ЗМІСТ

Вступ

В посібнику розглядаються основні поняття та терміни локальних та глобальних мереж, їх класифікація; мережеві протоколи та еталонна модель OSI і дано загальну характеристику протоколів локальних мереж; розглянуті стандарти мереж; описано етапи проектування мереж, структуру IP-адрес; повнокласова та безкласова IP – адресація; мережеві маски; статична і динамічна NAT; IP – данограми.

Дано опис предмета навчальної дисципліни у відповідності до болонського процесу, сформовано мету та завдання курсу дисципліни «**Комп'ютерні мережі**», викладено зміст лекційних тем курсу та перелік навчально-методичної літератури.

Мета і завдання курсу

Мета дисципліни «Комп'ютерні мережі» – придбання знань в області теорії комп'ютерних мереж, а також навичок проектування комп'ютерних мереж і їхнього використання для пошуку, обробки й аналізу даних, необхідних для прийняття ефективних управлінських рішень.

Завдання навчальної дисципліни – ознайомити студентів з основами побудови комп'ютерних мереж, засобами комунікаційної техніки, концепціями побудови локальних і глобальних комп'ютерних мереж. Вивчити сучасні комп'ютерні технології й основні засоби забезпечення їх працездатності. Ознайомитися із програмним забезпеченням мережевих технологій і тенденціями його розвитку на сучасному етапі. Дати практичні навички проектування корпоративної комп'ютерної мережі стосовно до умов конкретного об'єкту.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні засоби комунікаційної техніки, їхні характеристики й класифікацію;
- призначення, особливості функціонування й концепції побудови локальних і глобальних комп'ютерних мереж;
- основні технології локальних комп'ютерних мереж і особливості їхнього застосування;
- основи організації й функціонування глобальних комп'ютерних мереж і послуги, що надаються користувачам такою мережею;
- склад і призначення програмних засобів, що забезпечують ефективну й безперебійну роботу сучасних комп'ютерних технологій.

вміти:

- обирати й обґрунтовувати вибір моделі побудови проектованої комп'ютерної мережі, мережевої архітектури, типу кабельної системи, конфігурації мережевого устаткування, необхідного для забезпечення нормальної роботи мережі;
- проектувати карту-схему й розраховувати вартість установки та експлуатації спроектованої комп'ютерної мережі.

1. Історія виникнення. Основні визначення та терміни.

1.1. Історія комп’ютерних мереж.

Інтернет сьогодні – це глобальна комп'ютерна мережа яка об'єднує тисячі мереж та мільйони комп'ютерів на планеті з метою обміну даними та доступу до спільних інформаційних ресурсів. А почалось усе п'ятдесят років тому. Ідея з'єднати між собою комп'ютери з метою обміну інформацією та спільного використання їхніх ресурсів у США в минулому столітті під час "холодної війни". Радянський Союз 1975 року запустив перший супутник Землі. Це започаткувало технологічні змагання між Сполученими Штатами та СРСР у сфері телекомунікацій. Наступного року в США було створено Агентство перспективних розробок (ARPA) та Національну аерокосмічну адміністрацію (NASA) для розробки ефективних технологій зв'язку.

На той час більшість комп'ютерів були зосереджені у військовому комплексі. Кількість і потужність комп'ютерних систем постійно зростала. Виникала необхідність об'єднати територіально віддалені системи в одну мережу з метою раціонального й узгодженого використання їхніх спільних ресурсів. Зробити це треба було так, щоб у разі воєнних конфліктів чи природних катастроф вихід з ладу частини мережі не впливав на її функціонування в цілому.

У 1969 році вперше об'єднали комп'ютери, які були у дослідницькому центрі Стенфордського університету та у Каліфорнійському університеті в Лос-Анджелесі. Це стало початком створення мережі, яка одержала назву Arpanet.

Мережа швидко розвивалась і поступово вийшла за рамки суто військового проекту. У 1974 році була відкрита перша комерційна версія Arpanet – мережа Telnet. У 1976 році Роберт Меткалф створив локальну комп'ютерну мережу. У 1977 році число під'єднаних комп'ютерів досягло сотні.

Комп'ютерна мережа (обчислювальна мережа, мережа передачі даних) – система зв'язку комп'ютерів і/або комп'ютерного устаткування. Для передачі інформації можуть бути використані різні фізичні явища, як правило різні види електричних, світлових сигналів або електромагнітного випромінювання.

Розрізняють мережі : **комунікаційна мережа і інформаційна мережа**.

Комунікаційна мережа призначена для передачі даних, також вона виконує завдання, пов'язані з перетворенням даних. Комунікаційні мережі розрізняються за типом використовуваних фізичних засобів з'єднання.

Інформаційна мережа призначена для зберігання інформації і складається з інформаційних систем. На базі комунікаційної мережі може бути побудована група інформаційних мереж.

Телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту,

зображень та звуків або повідомлень будь-якого роду по радіо, провідних, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Під каналом зв'язку слід розуміти шлях або засіб, по якому передаються сигнали.

Канали зв'язку (data link) створюються по лініях зв'язку за допомогою мережевого устаткування і фізичних засобів зв'язку. Фізичні засоби зв'язку побудовані на основі витих пар, коаксіальних кабелів, оптичних каналів або ефіру. Між взаємодіючими інформаційними системами через фізичні канали комунікаційної мережі і вузли комутації встановлюються логічні канали.

Логічний канал - це шлях для передачі даних від однієї системи до іншої. Логічний канал прокладається по маршруту в одному або декількох фізичних каналах. Логічний канал можна охарактеризувати, як маршрут, прокладений через фізичні канали і вузли комутації.

Топологія – це опис фізичних з'єднань в мережі, що вказує які робочі станції можуть зв'язуватися між собою. Тип топології визначає продуктивність, працездатність і надійність експлуатації робочих станцій, а також час звернення до файлового сервера. Залежно від топології мережі використовується той або інший метод доступу.

Склад основних елементів в мережі залежить від її архітектури.

Архітектура – це концепція, що визначає взаємозв'язок, структуру і функції взаємодії робочих станцій в мережі. Вона передбачає логічну, функціональну і фізичну організацію технічних і програмних засобів мережі. Архітектура визначає принципи побудови і функціонування апаратного і програмного забезпечення елементів мережі.

У 1960-х та 1970-х роках багато різних мереж вживало власні протоколи і їх впровадження. Спільне використання інформації через ці мережі становило проблему, тому виникла потреба опрацювання спільного протоколу. При опрацювання такого спільного протоколу і системи протоколів ARPANET була впроваджена фундаментальна концепція розшарування. З використанням TCP/IP була створена мережа, яка головним чином використовувалася для потреб урядових організацій та науково-дослідних інститутів і дозволяла спільне використання інформації та співпрацю при дослідженнях.

1.2. Визначення локальної мережі.

Частіше всього термін "локальні мережі" або "локальні обчислювальні мережі" (LAN, Local Area Network) розуміють буквально, тобто це такі мережі, які мають невеликі, локальні розміри, з’єднують розташовані комп'ютери. Проте достатньо подивитися на характеристики деяких сучасних локальних мереж, щоб зрозуміти, що таке визначення не точне. Наприклад, деякі локальні мережі легко забезпечують зв'язок на відстані декількох десятків кілометрів. Це вже розміри не кімнати, не будівлі, не близько розташованих будівель, а, можливо, навіть цілого міста. З другого боку, по глобальній мережі (WAN, Wide Area Network або GAN, Global Area Network)

цілком можуть зв'язуватися комп'ютери, що знаходяться на сусідніх столах в одній кімнаті, але її чомусь ніхто не називає локальною мережею.

Найбільш точно б визначити як локальну таку мережу, яка дозволяє користувачам не помічати зв'язку. Локальна мережа повинна забезпечувати прозорий зв'язок. По суті, комп'ютери, зв'язані локальною мережею, об'єднуються в один віртуальний комп'ютер, ресурси якого можуть бути доступні всім користувачам, причому цей доступ не менше зручний, ніж до ресурсів, що входять безпосередньо в кожний окремий комп'ютер. Під зручністю в даному випадку розуміється висока реальна швидкість доступу, швидкість обміну інформацією між додатками, практично непомітна для користувача. При такому визначенні стає зрозуміло, що ні повільні глобальні мережі, ні повільний зв'язок через послідовний або паралельний порти не потрапляють під поняття локальної мережі.

Швидкість передачі по локальній мережі обов'язково повинна рости у міру зростання швидкодії найпоширеніших комп'ютерів. Саме це і спостерігається: якщо ще десять років тому цілком прийнятної вважалася швидкість обміну в 10 Мбіт/с, то зараз вже середньошвидкісною вважається мережа, що має пропускну спроможність 100 Мбіт/с, також активно використовуються засоби для швидкості 1000 Мбіт/с і навіть більше.

Таким чином, головна відмінність локальної мережі від будь-кого інший — висока швидкість передачі інформації по мережі. Не менше важливі і інші чинники.

Зокрема, принципово необхідний низький рівень помилок передачі, викликаних як внутрішніми, так і зовнішніми чинниками. Адже навіть дуже швидко передана інформація, яка спотворена помилками, просто не має сенсу, її доведеться передавати ще раз. Тому локальні мережі обов'язково використовують високоякісні і добре захищені від перешкод лінії зв'язку, що спеціально прокладаються.

Особливе значення має і така характеристика мережі, як можливість роботи з великими навантаженнями, тобто з високою інтенсивністю обміну (з великим трафіком). Адже якщо механізм управління обміном, що використовується в мережі, не дуже ефективний, то комп'ютери можуть довго чекати своєї черги на передачу.

Механізм управління обміном може гарантований успішно працювати тільки у тому випадку, коли наперед відомо, скільки комп'ютерів допустимо підключити до мережі. Інакше завжди можна включити стільки абонентів, що унаслідок перевантаження забуксує будь-який механізм управління. Нарешті, мережею можна назвати тільки таку систему передачі даних, яка дозволяє об'єднувати до декількох десятків комп'ютерів, але ніяк не два, як у разі зв'язку через стандартні порти.

Таким чином, сформулювати відмітні ознаки локальної мережі можна таким чином:

- Висока швидкість передачі інформації, велика пропускна спроможність мережі. Прийнятна швидкість зараз — не менше 10 Мбіт/с.

- Низький рівень помилок передачі. Допустима вірогідність помилок передачі даних повинна бути порядку 10^{-8} — 10^{-12}.
- Ефективний механізм управління обміном по мережі.
- Наперед чітко обмежена кількість комп'ютерів, що підключаються до мережі.

При такому визначенні зрозуміло, що глобальні мережі відрізняються від локальних перш за все тим, що вони розраховані на необмежене число абонентів. Крім того, вони використовують (або можуть використовувати) не дуже якісні канали зв'язку і порівняльно низьку швидкість передачі. А механізм управління обміном в них не може бути гарантований швидким. В глобальних мережах набагато важливий не якість зв'язку, а сам факт її існування.

Часто виділяють ще один клас комп'ютерних мереж — міські, регіональні мережі (MAN, Metropolitan Area Network), які звичайно по своїх характеристиках ближче до глобальних мереж, хоча іноді все-таки мають деякі риси локальних мереж, наприклад, високоякісні канали зв'язку і порівняльно високі швидкості передачі. У принципі міська мережа може бути локальною зі всіма її перевагами.

По локальній мережі може передаватися сама різна цифрова інформація: дані, зображення, телефонні розмови, електронні листи і т.д. Частіше за все локальні мережі використовуються для розділення таких ресурсів, як дисковий простір, принтери і вихід в глобальну мережу. Повноцінними абонентами (вузлами) мережі можуть бути не тільки комп'ютери, але і інші пристрої. Локальні мережі дають також можливість організувати систему паралельних обчислень на всіх комп'ютерах мережі, що багато разів прискорює рішення складних математичних задач. З їх допомогою можна управляти роботою технологічної системи або дослідницької установки з декількох ПК одночасно.

Проте мережі мають і досить істотні недоліки:

- мережа вимагає додаткових, іноді значних матеріальних витрат на покупку мережного устаткування, програмного забезпечення, на прокладку сполучних кабелів і навчання персоналу;
- мережа вимагає прийому на роботу фахівця (адміністратора мережі), який займатиметься контролем роботи мережі, її модернізацією та інше;
- мережа обмежує можливості переміщення ПК, підключених до неї;
- мережі є середовищем для розповсюдження комп'ютерних вірусів, тому питанням захисту від них доведеться надавати набагато більше увагу, ніж у разі автономного використовування комп'ютерів;
- мережа різко підвищує небезпеку несанкціонованого доступу до інформації з метою її крадіжки або знищення. Інформаційний

захист вимагає проведення цілого комплексу технічних і організаційних заходів.

Ніщо не дається дарма. І треба добре подумати, чи варто підключати до мережі всі комп'ютери компанії, або частина з них краще залишити автономними. Можливо, що мережа взагалі не потрібна, оскільки породить набагато більше проблем, чим дозволить вирішити.

1.3. Основні терміни.

Тут же слід згадати про такі найважливіші поняття теорії мереж, як абонент, сервер, клієнт.

Абонент (вузол, хост, станція) — цей пристрій, підключений до мережі і активно що бере участь в інформаційному обміні. Частіше за все абонентом (вузлом) мережі є комп'ютер, але абонентом також може бути, наприклад, мережний принтер або інший периферійний пристрій, що має нагоду напряму підключатися до мережі. Далі в тексті книги замість терміну "абонент" для простоти використовуватиметься термін "комп'ютер".

Сервером називається абонент мережі, який надає свої ресурси іншим абонентам, але сам не використовує їх ресурси. Таким чином, він обслуговує мережу. Серверів в мережі може бути дещо, і зовсім не обов'язкове, що сервер — наймогутніший комп'ютер. Виділений сервер — сервер, що займається тільки мережними задачами. Невиділений сервер може крім обслуговування мережі виконувати і інші задачі.

Клієнтом називається абонент мережі, який тільки використовує мережні ресурси, але сам свої ресурси в мережу не віддає, тобто мережа його обслуговує, а він нею тільки користується. Комп'ютер-клієнт також часто називають робочою станцією. У принципі кожний комп'ютер може бути одночасне як клієнтом, так і сервером.

Під сервером і клієнтом часто розуміють також не самі комп'ютери, а працюючі на них програмні додатки. В цьому випадку той додаток, який тільки віддає ресурс в мережу, є сервером, а то додаток, який тільки користується мережними ресурсами — клієнтом.

2. Класифікація мереж.

Для класифікації комп'ютерних мереж використовуються різні ознаки, вибір яких полягає в тому, щоб виділити з існуючого різноманіття такі, які дозволили б забезпечити цій класифікаційній схемі певні обов'язкові якості. В основному комп'ютерні мережі класифікують за ознаками структурної і функціональної організації.

2.1. Класифікація за географічним розташуванням:

- Локальна мережа (Local Area Network – LAN) – звичайно розташована у межах будинку.
- Глобальна мережа (Wide Area Network – WAN) – охоплює географічний регіон (країну або континент).

- Метропольна мережа (Metropolitain Area Network – MAN) – застосовується для об’єднання мереж в місті в одну велику мережу.
- Internet – індивідуальні комп’ютери під’єднані до інших мереж у світі через публічну мережу(мережу загального користування).
- Intranet – індивідуальні комп’ютери під’єднані до інших мереж через приватну мережу.
- Віртуальна приватна мережа (Virtual Private Network – VPN) – індивідуальні комп’ютери під’єднані до інших мереж через сегмент публічної мережі.

2.2. Класифікація локальних мереж за топологією.

Під топологією комп'ютерної мережі звичайно розуміється конфігураці, що фізично розташовує комп'ютери мережі один щодо одного і спосіб з'єднання їх лініями зв'язку.

Топологія визначає вимоги до устаткування, тип кабелю, що використовується, допустимі і найзручніші методи управління обміном, надійність роботи, можливості розширення мережі.

Існує три базові топології мережі:

Шина (bus) — всі комп'ютери паралельно підключаються до однієї лінії зв'язку. Інформація від кожного комп'ютера одночасно передається всій решті комп'ютерів (рис. 2.1).

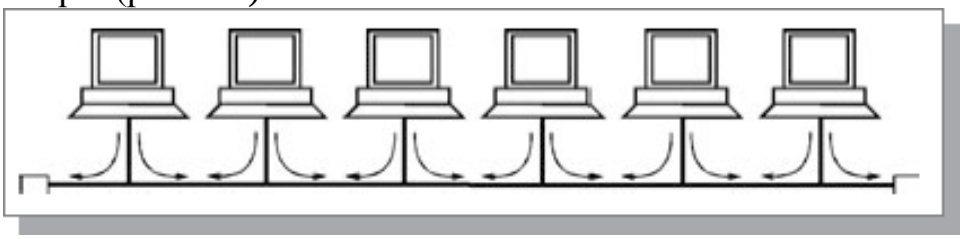


Рис. 2.1. Мережева топологія «Шина».

Зірка (star) — до одного центрального комп'ютера приєднується решта периферійних комп'ютерів, причому кожний з них використовує окрему лінію зв'язку (рис. 2.2). Інформація від периферійного комп'ютера передається тільки центральному комп'ютеру, від центрального — одному або декільком периферійним.

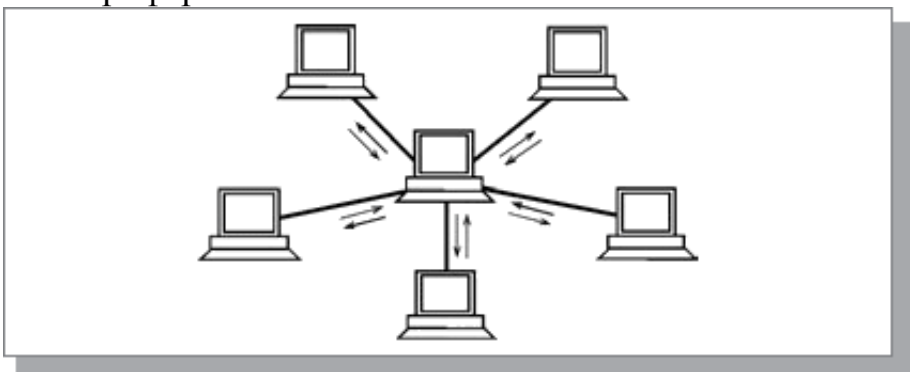


Рис. 2.2. Мережева топологія «Зірка».

Кільце (ring) — комп'ютери послідовно з'єднані в кільце. Передача інформації в кільці завжди проводиться тільки в одному напрямі. Кожний з комп'ютерів передає інформацію тільки одному комп'ютеру, наступному в ланцюжку за ним, а одержує інформацію тільки від попереднього (рис. 2.3).

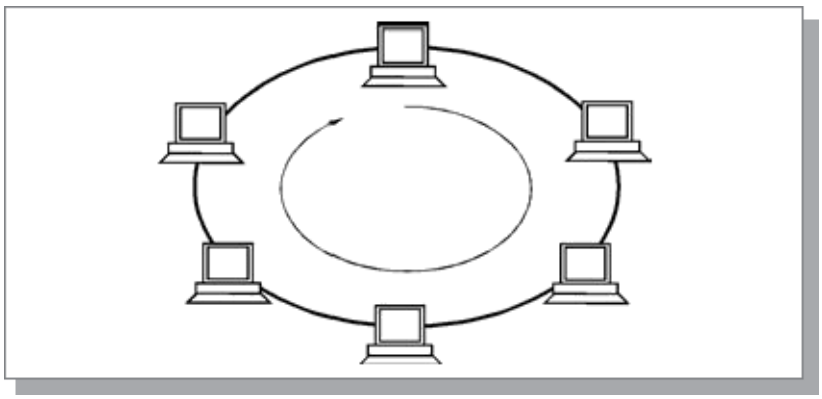


Рис. 2.3. Мережева топологія «Кільце».

На практиці нерідко використовують і інші топології локальних мереж, проте більшість мереж орієнтована саме на три базові топології.

Чинники, що впливають на фізичну працездатність мережі і безпосередньо пов'язані з поняттям топологія:

- Справність комп'ютерів (абонентів), підключених до мережі. В деяких випадках вихід з ладу абонента може заблокувати роботу всієї мережі.
- Справність мережного устаткування, тобто технічних засобів, безпосередньо підключених до мережі (адаптери, трансівери, роз'єми та інші.).
- Цілісність кабелю мережі. При обриві кабелю мережі може порушитися обмін інформацією у всій мережі або в одній з її частин. Для електричних кабелів таке ж критичне коротке замикання в кабелі.
- Обмеження довжини кабелю, пов'язане із загасанням сигналу, що розповсюджується по ньому. Як відомо, в будь-якому середовищі при розповсюдженні сигнал затухає. І чим більшу відстань проходить сигнал, тим більше він затухає (Рис. 2.4).

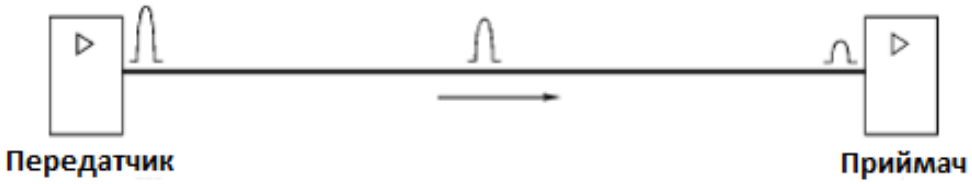


Рис. 2.4. Загасання сигналу при розповсюдженні по мережі.

Окрім трьох розглянутих базових топологій нерідко застосовується також мережева топологія «дерево» (tree), яку можна розглядати як комбінацію декількох зірок. Причому, як і у разі зірки, дерево може бути активним або істинним (рис. 2.5) і пасивним (рис. 2.6). При активному дереві в центрах об'єднання декількох ліній зв'язку знаходяться центральні комп'ютери, а при пасивному — концентратори (хаби).

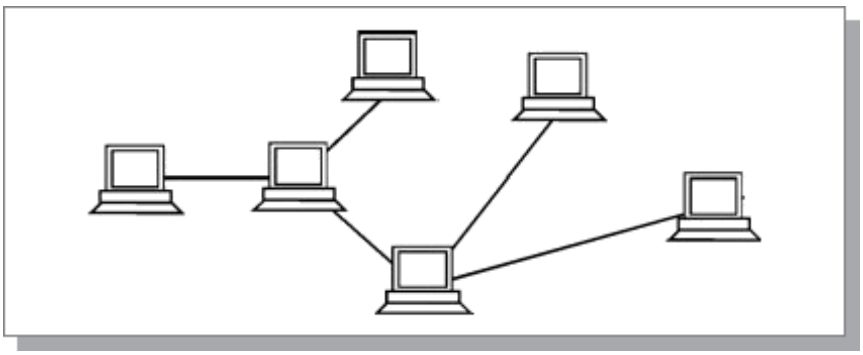


Рис. 2.5. Топологія «Активне дерево».

Існують й інші топології, які поєднують у собі основні види топологій. Їх прийнято називати гібридними.

Необхідно відзначити, що топологія все-таки не є основним чинником при виборі типу мережі. Набагато важливий, наприклад, рівень стандартизації мережі, швидкість обміну, кількість абонентів, вартість устаткування, вибране програмне забезпечення. Але, з другого боку, деякі мережі дозволяють використовувати різні топології на різних рівнях. Цей вибір вже цілком лягає на користувача, який повинен враховувати всі перераховані в даному розділі міркування.

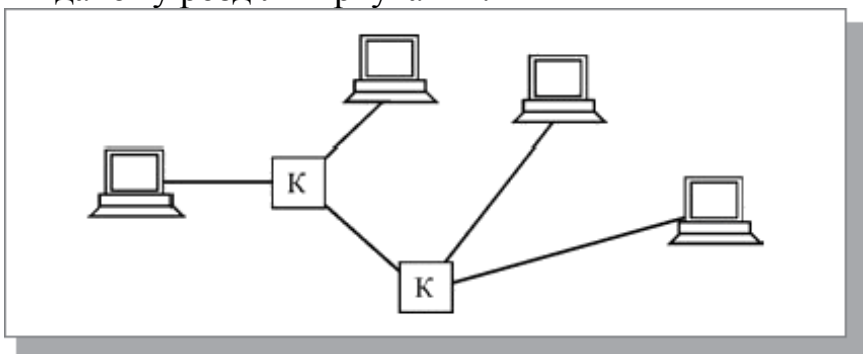


Рис. 2.6. Топологія «Пасивне дерево». К — концентратори.

2.3. Класифікація за типом функціональної взаємодії.

Архітектура термінал - головний комп'ютер – це концепція інформаційної мережі, в якій уся обробка даних здійснюється одним або групою головних комп'ютерів.

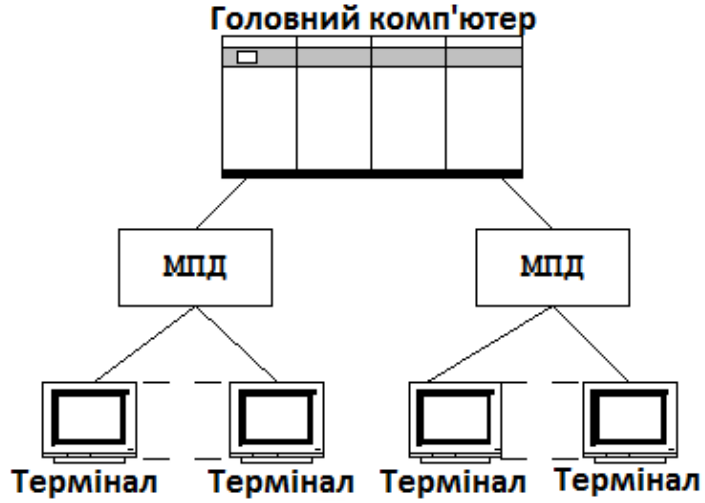


Рис. 2.6. Архітектура термінал - головний комп'ютер.

Дана архітектура припускає два типи устаткування:

- Головний комп'ютер, де здійснюється управління мережею, зберігання і обробка даних.
- Термінали, призначені для передачі головному комп'ютеру команд на організацію сеансів і виконання завдань, введення даних для виконання завдань і отримання результатів.

Головний комп'ютер через мультиплексори передачі даних (мультиплексор передачі даних (МПД) – пристрій, який один фізичний канал представляє у вигляді декількох незалежних один від одного логічних каналів) взаємодіють з терміналами, як представлено на мал. 1.

Одноранговa архітектура (peer - to - peer architecture) – це концепція інформаційної мережі, в якій її ресурси розосереджені по усіх системах. Ця архітектура характеризується тим, що в ній усі системи рівноправні.

До одноранговых мереж відносяться малі мережі, де будь-яка робоча станція може виконувати одночасно функції файлового сервера і робочої станції. У одноранговых локальних мережах дисковий простір і файли на будь-якому комп'ютері можуть бути загальними.

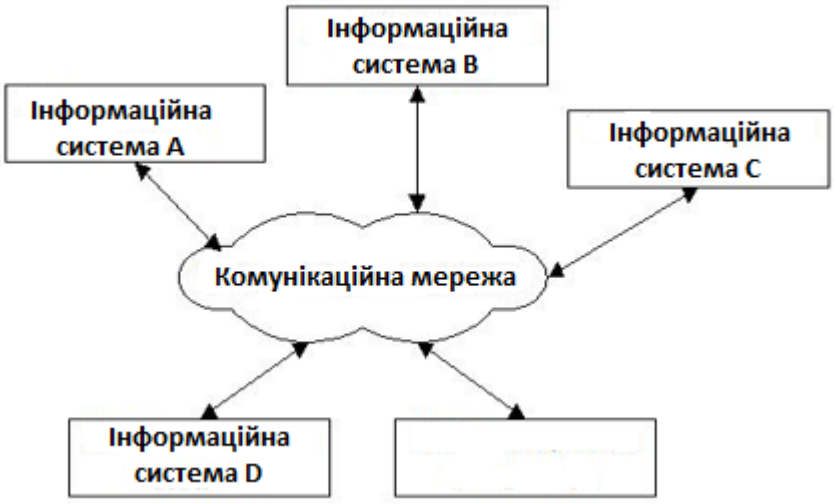


Рис. 2.7. Одноранговa архітектура.

Однорангові мережі мають наступні переваги:

- вони легкі в установці і налаштуванні;
- окремі ПК не залежать від виділеного сервера;
- користувачі в змозі контролювати свої ресурси;
- мала вартість і легка експлуатація;
- мінімум устаткування і програмного забезпечення;
- немає необхідності в адміністраторові;
- добре підходять для мереж з кількістю користувачів, що не перевищує десяти.

Проблемою одноранговой архітектури є ситуація, коли комп'ютери відключаються від мережі. У цих випадках з мережі зникають види сервісу, які вони надавали. Мережеву безпеку одночасно можна застосувати тільки до одного ресурсу, і користувач повинен пам'ятати стільки паролів, скільки мережевих ресурсів. При діставанні доступу до ресурсу, що розділяється,

відчувається падіння продуктивності комп'ютера. Істотним недоліком одноранговых мереж є відсутність централізованого адміністрування.

Використання одноранговой архітектури не виключає застосування в тій же мережі також архітектура "термінал - головний комп'ютер" або архітектура "клієнт - сервер".

Архітектура клієнт - сервер (client - server architecture) – це концепція інформаційної мережі, в якій основна частина її ресурсів зосереджена в серверах, обслуговуючих своїх клієнтів (рис. 2.7). Дана архітектура визначає два типи компонентів : сервери і клієнти.

Сервер – це об'єкт, що надає сервіс іншим об'єктам мережі по їх запитах. Сервіс – це процес обслуговування клієнтів.

Сервер працює по завданнях клієнтів і управляє виконанням їх завдань. Після виконання кожного завдання сервер посилає отримані результати клієнтові, що послав це завдання.

Рис. 2.7. Архітектура клієнт – сервер.

Сервісна функція в архітектурі клієнт - сервер описується комплексом прикладних програм, відповідно до якого виконуються різноманітні прикладні процеси.

Процес, який викликає сервісну функцію за допомогою певних операцій, називається клієнтом. Їм може бути програма або користувач. На рис. 2.8 наведено перелік сервісів, які можуть бути присутніми в архітектурі клієнт-сервер. Клієнтами можуть бути робочі станції, які використовують ресурси сервера і надають зручні інтерфейси користувача. Інтерфейси користувача це процедури взаємодії користувача з системою або мережею.

Клієнт є ініціатором і використовує електронну пошту або інші сервіси сервера. У цьому процесі клієнт запрошує вид обслуговування, встановлює сеанс, отримує потрібні йому результати і повідомляє про закінчення роботи.

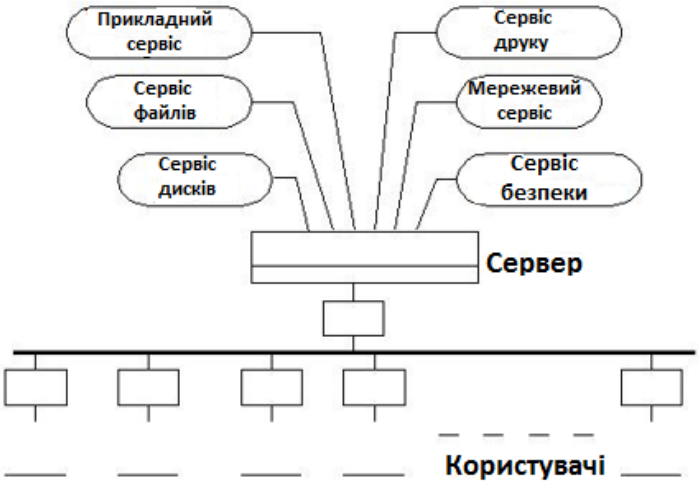


Рис. 2.8. Модель клієнт-сервер.

У мережах з виділеним файловим сервером на виділеному комп'ютері встановлюється серверна мережева операційна система. Цей ПК стає сервером. Програмне забезпечення (ПО), встановлене на робочій станції, дозволяє їй обмінюватися даними з сервером. Приклад мережевих операційних систем : операційні системи сімейства Windows Server.

У сучасній клієнт-серверній архітектурі виділяється чотири групи об'єктів : клієнти, сервери, ці і мережеві служби. Клієнти розташовуються в системах на робочих місцях користувачів. Дані в основному зберігаються в серверах. Мережеві служби є спільно використовуваними серверами і даними. Крім того служби управляють процедурами обробки даних.

У міру ускладнення функцій, що покладаються на сервери, і збільшення числа обслуговуваних ними клієнтів відбувається все більша спеціалізація серверів. Існує безліч типів серверів.

- Первинний контролер домена, сервер, на якому зберігається база бюджетів користувачів і підтримується політика захисту.
- Вторинний контролер домена, сервер, на якому зберігається резервна копія бази бюджетів користувачів і політики захисту.
- Універсальний сервер, призначений для виконання нескладного набору різних завдань обробки даних в локальній мережі.
- Сервер бази даних, що виконує обробку запитів, що направляються базі даних.
- Proxy сервер, що підключає локальну мережу до мережі Internet.
- Web - сервер, призначений для роботи з web - інформацією.
- Файловий сервер, що забезпечує функціонування розподілених ресурсів, включаючи файли, програмне забезпечення.
- інші.

Мережі клієнт - серверної архітектури мають наступні переваги:

- дозволяють організовувати мережі з великою кількістю робочих станцій;
- забезпечують централізоване управління обліковими записами користувачів, безпекою і доступом, що спрощує мережеве адміністрування;

- ефективний доступ до мережевих ресурсів;
- користувачеві потрібний один пароль для входу в мережу і для діставання доступу до усіх ресурсів, на які поширюються права користувача.

Недоліки:

- несправність сервера може зробити мережу непрацездатною, як мінімум втрату мережевих ресурсів;
- вимагають кваліфікованого персоналу для адміністрування;
- мають вищу вартість мереж і мережевого устаткування.
- Вибір архітектури мережі залежить від призначення мережі, кількості робочих станцій і від виконуваних на ній дій.
- Слід вибрати одноранговy мережу, якщо:
- кількість користувачів не перевищує десяти;
- усі машини знаходяться близько один від одного;
- мають місце невеликі фінансові можливості;
- немає необхідності в спеціалізованому сервері;
- немає можливості або необхідності в централізованому адмініструванні.

Слід вибрати клієнт серверну мережу, якщо:

- кількість користувачів перевищує десяти;
- вимагається централізоване управління, безпека, управління ресурсами або резервне копіювання;
- потрібний спеціалізований сервер;
- потрібний доступ до глобальної мережі;
- вимагається розділяти ресурси на рівні користувачів.

3. Середовища передавання даних.

3.1. Структура ланки передавання даних.

Канали зв’язку у мережах складаються з ланок передавання даних, які за сучасного рівня розвитку технічних засобів мають наступну структуру (рис. 3.1):

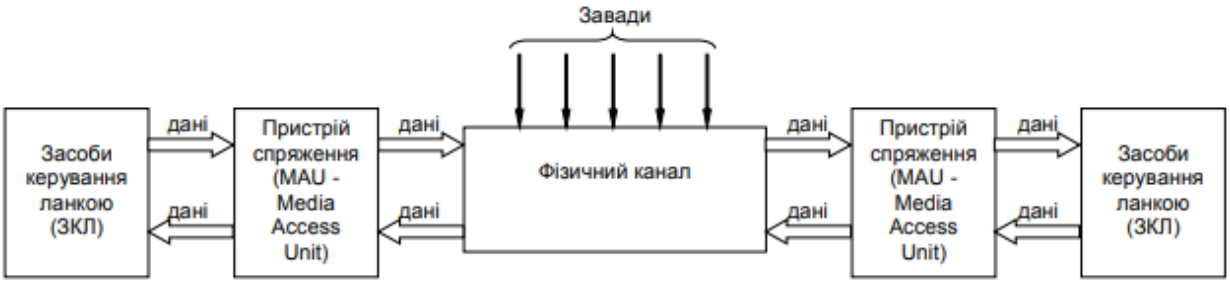


Рис. 3.1. Структура ланки передавання даних.

Призначення кожного елементу цієї структури повністю описується його назвою.

Дані ланкою можуть передаватись в обох напрямах.

В залежності від послідовності передавання даних в обох напрямах ланки розрізняють такі режими роботи: симплексний (почерговий) (simplex), напівдуплексний (duplex) та дуплексний (одночасний) (full duplex).

Канал зв’язку складається з ланок передавання даних та каналоуворюючого обладнання, причому у кожному сеансі склад ланок в каналі може бути різним в залежності від обраного маршруту зв’язку.

Канал зв’язку у телекомунікації – одно- або двонапрямлений спосіб передавання даних між двома або більше точками зі спільним середовищем.

Кожний канал зв’язку організований за принципом часового (time division) або частотного (frequency division) поділу.

У випадку часового поділу через рівні проміжки часу лінією зв’язку посилається кадр (фрейм), розділений усередині на фіксоване число слотів (за кількістю користувачів). Кожному користувачеві виділяється фіксований слот усередині кожного кадру. Частотний поділ полягає у виділенні кожному користувачеві фіксованої частотної смуги пропускання всередині заданого діапазону частот.

Основним елементом ланки передавання даних є фізичний канал, характеристики і властивості якого залежать від середовища передавання.

Зараз в комп’ютерних мережах використовують наступні середовища передавання: ефір, мідні проводи, оптичні середовища.

Через ефір здійснюється радіозв’язок і лазерний зв’язок. До провідних середовищ відносяться телефонні проводи і кабелі, спеціалізовані кабелі (коаксіальний, "кручена пара", плаский кабель). Оптичні середовища передавання представлені різними типами волоконно-оптичних кабелів.

3.2. Ефірне середовище.

В залежності від частоти несучого сигналу розрізняють наступні види каналів:

- радіоканал. Вартість обладнання - середня. Швидкість передавання від 20 до 150 Кбіт/с. Підлягає впливові усіх видів завад. Відстань зв’язку визначається радіо-досяжністю. Використовується в основному в пересувних об’єктах;
- інфрачервоний канал. Достатньо дешеве обладнання. Швидкість передавання від 2 до 4 Мбіт/с. Нечутливий до електромагнітних завад. Відстань зв’язку визначається прямою оптичною видимістю але не перевищує 3 км. Недоліком є недовговічність апаратури;
- ультрахвильовий канал. Швидкість передавання від 20 до 40 Мбіт/с. Нечутливий до завад. Відстань зв’язку визначається прямою оптичною видимістю і не перевищує 1,5 км;
- мікрохвильовий канал. Обладнання дуже дороге. Швидкість передавання до 20 Гбіт/с. Відстань зв’язку визначається радіо-досяжністю але не перевищує 20 км. Недоліком є недосконаліть апаратури.

3.3. Коаксіальний кабель.

Досить дешеве і поширене в недалекому минулому середовище передавання. Завдяки своїй конструкції (рис. 3.2) має велику механічну міцність. Їх можна прокладати відкрито будівельними конструкціями (стінами, стелями, підлогою) без додаткового механічного захисту.

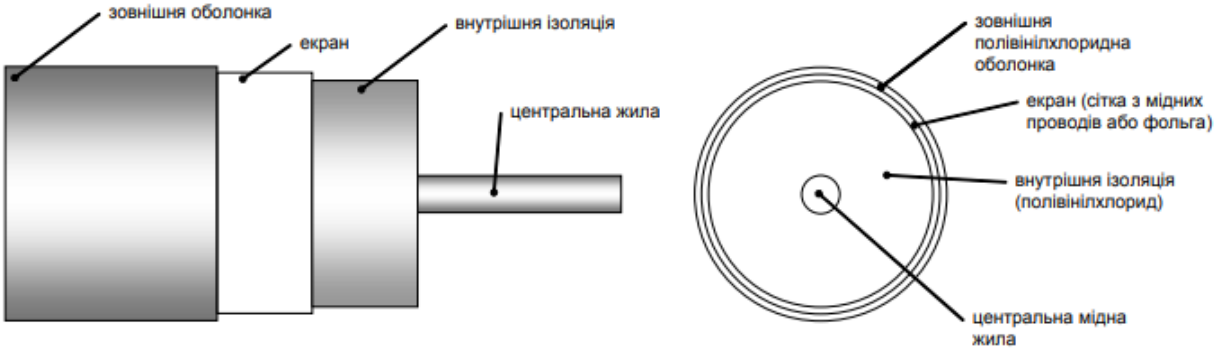


Рис. 3.2. Конструкція коаксіального кабелю.

За електричними характеристиками бувають:

- широкосмугові: швидкість передавання від 300 до 500 Мбіт/с. Загасання сигналу на частоті 100 МГц до 7 дб/100 м. Відстань передавання до 75 м;
- вузькосмугові: швидкість передавання до 50 Мбіт/с. Загасання сигналу на частоті 10 МГц до 4 дб/100 м. Відстань передавання до 50 м.

Коаксіальні кабелі, які використовуються для створення комп'ютерних мереж, мають хвильовий опір 50 Ом (на відміну від телевізійних, які мають хвильовий опір 75 Ом).

В зв'язку з великим загасанням сигналу в них коаксіальні кабелі практично зовсім перестали використовуватись для створення сучасних комп'ютерних мереж, оскільки на великих відстанях (понад 50 м) вимагають додаткового підсилення сигналу. Термін служби коаксіальних кабелів також обмежений і складає 10-12 років.

3.4. Волоконно-оптичний кабель.

За своєю конструкцією і зовнішнім виглядом волоконно-оптичні кабелі подібні до коаксіальних, але на відміну від них не мають екрану. Центральна жила кабелю (або пучок жил) виготовлена з прозорого пластику. Кабель має низьку механічну міцність і повинен прокладатись у спеціальних конструкціях (каналах, лотках, коробах). Світловий потік в такому кабелі створюється або малопотужними лазерами або суперлюмінесцентними світлодіодами.

Волоконно-оптичні кабелі зовсім не чутливі до електромагнітних завад і мають високі характеристики як середовище передавання.

За цими характеристика їх поділяють на:

- одномодові. Мають одну центральну жилу діаметром 10 мкм. Працюють з лазерами, частота хвилі яких становить або 1,3, або 1,55 мкм.
- багатомодові. Мають пучок центральних жил діаметром 50, 62,5, 100 або 140 мкм. Працюють з суперлюмінесцентними світлодіодами з частотою хвилі 1,3 та 0,85 мкм.

Волоконно-оптичні кабелі дозволяють передавати дані зі швидкістю до 1 Гбіт/с на відстань до 110 км.

Недоліком цього типу середовища передавання є поки що висока вартість кабелів та обладнання.

3.5. Кабель "скручена пара".

Кабель "скручена пара" є зараз найпоширенішим середовищем передавання у локальних комп'ютерних мережах завдяки своїй відносно невеликій вартості та високим електричним характеристикам.

Кабель "скручена пара" складається з чотирьох пар мідних ізольованих провідників скручених між собою по довжині. В кожній парі провідники також скручені між собою. Цим досягається незалежність сигналів (навіть малої амплітуди), що передаються кабелем, від впливу зовнішніх електромагнітних завад. Така незалежність дозволяє передавати сигнали без проміжного підсилення на відносно велику відстань (до 2 км) з достатньо великою швидкістю (до 1 Гбіт/с).

В залежності від конструкції кабелі поділяють на:

- неекрановані (UTP – Unshielded Twisted Pair);
- фольговані (FTP – Folded Twisted Pair);
- екрановані (STP – Shielded Twisted Pair).

Механічна міцність кабелю дуже низька із-за необхідності під час монтажу та експлуатації забезпечувати збереження геометрії розташування провідників всередині кабелю. Порушення цієї геометрії призводить до погіршення його електричних характеристик. З цієї причини кабель "кручена пара" повинен прокладатись виключно у спеціальних коробах з дотриманням усіх необхідних технологічних вимог.

3.6. Плаский кабель.

Плаский кабель складається з окремих мідних круглих чи пласких провідників (до 80-ти), розташованих в одній площині у спільній ізоляційній оболонці (рис. 3.3).

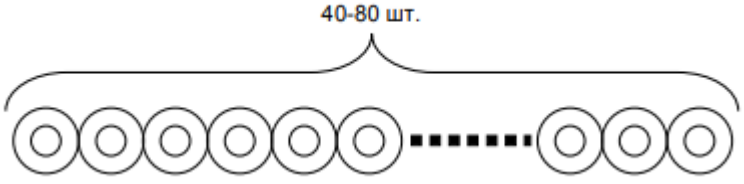


Рис. 3.3. Конструкція плаского кабелю (шлейфу).

В залежності від призначення кабель може мати спільний для всіх провідників екран. Теоретично такий кабель можна використовувати для передачі сигналів на відстань до 15 м, але в практиці такий кабель у вигляді шлейфів довжиною до 40 см використовують всередині процесорного блока чи периферійного пристрою для з'єднання елементів, які монтуються не на материнській платі, з роз'ємами на самій платі, або для рухомих елементів (як, наприклад, друкуючої головки в матричному принтері).

4. Мережеві протоколи та еталонна модель OSI.

4.1. Еталонна модель взаємодії відкритих систем (OSI).

Модель Open System Interconnect (OSI) — еталонна модель взаємодії відкритих систем була прийнята Міжнародною організацією зі стандартизації в 1978 році як перший крок до стандартизації численних протоколів, необхідних для побудови комп'ютерних мереж. Ця модель є ієрархічною структурою, в якій є сім рівнів. Кожен рівень виконує покладені на нього функції, надаючи сервіси верхньому рівню та запитуючи відповідний сервіс у сусіднього нижчого рівня.

На рис. 4.1 зображено два вузли (комп'ютери або процеси). Перший надсилає інформацію, другий її приймає. Відповідно до моделі OSI, кожен рівень вузла, що посилає інформацію, логічно взаємодіє з аналогічним рівнем вузла, що її отримує. Кожному рівню «здається», що він безпосередньо взаємодіє з таким же рівнем іншого комп'ютера. Проте насправді під час передачі інформації через мережу на вузлі-відправнику (комп'ютер 1) інформація послідовно перетворюється на рівнях від 7-го до 1-го. На кожному рівні до основного повідомлення додаються заголовки, які містять додаткову службову інформацію. Нарешті, інформація у вигляді електромагнітних чи оптичних сигналів (на фізичному рівні, рівень 1) відправляється через середовище передачі на вузол, який отримує повідомлення (комп'ютер 2). На ньому інформація знову послідовно перетворюється на рівнях від 1-го до 7-го з використанням відповідної службової інформації.

На кожному рівні виконуються свої функції та відповідне перетворення інформації. Основні функції рівнів моделі OSI наведено в таблиці 4.1.

Правила, за якими здійснюється обробка та перетворення інформації, називаються протоколами. У різних реалізаціях мережі функції протоколів можуть відповідати одному або кільком рівням еталонної моделі OSI. Умовну відповідність рівням моделі OSI найбільш відомих з мережевих протоколів і пристроїв, що працюють на цьому рівні, показано в таблиці 4.2.

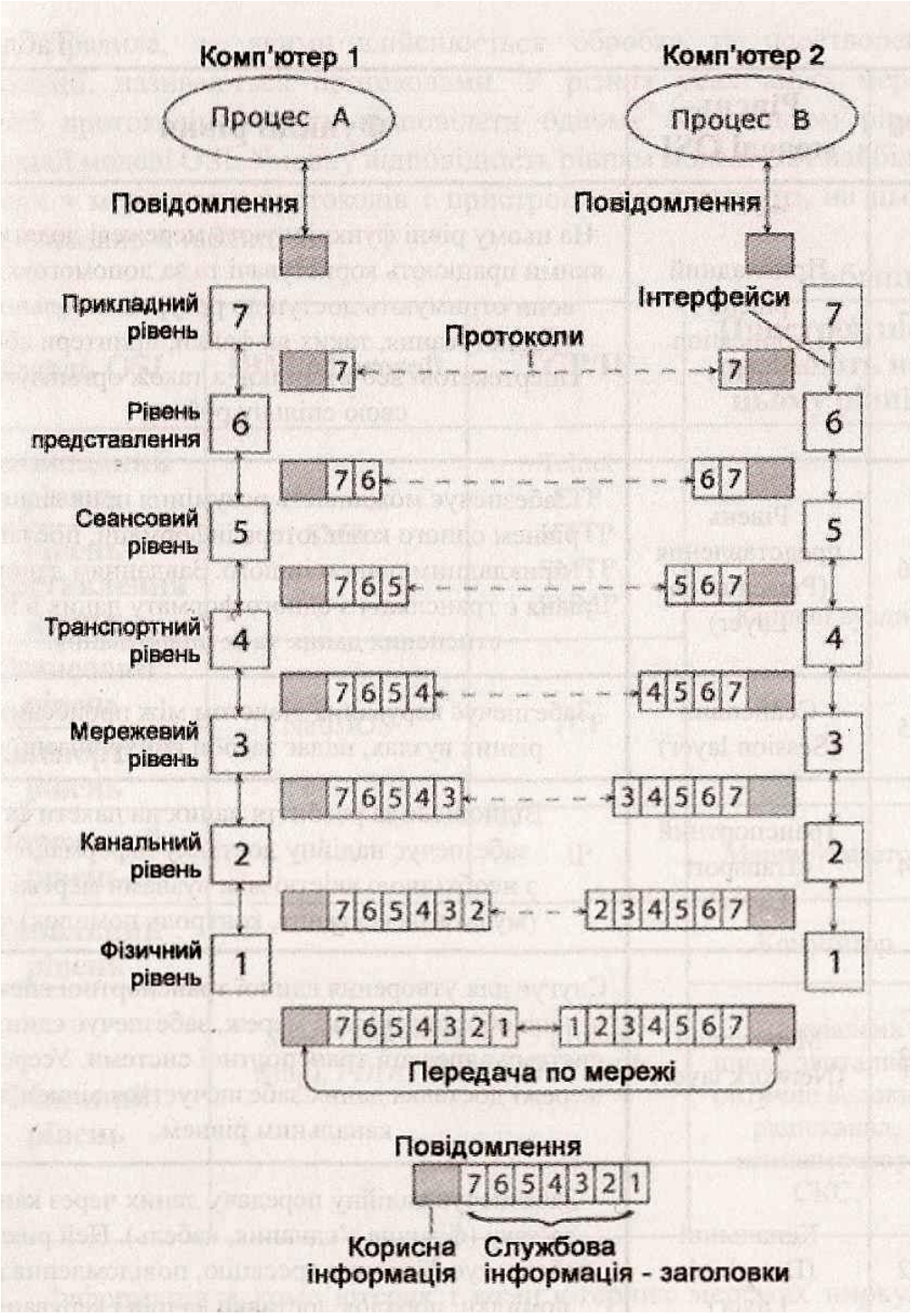


Рис. 4.1. Схема взаємодії мережевих вузлів відповідно до моделі OSI.

Інформація в комп'ютерах і комп'ютерних мережах циркулює певними структурними блоками, які містять крім корисної інформації також і службову.

Службова інформація, що додається до корисної на кожному рівні OSI, необхідна для правильної її обробки. Основну службову інформацію, яка додається на кожному рівні, та назви структурних одиниць інформації наведено в таблиці 4.3. На кожному рівні блоки інформації мають свою назву, але термін пакет часто використовують як узагальнюючу назву цих блоків.

Таблиця 4.1 Основні функції рівнів моделі OSI.

Рівень моделі OSI	**Функції рівня**
Прикладний рівень (Application Layer)	На цьому рівні функціонують мережеві додатки, з якими працюють користувачі та за допомогою яких вони отримують доступ до ресурсів загального користування, таких як файли, принтери або гіпертекстові веб-сторінки, а також організують свою спільну роботу.
Рівень представлення (Presentation Layer)	Забезпечує можливість розуміння прикладним рівнем одного комп'ютера інформації, надісланої прикладним рівнем іншого. Завданням даного рівня є трансляція з одного формату даних в інші, стиснення даних та їх шифрування.
Сеансовий (Session layer)	Забезпечує керування діалогом між процесами на різних вузлах, надає засоби синхронізації.
Транспортний (Transport Layer)	Відповідає за розбиття даних на пакети та забезпечує надійну доставку інформації з необхідною якістю між вузлами мережі (мультиплексування, контроль помилок).
Мережевий (Network layer)	Для утворення єдиної транспортної системи, що об'єднує кілька мереж, забезпечує єдину систему адресації. Усередині мережі доставка даних забезпечується відповідним канальним рівнем.
Канальний (Data-Link Layer)	Забезпечує надійну передачу даних через канал зв'язку (фізичне з'єднання, кабель). Цей рівень забезпечує фізичну адресацію, повідомлення про помилки, порядок доставки кадрів і керування потоком даних.
Фізичний (Physical Layer)	Електричні, механічні, процедурні та функціональні специфікації, що керують фізичним з'єднанням вузлів мережі. Даний рівень визначає тип середовища передачі, топологію, кодування сигналів, методи передачі, форму та тип роз'ємів тощо.

На прикладному рівні створюється корисна інформація (повідомлення), яка на рівні представлення даних кодується в певний формат, файл, документ тощо. У відповідній додатковій службовій інформації вказуються ці коди, формати, протоколи. На сеансовому рівні встановлюється контакт і організовується взаємодія між відправником й одержувачем інформації. Транспортний рівень переважно забезпечує якість передавання інформації. Мережевий рівень забезпечує передавання інформації по мережі, для чого

використовуються IP-адресування, маршрутизація. Канальний рівень забезпечує передавання логічних сигналів по каналам зв'язку, з якими з'єднаний відповідний пристрій. Фізичний рівень – це єдиний рівень, який реально здійснює передавання інформації. На цьому рівні фізичні сигнали переносять інформацію по реальним лініям зв'язку.

Таблиця 4.2. Відповідність мережевих протоколів і пристроїв рівням моделі OSI.

<table>
<tr><th>Модель OSI</th><th>IBM/Microsoft</th><th>TCP/IP</th><th>Пристрої, що працюють на цьому рівні</th></tr>
<tr><td>Прикладний</td><td rowspan="2">SMB</td><td rowspan="2">Telnet, FTP, HTTP, SMTP, SNMP</td><td rowspan="4">Кінцеві вузли</td></tr>
<tr><td>Представлення</td></tr>
<tr><td>Сеансовий</td><td rowspan="3">NetBIOS</td><td rowspan="2">TCP</td></tr>
<tr><td>Транспортний</td></tr>
<tr><td>Мережевий</td><td>IP</td><td>Маршрутизатор</td></tr>
<tr><td>Канальний</td><td colspan="2" rowspan="2">802.3 (Ethernet), 802.5 (Token Ring), FDDI, SLIP, LAP-B, PPP</td><td>Комутатор</td></tr>
<tr><td>Фізичний</td><td>Коаксіальна шина, звита пара, оптоволокно, радіоканал, концентратор</td></tr>
</table>

Модель OSI дотримується принципу прозорості. Кожний нижчий рівень ієрархії моделі OSI є прозорим для вищих рівнів. Це виявляється в тому, що засоби вищих рівнів не помічають наявність нижчих, ніби їх немає зовсім. Приміром, пакети з прикладного або транспортного рівня відправника якимось чином потрапляють на відповідний рівень одержувача. Але як саме це відбувається, які використовуються технології та канали зв'язку, не цікавить засоби вищих рівнів, тобто це є «прозорим» для них.

Аналогічно в мережі «прозорими» є концентратори та комутатори: користувачі їх не помічають, але вони роблять свою справу і забезпечують цю прозорість.

На кожному рівні існують правила, процедури та програми обробки інформації. Правила, що діють на одному рівні процесів, називаються протоколами. Протоколи здійснюють логічну взаємодію між відповідними рівнями процесів, що передають інформацію, та процесів, що її приймають. Сукупність протоколів різних рівнів утворює стек протоколів. Найбільш відомим стек протоколів TCP/IP. Правила та процедури, які відповідають за взаємодію між рівнями називаються інтерфейсами. Наприклад, мережева карта з'єднується з лінією зв'язку через мережевий інтерфейс.

Таблиця 4.3. Основна службова інформація на рівнях OSI.

№	Рівень моделі OSI	Додаткова службова інформація	Структурна одиниця інформації
7	Прикладний	Тип й ім’я прикладної програми, адреса одержувача	Потік даних
6	Представлення	Формат представлення даних, ім’я файлу	Потік, файл
5	Сеансовий	Контрольні точки	Потік
4	Транспортний	Номер пакету, розмір пакету, програмний порт	Дейтаграма
3	Мережевий	IP-адреси відправника й одержувача, контрольна сума	Пакет
2	Канальний	MAC-адреси відправника й одержувача	Кадр
1	Фізичний	-	Сигнал

5. Загальна характеристика протоколів локальних мереж.

При організації взаємодії вузлів у локальних мережах основна роль приділяється протоколу канального рівня. Однак для того, щоб канальний рівень міг справитися з цією задачею, структура локальних мереж повинна бути цілком визначеною, так, наприклад, найпопулярніший протокол канального рівня — Ethernet — розрахований на паралельне підключення усіх вузлів мережі до загальної для них шини — відрізку коаксіального кабелю чи ієрархічної деревоподібної структури сегментів, утворених повторювачами. Протокол Token Ring також розрахований на цілком визначену конфігурацію — з'єднання комп'ютерів у вигляді логічного кільця.

Для спрощення і, відповідно, здешевлення апаратних і програмних рішень розробники перших локальних мереж зупинилися на спільному використанні кабелів усіма комп'ютерами мережі в режимі поділу часу, тобто режимі TDM. Найбільш явним чином режим спільного використання кабелю виявляється в класичних мережах Ethernet, де коаксіальний кабель фізично являє собою неподільний відрізок кабелю, загальний для усіх вузлів мережі. Але й у мережах Token Ring і FDDI, де кожна сусідня пара комп'ютерів з'єднана, здавалося б, своїми індивідуальними відрізками кабелю з концентратором, ці відрізки не можуть використовуватися комп'ютерами, що безпосередньо до них підключені, у довільний момент часу. Ці відрізки утворять логічне кільце, доступ до якого як до єдиного цілого може бути отриманий тільки по цілком визначеному алгоритму, у якому беруть участь усі комп'ютери мережі. Використання кільця як загального поділюваного ресурсу спрощує алгоритми передачі кадрів по ньому, тому що в кожен конкретний момент часу кільце використовується тільки одним комп'ютером.

Використання поділюваних середовищ (shared media) дозволяє спростити логіку роботи мережі. Наприклад, відпадає необхідність контролю переповнення вузлів мережі кадрами від багатьох станцій, що вирішили одночасно обмінятися інформацією. У глобальних мережах, де відрізки кабелів, що з'єднують окремі вузли, не розглядаються як загальний ресурс, така необхідність виникає, і для рішення цієї проблеми в протоколи обміну інформацією вводяться дуже складні процедури керування потоком кадрів, що запобігають переповнення каналів зв'язку і вузлів мережі.

Використання в локальних мережах дуже простих конфігурацій поряд з позитивними мало і негативні наслідки, з яких найбільш неприємними були обмеження по продуктивності і надійності. Наявність тільки одного шляху передачі інформації, поділюваного усіма вузлами мережі, у принципі обмежувало пропускну здатність мережі пропускною здатністю цього шляху (яка поділялася в середньому на число комп'ютерів мережі), а надійність мережі — надійністю цього шляху. Тому в міру підвищення популярності локальних мереж і розширення їхніх сфер застосування усе більше стали застосовуватися спеціальні комунікаційні пристрої — мости і маршрутизатори, — які значною мірою знімали обмеження єдиного поділюваного середовища передачі даних. Базові конфігурації у формі загальної шини і кільця перетворилися в елементарні структури локальних мереж, які можна тепер з'єднувати один з одним більш складним чином, утворити паралельні основні чи резервні шляхи між вузлами.

Проте усередині базових структур як і раніше працюють все ті ж протоколи поділюваних єдиних середовищ передачі даних, що були розроблені більш 15 років тому. Це зв'язано з тим, що такі характеристики кабелів локальних мереж, як добра швидкість і надійність, задовольняли протягом усіх цих років користувачів невеликих комп'ютерних мереж, що могли побудувати мережу без великих витрат тільки за допомогою мережних адаптерів і кабелю. До того ж колосальна інсталяційна база устаткування і програмного забезпечення для технологій Ethernet і Token Ring сприяла тому, що склався наступний підхід: у межах невеликих сегментів використовуються старі протоколи в їхньому незмінному виді, а об'єднання таких сегментів у загальну мережу відбувається за допомогою додаткового і досить складного устаткування.

За останні кілька років намітився рух до відмови від поділюваних середовищ передачі даних у локальних мережах і переходу до застосування активних комутаторів, до яких кінцеві вузли приєднуються індивідуальними лініями зв'язку. У чистому виді такий підхід пропонується в технології ATM (Asynchronous Transfer Mode), а в технологіях, що носять традиційні назви з приставкою switched (такий, що комутується): switched Ethernet, switched Token Ring, switched FDDI, звичайно використовується змішаний підхід, що з’єднує поділювані та індивідуальні середовища передачі даних. Найчастіше кінцеві вузли з'єднуються в невеликі поділювані сегменти за допомогою повторювачів, а сегменти з'єднуються один з одним за допомогою індивідуальних зв'язків, що комутуються.

Існує і досить помітна тенденція до використання в традиційних технологіях так званої мікро-сегментації, коли навіть кінцеві вузли відразу з'єднуються з комутатором індивідуальними каналами. Такі мережі є дорожчими від поділюваних чи змішаних, але продуктивність їх вища.

При використанні комутаторів у традиційних технологіях з'явився новий режим роботи — напівдуплексний (full-duplex). У поділюваному сегменті станції завжди працюють у напівдуплексному режимі (half-duplex), тому що в кожен момент часу мережний адаптер станції або передає свої дані, або приймає чужі, але ніколи не робить це одночасно. Це справедливо для всіх технологій локальних мереж, тому що поділювані середовища підтримуються не тільки класичними технологіями локальних мереж Ethernet, Token Ring, FDDI, але і всіма новими – Fast Ethernet, lOOVG-AnyLAN, Gigabit Ethernet.

У напівдуплексному режимі мережний адаптер може одночасно передавати свої дані в мережу і приймати з мережі чужі дані. Такий режим нескладно забезпечується при прямому з'єднання з мостом/комутатором чи маршрутизатором, тому що вхід і вихід кожного порту такого пристрою працюють незалежно один від одного, кожний зі своїм буфером кадрів.

Сьогодні кожна технологія локальних мереж пристосована для роботи як у напівдуплексному, так і повнодуплексному режимах. У цих режимах обмеження, що накладаються на загальну довжину мережі, істотно відрізняються, так що та сама технологія може дозволяти будувати дуже різні мережі в залежності від обраного режиму роботи. Наприклад, технологія Fast Ethernet дозволяє для напівдуплексного режиму будувати мережі діаметром не більш 200 метрів, а для повнодуплексного режиму обмежень на діаметр мережі не існує. Тому при порівнянні різних технологій необхідно обов'язково мати на увазі можливість їхньої роботи в двох режимах.

Незважаючи на появу нових технологій, класичні протоколи локальних мереж Ethernet і Token Ring за прогнозами фахівців будуть повсюдно використовуватися ще принаймні років 5-10, у зв'язку з чим знання їхніх деталей необхідно для успішного застосування сучасної комунікаційної апаратури. Крім того, деякі сучасні високопродуктивні технології, такі як Fast Ethernet, Gigabit Ethernet, у значній мірі зберігають сумісність зі своїми попередниками. Це ще раз підтверджує важливість вивчення класичних протоколів локальних мереж поряд з вивченням нових технологій.

6. Стандарти мереж. Стандарти IEEE 802.

1980 року в інституті IEEE був організований комітет 802 зі стандартизації локальних мереж, у результаті роботи якого було прийняте сімейство стандартів IEEE 802.X, що містять рекомендації з проектування нижніх рівнів локальних мереж. Пізніше результати роботи цього комітету лягли в основу комплексу міжнародних стандартів ISO 8802-1..5. Ці стандарти були створені на основі найбільш розповсюджених фірмових стандартів мереж Ethernet, ArcNet Token Ring.

Стандарти сімейства IEEE 802.X охоплюють тільки два нижніх рівні семирівневої моделі OSI – фізичний і канальний. Це пов'язано з тим, що саме ці рівні найбільшою мірою відбивають специфіку локальних мереж. Старші ж рівні, починаючи з мережевого, у значній мірі мають спільні риси як для локальних, так і для глобальних мереж.

Специфіка локальних мереж також знайшла своє відображення в поділі канального рівня на два підрівня, що часто називають також рівнями:

- логічної передачі даних (Logical Link Control, LLC);
- керування доступом до середовища (Media Access Control, MAC).

Рівень MAC з'явився через існування в локальних мережах поділюваного середовища передачі даних. Саме цей рівень забезпечує коректне спільне використання загального середовища, надаючи його, відповідно до визначеного алгоритму, в розпорядження тій чи іншій станції мережі. Після того, як доступ до середовища отриманий, нею може скористатися більш високий рівень – рівень LLC, що організовує передачу логічних одиниць даних, кадрів інформації, з різним рівнем якості транспортних послуг. У сучасних локальних мережах одержали поширення кілька протоколів рівня MAC, що реалізують різні алгоритми доступу до поділюваного середовища. Ці протоколи цілком визначають специфіку таких технологій, як Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, FDDI.

Рівень LLC відповідає за передачу кадрів даних між вузлами з різним ступенем надійності, а також реалізує функції інтерфейсу разом з сусіднім мережевим рівнем. Саме через рівень LLC мережевий протокол подає запит канальному рівню на потрібну йому транспортну операцію з потрібною якістю. На рівні LLC існує кілька режимів роботи, що відрізняються наявністю чи відсутністю на цьому рівні процедур відновлення кадрів у випадку їхньої втрати чи перекручування, тобто транспортних послуг, що відрізняються якістю, цього рівня.

Протоколи рівнів MAC і LLC взаємно незалежні – кожен протокол рівня MAC може використовуватися з будь-яким протоколом рівня LLC, і навпаки.

Ця структура з'явилася в результаті великої роботи, проведеної комітетом 802 з виділення в різних фірмових технологіях загальних підходів і загальних функцій, а також узгодженню стилів їхнього опису. Опис кожної технології розділено на дві частин: опис рівня MAC і опис фізичного рівня.

Над канальним рівнем усіх технологій зображений загальний для них протокол LLC, що підтримує кілька режимів роботи, але незалежний від вибору конкретної технології. Стандартом LLC керує підкомітет 802.2. Навіть технології, стандартизовані не в рамках комітету 802, орієнтуються на використання протоколу LLC, визначеного стандартом 802.2, наприклад протокол FDDI, стандартизований ANSI.

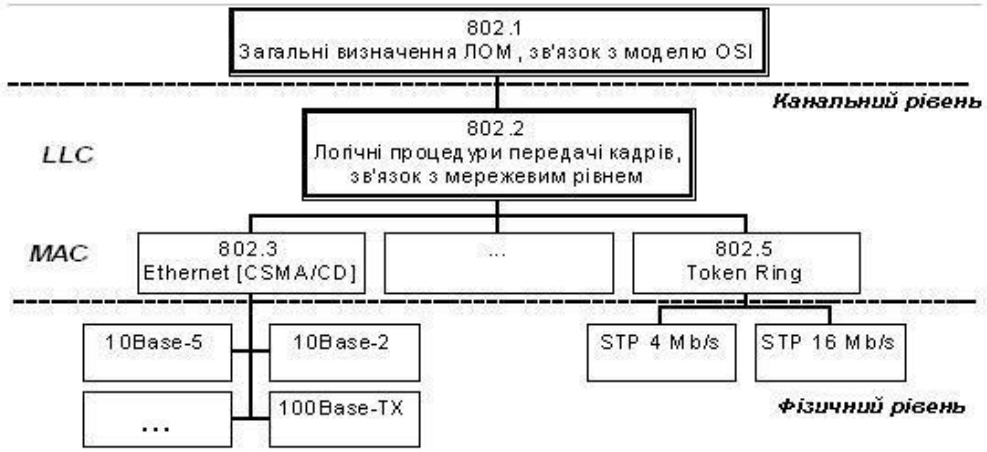


Рис. 6.1. Структура стандартів IEEE 802.X.

Окремо стоять стандарти, розроблені підкомітетом 802.1. Ці стандарти носять загальний для всіх технологій характер. У підкомітеті 802.1 розроблені загальні визначення локальних мереж і їх властивостей, визначений зв'язок трьох рівнів моделі IEEE 802 з моделлю OSI. Але найбільш практично важливими є стандарти 802.1, що описують взаємодію між собою різних технологій, а також стандарти для побудови більш складних мереж на основі базових топологій. Ця група стандартів носить загальну назву стандартів міжмережевої взаємодії (internetworking). Сюди входять такі важливі стандарти, як стандарт 802.1D, що описує логіку роботи моста/комутатора, стандарт 802.1H, який визначає роботу транслюючого моста, що може без маршрутизатора поєднувати мережі Ethernet і FDDI, Ethernet і Token Ring і т.п. Сьогодні набір стандартів, розроблених підкомітетом 802.1, продовжує зростати. Наприклад, недавно він поповнився важливим стандартом 802.1O, що визначає спосіб побудови віртуальних локальних мереж VLAN у мережах на основі комутаторів.

Стандарти 802.3, 802.4, 802.5 і 802.12 описують технології локальних мереж, що з'явилися в результаті поліпшення фірмових технологій, які лягли в їх основу. Так, основу стандарту 802.3 склала технологія Ethernet, розроблена компаніями Digital, Intel і Xerox (чи Ethernet DIX), стандарт 802.4 з'явився як узагальнення технології ArcNet компанії Datapoint Corporation, а стандарт 802.5 в основному відповідає технології Token Ring компанії IBM.

Вихідні фірмові технології і їх модифіковані варіанти – стандарти 802.x у ряді випадків довгі роки існували паралельно. Наприклад, технологія ArcNet так і не була повністю приведена у відповідність зі стандартом 802.4. Розбіжності між технологією Token Ring і стандартом 802.5 теж періодично виникають, тому що компанія IBM регулярно вносить удосконалення у свою технологію і комітет 802.5 відбиває ці удосконалення в стандарті з деяким запізненням. Виключення складає технологія Ethernet. Останній фірмовий стандарт Ethernet DIX був прийнятий у 1980 році.

Більш пізні стандарти розроблялися не однією компанією, а групою зацікавлених компаній, а потім передавалися у відповідний підкомітет IEEE 802 для затвердження. Так відбулося з технологіями Fast Ethernet, 100VG-AnyLAN, Gigabit Ethernet. Група зацікавлених компаній створювала спочатку невелике об'єднання, а потім у міру розвитку робіт до нього приєднувалися інші компанії, так що процес прийняття стандарту носив відкритий характер.

Сьогодні комітет 802 включає наступний ряд підкомітетів:

802.1 – Internetworking – об'єднання мереж;

802.2 – Logical Link Control, LLC – керування логічною передачею даних;

802.3 – Ethernet з методом доступу CSMA/CD;

802.4 – Token Bus LAN – локальні мережі з методом доступу Token Bus;

802.5 – Token Ring LAN – локальні мережі з методом доступу Token Ring;

802.6 – Metropolitan Area Network, MAN – мережі мегаполісів;

802.7 – Broadband Technical Advisory Group – технічна консультаційна група з широкополосної передачі;

802.8 – Fiber Optic Technical Advisory Group – технічна консультаційна група з волоконно-оптичних мереж;

802.9 – Integrated Voice and data Networks – інтегровані мережі передачі голосу і даних;

802.10 – Network Security – мережева безпека;

802.11 – Wireless Networks – безпровідникові мережі;

802.12 – Demand Priority Access LAN, 100VG-AnyLAN – локальні мережі з методом доступу за вимогою з пріоритетами.

802.15 – Wireless Personal Area Network (WPAN).

802.16 — стандарт для широкополосного радіозв'язку.

802.17 — Resilient Packet Ring (RPR) – технологія «стійких пакетних кілець».

7. Етапи проектування мереж.

Коли розглядаються завдання проектування нової мережі або можливості під’єднання наявної мережі, то виникають окремі важливі питання, які необхідно розв’язати. Наприклад, як розподілити адреси мережевих ресурсів, як змінити наявні адреси, чи вибрати статичний, чи динамічний раутінг, як налаштувати сервер імен і як захистити мережу. В той сам час слід вирішити питання надійності, доступності і резервування, а також питання адміністрування та управління мережею.

Проектування мережі слід здійснювати перед будь-яким впровадженням. Проект мережі повинен постійно переглядатися, коли протягом певного часу змінюються вимоги. Добрий проект включає детальну документацію мережі, потрібну для наступних посилань. Добре спроектовані мережі прості для впровадження і створюють небагато несподіванок.

Методика проектування. Рекомендованою методикою проектування IP-мереж є підхід “зверху вниз”. Ця технологія слідує стеку протоколів TCP/IP. Зверху стеку розташований рівень застосувань, тому він є першим рівнем, який розглядається при проектуванні IP-мережі. Наступні два рівні – це Транспортний і Мережевий, а Канальний рівень є останнім.

Наведемо основні аспекти проектування IP-мережі;

- Масштабованість.
- Відкриті стандарти.
- Доступність і надійність.
- Модульність.
- Безпека.
- Управління мережею.
- Характеристики.
- Економічні питання.

Етапи проектування мережі:

- Визначення цілей мережі.
- Збір інформації для проектування.
- Формування пропозицій або специфікацій.
- Огляд.

8. Структура IP – адреси. Повнокласова та безкласова IP – адресація.

8.1. Загальна структура IP-адрес та їх класи.

Кожному вузлу IP мережі призначається 32-розрядна логічна адреса, що називається IP-адресою. IP-адреса має довжину 4 байти і звичайно записується у вигляді чотирьох чисел, що представляють значення кожного байту в десятковій формі і розділених крапками, наприклад, 128.10.2.30 – традиційна десяткова форма представлення адреси, а 10000000 00001010 00000010 00011110 – двійкова форма представлення адреси.

Адреса складається з двох логічних частин – номеру мережі і номеру вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка – до номера вузла, визначається значеннями перших біт адреси. Значення цих біт є також ознаками того, до якого класу відноситься та або інша IP-адреса. На рисунку 8.1 показана структура IP-адрес різних класів.

Клас IP-адрес, а, отже, і співвідношення між розмірами полів номера мережі і номера вузла, можуть бути легко визначені по старших бітах першого байту. Основні характеристики мереж різних класів приведені в таблиці 8.1.

Деякі IP-адреси мають спеціальне призначення і не можуть бути використані для вузлів в реальних мережах (таблиця 8.2).

Рис. 8.1. Класи IP адрес.

Таблиця 8.1 – Характеристика IP адрес різних класів

Клас	Перші біти	Найменший номер мережі	Найбільший номер мережі	Максимальне число вузлів у мережі
A	0	1.0.0.0 (0 – не використовується)	126.0.0.0 (127 - зарезервований)	2^{24}, поле 3 байти
B	10	128.0.0.0	191.255.0.0	2^{16}, поле 2 байти
C	110	192.0.0.0	223.255.255.0	2^{8}, поле 1 байт
D	1110	224.0.0.0	239.255.255.255	групові адреси
E	11110	240.0.0.0	247.255.255.255	Зарезервовано

Таблиця 8.2 – Спеціальні IP адреси

Типи адрес		Значення
Всі нулі	0.0.0.0	Даний вузол
[Номер мережі].[Всі нулі]	192.168.1.0	Дана мережа
[Всі нулі].[Номер вузла]	0.0.0.1	Вузол даної мережі
Всі одиниці	255.255.255.255	Всі вузли даної мережі
[Номер мережі].[Всі одиниці]	192.168.1.255	Всі вузли заданої мережі
127.[Будь-яке число]	127.0.0.1	«Петля» (Loopback)

Для використання в приватних (внутрішніх, відомчих) мережах зарезервовані три блоки IP-адрес:

10.0.0.0 – 10.255.255.255 (1 мережа класу A);

172.16.0.0 – 172.31.255.255 (16 мереж класу B);

192.168.1.0 – 192.168.255.255 (255 мереж класу C).

Ці адреси призначені для внутрішнього використання і не використовуються в мережі Інтернет.

8.2. Структура IP-адрес при повнокласовій адресації.

Для супроводу мереж різного розміру при *повнокласовій адресації* IP-адреси, представлені 32-бітовим кодом, ділять на наперед задані *класи*: A, B, C, D, E. Практичне використання на даний час мають перші 3 класи: A, B і C. Кожен клас – A, B або C визначає границю між мережевим префіксом і номером станції всередині 32-бітової IP-адреси. При повнокласовій IP-адресації кожна адреса містить *ключ самоідентифікації* – перші зліва біти IP-адреси, які визначають пункт поділу між мережевим префіксом і номером станції. Це спрощує систему раутінгу в Internet, оскільки первинні протоколи раутінгу можуть не підтримувати “ключ дешифрування” або “мережеву маску” для визначення довжини мережевого префіксу. Для ключа самоідентифікації адрес класу A використовують 1 біт (0_2), для адрес класу B – 2 біти (10_2), для адрес класу C – 3 біти (110_2), для адрес класів D та E – 4 (1110_2) і 5 бітів (11110_2) відповідно. Формати основних класів адрес зображені на рис. 8.2, біти ключа самоідентифікації виділені зліва, там же вказані їх значення. Зауважимо, що ці біти входять до мережевого префіксу, тому діапазон його можливих значень визначається з урахуванням фіксованих значень цих бітів.

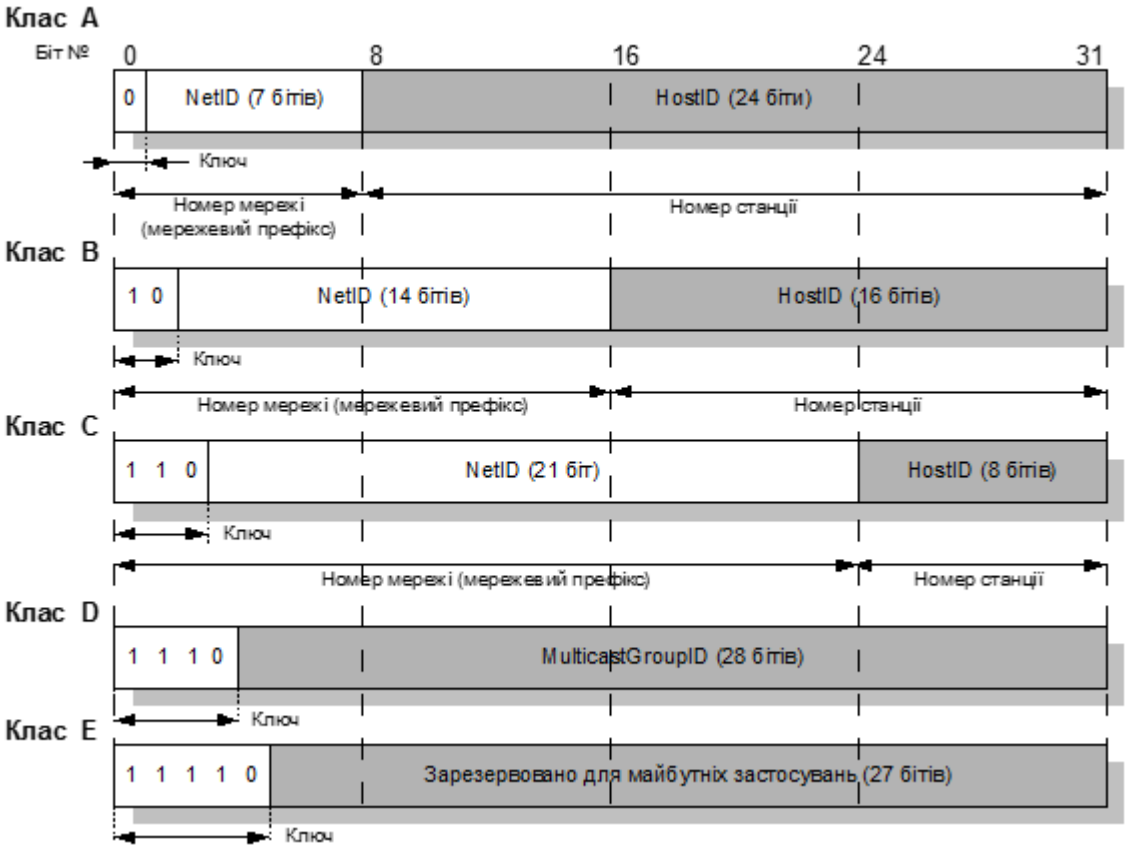


Рис. 8.2. Структура IP-адрес.

IP-адреса може бути використана для посилання як на мережу, так і на окрему станцію. За угодою, адреса станції (HostID), всі біти якої рівні 0, ніколи не призначається окремій станції, вона зарезервована для посилання на мережу з адресою NetID. IP-адреси можуть бути використані для позначення *всеадресного (широкомовного) повідомлення* для мережі NetID; для цього всі біти номера станції встановлюються в “1”. IP-адреса *обмеженого широкомовного повідомлення* або *широкомовного повідомлення в локальній мережі* має всі 32 біти встановлені в “1”. Поле IP-адреси, яке містить всі “1”, інтерпретується як “всі” (напр., “всі станції” в мережі); поле, яке складається з усіх “0”, інтерпретується як “цей/ця” (наприклад, HostID=0- “цей вузол”, NetID=0 – “ця мережа”).

Мережевий префікс NetID $127_{10} \equiv 01111111_2$, який відповідає IP-адресі класу A, зарезервований для *кільцевої перевірки (контрольної петлі)* і використовується для тестування стеку протоколів TCP/IP та для процесів внутрішньої комунікації в локальному вузлі. Трафік не передається в мережу - це не мережева адреса.

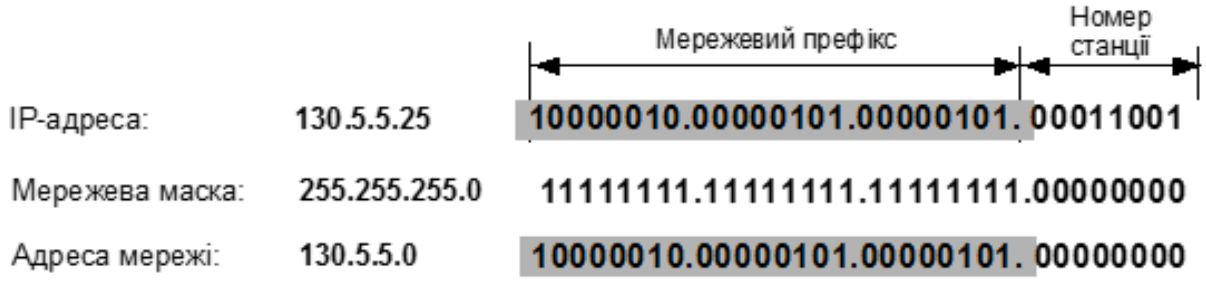
На практиці діють 5 комбінацій щодо використання нулів (“цей”) і одиниць (“всі”):

Всі “0”		Ця станція (host)
Всі “0”	Адреса станції (HostID)	Станція (host) у цій мережі
Всі “1”		Обмежена широкомовна (для локальної мережі)
Адреса мережі (NetID)	Всі “1”	Широкомовна адреса для мережі
$127_{10} \equiv 01111111_2$	Будь-що (часто “1”)	Кільцева перевірка

З урахуванням угод про спеціальні адреси розподіл кількості адрес у різних класах можна проілюструвати табл. 8.3:

Таблиця 8.3. Кількість мереж і станцій при повнокласовій адресації.

	Максимальна кількість мереж	**Максимальна кількість станцій в одній мережі**
Клас A	$N_d=2^7-2=126$	$N_h=2^{24}-2=16\ 777\ 214$
Клас B	$N_d=2^{14}=16\ 384$	$N_h=2^{16}-2=65\ 534$
Клас C	$N_d=2^{21}=2\ 097\ 152$	$N_h=2^8-2=254$



Оскільки 32-бітову IP-адресу можна поділити на чотири 8-бітові поля (байти), то для спрощення запису і читання IP-адрес людьми IP-адреси часто виражають чотирма десятковими числами, розділеними крапками, тобто у формі у AAA.BBB.CCC.DDD. Кожне десяткове число виражає десяткове значення відповідного байта IP-адреси. Таку форму представлення IP-адреси називають *крапкованим десятковим записом*. IP-адреси можна розрізняти за класами, використовуючи десяткове значення AAA першого байта:

Таблиця 8.4. Діапазони IP-адрес при повнокласовій адресації.

Клас	**Найменша адреса**	**Найбільша адреса**
A	1.xxx.xxx.xxx	126.xxx.xxx.xxx
B	128.0.xxx.xxx	191.255.xxx.xxx
C	192.0.1.xxx	223.255.255.xxx
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

8.3. Використання мережевої маски.

Мережева маска – це 32-розрядне число, що має біти, які відповідають полям NetID та SubNetID, рівні 1, а біти, які відповідають HostID, рівні 0. Наприклад, в десятковому крапкованому записі маска 255.255.255.0 виділяє перші 3 байти IP-адреси. Адреса мережі (мережевий префікс) визначається шляхом логічного перемноження IP-адреси і маски:

Адреса підмережі = IP-адреса ∩ мережева маска

Стандарти, які описують сучасні протоколи раутінгу, часто посилаються на довжину мережевого префіксу замість маски мережі, оскільки довжина префіксу дорівнює кількості послідовних двійкових одиниць в мережевій масці. Тоді для класу А маємо маску 255.0.0.0 і позначення /8, для класу В – маску 255.255.0.0 і позначення /16 та для класу С – маску 255.255.255.0 і позначення /24. Це означає, що визначаючи IP-адресу 130.5.5.25 з мережевою маскою 255.255.255.0, можна також писати 130.5.5.25/24. Запис /<довжина префіксу> більш компактний і зрозумілий. Однак важливо відзначити, що сучасні *протоколи раутінгу підтримують повну чотириоктетну мережеву маску*. На даний час відсутні стандартні протоколи, які б мали однобайтове поле в заголовку з числом бітів у розширеному мережевому префіксі.

8.4. Безкласова IP-адресація.

У 1992 році, внаслідок експоненціального зростання Internet, IETF розпочав роботи щодо забезпечення можливості масштабування системи раутінгу Internet і підтримки майбутнього зростання. Опрацьована концепція *безкласового внутрішньодоменного раутінгу* (*Classless Inter-Domain Routing – CIDR*). CIDR офіційно удокументована у вересні 1993 року в RFC 1517, RFC 1518, RFC 1519 та RFC 1520. CIDR підтримує дві важливі характеристики, які покращують глобальну систему раутінгу Internet:

- CIDR виключає традиційну концепцію мережевих адрес класів А, В і С, замінюючи її узагальненою концепцією мережевого префіксу. Замість перших трьох бітів IP-адреси, для визначення точки поділу IP-адреси на мережеву адресу (NetID) та адресу станції (HostID). раутери використовують мережевий префікс. Тому CIDR підтримує впровадження мережевих адрес *довільного розміру* замість стандартних 8-бітових, 16-бітових або 24-бітових мережевих адрес, властивих повнокласовій адресації. Це створює можливість ефективного розподілу адресного простору IPv4.
- CIDR підтримує агрегування маршрутів, коли окремий вхід таблиці раутінгу може репрезентувати адресний простір, який охоплює тисячі традиційних повнокласових маршрутів, визначаючи, як маршрутувати трафік до багатьох індивідуальних мережевих адрес. Агрегування маршрутів допомагає контролювати обсяг раутінгової інформації в раутерах магістралей Internet, зменшує швидкі зміни наявності маршрутів і спрощує локальні адміністративні витрати на модифікацію зовнішньої раутінгової інформації.

Раутер, який підтримує CIDR, не використовує перших трьох бітів адреси для визначення довжини мережевого префіксу. Натомість префікси розглядаються як неперервний блок адресного простору. Наприклад, всі

префікси /20 представляють той сам обсяг адресного простору (2^{12}=4096 адрес станцій). На відміну від повнокласової адресації, у моделі CIDR кожна частина раутінгової інформації оголошується разом з мережевою маскою або з довжиною префіксу. Наприклад, мережа з 20-бітовим номером мережі та 12-бітовими номерами станцій повинна оголошуватися з 20-бітовою довжиною префіксу, тобто як /20. Така IP-адреса може належати до колишнього класу A, B або C. Для ілюстрації в табл. наведені найбільш широко впроваджені адресні блоки CIDR.

Таблиця 8.5. Адресні блоки CIDR.

Довжина префіксу CIDR	**Мережева маска**	**Кількість індивідуальних адрес**	**Кількість повнокласових мереж**
/13	255.248.0.0	512 K	8 B або 2048 C
/15	255.254.0.0	128 K	2 B або 512 C
/16	255.255.0.0	64 K	1 B або 256 C
/17	255.255.128.0	32 K	128 C
/18	255.255.192.0	16 K	64 C
/19	255.255.224.0	8 K	32 C
/21	255.255.248.0	2 K	8 C
/22	255.255.252.0	1 K	4 C
/24	255.255.255.0	256	1 C
/25	255.255.255.128	128	½ C
/26	255.255.255.192	64	¼ C
/27	255.255.255.224	32	1/8 C

9. Спосіб впровадження підмереж. Організація підмереж.

Для раціонального здійснення раутінгу пакетів в IP-мережах адресний простір організований ієрархічно. Кожній мережі, яка звичайно пов’язана з деякою організаційною структурою (фірмою, підприємством, закладом тощо, яку надалі називатимемо *організацією*) виділяється частина адресного простору у вигляді блоку адрес зі спільним мережевим префіксом або декількох таких блоків. При повнокласовій адресації мінімальний розмір одного блоку визначається класом адреси і дорівнює максимальній кількості станцій в мережі з адресою такого класу (див. табл.). Оскільки на початках створення Internet його проектанти не змогли правильно передбачити масштабів майбутнього зростання, то опрацьована ними система повнокласової адресації на сьогодні створила ряд проблем. Очевидно, що 16777214 адрес станцій в одній мережі з мережевою адресою класу A незручні для використання, як і 65534 адрес класу B. Кількість мережевих адрес для підтримки мереж організацій середнього розміру недостатня.

Єдиними наявними блоками для середніх організацій є блоки /24, які дозволяють підтримувати 254 станції в одній мережі, що занадто мало у багатьох випадках, а виділення декількох таких блоків має негативний вплив на збільшення розмірів таблиць раутінгу в глобальному Internet.

Однак існує простий спосіб ієрархічної організації *підмереж* в мережах класів A, B і C: підмереж класу A у вигляді еквівалентних мереж класу B (або класу C), підмереж класу B у вигляді еквівалентних мереж класу C і підмереж класу C. Цей спосіб викладено в документі RFC 950, прийнятому в 1985 році. Основна ідея модифікації з впровадженням підмереж полягає в тому, щоб замість дворівневої ієрархії IP-адреси як сукупності мережевого префіксу NetID та суфіксу - номера станції HostID, впровадити трирівневу, тобто розділити початкове поле суфіксу HostID на адресу підмережі SubNetID та номер станції HostID (рис. 9.1).

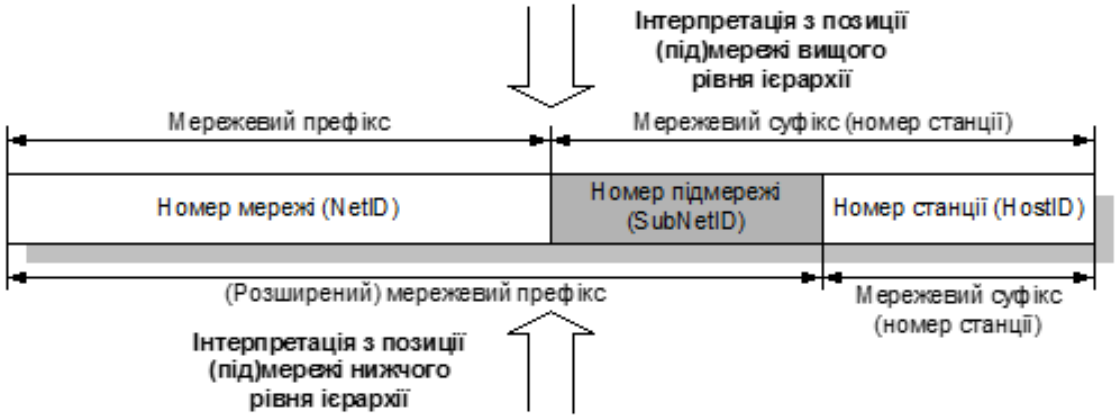


Рис. 9.1. Впровадження трирівневої ієрархії IP-адрес.

При цьому з позиції (під)мережі вищого рівня ієрархії те саме 32-бітове поле адреси інтерпретується згідно з розподілом на префікс і суфікс, прийнятим у цій (під)мережі, зокрема, згідно з класом мережевої адреси, а з позиції підмережі нижчого ієрархічного рівня – згідно з іншим розподілом (рис. 9.2). При цьому для маршрутування трафіку між підмережами раутери *всередині* мережі з підмережами використовують *розширений мережевий префікс*, який об’єднує повнокласовий мережевий префікс і номер підмережі

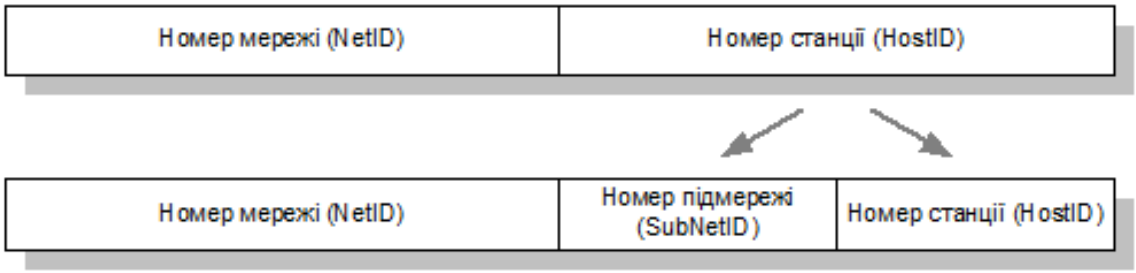


Рис. 9.2. Інтерпретація поля IP-адреси з позицій (під)мереж суміжних ієрархічних рівнів.

Кількість бітів, які відводять для розміщення номера підмережі, залежить від потрібної кількості підмереж і завжди повинна бути цілою степеню 2, тобто 2^1=2 (один біт), 2^2=4 (два біти), 2^3=8 (3 біти), 2^4=16 (4 біти) і т.д. Тому фактично потрібну кількість підмереж з урахуванням перспективи

розвитку мережі завжди необхідно округляти до більшого цілого числа, яке є цілою степеню 2.

Перевагою використання підмереж є значне зменшення таблиць маршрутизації, бо підмережева структура мережі невидима зовні приватної мережі організації. Наприклад, мережа класу B з великою кількістю підмереж може бути записана в таблиці маршрутизації одним записом, який посилається тільки на NetID. Якщо б замість підмереж використовувалися мережі класу C, то кількість записів в таблиці маршрутизації була б рівна кількості підмереж (рис. 9.3).

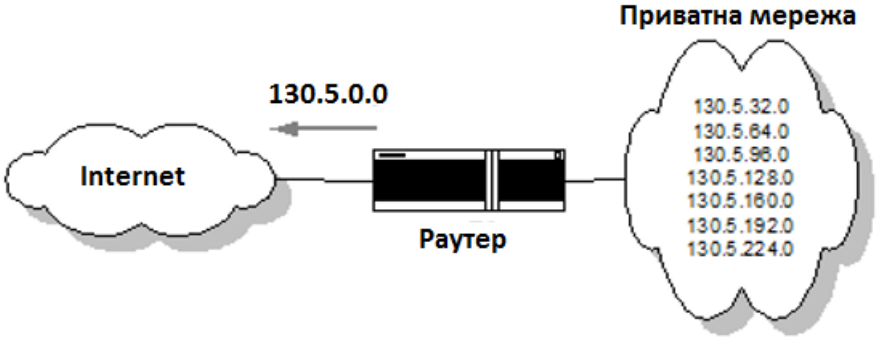


Рис. 9.3. Агрегування маршрутів до підмереж мережі класу B.

Кожна підмережа локально діє як окрема мережа, і комунікація між підмережами вимагає того ж, що й комунікація між мережами. Станції в різних підмережах не можуть бачити одна одну, доки не передбачено спеціального способу для цього. Раутери всередині організації повинні розрізняти індивідуальні підмережі, однак зовні всі підмережі організації об'єднані одним входом таблиці раутінгу з одним мережевим префіксом. Це дозволяє мережевому адміністратору впроваджувати довільну складність у мережі організації, не впливаючи на розмір таблиць раутінгу Internet.

10. Мережеві маски змінної довжини. Планування мереж із мережевими масками змінної довжини.

У 1987 році документ RFC 1009 визначив, як мережа з підмережами може використовувати більше, ніж одну мережеву маску. Якщо IP-мережі призначено понад одну мережеву маску, то вона вважається мережею з *мережевою маскою змінної довжини* (*Variable Length Subnet Mask – VLSM*), оскільки мережевий префікс може мати різну довжину в різних підмережах.

Ефективне використання адресного простору організації. VLSM підтримує більш ефективне використання IP-адресного простору, виділеного організації. Одна з проблем полягала в тому, що вибрана маска визначала організації фіксовану кількість підмереж фіксованого розміру. Наприклад, приймемо, що мережевий адміністратор вирішив конфігурувати мережу 130.5.0.0/16 з розширеним мережевим префіксом /22. Така мережа дозволяє утворення 64 (2^6) підмереж, кожна з яких може містити до 1022 станцій (2^{10}-2). Це добре, якщо організація хоче впровадити певну кількість великих підмереж, але створює проблему з неефективним використанням адресного простору для поодиноких малих підмереж, які містять кілька десятків

станцій, бо при цьому втрачається біля 1000 адрес для кожної малої підмережі.

Розв’язання цієї проблеми полягає у тому, щоб дозволити призначати понад одну мережеву маску в мережі. Припустимо, що мережевий адміністратор може конфігурувати мережу 130.5.0.0/16 з розширеним мережевим префіксом /26. Така мережа може мати 1024 підмережі, кожна з яких має до 62 (2^6-2) станцій. Тому префікс /26 добре придатний для малих підмереж (до 60 станцій), тоді як префікс /22 придатний для більших підмереж (до 1000 станцій).

Агрегування маршрутів. VLSM дозволяє ієрархічний (рекурсивний) поділ адресного простору організації, так що він може бути реасембльований і агрегований для зменшення обсягу раутінгової інформації на верхньому рівні. Концептуально це полягає в тому, що мережа спочатку ділиться на підмережі, далі окремі підмережі поділяють на під-підмережі і т.д. (рис. 10.1). Це дозволяє деталізовану структуру раутінгової інформації для однієї групи підмереж зробити невидимою для раутерів з інших груп підмереж.

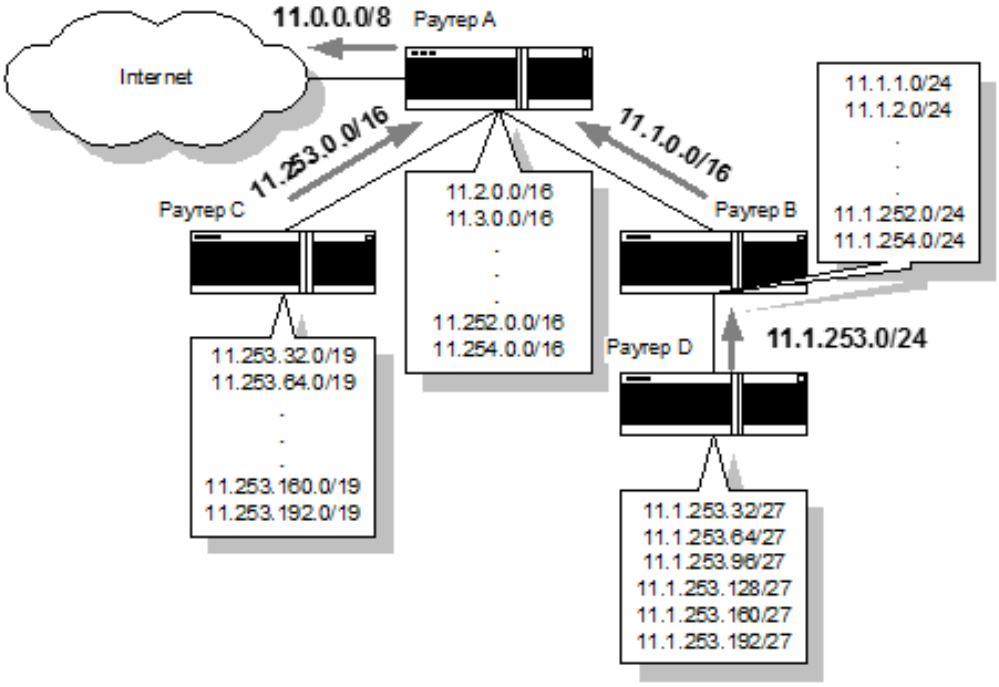


Рис. 10.1 . Рекурсивний поділ мережевого префіксу при VLSM.

Зауважимо, що рекурсивний процес не вимагає використання однакового розширеного мережевого префіксу на кожному рівні рекурсії. Рекурсивний поділ може здійснюватися доти, доки це потрібно.

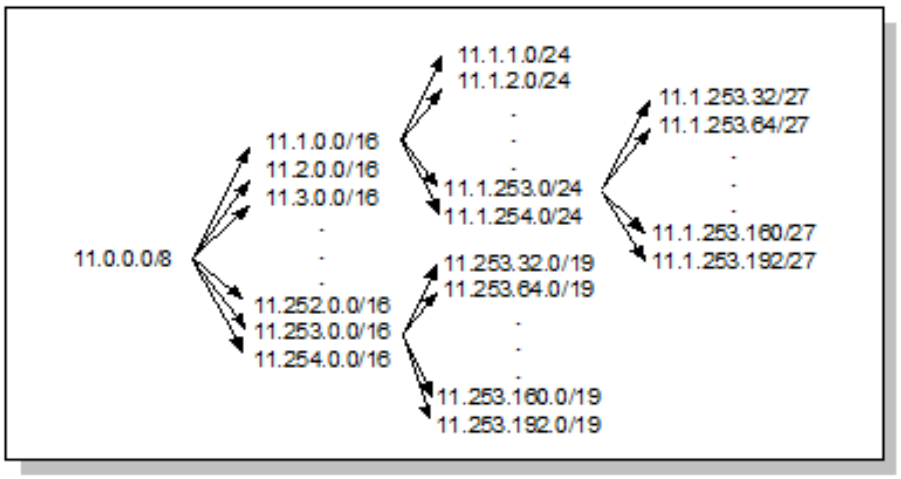


Рис. 10.2. Агрегування маршрутів для VLSM.

Рис. 10.2 показує, як використання VLSM може зменшити обсяг таблиць раутінгу організації за рахунок агрегування маршрутів. У виносках, зображених за раутерами, перелічені підмережі, розміщені за ними. Відзначимо, що раутер D здатний об'єднати 6 підмереж, розташованих за ним, в одному оголошенні маршруту (11.1.253.0/24), і що раутер B може агрегувати всі підмережі, розміщені за ним, в одне оголошення маршруту (11.253.0.0/16). Нарешті, раутер A вводить один маршрут для мережі до глобальної таблиці раутінгу Internet – 11.0.0.0/8.

Планування мереж з VLSM. При впровадженні VLSM мережевий адміністратор повинен рекурсивно задавати ті ж запитання, що й при традиційному плануванні підмереж. Ті ж самі рішення повинні бути прийняті на кожному рівні ієрархії:

1) Скільки підмереж потрібно на даному рівні сьогодні?
2) Скільки підмереж буде потрібно на даному рівні в майбутньому?
3) Скільки станцій наявно в найбільшій підмережі даного рівня сьогодні?
4) Скільки станцій буде потрібно в найбільшій підмережі даного рівня в майбутньому?

На кожному рівні планувальники повинні передбачити достатньо надлишкових бітів в адресах для підтримки потрібної кількості підмереж в майбутньому, а також для подальших рівнів рекурсії. Наприклад, верхній рівень ієрархії схеми підмереж організації може бути визначений кількістю кампусів, середній рівень – кількістю будинків у кожному кампусі і найнижчі рівні – максимальною кількістю підмереж та максимальною кількістю користувачів у підмережі в кожному будинку.

Для нижнього рівні слід подбати, щоб кількість підмереж була достатньо великою для підтримки потрібної кількості станцій. Коли адресний план впроваджено, то адреси від кожного вузла (станції, підмережі, групи підмереж будинку, кампусу) можуть бути об'єднані в один адресний блок, що запобігатиме надмірному збільшенню таблиць раутінгу.

Вимоги щодо впровадження VLSM. Успішне впровадження VLSM передбачає три передумови:

1) Протоколи раутінгу повинні переносити інформацію про розширений мережевий префікс для кожного оголошення маршруту.

2) Всі раутери повинні підтримувати узгоджений алгоритм пересилання, базований на “найдовшому узгодженні”.

3) Якщо з’являється агрегування маршрутів, то адреси повинні бути призначені так, щоб вони мали топологічну значимість (тобто були узгоджені з топологією мережі).

CIDR та VLSM по суті подібні, по вони дозволяють рекурсивно ділити частину IP-адрес на послідовні менші частини. Відмінність полягає в тому, що при VLSM рекурсія здійснюється над адресним простором, попередньо виділеним для організації і невидимим з глобального Internet. З другого боку, CIDR здійснює рекурсивний розподіл адресного блоку, виділеного з реєстру Internet для ISP верхнього рівня, спочатку для ISP середнього рівня, далі для ISP нижнього рівня і нарешті для мережі організації. Подібно як для VLSM, успішне впровадження CIDR базується на трьох передумовах:

1) Протоколи раутінгу повинні переносити інформацію про розширений мережевий префікс для кожного оголошення маршруту.

2) Всі раутери повинні підтримувати узгоджений алгоритм пересилання, базований на “найдовшому узгодженні”.

3) Якщо з’являється агрегування маршрутів, то адреси повинні бути призначені так, щоб вони мали топологічну значимість.

11.Трансляція мережевих адрес.

Використання трансляції мережевих адрес визначене документом RFC 1631. NAT працює на рівні раутера як агент між внутрішньою (локальною) і зовнішньою (глобальною) мережами і допомагає зберігати адресний простір, оскільки принципово потрібна лише одна унікальна IP-адреса, щоб репрезентувати цілу групу станцій. NAT часто використовується зі спеціальною групою приватних IP-адрес (див. табл. 3.4), однак може працювати з довільною схемою адресації IP. В основному NAT здійснює трансляцію (відображення) IP-адрес, встановлюючи їх відповідність одна одній (так звана схема $1\rightarrow1$) або відповідність багатьох адрес одній (схема $n\rightarrow1$). Відображення внутрішньої (локальної) IP-адреси на зовнішню (глобальну) адресу означає, що внутрішня IP-адреса замінюється відповідною зовнішньою і навпаки.

Внутрішня мережа – це звичайно локальна мережа організації (LAN), яку прийнято називати *доменом-відгалуженням* (*stub domain*). Організація має блок IP-адрес від свого надавача послуг Internet (ISP). Цей блок містить зареєстровані в IANA унікальні IP-адреси, які прийнято *називати внутрішніми глобальними адресами*. Внутрішні глобальні адреси використовуються окремими станціями з домену-відгалуження, які систематично комунікуються з зовнішніми мережами, і не потребують трансляції адрес. Станції, які мають незареєстровані IP-адреси, обов’язково мусять застосовувати NAT для комунікації з зовнішнім світом. Ці незареєстровані IP-адреси ділять на дві групи. Менша група – *зовнішні*

локальні адреси використовується раутером NAT. Друга, значно більша група, відома як *внутрішні локальні адреси* використовується тільки всередині домену-відгалуження. Більшість станцій в домені-відгалуженні комунікуються з використанням внутрішніх локальних адрес. Зовнішні локальні адреси застосовуються для трансляції зареєстрованих унікальних IP-адрес, тобто *зовнішніх глобальних адрес* пристроїв зовнішньої мережі.

Внутрішня локальна адреса (*Inside Local – IL*) – IP-адреса, призначена станції, розміщеній у внутрішній мережі. Такі адреси можуть бути глобально унікальними, виділеними з приватного адресного простору, визначеного RFC 1918, або можуть бути офіційно виділені деякій іншій організації.

Внутрішня глобальна адреса (*Inside Global – IG*) – IP-адреса внутрішньої станції, якою вона виявляється назовні. Такі адреси також можуть бути виділені з приватного адресного простору, визначеного RFC 1918, або можуть бути офіційно виділені іншій організації, або бути виділеними з глобально-унікального адресного простору, що звичайно забезпечують ISP (якщо організація під'єднана до Internet.

Зовнішня локальна адреса (*Outside Local - OL*) – IP-адреса зовнішньої станції, якою вона виявляється у внутрішній мережі. Ці адреси можуть бути виділені з приватного адресного простору RFC 1918.

Зовнішня глобальна адреса (*Outside Global – OG*) – IP-адреса, призначена станції, розташованій у зовнішній мережі.

NAT може бути сконфігурована різним чином. Для зрозуміння суті трансляції мережевих адрес розглянемо типову ситуацію використання різних IP-адрес в локальній мережі одної організації, коли раутер NAT сконфігурований для трансляції незареєстрованих (внутрішніх) IP-адрес у зареєстровані (зовнішні) IP-адреси.

Якщо станція з домену-відгалуження має внутрішню локальну IP-адресу і потребує комунікуватися з зовнішніми мережами, то пакет висилається до раутера NAT.

Раутер NAT перевіряє свою таблицю раутінгу для встановлення наявності входу для адреси призначення. Якщо такий вхід наявний, то раутер транслює адресу пакету і створює вхід для неї в таблиці трансляції адрес. Якщо адреса призначення відсутня в таблиці раутінгу, то пакет знищується.

Раутер висилає пакет до призначення, вживаючи внутрішню глобальну адресу.

Якщо станція з публічної мережі висилає пакет до приватної мережі, то адреса джерела – це зовнішня глобальна адреса, а адреса призначення – внутрішня глобальна адреса станції-призначення в домені-відгалуженні.

Отримавши такий пакет, раутер NAT визначає наявність цієї внутрішньої глобальної адреси в таблиці трансляції адрес.

Раутер транслює внутрішню глобальну адресу пакету у внутрішню локальну адресу станції-призначення і висилає пакет до цієї станції.

Трансляція мережевих адрес включає такі кроки:

IP-адреса в заголовку IP-пакету замінюється новою внутрішньою або зовнішньою адресою. Номер порта в заголовку пакету TCP або UDP замінюється новим портом, якщо потрібна *трансляція номерів портів*.

Контрольна сума IP-пакету перераховується і контролюється на цілісність.

Контрольна сума заголовка TCP також перераховується, оскільки вона обчислюється з використанням нової внутрішньої або зовнішньої IP-адреси, нового номера порта (якщо він використовується) і корисного навантаження.

Існують два типи NAT – статична і динамічна.

12.Статична і динамічна NAT.

12.1. Статична NAT.

Статична NAT визначає статично сконфігуровану (фіксовану) трансляцію внутрішніх локальних і глобальних адрес з відповідністю 1→1. На рис. 12.1 показано приклад статичної трансляції внутрішніх локальних адрес 10.1.1.13 і 10.1.1.27 у внутрішні глобальні адреси 206.245.160.13 та 206.245.160.27 відповідно. Ситуація, показана на рисунку, відповідає висиланню пакету від клієнта, визначеного парою <IP-адреса: порт>, до сервера, визначеного іншою парою <IP-адреса: порт>; наприклад, клієнт 10.1.1.13:1108 пересилає пакет до FTP-сервера 207.135.89.111:21, а клієнт 10.1.1.27:1101 – до Web-сервера 207.135.89.15:80. З боку зовнішнього середовища клієнти мають адреси джерела, замінені відповідно до таблиці статичної трансляції. Відзначимо, що як внутрішня, так і зовнішня мережі мають мережевий префікс /24, і перетворюється лише мережева частина адреси, а номер станції залишається незмінним.

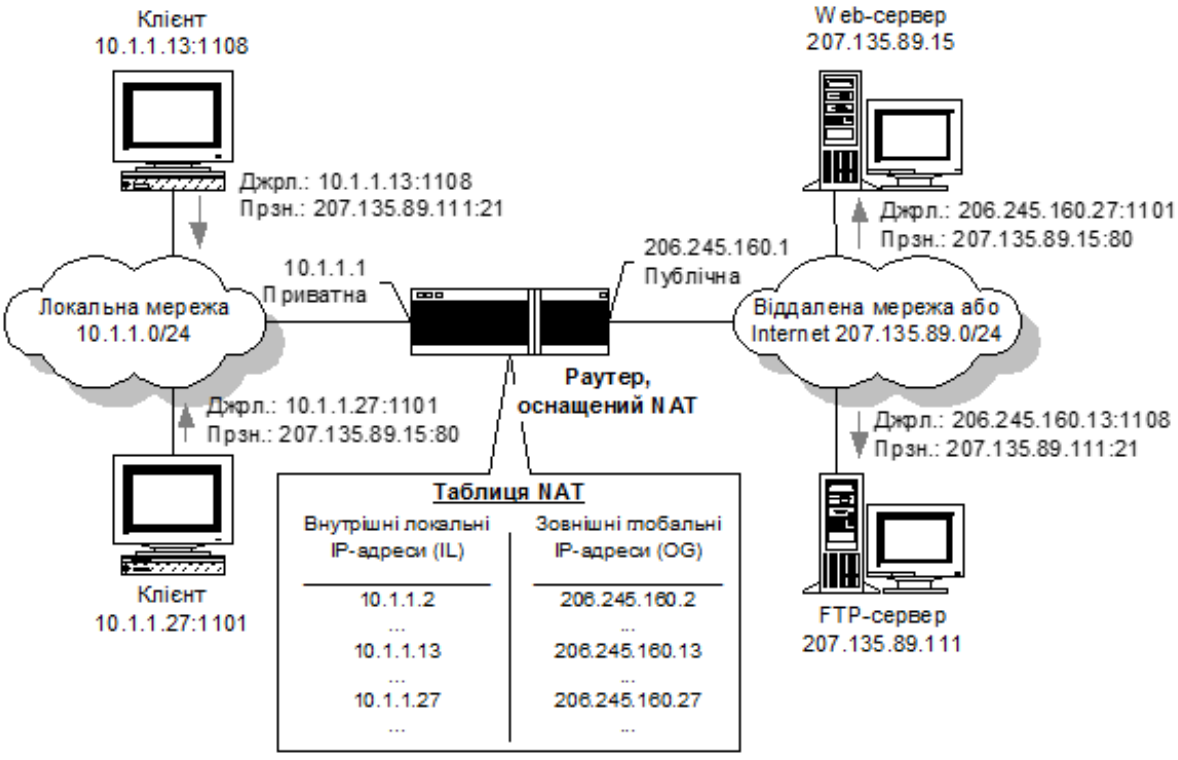


Рис. 12.1. Приклад статичної NAT.

За особливих обставин статична NAT, яку тоді також називають *вхідним відображенням* (*inbound mapping*) може дозволити зовнішнім пристроям зініціювати сполучення зі станцією в домені-відгалуженні. Наприклад, якщо потрібно перейти від внутрішніх глобальних адрес до визначених внутрішніх локальних адрес, які призначені Web-серверу домену-відгалуження, то статична NAT може забезпечити сполучення.

12.2. Динамічна NAT.

Динамічна NAT здійснює трансляцію з пулу внутрішніх локальних IP-адрес у пул внутрішніх глобальних IP-адрес, якщо це потрібно. Обидва пули адрес повинні бути визначені користувачем. Призначення адрес здійснюється раутером, оснащеним NAT, автоматично, динамічно будуючи таблицю NAT. Сполученням, ініційованим станціями з приватної мережі, призначаються публічні адреси з відповідного пулу. Користувач не має впливу на те, яка IP-адреса підібрана з адресного пулу. Доки приватна станція має вихідне сполучення, вона може бути досягнена вхідним пакетом, висланим за цією публічною адресою. Коли сполучення завершене, пов’язання адрес припиняється і адреса повертається до пулу для подальшого використання. Щоб пришвидшити конфігурування, можна відображати діапазон IP-адрес. На рис. 12.2 показано приклад динамічної NAT між локальним і віддаленим адресними пулами.

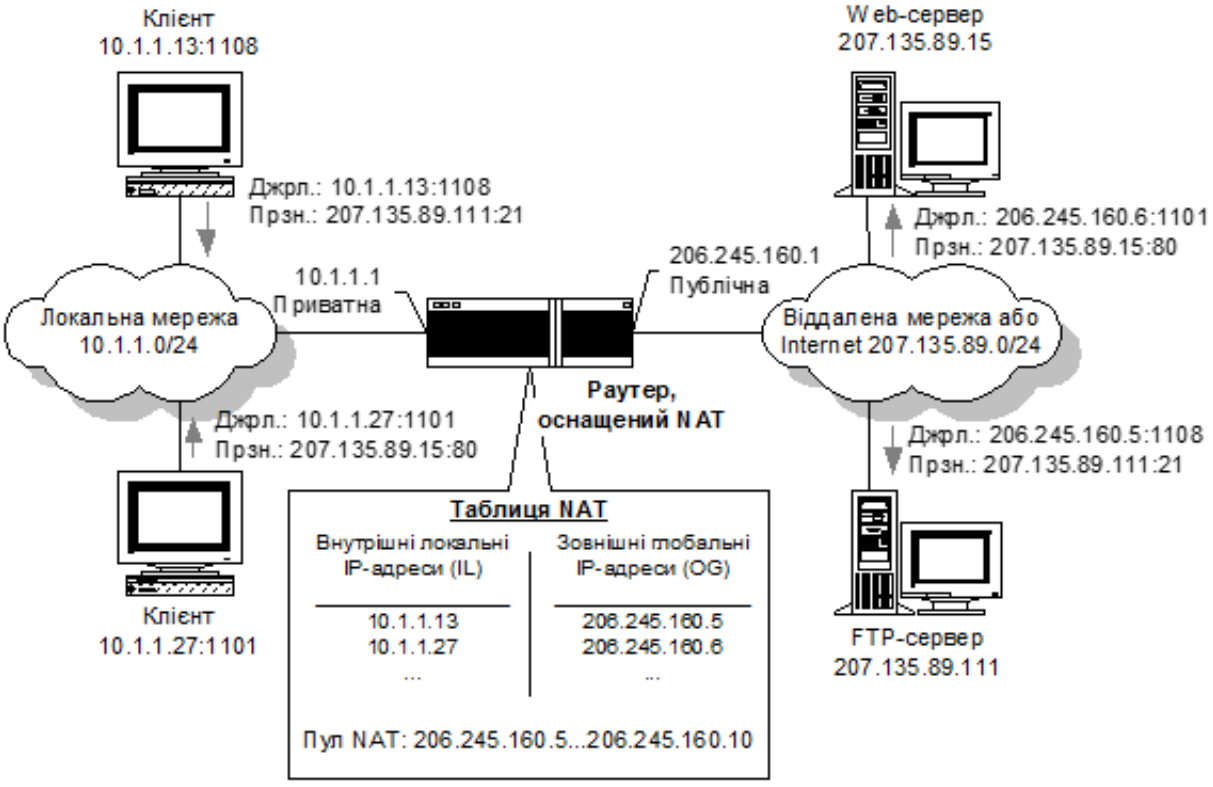


Рис. 12.2. Приклад динамічної NAT між локальним і віддаленим адресними пулами.

Динамічна NAT працює таким чином.

- Внутрішня мережа (домен-відгалуження) має незареєстровані IP-адреси, які не маршрутуються у зовнішньому середовищі, оскільки вони не є унікальними.
- Організація має раутер, оснащений NAT. Цей раутер має блок унікальних IP-адрес, зареєстрованих IANA.
- Станція у домені-відгалуженні потребує з'єднатися зі станцією зовні мережі організації, наприклад, з віддаленим Web-сервером.
- Раутер приймає пакет від станції в домені-відгалуженні.
- Раутер зберігає немаршрутовану IP-адресу станції-надавача в таблиці трансляції IP-адрес і замінює цю адресу першою наявною IP-адресою з блоку унікальних IP-адрес. Таблиця трансляції адрес тепер відображає немаршрутовану IP-адресу на узгоджену унікальну IP-адресу.
- Коли пакет-відповідь повертається від станції-призначення, раутер перевіряє адресу призначення в пакеті та контролює наявність такої адреси в таблиці трансляції адрес, щоб встановити, чи пакет адресований до станції в домені-відгалуженні. Далі раутер замінює адресу призначення в пакеті на відповідну адресу, яка зберігається в цій таблиці, і висилає пакет до станції. Якщо адреса призначення відсутня в таблиці, то пакет знищується.

Динамічна NAT більш складна, бо стани повинні обслуговуватися і сполучення повинне були вилучене, коли пул вичерпано і вільних адрес немає. Але, на відміну від статичної NAT, динамічна NAT дозволяє повторне використання адрес, зменшуючи потребу в легально зареєстрованих публічних адресах. Впровадження динамічної NAT автоматично створює "пожежну стінку" (firewall) між внутрішньою мережею організації та зовнішніми мережами. NAT дозволяє тільки сполучення, ініційовані зсередини домену-відгалуження. Це означає, що станція зі зовнішньої мережі не може з'єднатися зі станцією у внутрішній мережі якщо остання не зініціювала сполучення. Користувачі з домену-відгалуження можуть мати доступ до зовнішніх Web-серверів і отрмувати файли, наприклад, з допомогою FTP, однак будь-хто зовні не може отримати IP-адресу станції з домену-відгалуження і використати її для сполучення.

13.IP – данограма та її формат.

13.1. Концепція пересилання данограм.

Протокол internet (*Internet Protocol – IP*) – це основний робочий протокол в стеку TCP/IP. Всі протоколи вищих рівнів - TCP, UDP, TCP, ICMP, пересилають інформацію у вигляді IP-данограм. Більшість фундаментальних міжмережевих послуг базується на системі доручення пакетів. Послуга доручення данограм називається *ненадійною* (*unrealiable*), бо доручення не гарантоване - пакет може бути втрачений, повторений або доручений не в потрібній послідовності. Така послуга називається *послугою без встановлення сполучення* (*connectionless*). Послідовність пакетів від одного комп'ютера до іншого може пересилатися різними шляхами і одні

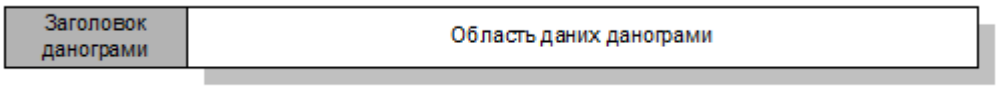
пакети можуть бути втрачені, тоді як інші будуть доручені. Нарешті, послугу називають такою, що застосовує *найкраще можливе доручення,* оскільки програмне забезпечення здійснює зусилля для доручення пакетів.

IP-протокол забезпечує *три важливі визначення*:

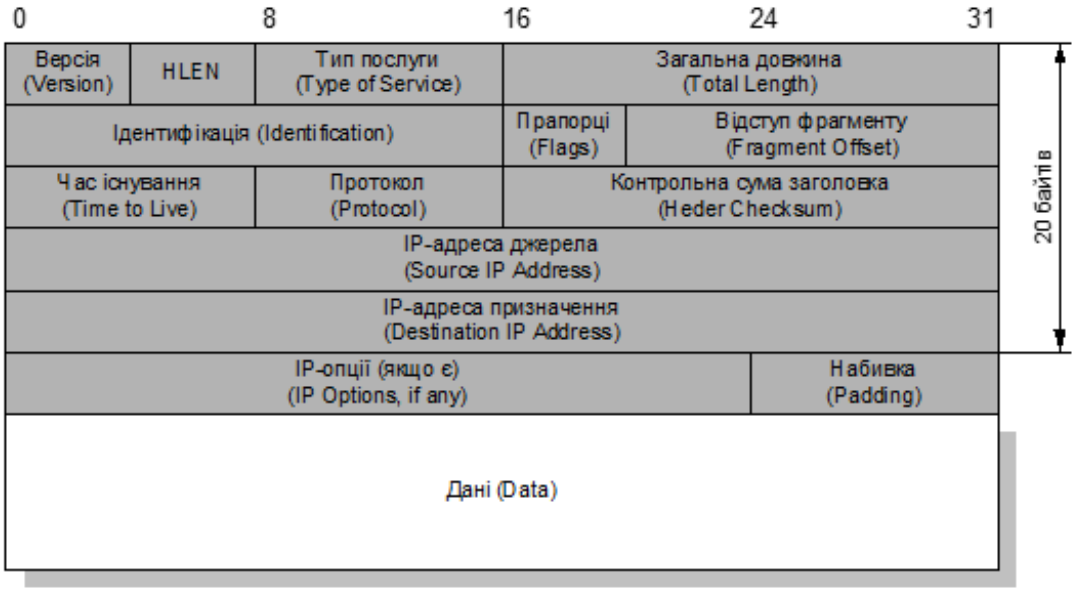
- IP-протокол визначає базисну одиницю передачі даних через TCP/IP, тобто специфікує точний формат для всіх даних;
- програмне забезпечення IP здійснює функцію *маршрутизації (routing),* визначаючи шлях, через який можуть передаватися дані;
- IP включає систему правил, які втілюють ідею *ненадійного* передавання пакетів. Ці правила характеризують як вузли та раутери повинні обробляти пакети, як і коли повинні генеруватися повідомлення про помилки, умови, при яких пакети можуть бути знищені.

13.2. IP-данограма та її формат.

Основна одиниця передавання в протоколі IP називається internet-данограмою (internet-datagram) або IP-данограмою чи просто данограмою (рис. 13.1):



а) загальний вигляд данограми;



б) поля данограми.

Рис. 13.1. IP-данограма.

Звичайно (коли IP-опції відсутні), розмір IP заголовку становить 20 байт. Через мережу IP данограма передається в такому порядку: біти 0-7, 8-15, потім 16-23 і 24-31, і так далі. Цей порядок пересилання дістав назву “мережевий порядок байтів” (network byte order).

Опис полів заголовку IP-данограми наведений нижче в таблиці:

VERS (version)	Версія IP протоколу, поточна версія 4;
HLEN (header length)	Довжина IP заголовку в 32-х розрядних словах. Максимальна довжина IP заголовку може становити 15×4 = 60 байтів. Якщо IP-опції відсутні, то тут зберігається значення 5, тобто мінімальна довжина IP-заголовку становить 5×4=20 байтів.

SERVICE TYPE (TOS - type of service)	Тип сервісу який вимагає IP даграма, містить:
	• старші 3 біти - приорітет IP даграми, може приймати значення від 000 до 111, ці значення на сьогодні ігноруються більшістю протоколів;
	• наступні 4 біти - кожен біт вказує тип сервісу:
	  • мінімальна затримка передавання;
	  • максимальна продуктивність передавання;
	  • максимальна надійність передавання;
	  • мінімальні кошти передавання.
	Тільки один біт може бути встановлений в 1. Якщо всі біти рівні 0, то це відповідає звичайному сервісу.
	• останній біт - не використовується і має бути рівний 0.

TOTAL LENGTH	Повна довжина IP даграми в байтах, максимально 64К=65535=2^{16} бітів.
IDENTIFICATION	Унікальний ідентифікатор кожної IP-даграми, використовується при фрагментації та копіюється в заголовки фрагментів.
FLAGS	Бере участь в процесі фрагментації, див. IP-фрагментація.
FRAGMENT OFFSET	Бере участь в процесі фрагментації, див. IP-фрагментація.
TIME TO LIVE (TTL)	Своєрідний час існування IP-даграми, який визначає максимальну кількість маршрутизаторів через які даграма може перейти. TTL зменшується на 1 при кожному проходженні через маршрутизатор (*лічильник стрибків як метрика –hop count metric*). Коли TTL стає рівне 0, то IP даграма знищується маршрутизатором і у відповідь до її джерела посилається ICMP-повідомлення про помилку. Це зроблено для того, щоб запобігти утворенню “вічних петель”. Якщо затримки при передачі дуже великі (співмірні секунді), то TTL трактується як час життя в секундах (*часова метрика – time metric*). Наприклад якщо час від отримання даграми до її висилання маршрутизатором становив 2 секунди, то маршутизатор зменшує TTL на 2. Початкове значення TTL повинне бути встановлене протоколом вищого рівня.
PROTOCOL	Номер протоколу вищого рівня, від якого IP-рівень дістав дані для пересилання (TCP чи UDP). На основі значення цього поля проводиться демультиплексування IP даграм на приймальному кінці. Окремі важливі значення цього поля: 0 – зарезервовано; 1 – протокол повідомлень для управління Internet (Internet Control Message Protocol – ICMP); 2 – протокол управління групами Internet (Internet Group Management Protocol – IGMP); 3 – протокол шлюз-шлюз (Gateway-to-Gateway Protocol – GGP) 4 – IP (IP-інкапсуляція); 5 – потік; 6 – протокол управління пересиланням (Transmission Conrol Protocl – TCP); 8 – зовнішній шлюзовий протокол (Exterior Gateway Protocol – EGP); 9 – приватний внутрішній протокол раутінгу (Private Interior Routing Protocol – PIRP) 17 – протокол даграм користувача (User Datagram Protocol – UDP); 89 – протокол “відкритий – першим найкоротший шлях” (Open Shortest Path First – OSPF)

HEADER CHECKSUM (FCS)	Контрольна сума IP заголовку, яка не охоплює даних IP-данограми. Протоколи ICMP, IGMP, UDP та TCP мають свої власні контрольні суми, які охоплюють їх заголовки та дані. Контрольна сума обчислюється так: спочатку FCS встановлюється рівною 0, потім сумуються всі 16-ти розрядні слова заголовку, далі шукається доповнення до 0xFFFF, яке записується в поле FCS. Якщо на приймальній стороні на підставі FCS виявляється помилка, то IP-данограма просто знищується та у відповідь не генерується ніякого повідомлення.
SOURCE IP ADDRESS	32-розрядна IP-адреса джерела IP-данограми.
DESTINATION IP ADDRESS	32-розрядна IP-адреса призначення IP-данограми.
IP OPTIONS	Поле змінної довжини (від 0 до 40 байтів), у якому вказують додаткові послуги, які використовує IP данограма; деякі з них це: • захист і контроль обмежень; • запис маршруту (кожен маршрутизатор записує свою IP адресу в поле опцій); • часова відмітка (кожен маршрутизатор записує свою IP адресу і свій час); • частковий маршрут (вказуються адреси маршрутизаторів через які має пройти IP данограма); • точний маршрут (задаються всі адреси маршрутизаторів, через які, і тільки через які має пройти IP данограма); Довжина поля опцій завжди повинна бути кратна 32-розрядному слову.
PADDING	Байт(и) набивки, присутні тоді, коли поле опцій не є кратним 32- розрядному слову, значення бітів рівні 0.
DATA	Дані IP данограми, які є інформацією, наданою для пересилання протоколом вищого рівня, визначеним полем *протокол*.

13.3. Опції данограми.

Від IP-впроваджень не вимагається здатність генерувати опції в данограмах, які вони створюють, але всі IP-впровадження повинні бути здатні обробляти данограми, які містять опції. Поле опції має змінну довжину. Опції можуть бути відсутні, або їх може бути багато. Існують два формати опцій. Формат кожної опції визначається за значенням номера опції (Option Number), який міститься у першому байті - октеті типу опції (Option Type). Перший формат передбачає тільки октет тип опції, другий – октет тип опції, октет довжини і систему октетів даних.

Октет типу опції має однакову структуру в обидвох випадках і поділений на три поля (рис. 13.2).

Поле *копіювання* (COPY) вказує раутеру, як поводитися при фрагментації:

- COPY = 1 - опція копіюється у всі фрагменти;
- COPY = 0 - опція копіюється тільки у перший фрагмент.

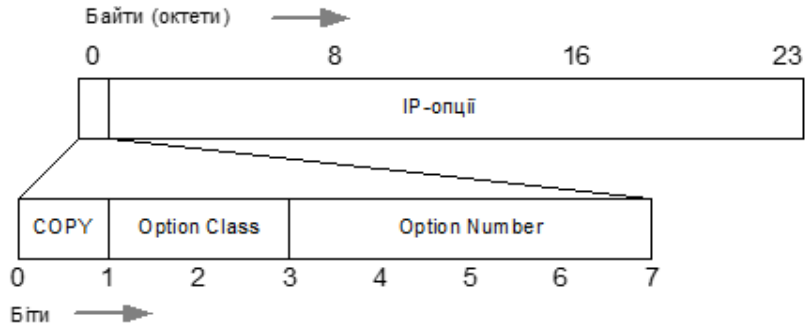


Рис. 13.2. Поле типу опції в загальному полі Option.

Поля *клас опції* (OPTION CLASS) і *номер опції* (OPTION NUMBER) визначають загальний клас опцій і конкретну опцію у цьому класі:

Клас опції	**Значення**
0	Данограма або контроль мережі
1	Зарезервовано для майбутнього вжитку
2	Відлагодження або вимірювання
3	Зарезервовано для майбутнього вжитку

Клас опції	Номер опції	Довжина	Опис
0	0	-	Кінець списку опцій. Використовується, якщо опції не закінчуються точно в кінці заголовка (див. поле PADDING)
0	1	-	Нема операції (використовується для вирівнювання октетів в списку опцій)
0	2	11 + 8 байтів	Рівень захисту та контроль обмежень (для захищених застосувань)
0	3	змінна	Вільний раутінг від джерела. Використовується для маршруту данограми вздовж визначеного шляху. Детальніше нижче.
0	7	змінна	Запис маршруту: збирання інформації про маршрут з міжмережевого інтерфейсу. Використовується при трасуванні маршруту. Детальніше нижче.
0	8	4 + 1 байт	Ідентифікатор потоку. Використовується для переносу ідентифікатора потоку SATNET.
0	9	змінна	Жорсткий раутінг від джерела. Використовується для маршруту данограми вздовж шляху, визначеного джерелом.
2	4	змінна, до 40 байтів	Часова відмітка (timestamp) в об’єднанні мереж: сумарний час (в мс) для міжмережевого інтерфейсу. Вживається до запису даних про сумарний час вздовж маршруту.

Опції раутінгу IP-данограми Поле опції дозволяє джерелу IP-данограми використати два методи для точного забезпечення раутінгової інформації і один метод для визначення маршруту IP-данограми.

Вільний раутінг від джерела. Ця опція (*Loose Source Routing* або *Loose Source and Record Route - LSRR*) забезпечує джерелу IP-данограми засіб для точної раутінгової інформації, яка буде використана раутерами при пересиланні данограми до призначення і для запису маршруту. Значення полів для цієї опції наведені в таблиці нижче:

1000011 (десяткове 131)	Значення байта *тип опції* для вільного раутінгу від джерела
довжина (*length*)	Містить довжину цього поля опції включно із полями *тип* і *довжина*
вказівник (*pointer*)	Вказує на дані опції для наступної IP-адреси, яка буде оброблятися. Обчислюється відносно початку опції, так що мінімальна довжина дорівнює 4. Якщо вказівник більший від довжини опції, то кінець маршруту від джерела досягнений і подальший раутінг базується на IP-адресі призначення (як для данограм без цієї опції).
дані маршруту (*route data*)	Це послідовність 32-бітових IP-адрес

Коли данограма досягає призначення і маршрут від джерела не порожній (*вказівник* < *довжина*), то приймальна станція може:

- Взяти наступну IP-адресу із поля *дані маршруту* (позначену *вказівником*) і помістити її у поле *адреси призначення* данограми.
- Помістити локальну IP-адресу у список джерела на місце, відзначене *вказівником*. IP-адреса для цього є локальною IP-адресою, відповідною мережі, до якої може бути вислана данограма (раутери під’єднані до багатьох фізичних адрес і тому мають багато IP-адрес).
- Збільшити *вказівник* на 4.
- Переслатити данограму до нової адреси призначення.

Ця процедура гарантує, що зворотній маршрут записується в дані маршруту (у зворотньому порядку), так що кінцевий приймач використовує ці дані для побудови вільного маршруту від джерела у зворотньому напрямку. Це *вільний* маршрут від джерела, бо раутер, який висилає данограму, може використати довільний маршрут і будь-яку кількість проміжних раутерів для досягнення наступної адреси в маршруті.

14.Інкапсуляція, фрагментація та реасемлювання данограм.

14.1. Інкапсуляція данограми.

Коли данограма поширюється від одної станції до іншої, то вона може перетинати межі різних фізичних мереж. Для розуміння наступних полів данограми важливо розглянути, як пакети-*данограми* співвідносяться з пакетами-*рамками* фізичної мережі. Ідея пересилання однієї данограми в одній мережевій рамці називається *упакуванням* або *інкапсуляцією (encapsulation)* (рис. 14.1).

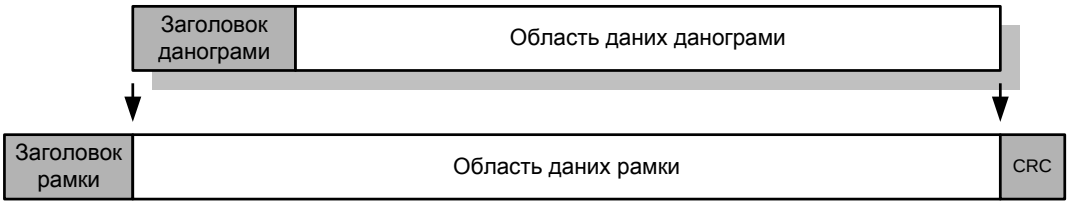


Рис. 14.1. Інкапсуляція данограми.

14.2. Фрагментація данограми.

В ідеальному випадку IP-данограма розміщається всередині однієї фізичної рамки. Мережеве обладнання звичайно накладає обмеження на довжину даних: Ethernet обмежує дані до 1500 байт, FDDI - приблизно до 4470 байт. Це обмеження називають *максимальним блоком для пересилання* (*Maximum Transfer Unit ~ MTU*). Кожен мережевий інтерфейс має відповідне значення MTU. Коли IP-рівень потребує передати данограму, розмір якої більший від MTU, то відбувається процес *IP-фрагментації*, тобто розбиття даних на частини (*фрагменти*).

Програмне забезпечення TCP/IP створює можливість для поділу довгої данограми на менші частини, якщо данограма передається через мережу із занадто малим MTU. Фрагментація може відбуватися як на комп'ютері, який є джерелом IP-данограми, так і на проміжному маршрутизаторі. Фрагментована данограма не збирається в одне ціле, аж поки не досягне свого місця призначення. Окремий фрагмент данограми є цілком незалежною IP-данограмою зі своїм IP-заголовком і маршрутизується незалежно від інших фрагментів, тобто фрагменти можуть приходити до джерела різними шляхами і не в тому порядку, як їх було відіслано, крім того, фрагментація може відбуватися неодноразово.

Нагадаємо які поля IP-заголовку використовуються при фрагментації:

IDENTIFICATION	Унікальний номер кожної IP данограми, він копіюється у кожний фрагмент при фрагментації для ідентифікації фрагментів при збиранні данограми в пункті призначення.
FLAGS	Два молодші біти з трьох контролюють фрагментацію. Один з бітів (*more fragments - MF*) вказує на те, що це не останній фрагмент, тобто очікується прийняття як мінімум ще одного фрагменту. Другий з бітів (*don't fragment - DF*) використовується для того, щоб позначити IP-данограму, яку не можна піддавати фрагментації. Коли при пересиланні

	такої данограми фрагментація все ж необхідна, то у відповідь до її джерела генерується ICMP-повідомлення про помилку.
FRAGMENT OFFSET	Використовується при фрагментації і означає відступ в оригінальній данограмі для даних, які передаються у фрагменті, від початку даних нефрагментованої IP-данограми; визначається числом, кратним 8 байтам. Для першого фрагенту або для нефрагментованої данограми це значення завжди дорівнює 0. Щоб здійснити реасемблювання, адресат повинен отримати всі фрагменти, починаючи від фрагменту з відступом 0 до фрагменту з найбільшим відступом.
TOTAL LENGTH	Вказує на довжину фрагменту.

Фрагментацію звичайно здійснює раутер, який з'єднує мережу з більшим MTU з мережею, в якій MTU менший, ніж довжина данограми. Довжина фрагменту повинна бути кратною 8 байтам (див. FRAGMENT OFFSET), останній останній фрагмент звичайно коротший. Щоб можна було відновити копію оригінальної данограми перед її подальшим опрацюванням у місці призначення, фрагменти повинні бути *реасембльовані (reassembled)*.

Протокол IP вимагає, щоб кожне сполучення мало MTU, не менший від 68 байтів, так що коли будь-яка мережа передбачає менше значення від вказаного (наприклад, мережа ATM має довжину комірки 53 байти, з яких 48 відведені для поміщення даних), то фрагментація і реасемблювання мусять бути вбудовані в мережевий інтерфейс у спосіб, прозорий для IP. 68 байтів – це сума максимальної довжини IP-заголовка (60 байтів) і мінімально можливої довжини даних у фрагменті, крім останнього (8 байтів). Маршрутизатор завжди повинен сприймати данограми з довжиною, яка не перевищує MTU мережі, до якої він під'єднаний, і завжди повинен опрацьовувати нефрагментовані данограми довжиною до 576 байтів. Хоч протокол IP не вимагає обслуговування нефрагментованих IP-данограм, довших від 576 байтів, однак конкретні впровадження IP-протоколу можуть працювати із довжинами 8192 байти і більше, і рідко працюють із меншими від 1500 байтів. Станції також повинні сприймати і при потребі реасемблювати данограми довжиною щонайменше 576 байтів.

Фрагменти данограм мають той самий формат, як данограми, за вийнятком поля FLAG, яке вказує, що це фрагменти.

15.Сервіси Internet.

15.1. Структура мережі Internet.

Хоча Internet і не є єдиною глобальною мережею, в практиці спілкування поняття Internet означає взагалі всі мережі (а швидше – ресурси) за межами нашої локальної мережі. Тому ми говоритимемо про сервіси глобальних мереж загалом, незалежно від того, де фізично знаходиться

потрібний нам ресурс чи сервер. Структуру підключення користувачів до мережі Internet наведено на рис. 15.1.

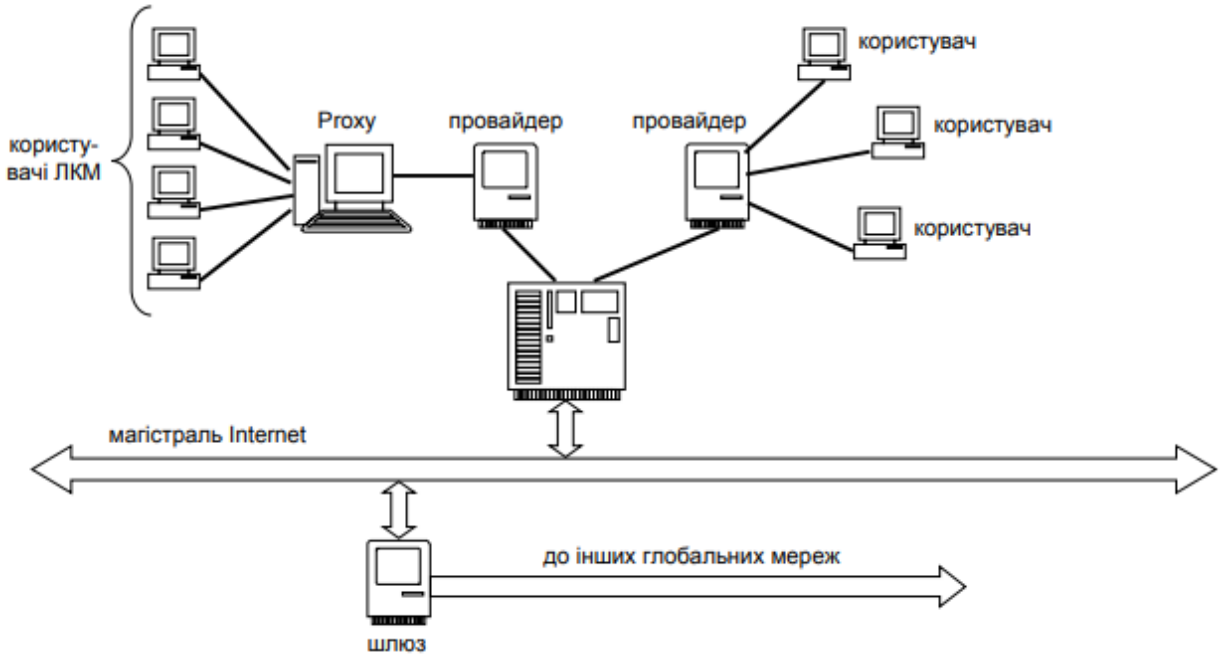


Рис. 15.1. Структура підключення користувачів до мережі Internet.

Магістраль - це лінії зв'язку, які можуть бути кабельними (здебільшого так воно і є), чи супутниковими радіолініями. Зі схеми рис. 15.1 видно, що магістраль з'єднує між собою вузли мережі (хости). До хостів підключаються сервери провайдерів - організацій, які надають послуги з доступу до Internet. До серверів провайдерів підключаються або індивідуальні користувачі (на схемі - справа), або через власні проксі - сервери (proxy-server) - колективні користувачі (локальні чи корпоративні мережі). Доступ до ресурсів інших глобальних мереж (FidoNET, BitNET, CompuServe тощо) здійснюється через спеціальні комп'ютери-шлюзи.

Для організації зв'язку між двома комп'ютерами в глобальній мережі, кожний з них повинен мати унікальне позначення. Таким позначенням є IP-адреса комп'ютера. IP-адреса – це комбінація з чотирьох чисел, розділених крапками, наприклад: 104.17.126.10. Кінцевим користувачам незручно працювати з такими числовими адресами, тому їм пропонується звична система так званих доменних імен – DNS (Domain Name System). DNS – це комбінація з імен доменів (підмереж) на шляху до комп'ютера, розділених крапками. Наприклад адреса uzhnu.edu.ua – адреса Ужгородського національного університету (uzhnu), який знаходиться в домені верхнього рівня для освітніх установ (edu), в Україні (ua). За таким принципом побудовані більшість DNS-адрес. Для переведення DNS адрес в IP-адреси призначені DNS-сервери (тут вже Domain Name Server).

IP-адреса складається з двох компонентів: адреси мережі та адреси вузла (хоста). Межа між адресами мережі і вузла рухома. Адреса мережі може займати 3, 6 або 9 розрядів. Решта – адреса вузла (табл. 15.1).

Таблиця 15.1. Типи мереж.

Клас мережі	Значення першого байта	Формат адреси мережі	Формат адреси вузлів	Кількість мереж	Кількість вузлів
A	1-126	w	x.y.z	126	16777214
B	128-191	w.x	y.z	16384	65534
C	192-223	w.x.y	z	2097151	254

Примітки: 1. Адреси з номером мережі 127 зарезервовані для тестової перевірки наявності зв'язку з собою (loop back) та перевірки функціонування міжпроцесорних зв'язків.

2. Адреси мереж з номерами 224 і вище призначені для спеціальних протоколів і їх не можна використовувати.

3. Позначення 192.168.y.z зарезервоване для локальних мереж.

4. Значення 255 використовується в масках мереж.

Маска мережі – це узагальнене представлення адреси вузла у мережі. Таким чином, в мережі класу A вузли мають маску 255.0.0.0, в мережі класу B – маску 255.255.0.0, а в мережі класу C – маску 255.255.255.0. Локальні мережі - це мережі класу C. Останній елемент DNS-адреси означає або тип організації (стара система позначень), або країну, де знаходиться абонент. Відповідність останнього елементу адреси типу організації або країні наведена в табл. 15.2.

Таблиця 15.2. Домени деяких типів організацій і країн.

Типи організацій		Країни			
com	Комерційні	us	США	hk	Гонконг
edu	Навчальні	fr	Франція	mx	Мексика
gov	Урядові	ca	Канада	au	Австрія
mil	Військові	dk	Данія	hu	Угорщина
net	Провайдери	de	Німеччина	ua	Україна
org	Неприбуткові	ch	Чехія	pl	Польща
int	мінародні	se	Швеція	fi	Фінляндія
		jp	Японія		

Кожний ресурс в глобальній мережі також повинен мати унікальне позначення, для чого використовується універсальний локатор ресурсів – URL (Uniform Resource Locator). Таке позначення складається з трьох частин:

1. Позначення служби (сервісу), що забезпечує доступ до ресурсу.
2. DNS-адреса комп'ютера, на якому знаходиться ресурс.
3. Повна назва ресурсу на комп'ютері, де він знаходиться.

Основним постачальником послуг (сервісів) доступу до глобальних мереж є провайдери. Хороший провайдер забезпечує самостійно або через спеціалізованих підрядників доступ до всіх сервісів Internet.

15.2. Порти.

Повний формат адреси Internet-ресурсу має такий вигляд:

{протокол}://{адреса_web-сторінки}/[#{закладка}]:[{порт}]

Зупинимось на двох поняттях, а саме: протокол і порт.

Поняття протоколу стосовно правил обміну даними в мережах було розглянуто раніше. На верхньому рівні протокольного стеку згадувались протоколи http та ftp. Тепер зупинимось на понятті "порт" стосовно технологій обміну даними в глобальних комп'ютерних мережах. Порт – одне з основних понять в обміні даними з використанням протоколів TCP/IP. В цьому випадку це ціле число, яке використовується для ідентифікації конкретного TCP-з'єднання. Для з'ясування того, чому для опису TCP-з'єднаня недостатньо лише IP-адреси, розглянемо приклад, наведений на рис. 15.2.

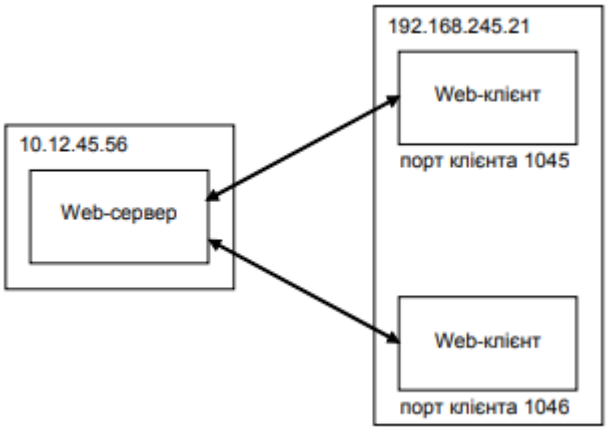


Рис. 15.2. Два клієнти з одного комп'ютера обмінюються даними з сервером.

В цьому прикладі до web-сервера, який знаходиться у вузлі з адресою 10.12.45.56, одночасно звертаються два клієнта, які знаходяться у вузлі з адресою 192.168.245.21. Це дуже поширений випадок, оскільки на одному комп'ютері може бути запущено, наприклад, два примірники браузера. Припустимо, що на вузол (комп'ютер) з адресою 10.12.45.56 надійшов інформаційний пакет, який містить http-запит. Запит передається web-серверу, який генерує відповідь. На яку адресу слід відправити цю відповідь? В цьому випадку для ідентифікації клієнтів потрібне додаткове позначення, функції якого виконує порт. Порт як частину адреси Internet-ресурсу не слід плутати з апаратним портом (COM, LPT), про які була мова в лекції 4. Аналогічна ситуація може виникнути, коли з одного вузла два клієнти передають запити до двох серверів, розміщених в одному вузлі (рис. 15.3).

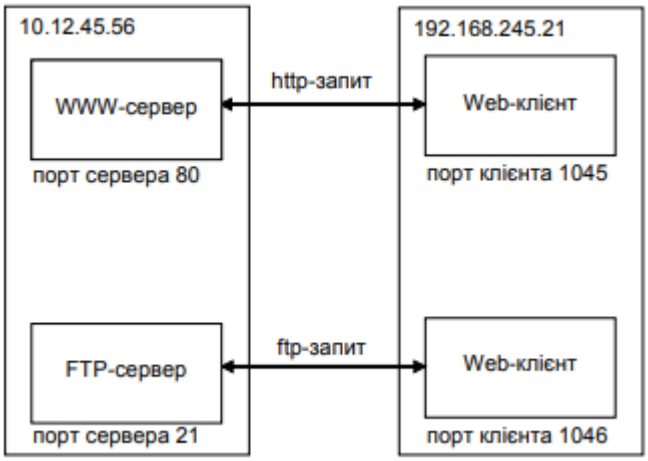


Рис. 15.3. Два клієнти з одного комп'ютера звертаються до двох серверів в одному вузлі.

Зрозуміло, що і в цьому випадку єдиним способом ідентифікації як клієнтів, так і серверів є використання номерів портів.

Сервери і клієнти використовують номери портів по-різному. За сервером конкретного типу закріплюється один номер порта. Цей номер називають стандартним портом. Він відомий усім клієнтським програмам, які використовують його підчас звертання до сервера. Застосування портів з номерами, відмінними від загально прийнятих (такий порт називають нестандартним), пов'язане з виконанням сервером спеціальних функцій.

Стандартними є наступні номери портів:

- WWW-сервери, які обмінюються даними за протоколом http, використовують порт 80;
- FTP-сервери використовують порт 21. Точніше FTP-сервери можуть використовувати порти 20 і 21, але під час встановлення зв'язку використовується порт 21;
- поштові сервери, в яких застосовується протокол SMTP, використовують порт 25.
- Telnet-сервери зазвичай використовують порт 23.

Клієнтові номер порту присвоюється на час взаємодії з сервером. За клієнтами не закріплюються конкретні номери портів. Під час встановлення зв'язку система вибирає номер порту, який в даний момент не використовується, і пов'язує його з конкретним клієнтом.

Загалом номер порту може вибиратись в межах від 1 до 65535. Для серверів прийнято виділяти номери від 1 до 1023, а для клієнтів - від 1024 до 65535. З цього правила існують і винятки. Наприклад деякі web-сервери використовують нестандартний порт з номером 8080. Proxy-сервери, які виконують функції посередників між локальними і глобальними мережами, використовують порт з номером 3128. Операційні системи, в яких застосовується графічна оболонка X Windows (Unix-подібні системи), використовують порти з номерами 6000, 6001, 6002.

Використання портів дозволяє однозначно ідентифікувати сервери і клієнти в сеансі передавання даних. Для опису з'єднання використовуються чотири параметри:

- IP-адреса сервера;
- IP-адреса клієнта;
- номер порту сервера;
- номер порту клієнта.

Останнє зауваження стосується клієнтів локальних комп'ютерних мереж. Тут слід пам'ятати те, що зв'язок усіх локальних вузлів з серверами в глобальних мережах відбувається за посередництвом proxy-сервера. Через це для вузлів глобальних мереж усі вузли локальної мережі мають одну й ту саму адресу – адресу proxy-сервера. Далі (в локальній мережі) маршрутизацію proxy-сервер здійснює власними апаратним і програмними засобами. При цьому, як уже згадувалось, для встановлення зв'язку між proxy-сервером і вузлами локальної мережі використовуються порти з номерами 8080 або 3128.

15.3. Сервіси Internet.

Кінцеві користувачі працюють в Internet, використовуючи його сервіси. Безпосереднім постачальником цих сервісів є провайдери.

Зараз Internet-технології розвиваються настільки стрімко, що нові сервіси з'являються швидше, ніж користувачі встигають їх освоювати. Однак, не дивлячись на велику загальну кількість сервісів (послуг) Internet, в основі більшості з них лежать базові сервіси, розроблені і освоєні ще в перші часи створення і розвитку глобальних мереж.

До таких сервісів можна віднести:

- WWW – доступ до гіпертекстового простору, для якого використовується протокол http. Гіпертекст – це документ, який містить посилання на інші документи. Це спосіб впорядкування інформації за допомогою зв'язків між документами. Термін уведено Т.Нельсоном 1965 року. Технологія гіпертексту забезпечує пошук заданих даних у масивах документів;
- FTP (File Transfer Protocol – протокол передачі файлів). Передавання даних між вузлами комп'ютерної мережі. При цьому використовується протокол ftp;
- DNS (Domain Name Service – сервіс доменних імен). Призначений для переведення IP-адрес у доменні і навпаки. Спочатку для цього в глобальних мережах були призначені спеціальні сервери. Згодом кожний великий сервер почав надавати таку послугу;
- Telnet – віддалений доступ. Цей сервіс дозволяв організувати доступ користувача з віддаленого комп'ютера до апаратних і програмних ресурсів іншого комп'ютера. Зараз ця послуга є інтегральною частиною, наприклад, операційної системи

Windows XP. Для її використання слід надати сторонньому користувачеві дозвіл використовувати з його комп'ютера ресурси вашого комп'ютера;

- E-Mail – електронна пошта. Передавання даних з використанням спеціальних протоколів побітової передачі даних, причому в більшості випадків для передавання використовується протокол UUCP (Unix to Unix Copy Program – програма копіювання даних з одної Unix-машини на іншу), а для приймання – протокол SMTP (Simple Mail Transfer Protocol – простий протокол передавання пошти). Останнім часом для електронної пошти почав широко використовуватись протокол POP3 (Post Office Protocol – протокол поштового офісу), який є комбінацією двох попередніх протоколів, і який в свою чергу поступово витісняється протоколом IMAP (Interactive Mail Access Protocol – протокол інтерактивного доступу до пошти);
- перелік розсилання – розсилання даних засобами електронної пошти за наперед сформованим переліком кореспондентів;
- Usenet – конференція користувачів. Обмін повідомленнями засобами електронної пошти між користувачами конференції та її організатором. Зміст повідомлень розміщується на сайті конференції в порядку їх надходження. На екран виводяться останні кілька повідомлень, але є можливість переглянути всю історію конференції. Конференція може бути модерована (керована модератором) і немодерована. Кожна конференція може мати свої специфічні правила участі, але для всіх конференцій є обов'язковим дотримання загальних правил мережевого етикету;
- IRC (Internet Relay Chat – система діалогового спілкування в Internet) – засіб ретрансляції обміну повідомленнями в режимі реального часу. Результати ретрансляції відображаються на сайті чату;
- ICQ (акронім фрази "I Seek You" - "шукаю тебе") – програма інтерактивних конференцій в Internet, розроблена 1996 року фірмою Mirabilis (Тель-Авів) і викуплена згодом фірмою AOL. Програма підтримує також електронну пошту і передавання файлів. Для використання цього сервісу потрібно, щоб усі користувачі працювали в режимі on-line;
- послуги Real Audio та Real Video - передавання потокового аудіо та відео. Послуга набула великого поширення із розширенням мережі надавачів таких потоків, а також технологій обробки аудіо та відео засобами комп'ютерних технологій.

Це, звісно, далеко не повний перелік сервісів глобальних мереж. Наприклад, тут не йшлося про блоги і підкасти, а також про низку інших поширених зараз технологій. Як було вказано раніше, більшість із них

принципово використовує базові сервіси, наведені вище. Змінюється лише форма представлення результатів.

На завершення слід відзначити, що технології стільникового зв’язку та сервіси цього зв’язку широко використовують комп’ютерні технології передавання даних. Отже, такі сервіси, як SMS, MMS, IP-телефонія, InfoStream також виникли і функціонують завдяки досягненням комп’ютерного зав’язку.

ПЕРЕЛІК ПИТАНЬ НА ІСПИТ

1. Означення локальної мережі.
2. Ознаки локальної мережі.
3. Визначення поняття «абонент».
4. Визначення поняття «сервер».
5. Визначення поняття «клієнт».
6. Визначення поняття «системний адміністратор».
7. Визначення поняття «мережевий адміністратор».
8. Визначення поняття IP-адреси.
9. Визначення поняття «патч-корд».
10. Визначення поняття «веб-інтерфейс».
11. Визначення поняття «мережевий концентратор».
12. Визначення поняття «мережевий комутатор».
13. Визначення поняття «мережевий маршрутизатор».
14. Визначення поняття «протокол».
15. Топології локальних мереж: означення, класифікація.
16. Топологія шина: означення, схема, переваги, недоліки.
17. Топологія зірка: означення, схема, переваги, недоліки.
18. Топологія кільце: означення, схема, переваги, недоліки.
19. Топологія дерево: означення, схема, переваги, недоліки.
20. Сіткова топологія : означення, схема, переваги, недоліки.
21. Топологія пункт-пункт: означення, схема, переваги, недоліки.
22. Гібридна топологія: означення, схема, переваги, недоліки.
23. Чинники, що впливають на фізичну працездатність мережі.
24. Класифікація мереж за типом функціональної взаємодії.
25. Однорангова архітектура.
26. Архітектура клієнт – сервер.
27. Типи серверів клієнт – серверної архітектури.
28. Недоліки клієнт – серверної архітектури.
29. Еталонна модель взаємодії відкритих систем (OSI).
30. Прикладний рівень OSI.
31. Рівень представлення OSI.
32. Сеансовий рівень OSI.
33. Транспортний рівень OSI.
34. Мережевий рівень OSI.
35. Канальний рівень OSI.
36. Фізичний рівень OSI.
37. Типи перетворення адрес.
38. Перетворення адрес.

39. Загальна характеристика протоколів локальних мереж.
40. Протокол локальних мереж Ethernet.
41. Протокол локальних мереж Token Ring.
42. Повнокласова адресація.
43. Визначити термін: TCP/IP.
44. Визначити термін: раутер.
45. Визначити термін: PPTP.
46. Визначити термін: L2TP.
47. Визначити термін: Open VPN.
48. Визначити термін: IPSec.
49. Визначити термін: Firewall.
50. Визначити термін: PAP (MSPAP).
51. Визначити термін: CHAP (MSCHAP).
52. Визначити термін: PPPoE.
53. Визначити термін: «звита пара».
54. Потреба в проектуванні IP-мереж.
55. Методика проектування мереж.
56. Етапи проектування мережі.
57. Загальна структура IP-адрес та їх класи.
58. Характеристика IP адрес різних класів та спеціальні IP адреси.
59. Структура IP-адрес при повнокласовій адресації.
60. Використання мережевої маски.
61. Безкласова міждоменна маршрутизація CIDR.
62. Розділення мереж на під мережі: загальні принципи та поняття розширеного мережевого префіксу.
63. Розділення IP мереж на під мережі.
64. Спосіб розбиття мережі на під мережі (якщо задана необхідна кількість вузлів у кожній підмережі $N_{\text{вузл.підм.}}$).
65. Мережеві маски змінної довжини.
66. Вимоги щодо впровадження VLSM, Алгоритм пересилання, базований на “найдовшому узгодженні”.
67. Трансляція мережевих адрес.
68. Статична NAT.
69. Динамічна NAT.
70. Концепція пересилання данограм.
71. IP-данограма та її формат.
72. Інкапсуляція.
73. Фрагментація.

Література

1. Кулаков Ю. О., Луцький Г. М. Комп'ютерні мережі: Підручник / За ред. Ю. С. Ковтанюка. – К.: Юніор, 2003. – 400 с.
2. Гаевский А. Основы работы в Интернете. – СПб.: БХВ – Петербург, 2003. – 127 с.
3. Основи інформаційних систем: Навч. Посібник. – Вид. 2-ге, перероб. і доп. / В.Ф. Ситник, Т.А. Писаревська, Н.В. Єрьоміна, О.С. Краєва; За ред. В.Ф. Ситника. – К.: КНЕУ, 2001. – 420 с.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Ученик для вузов. – СПб.: Питер, 2010.
5. Олифер В.Г., Олифер Н.А. Операционные системы компьютерных сетей. – СПб.: Питер, 2008.
6. Кульгин М. Технологии корпоративных сетей: Энциклопедия. – СПб.: Питер, 2000.
7. Столингс В. Современные компьютерные сети. – СПб.: Питер, 2003.
8. Куроуз Дж., Росс К. Компьютерные сети. – СПб.: Питер, 2004.
9. Андэрсон К., Минаси М. Локальные сети. Полное руководство: Пер. с англ. – К.: ВЕК+, М.: ЭНТРОП, СПб.: КОРОНА принт, 2001.
10. Буров Є.В. Комп’ютерні мережі: Підручник. – Львів: Магнолія плюс, 2006.
11. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2004.
12. Вишневский В.М. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003.
13. Стеклов В.К., Беркман Л.Н. Нові інформаційні технології: транспортні мережі телекомунікацій. – К.: Техніка, 2004.
14. Майкл Дж. Мартин. Введение в сетевые технологии.: Пер. с англ. – М.: Изд-во «Лори», 2002.
15. Валецька Т.М. Комп’ютерні мережі: Апаратні засоби. Навч. посібник. – К.: Ельга, 2004.