ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
ТА ІНФОРМАТИЗАЦІЇ

О.В. Полоневич, В.Р.Косенко, К.П.Сторчак, О.М.Ткаленко

ІНФОРМАЦІЙНІ МЕРЕЖІ

Навчальний посібник

для студентів, що навчаються за спеціальністю

126 - "Інформаційні системи та технології"

Київ - 2019

УДК 004.72

ББЛ 32.973.202

Рецензенти: директор Навчально-наукового інституту телекомунікацій та інформатизації доктор технічних наук, професор С.В.Козелков

декан факультету Інформаційних систем та технологій
доктор технічних наук А.П.Бондарчук

Затверджено Вченої радою факультету Інформаційних технологій Навчально-наукового інституту телекомунікацій та інформатизації Державного університету телекомунікацій в якості навчального посібника

Навчальний посібник призначений для самостійної роботи студентів вищих навчальних закладів під час поглибленого вивчення дисципліни «Інформаційні мережі» та забезпечує формування знань, вмінь та навичок, необхідних для роботи з комп'ютерними мережами, які об'єднують велику кількість персональний комп'ютерів, робочих станцій, серверів, для автоматизації сучасного процесу виробництва та телекомунікацій з процесом прийняття рішень у всіх галузях життя.

ЗМІСТ

1 ЗАГАЛЬНІ ПОНЯТТЯ ПРО ІНФОРМАЦІЙНІ МЕРЕЖІ

1.1 Визначення поняття інформаційна мережа

Поняття «інформаційна мережа» передбачає розгляд телекомунікаційної мережі в сукупності зі взаємодіючими за допомогою неї об'єктами. У такому розумінні інформаційна мережа – це «навантажена» телекомунікаційна мережа.

Поняття «інформаційна мережа» відображає інформаційні процеси, які протікають в мережі в результаті взаємодії кінцевих систем, під'єднаних до телекомунікаційної мережі.

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

Прикладні процеси ініціюються кінцевими системами під час запуску програм користувача, які ще називаються *застосуваннями.*

Процеси взаємодії – це процеси в мережі, призначені для обслуговування прикладних процесів. Прикладні процеси та процеси взаємодії підтримуються *мережевими операційними системами* (МОС).

Кінцеві системи інформаційної мережі класифікуються таким чином:

- *термінальні системи* – комп'ютери користувачів мережі;
- *хостингові системи* – комп'ютери, на яких розміщено інформаційні та програмні ресурси мережі;

- *сервери* – комп'ютери, на яких інстальоване спеціальне програмне забезпечення, яке дозволяє надавати мережеві сервіси. Серверний комп'ютер, залежно від можливості його операційної системи, може бути налаштований як для роботи в режимі хосту (інформаційний сервер), так і в режимі комунікаційного пристрою (наприклад, шлюзу);

- *адміністративні системи* – комп'ютери, які забезпечують роботу застосувань керування мережею та окремих її частин.

Інформаційні ресурси формуються і використовуються на основі всіх соціальних процесів, усіх форм власності та різних способів організації

суспільно корисної діяльності. Процеси перетворення та реалізації знань через матеріалізацію інформаційного ресурсу отримують розвиток за рахунок високих інформаційних технологій, а для отримання і збереження переваг в умовах конкуренції кожна дія в інформаційному середовищі буде мати значний вплив у світі фізичних ресурсів: предметних, фінансових – і в різних абстрактних галузях.

Усе це систематизується в мережевих банках даних, з якими взаємодіють користувачі мережі. Ці ресурси визначають споживчу цінність інформаційної мережі, тому їх необхідно: постійно створювати та поповнювати; вчасно архівувати та оновлювати; користування мережею повинно забезпечувати можливість отримання актуальної інформації саме тоді, коли в ній виникає необхідність.

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

Програмні ресурси – мережеве програмне забезпечення (ПЗ): мережеві операційні системи, серверне ПЗ, ПЗ робочих станцій; прикладне ПЗ;

Інструментальні засоби - утиліти, аналізатори проходження трафіку, засоби мережевого контролю, програми додаткових функцій, основними серед яких є виписка рахунків, облік оплати послуг, навігація (забезпечення пошуку інформації в мережі), обслуговування мережевих електронних поштових скриньок, організація мостів для телеконференцій, перетворення форматів переданих інформаційних повідомлень, криптозахист інформації (кодування й шифрування), автентифікація (електронний підпис документів, що засвідчує їх справжність).

Комунікаційні ресурси – це ресурси, які беруть участь у транспортуванні та перерозподілі потоків інформації в мережі (ресурси телекомунікаційної мережі), основними з яких є пропускні спроможності ліній зв’язку та устаткування вузлових пунктів, а також їх використання під час взаємодії користувача з мережею. Вони класифікуються відповідно до використаного середовища

передачі та телекомунікаційної технології. Ресурси інформаційної мережі можуть використовуватися одночасно кількома прикладними процесами, тобто *розділятися в часі*.

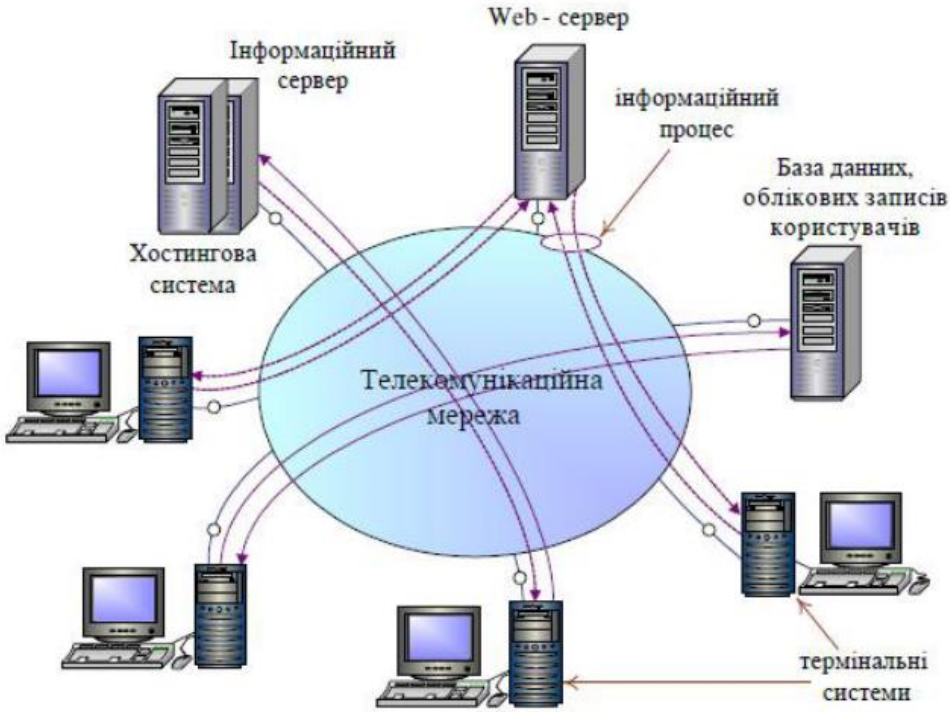


Рис.1.1 Інформаційна мережа

Ресурси інформаційної мережі дозволяють:

- виконувати обробку інформації;
- забезпечувати ефективний пошук інформації в будь-якому місці мережі;
- уможливлюють накопичення й зберігання інформації.

Отже, під *інформаційною мережею* як *фізичним об'єктом* розуміють *сукупність територіально розрізнених кінцевих систем, об'єднаних телекомунікаційною мережею, за допомогою якої забезпечуються взаємодія прикладних процесів, активізованих в кінцевих системах, та їх колективний доступ до ресурсів мережі.*

Уся інтелектуальна робота в інформаційній мережі виконується на перефирії, тобто в кінцевих системах мережі, а телекомунікаційна мережа,

займаючи центральне положення є з'єднувальним компонентом (рис. 1.1) Телекомунікаційна мережа у складі інформаційної мережі виконує функції *транспортувальної системи.*

Поняття інформаційна мережа зосереджує увагу на *інформаційних процесах,* які виникають у мережі під час взаємодії кінцевих систем через телекомунікаційнійну мережу. Опис цієї взаємодії демонструє всю складність організації зв'язку в мережі як у режимі «запит-відповідь», так і в реальному масштабі часу. Основною вимогою, якій має відповідати інформаційна мережа, є забезпечення користувачів *ефективним доступом до ресурсів, які можуть розділятися* (тобто колективного використовуватися). Усі інші вимоги – пропускна здатність, надійність, живучість – лише забезпечують якісне виконання цієї основної вимоги.

Параметри оцінки ефективності інформаційної мережі визначаються рівнем продуктивності інформаційної мережі як системи розподільчих ресурсів складаються з:

- часу реакції мережі;
- затримки передачі;
- варіації затримки передачі;
- прозорості.

Час реакції мережі визначається як інтервал часу між поданням запиту користувача до певної мережевої служби (наприклад, передачі файлів) і отримання відповіді на цей запит. Значення цього показника залежать від:

- типу служби, до якої звертається користувач;
- до якої категорії належить користувач;
- продуктивності сервера, куди він звертається;
- ступеня завантаженості елементів мережі через які проходить запит.

Затримка передачі визначається як час між моментом надходження пакету даних на вхід будь-якого мережевого пристрою або фрагмента мережі і моментом виходу з неї тобто визначаються етапи тимчасової обробки пакетів

при проходженні їх мережею. При цьому продуктивність мережі оцінюється максимальною затримкою передачі та варіацією затримки.

Варіація затримки (джитер затримки) характеризує коливання затримки в часі. Великий діапазон в значеннях затримки негативно позначаються на якості наданої користувачеві інформації при передаванні чутливих до затримки видів трафіку таких як відеодані, мовленнєвий трафік.

Прозорість характеризується властивістю мережі приховувати від користувача принципи її внутрішньої організації. Для роботи з віддаленими ресурсами мережі користувач повинен використовувати ті ж самі команди й процедури, що й для роботи з ресурсами свого комп'ютера.

1.2 Моделі системного опису мережевої архітектури

Усі мережі зв'язку належать до класу об'єктів, які називають великими чи складними системами. Складні системи за своїм складом є гетерогенними, тобто характеризуються величезною кількістю неоднорідних елементів і зв'язків між ними. Мережам зв'язку властиво мати всі ознаки складних систем і підпорядковуватися відповідним їм закономірностям.

Ієрархічність – розташування частин та елементів цілого в порядку від вищого до нижчого. Дотримуючись цієї закономірності, ми можемо розчленовувати мережу на окремі підмережі (сегменти) нижчого порядку.

Комунікаційність – закономірність, яка вказує на численність зв'язків (комунікацій) системи: зовнішніх – з навколишнім середовищем і внутрішніх – із власними підсистемами та елементами. Це означає, що мережу будь-якого рівня ієрархії не можна розглядати ізольовано, без урахування факторів, які впливають ззовні (вищерозташованих систем) і не можна розчленовувати її без урахування типу взаємозв'язку підмереж й елементів нижчого порядку.

Емержентність – закономірність, що полягає в прояві системою інтегрованої риси – цілісності, яка не притаманна окремим її елементам.

Наприклад, у мережі можна виокремити такі функціонально важливі й відносно незалежні підсистеми, як система мережевих застосувань, транспортна система, система керування мережею та ін.

Процес побудови ряду окремих структур системи має назву «*структуризація*».

Отримані в результаті структуризації окремі структури системи взаємопов'язані між собою. Щоб відобразити міжструктурні зв'язки, ізольовані структури розташовують у певному порядку, наприклад, ієрархічному, де ієрархія відбудовується відповідно до пріоритету аспектів дослідження системи.

Структуризація складної системи не піддається формалізації і тому її часто ототожнюють з архітектурою.

А*рхітектура* – це багаторівневий опис системи, отриманий шляхом структуризації.

Уявлення про будову та функціонування мережі зв'язку, як складної системи, може бути сформовано в результаті формування та дослідження її архітектури. При цьому доцільним є розгляд таких відокремлених структур:

1. *топологічної,* яка визначає розташування пунктів мережі та ліній зв'язку;
2. *організаційної,* яка визначає тип, призначення, статус елементів мережі залежно від виконуваних ними функцій;
3. *логічної,* яка описує роботу мережі на рівні взаємодії мережевих функцій та правил встановлення зв'язку між кінцевими системами, взаємодіючими через телекомунікаційну мережу;
4. *фізичної,* яка відображає фізичні пристрої та програмні засоби, в котрих реалізовано функціональні елементи мережі, фізичні середовища передавання сигналів.

Кожна з конкретних структур може бути змодельована. Модель дозволяє відобразити *найбільш важливі компоненти та зв'язки об'єкта,* і не враховувати несуттєві, відповідно до мети дослідження, деталі.

Сукупність таких моделей будемо називати *системним описом мережевої архітектури* (рис. 1.2).

Рис.1.2. Системний опис мережевої архітектури

1.2.1 Моделі топологічної структури мережі

На рівні найбільш узагальненого уявлення, будь-яка мережа складається з сукупності *пунктів* і з'єднуючих їх *ліній,* взаємне розташування яких характеризує зв'язність мережі та здатність забезпечувати інформаційний обмін між різними адресатами. Така відокремлена структура мережі має назву «*топологія*».

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

Топологія фізичних зв'язків відображає схему з'єднань елементів мережі.

Для дослідження топологічних особливостей мережі її зручно зображувати у вигляді *точок* і з'єднуючих їх *дуг.* Така геометрична фігура має назву *граф.* Точки в графі називають *вершинами,* а дуги, якщо не враховується їх спрямованість, – *ребрами.* Граф є моделлю топологічної структури мережі.

Вибір топології – це завдання, вирішення якого є першочерговим при побудові мережі. Він здійснюється з урахуванням таких вимог, як *економічність* і *надійність зв'язку*.

Задача вибору топології мережі вирішується, якщо відомим є набір *типових топологій (примітивів),* які можна використовувати як окремо, так і в комбінації.

Розглянемо ряд типових топологій (назвемо їх базовими) та охарактеризуємо їх особливості.

Топологія «точка – точка» уявляє собою сегмент мережі, який зв'язує фізично й логічно два пункти (рис. 1.3).

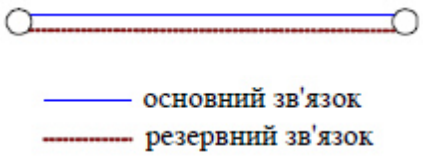


Рис. 1.3. Топологія «точка – точка»

Надійність зв'язку в такому сегменті може бути підвищена за рахунок долучення резервного зв'язку, який забезпечує стовідсоткове резервування, яке називають «*захистом типу 1+1».* У разі виходу з ладу основного зв'язку мережа автоматично від'єднується до резервного. Ця базова топологія найбільш широко використовується:

при передачі великих потоків інформації високошвидкісними магістральними каналами, наприклад, трансокеанськими підводними кабелями, які обслуговують цифровий телефонний трафік;

як складова частина радіально-кільцевої топології (у якості радіусів).

Топологія «точка – точка» з резервуванням типу 1+1 може розглядатися як варіант топології «кільце».

Деревоподібна топологія може мати різні варіанти (рис.1.4)

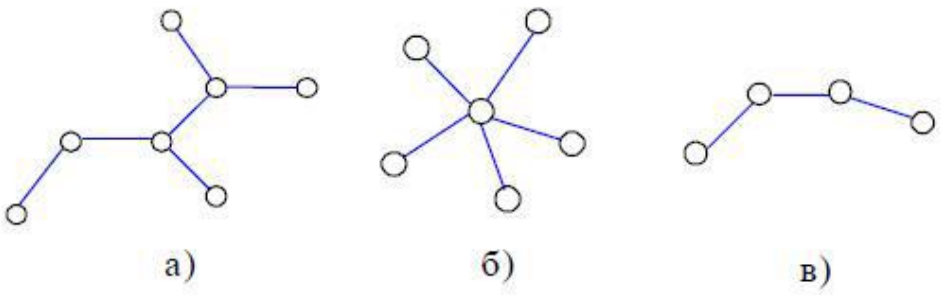


Рис. 1.4. Деревоподібна топологія: а) дерево; б) зірка; в) ланцюг

Особливістю сегменту мережі, що має деревоподібну топологію, будь-якого з перелічених варіантів, є те, що зв'язність *n* пунктів на рівні фізичної топології тут досягається числом ребер $K = n - 1$, що забезпечує високу економічність такої мережі. На логічному рівні, кількість зв'язних шляхів передавання інформації між кожною парою пунктів у такому сегменті завжди дорівнює $H = 1$. З точки зору надійності, це досить низький показник. Підвищення надійності в таких мережах досягається введенням резервних зв'язків (наприклад, захисту типу 1+1).

Деревоподібна топологія застосовується в локальних мережах, мережах абонентського доступу.

Топологія «кільце» (рис. 1.5) характеризує мережу, в якій до кожного пункту приєднано *дві (і тільки дві)* лінії. Кільцева топологія використовується в локальних мережах, у сегментах міжвузлових з'єднань територіальних мереж, а також у мережах абонентського доступу, організованих на базі волоконно-оптичного кабелю.

Число ребер графа, яке відображає фізичну топологію, дорівнює кількості вершин: $K = n$ і вказує на порівняно незначні витрати на мережу.

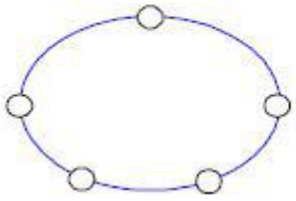


Рис. 1.5. Типологія «кільце»

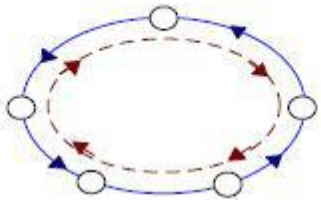


Рис.1.6 – Типологія «подвійне кільце»

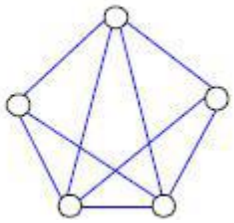


Рис. 1.7 – Повнозв'язана типологія

На логічному рівні між кожною парою пунктів можна організувати $к = 2$ незалежних зв'язаних шляхи (прямий та альтернативний), що забезпечує підвищення надійності зв'язку в такому сегменті, особливо при використанні резервування 1+1, так званого «подвійного кільця» (рис. 1.6). Подвійне кільце утворюється фізичними з'єднаннями між парами пунктів, при яких інформаційний потік направляється в двох протилежних напрямках (східному і

західному), причому один напрям використовується як основний, другий – як резервний.

Повнозв'язна топологія (рис. 1.7) забезпечує фізичне та логічне з'єднання пунктів за принципом «кожен з кожним». Граф, який включає *n* вершин, містить $K = n(n-1)/2$ ребер, що впливає на високу вартість мережі. Кількість незалежних зв'язних шляхів між кожною парою пунктів у такому сегменті мережі дорівнює $H = n - 1$. Повнозв'язна топологія на логічному рівні забезпечує максимальну надійність зв'язку завдяки можливості організовувати велику кількість обхідних шляхів. Така топологія притаманна територіальним мережам при формуванні сегментів базових і опорних (магістральних) мереж. Максимальної надійності зв'язку в сегменті можна досягти, використовуючи на обхідних напрямках альтернативні середовища поширення сигналів (наприклад, волоконно-оптичний кабель і радіорелейна лінія).

Коміркова топологія (рис. 1.8). Кожен пункт сегмента має безпосередній зв'язок із невеликою кількістю пунктів, найближчих за відстанню.

При великій кількості вершин число ребер $R \approx r\ n/2$, де *r* – кількість ребер, інцидентних кожній вершині. Коміркові сегменти мають високу надійність зв'язку при меншій кількості ребер у порівнянні з повнозв'язним сегментом.

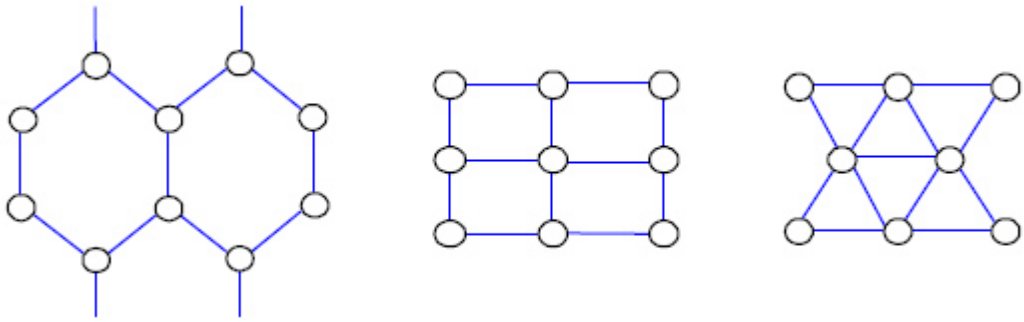


Рис. 1.8. Коміркова тополо

Використання повнозв'язної та коміркової топологій є доцільним лише в сегментах із високою концентрацією трафіку, тому що їх реалізація пов'язана із значними витратами.

Складні (змішані) топології. Реальні мережі часто мають складні топології, що є розширеннями та/або комбінаціями базових фізичних топологій (рис. 1.9). За рахунок використання складних топологій вдається забезпечувати вимоги до *розширюваності* та *масштабованості* мереж.

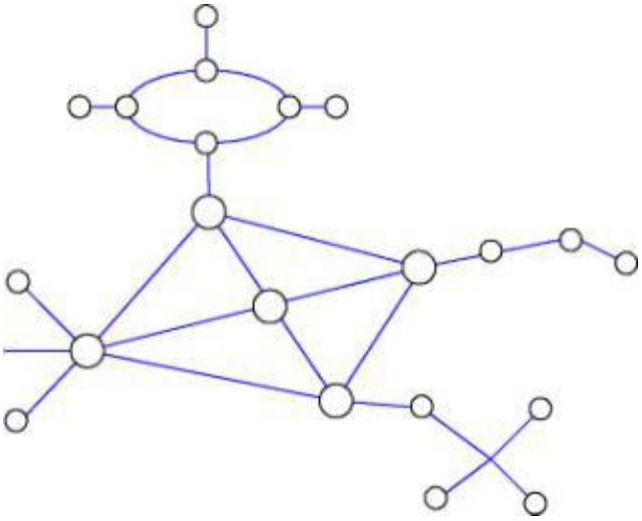


Рис. 1.9. Складна мережева топологія

Топологія логічних зв'язків дає уявлення про шляхи переміщення інформаційних повідомлень у мережі від джерел до одержувачів відповідно до адресної інформації. Зв'язані шляхи можуть бути визначені лише в зв'язних фізичних топологіях (методи знаходження зв'язуючих шляхів із урахуванням різних критеріїв.

Під *зв'язуючим шляхом* розуміють послідовність ліній і вузлових пунктів, через які проходить маршрут перенесення інформації в мережі.

Маршрут вказує на спрямованість шляху (траєкторію перенесення інформації по мережі).

Сукупність потоків інформації (службової та призначеної для користувача), які переміщаються в мережі за певними маршрутами та навантажують мережу протягом певного інтервалу часу, називається *мережевим трафіком*.

Таким чином, *топологія логічних зв'язків є адекватною плану розподілу потоків мережевого трафіку.*

Узагальнено *планом розподілення потоків у мережі* називають суперпозицію (накладання) маршрутів передачі інформації, визначених у мережі для кожної пари джерело – одержувач.

Елементами моделі логічної топології є *логічні вузли* та *маршрути, які їх поєднують.*

Логічними вузлами, або далі скорочено *вузлами* мережі на рівні топології логічних зв'язків називаються будь-які фізичні пристрої, яким призначені адресні ідентифікатори.

Вузол може бути комп'ютером (робочою станцією або сервером), комунікаційним пристроєм, мережевим принтером – будь-яким пристроєм з *мережевим інтерфейсом* (встановленою мережевою платою).

Вузол, у якому не передбачено виконання функцій вузлових пунктів (концентрації, мультиплексування, комутації або маршрутизації), називається *хостом.*

Хост – це вузол, який є кінцевою системою мережі і не може виконувати функції транзитного вузлового пункту.

Адресні ідентифікатори підрозділяються на адреси вузлів і мережеві адреси.

Адреси вузлів мають назву локальні чи апаратні адреси.

У локальних сегментах локальні адреси ще називають *фізичними адресами, адресами точки доступу до середовища***.** Це унікальні числові значення можуть встановлюватися як програмно, так і апаратно.

У територіальних сегментах локальні розширення ідентифікують мережеві інтерфейси взаємодіючих всередині передбаченої використовуваною телекомунікаційною технологією.

Мережева адреса – це логічна адреса, яка присвоюється адміністрацією (спеціальним міжнародним органом) і визначає сегмент приєднання пристрою. Повна мережева адреса складається зі спільного для всіх вузлів номера мережі й унікального в цій мережі номера вузла.

В інформаційній мережі (як логічній надбудові) застосовуються також ідентифікатори (адреси) прикладних процесів, які взаємодіють через мережу.

Моделями топологій логічних зв’язків прийнято вважати:

- логічну шину;
- логічне кільце;
- комутовану топологію.

Принцип побудови тієї чи іншої моделі топологічних зв’язків ґрунтується на виборі механізму, який забезпечує зв’язність вузлів. Топологія логічних зв’язків може збігатися з топологією фізичних зв’язків у мережі або відрізнятися. На основі однієї й тієї ж топології фізичних зв’язків можна побудувати різні топології логічних зв’язків, використовуючи відповідне комунікаційне (мережеве) обладнання.

1.2.2 Моделі організаційної структури мережі

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

Елементами моделі організаційної структури є *пункти та лінії зв’язку*.

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

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

Пункти, призначені для розміщення термінального обладнання користувачів, яке забезпечує доступ в мережу, функціонують у ролі

абонентських пунктів **(**АП**)**. Пункти, у яких зосереджено інформаційні ресурси, називаються *інформаційними центрами* **(**ІЦ**),** а пункти системи керування відповідно – *центрами керування* **(**ЦК**).**

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

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

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

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

Розподілення – функція, протилежна концентрації, тобто відгалуження від концентрованого вхідного інформаційного потоку малих за потужністю вихідних потоків і розподіл їх між виходами. Функція реалізується в пристроях, які називаються *відгалужувачі.*

Мультиплексування забезпечує можливість передачі декількох потоків інформації однією лінією, що здійснюється закріпленням за кожним із них фіксованої частини ресурсу лінії (смуги пропускання або часу зайняття). Фіксований розподіл ресурсу лінії залишається незмінним навіть у періоди відсутності інформації, тобто функція концентрації не спрацьовує. Зворотна

функція – *демультиплексування.* Реалізація в комунікаційних пристроях (мультиплексорах) функції мультиплексування завжди поєднується з демультиплексуванням.

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

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

У комунікаційному пристрої може бути реалізована одна з перерахованих функцій, саме тоді цей пристрій відповідно називається або *концентратором*, або *мультиплексором*, або *комутатором*, або *маршрутизатором* та ін.

Порядок співвідношення між елементами (їх статус) в моделі організаційної структури визначається рівнями їх ієрархії (рис. 1.10).

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

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

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

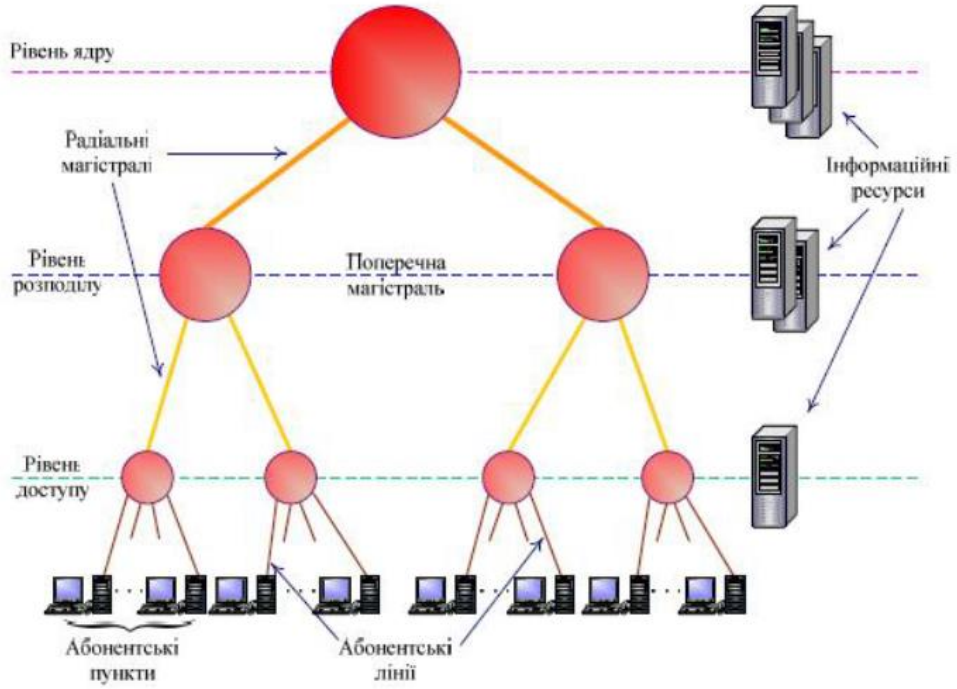


Рис. 1.10. Узагальнена схема організаційної структури мере

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

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

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

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

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

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

Призначення вузлових пунктів в моделі організаційної структури відносно кінцевих пунктів, які він обслуговує, незалежно від статусу, може виступати в ролі: опорного вузла; транзитного вузла; опорно-транзитного вузла.

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

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

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

Для мереж операторів і сервіс-провайдерів актуальними є терміни, що визначають призначення вузлових пунктів відповідно до реалізації функцій доступу.

Функції доступу в територіальних мережах незалежно від рівня ієрархії вузлового пункту прийнято розглядати за наступними аспектами:

- забезпечення доступу користувачів до телекомунікаційних служб та мережевих ресурсів;
- забезпечення доступу при з’єднанні сегментів телекомунікаційної мережі;
- забезпечення доступу до інформаційних ресурсів глобальної мережі Інтернет.

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

Вузловий пункт, де забезпечується з'єднання сегментів телекомунікаційної мережі, наприклад, мережі доступу та транспортної мережі, називається *вузлом доступу***.**

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

2 КОМП’ЮТЕРНІ МЕРЕЖІ ТА ЇХ КЛАСИФІКАЦІЯ

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

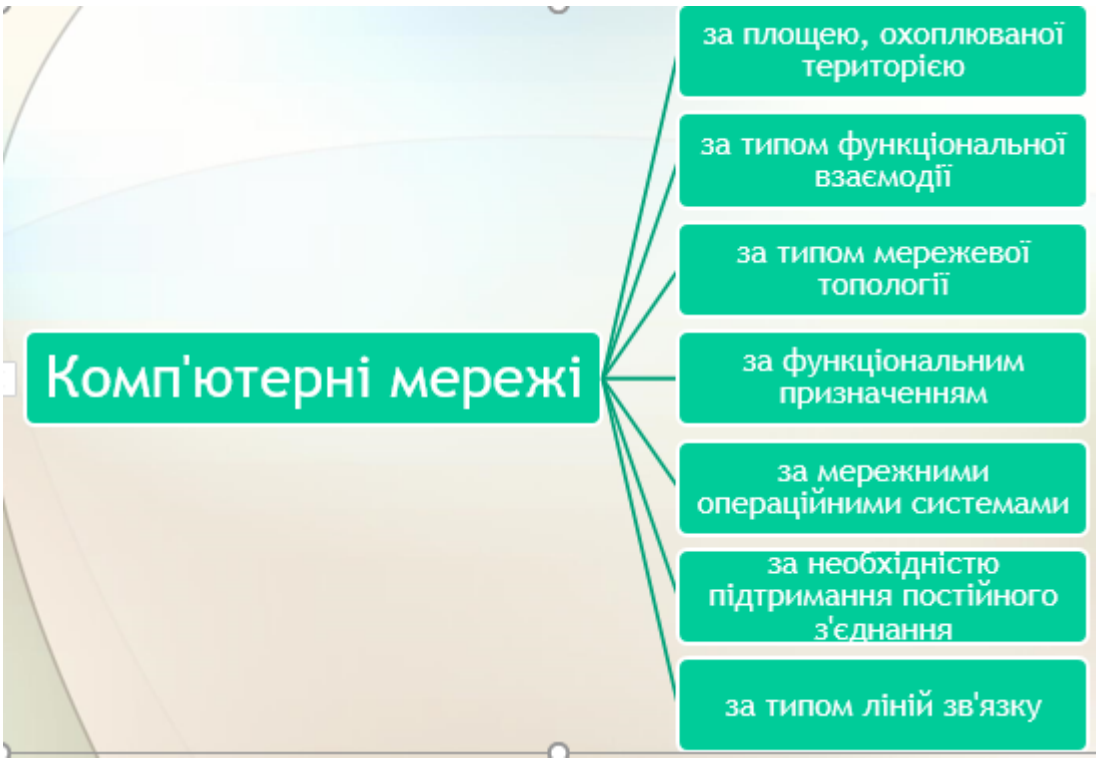


Рис.2.1. Види класифікації комп'ютерних мереж

Класифікація комп'ютерних мереж за площею охоплюваної території:

А) Персональна мережа (*Personal Area Network, PAN*) – це мережа, побудована „навкруг” людини. Такі мережі покликані об’єднувати усе персональне електронне обладнання користувача (телефони, КПК, ноутбуки, гарнітури і т.д.). До стандартів таких мереж зараз відносять Bluetooth.

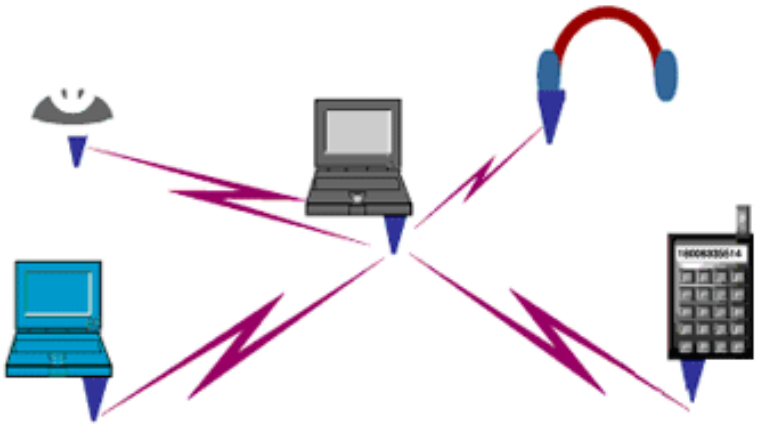


Рис.2.2. Мережа PAN

Параметры PAN:

1. Мала кількість абонентів
2. Некритичність к напрацюванню на відмову
3. Усі пристрої можливо контролювати
4. Малий радіус дії (100 футів (30 метрів))
5. Мережа повинна підтримувати до 8 учасників

Б) Локальна мережа (*Local Area Network, LAN*) - це комп'ютерна мережа, яка покриває відносно невелику територію, таку як дім, офіс, або невелику групу будинків, наприклад, інститут.

Кожен комп'ютер, підключений до локальної мережі, повинен мати спеціальну плату (мережевий адаптер). Між собою комп'ютери (мережеві адаптери) з'єднуються, наприклад, за допомогою кабелів.

В) Об'єднання кількох будівель (*Campus Area Network, CAN*) - це комп'ютерна мережа, що об'єднує групу близько розташованих будівель.

Г) Міська мережа (*Metropolitan Area Network, MAN*) - це комп'ютерна мережа, що об'єднує комп'ютери в межах міста. Простим прикладом міської мережі є система кабельного телебачення.

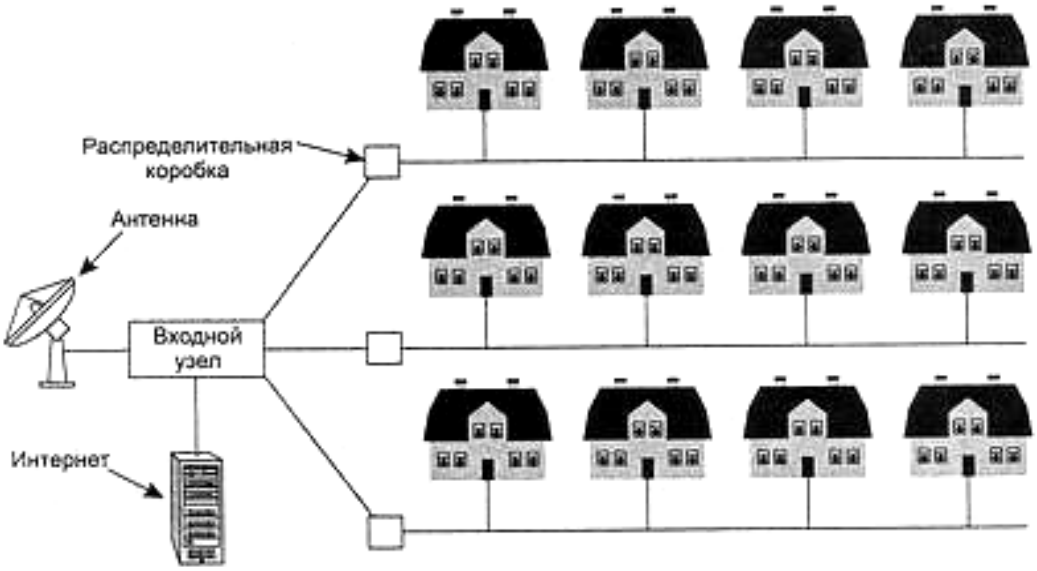


Рис.2.3. Мережа MAN

Д) Глобальна обчислювальна мережа (*Wide Area Network, WAN*) - це комп'ютерна мережа, що об'єднує великі території та включає в себе десятки та сотні тисяч комп'ютерів.

Кращим зразком WAN є Інтернет, але існують і інші мережі, наприклад Fido Net.

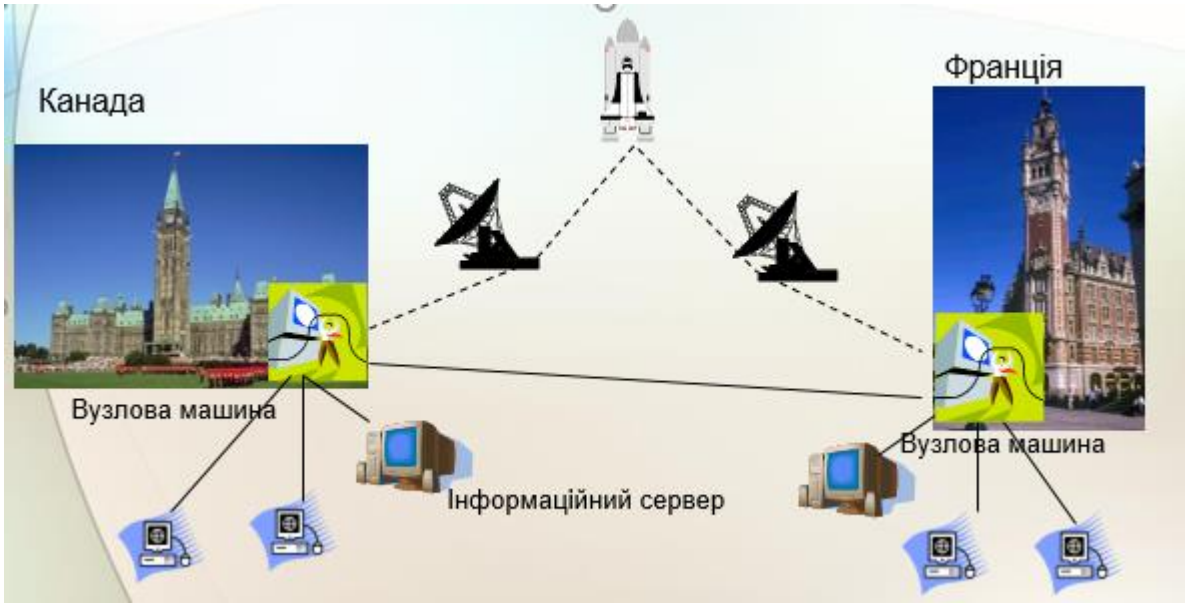


Рис.2.4. Мережа WAN

Класифікація комп'ютерних мереж за типом функціональної взаємодії:

А) Мережа типу “крапка-крапка” - простий вид комп'ютерної мережі, при якому два комп'ютери з'єднуються між собою безпосередньо через комунікаційне устаткування. Перевагою такого виду з'єднання є простота і дешевизна, недоліком - з'єднати таким чином можна тільки два комп'ютери і не більше.

Часто використовується коли необхідно швидко передати інформацію з одного комп'ютера, наприклад, ноутбука, на інший.

Б) Клієнт-сервер (*Client-server*) - мережева архітектура, в якій пристрої є або клієнтами, або серверами. Клієнтом (*front end*) є запрошуюча машина (зазвичай ПК), сервером (*back end*) - машина, яка відповідає на запит. Обидва терміни (клієнт і сервер) можуть застосовуватися як до фізичних пристроїв, так і до програмного забезпечення.

Мережа з виділеним сервером (*Client/server network*) - це локальна обчислювальна мережа (LAN), в якій мережеві пристрої централізовані і управляються одним або декількома серверами. Індивідуальні робочі станції або клієнти (такі, як ПК) повинні звертатися до ресурсів мережі через сервер(и).

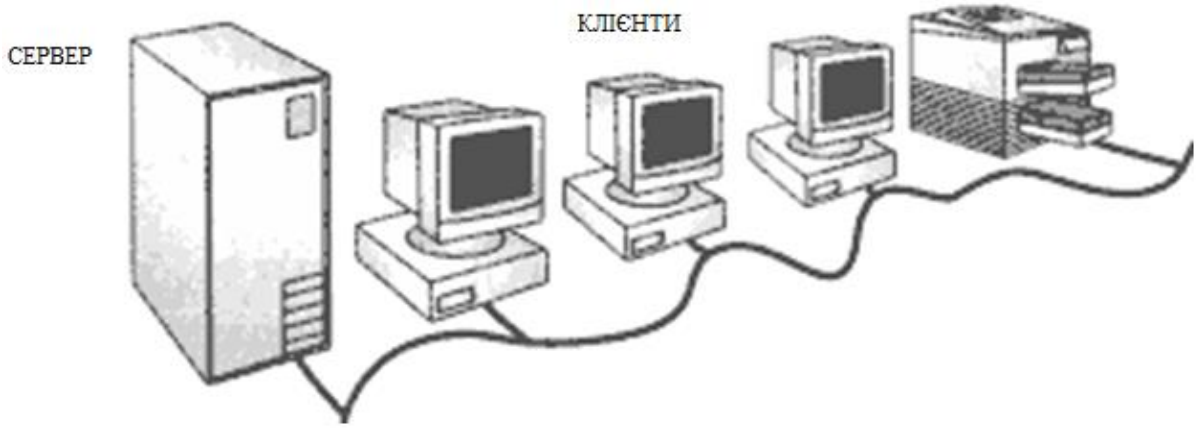


Рис.2.5. Мережа з виділеним сервером

В) Однорангові, децентралізовані або пірінгові (*peer-to-peer, P2*P - один на один, віч-на-віч) мережі - це комп'ютерні мережі, засновані на рівноправ'ї учасників. У таких мережах відсутні виділені сервери, а кожен вузол (*peer*) є як клієнтом, так і сервером. На відміну від архітектури клієнт-сервер, така організація дозволяє зберігати працездатність мережі при будь-якій кількості і будь-якому поєднанні доступних вузлів.

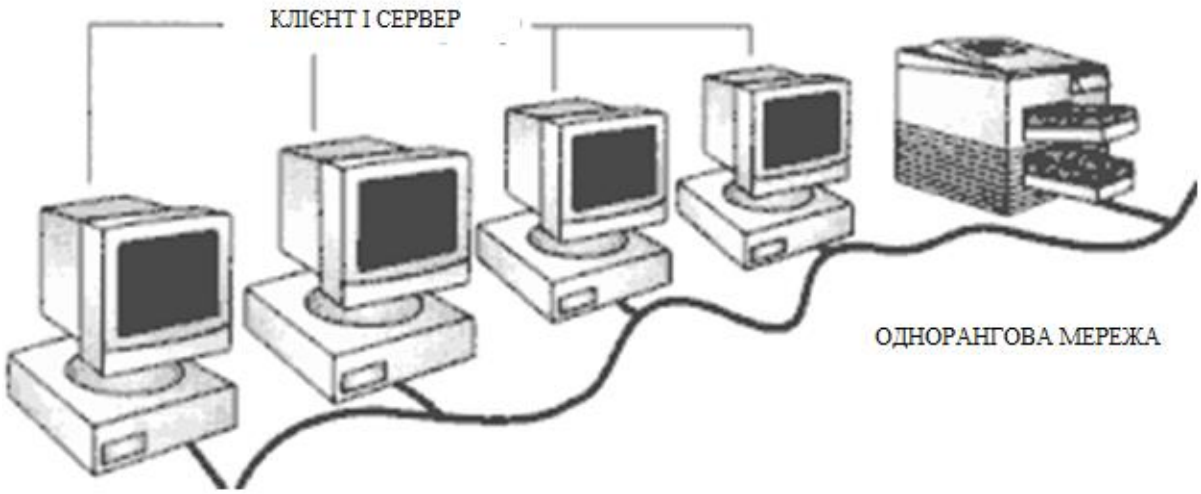


Рис.2.6. Одноранговa мережа

Порівняльна характеристика одноранговоїмережі та мережі з виділеним сервером

+	-
Одноранговa мережа	
Легко настроювати	Менша безпека
Не потребує серверного ПЗ	Складність адміністрування кожного комп'ютера
Не потрібен системний адміністратор	Погіршення продуктивності при сумісному використанні ресурсів
Невелика вартість проекту	
Мережа з виділеним сервером	
Більша безпека	Складність настройки, адміністрування клієнтів, ресурсів
Легше керувати, оскільки управління централізовано	Відсутність доступу до мережі в випадку виходу з ладу серверу

Класифікація комп'ютерних мереж за типом мережевої топології:

А) Топологія типу шина, є загальний кабель (що зветься шиною або магістраллю), до якого приєднані всі робочі станції. На кінцях кабелю знаходяться термінатори, для запобігання віддзеркаленню сигналу.

Термінатори (поглиначі енергії) застосовуються на всіх лініях, що з'єднують передавач і приймач сигналу, коли відбитий від кінця лінії сигнал значно впливає на роботу лінії зв'язку. При невеликих довжинах ліній накладення відбитого сигналу призводить до затягування фронтів (тобто до зниження швидкості передачі), при збільшенні довжини лінії таке накладення сигналів призводить лінію в зумовити.

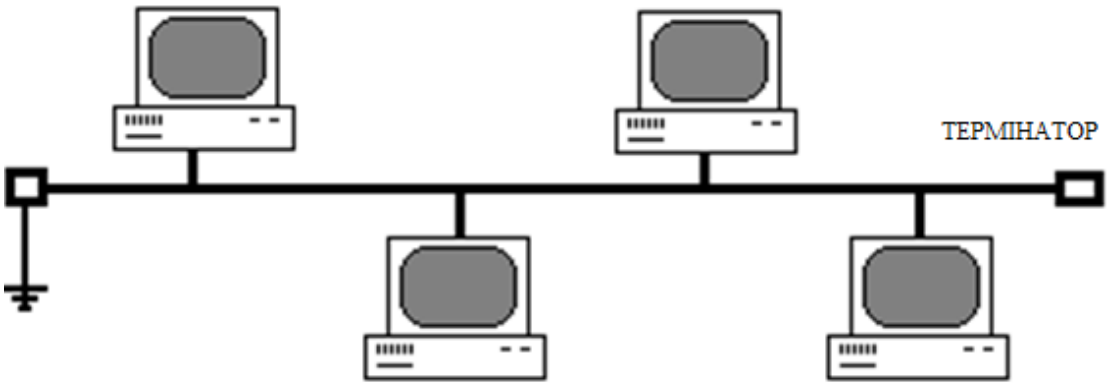


Рис.2.7. Топологія типу шина

Б) *Зірка* - базова топологія комп'ютерної мережі, в якій всі комп'ютери мережі приєднані до центрального вузла (зазвичай мережевий концентратор), утворюючи фізичний сегмент мережі. Подібний сегмент мережі може функціонувати як окремо, так і у складі складної мережевої топології (як правило "дерево").

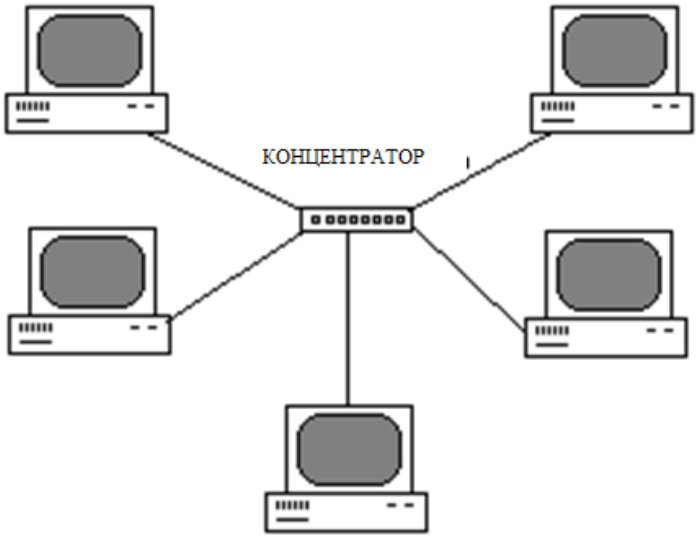


Рис.2.8. Топологія типу зірка

В) Кільце - базова топологія комп'ютерної мережі, в якій робочі станції підключені послідовно одна до одної, утворюючи замкнуту мережу. Наприклад, мережа Token ring.

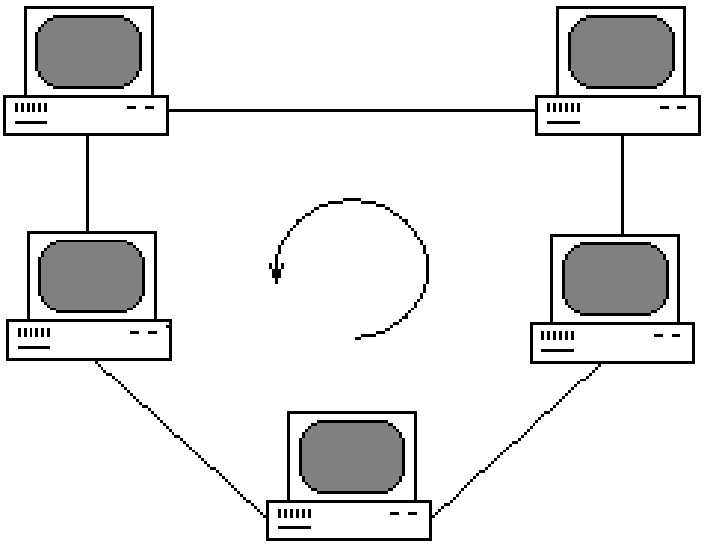


Рис.2.9. Топологія кільце

Г) *Сітка* (англ. *mesh*) – мережева топологія, при якій комп'ютери зв'язуються між собою не одною, а багатьма лініями зв'язку, що створюють сітку.

У повній сітковій топології кожен комп'ютер безпосередньо пов'язаний з рештою всіх комп'ютерів. При збільшенні числа комп'ютерів різко зростає кількість ліній зв'язку. Зміна в конфігурації мережі вимагає внесення змін до мережевої апаратури всіх комп'ютерів, тому повна сіткова топологія не набула широкого поширення.

Часткова сіткова топологія припускає прямі зв'язки тільки для найактивніших комп'ютерів, передавальних максимальні об'єми інформації. Решта комп'ютерів з'єднується через проміжні вузли.

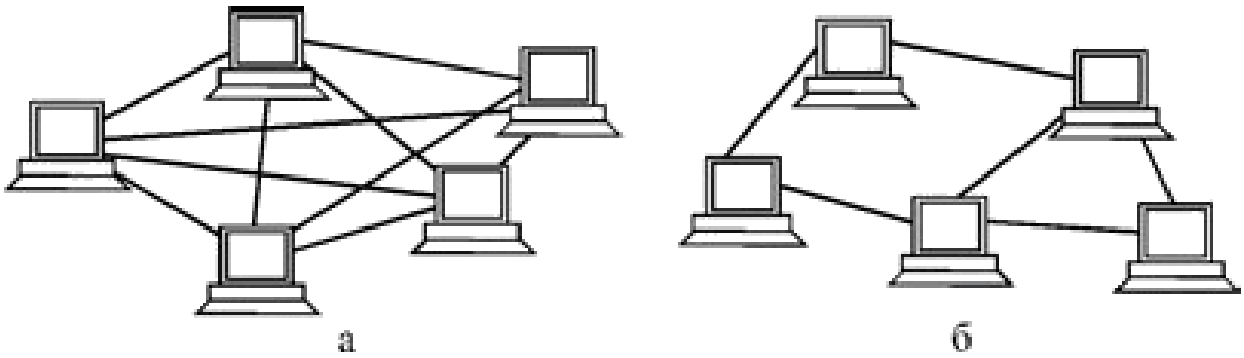


Рис.2.10. Топологія сітка

Д) Змішана топологія – мережева топологія переважаюча в крупних мережах з довільними зв'язками між комп'ютерами. У таких мережах можна виділити окремі зв'язані фрагменти (підмережі), що мають типовою топологію, тому їх називають мережами із змішаною топологією.

Класифікація комп'ютерних мереж за функціональним призначенням

А) Мережа зберігання даних (англ. *Storage Area Network, SAN*) - є архітектурне рішення для підключення зовнішніх пристроїв зберігання даних, таких як дискові масиви, стрічкові бібліотеки, оптичні накопичувачі до серверів так, щоб операційна система розпізнала підключені ресурси, як локальні. Не дивлячись на те, що вартість і складність таких систем постійно падають, мережі зберігання даних залишаються рідкістю за межами великих підприємств.

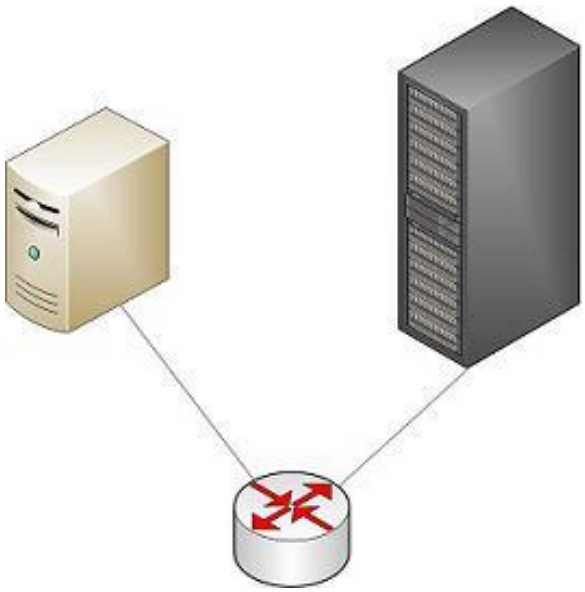


Рис.2.11. Мережа зберігання даних

Б) Серверна ферма - це асоціація серверів, сполучених мережею передачі даних і таких, що працюють як єдине ціле. Один з видів серверної ферми визначає метакомп'ютерна обробка. У всіх випадках дана ферма забезпечує розподілену обробку даних. Вона здійснюється в розподіленому середовищі обробки даних.

Серверна ферма є ядром крупного центру обробки даних.

В) Мережа керування процесом – сукупність мережевих пристроїв для забезпечення функціонування різних (виробничих, технологічних та ін.) процесів.

Г) Мережі SOHO (від англ. *Small Office, Home Office*) - назва сегменту ринку електроніки, призначеного для домашнього та офісного використання. Як правило характеризує пристрої не призначені для виробничих навантажень і досить добре переносить тривалі періоди бездіяльності.

Класифікація комп'ютерних мереж за мережною операційною системою.

Мережна операційна система (ОС) – це пакет програм, що забезпечує реалізацію та управління мережею, дає змогу клієнтам користуватись мережним сервісом. Основними завданнями мережної ОС є забезпечення сумісного використання та розподілу ресурсів мережі; надання клієнтам мережного

сервісу; адміністрування мережі; обміну повідомленнями між вузлами мережі; взаємодії процесів у мережі; надійного зберігання даних та інших завдань, пов’язаних з функціонуванням мережі. Важливою функцією мережної ОС є забезпечення системи захисту – конфіденційності зберігання даних, розмежування прав доступу до ресурсів, парольний захист, виявлення спроб несанкціонованого доступу, трасування дій користувачів, ведення журналів системних подій тощо.

А) Microsoft Windows – сімейство операційних систем компанії Майкрософт (Microsoft).

Б) UNIX - група переносимих, багатозадачних і багатокористувацьких операційних систем.

В) Netware - мережева операційна система і набір мережевих протоколів, які використовуються в цій системі для взаємодії з комп'ютерами-клієнтами, підключеними до мережі.

Класифікація комп'ютерних мереж за необхідністю підтримання постійного з'єднання:

А) Пакетна мережа.

Для здійснення комутації зв'язків визначена спеціальна група пакетів установлення з'єднання (call setup). Після того як установлений маршрут через мережу (або віртуальний канал), наступні пакети випливають один за іншим по встановленому шляху доти, поки канал не буде розірваний. Таким чином, пакети досягають свого місця призначення послідовно.

FidoNet - міжнародна некомерційна комп'ютерна мережа, побудована по технологіях «з крапки в крапку» і «комутація із запам'ятовуванням». Спочатку програмне забезпечення FidoNet розроблялося під MS DOS, проте незабаром було адаптовано під всі розповсюджені операційні системи, включаючи UNIX, GNU / Linux, Microsoft Windows, OS / 2, Android, і Mac OS. Особливістю FidoNet, що визначила широке розповсюдження цієї мережі, була фактична безкоштовність підключення і використання ресурсів мережі. Учасникам був

необхідний лише канал зв'язку у вигляді телефонної лінії (плата за стаціонарний телефон зазвичай була фіксованою). Пізніше для пересилки Фідо-даних все частіше стали використовуватися лінії Інтернету.

Б) Онлайнова мережа

Інтернет (англ. *Internet*, від *Interconnected Networks* - об'єднані мережі) - глобальна телекомунікаційна мережа інформаційних і обчислювальних ресурсів.

GSM (від назви групи *Groupe Special Mobile*, пізніше перейменований в *Global System for Mobile Communications*) - глобальний цифровий стандарт для мобільного стільникового зв'язку, з розділенням каналу за принципом TDMA (метод часового поділу одного фізичного каналу зв'язку) і високим ступенем безпеки завдяки шифруванню з відкритим ключем.

1. Класифікація комп'ютерних мереж за типом ліній зв'язку

А) Дротові або кабельні мережі

Можна виділити наступні основні параметри кабелів, принципово важливі для використання в локальних мережах:

* Смуга пропускання кабелю (частотний діапазон сигналів, що пропускаються кабелем) і загасання сигналу в кабелі. Загасання вимірюється в децибелах і пропорційно довжині кабелю.

* Перешкодозахищеність кабелю і забезпечувана ним секретність передачі інформації.

* Швидкість розповсюдження сигналу по кабелю або, зворотний параметр - затримка сигналу на метр довжини кабелю. Відповідно типові величини затримок - від 4 до 5 нс/м.

* Хвилевий опір кабелю. Типові значення хвилевого опору - 50 - 150 Ом.

В даний час діють наступні стандарти на кабелі:

* EIA/TIA 568 - американський; * ISO/IEC IS 11801 - міжнародний;

- CENELEC EN 50173 - європейський.
- ДСТУ 4809:2007 - Україна

3 МОДЕЛЬ OSI. АПАРАТУРА ЛОКАЛЬНИХ МЕРЕЖ

3.1 Модель відкритої системи OSI. Протоколи обміну.

Мережева модель OSI (базова еталонна модель взаємодії відкритих систем, англ. *Open Systems Interconnection Basic Reference Model*) - абстрактна мережева модель для комунікацій і розробки мережевих протоколів. Представляє рівневий підхід до мережі. Кожен рівень обслуговує свою частину процесу взаємодії. Завдяки такій структурі спільна робота мережевого устаткування і програмного забезпечення набагато простіша і прозоріша.

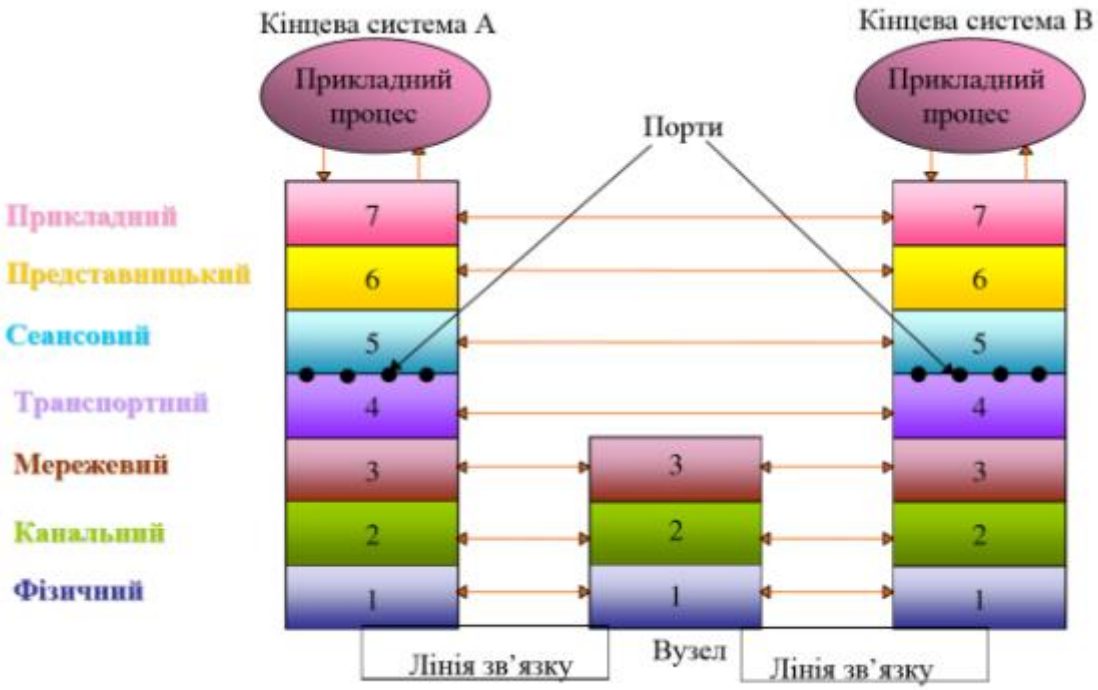


Рис.3.1. Модель OSI

Прикладний рівень

Прикладний (7) рівень (англ. *Application Layer*) або рівень застосувань забезпечує послуги, що безпосередньо підтримують застосування користувача, наприклад, програмні засоби передачі файлів, доступу до баз даних, засоби

електронної пошти, службу реєстрації на сервері. Цей рівень управляє рештою всіх шести рівнів. Наприклад, якщо користувач працює з електронними таблицями Excel і вирішує зберегти робочий файл в своїй директорії на мережевому файл-сервері, то прикладний рівень забезпечує переміщення файлу з робочого комп'ютера на мережевий диск прозоро для користувача.

Представницький рівень

Представницький (6) рівень (англ. *Presentation Layer*) або рівень представлення даних визначає і перетворює формати даних і їх синтаксис у форму, зручну для мережі, тобто виконує функцію перекладача. Тут же проводиться шифрування і дешифрування даних, а при необхідності - і їх стиснення. Стандартні формати існують для текстових файлів (ASCII, EBCDIC, HTML), звукових файлів (WAV, AIFF, APE, FLAC, mp3, ogg), малюнків (JPEG, GIF,PNG, BMP), відео (AVI). Всі перетворення форматів виконуються на представницькому рівні. Якщо дані передаються у вигляді двійкового коду, то перетворення формату не вимагається.

Сеансовий рівень

Сеансовий (5) рівень (англ. *Session Layer*) управляє проведенням сеансів зв'язку (тобто встановлює, підтримує і припиняє зв'язок). Цей рівень передбачає три режими установки сеансів: симплексний (передача даних в одному напрямі), напівдуплексний (передача даних по черзі в двох напрямах) і повнодуплексний (передача даних одночасно в двох напрямах). Сеансовий рівень може також вставляти в потік даних спеціальні контрольні крапки, які дозволяють контролювати процес передачі при розриві зв'язку. Цей же рівень розпізнає логічні імена абонентів, контролює надані їм права доступу.

Транспортний рівень

Транспортний (4) рівень (англ. *Transport Layer*) забезпечує доставку пакетів без помилок і втрат, а також в потрібній послідовності. Тут же проводиться розбиття на блоки даних, що передаються, поміщаються в пакети, і відновлення даних, що приймаються, з пакетів. Доставка пакетів можлива як зі встановленням з'єднання (віртуального каналу), так і без. Транспортний рівень є

прикордонним і таким, що пов'язує верхні три, що сильно залежать від додатків, із трьома нижніми рівнями, які сильно прив'язані до конкретної мережі.

Мережний рівень

Мережевий (3) рівень (англ. *Network Layer*) відповідає за адресацію пакетів і переклад логічних імен (логічних адрес, наприклад, IP-адрес або IPX-адрес) у фізичні мережеві MAC-адреси (і назад). На цьому ж рівні вирішується завдання вибору маршруту (шляху), по якому пакет доставляється за призначенням (якщо в мережі є декілька маршрутів). На мережевому рівні діють такі складні проміжні мережеві пристрої, як маршрутизатори.

Канальний рівень

Канальний (2) рівень або рівень управління лінією передачі (англ. *Data link Layer*) відповідає за формування пакетів (кадрів) стандартного для даної мережі (Ethernet, Token-ring, FDDI) вигляду, що включають початкове і кінцеве поля, що управляють. Тут же проводиться управління доступом до мережі, виявляються помилки передачі шляхом підрахунку контрольних сум, і проводиться повторна пересилка приймачу помилкових пакетів. Канальний рівень ділиться на два підрівні: верхній LLC і нижній MAC. На канальному рівні працюють такі проміжні мережеві пристрої, як комутатори.

Верхній підрівень (*LLC - Logical Link Control*) здійснює управління логічним зв'язком, тобто встановлює віртуальний канал зв'язку. Строго кажучи, ці функції не пов'язані з конкретним типом мережі, але частина з них все ж таки покладається на апаратуру мережі (мережевий адаптер). Інша частина функцій підрівня LLC виконується програмою драйвера мережевого адаптера. Підрівень LLC відповідає за взаємодію з рівнем 3 (мережевим).

Нижній підрівень (*MAC - Media Access Control*) забезпечує безпосередній доступ до середовища передачі інформації (каналу зв'язку). Він безпосередньо пов'язаний з апаратурою мережі. Саме на підрівні MAC здійснюється взаємодія з фізичним рівнем. Тут проводиться контроль стану мережі, повторна передача пакетів задане число разів при колізіях, прийом пакетів і перевірка правильності передачі.

Фізичний рівень

Фізичний (1) рівень (англ. *Physical Layer*) - це найнижчий рівень моделі, який відповідає за кодування інформації, що передається на рівні сигналів, прийнятті у середовищі передачі, що використовується, і зворотне декодування. Тут же визначаються вимоги до з'єднувачів, роз'ємів, електричного узгодження, заземлення, захисту від перешкод і т.д. На фізичному рівні працюють такі мережеві пристрої, як трансивери, репітери і репітерні концентратори.

3.2 Апаратура локальних мереж

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

- кабелі для передачі інформації;
- роз'єми для приєднання кабелів;
- термінатори, що погоджують;
- мережеві адаптери;
- репітери;
- трансивери;
- концентратори;
- мости;
- маршрутизатори;
- шлюзи.

Мережева плата (також відомий як мережевий адаптер, Ethernet-адаптер, NIC (англ. *network interface card*)) - периферійний пристрій, що дозволяє комп'ютеру взаємодіяти з іншими пристроями мережі.

По фізичній реалізації мережеві плати діляться на:

* внутрішні - окремі плати, що вставляються в PCI, ISA або PCI-E слот

* зовнішні, що підключаються через USB, PCMCIA інтерфейс (ноутбуки);

* вбудовані в материнську плату

На 10-мегабітних мережевих платах для підключення до локальної мережі використовуються 3 типи роз'ємів:

* 8p8c для витої пари

* BNC-конектор для тонкого коаксіального кабелю

* 15-контактний роз'єм трансивера для товстого коаксіального кабелю

Ці роз'єми можуть бути присутніми в різних комбінаціях, іноді навіть все три відразу, але в будь-який даний момент працює тільки один з них.

На 100 та 1000-мегабітних платах встановлюють тільки роз'їм для витої пари (8p8c).

Поряд з роз'ємом для витої пари встановлюють один або декілька інформаційних світлодіодів, що повідомляють про наявність підключення і передачу інформації.

Параметри мережевого адаптера.

При конфігурації карти мережевого адаптера можуть бути доступні наступні параметри:

- номер лінії запиту на апаратне переривання IRQ
- номер каналу прямого доступу до пам'яті DMA (якщо підтримується)
- базова адреса введення/виводу
- базова адреса пам'яті ОЗУ (якщо використовується)
- підтримка стандартів автоузгодження дуплексу/напівдуплекса, швидкості
- підтримка тегрірованих пакетів VLAN (801.q) з можливістю фільтрації пакетів заданого VLAN ID

- параметри WOL (WAKE-ON-LAN)

Залежно від потужності і складності мережевої карти вона може реалізовувати обчислювальні функції (переважно підрахунок і генерацію контрольних сум кадрів) апаратно або програмно (драйвером мережевої карти з використанням центрального процесора).

Серверні мережеві карти можуть поставлятися з двома (і більш) мережевими роз'ємами. Деякі мережеві карти (вбудовані на материнську плату) також забезпечують функції міжмережевого екрану (наприклад, nforce).

Функції мережевого адаптера діляться на магістральні та мережеві. До магістральних відносяться ті функції, які здійснюють взаємодію адаптера з магістраллю (системною шиною) комп'ютера (тобто визначення своєї магістральної адреси, пересилка даних в комп'ютер і з комп'ютера, вироблення сигналу переривання комп'ютера і так далі). Мережеві функції забезпечують спілкування адаптера з мережею.

Мережеві функції адаптерів:

- гальванічна розв'язка комп'ютера і кабелю локальної мережі (використовується передача сигналів через імпульсні трансформатори);

- перетворення логічних сигналів в мережеві (електричні або світлові) і навпаки;

- кодування і декодування мережевих сигналів (наприклад, манчестерський код);

- упізнання пакетів, що приймаються (вибір зі всіх пакетів, що приходять, тих, які адресовані даному абонентові або всім абонентам мережі одночасно);

- перетворення паралельної коди в послідовний при передачі і зворотне перетворення при прийомі;

- буферизація інформації в буферній пам'яті адаптера;

- організація доступу до мережі відповідним методом управління обміном;

- підрахунок контрольної суми пакетів при передачі і прийомі.

Якщо комп'ютер хоче передати пакет, то він спочатку формує цей пакет в своїй пам'яті, потім пересилає його в буферну пам'ять мережевого адаптера і дає

команду адаптеру на передачу. Адаптер аналізує поточний стан мережі і при першій же нагоді видає пакет в мережу (виконує управління доступом до мережі). При цьому він проводить перетворення інформації з буферної пам'яті в послідовний вигляд для побітної передачі по мережі, підраховує контрольну суму, кодує біти пакету в мережевий код і через вузол гальванічної розв'язки видає пакет в кабель мережі. Буферна пам'ять в даному випадку дозволяє звільнити комп'ютер від контролю стану мережі, а також забезпечити потрібний для мережі темп видачі інформації.

Якщо по мережі приходить пакет, то мережевий адаптер через вузол гальванічної розв'язки приймає біти пакету, проводить їх декодування з мережевої коди і порівнює мережеву адресу приймача з пакету зі своєю власною адресою. Адреса мережевого адаптера, як правило, встановлюється виробником адаптера. Якщо адреса співпадає, то мережевий адаптер записує пакет, що прийшов, в свою буферну пам'ять і повідомляє комп'ютер (зазвичай - сигналом апаратного переривання) про те, що прийшов пакет і його треба читати. Одночасно із записом пакету робиться підрахунок контрольної суми, що дозволяє до кінця прийому зробити вивід, чи є помилки в цьому пакеті. Буферна пам'ять в даному випадку знову ж таки дозволяє звільнити комп'ютер від контролю мережі, а також забезпечити високий ступінь готовності мережевого адаптера до прийому пакетів.

Трансивери або *приймачі* (від англ. *Transmitter + receiver*) служать для передачі інформації між адаптером і кабелем мережі або між двома сегментами (частинами) мережі. Трансивери підсилюють сигнали, перетворюють їх рівні або перетворюють сигнали в іншу форму (наприклад, з електричної в світлову і назад). Трансиверами також часто називають вбудовані в адаптер приймачі.

Репітери або *повторітелі* (*repeater*) виконують простішу функцію, ніж трансивери. Вони не перетворять ні рівні сигналів, ні їх фізичну природу, а тільки відновлюють ослаблені сигнали (їх амплітуду і форму), приводячи їх до початкового вигляду. Мета такої ретрансляції сигналів полягає виключно в збільшенні довжини мережі

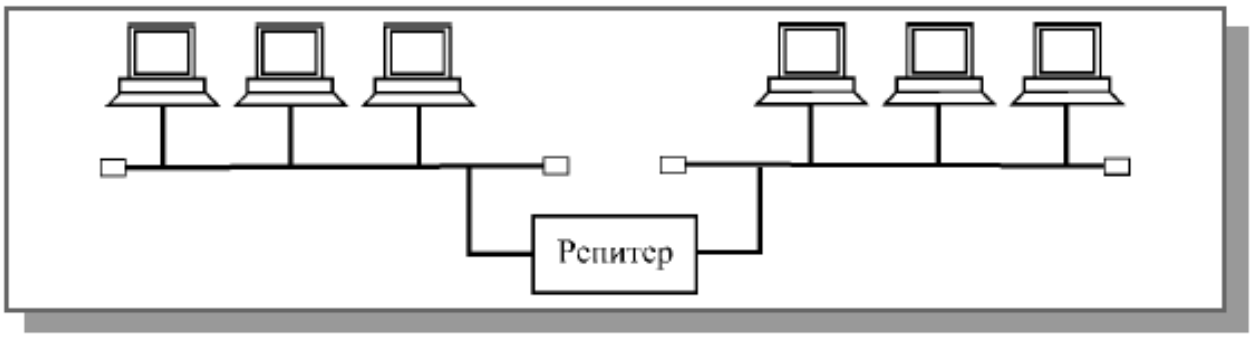


Рис.3.2. Принцип підключення репітера

Концентратори (хаби, *hub*), як випливає з їх назви, служать для об'єднання в мережу декількох сегментів. Концентраторами (або репітерниє концентратори) є декілька зібраних в єдиному конструктиві репітерів, вони виконують ті ж функції, що і репітери.

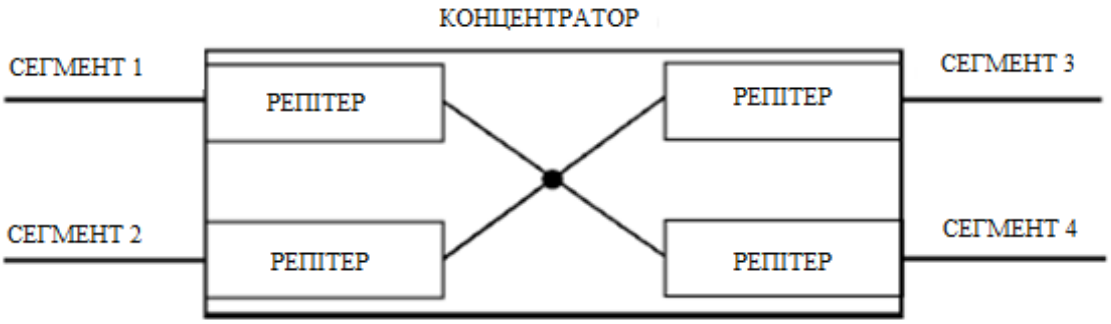


Рис. 3.3. Принцип підключеннння

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

Комутатори (світч, англ. *switch*), як і концентратори, служать для з'єднання сегментів в мережу. Вони також виконують складніші функції, проводячи сортування пакетів, що поступають на них.

Комутатори передають з одного сегменту мережі в іншій не всі пакети, що поступають на них, а тільки ті, які адресовані комп'ютерам з іншого сегменту. Пакети, що передаються між абонентами одного сегменту, через комутатор не проходять. При цьому сам пакет комутатором не приймається, а тільки пересилається. Інтенсивність обміну в мережі знижується унаслідок розділення навантаження, оскільки кожен сегмент працює не тільки зі своїми пакетами, але і з пакетами, що прийшли з інших сегментів.

Комутатор працює на другому рівні моделі OSI (підрівень MAC), оскільки аналізує MAC-адреса усередині пакету. Природно, він виконує і функції першого рівня.

Мости (англ. *bridge*) - найбільш прості пристрої, що служать для об'єднання мереж з різними стандартами обміну, наприклад, Ethernet і Arcnet, або декількох сегментів (частин) однієї і тієї ж мережі, наприклад, Ethernet. У останньому випадку міст, як і комутатор, тільки розділяє навантаження сегментів, підвищуючи тим самим продуктивність мережі в цілому. На відміну від комутаторів мости приймають пакети, що поступають, цілком і у разі потреби проводять їх просту обробку. Мости, як і комутатори, працюють на другому рівні моделі OSI, але на відміну від них можуть захоплювати також і верхній підрівень LLC другого рівня (для зв'язку різнорідних мереж). Останнім часом мости швидко витісняються комутаторами, які стають більш функціональними.

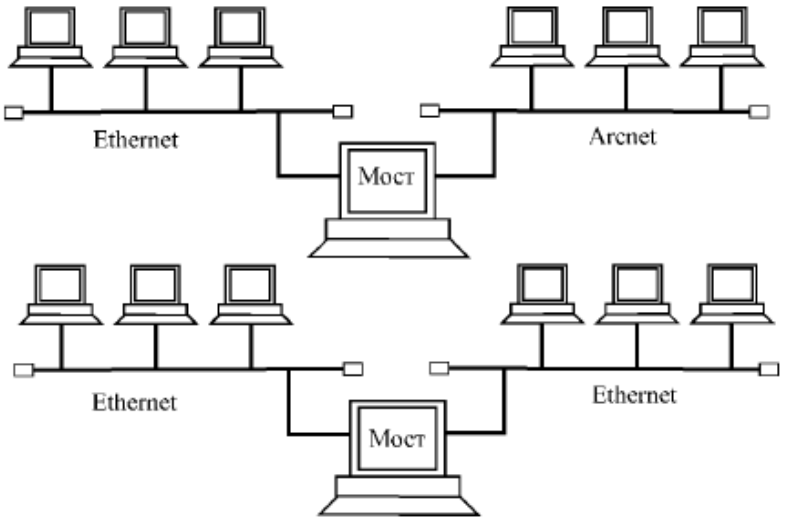


Рис.3.4. Мости в мережі

Маршрутизатори (англ. *router*) здійснюють вибір оптимального маршруту для кожного пакету з метою уникнення надмірного навантаження окремих ділянок мережі і обходу пошкоджених ділянок. Вони застосовуються, як правило, в складних розгалужених мережах, що мають декілька маршрутів між окремими абонентами. Маршрутизатори не перетворюють протоколи нижніх рівнів, тому вони з'єднують тільки сегменти однойменних мереж.

Маршрутизатори працюють на третьому рівні моделі OSI, оскільки вони аналізують не тільки MAC-адреса пакету, але і IP-адреса, тобто більш глибоко проникають в інкапсульований пакет.

Шлюзи (англ. *gateway*) - це пристрої для з'єднання мереж з різними протоколами, наприклад, для з'єднання локальних мереж з великими комп'ютерами або з глобальними мережами. Це найдорожчі і рідко вживані мережеві пристрої. Шлюзи реалізують зв'язок між абонентами на верхніх рівнях моделі OSI (з четвертого по сьомий). Відповідно, вони повинні виконувати і всі функції нижчерозташованих рівнів.

4 ПРОТОКОЛИ ЛОКАЛЬНИХ МЕРЕЖ.

4.1 Стандартні мережеві протоколи

Протоколи - це набір правил і процедур, регулюючих порядок здійснення зв'язку. Комп'ютери, що беруть участь в обміні, повинні працювати по одних і тих же протоколах, щоб в результаті передачі вся інформація відновлювалася в первинному вигляді.

Зв'язок мережевого адаптера з мережевим програмним забезпеченням здійснюють *драйвери* мережевих адаптерів. Саме завдяки драйверу комп'ютер може не знати ніяких апаратних особливостей адаптера (його адрес, правил обміну з ним, його характеристик). Драйвер уніфікує, робить одноманітною взаємодію програмних засобів високого рівня з будь-яким адаптером даного класу. Мережеві драйвери, що поставляються разом з мережевими адаптерами, дозволяють мережевим програмам однаково працювати з платами різних постачальників і навіть з платами різних локальних мереж (Ethernet, Arcnet, Token-ring і так далі).

Драйвери, як правило, виконують функції канального рівня, хоча іноді вони реалізують і частину функцій мережевого рівня. Наприклад, драйвери формують пакет, що передається, в буферній пам'яті адаптера, читають з цієї пам'яті пакет, що прийшов по мережі, дають команду на передачу, інформують комп'ютер про прийом пакету.

Існує декілька стандартних наборів (або, як їх ще називають, стеків) протоколів, що набули зараз широкого поширення:

* набір протоколів ISO/OSI;
* IBM System Network Architecture (SNA);
* Digital Decnet;
* Novell Netware;
* Apple AppleTalk;
* набір протоколів глобальної мережі Інтернет, TCP/IP.

Включення в цей список протоколів глобальної мережі цілком обґрунтовано, адже, як вже наголошувалося, модель OSI використовується для будь-якої відкритої системи: на базі як локальної, так і глобальної мережі або комбінації локальної і глобальної мереж.

Протоколи перерахованих наборів діляться на три основні типи:

1. Прикладні протоколи (виконуючі функції трьох верхніх рівнів моделі OSI - прикладного, представницького і сеансового);

2. Транспортні протоколи (що реалізовують функції середніх рівнів моделі OSI - транспортного і сеансового);

3. Мережеві протоколи (здійснюючі функції трьох нижніх рівнів моделі OSI).

Прикладні протоколи забезпечують взаємодію додатків і обмін даними між ними:

***FTAM (**File Transfer Access and Management) - протокол OSI доступу до файлів;

*X.400 - протокол CCITT для міжнародного обміну електронною поштою;

*X.500 - протокол CCITT служб файлів і каталогів на декількох системах;

***SMTP** (Simple Mail Transfer Protocol) – протокол Інтернет для обміну ел. поштою;

***FTP** (File Transfer Protocol) – протокол Інтернет для передачі файлів;

***SNMP** (Simple Network Management Protocol) - протокол для моніторингу мережі, контролю за роботою мережевих компонентів і управління ними;

***Telnet**–протокол Інтернет для реєстрації на серверах і обробки даних на них;

*Microsoft SMBs (Server Message Blocks, блоки повідомлень сервера) і клієнтські оболонки або редіректори фірми Microsoft;

***NCP** (Netware Core Protocol) надбудова над IPX, що використовується для обміну між робочої станцією та сервером.

Транспортні протоколи підтримують сеанси зв'язку між комп'ютерами і гарантують надійний обмін даними між ними:

*__TCP__ (Transmission Control Protocol) - частина набору протоколів TCP/IP для гарантованої доставки даних, розбитих на послідовність фрагментів;

*__SPX__ - частина набору протоколів IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) для гарантованої доставки даних, розбитих на послідовність фрагментів, запропонованих компанією Novell;

*__NWLink__ - реалізація протоколу IPX/SPX компанії Microsoft;

*__NETBEUI__ - (NETBIOS Extended User Interface, розширений інтерфейс NETBIOS) встановлює сеанси зв'язку між комп'ютерами (NETBIOS) і надає верхнім рівням транспортні послуги (NETBEUI).

Мережеві протоколи управляють адресацією, маршрутизацією, перевіркою помилок і запитами на повторну передачу.

* **IP** (Internet Protocol) - TCP/IP-протокол для негарантованої передачі пакетів без встановлення з'єднань;

* **IPX** (Internetwork Packet Exchange) - протокол компанії Netware для негарантованої передачі пакетів і маршрутизації пакетів;

* **NWLink** - реалізація протоколу IPX/SPX компанії Microsoft;

* **NETBEUI** - транспортний протокол, що забезпечує послуги транспортування даних для сеансів і застосувань NETBIOS.

4.2 Методи взаємодії абонентів в мережі

Модель OSI допускає два основні методи взаємодії абонентів в мережі:

1) без логічного з'єднання (метод дейтаграм)
2) з логічним з'єднанням.

Метод дейтаграм - це простий метод, в якому кожен пакет передається без встановлення логічного каналу, тобто без попереднього обміну службовими пакетами для з'ясування готовності приймача, а також без ліквідації логічного каналу, тобто без пакету підтвердження закінчення передачі. Дійде пакет до приймача чи ні - невідомо (перевірка факту отримання переноситься на вищі рівні). Приклади протоколів: IP, IPX.

Переваги

- передавач і приймач працюють незалежно один від одного;
- пакети можуть накопичуватися в буфері і потім передаватися разом;
- є можливість використовувати широкомовну передачу, тобто адресувати пакет всім абонентам одночасно;

недоліки.

- підвищені вимоги до апаратури (приймач завжди повинен бути готовий до прийому пакету);
- можливість втрати пакетів;
- даремне завантаження мережі пакетами у разі відсутності або неготовності приймача.

При *методі з логічним з'єднанням* пакет передається тільки після того, як буде встановлено логічне з'єднання (канал) між приймачем і передавачем. Кожному інформаційному пакету супроводить один або декілька службових пакетів (установка з'єднання, підтвердження отримання, запит повторної передачі, розривши з'єднання). Логічний канал може встановлюватися на час передачі одного або декількох пакетів. Приклади протоколів: TCP, SPX.

Переваги

- більш надійний ніж метод дейтаграм;;
- немає перенавантаження системи;

недоліки

- більш складний ніж метод дейтаграм;
- складно розв'язати ситуацію коли абонент по тій чи інший причині не готовий до обміну;
- немає можливості організувати передачу широкомовних пакетів, оскільки неможливо організувати логічні канали одразу з усіма абонентами.

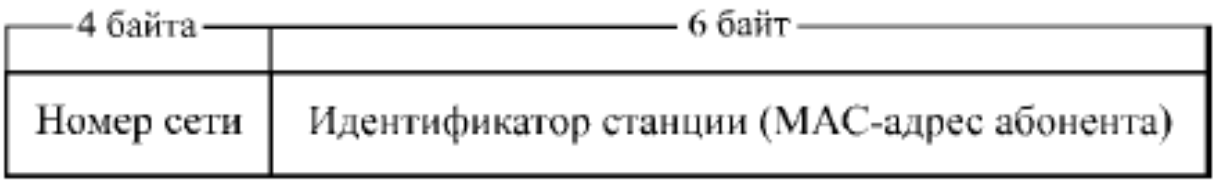
Протоколи IPX/SPX, розроблені компанією Novell, утворюють набір (стек), використовуваний в мережевих програмних засобах досить широко поширених локальних мереж Novell (Netware). Це порівняно невеликий і швидкий протокол, що підтримує маршрутизацію. Прикладні програми можуть звертатися

безпосередньо до рівня IPX, наприклад, для посилки широкомовних повідомлень, але значно частіше працюють з рівнем SPX, що гарантує швидку і надійну доставку пакетів. Якщо швидкість не дуже важлива, то прикладні програми застосовують ще вищий рівень, наприклад, протокол NETBIOS, що надає зручний сервіс. Компанією Microsoft запропонована своя реалізація протоколу IPX/SPX, звана NWLink. Протоколи IPX/SPX і NWLink підтримуються операційними системами Netware і Windows. Вибір цих протоколів забезпечує сумісність по мережі будь-яких абонентів з даними операційними системами.

Набір (стек) протоколів TCP/IP був спеціально розроблений для глобальних мереж і для міжмережевої взаємодії. Він орієнтований на низьку якість каналів зв'язку, на велику вірогідність помилок і розривів зв'язків. Цей протокол прийнятий в усесвітній комп'ютерній мережі Інтернет, значна частина абонентів якої підключається по комутованих лініях (тобто звичайним телефонним лініям). Як і протокол IPX/SPX, протокол TCP/IP також підтримує маршрутизацію. На його основі працюють протоколи високих рівнів, такі як SMTP, FTP, SNMP. Недолік протоколу TCP/IP - більш низька швидкість роботи, чим у IPX/SPX. Проте зараз протокол TCP/IP використовується і в локальних мережах, щоб спростити узгодження протоколів локальних і глобальних мереж. В даний час він вважається основним в найпоширеніших операційних системах.

Формати IP та IPX адрес.

Як протокол IPX, так і протокол IP є самими низькорівневими протоколами, тому вони безпосередньо інкапсулюють свою інформацію, що називається дейтаграмой, в поля даних пакету, що передається по мережі. При цьому в заголовок дейтаграми входять адреси абонентів (відправника і одержувача) більш високого рівня, ніж MAC-адреса, - це IPX-адреса для протоколу IPX або IP-адреса для протоколу IP. Ці адреси включають номери мережі і вузла, хоста (індивідуальний ідентифікатор абонента). При цьому IPX-адреса простіші, мають всього один формат, а в IP-адрес можуть входити три формати (класу A,B і C), що розрізняються значеннями трьох початкових бітів.



Протокол NetBIOS

Протокол NETBIOS (мережева базова система введення/виводу) був розроблений компанією IBM для мереж IBM PC Network і IBM Token-ring за зразком системи BIOS персонального комп'ютера. З тих пір цей протокол став фактичним стандартом (офіційно він не стандартизований), і багато мережевих операційних систем містять в собі емулятор NETBIOS для забезпечення сумісності. Спочатку NETBIOS реалізовував сеансовий, транспортний і мережевий рівні, проте в подальших мережах на нижчих рівнях використовуються стандартні протоколи (наприклад, IPX/SPX), а на долю емулятора NETBIOS залишається тільки сеансовий рівень. NETBIOS забезпечує вищий рівень сервісу, чим IPX/SPX, але працює повільніше.

На основі протоколу NETBIOS був розроблений протокол NETBEUI, який є розвитком протоколу NETBIOS до транспортного рівня. Проте недолік NETBEUI полягає в тому, що він не підтримує міжмережеву взаємодію і не забезпечує маршрутизацію. Тому даний протокол використовується тільки в простих мережах, не розрахованих на підключення до Інтернет. Складні мережі орієнтуються на більш універсальні протоколи TCP/IP і IPX/SPX. Протокол

NETBEUI в даний час вважається застарілим, хоча навіть в операційній системі Windows XP передбачена його підтримка, правда, тільки як додаткова опція.

4.3 Призначення та адресація пакетів. Методи управління обміном інформації в локальних мережах

Інформація в локальних мережах, як правило, передається окремими порціями, шматками, званими в різних джерелах *пакетами* (*packets*), *кадрами* (*frames*) або *блоками*. Причому гранична довжина цих пакетів строго обмежена (зазвичай величиною в декілька кілобайт). Обмежена довжина пакету і знизу (як правило, декількома десятками байт). Вибір пакетної передачі пов'язаний з декількома важливими міркуваннями.

Існує деяка оптимальна довжина пакету (або оптимальний діапазон довжин пакетів), при якій середня швидкість обміну інформацією по мережі буде максимальна. Ця довжина не є незмінною величиною, вона залежить від рівня перешкод, методу управління обміном, кількості абонентів мережі, характеру інформації, що передається, і від багатьох інших чинників. Є діапазон довжин, який близький до оптимуму.

Структура і розміри пакету в кожній мережі жорстко визначені стандартом на дану мережу і зв'язані, перш за все, з апаратурними особливостями даної мережі, вибраною топологією і типом середовища передачі інформації. Крім того, ці параметри залежать від протоколу (порядку обміну інформацією), що використовується.

Типова структура пакету.

Стартова комбінація бітів або преамбула, яка забезпечує попереднє настроювання апаратури адаптера або іншого мережевого пристрою на прийом і обробку пакету. Це поле може бути повністю відсутнім або ж зводитися до єдиного стартового біта.

Рис.4.1. Типова структура пакету

Мережева адреса (ідентифікатор) приймаючого абонента, тобто індивідуальний або груповий номер, привласнений кожному приймаючому абонентові в мережі. Ця адреса дозволяє приймачу розпізнати пакет, адресований йому особисто, групі, в яку він входить, або всім абонентам мережі одночасно (при широкому віщанні).

Мережева адреса (ідентифікатор) передавального абонента, тобто індивідуальний номер, привласнений кожному передавальному абонентові. Ця адреса інформує приймаючого абонента, звідки прийшов даний пакет.

Службова інформація, яка може указувати на тип пакету, його номер, розмір, формат, маршрут його доставки, на те, що з ним треба робити приймачу і т.д.

Дані (поле даних) - це та інформація, яку передає пакет. Поле даних має змінну довжину, яка, власне, і визначає повну довжину пакету. Існують спеціальні пакети, що управляють, які не мають поля даних. Їх можна розглядати як мережеві команди.

Контрольна сума пакету - це числовий код, що формується передавачем по певних правилах і що містить в згорнутому вигляді інформацію про весь пакет. Приймач, повторюючи обчислення, зроблені передавачем, з прийнятим пакетом, порівнює їх результат з контрольною сумою і робить вивід про правильність або

помилковість передачі пакету. Якщо пакет помилковий, то приймач запрошує його повторну передачу. Зазвичай використовується циклічна контрольна сума (*CRC*).

Стопова комбінація служить для інформування апаратури приймаючого абонента про закінчення пакету, забезпечує вихід апаратури приймача із стану прийому. Це поле дозволяє визначати момент закінчення передачі пакету.

Багаторівнева система вкладення пакетів

При реальному обміні по мережі застосовуються багаторівневі протоколи, кожен з рівнів яких припускає свою структуру пакету (адресацію, інформацію, що управляє, формат даних і так далі). Адже протоколи високих рівнів мають справу з такими поняттями, як файл-сервер або додаток, що запрошує дані у іншого застосування, і цілком можуть не мати уявлення ні про тип апаратури мережі, ні про метод управління обміном. Всі пакети вищих рівнів послідовно вкладаються в пакет, що передається, в поле даних. Цей процес послідовної упаковки даних для передачі називається також *інкапсуляцією* пакетів. Зворотний процес послідовного розпаковування даних приймачем називається *декапсуляцією* пакетів.

Кожен абонент (вузол) локальної мережі повинен мати свою унікальну адресу (ідентифікатор або *MAC*-адрес), для того, щоб йому можна було адресувати пакети. Існують дві основні системи привласнення адрес абонентам мережі (точніше, мережевим адаптерам цих абонентів).

Перша система (мережа *Arcnet*) зводиться до того, що при установці мережі кожному абонентові користувач привласнює індивідуальну адресу по порядку, наприклад, від 0 до 30 або від 0 до 254. Привласнення адрес проводиться програмно або за допомогою перемикачів на платі адаптера. При цьому необхідна кількість розрядів адреси визначається з нерівності:

$$2^n > N_{max}$$

де n - кількість розрядів адреси, а N_{max} - максимально можлива кількість абонентів в мережі. Наприклад, вісім розрядів адреси достатні для мережі з 255 абонентів. Одна адреса (зазвичай 1111....11) відводиться для широкомовної

передачі, тобто він використовується для пакетів, адресованих всім абонентам одночасно.

Переваги:

- малий об'єм службової інформації в пакеті;
- простота апаратури адаптера, що розпізнає адресу пакету.

Недоліки

- трудомісткість завдання адрес і можливість помилки (наприклад, двом абонентам мережі може бути привласнений одна і та ж адреса). Контроль унікальності мережевих адрес всіх абонентів покладається на адміністратора мережі.

MAC-адреса.

Другий підхід до адресації був розроблений міжнародною організацією IEEE, яка займається стандартизацією мереж. Саме він використовується в більшості мереж і рекомендований для нових розробок. Ідея цього підходу полягає в тому, щоб привласнювати унікальну мережеву адресу кожному адаптеру мережі ще на етапі його виготовлення.

MAC-адреса (від англ. Media Access Control - управління доступом до середовища) - це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж.

1	**1**	**22 біта**	**24 біта**
I/G	U/L	OUI (ідентифікатор)	OUA (мережева адреса)

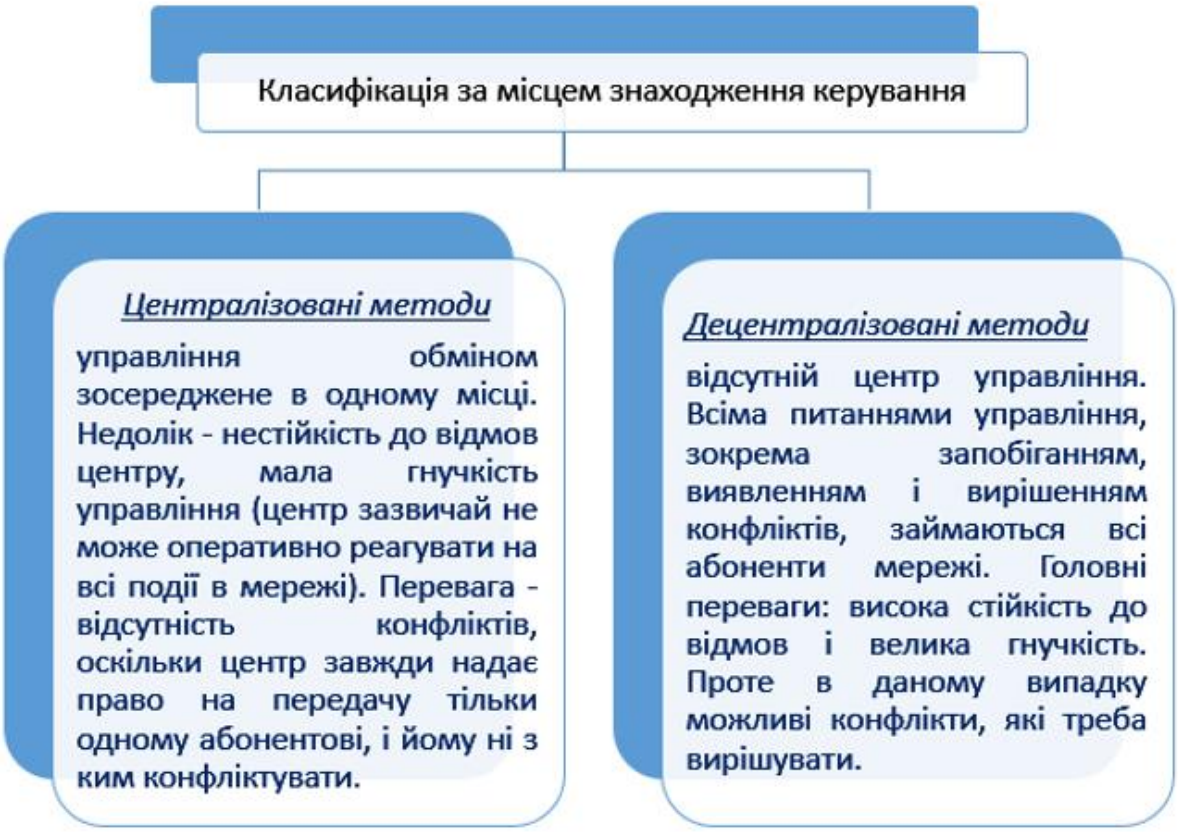
* OUA (Organizationally Unique Address) - організаційно унікальна адреса. Їх привласнює кожен із зареєстрованих виробників мережевих адаптерів.

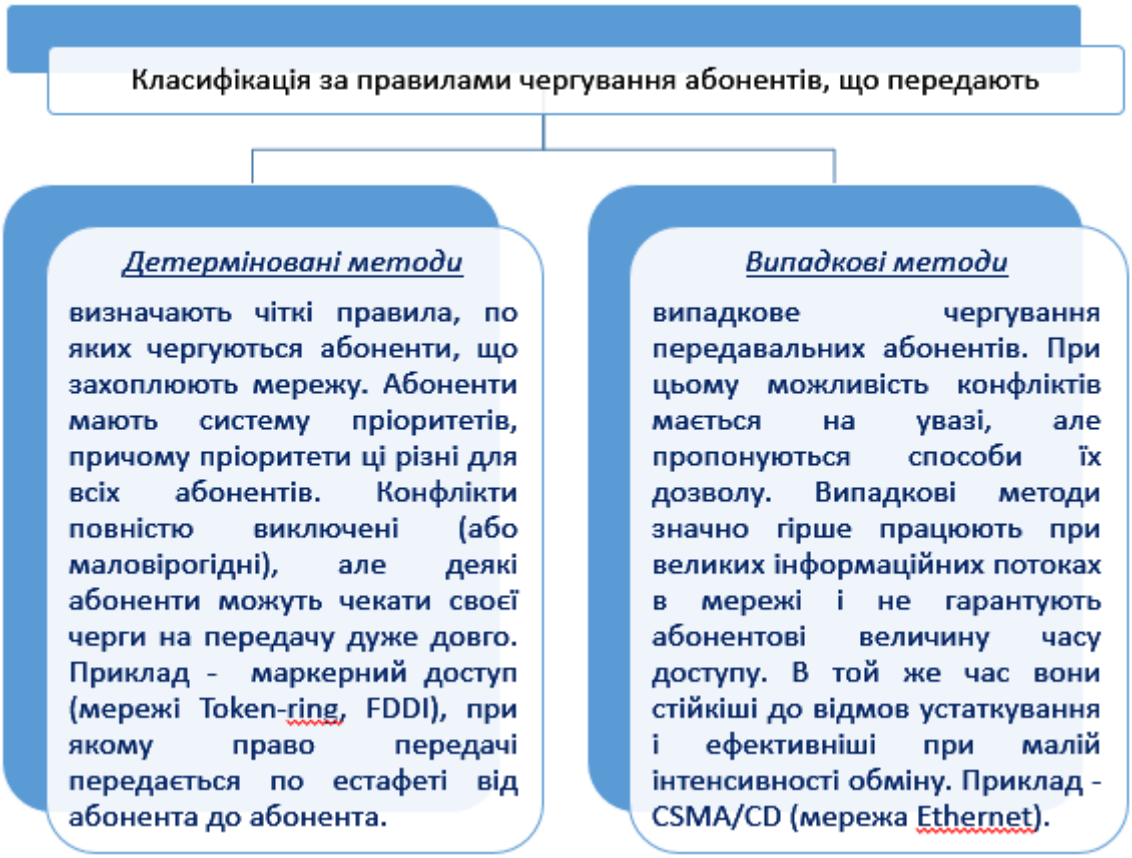
* OUI (Organizationally Unique Identifier) - організаційно унікальний ідентифікатор. IEEE привласнює один або декілька OUI кожному виробникові мережевих адаптерів.

* I/G (Individual/group) указує на тип адреси. Якщо він встановлений в 0, то індивідуальний, якщо в 1, то груповий (багатопунктовий або функціональний). Пакети з груповою адресою отримають всі мережеві адаптери, що мають цю групову адресу.

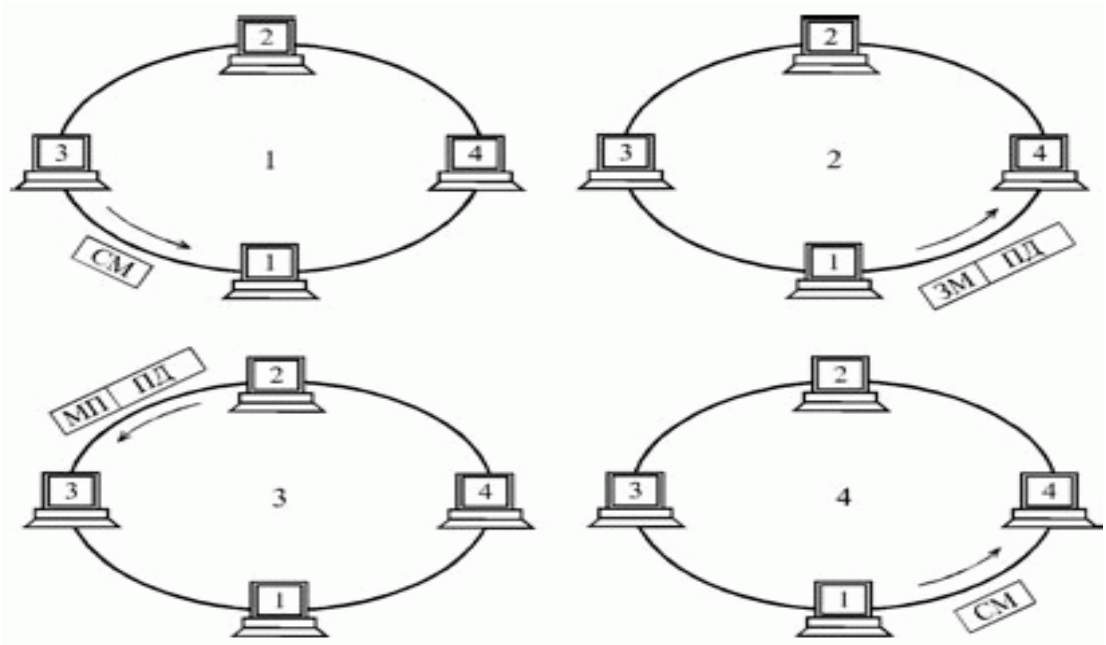
* U/L (Universal/local) прапор управління. Зазвичай він встановлений в 0. Установка біта в 1 означає, що адреса задана не виробником мережевого адаптера, а організацією, що використовує дану мережу.

Методи управління обміном:





Маркерний метод управління обміном



СМ - вільний маркер, ЗМ - зайнятий маркер,

МП - зайнятий маркер з підтвердженням, ПД-пакет даних

1. Абонент 1, охочий передати свій пакет, повинен дочекатися приходу до нього вільного маркера. Потім він приєднує до маркера свій пакет, позначає маркер як зайнятий і відправляє цю посилку наступному по кільцю абонентові.

2. Решта всіх абонентів (2, 3, 4), отримавши маркер з приєднаним пакетом, перевіряють, чи їм адресований пакет. Якщо пакет адресований не ним, то вони передають отриману посилку (маркер + пакет) далі по кільцю.

3. Якщо якийсь абонент (в даному випадку це абонент 2) розпізнає пакет як адресований йому, то він його приймає, встановлює в маркері біт підтвердження прийому і передає посилку (маркер + пакет) далі по кільцю.

4. Абонент, що передавав, 1 отримує свою посилку, що пройшла по всьому кільцю, назад, позначає маркер як вільний, видаляє з мережі свій пакет і посилає вільний маркер далі по кільцю. Абонент, охочий передавати, чекає цього маркера, і все повторюється знову.

Пріоритет при даному методі управління виходить географічний, тобто право передачі після звільнення мережі переходить до наступного по напряму кільця абонента від останнього абонента, що передавав. Але ця система пріоритетів працює тільки при великій інтенсивності обміну. При малій інтенсивності обміну всі абоненти рівноправні, і час доступу до мережі кожного з них визначається тільки положенням маркера у момент виникнення заявки на передачу.

Основна перевага маркерного методу перед CSMA/CD полягає в гарантованій величині часу доступу.

Метод маркерного доступу використовується не тільки в кільці (наприклад, в мережі IBM Token Ring або FDDI), але і в шині (зокрема, мережа ARCNET-BUS), а також в зірці (наприклад, мережа ARCNET-STAR). У цих випадках реалізується не фізичне, а логічне кільце, тобто всі абоненти послідовно передають один одному маркер, і цей ланцюжок передачі маркерів замкнутий в кільце.

Метод управління обміном CSMA/CD

CSMA/CD (*Carrier Sense Multiple Access with Collision Detection* - множинний доступ з контролем тієї, що несе і виявленням колізій) – технологія множинного доступу до загального передавального середовища в локальній комп'ютерній мережі з контролем колізій. CSMA/CD відноситься до децентралізованним випадкових методів. Він використовується як в звичайних мережах типу Ethernet, так і у високошвидкісних мережах (Fast Ethernet, Gigabit Ethernet).

Технологія доступу.

Якщо під час передачі кадру робоча станція виявляє інший сигнал, що займає передавальне середовище, вона зупиняє передачу, посилає *jam signal* і чекає протягом випадкового проміжку часу (відомого як «*Backoff delay*» і находімого за допомогою алгоритму *truncated binary exponential backoff*), перш ніж знову відправити фрейм. Виявлення колізій використовується для поліпшення продуктивності CSMA за допомогою переривання передачі відразу після виявлення колізії і зниження вірогідності другої колізії під час повторної передачі.

При описі тимчасових діаграм мереж типу Ethernet, а також граничних розмірів пакетів (кадрів) широко використовуються наступні терміни:

IPG (interpacket gap, міжпакетна щілина) - мінімальний проміжок часу між передаваними пакетами (9,6 мкс для Ethernet / 0,96 мкс для Fast Ethernet).

BT (Bit Time, час бита) - інтервал часу для передачі одного біта (100 нс для Ethernet / 10 нс для Fast Ethernet).

PDV (Path Delay Value, значення затримки в дорозі) - час кругового проходження сигналу між двома вузлами мережі.

Collision window (вікно колізій) - максимальне значення PDV.

Collision domain (область колізій, зона конфлікту) - частина мережі, на яку розповсюджується ситуація колізії, конфлікту.

Slot time (час каналу) – макс.допустиме вікно колізій для сегменту (512*ВТ).

Minimum frame size - мінімальний розмір кадру (512 біт).

Maximum frame size - максимальний розмір кадру (1518 байт).

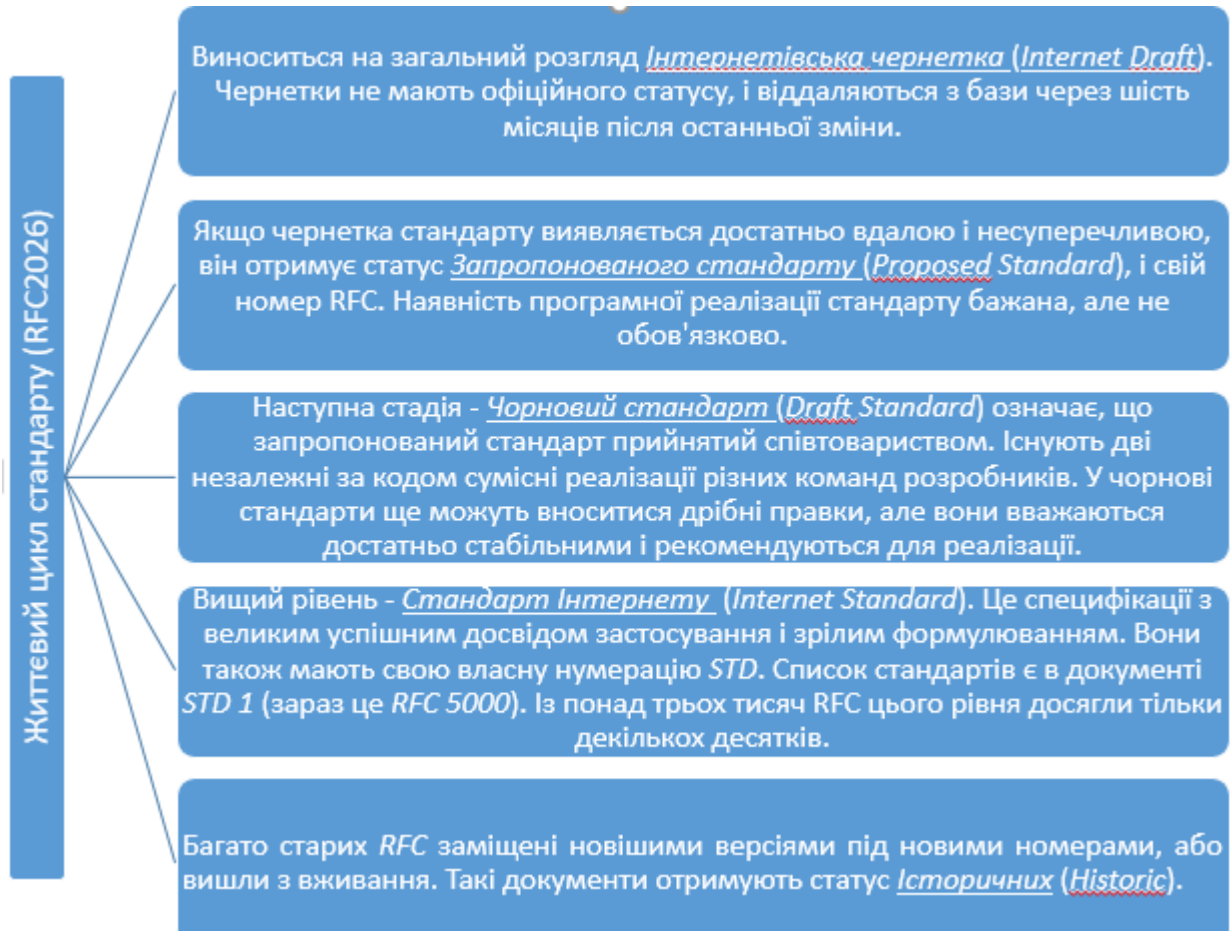
Maximum network diameter (максимальний діаметр мережі) – макс. допустима довжина сегменту, при якій його вікно колізій ≤ slot time.

Truncated binary exponential back off (усічене двійкове експоненціальне відстрочення) - затримка перед наступною спробою передачі пакету після колізії (максимум 16 спроб).

5 СТЕК ПРОТОКОЛІВ TCP/IP

5.1 Фізичний рівень стеку протоколів TCP/IP

Запит коментарів (англ. Request for Comments, RFC) - документ з серії пронумерованих інформаційних документів Інтернету, що містять технічні специфікації і Стандарти, що використовуються в Інтернеті. Назву «Request for Comments» ще можна перевести як «заявка на обговорення» або «тема для обговорення». В даний час первинною публікацією документів RFC займається IETF (Спеціальна комісія інтернет розробок) під егідою відкритої організації Суспільство Інтернету (англ. Internet Society, ISOC). Правами на RFC володіє саме Суспільство Інтернету.



TCP/IP розроблений DARPA (Defense Advanced Research Projects Agency) Міністерство оборони США в 70-х роках. Метою його розробки було створення

можливості для обміну інформацією між різними комп'ютерами, незалежно від їх місцеположення.

Протоколи TCP/IP в моделі OSI

Рівень OSI	TCP/IP	Приклади протоколів
Прикладний	Прикладний	DNS, DHCP, RIP, BGP, HTTP, SMTP, SNMP, FTP, Telnet, scp, SMB, NFS, RTSP, BGP
Представницький		XML, XDR, ASN.1, AFP
Сеансовий		TLS, SSL, ISO 8327 / CCITT X.225, RPC, NetBIOS, ASP
Транспортний	Транспортний	TCP, UDP, RTP, SCTP, SPX, ATP, DCCP, GRE
Мережевий	Мережний	IP, ICMP, IGMP, CLNP, OSPF, IPX, DDP
Канальний	Фізичний	ARP, Ethernet, Token ring, PPP, HDLC, X.25, Frame relay, ISDN, ATM, MPLS, Wi-Fi, RARP
Фізичний		електричні дроти, радіозвязок, оптоволоконні дроти

Адресація у IP-мережах

IP-адрес (ай-пі адреса, скорочення від англ. *Internet Protocol Address*) - унікальний ідентифікатор (адреса) пристрою (зазвичай комп'ютера), підключеного до локальної мережі і (або) Інтернету.

IP-адрес є 32-бітове (за версією IPv4) або 128-бітове (за версією IPv6) двійкове число. Зручною формою запису IP-адреса (IPv4) є запис у вигляді чотирьох десяткових чисел (від 0 до 255), розділених крапками.

Ідентифікатор мережі				Ідентифікатор вузла		
128	.	121	.	188	.	201

IANA (від англ. *Internet Assigned Numbers Authority* - «Адміністрація адресного простору Інтернет») - американська організація, що управляє просторами IP-адресов, доменів верхнього рівня. *IANA* відповідає за розподіл всіх зарезевірованних імен і номерів, які використовуються в протоколах, визначених в *RFC*. *IANA* делегує свої повноваження по розподілу IP-адресов регіональним реєстраторам у вигляді діапазонів класу A. Регіональні реєстратори, у свою чергу, делегують дрібніші діапазони інтернет-провайдерам.

Класи IP-адрес

Клас	IP-адрес	Ідентифікатор		Виділяються
		мережі	вузла	
A	w.x.y.z	w	x.y.z	організаціям з великою кількістю вузлів. Майже усі були виділені багато років по тому.
B	w.x.y.z	w.x	y.z	середнім та великим мережам. Їх непросто отримати, ще є незайняті.
C	w.x.y.z	w.x.y	z	невеликим мережам.
D	w.x.y.z	w.x.y	z	для широковіщаючих повідомлень.
E	w.x.y.z	w.x.y	z	для майбутнього користування. Зарезервовані.

Класи IP-адрес і відповідні ідентифікатори мереж та вузлів

Клас	Старші біти	Десятині значення першого октету	Доступна кількість мереж	Доступна кількість вузлів
A	0	1-126	126	16 777 214
B	10	128-191	16 384	65 534
C	110	192-223	2 097 152	254
D	1110	224-239	-	-
E	1111	240-254	-	-

Особливі IP-адреса

1) якщо весь IP-адрес складається тільки з двійкових нулів, то він позначає адресу того вузла, який згенерував цей пакет; цей режим використовується тільки в деяких повідомленнях *ICMP*;

2) якщо в полі номера мережі знаходяться тільки нулі, то за умовчанням вважається, що вузол призначення належить тій же самій мережі, що і вузол, який відправив пакет; цей режим використовується тільки в деяких повідомленнях ICMP;

3) якщо всі двійкові розряди IP-адреса рівні 1, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що знаходяться в тій же мережі, що і джерело цього пакету. Така розсилка називається обмеженим широкомовним повідомленням (*limited broadcast*);

4) якщо в полі номера вузла призначення знаходяться тільки одиниці, то пакет, що має таку адресу, розсилається всім вузлам мережі із заданим номером мережі. Наприклад, в мережі 192.190.21.0 з маскою 255.255.255.0 пакет з

адресою 192.190.21.255 доставляється всім вузлам цієї мережі. Така розсилка називається широкомовним повідомленням (*broadcast*).

Приватні IP-адреса

* 10.0.0.0 - 10.255.255.255. Блок 10 - один мережевий номер класу А.

* 172.16.0.0 - 172.31.255.255. Блок 172 - 16 мережевих номерів класу В.

* 192.168.0.0 - 192.168.255.255. Блок 192 – 256 мережевих номерів класу С.

Маска підмережі

Маскою підмережі або *маскою мережі* називається бітова маска, що визначає, яка частина IP-адреса вузла мережі відноситься до адреси мережі, а яка - до адреси самого вузла в цій мережі. Наприклад, вузол з IP-адресом 12.34.56.78 і маскою підмережі 255.255.255.0 знаходиться в мережі 12.34.56.0/24.

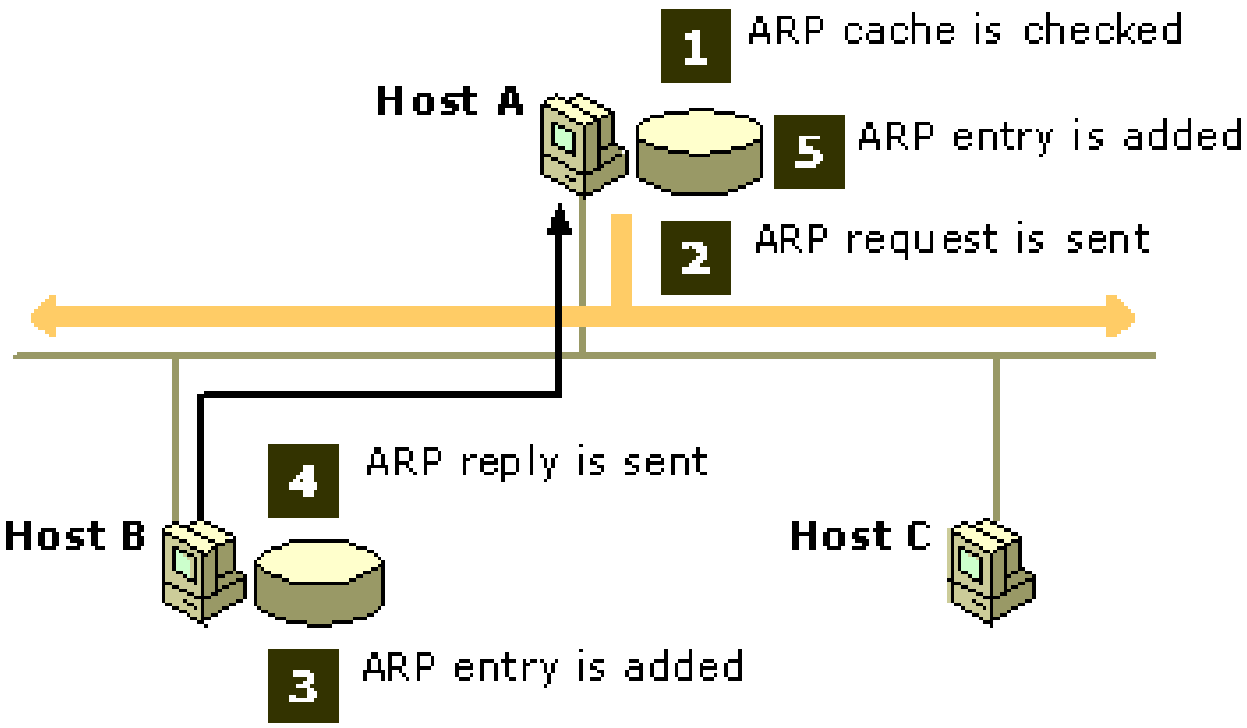
Інший варіант визначення - це визначення підмережі IP-адресов. Наприклад, за допомогою маски підмережі можна сказати, що один діапазон IP-адресов буде в одній підмережі, а інший діапазон відповідно в іншій підмережі.

Щоб отримати адресу мережі, знаючи IP-адрес і маску підмережі, необхідно застосувати до них операцію порозрядної кон'юнкції (логічне І).

Наприклад:

IP-адрес	11000000	10101000	00000001	00000010	192.168.1.2
маска підмережі	11111111	11111111	11111111	00000000	255.255.255.0
адреса мережі	11000000	10101000	00000001	00000000	192.168.1.2

Схема вирішення протоколом ARP IP-адреса в апаратний адрес вузла, що розташований в тій же локальній мережі.



1. На підставі вмісту таблиці маршрутизації вузла А, протокол IP визначає, що для того, щоб пакети досягали вузла В, їх потрібно відправити по IP-адресу 10.0.0.100. Потім вузол А шукає в своєму локальному кеші ARP відповідну апаратну адресу вузла В.

2. Якщо вузол А не може знайти в кеш потрібної адреси, він відправляє широкомовний ARP-запит всім вузлам локальної мережі з питанням «Яка апаратна адреса відповідає IP-адресу 10.0.0.100?» Цей ARP-запит містить в собі програмну (IP) і апаратну адреси джерела - вузла А. Кожен вузол локальної мережі отримує ARP-запит і перевіряє, чи не відповідає його IP-адрес IP-адресу, вказаній в запиті. Якщо IP-адрес вузла не співпадає з вказаною в запиті IP-адресом, вузол відкидає ARP-запит.

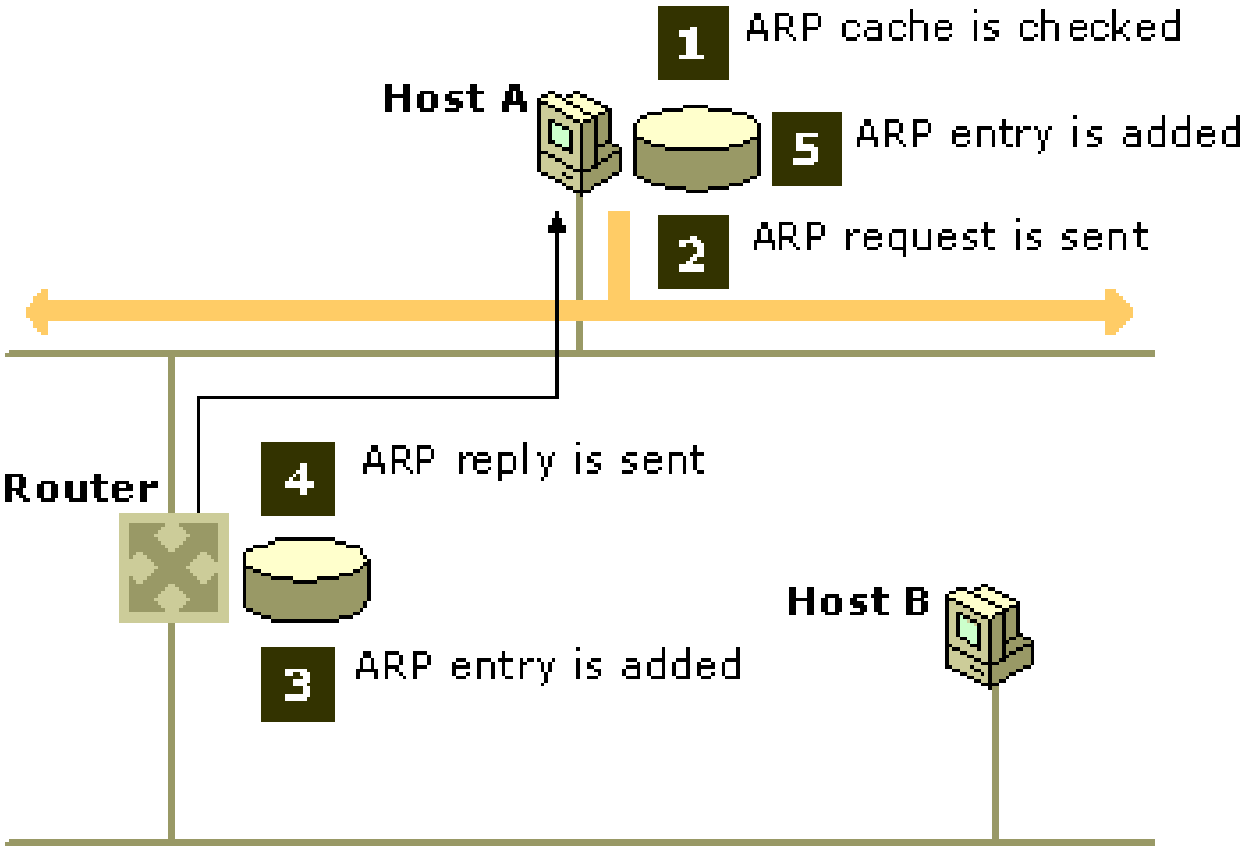
3. Вузол В визначає, що IP-адрес, вказана в ARP-запиті, відповідає його IP-адресу, і додає зіставлення програмної і апаратної адреси вузла А в свій локальний кеш ARP.

4. Вузол В відправляє ARP-ответ, що містить його апаратну адресу, безпосередньо вузлу А.

5. Коли вузол А отримує ARP-ответ від вузла В, він заносить в свій кеш ARP зіставлення програмної і апаратної адрес вузла В. Коли апаратна адреса вузла В

буде визначена, вузол А зможе відправляти IP-трафик вузлу В за апаратною адресою останнього.

Схема вирішення протоколом ARP IP-адреса в апаратний адрес вузла, що розташований в іншій локальній мережі.



1. На підставі вмісту таблиці маршрутизації вузла А, протокол IP визначає, що для того, щоб пакети досягали вузла В, їх потрібно відправити по IP-адресу основного шлюзу - 10.0.0.1. Потім вузол А шукає в своєму локальному кеш *ARP* відповідну апаратну адресу для *IP*-адреса 10.0.0.1.

2. Якщо вузол А не може знайти в кеш потрібної адреси, він відправляє широкомовний ARP-запит всім вузлам локальної мережі з питанням «Яка апаратна адреса відповідає IP-адресу 10.0.0.1?» Цей ARP-запит містить в собі програмну (*IP*) і апаратну (*MAC*) адреси джерела - вузла А. Кожен вузол локальної мережі отримує ARP-запит і перевіряє, чи не відповідає його IP-адрес *IP*-адресу, вказаній в запиті. Якщо IP-адрес вузла не співпадає з вказаною в запиті IP-адресом, вузол відкидає ARP-запит.

3. Маршрутизатор визначає, що IP-адрес вказаний в ARP-запиті, відповідає його IP-адресу, і додає зіставлення програмної і апаратної адреси вузла А в свій локальний кеш *ARP*.

4. Потім маршрутизатор відправляє ARP-відповідь, що містить його апаратну адресу, безпосередньо вузлу А.

5. Коли вузол А отримує ARP-ответ від маршрутизатора, він заносить в свій кеш ARP зіставлення програмної і апаратної адрес для адреси 10.0.0.1.

Кеш ARP

Щоб зменшити число широкомовних запитів, протокол ARP використовує кеш зіставлень IP-адрес і апаратних адрес пристроїв. Кеш ARP може містити як динамічні, так і статичні записи. Динамічні записи додаються і віддаляються автоматично, з часом. Статичні записи залишаються в кеші до тих пір, поки комп'ютер не буде перезавантажений.

Кожен динамічний запис кеш ARP має потенційний час життя, рівний 10 хвилинам. Нові записи, що додаються в кеш, отримують штамп часу. Якщо запис не буде повторно використаний протягом двох хвилин після додавання, термін її життя закінчується і вона віддаляється з кеш ARP. Якщо запис буде повторно використаний, термін її життя збільшується на дві хвилини. Якщо запис буде використаний ще раз, час її життя знову збільшується на дві хвилини; максимальне значення часу життя дорівнює 10 хвилинам.

Порівняння ARP, InARP, RARP

ARP переводить адреси мережевого рівня в адреси канального рівня, в той же час INARP можна розглядати як його інверсію. INARP реалізоване як розширення ARP. Формати пакетів цих протоколів одні і ті ж, розрізняються лише коди операцій і заповнювані поля.

Reverse ARP (RARP), як і InARP, переводить адреси канального рівня в адреси мережевого рівня. Але RARP використовується для отримання логічних адрес самих станцій відправників, тоді як в InARP-протоколі відправник знає свої адреси і запрошує логічну адресу іншої станції. Від RARP відмовилися на користь BOOTP, який був у свою чергу замінений DHCP.

5.2 Мережний та транспортний рівні стеку протоколів TCP/IP.

IP (англ. *Internet Protocol* - міжмережевий протокол) - мережевий протокол, що маршрутизується, основа стека протоколів TCP/IP.

IP - це не орієнтований на встановлення з'єднання і ненадійний протокол передачі датаграм, який орієнтований, головним чином, на адресацію і маршрутизацію пакетів між вузлами.

Термін «не орієнтований на встановлення з'єднання» означає, що сеанс для обміну даними не встановлюється. Термін «ненадійний» означає, що доставка не гарантується. При використанні протоколу IP робиться все можливе для того, щоб пакет був доставлений. IP-пакет може бути втрачений, доставлений поза чергою, дубльований або затриманий. Протокол IP не намагається виправити помилки такого типу. Підтвердження отримання пакетів і повторне звернення за втраченими пакетами входять в круг завдань протоколу більш високого рівня, наприклад TCP.

IP-пакет - форматований блок інформації, що передається по обчислювальній мережі. З'єднання обчислювальних мереж, які не підтримують пакети, такі як традиційні з'єднання типу «крапка-крапка» в телекомунікаціях, просто передають дані у вигляді послідовності байтів, символів або бітів. При використанні пакетного форматування мережа може передавати довгі повідомлення надійніше і ефективно.

Структура IP - дейтаграми (пакета) (IPv4)

4	**8**	**16**	**32**	
Версія	IHL	Тип сервісу	Загальний розмір	
Ідентифікатор			Прапори	Зсув фрагменту
Час життя (TTL)		Протокол	Контрольна сума заголовку	

Адреса відправника (32 бита)
Адреса одержувача (32 бита)
Опції та заповнення (до 320 бітів)
Дані (до 65535 байтів мінус заголовок)

Версія - IPv4 = 4.

IHL - довжина заголовка IP-пакета в 32-бітових словах (dword). Саме це поле указує на початок блоку даних в пакеті. Мінімальне коректне значення для цього поля рівне 5.

Тип обслуговування - байт, що містить набір критеріїв, що визначають тип обслуговування IP-пакетів.

Загальний розмір - розмір дейтаграми в байтах з урахуванням заголовка і даних.

Ідентифікатор - значення, що призначається відправником пакету і призначене для визначення коректної послідовності фрагментів при збірці датаграми. Для фрагментованого пакету всі фрагменти мають однаковий ідентифікатор.

3 біта прапорів. Перший біт повинен бути завжди рівний нулю, другий біт *DF (don't fragment)* визначає можливість фрагментації пакету і третій біт *MF (more fragments)* показує, чи не є цей пакет останнім в ланцюжку пакетів.

Зсув фрагменту - значення, що визначає позицію фрагмента в потоці даних.

Час життя - показує максимальний час існування дейтаграми в мережі Internet. При нульовому значенні цього поля дейтаграма повинна бути знищена. Час життя дейтаграм вимірюється в секундах. Проте, оскільки кожен модуль, що працює з дейтаграмой, повинен зменшувати значення поля *TTL (time-to-life)* принаймні на 1 (навіть у тих випадках, коли обробка дейтаграми займає менше секунди), значення цього поля повинне бути не менше бажаного часу життя

дейтаграми. Дейтаграми з минулим в процесі доставки часом життя не потрапляють до одержувача.

Протокол - ідентифікатор інтернет-протоколу наступного рівня (див. IANA protocol numbers і RFC 1700).

Ідентифікатор	Протокол	RFC
1	ICMP	RFC792
2	IGMP	RFC1112
4	IP	RFC2003
6	TCP	RFC793
17	UDP	RFC768

Контрольна сума заголовку - контрольна сума, розрахована з обліком тільки полів заголовка дейтаграми. Оскільки деякі поля заголовка (наприклад, час життя) можуть мінятися в процесі доставки, значення контрольної суми наново обчислюється і перевіряється в кожній точці обробки заголовків.

Адреса відправника / одержувача - 32-бітові значення адреси відправника і одержувача дейтаграмми.

Опції - поле містить необов'язкові опції дейтаграми.

Дані - дані IP або протоколів рівнів, що розміщені вище.

Протокол міжмережневих управляючих повідомлень ICMP.

Протокол міжмережевих повідомлень *ICMP (Internet Control Message Protocol)* є обов'язковим стандартом *TCP/IP*, описаним в документі *RFC 792, «Internet Control Message Protocol (ICMP)»*. Використовуючи *ICMP*, вузли і маршрутизатори, що зв'язуються по протоколу IP, можуть повідомляти про

помилки і обмінюватися обмеженою інформацією, що управляє, і відомостями про стан.

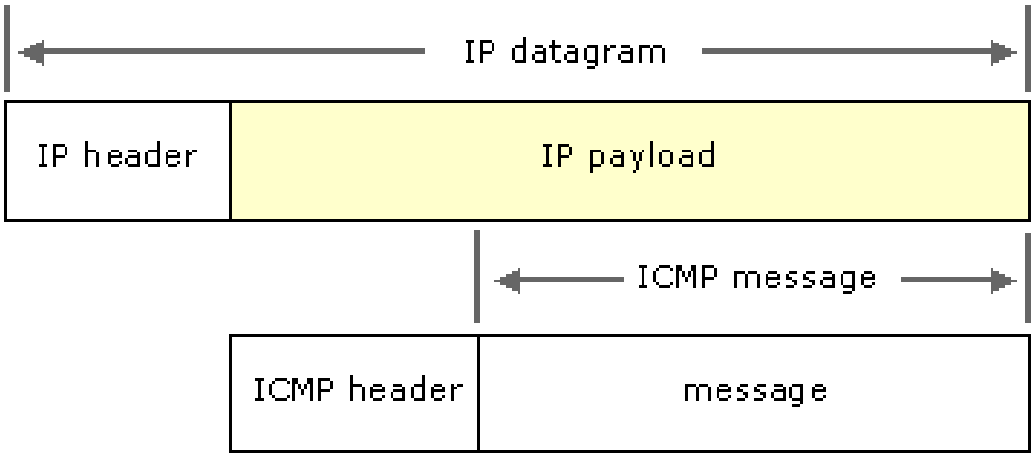
ICMP-повідомлення зазвичай автоматично відправляються в наступних випадках:

- IP-датаграмма не може потрапити до вузла призначення;

- IP-маршрутизатор (шлюз) не може перенаправляти датаграми з поточною швидкістю передачі;

- IP-маршрутизатор перенаправляє вузол-відправник на іншій, вигідніший маршрут до вузла призначення.

Інкапсуляція і передача ICMP-повідомлень в IP-датаграмах



Типи ICMP-сообщений розрізняються по заголовку *ICMP*. Оскільки *ICMP*-сообщения переносяться *IP*-датаграмами, їх доставка не гарантується.

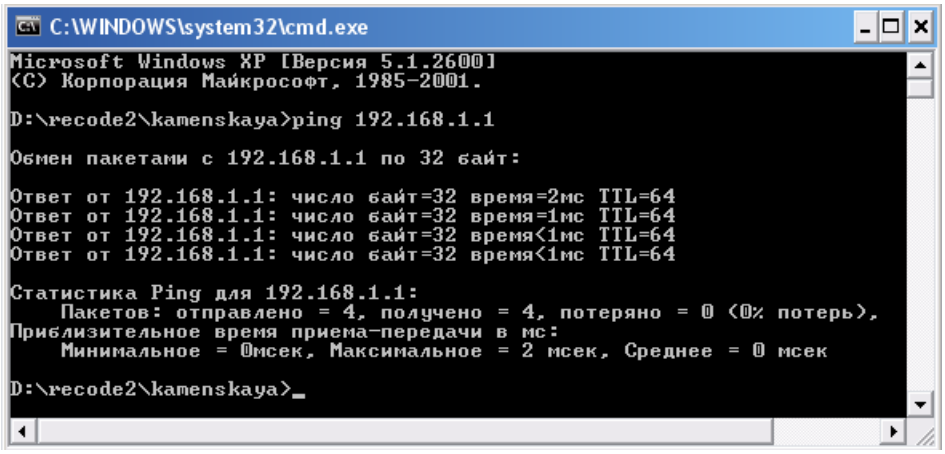
Формат ICMP-пакету

Біт	**0-7**	**8-15**	**16-31**
0	Тип	Код	Контрольна сума
32	Зміст повідомлення (залежить від значень полий «Код» і «Тип»)		

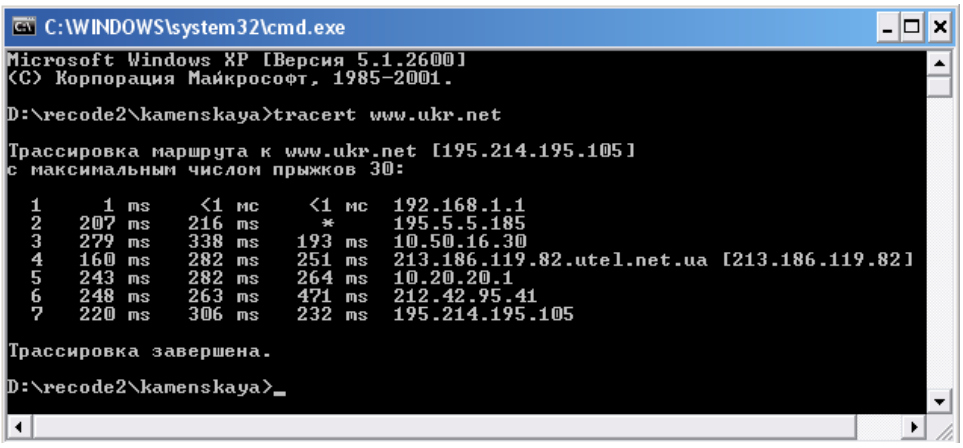
ICMP - повідомлення, що часто зустрічаються

ICMP-повідомлення	Тип	Опис
Exo - запит (Echo request)	8	Визначає, чи доступний в мережі IP-узел (комп'ютер або маршрутизатор). Команда *ing*.
Exo – відповідь (Echo reply)	0	Відповідає на відлуння-запит ICMP. оманда *ping*.
Адресат недоступний (Destination nreachable)	3	Інформує вузол про те, що датаграма не оже бути доставлена.
Уповільнення жерела (Source quench)	4	Вимагає від вузла понизити швидкість дправки датаграм, оскільки в мережі виник тор.
Перенаправлення Redirect)	5	Інформує вузол про наявність кращого аршруту.
Закінчення часу (Time exceeded)	11	Повідомляє, що час життя *IP*-датаграми *TTL*) закінчився (команда *traceroute* (в *Windows - tracert*)).

Команда ping



Команда tracert



Протокол управління групами Інтернету IGMP.

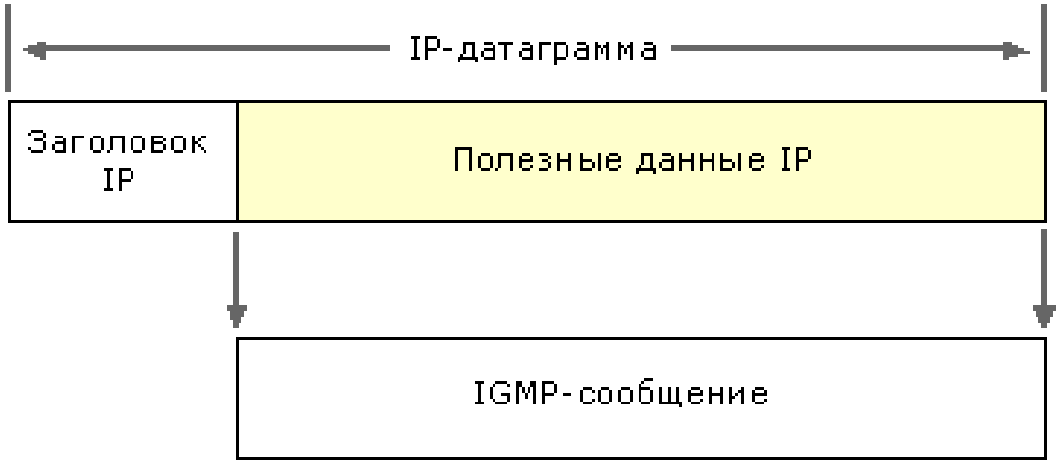
IGMP (англ. *Internet Group Management Protocol* - протокол управління групами Інтернету) мережевий протокол, використовується для обміну інформацією про членство в групах між IP-маршрутизаторами, що підтримують багатоадресну розсилку, і членами груп багатоадресної розсилки. Про членство вузлів в групах багатоадресної розсилки повідомляють самі вузли, а стан членства періодично перевіряється маршрутизаторами, що підтримують багатоадресну розсилку.

IGMP версії 3 визначений в RFC 3376. Попередні версії IGMP визначені в RFC 2236 (версія 2) і RFC 1112 (версія 1).

Версія 2 дозволяє маршрутизатору швидше виявити, що членів якої-небудь IP-группы більше немає.

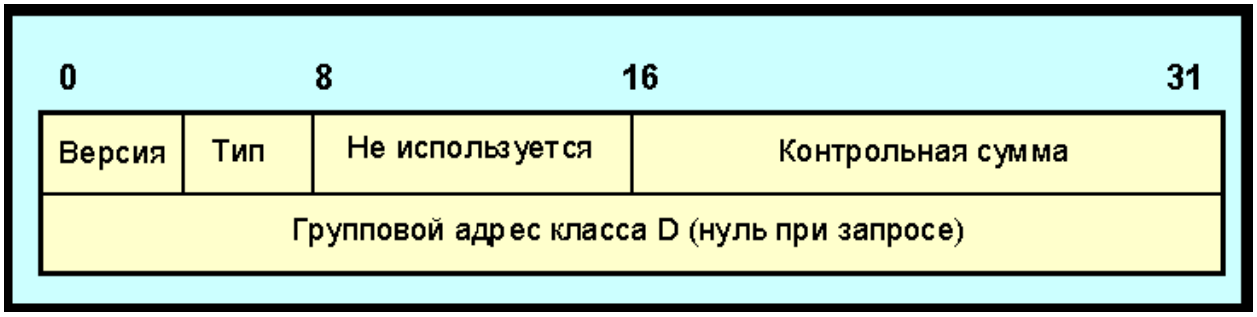
У версії 3 була додана підтримка фільтрації адрес. За допомогою цього механізму вузол може повідомити, з яких адрес він хоче отримувати пакети, а з яких немає.

Інкапсуляція і передача IGMP-повідомлень в IP-датаграмах



Оскільки *IGMP*-сообщения переносяться *IP*-датаграмами, їх доставка не гарантується.

Формат IGMP-пакету



IGMP - повідомлення

IGMP-повідомлення	Тип	Опис
Host Membership Query	1	запит включення в групу
Host Membership Report	2	повідомлення про приналежність до групи

Протокол датаграм UDP, що призначені для користувача.

UDP (англ. *User Datagram Protocol* - протокол призначених для користувача датаграм) - це транспортний протокол для передачі даних в мережах IP без встановлення з'єднання. Він є одним з найпростіших протоколів транспортного рівня моделі OSI.

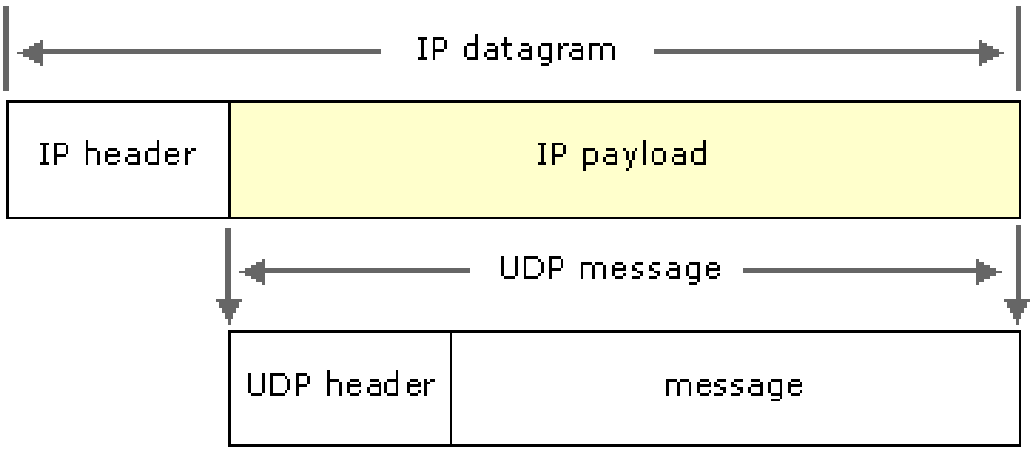
На відміну від TCP, UDP не гарантує доставку пакету. Це дозволяє йому набагато швидше і ефективніше доставляти дані для додатків, яким потрібна велика пропускна спроможність ліній зв'язку, або потрібний малий час доставки даних.

Недостатня надійність протоколу може виражатися як у втраті окремих пакетів, так і в їх дублюванні. UDP використовується при передачі потокового відео, ігор реального часу, а також деяких інших типів даних.

Ненадійність протоколу UDP треба розуміти в тому сенсі, що у випадках впливу зовнішніх чинників, що приводять до збоїв, протокол UDP не передбачає стандартного механізму повторення передачі втрачених пакетів. У цьому сенсі він настільки ж надійний, як і протокол ICMP.

Якщо додатку потрібна велика надійність, то використовується протокол *TCP* або реалізується який-небудь свій нестандартний алгоритм повторення передач залежно від умов.

Інкапсуляція і передача UDP-повідомлень в IP-датаграмах



Склад UDP-датаграми

Біт	0-15	16-31
0	Порт відправника (Source port)	Порт одержувача (Destination ort)
32	Довжина датаграми (Length)	Контрольна сума (Checksum)
64	Дані (Data)	

Порт відправника - номер порту-відправника.

Порт одержувача - номер порту-одержувача.

Розмір – розмір дейтаграми в октетах з урахуванням заголовка і даних.

Контрольна сума - 16-бітове значення контрольної суми датаграми.

Дані - поле даних *UDP*.

Серверні порти UDP, що часто використовуються

Номер порту UDP	Опис
53	запити імен DNS
69	протокол TFTP
137	служба імен NETBIOS
138	служба датаграм NETBIOS
161	протокол SNMP
520	протокол RIP

Протокол управління передачею TCP.

Transmission Control Protocol (TCP) (протокол управління передачею) - один з основних мережевих протоколів Інтернет, призначений для управління передачею даних в мережах і підмережах *TCP/IP*. Виконує функції протоколу транспортного рівня моделі OSI.

TCP - це транспортний механізм, що надає потік даних, з попередньою установкою з'єднання, за рахунок цього що дає упевненість в достовірності отримуваних даних, здійснює повторний запит даних у разі втрати даних і усуває дублювання при отриманні двох копій одного пакету. На відміну від *UDP*, гарантує, що додаток отримає дані точно в такій же послідовності, в якій вони були відправлені, і без втрат.

Механізм дії протоколу

На відміну від традиційної альтернативи - UDP, який може відразу ж почати передачу пакетів, TCP встановлює з'єднання, які повинні бути створені перед передачею даних. TCP з'єднання можна розділити на 3 стадії:

* Установка з'єднання
* Передача даних
* Завершення з'єднання

Формат TCP-сегменту

Біт	**0-3**	**4-9**	**10-15**	**16-31**
0	Порт відправника (Source port)			Порт держувача Destination port)
32	Номер кадру (Sequence Number)			

64	Номер підтвердження (Acknowledgment Number)			
96	Зсув даних (Data offset)	Резерв (Reserved)	Прапори (Flags)	Вікно (Window)
128	Контрольна сума (Checksum)			Покажчик ажливості (Urgent ointer)
160	Опції (необов'язкове) (Options)			
160/192+	Дані (Data)			

Порт відправника - номер порту-відправника.

Порт одержувача - номер порту-одержувача.

Номер кадру - номер кадру першого октету даних в цьому сегменті (за винятком пакету, де присутній прапор SYN). Якщо в пакеті присутній прапор SYN, то номер даного пакету стає номером почала послідовності (ISN) і номером першого октету даних стає номер Isn+1.

Номер підтвердження - поле номера кадру підтвердженого отримання. Якщо пакет містить встановлений контрольний біт ACK, то це поле містить номер наступного пакету даних відправника, який чекає одержувач. При встановленому з'єднанні пакет підтвердження відправляється завжди.

Зсув даних - 4-бітове поле, що вказує число 32-бітових слів в заголовку TCP. Після заголовка розміщуються дані, тому поле указує на початок даних в пакеті. Заголовок пакетів *TCP* завжди має розмір, кратний 32 бітам.

Резерв - зарезервоване поле розміром 6 бітів.

Біти управління - 6 бітове поле, що містить прапори управління:

U (URG) - значуще поле покажчика важливості;

A (ACK) - значуще поле підтвердження;

P (PSH) - функція push;

R (RST) - скидання з'єднання;

S (SYN) - синхронізація порядкових номерів;

F (FIN) - немає даних від відправника.

Вікно - 16-бітове поле, що містить число октетів даних, які відправник даного сегменту сприйматиме, починаючи з октету, вказаного в полі підтвердження.

Контрольна сума - 16-бітове значення контрольної суми, що обчислюється для 16-бітових слів заголовка і тексту. Якщо сегмент містить непарне число октетів в заголовку або тексті, останні октети доповнюються справа 8 нулями для вирівнювання по 16-бітовій межі. Біти заповнення (0) не передаються в сегменті і служать тільки для розрахунку контрольної суми. При розрахунку контрольної суми значення самого поля контрольної суми приймається рівним 0.

Покажчик важливості - 16-бітове значення позитивного зсуву від порядкового номера в даному сегменті. Це поле указує порядковий номер октету, з якого починаються важливі (urgent) дані. Поле береться до уваги тільки для пакетів зі встановленим прапором U.

Опції - передаються в кінці заголовка TCP і завжди мають розмір, кратний 8 бітам. При розрахунку контрольної суми пакету значення опцій беруться до уваги. Опції можуть починатися на будь-якій межі октету.

Дані - поле даних *TCP* або протоколів вищих рівнів.

Серверні порти TCP, що часто використовуються

Номер порту TCP	Опис
20	сервер FTP (канал даних)
21	сервер FTP (канал, що управляє)
23	сервер Telnet
53	передача зон DNS
80	веб-сервер-сервер (HTTP)
139	служба сеансу NETBIOS

5.3 Прикладний рівень стеку протоколів TCP/IP.

Протокол динамічної конфігурації вузла DHCP.

IP-адреса є основним типом адрес, на підставі яких мережевий рівень протоколу IP передає пакети між мережами. IP-адрес призначається адміністратором під час конфігурації комп'ютерів і маршрутизаторів (*статична адресація*) або автоматично при підключенні пристрою до мережі (*динамічна адресація*), який використовується протягом обмеженого проміжку часу до завершення сеансу підключення.

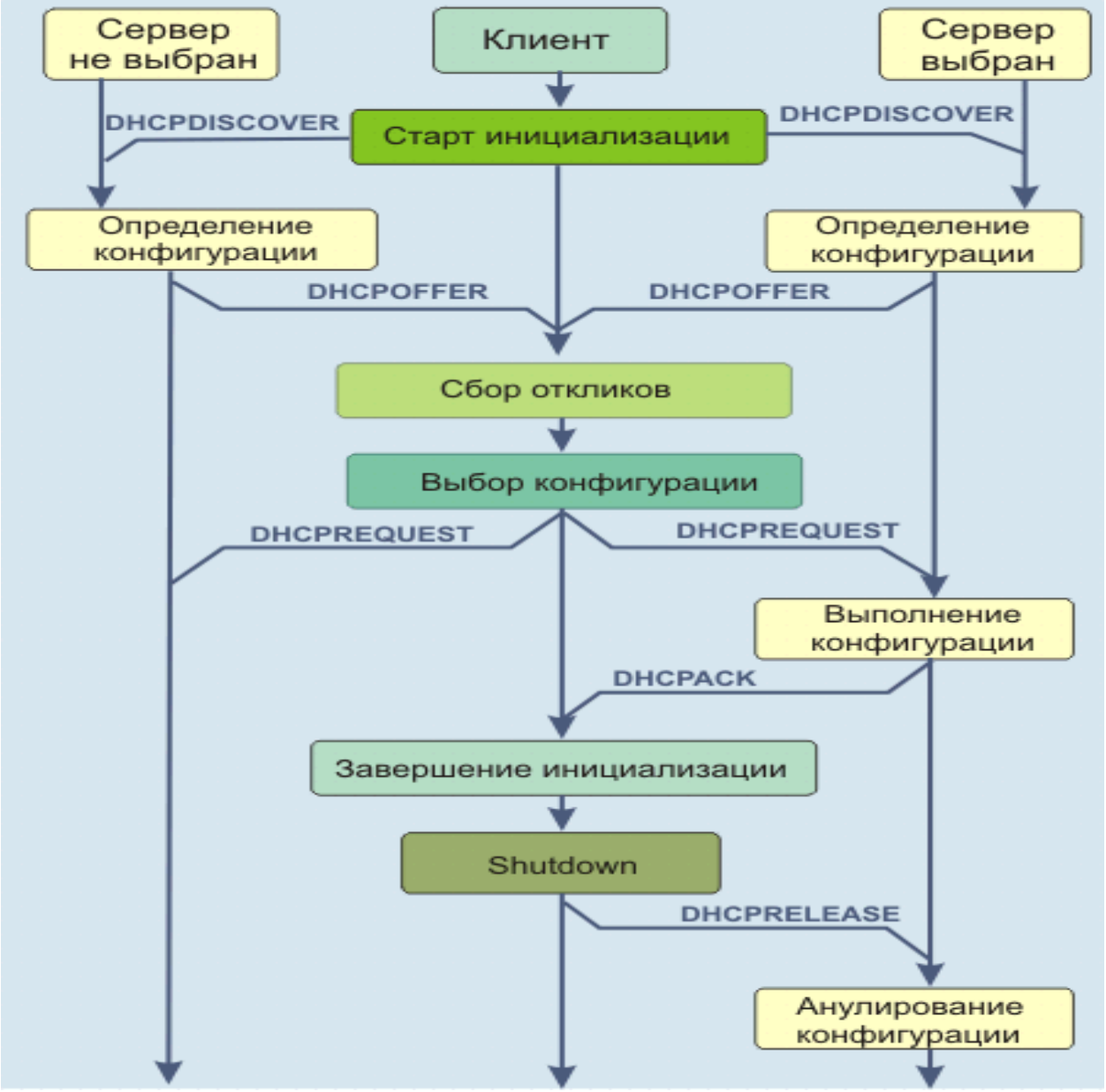
DHCP (англ. *Dynamic Host Configuration Protocol* - протокол динамічної конфігурації вузла) - це мережевий протокол, що дозволяє комп'ютерам автоматично отримувати IP-адрес і інші параметри, необхідні для роботи в мережі *TCP/IP*. Модель роботи «клієнт-сервер». Комп'ютер-клієнт на етапі

конфігурації мережевого пристрою звертається до сервера *DHCP*, і отримує від нього потрібні параметри. Адміністратор може задати діапазон адрес, що розподіляються сервером серед комп'ютерів. Це дозволяє уникнути ручної настройки комп'ютерів і зменшує кількість помилок. Протокол *DHCP* використовується в більшості крупних (і не дуже) мереж *TCP/IP*.

DHCP є розширенням протоколу *BOOTP*, що використався раніше для забезпечення бездискових робочих станцій *IP*-адресами при їх завантаженні. *DHCP* зберігає зворотну сумісність з *BOOTP*.

Стандарт протоколу *DHCP* був прийнятий в жовтні 1993 року. Версія протоколу (березень 1997 року), що діє, описана в *RFC 2131*. Нова версія *DHCP*, призначена для використання в середовищі *IPv6*, носить назву *DHCPv6* і визначена в *RFC 3315* (липень 2003 року).

Тимчасова діаграма обміну повідомленнями між DHCP-клієнтом і сервером



1. Клієнт широкомовно пересилає повідомлення DHCPDISCOVER по локальній фізичній субмережі. Повідомлення DHCPDISCOVER може включати опції, які пропонують значення для мережевої адреси і тривалості його використання. Агент транспортування BOOTP може передати повідомлення DHCP-серверам, які розміщені за межами даної фізичної субмережі.

2. Кожен сервер може відгукнутися повідомленням DHCPOFFER, яке містить мережеву адресу (і інші конфігураційні параметри в опціях DHCP). Сервери не повинні резервувати пропоновану мережеву адресу, хоча протокол працюватиме ефективніше, якщо сервер уникає привласнення пропонованої

мережевої адреси іншому клієнтові. При виділенні нової адреси, сервери повинні перевіряти, щоб пропонована мережева адреса не використовувалася десь ще. Сервер відправляє клієнтові повідомлення DHCPOFFER, використовуючи, якщо необхідно транспортні засоби BOOTP.

3. Клієнт отримує одне або більш за повідомлення DHCPOFFER від одного або більш за сервери. Клієнт може вважати за краще дочекатися декількох відгуків. Клієнт вибирає один сервер, якому пошле запит конфігураційних параметрів, згідно пропозиції, що міститься в повідомленні DHCPOFFER. Клієнт широкомовно відправляє повідомлення DHCPREQUEST, щоб вказати, який сервер їм вибраний.

4. Сервери отримують широкомовне повідомлення DHCPREQUEST від клієнта. Сервери, не вибрані повідомленням DHCPREQUEST, використовують повідомлення як повідомлення про те, що клієнт відкинув пропозицію сервера. Сервер, вибраний повідомленням DHCPREQUEST, здійснює запис конфігураційного набору клієнта в постійну пам'ять і реагує повідомленням DHCPACK, що містить конфігураційні параметри для клієнта, що прислав запит.

5. Клієнт отримує повідомлення DHCPACK, що містить конфігураційні параметри. Клієнт повинен виконати остаточну перевірку параметрів (наприклад, запустити ARP для виділеної мережевої адреси), і фіксувати тривалість надання конфігураційних параметрів, прописану в повідомленні DHCPACK. Клієнт остаточно конфігурований. Якщо клієнт виявляє, що адреса вже використовується (наприклад, за допомогою ARP), він повинен послати серверу повідомлення DHCPDECLINE і повторно запустити процес конфігурації. Клієнт повинен почекати як мінімум 10 секунд, перш ніж наново починати конфігураційну процедуру, щоб уникнути виникнення зайвого мережевого трафіку. Якщо клієнт отримує повідомлення DHCPNAK message, клієнт перезапускає конфігураційний процес.

6. Клієнт може вирішити відмовитися від оренди мережевої адреси шляхом посилки серверу повідомлення DHCPRELEASE. Клієнт ідентифікує набір

параметрів, від якого він відмовляється, за допомогою свого ідентифікатора і мережевої адреси в повідомленні DHCPRELEASE.

Опції DHCP

Крім IP-адреса, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP. Список стандартних опцій можна знайти в RFC 2132.

Деякими з найчастіше використовуваних опцій є:

- IP-адрес маршрутизатора за умовчанням;
- маска підмережі;
- адреси серверів DNS;
- ім'я домена DNS.

Протокол DHCP є клієнт-серверним, тобто в його роботі беруть участь клієнт DHCP і сервер DHCP. Передача даних проводиться за допомогою протоколу UDP, при цьому сервер приймає повідомлення від клієнтів на порт 67 і відправляє повідомлення клієнтів на порт 68.

Система доменних імен DNS.

DNS (англ. *Domain Name System* - система доменних імен) - розподілена система (розподілена база даних), здатна за запитом, що містить доменне ім'я хосту (комп'ютера або іншого мережевого пристрою), повідомити IP адресу або (залежно від запиту) іншу інформацію.

DNS була розроблена в 1983 році; оригінальний опис механізмів роботи описаний в RFC 882 і RFC 883. У 1987 публікація RFC 1034 і RFC 1035 змінили специфікацію DNS і відмінили RFC 882 і RFC 883 як застарілі. Деякі нові RFC доповнили і розширили можливості базових протоколів.

Характеристики DNS

* *Розподіленність зберігання інформації*. Кожен вузол мережі в обов'язковому порядку повинен зберігати тільки ті дані, які входять в його зону відповідальності і (можливо) адреси кореневих DNS-серверов.

* *Кеширование інформації*. Вузол може зберігати деяку кількість даних не зі своєї зони відповідальності для зменшення навантаження на мережу.

* *Ієрархічна структура*, в якій всі вузли об'єднані в дерево, і кожен вузол може або самостійно визначати роботу нижчестоячих вузлів, або делегувати (передавати) їх іншим вузлам.

* *Резервування*. За зберігання і обслуговування своїх вузлів (зон) відповідають (зазвичай) декілька серверів, розділені як фізично, так і логічно, що забезпечує збереження даних і продовження роботи навіть у разі збою одного з вузлів.

Повністю визначене доменне ім'я FQDN (Fully Qualified Domain Name)

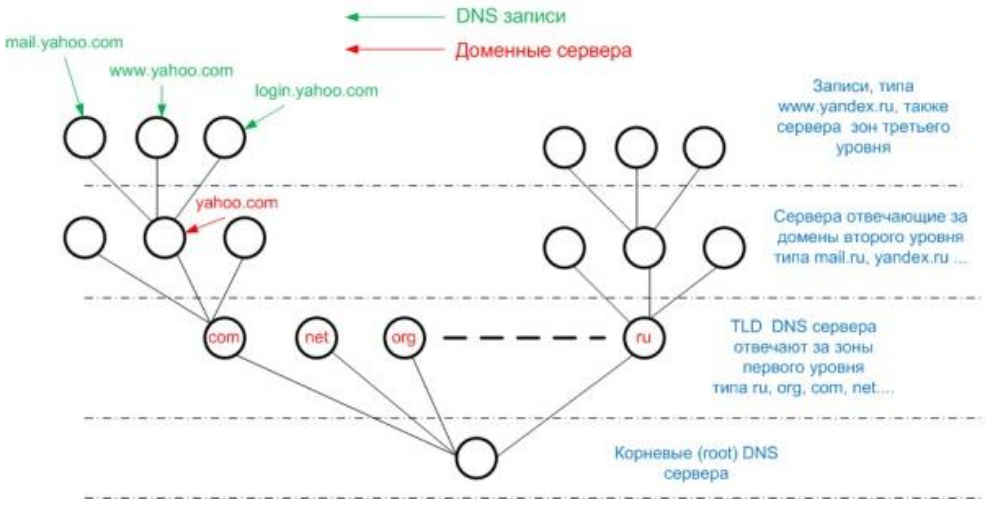
Ім'я омп'ютера	**Ім'я домену**		
	3 рівень	2 рівень	1 рівень
ukr			.net
www		.asplinux	.ru
www	.dynamo	.kiev	.ua

Класифікація основних доменів

Домен	**Опис**
com	комерційні організації
edu	учбові організації

gov	урядові організації США
int	міжнародні організації
mil	військові організації США
net	мережі
org	інші організації
arpa	використовується для перетворення ip-адреси в ім'я

Структура DNS



Зона - логічний вузол в дереві імен.

Домен - назва зони в системі доменних імен (DNS) Інтернету, виділеній якій-небудь країні, організації або для інших цілей.

Піддомен (англ. *subdomain*) - ім'я підлеглої зони.

DNS-сервер - спеціалізоване ПО для обслуговування DNS. DNS-сервер може бути відповідальним за деякі зони і/або може перенаправляти запити вищестоящим серверам.

DNS-клиент - спеціалізована бібліотека (або програма) для роботи з DNS. У ряді випадків DNS-сервер виступає в ролі DNS-клиента.

Відповідальність (англ. authoritative) - ознака розміщення зони на DNS-сервері. Відповіді DNS-сервера можуть бути двох типів: *відповідальні або авторитетні* (коли сервер заявляє, що сам відповідає за зону) і *невідповідальні або не авторітетні* (англ. Non-authoritative), коли сервер обробляє запит, і повертає відповідь інших серверів. В деяких випадках замість передачі запиту далі DNS-сервер може повернути вже відоме йому (по запитах раніше) значення (из кешу в режимі кеширования).

DNS-запит (англ. *DNS query*) - запит від клієнта (або сервера) серверу. Запит може бути *рекурсивним* або *нерекурсивним*. Нерекурсивний запит або повертає дані про зону, яка знаходиться в зоні відповідальності DNS-сервера (який отримав запит) або повертає адреси кореневих серверів (точніше, адреса будь-якого сервера, який володіє великим об'ємом інформації про запитану зону, чим сервер, що відповідає). У разі рекурсивного запиту сервер опитує сервери (в порядку убування рівня зон в імені), поки не знайде відповідь або не виявить, що домен не існує.

Система DNS містить ієрархію серверів DNS. Кожен домен або піддомен підтримується як мінімум одним авторитетним сервером DNS (від англ. authoritative - авторитетний, заслуговуючий довіри), на якому розташована інформація про домен. Ієрархія серверів DNS співпадає з ієрархією доменів.

Ім'я і IP-адреса не тотожні - одна IP-адреса може мати безліч імен, що дозволяє підтримувати на одному комп'ютері безліч веб-сайтів (це називається віртуальний хостинг). Зворотне теж справедливо - одному імені може бути зіставлене безліч IP-адресов: це дозволяє створювати балансування навантаження.

Для підвищення стійкості системи використовується безліч серверів, що містять ідентичну інформацію, а в протоколі є засоби, що дозволяють підтримувати синхронність інформації, розташованої на різних серверах. Існує 13 кореневих серверів, їх адреси практично не змінюються.

Протокол DNS використовує для роботи TCP- або UDP-порт 53 для відповідей на запити. Традиційно запити і відповіді відправляються у вигляді однієї UDP датаграми.

Приклад роботи системи DNS

Припустимо, ми набрали адресу ru.wikipedia.org. Браузер питає у сервера DNS: «яка IP-адрес у ru.wikipedia.org»? Проте, сервер DNS може нічого не знати не тільки про запитане ім'я, але навіть про весь домен wikipedia.org. В цьому випадку має місце рекурсія: сервер звертається до кореневого сервера - наприклад, 198.41.0.4. Цей сервер повідомляє - «У мене немає інформації про дану адресу, але я знаю, що 204.74.112.1 є авторитетним для зони org.» Тоді сервер DNS направляє свій запит до 204.74.112.1, але той відповідає «У мене немає інформації про даний сервер, але я знаю, що 207.142.131.234 є авторитетним для зони wikipedia.org.» Нарешті, той же запит відправляється до третього DNS-серверу і отримує відповідь - IP-адрес, яка і передається клієнтові - браузеру.

В даному випадку в процесі пошуку IP по імені:

* браузер відправив відомому йому DNS-серверу т.з. *рекурсивний запит* - у відповідь на такий тип запиту сервер зобов'язаний повернути «готовий результат», тобто IP-адрес, або повідомити про помилку;

* DNS-сервер, отримавши запит від клієнта, послідовно відправляв *ітеративні (нерекурсивні) запити*, на які отримував від інших DNS-серверів відповіді, поки не отримав авторитетну відповідь від сервера, відповідального за запитану зону.

Запит на визначення імені зазвичай не йде далі кеша DNS, який зберігає відповіді на запити, що проходили через нього раніше. Разом з відповіддю приходить інформація про те, скільки часу дозволяється зберігати цей запис в кеш.

Зворотний DNS-запрос

DNS використовується в першу чергу для перетворення символьних імен в IP-адреса, але він також може виконувати зворотний процес. Для цього використовуються вже наявні засоби DNS. Річ у тому, що із записом DNS можуть бути зіставлені різні дані, у тому числі і яке-небудь символьне ім'я. Існує спеціальний домен in-addr.arpa, записи в якому використовуються для перетворення IP-адресов в символьні імена. Наприклад, для отримання DNS-имени для адреси 11.22.33.44 можна запитати у DNS-сервера запис 44.33.22.11.in-addr.arpa, і той поверне відповідне символьне ім'я. Зворотний порядок запису частин IP-адреса пояснюється тим, що в IP-адресах старші біти розташовані на початку, а в символьних DNS-іменах старші (що знаходяться ближче до кореня) частини розташовані в кінці.

Зарезервовані доменні імена

Документ *RFC 2606* (*Reserved Top Level DNS Names* - Зарезервовані імена доменів верхнього рівня) визначає назви доменів, які слід використовувати як прикладів (наприклад, в документації), а також для тестування. Окрім *example.com*, *example.org* і *example.net*, до цієї групи також входять *test*, *invalid* і ін.

Формат DNS-повідомлення

DNS має два типи повідомлення: запит і відгук. Обидва типи мають один і той же формат.

Обидва повідомлення, запит і відгук, мають один і той же формат заголовка з декількома полями зі встановленими нулями для повідомлень відгуку. Заголовок має довжину - 12 байт.

Ідентифікація - застосовується клієнтом для того, щоб порівняти відгук із запитом. Клієнт використовує різний номер ідентифікації кожного разу, коли він посилає запит. Сервер дублює цей номер у відповідному відгуку.

Прапори

0	1-4	5	6	7	8	9-11	12-15
QR	OpCode	AA	TC	RD	RA	Reserved	rCode

QR (*query/response*) - запит/відповідь. Це однобітовоє субполе, яке визначає тип повідомлення. Якщо воно рівне 0, повідомлення є запитом. Якщо воно рівне 1, то повідомлення - відповідь.

OpCode (код операції). Це 4-бітове субполе, яке визначає тип запиту або відповіді (0 - тип стандартний, 1 - тип інверсний і 2 - сервер запрошує стан).

AA (*authoritative answer* - авторитетна відповідь). Це однобітовоє поле. Коли воно встановлене (значення 1), це означає, що ім'я сервера є повноважною північчю. Використовується тільки в у відповідь повідомленні.

TC (*truncated* - усічене). Це однобітовоє поле. Коли воно встановлене (значення 1), це означає, що відповідь була більш ніж 512 байт і усічена до 512. Застосовується, коли DNS користується послугою UDP.

RD (*recursiondesired* - бажана рекурсія). Це однобітовоє субполе. Коли воно встановлене (значення 1), це означає, що клієнтові бажана рекурсивна відповідь. Він встановлюється в повідомленні запиту і повторюється в у відповідь повідомленні.

RA (*recursion available* - рекурсія можлива). Однобітове субполе. Коли воно встановлене відповідає, це означає, що можлива рекурсивна відповідь. Встановлюється тільки в у відповідь повідомленні.

Reserved (резервні). Це трьохбітове субполе зі встановленими нулями.

rCode (r-код). Це 4-бітове поле, яке показує стан помилки відповідає. Тільки відповідальний сервер може зробити таку оцінку.

Значення	Коментар
0	Немає помилки
1	Помилка формату
2	Проблема імені сервера
3	Проблема посилання на домен
4	Тип запиту не підтримується
5	Адміністративна заборона
6-15	Резервні

Лічильник питань. Це 16-бітове поле, що містить кількість запитів.

Лічильник відповідей. Це 16-бітове поле, що містить кількість відповідей.

Кількість записів повноважень. Це 16-бітове поле, що містить кількість записів повноважень.

Кількість записів додаткової інформації. Це 16-бітове поле, що містить кількість записів додаткової інформації.

Секція запиту. Це секція, що містить одну або більш за записи. Вона міститься і в запиті, і в відповіді.

Секція відповіді. Це секція, що містить одну або більш за записи. Вона представляє тільки повідомлення відповіді. Секція включає відповідь від сервера до клієнта (повідомлення распознавателя).

Секція повноважень. Це секція, що містить одне або більше повідомлень джерела. Вона представлена тільки у повідомленні-відповіді. Секція дає інформацію (ім'я домена) про один або більш повноважних серверів для запиту.

Секція додаткової інформації. Це секція, що містить одну або більше записів джерел. Вона представлена тільки у повідомленні-відповіді. Секція забезпечує додатковою інформацією, яка може допомогти роспізнавателю.

Запис запиту DNS

	⇐ змінна величина ⇒	
	Ім'я запиту	
	Тип запиту	Клас запиту
Біт	0-15	16-31

Клас запиту. Це 16-бітове поле, яке визначає спеціальний протокол, що використовується DNS.

Клас	**Мнемоніка**	**Опис**
1	IN	Інтернет
2	Зарезервовано	-
3	Зарезервовано	-
4	Зарезервовано	-

Тип запиту. Це 16-бітове поле, що визначає тип запиту.

Тип	Код	Ім'я	Запит	Відгук	Опис
1	A	Address	+	+	32-бітова IPv4-адреса
2	NS	Name server	+	+	повноважний сервер зони
5	CNAME	Canonical name	+	+	Канонічне ім'я. Визначає псевдонім для офіц. імені хосту.
6	SOA	Start of authority	+	+	Старт повноваженням. Початок зони. Перший запис у файлі зони.
11	WKS	Well-know services	+	+	Добре відомий сервіс. Мережевий сервіс, що забезпечується хостом.
12	PTR	Pointer	+	+	Покажчик. Використовується для перетворення адреси в доменне ім'я.
13	HINFO	Host information	+	+	Інформація хоста. Апаратура і ОС, що використовується хостом.

15	MX	Mail exchange	+	+	Обмін повідомленнями. Направляє інформацію до поштового серверу.
28	AAA	IPv6 address	+	+	адреса IPv6
252	AXFR		+	-	запит на передачу по усій зоні
255	ANY		+	-	запит на усі записи

Запис ресурсу DNS.

Кожне доменне ім'я (кожен вузол дерева) пов'язаний із записом ресурсу. Сервер бази даних містить записи ресурсу. Записи ресурсу - це також те, що повертається сервером клієнтові.

	⇐ змінна величина ⇒	
	Доменне ім‘я	
	Тип домену	Клас домену
	Час життя	
Біт	0-15	16-31
	Довжина ресурсу даних	
	Данні ресурсу (номер або ім'я домену,)	
	⇐ змінна величина ⇒	

Ім'я домену. Це поле змінної довжини, що містить ім'я домену. Воно дублює ім'я домена в записі запиту. DNS використовує стиснення скрізь де повторюється ім‘я.

Тип домену. Це поле таке ж, як поле типу запиту в секції запиту, виключаючи два останні типи, які не дозволені.

Клас домену. Це поле таке ж, як поле класу запиту в секції запиту.

Час життя. Це 32-бітове поле, що визначає число секунд, при якому відповідь дійсна. Приймач може кешувати відповідь на цей період часу. Значення нуль означає, що запис ресурсів використовується тільки на один перехід і не може бути кешована.

Довжина ресурсу даних. 16-бітове поле визначає довжину ресурсу даних.

Дані ресурсу. Це поле змінної довжини, що містить відповідь на запит (у секції відповідь), або ім'я домену повноважного сервера (у секції повноважень), або додаткову інформацію (у додатковій секції).

Номер. IPv4-адрес - це ціле число з 4-х октетів, IPv6-адрес - з 16-ти октетів.

Ім'я домену. Імена домена виражаються як послідовність міток. Кожна мітка позначається полем однобайтової довжини, яке визначає число символів в мітці. Кожне ім'я домену закінчується нульовою міткою, останній байт кожного імені домену - поле довжини із значенням 0. Для того, щоб відрізнити поле довжини і точку відгалуження, два старші розряди довжини поля повинні бути завжди нульовими (00). Це не створюватиме проблем, тому що довжина мітки не може бути більше 63 - максимального значення з 6-ти (111111).

Точка відгалуження. Ім'я домену може бути замінене точкою відгалуження. Точка відгалуження - двобайтове поле з двома старшими бітами, встановленими в положення 1 (11).

Рядок символів. Поле довжини (1 байт) + символи. Може мати довжину до 256 символів (з полем довжини).

Стиснення

Коли ім'я домену повторюється, DNS вимагає, щоб воно замінювалося покажчиком зсуву. Наприклад, запис ресурсу імені домена зазвичай повторює ім'я домена в запиті. Для того, щоб уникнути дублювання, DNS визначає двобайтовий покажчик зсуву, який указує на попереднє входження імені домену.

Перші два старші розряди - це дві одиниці, необхідні для того, щоб відрізнити точку-покажчик зрушення від інформації "довжина поля".) Інші 14 біт представляють число, яке указує на відповідний байт номера повідомлення. Цей байт відлічується від початкового повідомлення з першим байтом, який вважається нульовим.

СПИСОК ЛІТЕРАТУРИ

1. Наталия Олифер, Виктор Олифер Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 5-е изд. 992 стр.

2. Дуглас Е. Камер Сети TCP/IP, том 1. Принципы, протоколы и структура, 4-е издани: учебное пособие. – здательский дом Вильямс, 2015 .– 800 стр.

3. Джеймс Куроуз, Кит Росс. Компьютерные сети. Нисходящий подход. 6-ое издание. -М.: Изд-во «Є», 2016. – 912 с.

4. Фролов, А.В.; Фролов, Г.В. Локальные сети персональных компьютеров. Использование протоколов IPX, SPX, NETBIOS; Диалог-Мифи - Москва, 2013. - 160 с.

5. Мезенцев, К.Н. Автоматизированные информационные системы: учебник для студентов образоват. учреждений сред. проф. образования /К. Н. Мезенцев. - 5-е изд., стер.-М.: Академия, 2014.-176 с.

6. Олифер, В.Г.; Олифер, Н.А. Компьютерные сети принципы, технологии, протоколы; СПб: Питер - Москва, 2011. - 672 с.

7. Андерсон Криста, Минаси Марк Локальные сети; Корона-Принт, Энтроп, Век + - Москва, 2013. - 624 с.