SMTP-з'єднання збігається з напрямком передачі повідомлення. Якщо сервер виявляється готовим, то після встановлення TCP-з'єднання повідомлення Романа передається.

4. Лист зберігається в буфері поштового сервера, а потім направляється в індивідуальний буфер, відведений системою для зберігання кореспонденції Поліни. Такі буфери називають **поштовими скриньками**. Важливо зауважити, що крім Поліни у поштового сервера є ще багато інших клієнтів, і це ускладнює його роботу. Тобто поштовий сервер повинен вирішувати найрізноманітніші завдання по організації багатокористувацького доступу, включаючи управління поділюваними ресурсами і забезпечення безпечного доступу.

5. У певний момент, який принципово не пов'язаний з моментом надходження повідомлень на поштовий сервер, Поліна запускає свою поштову програму і виконує команду перевірки пошти. Після цієї команди поштовий клієнт повинен запустити протокол доступу до поштового сервера. Однак цим протоколом вже не буде SMTP, оскільки протокол SMTP використовується тоді, коли необхідно передати дані на сервер, а Поліні, навпаки, потрібно отримати їх з сервера.

Для цього випадку були розроблені інші протоколи, узагальнено названі протоколами доступу до поштового сервера, такі, наприклад, як POP3 і IMAP. Обидва ці протоколи відносяться до протоколів, орієнтованим на прийом даних (протокол POP3 очікує запит на встановлення TCP-з'єднання через порт 110, IMAP – через порт 143, на рис. 12.4 ці порти узагальнено показані як порт TCP). В результаті роботи будь-якого з них лист Романа виявиться в пам'яті комп'ютера Поліни. На цей раз направлення запиту від клієнта до сервера не збігається з напрямком передачі даних, який показаний стрілкою.

Протоколи доступу до пошти **POP3** (Post Office Protocol v.3 – протокол поштового відділення версії 3) і **IMAP** (Internet Protocol Access Mail – протокол доступу до електронної пошти Інтернету) вирішують одну і ту ж задачу – забезпечують доступ користувачів до кореспонденції, що зберігається на поштовому сервері.

У зв'язку з багатокористувацьким характером роботи поштового сервера обидва протоколи підтримують автентифікацію користувачів на основі ідентифікаторів і паролів. Однак протоколи POP3 і IMAP мають принципові відмінності, найважливіша з яких полягають в наступному. Отримуючи доступ

до поштового сервера по протоколу POP3, клієнт переміщує адресовані йому повідомлення в пам’ять свого комп’ютера, при цьому на сервері не залишається жодної інформації про це. Якщо ж доступ здійснюється по протоколу IMAP, то в пам’ять комп’ютера клієнта передаються лише копії повідомлень, що зберігаються на поштовому сервері. Ця різниця серйозно впливає на характер роботи з електронною поштою.

**Схема з двома поштовими серверами-посередниками**

На рис. 11.5. показано схему організації поштової служби, найбільш наближену до реальності.

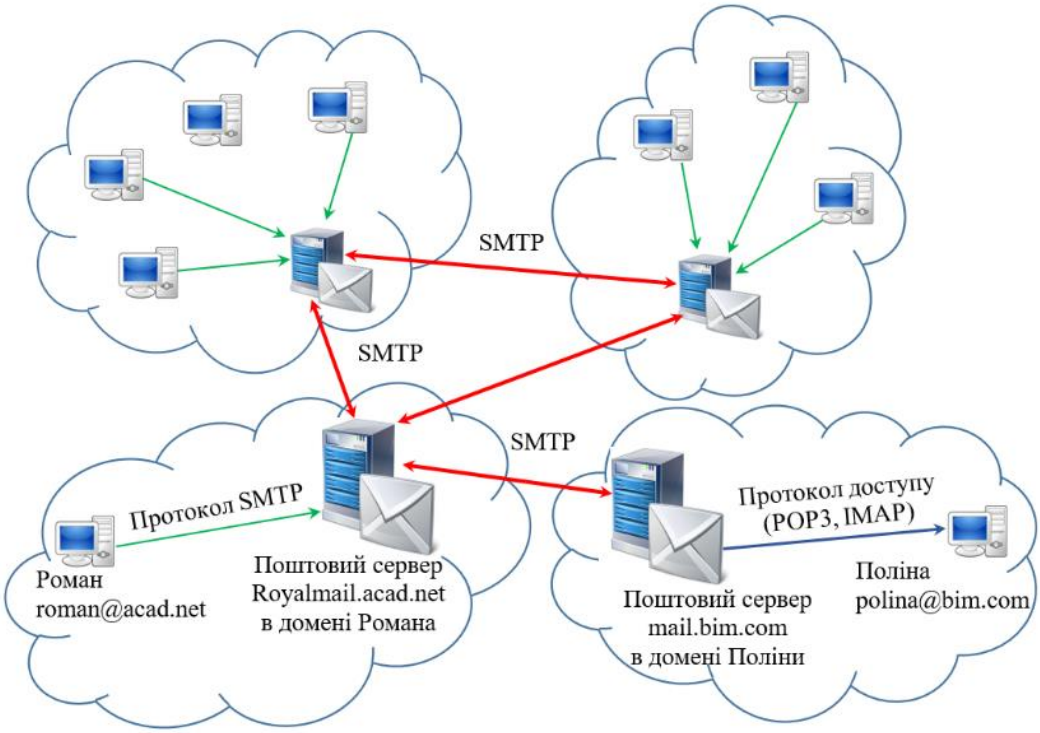



Рис. 11.5. Схема з двома поштовими серверами-посередниками

Тут передача повідомлень між клієнтами пошти (між відправником Романом і одержувачем Поліною) проходить через два проміжних поштових сервера, кожен з яких обслуговує домен свого клієнта. На кожному з цих серверів встановлені також і клієнтські частини протоколу SMTP. При відправці листа поштовий клієнт Романа передає повідомлення по протоколу SMTP поштовому серверу домена, до якого належить Роман – Royalmail.acad.net. Це повідомлення буферизується на даному сервері, а потім по протоколу SMTP передається далі на поштовий сервер домену Поліни – mail.bim.com, звідки потрапляє на комп’ютер Поліни.

Показана на рис. 14.5 двоступенева передача повідомлень через два

поштових сервера підвищує надійність і гнучкість процедури доставки повідомлення. Дійсно, в схемі з передачею повідомлення відразу на сервер одержувача поштовий клієнт відправника в разі несправності поштового сервера повинен самостійно справлятися з нештатної ситуацією. Якщо ж посередником у передачі повідомлення є інший поштовий сервер, то це дозволяє реалізовувати різноманітні логічні механізми реакції на відмови на стороні сервера, який до того ж завжди знаходиться в режимі онлайн. Наприклад, при неможливості передати лист поштовому серверу одержувача сервер відправника може не лише рапортувати про це свого клієнта, а й робити власні дії – намагатися знову переслати лист, повторюючи ці спроби протягом досить тривалого періоду.

## 11.4. Послуга IPTV

Послуги **IPTV** забезпечують можливість переглядати відеофільми, телевізійні канали, які передаються у мережі IP-пакетами. Оскільки відеофільм містить як зображення, так і звук, послугу IPTV ще називають **послугою передавання мультимедійних даних.**

Надання послуг IPTV у мережі можна організувати, використовуючи службу за запитом (Service On Demand) у режимі негрупового розсилання (Unicast) або дистрибутивну службу в режимі групового розсилання (Multicast).

Послуга IPTV, яку надають у режимі Unicast, має назву **відео за запитом** (Video on Demand, **VoD**). Відеоконтент розміщається на спеціалізованому відеосервері й за потребою користувач може завантажити його на свій комп'ютер або спеціальний термінал з наступним відтворенням. Таким чином послуга VoD надається не в реальному масштабі часу.

IPTV у режимі Multicast дає змогу переглядати програми телевізійного каналу в реальному масштабі часу.

У разі, коли певна кількість користувачів бажає дивитися один і той самий телевізійний канал, у мережі формується Multicast-група. При цьому відпадає необхідність організовувати окремий канал передавання мультимедійних даних для кожного користувача. Потік даних передають до найближчого сервісного вузла, де дані дублюються, а потім передаються усім членам групи. Це дає змогу істотно розвантажити ресурси мережі.

Для забезпечення роботи Multicast-груп логічні вузли мережі повинні обмінюватися інформацією про склад груп і вказівками, кому який контент необхідно доправити. Ці процедури реалізує **протокол керування групами користувачів у Інтернеті** (Internet Group Membership Protocol, **IGMP**). Протокол IGMP забезпечує повне керування режимом групового розсилання, починаючи від створення Multicast-групи і завершуючи забезпеченням

можливості як під'єднання до неї нових користувачів, так і від'єднання окремих користувачів від групи за їх бажанням.

Мультимедійні дані в IPTV відображають у форматі одного зі стандартів сімейства MPEG (Moving Picture Experts Group – експертна група з питань рухомого зображення). MPEG-стандарти описують основні алгоритми, які використовують для стиснення аудіовізуальної інформації, компонентами якої є відео, звук, графіка, текстові та графічні документи. Алгоритми MPEG забезпечують стиснення кожного з них, забезпечуючи тим самим можливість передавати мультимедійні дані наявними мережами зв'язку.

У даний час існують наступні стандарти, які використовують у IPTV:

- **MPEG-1**: Вихідний стандарт аудіо- та відеокомпресії, що забезпечує швидкість передавання 1,5 Мбіт/с. Застосовувався, як стандарт для Video CD, також включає популярний формат MP3.
- **MPEG-2**: Транспортні, аудіо- і відеостандарти для широкомовного телебачення. Використовується в цифровому телебаченні, цифрових супутникових ТВ службах, цифровому кабельному телебаченні, і (з невеликими змінами) у DVD. Забезпечує швидкості передавання до 15 Мбіт/с для **телебачення високої роздільної здатності**, (High-Definition Television, **HDTV**).
- **MPEG-3**: Початково розроблявся для HDTV, але від нього відмовилися, коли виявилося, що MPEG-2 цілком достатньо для HDTV.
- **MPEG-4**: Розширює MPEG-1 для підтримки відео/аудіо «об'єктів», 3D контенту, стиснення з низьким бітрейтом. У нього включено декілька нових високоефективних відеостандартів (альтернатив MPEG-2).

Останній стандарт вважають найбільш перспективним. Розглянемо його детальніше.

Формування потоку мультимедійних даних послуги IPTV у форматі MPEG-4 показано на рисунку 11.6.

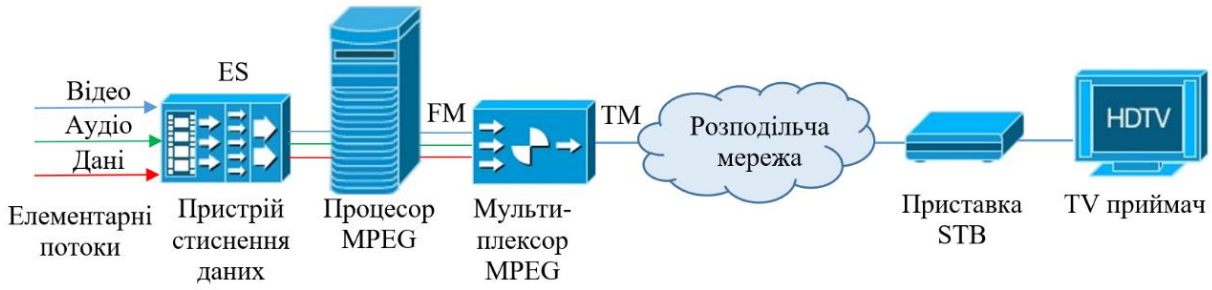



Рис. 11.6. Формування потоку мультимедійних даних послуги IPTV у форматі MPEG-4

Узагальнено функціонування MPEG-4 можна описати таким чином.

Так звану «**мультимедійну сцену**» (Scene Description) розбивають на елементарні об'єкти (відео, графічні об'єкти, фон, рухомі об'єкти, фонові звуки, мова та ін.). З'ясовують абсолютне положення об'єктів, їх взаємовідношення та поведінку кожного з них у межах сцени. Кожному з об'єктів присвоюють ярлик із властивостями й інформацією про синхронізацію.

Об'єкти подаються у вигляді **елементарних потоків** (Elementary Stream, **ES**). Кожен з елементарних потоків – це певний тип цифрового сигналу зі своїми правилами кодування та форматом MPEG. Для кожного елементарного потоку визначаються параметри декодера, необхідні для його подальшого декодування із заданою якістю.

Потім усі елементарні потоки за допомогою процесора MPEG перетворюються у вторинні потоки FM (FlexMux) відповідно до заданої якості на канал QoS та здійснюється завадостійке кодування. Прикладом QoS може бути час затримки або достовірність передавання. Потоки FM не залежать від середовища передавання, через яке здійснюється постачання мультимедіа контенту користувачу. Далі потоки FM мультиплексуються мультиплексором MPEG у транспортний пакетизований потік TM (TransMux) відповідно до наявних і запитуваних мережевих ресурсів. Структуру цього потоку повністю визначає використовуваний канал зв'язку.

Декодування прийнятого потоку MPEG-4 здійснюється в зворотному порядку. На приймальному кінці в абонента телевізійний сигнал відновлюється за допомогою телевізійної приставки **STB** (Set-Top-Box – дослівно – «коробка, яку установлюють нагорі»). STB відіграє активну роль у відтворенні мультимедійної сцени, в процес якої може втручатися й сам користувач.

**STB** – це багатофункційна домашня приставка-адаптер для приймання програм цифрового та кабельного ТБ за допомогою звичайних телевізорів, що забезпечує інтерактивну взаємодію «глядач-телеканал» і можливість роботи в мережі Інтернет через будь-яку широкосмугову мережу доступу. Залежно від закладеної функціональності приставка може додатково мати можливості сучасних мультимедійних цифрових платформ інтерактивного телебачення й підтримувати широкий спектр послуг: відео за запитом, електронний програмний гід, інтелектуальний відеомагнітофон, інтерактивні ігри, електронну пошту, а також покупки через Інтернет, банківські операції з дому, телефонні послуги та багато іншого. Таким чином, постачаючи аудіо-, відеоінформацію та дані не тільки в будинок, але й у зворотному напрямку та всередині локальної будинкової мережі, STB стає своєрідним домашнім шлюзом у різні телекомунікаційні мережі.

## 11.5. IP-телефонія

### Етапи розвитку IP-телефонії

**IP-телефонія** – це мережева служба, яка надає телефонні послуги передавання голосу по IP-мережі.

Поняття «IP-телефонія» поширюється також і на ті випадки, коли голос передається разом з іншими видами інформації, зокрема з текстом і зображенням. Крім Терміну «IP-телефонія» вживаються також терміни «VoIP» (Voice over IP – голос через IP) і «інтернет-телефонія». Хоча абревіатура VoIP часто використовується як синонім терміну «IP-телефонія», існує її більш широке трактування – будь-яка послуга, що включає передачу голосу по протоколу IP; це може бути, наприклад, передача голосової реклами при натисканні на відповідному значку, розташованому на веб-сторінці. Інтернет-телефонія – це окремий випадок IP-телефонії, коли розмова відбувається через Інтернет, а не, наприклад, в межах локальної мережі підприємства.

У своєму розвитку IP-телефонія пройшла три етапи.

На *першому етапі* це була, скоріше, інтернет-забава, придатна хіба що для спілкування двох ентузіастів, готових миритися з низькою якістю передавання голосу. Два комп'ютери, оснащені мікрофонами, динаміками, звуковими картами з підтримкою оцифровування звуку і не складним програмним забезпеченням, дозволяли вести двосторонній діалог через Інтернет в реальному часі (рис. 12.7).

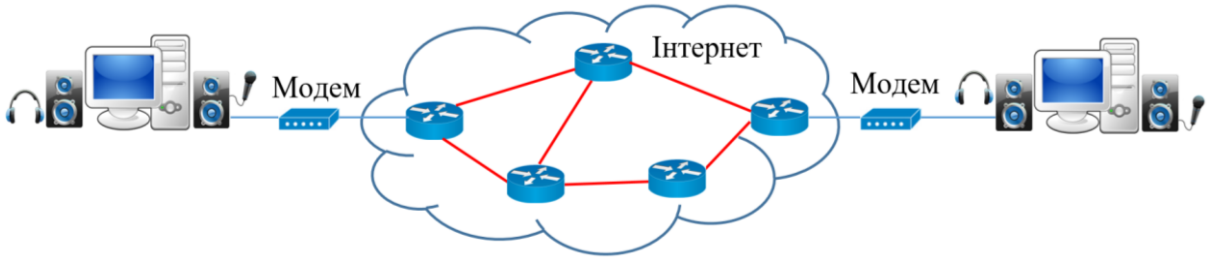



Рис. 11.7. Засоби підтримки розмови користувача через Інтернет

Однак до зручностей звичайної телефонної послуги такий спосіб спілкування явно недотягав. Абонентам потрібно було знати IP-адресу комп'ютера співрозмовника, домовлятися про час розмови, вибирати момент для якіснішої передачі мови, коли трафік Інтернету між даними конкретними точками не стикався з перевантаженнями і затримками. Крім того, при відсутності стандартів на обох комп'ютерах потрібно було встановити таке

програмне забезпечення, яке підтримувало б один і той же спосіб кодування голосу. Взаємодії між комп'ютером і телефоном, під'єднаним до звичайної телефонної мережі, не передбачалась. Проте витрати обмежувалися невеликою платою провайдерові за звичайне комутоване під'єднання до Інтернету.

*Другий етап* ознаменувався появою стандартів IP-телефонії, перш за все – стандартів групи H.323, розроблених ITU-T, і стандартів на основі протоколу SIP, розробленого IETF.

До *третього етапу* можна віднести появу нового покоління IP-телефонії, що підтримує широкий спектр додаткових послуг, подібний до того, який надають абонентам розвинені телефонні мережі.

## Стандарти H.323

Розробники **стандартів H.323** виходили з того, що дві мережі – телефонна і IP – співіснуватимуть пліч-о-пліч досить тривалий час, а значить, важливо регламентувати їх взаємодію з урахуванням існуючих в традиційних телефонних мережах процедур встановлення з'єднання, а також домовитися про спосіб передачі виклику і власне голосу по IP-мережі.

В рамках встановленого сеансу H.323 абоненти можуть обмінюватися не тільки голосовою, але і відеоінформацією, тобто користуватися відеотелефонами або обладнанням для організації відеоконференцій.

У стандартах H.323 визначається дві групи протоколів (рис. 11.8).

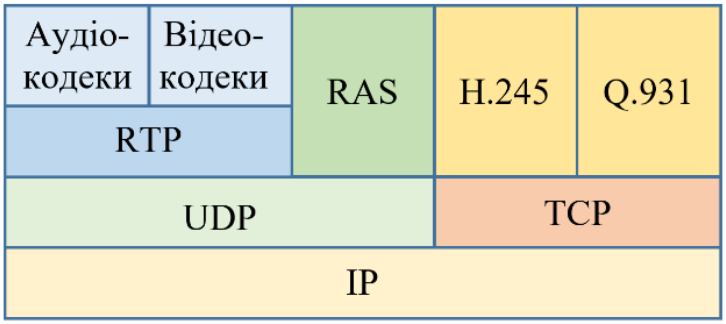



Рис. 11.8. Стек протоколів H.323

**Протоколи транспортної площини** (transport plane) відповідають за безпосередню передачу голосу по мережі з комутацією пакетів. Протоколи цієї площини визначають способи кодування голосу (сюди входять стандарти різних кодеків, наприклад G.711, G.723.1, G.729, G.728 і ін.) і відео (кодеки H.261, H.263 і ін.). Голос і відео передаються в пакетах протоколу RTP (Real Time Protocol – протокол реального часу), який визначений в RFC 3550 і переносить позначки часу і послідовні номера пакетів, допомагаючи кінцевим вузлам сеансу

відновлювати аналогову інформацію реального часу. Пакети RTP переносяться в пакетах протоколу UDP.

**Протоколи площини управління викликами** (call control plane) переносять по мережі запити на встановлення з'єднань і реалізують такі службові функції, як авторизація доступу абонента до мережі і облік часу з'єднання. Ця група протоколів працює через надійні TCP-з'єднання і включає протокол сигналізації Q.931, що забезпечує встановлення і завершення з'єднання між абонентами; протокол H.245, за допомогою якого абонентське обладнання дізнається про функціональні можливості протилежної сторони, наприклад про те, які аудіо- і відеокодеки підтримуються, а також про те, скільки аудіо- і відеопотоків використовуватимуть абоненти в рамках даного з'єднання. За замовчуванням IP-телефон підтримує тільки один голосовий потік, але відеотелефон вже підтримує два потоки – один голосовий і один відео, а обладнання відеоконференцій може підтримувати кілька аудіопотоків і кілька відеопотоків. Ще один протокол цієї групи – RAS (Registration, Admission, Status) – служить для обліку дзвінків, реєстрації користувача в деякому адміністративному домені (наприклад, в домені організації, де працює користувач) і контролю доступу в мережу. Контроль доступу полягає в перевірці наявності мережевих ресурсів, необхідних для якісного обслуговування телефонного виклику, наприклад вільної пропускної спроможності).

Основними елементами мережі H.323, в яких реалізуються протоколи цього стеку, є IP-телефони, шлюзи і контролери зони H.323 (рис. 11.9).

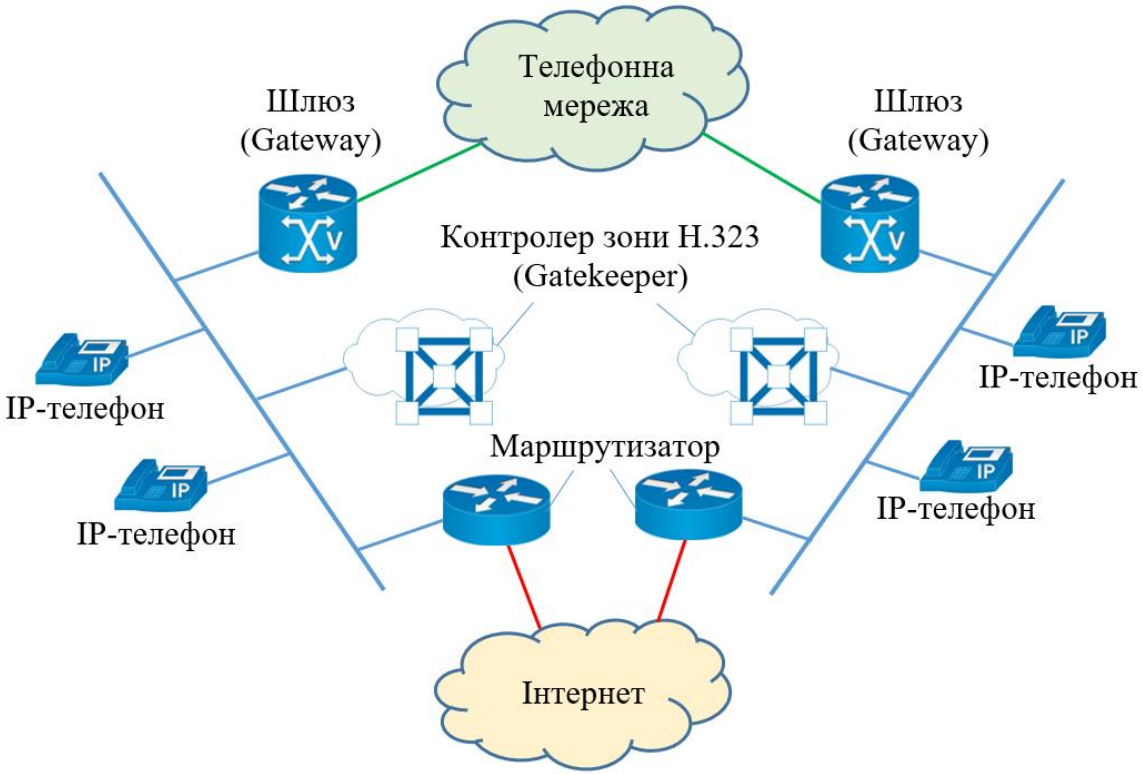



Рис. 11.9. Елементи мережі H.323

**IP-телефон** являє собою звичайний телефонний апарат з кнопковим набором і дисплеєм для відображення інформації про виклики і довідкової інформації (наприклад, телефонних номерів абонентів). IP-телефон під'єднується до IP-мережі через з'єднання Ethernet.

**Шлюз** (**Gateway**) з'єднує традиційну телефонну мережу з IP-мережею, він забезпечує трансляцію запакованого в пакети оцифрованого і часто стисненого голосу в форму, придатну для передачі по телефонній мережі загального користування. Крім того, в функції шлюзу H.323 входить трансляція протоколів сигналізації телефонних мереж, таких, наприклад, як SS7, в протоколи сигналізації стека H.323. Шлюз дозволяє абонентам із звичайним телефонним апаратом спілкуватися з користувачами IP-телефонів або ж задіяти IP-мережу як транзитну.

Основне завдання площини управління викликами – встановлення з'єднання між абонентами через мережі з комутацією пакетів – в простому випадку може бути вирішена шлюзом, а в більш загальній постановці доручається спеціальному елементу мережі – контролеру зони H.323.

**Контролер зони H.323** (Gatekeeper) виконує реєстрацію і авторизацію абонентів по протоколу RAS, а також, в разі необхідності, трансляцію адрес (наприклад, DNS-імен в телефонні номери). Крім того, він займається маршрутизацією викликів до IP-телефону або шлюзу, а якщо буде потрібно, то і до іншого контролера зони H.323.

У функції контролера зони H.323 може також входити взаємодія з інтелектуальною мережею. Інтелектуальна мережа (IN) є частиною сучасної цифрової телефонної мережі, яка надає її абонентам додаткові послуги, такі як переадресація виклику, конференц-зв'язок, телеголосування і ін. Інтелектуальна мережа по своїй структурі є комп'ютерною мережею з серверами, на яких програмується логіка послуг.

## Стандарти на основі протоколу SIP

Основним конкурентом протоколів стандарту H.323 є **протокол SIP** (Session Initiation Protocol – протокол ініціювання сеансу), розроблений інтернет-спільнотою і стандартизований IETF в RFC 3261. SIP є протоколом сигналізації, він відповідає за встановлення сеансу між абонентами, при цьому SIP виконує функції протоколів Q.931, RAS і H.245 стандарту H.323 (точніше – частину з них). Для передачі аудіо- та відеоданих під час сеансу зв'язку протокол SIP передбачає використання протоколу RTP.

Протокол SIP дуже близький за стилем до протоколу HTTP: він має схожий набір і синтаксис повідомлень, якими обмінюються сторони в процесі

встановлення сеансу. Як і у протоколу HTTP, SIP-повідомлення текстові, вони добре зрозумілі програмістам, які мають досвід створення веб-додатків. Тому системи IP-телефонії, побудовані на основі SIP, виявилися набагато ближче до світу Інтернету, ніж стандарти H.323, що прийшли від «телефоністів». Сьогодні SIP-телефонія більш тісно інтегрована з веб-послугами, ніж телефонія стандарту H.323.

Архітектура SIP передбачає як безпосередню взаємодію абонентів через IP-мережу, так і більш масштабовані схеми, що включають участь серверів-посередників (proxy servers). Основним таким сервером є так **проксі-сервер SIP**, він виконує функції, близькі до функцій контролера зони H.323. Крім того, в архітектурі SIP може бути присутнім сервер позиціонування (SIP Location Server).

Роботу протоколу SIP в архітектурі з серверами обох типів ілюструє рис. 11.10.

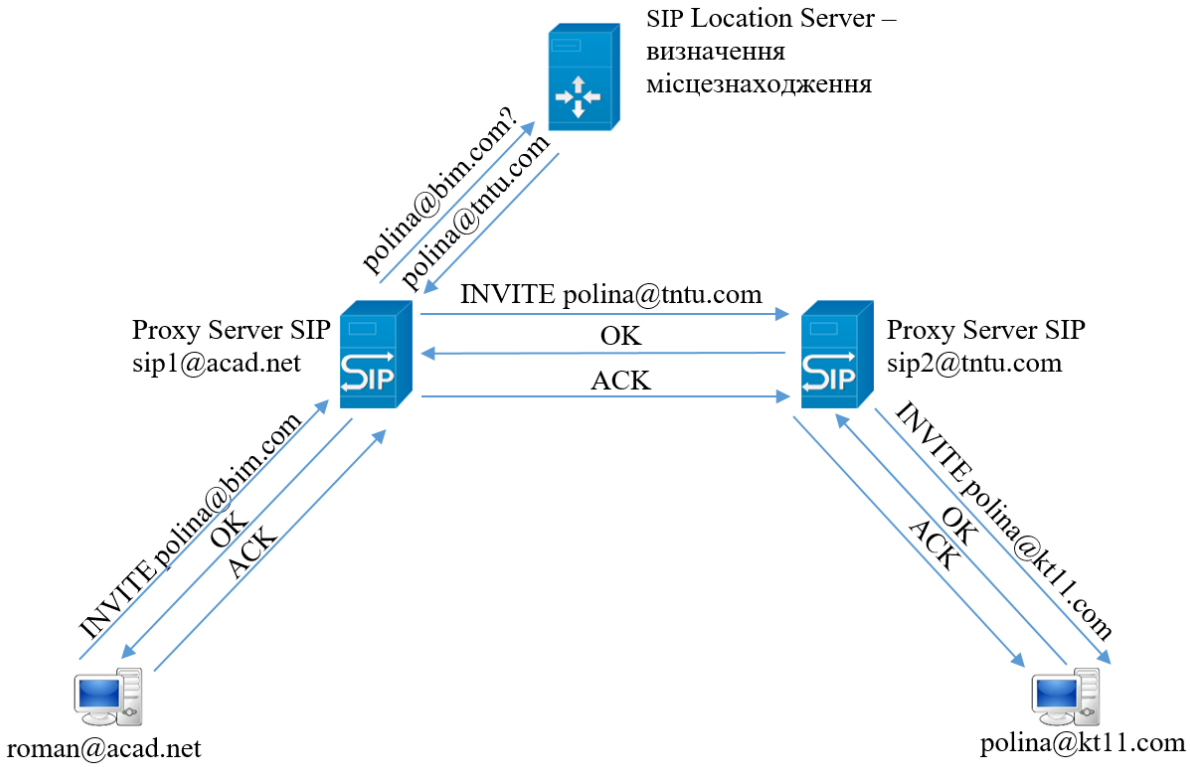



Рис. 11.10. Взаємодія елементів SIP

Адресами абонентів в протоколі SIP є універсальні ідентифікатори (URI), що використовуються в усіх веб-службах. На рис. 12.10 абонент roman@acad.net хоче встановити сеанс з абонентом polina@bim.com. В домені acad.net встановлений проксі-сервер SIP з ім’ям sip1@acad.net, через нього проходять усі виклики абонентів цього домену (за рахунок того, що в IP-телефонах абонентів задано IP-адреси цього проксі-сервера).

Запитом на встановлення сеансу в протоколі SIP є передача повідомлення INVITE з URI абонента, тому абонент roman@acad.net направляє своєму проксі-серверу повідомлення INVITE polina@bim.com. Проксі-сервер для виконання цього запиту звертається до сервера визначення місця розташування, який повертає йому відповідь про те, що абонент polina@bim.com в даний момент зареєстрований в домені tntu.com з ім'ям polina@tntu.com. Проксі-сервер використовує цю інформацію для того, щоб направити повідомлення INVITE проксі-серверу домена tntu.com (сервер з ім'ям sip2@tntu.com), вказавши в ньому ім'я polina@tntu.com.

Розмова завершується проксі-сервером sip2@tntu.com, який виявляє, що користувач polina@tntu.com зареєструвався і працює в даний час за комп'ютером kt11, тому виклик INVITE передається на цей комп'ютер. Далі протокол SIP працює подібно до більшості протоколів сигналізації: якщо користувач polina@kt11.com погоджується прийняти виклик, то вона знімає трубку свого SIP-телефону (або клацає на відповідному значку свого програмного SIP-телефону) і тим самим посилає відповідь ОК назад по ланцюжку. Остаточне встановлення сеансу фіксується відправкою повідомлення АСК (підтвердження) від викликаючого абонента.

Після встановлення сеансу розмова відбувається між телефонами абонентів в рамках протоколу RTP.

Існують також фірмові протоколи IP-телефонії, з яких найбільш відомими є **протоколи Skype** – популярного сервісу інтернет-телефонії. Цей сервіс до того ж підтримує такі додаткові послуги, як відеоконференції, передача миттєвих повідомлень, передача файлів між абонентами.

**Взаємодія телефонних мереж через Інтернет**

На другому етапі розвитку IP-телефонії IP-мережу (Інтернет або приватну мережа) широко використовувалася в якості транзитної мережі між двома місцевими телефонними мережами (рис. 11.11).

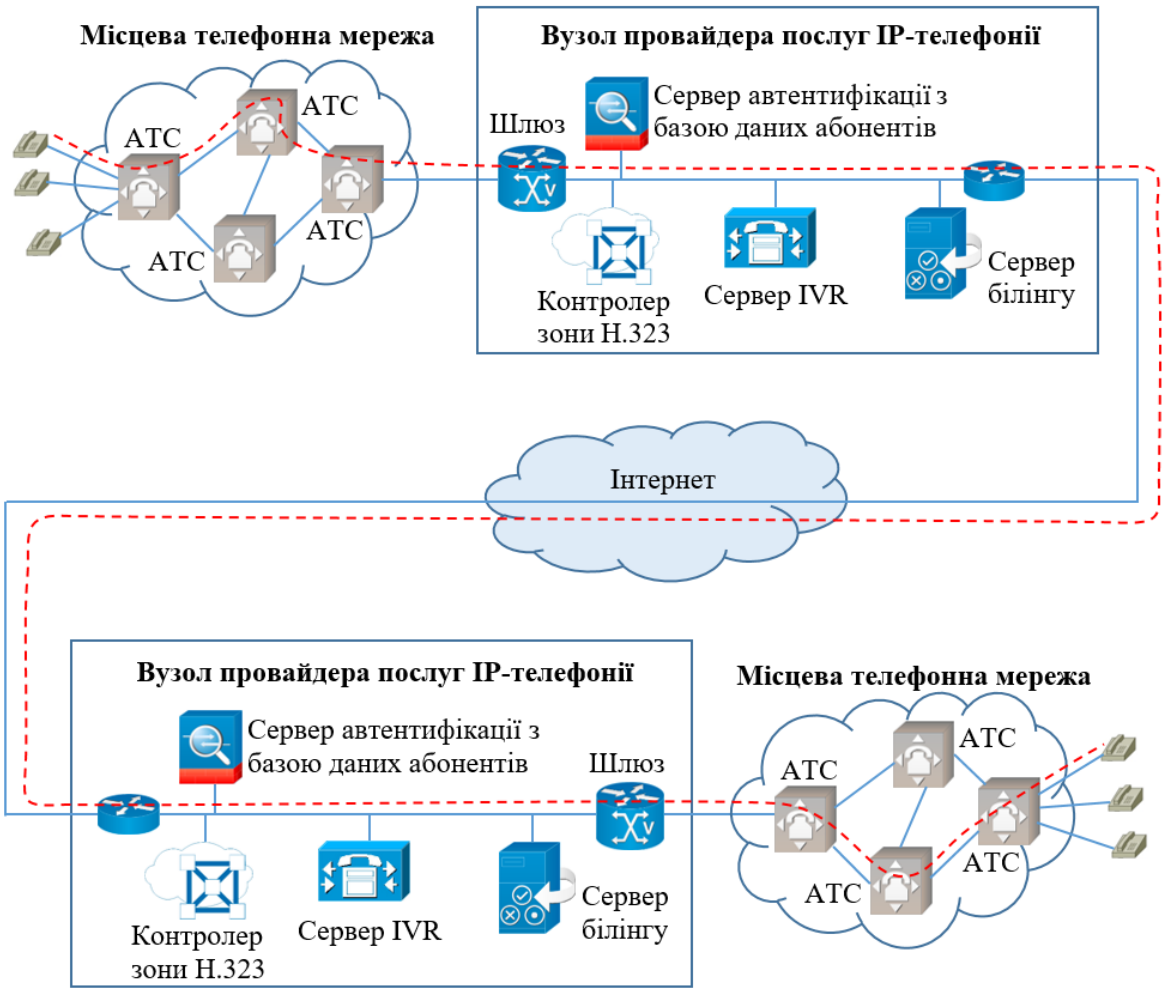



Рис. 11.11. Взаємодія двох місцевих телефонних мереж через Інтернет

Дана схема реалізації загальнодоступних послуг IP-телефонії полягає в тому, що абонент дзвонить за вказаним номером, який закріплений за провайдером місцевої телефонної мережі, і на дзвінок відповідає **сервер інтерактивної голосової відповіді** (Interactive Voice Response, **IVR**). IVR-сервер запрограмований на виконання процедур автентифікації абонента і прийому номера викликаючого абонента. Для цього залучається техніка розпізнавання голосових відповідей (якими можуть бути і сигнали тонового набору, що використовуються абонентом для відповідей на запити IVR-сервера).

Для реалізації послуги IP-телефонії за описаною схемою оператору зв'язку не треба створювати власну дорогу транспортну інфраструктуру і мати

безпосередній доступ до абонентів. Однак стратегічні перспективи такого підходу залишають бажати кращого через погану масштабованість і вузький спектр послуг.

Масштабованість такого варіанту обмежується декількома факторами. По-перше, провайдеру доводиться встановлювати численні однорангові зв'язку з іншими провайдерами. По-друге, протоколи обох площин необхідно реалізовувати в усіх елементах мережі IP-телефонії: і в контролерах зони, і в шлюзах, і в терміналах, що призводить до зайвої складності і дорожнечі всіх цих пристроїв. І нарешті, користувачам надаються тільки базові послуги з обробки викликів, оскільки взаємодія з такими протоколами телефонної мережі, як протокол міжстанційної сигналізації (SS7) і протоколи інтелектуальної мережі (IN) відсутні. Цю останню групу недоліків неможна віднести на рахунок стандартів H.323, в яких явно не йдеться про те, які протоколи сигналізації повинен підтримувати шлюз з боку телефонної мережі. Перелік додаткових послуг по обробці викликів визначений в Специфікації H.450. Таким чином, це скоріше недолік реалізації шлюзів того покоління, в яких підтримка SS7 і IN, як правило, відсутня.

Крім того, сам діалог досить обтяжливий – набагато зручніше просто набрати номер і отримати доступ до послуг міжнародної IP-телефонії. Але для цього провайдеру потрібен прямий доступ до абонента або домовленість з місцевими операторами про переадресації таких викликів на шлюз IP-телефонії провайдера за допомогою засобів інтелектуальної мережі (а вони поки підтримуються далеко не всіма місцевими операторами). Таким чином, для виходу IP-телефонії на більш високий рівень національного або міжнародного оператора потрібні інші стандарти і обладнання, щоб мережі, побудовані на базі протоколу IP, могли рівноправно співпрацювати з традиційними телефонними мережами.

Багато з необхідних стандартів уже з'явилися і втілені в новому поколінні обладнання, яке стало основою для третього етапу розвитку IP-телефонії.

## Третє покоління мереж IP-телефонії

Укрупнена схема повномасштабної мережі IP-телефонії показана на рис. 11.12. Така мережа може підтримувати власних абонентів і бути транзитною для традиційних телефонних мереж з наданням повного спектру послуг, включаючи послуги інтелектуальної мережі.

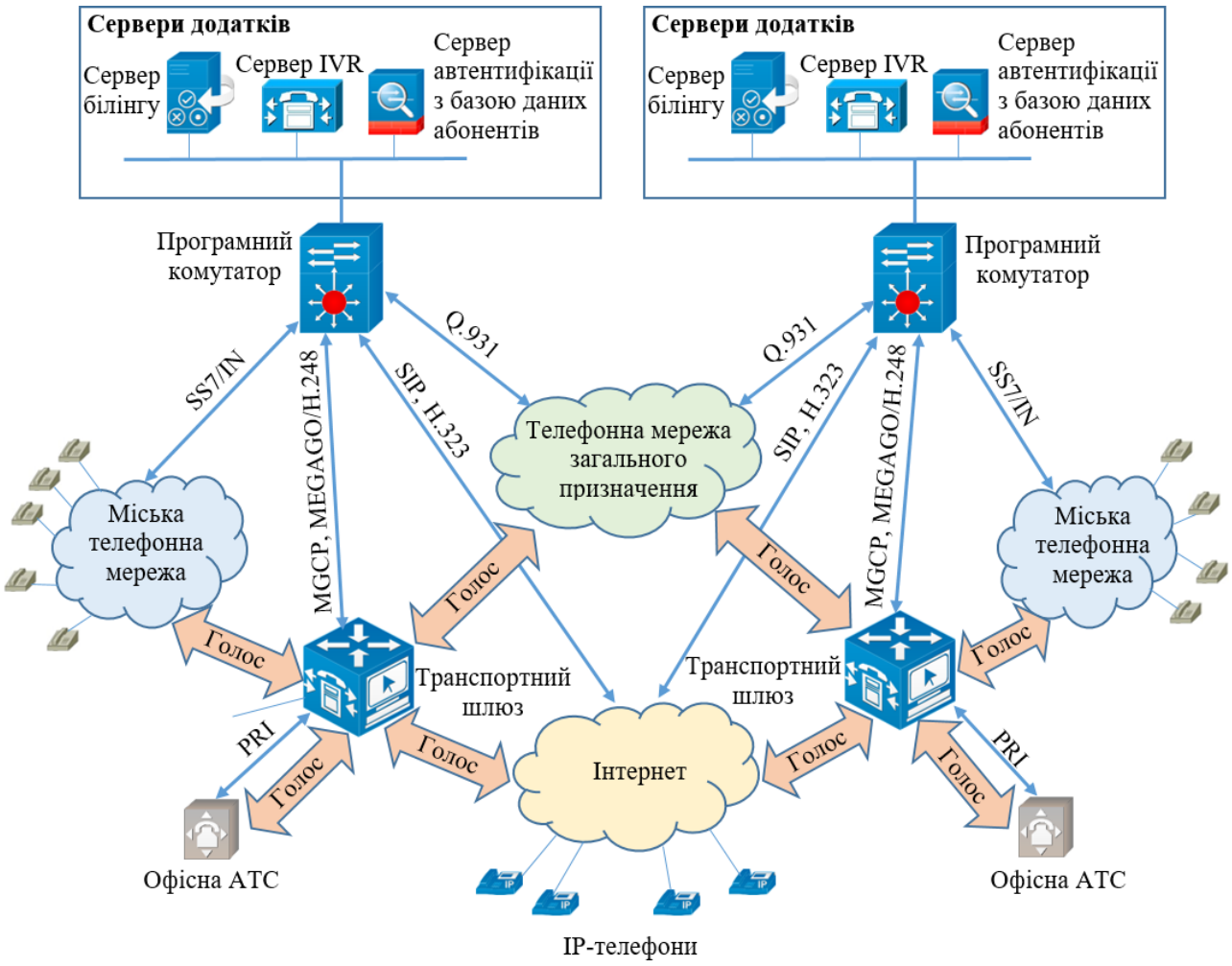



Рис. 11.12. Масштабована архітектура IP-телефонії

В вузлах мережі IP-телефонії нового покоління відбувся чіткий поділ функцій на три групи:

- транспортну;
- управління викликами;
- прикладних сервісів.

Транспортна група утворилася за рахунок виділення з шлюзу функціональної частини, яка виконує дуже просту операцію – комутацію між вхідними та вихідними портами (фізичними або віртуальними). Цей елемент,

який отримав назву **транспортного шлюзу** (Media Gateway), є свого роду аналогом комутаційного поля телефонної станції.

Групу управління викликами складають протоколи сигналізації IP-телефонії (H.225.0, RAS із стандарту H.323 або SIP). До цієї групи відносять також протоколи керування транспортними шлюзами, які ініціюють дії по комутації портів. Всі перераховані базові функції по обробці викликів сьогодні часто реалізуються одним пристроєм – **програмним комутатором** (Softswitch).

Третя група функцій утворює рівень сервісів, який реалізований універсальними серверами у вигляді звичайних мережевих додатків. Прикладами таких сервісів є ініціювання телефонного виклику при натисканні на певній кнопці веб-сторінки, передача виклику абоненту, підключеного до Інтернету по телефонній мережі, а також послуги інтелектуальної мережі. У мережах IP-телефонії другого етапу розвитку рівень сервісів практично був відсутній –користувацькі послуги надавав лише IVR-сервер, а решта прикладні програмні системи цього рівня реалізовували внутрішні для провайдера функції – білінг, автентифікацію і т. п. Тепер рівень сервісів підтримує весь спектр додаткових послуг, які можуть надавати абонентам розвинені телефонні комутатори міського типу, в тому числі і за допомогою інтелектуальної мережі: переадресацію викликів у відповідності з різними умовами, телеголосування, безкоштовний дзвінок, дзвінок за спеціальним тарифом, скорочений набір і т. п.

Взаємодія між рівнями здійснюється через стандартні інтерфейси, а це створює серйозні передумови для побудови телефонних вузлів IP-телефонії на основі продуктів різних виробників із застосуванням загальноприйнятих методів обробки викликів. Такий уніфікований модульний підхід був би дуже привабливий і при розробці традиційних телефонних мереж, однак виробники телефонних комутаторів зазвичай реалізовували функції двох нижніх рівнів і взаємодію між ними з використанням власних корпоративних стандартів. Тільки при створенні архітектури інтелектуальної мережі вдалося, нарешті, втілити в життя принцип незалежності верхнього рівня від двох нижніх і прийняти в якості стандарту міжрівневої взаємодії **прикладний протокол інтелектуальної мережі** (Intelligent Network Application Protocol, **INAP**), що працює поверх **протоколів системи сигналізації №7** (Signalling System No. 7, **SS7**).

Масштабованість комутації і незалежність транспортного рівня від рівня управління викликами в новому поколінні вузлів IP-телефонії досягається завдяки застосуванню концепції програмного комутатора. Даний керуючий елемент відповідає за обробку повідомлень протоколів сигналізації, на підставі яких відбуваються з'єднання: наприклад, протоколу H.225.0 стеку H.323, протоколу встановлення з'єднань SIP або ж протоколу сигналізації SS7.

За допомогою спеціального протоколу «головний-підлеглий» програмний комутатор управляє транспортними шлюзами, які, в кінцевому рахунку, і здійснюють комутацію голосових каналів. Для управління шлюзами можуть використовуватися кілька близьких за логікою роботи протоколів: **SGCP** (Simple Gateway Control Protocol – простий протокол управління шлюзом), **MGCP** (Media Gateway Control Protocol – протокол управління медіашлюзами) або **MEGACO/H.248** (Media Gateway Control Protocol (MEGACO) або H.248 – протокол, що використовується між елементами телекомунікаційних мереж: шлюзом (Media Gateway) і контролером шлюзів (Media Gateway Controller). Стандартом, прийнятим як IETF, так і ITU-T, є тільки спільно розроблений ними протокол MEGACO/H.248, однак і попередники цього стандарту, протоколи SGCP та MGCP, успішно реалізуються в продуктах різних виробників. За допомогою одного з названих протоколів програмний комутатор з'ясовує деталі поточного стану з'єднань і портів шлюзу, а також передає йому вказівки про те, яку пару портів (фізичних або логічних) потрібно з'єднати, і деякі інші приписи. Таким чином, реалізація шлюзу може бути досить простою, а весь інтелект управління з'єднаннями переміщається на рівень програмного комутатора, який в моделі розподіленої комутації управляє одночасно декількома шлюзами. Саме такий варіант показаний на рис. 11.12.

У протоколах SGCP, MGCP і MEGACO/H.248 керуючий елемент називається **агентом виклику** (call agent). Зазвичай, в Softswitch виробники поміщають елементи рівня управління викликами декількох стандартів, щоб такий програмний комутатор міг взаємодіяти з іншими зонами телефонної мережі по найбільш популярних протоколах сигналізації. Так, в програмний комутатор може входити контролер зони стандарту H.323, сервери стандарту SIP (проксі-сервер, сервер переадресації і сервер позиціонування користувачів), а також шлюзи телефонної сигналізації для перетворення протоколів телефонних мереж до протоколів сигналізації IP-телефонії – ті ж SIP і H.225.0 стеку H.323. Широка підтримка протоколів сигналізації дозволяє програмному комутатора взаємодіяти практично з будь-якими типами телефонних мереж, як з традиційними (з комутацією каналів), так і з пакетними.

## Нові послуги IP-телефонії

У проміжним пристроях IP-мережі не зберігається інформація про кожне з'єднання абонентів (комп'ютерів користувачів) з серверами. Це одна з принципових її відмінностей від телефонної мережі. Комутатори телефонної мережі, навпаки, відстежують і запам'ятовують стан кожного виклику, що є

однією з причин більш високої вартості передавання ними транзитного трафіку в порівнянні з IP-маршрутизаторами.

ITU неодноразово наголошує на тому, що здешевлення дзвінків і конкурентний тиск на сектор традиційної міжнародної телефонії є короткостроковою перевагою IP-телефонії. В стратегічній перспективі основним напрямом стане розгортання нових послуг, зокрема інтегрованих з послугами передавання й маніпулювання даними, якими є:

- **Click to Talk** – ініціювання телефонної розмови при перегляді сторінки Web;
- **Internet Call Waiting** – повідомлення абонента, який під'єднується за допомогою телефонної мережі до Інтернету, про наявність вхідного виклику і, можливо, організація паралельної з Інтернет-сеансом розмови за допомогою пакетного передавання;
- **Unified Messaging** – організація єдиної поштової служби для будь-яких повідомлень: електронної пошти, факсів і голосу, з можливістю трансформації виду представлення інформації.

Різноманітність послуг, їх налаштування відповідно до потреб конкретного користувача, простота програмування нової пропозиції, легкість інтеграції голосових послуг із послугами маніпулювання даними є перевагами IP-телефонії. Частину цих послуг, що описані стандартами SIP та H.245 як додаткові, може надавати безпосередньо програмний комутатор, а складніші сервіси реалізуються за допомогою серверів додатків вузла IP- телефонії.

## Інтеграція систем адресації E.164 і DNS на основі ENUM

Однією з проблем сучасної IP-телефонії є неможливість встановлення з'єднання, коли абонент, що ініціював дзвінок, використовує звичайний телефонний апарат, під'єднаний до традиційної телефонної мережі, а абонент, що викликається – комп'ютер або IP-телефон, з'єднаний з Інтернет або приватною IP- мережею. Складність подібного з'єднання пов'язана із застосуванням в загальнодоступних телефонних мережах і Інтернеті різних схем адресації – системи телефонних номерів на основі стандарту E.164 і системи імен DNS.

Для подолання цієї проблеми робочою групою IETF запропоновано метод трансляції однієї схеми адресації в іншу – **ENUM** (E.164 NUmbering Mapping – відображення адресів стандарту E.164), який описаний у RFC 2916.

Підхід ENUM полягає в призначенні всім абонентам IP-телефонії, що під'єднані до Інтернету або приватної IP-мережі, ідентифікаторів ще одного типу – телефонних номерів за стандартом E.164. Однак, на кінцевих вузлах і

навіть мережах, у яких виклик термінується, ці телефонні номери не використовуються – вони потрібні лише для ідентифікації абонента, що викликається стороною-ініціатором, що застосовує звичайний телефон, і маршрутизації виклику в межах традиційної телефонної мережі. Потім телефонні номери перетворюються в імена Інтернет за допомогою системи доменних імен (DNS).

# СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ


1. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ № 1/11-8052 від 28.05.12р.) – Львів, «Магнолія 2006», 2013. – 256 с.
2. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ № 1/11-11650 від 16.07.12р.) – Львів, «Магнолія 2006», 2014. – 312 с.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологи, протоколы: Ученик для вузов. 5-е узд.– СПб.: Питер, 2016. – 992 с.
4. Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. – СПб.: Питер, 2012. – 960 с.
5. Жуков І.А., Дрововозов В.І., Махновський Б.Г.Експлуатація комп'ютерних систем та мереж. – К.: НАУ , 2007.-361с.
6. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мереж: Підручник для вищих навчальних закладів. – К.: САММІТ-КНИГА, 2010. – 640 с.
7. Антонов, В.М. Сучасні комп'ютерні мережі. – К. : МК-Прес, 2005. – 478 с.
8. В.П. Бабак, О.Г. Корченко. Інформаційна безпека та сучасні мережеві технології. – К. : НАУ, 2003. – 670 с.
9. Буров Є.В. Комп'ютерні мережі: підручник.– Львів: Магнолія 2006, 2010. – 262 с.
10. Мельник І.В. За ред. Л.С. Глоби. Інформаційні комп'ютерні мережі: Навч. посіб. для дистанційного навч. – К.: Ун- т "Україна", 2006. – 250с.
11. Ю.С. Рамський, В.П. Олексюк, А.В. Балик. Адміністрування комп'ютерних мереж і систем: навчальний посібник.– Тернопіль: Навч. кн. – Богдан, 2010. – 196 с.
12. Токарев В.Л. Вычислительные системы, сети и телекоммуникации. – М.: Промпилот, 2010. – 477 с.
13. В. Олексюк, Н. Балик, А. Балик. Організація комп'ютерної локальної мережі. – К.: Підручники та посібники, 2006. – 80 с.
14. Кулябов Д.С., Королькова А.В.. Архитектура и принципы построения современных сетей и систем телекоммуникаций. – М.: РУДН, 2008. – 281 с.
15. Брейман А.Д. Сети ЭВМ и телекоммуникации. Глобальные сети. – М.: МГУПИ, 2006. – 117 с.
16. Пескова С.А., Кузин А.В., Волков А.Н.. Сети и телекоммуникации (3-е изд.) – М.: Академия, 2008. – 354 с.
17. Росляков А.В.. Сети доступа. – М.: Горячая Линия-Телеком, 2008. – 96 с.
18. Шиндер Д.Л. Основы компьютерных сетей. – М.: Вильямс, 2002. – 615с.

19. Пролетарский А.В., Баскаков И.В., Федотов Р.А. и др. Организация беспроводных сетей. – Москва, 2006. – 181 с.

20. Родичев Ю.А. Коммутаторы Компьютерные сети – архитектура, технологии, защита. – М.: Универс-групп, 2006. – 468 с.

21. А. Ватаманюк. Создание и обслуживание локальных сетей. – Питер, 2008.

22. Петраков А.М., Клейменов С.А., Мельников В.П. Администрирование в информационных системах. – М.: ИЦ Академия, 2008.

23. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей – М.: Горячая линия – Телеком, 2008.

24. Камнев В.Е., Черкасов В.В., Чечин Г.В. Спутниковые сети связи – М.: Альпина Паблишер, 2004. – 536 с.

25. Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / За ред. С.О. Довгого. – К.: Український Видавничій Центр, 2002. – 520 с.

26. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. Вид. Львів: Бак, 2003. – 584 с.

27. Крук Б.И, Попантонопуло В.Н., Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2003. – 647 с.

28. Катунин Г.П., Мамчев Г.В., Попантонопуло Б.И, Шувалов В.П. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 2 – Радиосвязь, радиовещание, телевидение; под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2004. – 672 с.

29. Величко В.В., Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 3 – Мультисервисные сети / под ред. проф. В.П. Шувалова. – Изд. 3-е, испр. и доп. – М.: Горячая линия-Телеком, 2005. – 592 с.

30. Рослякв А.В., Ваняшин С.В., Самсонов М.Ю. и др. Сети следующего поколения NGN / Под ред. А.В. Рослякова. – М.: Эко-Трендз, 2008. – 424 с.

31. Величко В.В., Катунин Г.П., Шувалов В.П. Основы инфокоммуникационных технологий. Учебное пособие для вузов / Под ред. В.П. Шувалова. – М.: Горячая линия – Телеком, 2009. – 712 с.

32. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. – СПб.: БХВ-Санкт-Петербург, 2010.

33. Захватов М.. Построение виртуальных частных сетей (VPN) на базе технологий MPLS. – М., 2004. – 52 с.

34. Андрончик А.Н. и др. Защита информации в компьютерных сетях. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.

## ДЛЯ НОТАТОК

## ДЛЯ НОТАТОК

## ДЛЯ НОТАТОК

## ДЛЯ НОТАТОК

Навчально-методична література

**Микитишин А.Г., Митник М.М., Стухляк П.Д.**

## Навчальний посібник

# «Телекомунікаційні системи та мережі»

Для студентів спеціальності 151
«Автоматизація та комп’ютерно-інтегровані технології»

Комп’ютерне макетування та верстка *А.П. Катрич*

Формат 60х90/16. Обл. вид. арк. 16,73. Тираж 10 прим. Зам. № 2917.

Тернопільський національний технічний університет імені Івана Пулюя.
46001, м. Тернопіль, вул. Руська, 56.
Свідоцтво суб’єкта видавничої справи ДК № 4226 від 08.12.11.