Міністерство освіти й науки України
Запорізький національний університет

КОМП’ЮТЕРНІ МЕРЕЖІ

Навчальний посібник
для здобувачів ступеня вищої освіти бакалавра
спеціальності «Комп’ютерні науки» освітньо-професійної
програми «Комп’ютерні науки»

Затверджено
вченою радою ЗНУ
Протокол № 7
від 29.12.2025

Запоріжжя
2025

УДК 004.7:004.056
Р741

Решевська К. С. Комп’ютерні мережі : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності «Комп’ютерні науки» освітньо-професійної програми «Комп’ютерні науки». Запоріжжя : Запорізький національний університет, 2025. 95 с.

У навчальному посібнику представлено теоретичні матеріали, в яких розглянуто архітектуру та технології сучасних комп’ютерних мереж. Також в ньому розглянуто питання базових концепцій:

– комп’ютерних мереж;

– технологій дротових та бездротових локальних і глобальних мереж.

Посібник складається з теоретичного матеріалу, контрольних запитань, практичних завдань та системи тестів для перевірки знань, отриманих при вивченні змісту викладеного курсу.

Навчальний посібник призначений насамперед для здобувачів вищої освіти спеціальності «Комп’ютерні науки», він може бути також корисним для технічних спеціалістів, які прагнуть отримати базові знання з принципів побудови комп’ютерних мереж, зрозуміти особливості традиційних технологій комп’ютерних мереж .

Рецензент

С. Ю. Борю, кандидат технічних наук, доцент кафедри комп’ютерних наук

Відповідальний за випуск

О. С. Пшенична, кандидат педагогічних наук, доцент, в.о. завідувача кафедри комп’ютерних наук

ВСТУП

Дисципліна «Комп’ютерні мережі» належить до циклу професійної підготовки спеціальності «Компютерні науки» оскітньо-професійної програми «Компютерні науки» та має статус обов’язкової.

Метою викладання навчальної дисципліни «Комп’ютерні мережі» є формування у студентів знань з теорії побудови мереж ЕОМ і навичок застосування технологій побудови мереж для створення, експлуатування та розробки нових сучасних програмно-апаратних систем для використання в локальних та глобальних обчислювальних мережах.

Основними завданнями вивчення дисципліни «Комп’ютерні мережі» є: вивчення основних визначень з дисципліни, рівнів моделі OSI та відповідних їм протоколів; засвоєння принципів побудови сучасних інформаційних мереж та їх моделювання за допомогою емуляторів мереж; отримання навичок роботи із апаратними засобами комп‘ютерних мереж.

Згідно з вимогами освітньої-професійної програми здобувачі освіти мають досягти таких компетентностей та програмних результатів навчання:

Компетентності:

Здатність до абстрактного мислення, аналізу та синтезу

Здатність застосовувати знання у практичних ситуаціях

Знання та розуміння предметної області та розуміння професійної діяльності

Здатність вчитися і оволодівати сучасними знаннями

Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення

Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп’ютерні системи і мережі передачі даних та аналізує якість роботи комп’ютерних мереж

Результати навчання:

Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп’ютерних систем, знати мережні технології, архітектури комп’ютерних мереж, мати практичні навички технології адміністрування комп’ютерних мереж та їх програмного забезпечення

Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних

Дисципліна «Комп'ютерні мережі» базується на знаннях та вміннях, отриманих під час вивчення дисциплін циклу професійної підготовки, а саме:

1. «Архітектура обчислювальних систем»
2. «Операційні системи»

Знання та уміння, отримані під час вивчення дисципліни «Комп'ютерні мережі», можуть бути використані при вивчені таких дисциплін:

1. «Паралельні та розподілені обчислення»
2. «Платформи корпоративних інформаційних систем»
3. «Проєктування та розробка WEB-застосунків»
4. «Технології захисту інформації»

Представлений навчальний посібник допоможе засвоїти основні принципи взаємодії комп'ютерів у мережі, ознайомить з мережними топологіями, типами ліній зв'язку, з технологіями локальних і глобальних мереж та з комунікаційними пристроями.

Навчальний посібник складається з чотирьох розділів:

1. Основи комп'ютерних мереж
2. Організація локальних комп'ютерних мереж
3. Технології передавання даних у глобальних мережах
4. Автоматизація управління комп'ютерними мережами

Кожний розділ супроводжується переліком контрольних запитань і завдань для перевірки знань і навичок з курсу.

Структура та зміст навчального посібника відповідають силабусу дисципліни «Комп'ютерні мережі».

РОЗДІЛ 1 ОСНОВИ КОМП'ЮТЕРНИХ МЕРЕЖ

Тема 1 Основні поняття та класифікація комп'ютерних мереж

Ключові поняття: комп'ютерна мережа, ресурси мережі, персональна мережа, локальна обчислювальна мережа, глобальна мережа, регіональна мережа, мережа рівня відділу, мережа кампусів, корпоративна мережа, сервер, клієнтський комп'ютер (клієнт, робоча станція), однорангові та клієнт-серверні мережі, служби, мережний адаптер, адміністратор мережі, адміністрування мережі

Якщо комп'ютери фізично незв'язаних між собою, то для сумісної роботи з даними, які знаходяться на різних комп'ютерах необхідно копіювати файли на зовнішній носій та переносити їх між комп'ютерами. Для друку документів або треба забезпечувати кожний комп'ютер окремим принтером, або, знову ж таки, переносити файли на той комп'ютер, до якого підключено принтер. Іншим недоліком відсутності зв'язку між вузлами є те, що не можливо виконувати спільну робота з одним документом. Такі ситуації при окремій роботі комп'ютерів призвели до необхідності у організації комп'ютерів у мережу.

Мережа (Network) [**Ошибка! Источник ссылки не найден.**] (рис. 1.1) − набір апаратних і програмних засобів, які дозволяють об'єднати комп'ютери між собою за певними правилами для спільного використання ресурсів.

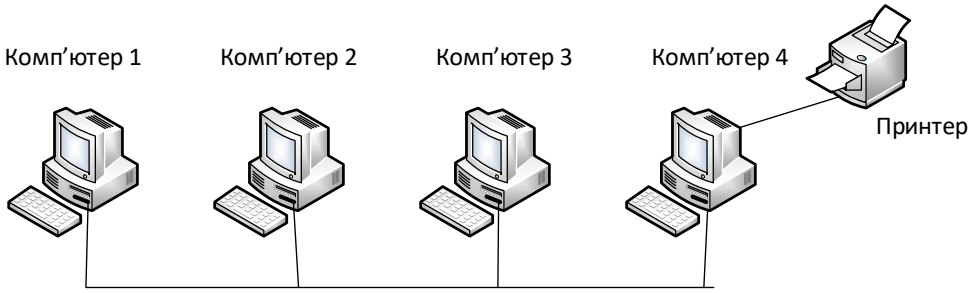


Рисунок 1.1 – Мережа: кілька комп'ютерів і загальний принтер

Ресурси мережі [**Ошибка! Источник ссылки не найден.**] – програми, файли даних, а також принтери й інші спільно використовувані периферійні пристрої в мережі.

1.1 Основна класифікація комп'ютерних мереж

Розглянемо класифікацію комп'ютерних мереж за різними ознаками.

За розміром охопленої мережею території розділяють на такі класи: персональні (PAN, Personal Area Network), локальні (LAN, Local Area Network),

регіональні (MAN, Metropolitan Area Network) й глобальні (WAN, Wide Area Network).

Персональна мережа (рис. 1.2) – це мережа, яка побудована «навколо» людини. Такі мережі об'єднують всі персональні електронні пристрої користувача (телефони, кишенькові персональні комп'ютери, смартфони, ноутбуки, гарнітури то що).

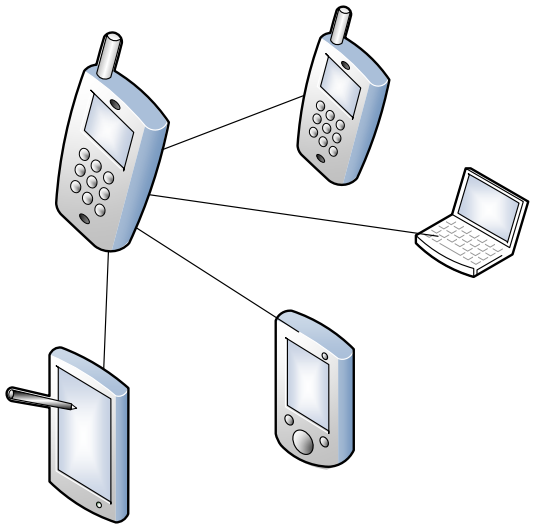


Рисунок 1.2 – Персональна мережа (PAN, Personal Area Network)

Локальна обчислювальна мережа (ЛОМ) [Ошибка! Источник ссылки не найден.] (рис.1.3) – мережі, розташовані територіально в одному місці (найчастіше в одній будівлі) і які належать зазвичай одній організації.

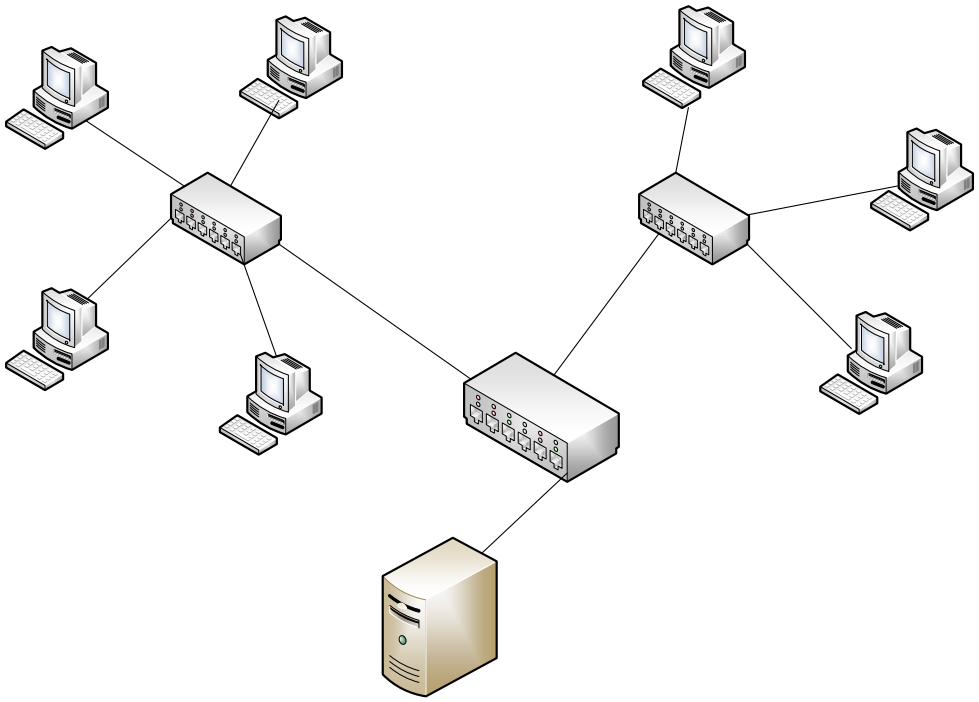


Рисунок 1.3 – Локальна мережа (LAN, Local Area Network)

✎**Регіональна мережа** [**Ошибка! Источник ссылки не найден.**] – мережа, що з'єднує комп'ютери, а частіше локальні мережі організацій в межах одного великого міста

✎**Глобальна мережа** [**Ошибка! Источник ссылки не найден.**] – мережа, що поєднує комп'ютери різних міст, країн та континентів.

Глобальні, регіональні і локальні обчислювальні мережі об'єднуються та створюють багаторівневі ієрархії, які надають потужні засоби для обробки великих масивів даних і доступ до практично необмежених інформаційних ресурсів.

Локальні обчислювальні мережі (ЛОМ) можуть входити як компоненти до складу регіональної мережі; регіональні мережі – об'єднуватися у глобальні мережі; нарешті, глобальні мережі можуть утворювати ще більш великі структури. Найбільшим об'єднанням комп'ютерних мереж у масштабах планети Земля на сьогодні є «мережа мереж» – **Інтернет**.

Цікавим прикладом зв'язку локальних і глобальних мереж є віртуальна приватна мережа (Virtual Private Network, VPN). Так називається мережа організації, що отримується у результаті об'єднання двох або декількох територіально розділених ЛОМ за допомогою загальнодоступних каналів глобальних мереж, наприклад, через Інтернет.

Також мережі розділяються за типом корпоративної належності: мережі рівня відділу, мережі кампусів та корпоративні мережі.

✎**Мережа рівня відділу** – мережа з невеликою (до 150) кількістю комп'ютерів, які виконують завдання конкретного підрозділу організації і перебувають в межах однієї будівлі (найчастіше – поверху, офісу).

✎**Мережа кампусів** – мережа, яка об'єднує мережі відділів без використання глобальних з'єднань і територіально розташована в одному або декількох поруч розташованих будинках.

✎**Корпоративна мережа** – мережа, яка об'єднує практично всі комп'ютери, мережі відділів і кампусів корпоративної структури незалежно від їх територіального розташування (можливо навіть на різних континентах планети).

За типом середовища передачі мережі діляться на **дротові й бездротові**. Дротові мережі організуються з використанням мідного коаксіального кабелю, витої пари або оптичного волокна.

За розподілом ролей між комп'ютерами мережі бувають **одноранговi й клієнт-серверн**і. Для розуміння різниці між одноранговими та клієнт-серверними мережами введемо визначення поняття «серверу» та «клієнтського комп'ютеру».

✎**Сервер** [**Ошибка! Источник ссылки не найден.**] – спеціально виділений високопродуктивний комп'ютер, оснащений відповідним програмним забезпеченням, що централізовано керує роботою мережі й/або той, що надає іншим комп'ютерам мережі свої ресурси (файли даних, накопичувачі, принтер і т.д.).

Клієнтський комп’ютер (клієнт, робоча станція) [**Ошибка! Источник ссылки не найден.**] – комп’ютер рядового користувача мережі, що отримує доступ до ресурсів сервера (серверів).

1.2 Однорангові та клієнт-серверні мережі

В одноранговій мережі (рис. 1.4) всі комп’ютери мають однакові права доступу до загального середовища передачі даних. Кожний з них може виступати як у ролі сервера, тобто надавати файли й апаратні ресурси (накопичувачі, принтери та ін.) іншим комп’ютерам, так і в ролі клієнта, що користується ресурсами інших комп’ютерів. Наприклад, якщо на комп’ютері встановлено принтер, то з його допомогою роздруковувати свої документи зможуть всі інші користувачі мережі.

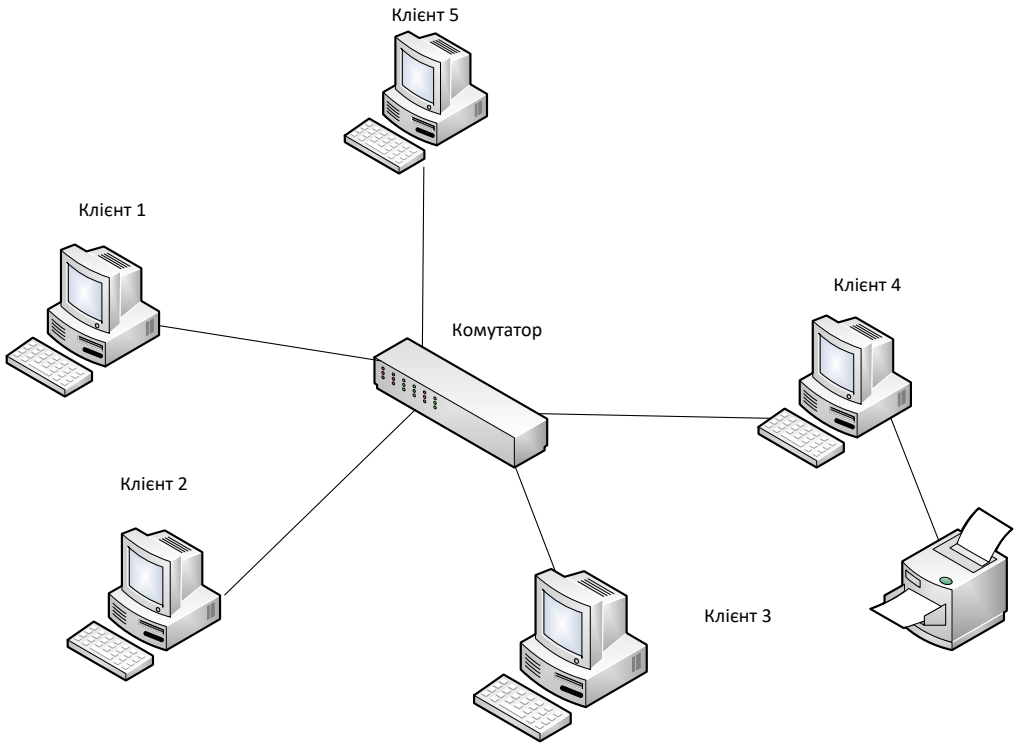


Рисунок1.4 – Приклад однорангової мережі

Однорангові мережі мають як переваги, так і недоліки у використанні, наявність яких слід враховувати при побудові архітектури мережі.

Переваги однорангових мереж:

– легко встановлюються і налагоджуються;

– кожен комп’ютер мережі працює незалежно від інших вузлів мережі;

– користувач має можливість контролювати ресурси свого персонального комп’ютера;

– низька собівартість;

– немає необхідності в додатковому програмному забезпеченні (крім операційної системи) та в постійній присутності адміністратора мережі.

Недоліки однорангових мереж

– необхідно пам’ятати паролі до всіх розділених ресурсів;

– незручність при спільному використанні даних у зв’язку з відсутністю централізованого сховища;

– відсутність можливості централізованого керування мережею й доступом до даних;

– низька загальна захищеність мережі й даних.

Таким чином, однорангові мережі слід використовувати при організації мережі з невеликою кількістю комп’ютерів у випадках, коли безпека передачі даних не важлива. Однак, при побудові сучасних комп’ютерних мереж виникає потреба у керуванні комп’ютерами у мережі з метою розподілення між ними ресурсів або для забезпечення певного рівня безпеки. Всі ці задачі виконуються адміністраторами клієнт-серверних мереж.

Адміністратор мережі [**Ошибка! Источник ссылки не найден.**] – людина, що володіє всіма повноваженнями для керування комп’ютерами, правами користувачів й ресурсами в мережі.

Адміністрування мережі [**Ошибка! Источник ссылки не найден.**] – рішення цілого комплексу завдань з керування роботою комп’ютерів, мережного устаткування й правами користувачів, захисту даних, забезпечення доступу до ресурсів, установка й модернізації системного й прикладного програмного забезпечення.

Число комп’ютерів в однорангових мережах зазвичай не перевищує 10, саме тому вони і називаються робочою групою. Типовими прикладами робочих груп є домашні мережі або мережі невеликих офісів.

Як правило, мережі створюються в установах або великих організаціях. У таких мережах (рис. 1.5) виділяються один або кілька комп’ютерів, так званих серверів, завданням яких є забезпечення швидкої та ефективної обробки великої кількості запитів інших комп’ютерів-клієнтів.

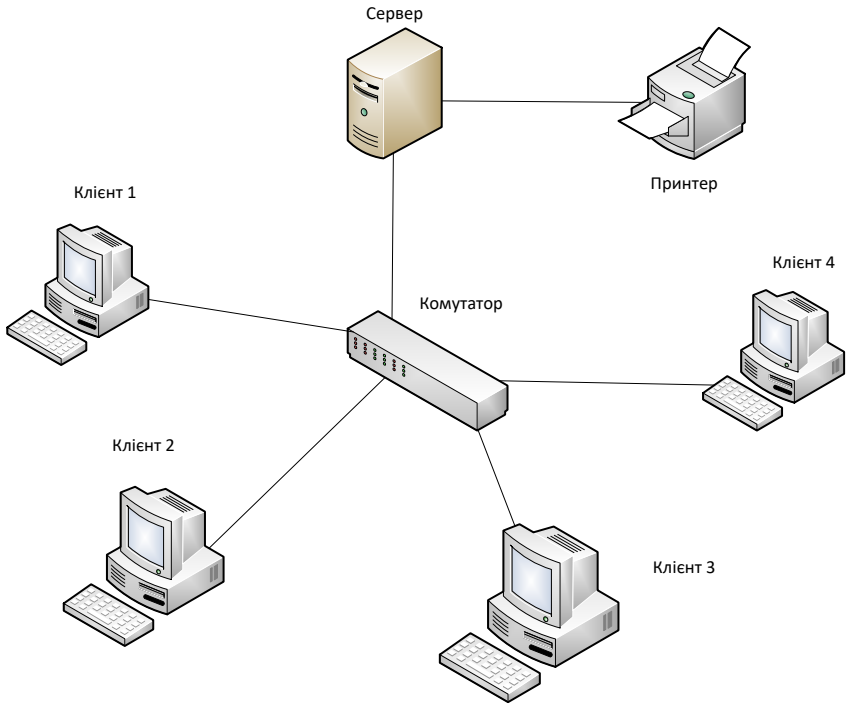


Рисунок 1.5 – Приклад мережі з виділеним сервером

При цьому клієнтські запити бувають різними, від найпростішої перевірки імені та пароля користувача при вході в систему до складних пошукових запитів до баз даних, на обробку яких сучасний багатопроцесорний комп'ютер може витратити кілька годин.

Зазвичай в якості серверів використовуються потужні та більш надійні комп'ютери, ніж робочі станції користувачів. Сервери зазвичай оснащують спеціалізованим устаткуванням, наприклад ємними сховищами даних, високошвидкісними мережними адаптерами та ін. Ці комп'ютери працюють постійно, цілодобово надаючи користувачам свої ресурси й забезпечуючи доступ до своїх служб.

Служби (services) [**Ошибка! Источник ссылки не найден.**] – серверні програми, що виконують певні дії за запитом клієнта.

Переваги клієнт–серверних мереж:

– наявність потужного серверу забезпечує швидкий доступ до ресурсів і ефективну обробку запитів клієнтів;

– можливість керування даними, які спільно використовуються;

– процедури резервного копіювання значно легша;

– висока захищеність даних у мережі.

Недоліки клієнт–серверних мереж:

– несправність сервера призводить до недоступності ресурсів;

– висока вартість супроводу мережі;

– потреба у виділеному обладнанні й спеціалізованому програмному забезпеченні;

– необхідність у значно більшому адмініструванні системи.

1.3 Взаємодія комп'ютерів у мережі

Оглядово розглянемо, як комп'ютери взаємодіють між собою в мережі. Для сумісної роботи ресурсів (серверів, стаціонарних робочих станцій користувачів, ноутбуків, принтерів, мережних сховищ даних та ін.) в мережі, вони певним чином з'єднуються між собою. Для цього застосовуються мережні кабелі різних типів, телефонні або супутникові канали або бездротові канали зв'язку (WLAN, Wi-Fi, Wi-MAX, Bluetooth).

Для з'єднання комп'ютерів з кабелями використовуються спеціальні конектори, закріплені на кінцях. Один кінець кабелю вставляється в мережний адаптер, а інший – до будь-якого пристрою зв'язку (концентратор, міст, комутатор, маршрутизатор, шлюз та ін.). –

✎**Мережний адаптер (**network interface controller/card**) –** спеціальна плата («карту розширення»), яка встановлюється на комп'ютері підключення його до мережі.

У більшості сучасних комп'ютерів мережний адаптер є вбудованим. Якщо ж використовується бездротовий мережний адаптер, то взаємодія з мережею відбувається за рахунок передачі радіосигналів між адаптером і точкою доступу, з'єднаною з локальною мережею.

? Контрольні запитання:

1. Як ви розумієте поняття «мережа» та «ресурси»?
2. Як класифікуються мережі за принципом територіальної приналежності?
3. У чому полягають відмінності глобальних та локальних мереж?

Тести з теми «Основні поняття та класифікація комп'ютерних мереж»

1.Оберіть найбільш точну причину об'єднання комп'ютерів у мережу.

A. Для обміну інформацією й спільного використання ресурсів.

B. Для обміну інформацією та спільного керування роботою ресурсів.

C. Для обміну файлами між комп'ютерами, що знаходяться на великих відстанях один від одного.

2.Вкажіть відповідність між визначеннями та термінами.

A. Локальна обчислювальна мережа	1. невелика група комп'ютерів, зв'язаних один з одним і розташованих звичайно в межах одного будинку або організації;
B. Регіональна мережа	2. мережа, що з'єднує безліч локальних мереж у рамках одного
C. Глобальна мережа	

району, міста або регіону;

3. мережа, що поєднує комп’ютери різних міст, регіонів і держав;

3.Оберіть переваги однорангових мереж.

A.Легкість в установці й настроюванні.

B.Порівняно низька вартість розгортання й підтримки.

C.Підвищення загальної захищеності мережі й схоронності даних.

D.Централізація даних і ресурсів дозволяє налагодити чітке керування інформацією й користувальницькими даними.

E.Відсутність необхідності в постійній присутності адміністратора мережі.

4.Оберіть недоліки однорангових мереж.

A.Необхідність робити резервне копіювання окремо на кожному комп’ютері, щоб захистити всі дані, які спільно використовуються;

B.Вартість супроводу мережі;

C.Потреба у виділеному обладнанні та спеціалізованому програмному забезпеченні;

D.Необхідність у значно більшому адмініструванні системи.

E. Відсутність можливості централізованого керування мережею й доступом до даних;

F. Низька загальна захищеність мережі й даних.

5.Оберіть переваги клієнт-серверних мереж.

A.Централізація даних і ресурсів дозволяє налагодити чітке керування інформацією й користувальницькими даними;

B.Розміщення даних на сервері істотно спрощує процедури резервного копіювання;

C.Легкість в установці й настроюванні;

D.Незалежність окремих комп’ютерів і їхніх ресурсів один від одного;

E.Підвищується загальна захищеність мережі й схоронність даних.

6.Оберіть недоліки клієнт-серверних мереж.

A.Несправність сервера може зробити всю мережу практично непрацездатною, а ресурси – недоступними;

B.Складність розгортання й підтримки вимагає наявності кваліфікованого персоналу, що збільшує загальну вартість супроводу мережі;

C.Відсутність можливості централізованого керування мережею й доступом до даних;

D. Низька загальна захищеність мережі й даних.

Тема 2 Принципи взаємодії комп'ютерів у мережі

Ключові поняття: протокол, модель OSI, фізичний рівень, канальний рівень, мережний рівень, транспортний рівень, сеансовий рівень, рівень представлення, прикладний рівень

Взаємодія комп'ютерів у мережі подібна до спілкування людей за допомогою листів. Щоб передати лист з одного міста до іншого, яке може бути розташоване і в іншій країні, і, навіть, на іншому континенті. Для цього необхідно виконати цілий ряд певних дій: потрібно написати текст на аркуші паперу, підписати його, вкласти в конверт, указати на ньому адреси відправника й отримувача, наклеїти марку й віддати листоноші (або кинути в поштову скриньку). Подальша доля листа залежить вже від поштової служби. Яким-небудь засобом – на поїзді, кораблі, літаку або якось інакше, але лист доходить до адресата. Адресат отримує можливість відкрити конверт і прочитати повідомлення. Якщо яка-небудь зі стадій доставки не виконається, то інформація до адресата так і не дійде.

Так само і для спілкування вузлів у мережі, доводиться застосовувати цілий ряд послідовно виконуваних процедур – мережних протоколів. Для надійної та узгодженої роботи протоколів кожна операція в них повинна підпорядковуватись певним правилам. А для взаємодії програм й устаткування різних виробників одного з одним протоколи повинні відповідати певним промисловим стандартам.

Протокол [**Ошибка! Источник ссылки не найден.**] **–** набір правил і процедур, що регулюють порядок взаємодії комп'ютерів у мережі.

За роки існування комп'ютерних мереж було створено безліч різних протоколів – як відкритих (опублікованих для безкоштовного застосування), так і закритих (розроблених комерційними компаніями з необхідністю придбання ліцензії для використання). Однак всі ці протоколи прийнято зіставляти) з еталонною моделлю взаємодії відкритих систем (Open Systems Interconnection Reference Model), або просто моделлю OSI. Її опис був опублікований у 1984 р. Міжнародною організацією зі стандартизації (InterNATional Standards Organization, ISO), тому для неї часто використовується інша назва – модель ISO/OSI. Ця модель поєднує набір специфікацій, що описують мережі з неоднорідними обладнаннями, вимоги до них, а також способи їх взаємодії.

2.1 Структура моделі OSI

Модель OSI має вертикальну структуру, у якій усі мережні функції розподілені між сімома рівнями (рис. 1.6). Кожному такому рівню відповідають строго певні операції, устаткування й протоколи.

Реальна взаємодія рівнів при передачі інформації можлива тільки за вертикаллю й тільки із сусідніми рівнями.

Логічна взаємодія (відповідно до правил того чи іншого протоколу) здійснюється за горизонталлю – з аналогічним рівнем іншого комп'ютера на протилежному стороні лінії зв'язку. Кожний більш високий рівень користується послугами рівня, що знаходиться нижче, знаючи, у якому виді і яким способом (тобто через який інтерфейс) потрібно передати йому дані.

Рисунок 1.6 – МодельOSI

Завдання більш низького рівня – прийняти дані, додати свою інформацію (наприклад, адресну, яка необхідна для правильної взаємодії з аналогічним рівнем на іншому комп'ютері) і передати дані далі. Тільки на найнижчому, фізичному рівні мережної моделі, інформація попадає до середовища передачі й досягає комп'ютера-отримувача. На ньому вона проходить всі рівні у зворотному напрямку, поки не досягне прикладного.

Як бачимо, усе це дуже схоже, наприклад, з роботою пошти – програми «спілкуються» у мережі приблизно так само, як люди спілкуються, пишучи листи та відсилаючи їх поштою. Лист передається з верхнього рівня вниз, проходячи безліч необхідних стадій. При цьому він «обростає» службовою інформацією (конверт певного виду, адреса на конверті, поштовий індекс) і зазнає певну обробку (листоноша у відділенні забирає лист, на конверт наклеює марки, ставить штемпелі, а після сортування лист потрапляє в контейнер для перевезення пошти в інше місто). Так інформація доходить до самого нижнього рівня – поштового транспорту, яким вона перевозиться в пункт призначення. Там відбувається зворотній процес: відкривається контейнер, лист витягується, зчитується адреса, після чого листоноша доставляє лист адресатові, який

отримує інформацію в первісному вигляді – коли витягає аркуш із конверта, перевіряє підпис і читає текст.

Таким чином, люди мають прямий зв'язок, і деталі доставки їх мало турбують. Листоноші також мають прямий зв'язок: листоноша в місті доставки отримує у точності те, що передається листоноші у місті відправки– конверт із листом і адресною інформацією. Листонош при цьому не хвилюють проблеми, наприклад, залізничників, які в дійсності й здійснювали перевезення поштової кореспонденції.

Тепер познайомимося ближче з рівнями моделі OSI і визначимо мережні послуги, які вони надають суміжним рівням.

2.2 Рівні моделі OSI

Розглянемо детальніше усі рівні моделі OSI [**Ошибка! Источник ссылки не найден.**].

Рівень 1 – Фізичний (Physical). Фізичний рівень відповідає за передачу біт у фізичному середовищі у вигляді електричних або світлових сигналів. На цьому рівні визначаються електричні, оптичні, механічні й функціональні характеристики ліній зв'язку: напруга, частота, довжина хвиль, типи конекторів, кількість й функціональність контактів, схеми кодування сигналів тощо. Також на цьому рівні визначається топологія мережі (це поняття буде розглянуто у рамках наступної теми)

Рівень 2 – Канальний (Data Link). Канальний рівень забезпечує безпомилкову передачу даних, отриманих від вищого мережного рівня 3, через фізичний рівень 1 між двома робочими станціями у мережі. Повідомлення на цьому рівні формуються у кадри.

Кадр (frame) – мінімальний фрагмент даних, що передається у мережі.

Канальний рівень складається з двох підрівнів: керування доступом до середовища (Media Access Control, MAC) і керування логічним зв'язком (Logical Link Control, LLC).

Рівень MAC забезпечує спільний доступ мережних адаптерів до фізичного рівня, визначення границь кадрів, розпізнавання адреси призначення кадрів (їх часто називають фізичними, або Mac-Адресами).

Рівень LLC, що діє над рівнем MAC, відповідає за встановлення каналу зв'язку й за безпомилкове посилання й приймання повідомлень із даними.

Рівень 3 – Мережний (Network). Мережний рівень відповідає за забезпечення зв'язку між будь-якими вузлами мережі з довільною топологією. На цьому рівні визначається маршрут проходження повідомлення, а також вирішується завдання керування потоками даних і обробки помилок передачі.

Маршрут – послідовність маршрутизаторів складеної мережі, через які проходить пакет.

Рівень 4 – Транспортний (Transport). На транспортному рівні визначається ступінь надійності доставки інформації від одного комп'ютера іншому. На цьому рівні виконуються наступні дії: повідомлення сеансового рівня розбиваються на пакети, та нумеруються, буферизуються прийняті

пакети, упорядковуються пакети, які прибувають, адресуються прикладні процеси (назначаються порти) та здійснюється управління потоком.

Таким чином, транспортний рівень завершує процес передачі даних, приховуючи від більш високих рівнів усі деталі й проблеми, пов'язані з доставкою інформації будь-якого обсягу між будь-якими точками мережі.

✎**Рівень 5 – Сеансовий (Session).** Сеансовий рівень дозволяє двом мережним додаткам на різних комп'ютерах встановлювати, підтримувати й завершувати з'єднання, що називається мережним сеансом. Орім цього, на 5-му рівні моделі OSI здійснюється відновлення аварійно перерваних сеансів зв'язку та виконується перетворення зручних для людей імен комп'ютерів у мережні адреси (розпізнавання імен), а також реалізуються функції захисту сеансу.

✎**Рівень 6 – Представницький, або Рівень представлення (Presentation).** Визначає формати інформації, що передається між комп'ютерами. На цьому рівні здійснюється перекодування, стиск і розпакування даних, шифрування й дешифрування, підтримка мережних файлових систем та ін.

✎**Перекодування** – переведення інформації у вид, зрозумілий всім комп'ютерам, які беруть участь в обміні)

✎**Рівень 7 – Прикладний (Application), або Рівень додатків.** Забезпечує взаємодію мережних програм, що працюють на комп'ютерах. Саме за допомогою цих програм користувач отримує доступ до таких мережних послуг, як обмін файлами, передача електронних листів, вилучений термінальний доступ та ін.

До моменту появи моделі OSI вже існували й показали високу ефективність інші набори (стеки) протоколів, наприклад стек TCP/IP. Тому побудований у повній відповідності з описаною вище моделлю набір протоколів OSI так і не отримав широкого поширення. Більшість сучасних мережних архітектур і наборів протоколів відповідають цій моделі лише до певного ступеня. Незважаючи на це, сама модель ISO/OSI дотепер широко використовується для опису взаємодії в мережних середовищах.

? Контрольні запитання:

1. Що розуміється під терміном «мережний протокол»?
2. Які мережні функції здійснюються в моделі OSI?
3. Який рівень, згідно з моделлю OSI, відповідає за вибір маршруту передачі даних?
4. На якому рівні моделі OSI взаємодіють програми, що забезпечують передачу повідомлень електронної пошти?

✍Практичні завдання:

Завдання 1.

Заповнити таблицю 1.1:

1. вказати номер порту, який відповідає протоколу;

2. описати основні функції, які виконує протокол у мережі при передачі даних.

Таблиця 1.1 – Опис основних протоколів мережної взаємодії

№	Протокол	Порт	Опис призначення та основних функцій
1	ARP		
2	DHCP		
3	DNS		
4	FTP		
5	HTTP		
6	HTTPS		
7	ICMP		
8	ICMPv6		
9	NTP		
10	POP3		
11	SMTP		
12	SNMP		
13	SSH		
14	TCP		
15	TFTP		
16	Telnet		
17	RDP		
18	VNC		
19	UDP		
20	VTP		

Завдання 2.

Заповнити таблицю 1.2, вказавши протоколи рівнів моделі OSI (прикладного, представлення, сеансового, транспортного, мережного, канального, фізичного)

Таблиця 1.2 – Опис основних протоколів відповідних рівнів OSI

№	Рівень моделі OSI	Перелік загальних протоколів та технологій
7	Прикладний	
6	Представлення	
5	Сеансовий	
4	Транспортний	
3	Мережний	
2	Канальний	
1	Фізичний	

Тести з теми «Принципи взаємодії комп'ютерів у мережі»

1. На якому рівні моделі OSI працює прикладна програма?

A. Physical layer

B. Data-link layer

C. Network layer

D. Transport layer

E. Session layer

F. Presentation layer

G. Application layer

2. На якому рівні моделі OSI працюють мережні служби?

A. Physical layer

B. Data-link layer

C. Network layer

D. Transport layer

E. Session layer

F. Presentation layer

G. Application layer

3. Яка назва традиційно використовується для одиниці переданих даних на канальному рівні?

A. Пакет

B. Повідомлення

C. Кадр

D. Потік

E. Сегмент

4. Яка назва традиційно використовується для одиниці переданих даних на мережному рівні?

A. Пакет

B. Повідомлення

C. Кадр

D. Потік

E. Сегмент

5. Перерахуйте рівні моделі OSI

layer 7 -_____

layer 6 -_____

layer 5 -_____

layer 4 -_____

layer 3 -_____

layer 2 -_____

layer 1 -_____

6. Вкажіть, принаймні, три причини, за якими промисловість повинна використовувати рівневу модель (наприклад, модель OSI)_____
_____
_____

7. З яких підрівнів складається канальний рівень в технологіях локальних мереж?_____
_____
_____

Тема 3 Мережні топології та способи доступу до середовища передачі даних

Ключові поняття: топологія комп'ютерної мережі, шина, кільце, зірка, ієрархічна зірка, сітчаста топологія, доступ, множинний доступ до середовища передачі даних з контролем несучої і виявленням зіткнень, множинний доступ до середовища передачі даних з контролем несучої та запобіганням зіткнень, передача маркера.

Першим завданням, яке постає при організації комп'ютерної мережі, є вибір її топології.

Топологія комп'ютерної мережі – це схема розташування вузлів у мережі один відносно іншого та спосіб їх з'єднання лініями зв'язку.

При виборі топології мережі враховується багато факторів, які забезпечують надійну та ефективну роботу мережі, зручне управління потоками мережних даних. Щоб вирішити це завдання, необхідно знати, які взагалі бувають мережні топології. Зауважимо, що при цьому слід розрізняти поняття фізичної топології, тобто способу розміщення комп'ютерів, мережного обладнання та їх з'єднаннях за допомогою кабельної інфраструктури, і логічної топології – структури взаємодії комп'ютерів та характеру поширення сигналів у мережі.

3.1 Базові мережні топології

До базових топологій, на основі яких будуються комп'ютерні мережі, належать: шина, кільце, зірка-шина [**Ошибка! Источник ссылки не найден.**].

Шина (Bus). Комп'ютери у мережі з'єднуються між собою одним кабелем (рис. 1.7). Надіслані в таку мережу дані передаються всім комп'ютерам, але обробляє їх тільки той комп'ютер, апаратна MAC-адреса мережного адаптера якого записана в кадрі як адреса одержувача.

Ця топологія виключно проста в реалізації та дешева (вимагає найменше кабелю), проте має ряд істотних недоліків.

Недоліки мереж типу «шина»:

– мережі з топологією типу «шина» важко розширювати; збільшення як числа комп'ютерів у мережі, так і кількості сегментів – окремих відрізків кабелю, які їх з'єднують, неможливе без припинення роботи всієї мережі;

– передачу даних може вести тільки один з комп'ютерів, оскільки шина використовується спільно, у кожен момент часу;

Коли два комп'ютери водночасно передають кадри у мережу, вони накладаються один на одного і спотворюються. Ця ситуація називається **колізією**.

Після виникнення колізії комп'ютери змушені призупинити передачу, а потім почати поторну відправку даних. Вплив зіткнень тим помітніший, чим вищий обсяг переданої по мережі інформації і чим більше комп'ютерів підключено до шини. Обидва ці фактори, природно, знижують як максимально

можливу, так і загальну продуктивність мережі, сповільнюючи її роботу.

– «шина» є пасивною топологією – комп'ютери тільки «слухають» кабель і не можуть відновлювати сигнали, що затухають при передачі в мережі. Щоб подовжити мережу, потрібно використовувати повторювачі (репітери), які посилюють сигнал перед його передачею у наступний сегмент;

– надійність мережі з топологією «шина» невисока. Коли електричний сигнал досягає кінця кабелю, він (якщо не прийняті спеціальні заходи) відбивається, порушуючи роботу всього сегмента мережі. Щоб запобігти такому відображенню сигналів, на кінцях кабелю встановлюються спеціальні резистори (термінатори), які поглинають сигнали. Якщо ж у будь-якому місці кабелю виникає обрив – наприклад, при порушенні цілісності кабелю або просто при від'єднанні конектора, – то виникають два незатермінованих сегменти, на кінцях яких сигнали починають відбиватися, і вся мережа перестає працювати.

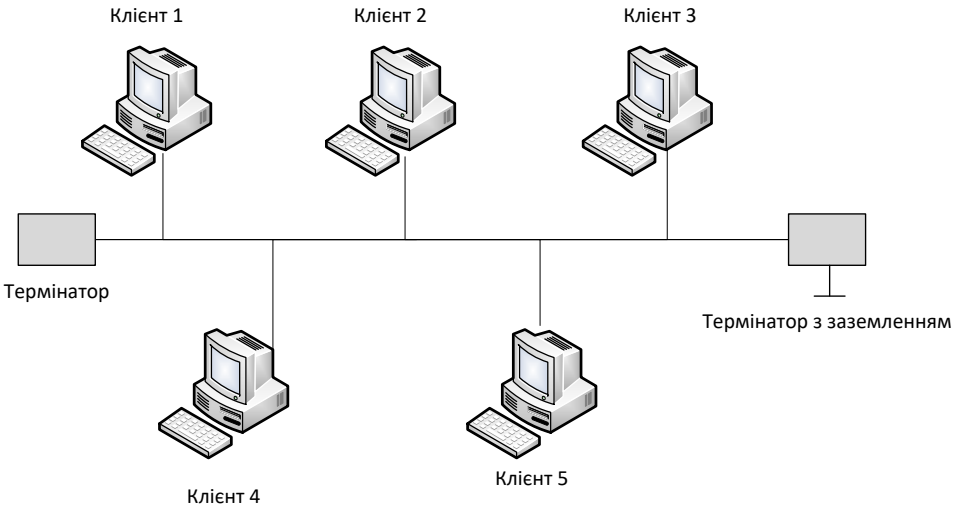


Рисунок 1.7 – Мережа з топологією «шина»

Проблеми, характерні для топології «шина», призвели до того, що на сучасному етапі вона практично не використовується.

Кільце (Ring). У цій топології кожен з комп'ютерів з'єднується з двома іншими так, щоб від одного він отримував інформацію, а іншому – передавав її (рис.1.8). Останній комп'ютер підключається до першого, та кільце замикається.

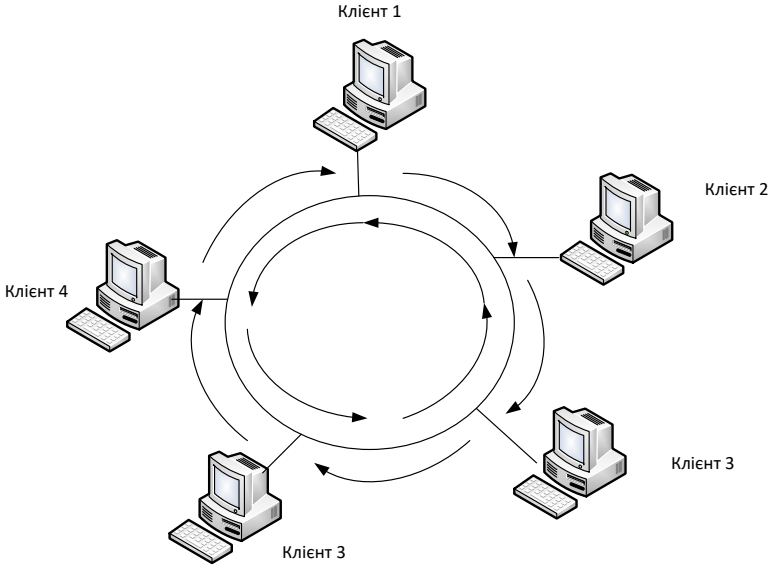


Рисунок 1.8 – Мережа з топологією «кільце»

Переваги мереж з топологією «кільце»:

– оскільки у кабелів в цій мережі немає вільних кінців, термінатори не потрібні;

– кожен комп’ютер виступає в якості повторювача, посилюючи сигнал, що дозволяє будувати мережі великої протяжності;

– через відсутність зіткнень топологія має високу стійкість до перевантажень, що забезпечує ефективну роботу з великими потоками переданої мережею інформації

Недоліки мереж з топологією «кільце»:

– сигнал в «кільці» повинен пройти послідовно (і тільки в одному напрямку) через всі комп’ютери, кожен з яких перевіряє, чи не йому адресована інформація, тому час передачі може бути достатньо великим;

– підключення до мережі нового комп’ютера часто вимагає припинення її роботи;

– вихід з ладу хоча б одного комп’ютера або пристрою порушує роботу всієї мережі;

– розрив або коротке замикання в будь-якому з кабелів кільця робить роботу

У мережі з топологією «кільце» (як і в мережі з топологією «шина») недоліків більше ніж переваг, що призвело до достатньо рідкого використання цієї топології на практиці.

Найбільш поширеною топологією є топологія **«зірка-шина» (Star Bus)**, або **«пасивна зірка»** (рис. 1.9). Тут периферійні комп’ютери підключаються не до центрального комп’ютера, а до пасивного концентратора, або хабу (hub). Останній, на відміну від центрального комп’ютера, ніяк не відповідає за управління обміном даними, а виконує ті ж функції, як повторювач, тобто відновлює сигнали, які надходять, та пересилає їх усім іншим комп’ютерам і

пристроям, підключеним до нього. Саме тому дана топологія, хоча фізично і виглядає як «зірка», логічно є топологією «шина» (що й відображено в її назві).

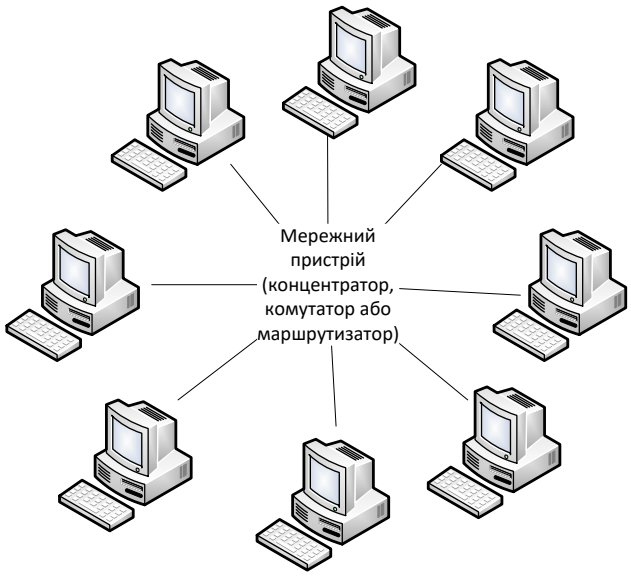


Рисунок 1.9 – Мережа з топологією «зірка-шина»

Незважаючи на більшу витрату кабелю, характерну для мереж типу «зірка», ця топологія має суттєві переваги перед іншими, що й зумовило її найширше застосування в сучасних мережах.

Переваги мереж типу «зірка-шина»:

– надійність – підключення до центрального концентратора та відключення комп'ютерів від нього ніяк не відбивається на роботі решти мережі, розриви кабелю впливають тільки на одиничні комп'ютери; термінатори не потрібні;

– легкість при обслуговуванні та усуненні проблем – всі комп'ютери та мережні пристрої підключаються до центрального з'єднувального пристрою, що істотно спрощує обслуговування та ремонт мережі;

– захищеність – концентрація точок підключення в одному місці дозволяє легко обмежити доступ до важливих об'єктів мережі.

При використанні замість концентраторів мостів, комутаторів або маршрутизаторів (на них докладніше ми зупинимося пізніше) виходить «проміжний» тип топології між активною та пасивною зіркою. В цьому випадку пристрій зв'язку не тільки ретранслює сигнали, що надходять, але і проводить управління їх обміном.

3.2 Інші мережні топології

У реальності комп'ютерні мережі постійно розширюються та модернізуються. Тому майже завжди така мережа є гібридною, тобто її топологія представляє собою комбінацію декількох базових топологій. Легко

уявити собі гібридні топології, які є комбінацією «зірки» і «шини», або «кільця» і «зірки».

Однак особливо слід виділити топологію «дерево» (tree), яку можна розглядати як об'єднання кількох «зірок». Саме ця топологія сьогодні є найбільш популярною при побудові локальних мереж.

Свого роду «предтечею» Інтернету була мережа ARPANet, спочатку створена на замовлення Міністерства оборони США. Метою цього проекту була розробка такої системи зв'язку, яка могла б функціонувати навіть в умовах атомної війни. Нинішній Інтернет, як вільно доступна всесвітня комп'ютерна мережа, став несподіваним, «конверсійним» результатом військових розробок.

Нарешті, слід згадати про **сітчасту**, або **сіткову (mesh) топологію**, в якій всі або майже всі комп'ютери та інші пристрої з'єднані один з одним безпосередньо (рис. 1.10). Така топологія виключно надійна – при обриві будь-якого каналу передача даних не припиняється, оскільки можливі декілька маршрутів доставки інформації. Сіткові топології (найчастіше не повні, а часткові) використовуються там, де потрібно забезпечити максимальну відмовостійкість мережі, наприклад, при об'єднанні кількох ділянок мережі великого підприємства або при підключенні до Інтернету, хоча за це, звичайно, доводиться платити: істотно збільшується витрата кабелю, ускладнюється мережне обладнання та його налаштування.

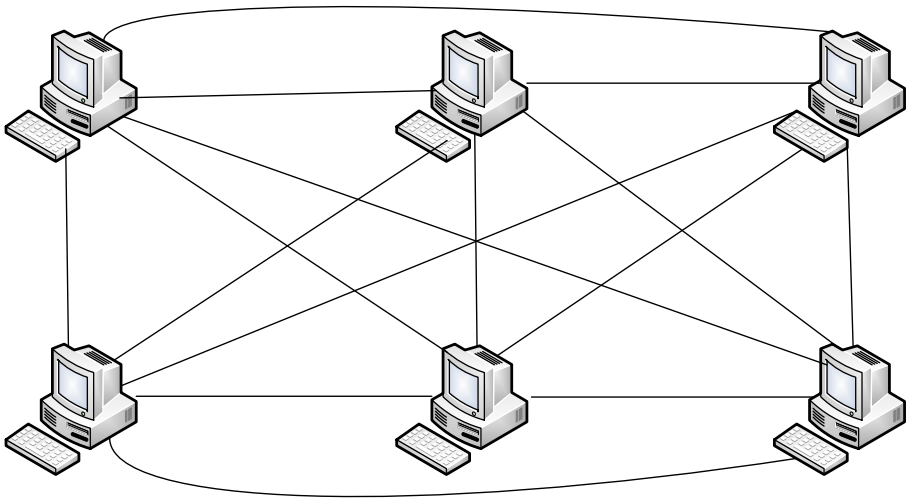


Рисунок 1.10 – Мережа з сітчастою топологією

3.3 Доступ до середовища передачі

З мережною топологією тісно пов'язане поняття способу доступу до середовища передачі, під яким розуміється набір правил, що визначають, як саме комп'ютери повинні відправляти і приймати дані по мережі.

Таких способів можливо декілька. Основними з них є:

– множинний доступ з контролем несучої і виявленням зіткнень;

– множинний доступ з контролем несучої та запобіганням зіткнень;

– передача маркера.

При **множинному доступі з контролем несучої і виявленням зіткнень** (Carrier Sense Multiple Access with Collision Detection, CSMA/CD) усі комп'ютери (множинний доступ) «слухають» кабель (контроль несучої), щоб визначити, передаються по ньому дані чи ні. Якщо кабель вільний, то будь-який комп'ютер може почати передачу, а всі інші комп'ютери мають чекати, поки кабель не звільниться. Якщо комп'ютери почали передачу одночасно і виникло зіткнення, всі вони призупиняють передачу (виявлення зіткнень), кожний – на різні проміжки часу, після чого ретранслюють дані.

Серйозним недоліком цього способу доступу є те, що при великій кількості комп'ютерів та високому навантаженні на мережу число зіткнень зростає, а пропускна спроможність зменшується, іноді дуже істотно.

Однак цей метод дуже простий за технічною реалізацією, тому саме він використовується у найбільш популярній сьогодні технології Ethernet. А щоб зменшити кількість зіткнень, в сучасних мережах застосовуються такі пристрої, як мости, комутатори та маршрутизатори.

Метод **множинного доступу з контролем несучої та запобіганням зіткнень** (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) відрізняється від попереднього тим, що перед передачею даних комп'ютер посилає в мережу спеціальний невеликий пакет, який повідомляє іншим комп'ютерам про свій намір розпочати трансляцію. Так інші комп'ютери «дізнаються» про підготовку передачі, що дозволяє уникнути зіткнень. Звичайно, ці повідомлення збільшують загальне навантаження на мережу і знижують її пропускну спроможність (через що метод CSMA/CA працює повільніше, ніж CSMA/CD), однак вони, безумовно, необхідні для роботи, наприклад, бездротових мереж.

У мережах з **передачею маркера** (Token Passing) від одного комп'ютера до іншого по колу постійно курсує невеликий блок даних, який називається маркером. Якщо у комп'ютера, який отримав маркер, немає інформації для передавання, він просто пересилає його наступному комп'ютеру. Якщо ж така інформація є, комп'ютер «захоплює» маркер, доповнює його даними і відсилає все це наступному комп'ютеру по колу. Такий інформаційний пакет передається від комп'ютера до комп'ютера, поки не досягне станції призначення. Оскільки у момент передачі даних маркер в мережі відсутній, інші комп'ютери вже не можуть нічого передавати. Тому в мережах з передачею маркера неможливі ні зіткнення, ні тимчасові затримки, що робить їх дуже привабливими для використання в системах автоматизації роботи підприємств.

3.4 Вибір комп'ютерної мережі

Розглянувши найбільш часто використовувані сьогодні мережні топології та методи доступу, обговоримо й інші чинники, що визначають вибір потрібного типу мережі.

При цьому слід враховувати:

– вже наявну кабельну систему та обладнання – чи є у вас дома,

навчальному закладі, офісі мережа, яку потрібно просто розширити, або у вас є тільки окремі комп'ютери;

– місце фізичного розташування – важливо враховувати, як розташовані комп'ютери і де ви збираєтеся розмістити мережне обладнання. Об'єднати комп'ютери в одній кімнаті досить просто, проте якщо ваші комп'ютери розташовуються на різних поверхах будівлі або навіть в декількох будівлях, найкращу конфігурацію мережі та її топологію слід ретельно продумати;

– розміри планованої мережі – якщо у вас є лише кілька комп'ютерів, структура мережі буде досить простою; якщо ж комп'ютерів сотні або тисячі, то, швидше за все, доведеться зупинити свій вибір на складній гібридній топології;

– обсяг і тип інформації для спільного використання – ці параметри повинні обов'язково враховуватися при виборі типу мережі: якщо між комп'ютерами передаються великі файли – музичні, відео-або графічні, то вам буде потрібна високошвидкісна мережа, яка дозволяє швидко і без затримок передавати такі обсяги інформації.

Переважна більшість сучасних мереж використовують топологію «зірка» або гібридну топологію, що представляє собою об'єднання кількох «зірок» (наприклад, топологію типу «дерево»), та метод доступу до середовища передачі CSMA/CD (множинний доступ з контролем несучої і виявленням зіткнень).

? Контрольні запитання:

1. У чому полягає відмінність між фізичними та логічними зв'язками?
2. Які базові мережні топології ви знаєте?
3. Які переваги та недоліки конфігурації «зірка»? У яких локальних мережах вона застосовується?
4. Які переваги та недоліки топології «кільце»? У яких локальних мережах вона застосовується?
5. Які переваги та недоліки конфігурації «шина»? У яких локальних мережах вона застосовується?
6. Які гібридні топології вам відомі?
7. Які фактори необхідно враховувати при плануванні мережі?

✍Практичні завдання:

Завдання 1.

Вам доручено встановити мережу для невеликої компанії, яка розвивається і займає половину поверху (рис.1.11). До складу компанії входять директор, керуючий, адміністратор і п'ять співробітників. Планується взяти на роботу ще двох співробітників. У кожного співробітника компанії є комп'ютер. Якщо необхідно обмінятися діловою інформацією, доводиться робити це усно або за допомогою зовнішніх носіїв інформації. Лазерний принтер знаходиться у адміністратора. У кожного співробітника є окремий принтер.

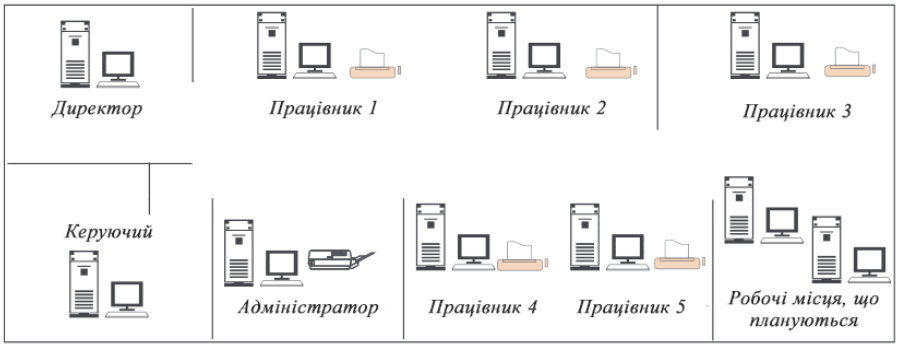


Рисунок 1.11 – Склад мережі компанії

Яку топологію мережі ви запропонували б для цієї компанії? Оцініть сумарну довжину кабелю, необхідного для прокладки мережі, в кожному із запропонованих варіантів та виберіть з них найбільш оптимальний.

Завдання 2.

Визначте топологію локальної мережі комп'ютерних класів у Запорізькому національному університеті, складіть її схему та оцініть оптимальність архітектури.

Тести з теми «Мережні топології й способи доступу до середовища передачі даних»

1. Дайте визначення поняттю «топологія».

A. Граф, вузлами якого є станції мережі або комунікаційні пристрої, а ребрами – фізичні лінії зв'язку

B. Повний граф, що демонструє взаємодію усередині базової мережної технології

C. Граф, що демонструє правила взаємодії вузлів мережі на транспортному рівні.

2. До якого типу топології можна віднести структуру, утворену чотирма зв'язаними один з одним вузлами (у вигляді квадрата)?

A. Зірка
B. Кільце
C. Сітчаста
D. Шина
E. Ієрархічна зірка

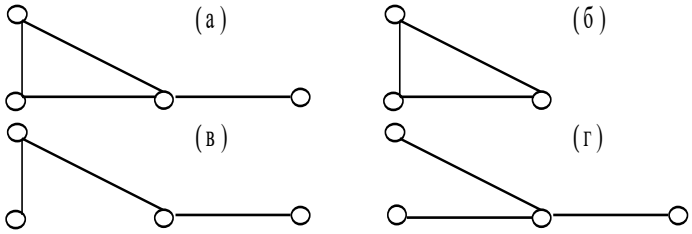
3. Яка з відомих топологій має підвищену надійність?

A. Кільце
B. Сітчаста
C. Шина

4. Який тип топології найпоширеніший сьогодні в локальних мережах?

A. Кільце
B. Сітчаста
C. Шина
D. Ієрархічна зірка

5. Зіставте зображеним на малюнку фрагментам мережі назви відповідних топологій :



(а) _____ (в) _____
(б) _____ (г) _____

6. Назвіть недоліки топології «зірка».

_____

7. Яка мережна топологія найбільш стійка до руйнувань і має найбільшу надмірність?

A. Загальна шина
B. Кільце
C. Зірка
D. Комірчаста
E. Перерахуйте недоліки повнозв'язної топології.

_____

8. Назвіть недоліки топології «загальна шина».

_____

9. Яка мережна топологія найбільш дешева в реалізації?

A. Загальна шина
B. Кільце
C. Зірка
D. Комірчаста

10. Назвіть недоліки топології «кільце».

_____

11. Яка топологія мережі є легко масштабованою і зручною при визначенні і дозволі проблем :

A. Загальна шина
B. Кільце
C. Зірка
D. Комірчаста

РОЗДІЛ 2 ОРГАНІЗАЦІЯ ЛОКАЛЬНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

Тема 4 Лінії зв'язку

Ключові поняття: лінії зв'язку, канали зв'язку, кабельні з'єднання, коаксіальний кабель, кручена пара, оптоволоконний кабель, бездротові мережі.

Взаємодію комп'ютерів у мережі на фізичному рівні забезпечує певне фізичне середовище, у якості якого можуть виступати кабелі (по ним поширюються електричні сигнали) або земна атмосфера та космічний простір (вони є середовищем електромагнітних хвиль).

Фізичне середовище разом із мережними пристроями передачі даних та пристроями зв'язку утворюють **лінії зв'язку** або **канали зв'язку** у мережі.

Розглянемо детальніше всі різновиди середовищ зв'язку у комп'ютерних мережах.

4.1 Кабельні з'єднання

У якості кабельних ліній зв'язку використовують такі їх різновиди [**Ошибка! Источник ссылки не найден.**]:

- коаксіальний кабель (coaxial cable);
- кручена пара (twisted pair):
  a) неекранована (unshielded, UTP),
  b) екранована (shielded);
- волоконно-оптичний, або оптоволоконний кабель (fiber optic).

Раніше при створенні мереж в основному застосовувався коаксіальний кабель (рис. 2.1). Коаксіальний кабель складається з несиметричних пар провідників. Кожна пара складається із внутрішньої мідної жили і співвісної з нею зовнішньої жили, яка може бути порожнистою мідною трубкою або опліткою, відокремленою від внутрішньої жили діелектричною ізоляцією. Зовнішня жила грає двояку роль - по ній передаються Комп'ютерні сигнали і вона є екраном, що захищає внутрішню жилу від зовнішніх електромагнітних полів.

Рисунок 2.1 – Коаксіальний кабель

Відповідно до сучасних стандартів коаксіальний кабель не вважається хорошим вибором при побудові структурованої кабельної системи будівель.

Основні типи і характеристики коаксіальних кабелів:

– «Товстий» коаксіальний кабель з хвильовим опором 50 Ом і зовнішнім діаметром близько 12 мм. Цей кабель має досить товстий внутрішній провідник діаметром 2,17 мм, який забезпечує хороші механічні та електричні характеристики (загасання на частоті 10 МГц - не гірше 18 д Б / км). Однак цей кабель складно монтувати – він погано гнеться.

– «Тонкий» коаксіальний кабель призначений для мереж із зовнішнім діаметром близько 50 мм і тонким внутрішнім провідником 0,89 мм, цей кабель не такий міцний, як «товстий» коаксіал, зате має набагато більшу гнучкість, що зручно при монтажі. «Тонкий» коаксіальний кабель також має хвильовий опір 50 Ом, але його механічні та електричні характеристики гірші, ніж у «товстого» коаксіального кабелю. Згасання в цьому типі кабелю вище, ніж в «толстому» коаксіальному кабелі, що призводить до необхідності зменшувати довжину кабелю для отримання однакового загасання в сегменті.

Згодом коаксіальний кабель в більшості мереж було замінено крученою парою або оптичними кабелями.

Кручена пара – два скручених один з одним ізольованих мідних дроти. Переважна більшість кабелів на основі крученої пари складається з чотирьох пар, перекручених з різним кроком для зменшення електричних наводок з боку сусідніх пар та зовнішніх джерел і покритих пластиковою оболонкою (рис. 2.2). В екранованій кручений парі, крім того, використовується одне або кілька обплетень з алюмінієвої або мідної фольги, що істотно підвищує захищеність кабелю від перешкод.

Такі кабелі випускаються відповідно до стандарту EIA/TIA 568 («Американський стандарт проводки у комерційних будівлях») і поділяються на категорії. Кабелі різної категорії розрізняються, в першу чергу, кроком скручення кручених пар. Чим менше крок, тим вище категорія та тим більших швидкостей передачі даних можна досягти при його використанні (табл. 2.1).

Рисунок 2.2 – Кручена пара

Завдяки своїй дешевизні, легкості в установці та універсальності (може використовуватися в більшості мережних технологій), неекранована кручена пара зараз є найпоширенішим типом кабелю, який використовується при побудові локальних мереж. Екранована кручена пара, незважаючи на велику захищеність від перешкод, не отримала широкого розповсюдження через складнощі в установці – потрібно дбати про заземлення, та й кабель порівняно з неекранованою крученою парою більш жорсткий.

Кручена пара підключається до комп'ютерів та інших пристроїв за допомогою роз'єму RJ-45 (Registered Jack 45). Цей конектор (рис. 2.3) схожий на конектор RJ-11, який застосовується в телефонних лініях, тільки трохи більший за нього. У табл. 2.2 наведений опис способів закладення кабелю «кручена пара» у конектор RJ-45 відповідно до стандартів EIA/TIA 56BA та 56BB; ця операція виконується за допомогою спеціального обжимного інструменту. (Якщо розташувати роз'єм контактами вгору і від себе, то нумерувати їх треба зліва направо, від 1 до 8.)

Рисунок 2.3 – Роз'єм RJ-45

Зауважимо, що кабелі, які вживаються для підключення комп'ютерів до концентраторів та комутаторів, обжимаються з двох боків однаково, тобто по одному й тому ж стандарту. При цьому виходить так званий прямий кабель. Однак для безпосереднього з'єднання мережних адаптерів комп'ютерів або для зв'язку між концентраторами та комутаторами використовується перехресний кабель («крос-кабель»). З одного боку такого кабелю кручені пари при їх закладенні в рознім міняють місцями: зелений провід – на місце помаранчевого, а блакитний – на місце коричневого, і навпаки.

Оптоволоконний кабель (рис. 2.4) відрізняється від інших видів мережної проводки тим, що передає світлові, а не електричні імпульси. Він дуже схожий на коаксіальний, але замість мідної або алюмінієвої жили використовується скловолокно.

При цьому можуть застосовуватися два види оптоволоконних кабелів: багатомодовий (multi-mode) або одномодовий (single-mode).

У відносно дешевому багатомодовому кабелі центральне скловолокно має діаметр 50 або 62,5 мкм, а оболонка – 125 мкм. Для передачі сигналів по багатомодовому кабелю застосовують недорогі світлодіодні трансивери з довжиною хвилі 850 нм.

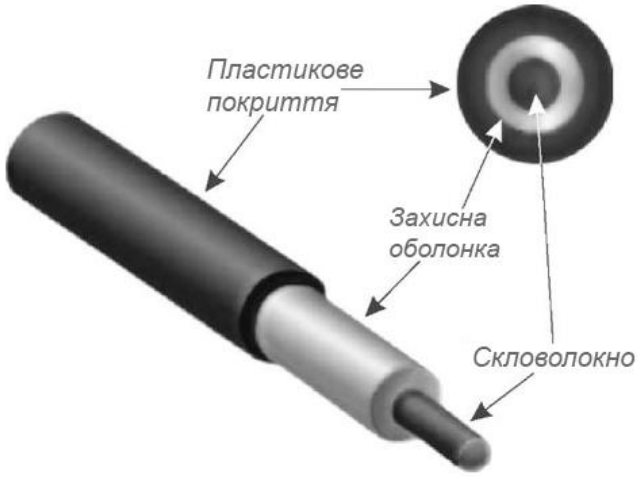


Рисунок 2.4 – Оптоволоконний кабель

У високоякісному (але дорогому) одномодовому кабелі волокно тонше – діаметром 9-10 мкм, а згасання світлового сигналу в ньому істотно менше. Крім того, для передачі сигналів по одномодовому кабелю використовуються лазерні трансивери з довжиною хвилі 1300 нм. У результаті максимальна відстань передачі світлового сигналу при застосуванні одномодових кабелів і трансиверів набагато більше, ніж для багатомодових.

Для підключення оптоволоконного кабелю використовуються спеціальні конектори (рис.2.5). Конектори FC та ST сьогодні вважаються застарілими, тому у новому обладнанні найчастіше застосовуються розніми для конекторів SC. Монтаж конекторів (закладення оптоволоконного кабелю в конектор) досить складний і вимагає спеціального обладнання. Правда, останнім часом з’явилися набори, що дозволяють закладати такі конектори і в домашніх умовах. Проте їх використання вимагає точності та терпіння, оскільки робиться шляхом вклеювання оптичного волокна в наконечник з подальшою сушкою та тонким шліфуванням.

Рисунок 2.5 – Оптоволоконні конектори різних типів

У порівнянні з електричними кабелями оптоволокно забезпечує підвищений захист від перешкод та перехоплення. Крім того, при його використанні дані вдається передавати на істотно більші відстані, та й

теоретично швидкість передачі в оптоволокні набагато вища. Недоліки оптоволокна – велика вартість кабелю, складність закладення конекторів (при якій потрібно зварювання скловолокна) і необхідність застосування додаткових трансиверів, які перетворюють світлові сигнали в електричні і навпаки. Все це помітно підвищує загальну вартість розгортання мережі, тому досі оптоволокно в локальних мережах застосовується рідше, ніж кручена пара.

Після вибору відповідного типа кабелю, яким збираються з'єднувати комп'ютери та мережні пристрої, та визначення місця комутації і розподілу можна приступити до прокладання кабелю. При прокладанні кабелю у будівлі проводку зазвичай закладають в стіни або розміщують у спеціальному просторі під фальшпідлогою або за навісною стелею, а потім виводять в настінні мережні розетки.

4.2 Бездротові мережі

Використання кабельних середовищ зв'язку у мережі призводить до низької мобільності, досить великих капіталовкладень в кабельну інфраструктуру та відносно малої дальності передачі сигналу. Уникнути цих недоліків допомагає викристання бездротових мереж.

Радіоканали наземного і супутникового зв'язку утворюються за допомогою передавача і приймача радіохвиль. Існує велика різноманітність типів радіоканалів, що відрізняються як частотним діапазоном, так і дальністю каналу. Діапазони широкомовного радіо (довгих, середніх і коротких хвиль), які також називаються АМ-діапазонами, або діапазонами амплітудної модуляції (Amplitude Modulation, AM) [**Ошибка! Источник ссылки не найден.**], забезпечують телекомунікацію, але при невисокій швидкості передачі даних.

Більш швидкісними є канали, які використовують діапазони дуже високих частот (Very High Frequency, VHF), в яких застосовується частотна модуляція (Frequency Modulation, FM). Для передачі даних також використовуються діапазони ультрависоких частот (Ultra High Frequency, UHF), це діапазонами мікрохвиль (понад 300 МГц). При такій частоті сигнали вже не відображаються іоносферою Землі і для стійкого зв'язку потрібна наявність прямої видимості між передавачем і приймачем. Тому зазначені частоти використовуються в супутникових або радіорелейних каналах або в таких локальних або мобільних мережах, в яких ця умова виконується.

? Контрольні запитання:

1. Яку роль в коаксіальному кабелі грає обплетення з мідних дротів або алюмінієвої фольги?
2. До якої категорії відноситься кабель з неекранованої крученої пари, здатний передавати дані зі швидкістю до 10 Мбіт/с?
3. Передача електричного сигналу вимагає наявності двох провідників. Які саме провідники використовуються в коаксіальному кабелі? Навіщо у кабелі «кручена пара» використовується кілька пар провідників (2 або 4)?

4. Який роз’єм використовується для підключення кабелю «кручена пара» до комп’ютерів?

5. Основне завдання конекторів для металевих кабелів – забезпечити надійний електричний контакт при з’єднанні відрізків кабелю або пристроїв мережі. Яка основна задача конекторів для оптоволоконного кабелю?

6. Що може створити перешкоду для роботи бездротової мережі, якщо в ній використовується радіозв’язок? Що може створити перешкоду роботі бездротової мережі, заснованої на використанні інфрачервоного випромінювання?

✍Практичні завдання:

Завдання 1.

Для раніше розробленої мережі компанії, яка розвивається (див. запитання та завдання до попередньої теми) складіть проект прокладення коаксіального кабелю у кабельних каналах відповідно до обраної вами топології.

Завдання 2.

Заповніть таблицю 2.1, описавши типи кабелів, які використовуються у Packet Tracer для з’єднання відповідних інтерфейсів. Вкажіть який саме інтерфейс підтримує тип кабелю.

Таблиця 2.1 – Типи з’єднань у Packet Tracer

Тип кабелю	Опис
 Console	
 Copper Straight-through	
 Copper Cross-over	
 Fiber	
 Phone	
 Coaxial	
  Serial	

DCE and DTE	

Тести з теми «Лінії зв’язку»

1. Який тип розніму використовується для під’єднання кабелю UTP до вузла мережі?

A. RJ – 11
B.RJ – 45
C.RS – 232

2. Які типи кабелю доцільно використати для зовнішніх ліній зв’язку?

A.Оптоволокно
B.UTP
C. STP
D. Тонкий коаксіальний кабель
E.Товстий коаксіальний кабель

3. Який тип розніму використовується для під’єднання тонкого коаксіального кабелю до вузла мережі?

A. RG – 8
B. RJ – 11
C. RG – 58
D. BNC – T конектор

4. Назвіть типи оптичного кабелю:

A. Одномодовий
B. Середньомодовий
C. Багатомодовий
D. Високодисперсний

5. Скільки пар кабелю використовується для передачі даних у версії 100base – T4?

A. 1
B. 2
C. 4
D. 8

6. Яку роль виконує обплетення коаксіального кабелю?

A. Ніякий
B. Вона є екраном, що захищає внутрішню жилу від зовнішніх електромагнітних полів.
C. По ній передається електричний струм для живлення проміжних повторювачів

7. Яким чином поширюються промені світла в одномодовому оптичному волокні?

A. Уздовж оптичної осі волокна

B. Заломлюючись від стінок, уздовж оптичної осі волокна
D. Упоперек оптичної осі волокна

Тема 5. Комунікаційні пристрої

Ключові поняття: мережний адаптер, мост, комутатор, марштрутизатор, шлюз, віртуальна локальна мережа.

Після того як кабельна інфраструктура вже готова – у потрібних місцях прокладені кабелі, змонтовані розетки та панелі для підключення мережних пристроїв, виникає необхідність у виборі пристроїв, які дозволять об'єднати комп'ютери, сервери, ноутбуки та персональні комп'ютери у єдину мережу.

5.1 Мережний адаптер

Для взаємодії з мережею, комп'ютеру потрібен мережний адаптер (провідний чи безпровідний). Крім того, слід встановити драйвер мережного адаптера – спеціальне програмне забезпечення, що дозволяє операційній системі (ОС) працювати з цим пристроєм. Як правило, сучасна ОС сама розпізнає пристрій та встановлює для нього потрібний драйвер. Якщо ж цього не сталося (або з автоматично встановленим драйвером мережа не працює), то потрібно власноруч встановити драйвер, що входить у комплект поставки адаптера.

Мережний адаптер та драйвер працюють на фізичному рівні та підрівні управління доступом до середовища (MAC) моделі OSI, забезпечуючи взаємодію фізичного та мережного рівнів.

Відповідно, адаптер повинен мати потрібний роз'єм для підключення конектора (звичайно RJ-45), а також унікальна фізична (або «MAC») адреса, що використовується для однозначної ідентифікації комп'ютеру у даному сегменті мережі. Зазвичай ця адреса назначається виробником адаптера при виготовленні, однак деякі моделі адаптерів допускають зміну MAC-адреси власноруч, наприклад, через налаштування BIOS адаптера або за допомогою спеціальної програми.

Якщо на комп'ютері встановлений протокол TCP/IP, то MAC-адреси встановлених на цьому комп'ютері адаптерів можна легко визначити за допомогою цілого ряду утиліт: IPCONFIG, NBTSTAT, ROUTE PRINT, NETSTAT, NET CONFIG. Достатньо у командному рядку ввести команду [**Ошибка! Источник ссылки не найден.**]:

IPCONFIG /ALL

і у виданому на екран тексті звернути увагу на параметр «Фізична адреса».

В операційній системі Windows це зробити ще простіше – достатньо двічі клацнути мишею на значку підключення у вікні **Сетевые подключения**, у вікні стану адаптера, що відкрилося, вибрати вкладку **Поддержка** та на ній натиснути кнопку **Подробности.**

5.2 Пристрої зв’язку

Для з’єднання комп’ютерів у мережі використовуються різні типи мережних пристроїв. Їх детальний розгляд дозволить з’ясувати яке саме обладнання слід використовувати при проектуванні різних типів мереж, оскільки від правильного вибору пристрою зв’язку залежить не тільки якість та швидкість роботи мережі, але й можливості її подальшого розширення.

Для об’єднання мережею двох комп’ютерів достатньо мати в них сумісні мережні адаптери. При використанні найпоширенішої на сьогодні технології локальних мереж Ethernet достатньо кабель вставити у роз’єм RJ-45 мережних адаптерів. При організації бездротової передачі даних типу Wi-Fi треба переключити бездротові адаптери у спеціальний режим Ad-Hoc, який забезпечує пряму взаємодію комп’ютерів один з одним.

5.2.1 Мости та комутатори

Мости (bridge) та комутатори (switch) використовуються в мережах з метою усунення виникнення частих колізій. Навідміну від концентраторів вони вміють визначати MAC-адреси джерела та приймача сигналів, а також підтримувати таблицю відповідностей своїх портів та MAC–адреса, що використовуються в мережі. Таку таблицю міст (чи комутатор) формує одразу після підключення за наступним принципом – як тільки порт отримує відповідь від пристрою з певною фізичною адресою, у таблиці з’являється рядок відповідностей: «MAC-адреса ↔ порт».

Мости працюють на підрівні управління доступом до середовища (MAC) канального рівня моделі OSI. Отримавши кадр та визначивши адресу призначення, міст або комутатор транслює кадр тільки у той порт, з яким ця MAC-адреса зіставлена у таблиці відповідностей. Кадри, що передаються між комп’ютерами одного сегменту, комутатор отримує, але нікуди не транслює (рис.2.8).

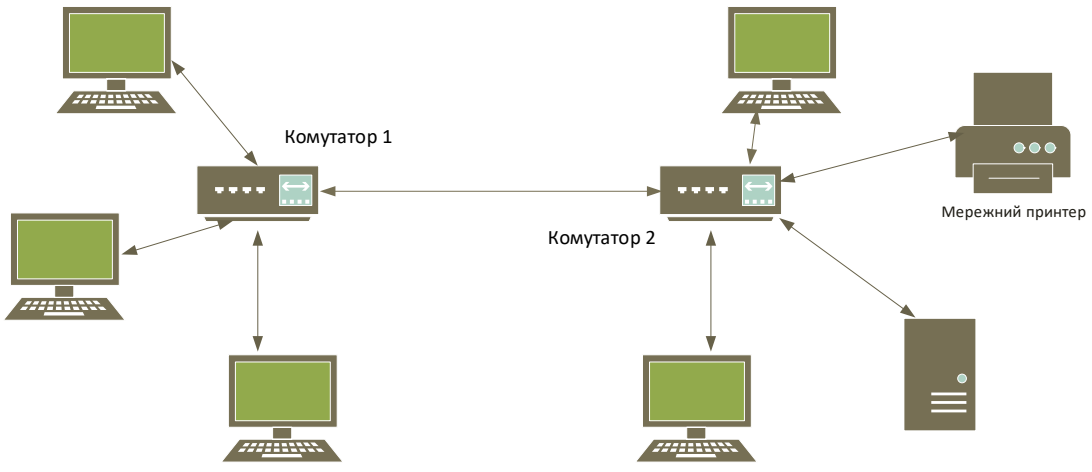


Рисунок 2.8 – Передача кадрів за допомогою комутаторів

Для ознайомлення з mac-адресами усіх вузлів мережі мости та комуттори посилають широкомовне повідомлення, призначене усім комп'ютерам локальної мережі.

Мости та комутатори відрізняються тим, що міст у кожен момент часу може передавати тільки один кадр, обслуговуючи передачу від одного комп'ютера до іншого (тому перші моделі мостів були двопортовими). Комутатор вміє вибудовувати велику кількість віртуальних каналів зв'язку між портами (тобто комутувати порти один з одним, звідси й назва пристрою), виробляючи паралельну обробку кадрів, що поступають з різних портів. Звісно, продуктивність мереж, побудованих на базі комутаторів, значно вище.

Сьогодні більшість локальних мереж будується саме на комутаторах.

5.2.2 Маршрутизатори та шлюзи

Маршрутизатори працюють на мережному рівні моделі OSI. На цьому рівні використовується логічна адресація в мережі, аналізується логічна структура мержі та визначається найкращий маршрут доставки пакету даних за призначенням. Звичайно, маршрутизатори працюють на більш низьких рівнях моделі OSI – як концентратори вони відновлюють рівень та форму сигналу, що передається, як мости та комутатори – дозволяють уникнути колізій. Однак маршрутизатори змінюють кадри Ethernet, що передаються, – точніше, «розбирають» їх до мережного рівня, а потім формують заново за певними правилами. За відсутністю певного налаштування маршрутизатори не передають в інші порти навіть широкомовні пакети і, таким чином, виступають у мережах межами областей зіткнень та широкомовлень.

Разом з програмами більш високого рівня моделі OSI, маршрутизатори вміють виконувати цілий ряд досить складних дій, наприклад виявляти проблеми у мережі та повідомляти про них, вести статистику отриманих та переданих даних, фільтрувати пакети, проводити авторизацію користувачів при виході в Інтернет тощо.

Потужні маршрутизатори є досить складними та дорогими програмно-апаратними комплексами, тому у деяких мережах вони замінюються комутаторами 3-го рівня – пристроями, що займають проміжну ступінь між комутаторами та маршрутизаторами. Від звичайних комутаторів вони відрізняються тим, що можуть виконувати найпростіші функції маршрутизації, залишаючись при цьому продуктивними та не дуже дорогими.

Також сучасні комутатори володіють можливістю будувати віртуальні локальні мережі (Virtual LAN), коли в один логічний сегмент мережі об'єднуються комп'ютери, фізично підключені до різних комутаторів (рис. 2.9). Критерії для такого об'єднання можуть бути різними, починаючи з MAC- або IP-адрес та завершуючи іменами комп'ютерів.

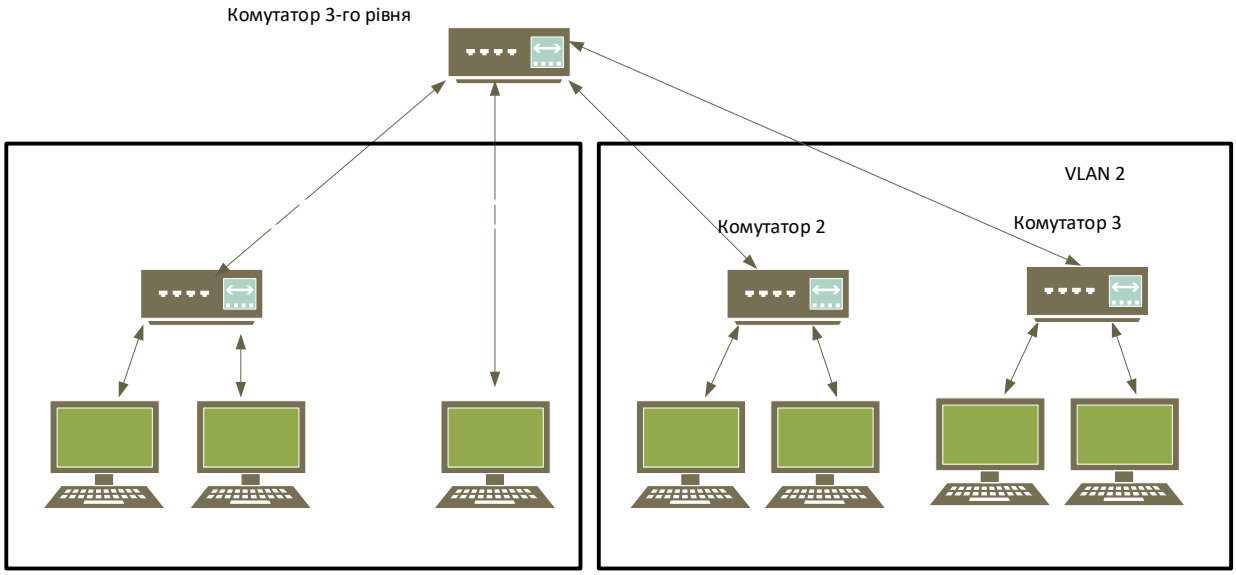


Рисунок 2.9 – Приклад формування локальної віртуальної мережі

Поняття «шлюз» визначає будь-який пристрій або програму, що дозволяє об’єднати різнорідні системи (наприклад, існують почтові шлюзи, що використовуються для зв’язку різних систем електронної пошти). Стосовно взаємодії у мережі, під шлюзом розуміють пристрій, що об’єднує різні мережні архітектури (наприклад, шлюз Ethernet з Token Ring). Важливо тут те, що шлюз повинен не тільки мати фізичні порти для підключення різнорідних систем, але й «розуміти» різні протоколи, виступаючи для них у ролі «перекладача».

Сформулюємо декілька рекомендацій, якими можна керуватися при виборі пристроїв зв’язку.

Найбільш поширеними пристроями зв’язку у мережах сьогодні є комутатори Fast та Gigabit Ethernet, а підключення бездротових пристроїв до локальної мережі здійснюється за допомогою шлюзів, що об’єднують функції комутаторів та точки бездротового доступу, що працюють за стандартом 802.11g.

Для домашніх та невеликих офісних мереж цілком підходять недорогі 8- або 16-портові комутатори Fast Ethernet, бажано з функцією управління портами. Якщо передача великих об’ємів даних не планується, можна зупинитися на бездротових точках доступу, хоча це мобільне рішення обійдеться дорожче та буде менш корисним.

У великих мережах основу повинні складати потужні та надійні комутатори Gigabit або 100Gigabit Ethernet, до яких підключаються комутатори підрозділів (будівель), а до них, у свою чергу, – комутатори поверхів (офісів). Розміщення точок доступу в них треба ретельно планувати, щоб користувач при переміщенні територією підприємства послідовно переключався з однієї точки доступу до іншої, зберігаючи зв’язок з локальною мережею.

Застосування маршрутизаторів слід там, де потрібно чітко контролювати потоки IP-пакетів у складній маршрутизованій мережі, а також забезпечувати резервні маршрути доставки пакетів, – наприклад, при взаємодії з віддаленим офісом чи Інтернетом.

При виборі мережного адаптеру для комп'ютера слід звернути увагу на можливість підтримки стандартів Ethernet або Wi-Fi. Краще за все обрати дещо більш дорогий, але сучасний мережний адаптер, наприклад Gigabit Ethernet або Wi-Fi стандарту 802.3g. Оскільки ці стандарти зворотно сумісні з попередніми, такі адаптери зможуть працювати зі старими концентраторами 10Base-T та точками доступу 802.11b, поки не будуть замінені вказані пристрої зв'язку.

❓Контрольні запитання:

1. Який пристрій забезпечує інтерфейс між комп'ютером та мережним кабелем?
2. Що розуміється під назвою «пристрій зв'язку»?
3. У чому схожість та відмінності між концентраторами та повторювачами?
4. У чому схожість та відмінність між мостами та комутаторами? Чим вони відрізняються від концентраторів?
5. Що таке маршрутизатор? Чи може він замінити концентратор, міст чи комутатор?
6. Для чого призначені шлюзи?
7. Що таке «точка бездротового доступу»? Для чого вона призначена?

✍Практичні завдання:

1. Заповнити таблицю охарактеризувавши основні мережні пристрої: мережний адаптер, модем, маршрутизатор, комутатор, повторювач, міст, шлюз, концентратор, ретрансляція та ін.

Таблиця 2.8 – Характеристика основних мережних пристроїв

№	**Назва мережного пристрою**	**Зовнішній вигляд (Рисунок)**	**Основні можливості**	**Особливості роботи**	**Різновиди**
1.	мережний адаптер				
2.	модем				
3.	маршрутизатор				
4.	комутатор				
5.	півторювач				
6.	міст				
7.	шлюз				
8.	концентратор				

2. Проаналізувати використання засобів зв'язку у комп’ютерній мережі Запорізького національного університету.

3. Спроектуйте (у вигляді приблизної структурної схеми) мережу крупної фірми, що складається з трьох підрозділів:

– склад (розташований окремо від офісу), оснащений 5 стаціонарними робочими станціями;

– торговий центр (ринок будматеріалів великої площі плюс автостоянки для покупців), персонал якого при роботі з клієнтами використовує мобільні пристрої, вільно переміщуючись по території торгового центру та стоянок на відстані до 1,5-2 км.

При цьому у межах офісу та складу підмережі повинні мати зіркоподібну структуру, для офісу адміністрації необхідно забезпечувати можливість виходу в Інтернет по каналу ADSL, а зв’язок між підрозділами фірми здійснюється за допомогою оптоволоконного кабелю. Вважати визначаючими параметри швидкості та надійності роботи мережі, нехтуючи її вартістю.

Тести з теми «Комунікаційні пристрої»

1. Оберіть зі списку облаштування DCE (апаратура передачі даних)

A. Модем
B. DSU/CSU (облаштування обслуговування даних/облаштування обслуговування каналу)
C. Мережний адаптер
D. Мультиплексор/демультиплексор

2. Оберіть зі списку проміжне устаткування ліній зв’язку :

A. Модем
B. Мультиплексор/демультиплексор
C. Комутатор
D. Підсилювач

3. До додаткових функцій концентраторів відносять:

A. Автосегментацію мережі
B. Мікросегментацію мережі
C. Підтримку резервних зв’язків
D. Корекцію помилок на рівні кадрів
E. Призначення дозволених MAC-адрес портам
F. Шифрування кадрів

4. Міст дозволяє міняти:

A. Фізичну структуру і логічну структуру мережі
B. Тільки фізичну структуру мережі
C. Тільки логічну структуру мережі

5. Мости можна сполучати між собою так, щоб утворювалися петлі

A.Так
B.Ні

6. У яких режимах може працювати мережний адаптер, сполучений з концентратором :

A. Напівдуплексному
B. Повнодуплексному
C. У обох режимах

7. Комутатор – це:

A. Пристрій для просування кадрів з одного сегменту мережі в інший
B. Пристрій для просування кадрів між декількома сегментами
C. Багатопортовий повторювач
D.Облаштування для об’єднання декількох сегментів мережі в один сегмент

8. Вкажіть основні елементи в структурі комутатора

_____
_____

9. Чому говорять, що комутатори і мости виконують логічну структуризацію мережі?

_____
_____

10. Призначення комутатора/моста полягає в:

A. Повторення кадру на усіх портах
B. Повторення кадру тільки на певних портах
C. Дозвіл колізій, що відбуваються в мережі
D. Об’єднання сегментів в один домен колізій
E. Розділення мережі на окремі домени колізій

11. Яким чином міст або комутатор в мережі Ethernet будує свою внутрішню адресну таблицю?

A. Таблиця створюється адміністратором мережі
B. Таблиця створюється шляхом пасивного прослуховування мережі
C. У мережах Ethernet мостів/комутатори не мають внутрішніх адресних таблиць

12. Чи Вірне твердження, що біля будь-якого моста швидкість просування меньша за швидкість фільтрації?

A. Так
B. Ні

Тема 6 Базові мережні архітектури локальних мереж

Ключові поняття: технології «останньої милі», Home PNA, Digital Subscribe Line, FTTx, базові технології локальних мереж, Ethernet, Fast Ethernet, Gigabit Ethrnet, метод доступу CSMA/CD, CSMA/CA, Wifi, WiMax, Bluetooth, покоління бездротових високошвидкісних мереж мобільного зв'язку (1G, 2G, 3G, 4G)

За багато років розвитку мережних технологій було розроблено багато різноманітних архітектур. Деякі з них вже вийшли з ужитку, тоді як інші, такі як Ethernet, не тільки активно використовуються досі, але і постійно вдосконалюються.

6.1 Технології локальних мереж Ethernet

Тепер перейдемо до вивчення найбільш популярних технологій, що використовуються у сучасних локальних мережах.

6.1.1 Fast Ethernet. Gigabit Ethernet

Ethernet [Ошибка! Источник ссылки не найден.**]** – це найбільш поширена технологія організації локальних мереж. Стандарти Ethernet описують реалізацію двох перших рівнів моделі OSI – кабельні з'єднання і електричні сигнали (фізичний рівень) та формати блоків даних і протоколи управління доступом до мережі (канальний рівень).

Назва Ethernet походить від двох англійських слів - ether (ефір) і net (мережа). Ethernet використовує концепцію загального ефіру. Кожен вузол посилає дані в цей ефір і вказує, кому вони адресовані. Дані можуть дійти до всіх вузлів мережі, але обробляє їх тільки той вузол, якому вони призначені. Ethernet було розроблено в 70-х роках XX століття в Xerox PARC (Xerox Palo Alto Research Center) – науково-дослідному центрі Xerox. Після доробки за участю компанії Intel та DEC архітектура Ethernet стала основою прийнятого у 1985 р. стандарту IEEE 802.3, що визначив для неї наступні параметри:

– топологія – «шина»;
– метод доступу – CSMA/CD;
– швидкість передачі – 10 Мбіт/с;
– середовище передачі – коаксіальний кабель;
– застосування термінаторів – обов'язкове;
– максимальна довжина сегменту мережі – до 500 м;
– максимальна довжина мережі – до 2,5 км;
– максимальна кількість комп'ютерів у сегменті – 100;
– максимальна кількість комп'ютерів у мережі – 1024.

У початковій версії Ethernet передбачалось використання коаксіального кабелю двох видів – «товстого» та «тонкого» (стандарти 10Base-5 та 10Base-2, відповідно). Однак на початку 90-х р. також з'явилися специфікації для

побудови мереж Ethernet з використанням крученої пари (10Base-T) та оптоволокна (10Base-FL). Пізніше, у 1995 р., був опублікований стандарт архітектури Fast Ethernet (IEEE 802.3u), що забезпечує передачу на швидкостях до 100 Мбіт/с, у 1998 р. – стандарт Gigabit Ethernet (IEEE 802.3z та 802.3ab), а у 2002 р. – стандарт 10 Gigabit Ethernet (IEEE 802.3ac).

Порівняння різних стандартів Ethernet наведено у табл. 2.11.

Таблиця 2.11 – Характеристики різних стандартів Ethernet [**Ошибка! Источник ссылки не найден.**]

Реалізація	**Швидкість передачі даних, Мбіт/с**	**Топологія**	**Середовище передачі**	**Максимальна довжина кабелю, м**
Ethernet				
10Base-5	10	«шина»	Товстий коаксіальний кабель	500
10Base-2	10	«шина»	Тонкий коаксіальний кабель	185; Реально – до 800
10Base-T	10	«зірка»	Кручена пара	100
10Base-FL	10	«зірка»	Оптоволокно	500 (станція-концентратор); 2000 (між концентраторами)
Fast Ethernet				
100Base-TX	100	«зірка»	Кручена пара категорії 5 (2 пари)	100
100Base-T4	100	«зірка»	Кручена пара категорії 3,4 або 5 (4 пари)	100
100Base-FX	100	«зірка»	Багатомодове або одномодове оптоволокно	2000 (багатомодовий); 15000 (одномодовий); Реально – до 40 км
Gigabit Ethernet				
1000Base-T	1000	«зірка»	Кручена пара категорії 5 або вище	100
1000Base-CX	1000	«зірка»	Спеціальний кабель типу STP	25
1000Base-SX	1000	«зірка»	Оптоволокно	225-550 (багатомодовий), в залежності від типу
1000Base-LX	1000	«зірка»	Оптоволокно	550 (багатомодовий); 5000 (одномодовий);

				Реально – до 80 км.

Продовження таблиці 2.11

10 Gigabit Ethernet				
10GBase-x (x – набір стандартів)	10000	«зірка»	Оптоволокно	800-40000 (в залежності від типу кабелю та довжини хвилі лазеру)

Застосування комутаторів замість концентраторів у сучасних мережах з архітектурою Ethernet та методом доступу до середовища CSMA/CD («багаторазовий доступ з контролем несучої та виявленням колізій») дозволяє «ізолювати» передачу даних між двома комп'ютерами у мережі від інших та практично виключає ситуацію виникнення зіткнення кадрів (колізії) у мережі.

Розглянемо переваги мережі за технологією Ethernet:

– простота у реалізації;

– Ethernet-пристрої (мережні адаптери, концентратори, комутатори тощо) виявляються значно дешевшими аналогічних пристроїв інших мережних архітектур;

– можна використовувати майже будь-які види кабелю, а використання оптоволокна дозволяє об'єднати ділянки мереж, які розміщені далеко одна від одної;

– сумісність різних варіантів Ethernet дуже велика, що дозволяє не тільки нарощувати потужності мережі з використанням кабельної інфраструктури, що існує, але й легко розширювати мережу, підключаючи до неї нові, більш швидкісні сегменти.

6.2 Бездротові мережі

Найпоширенішими архітектурами бездротових локальних мережах є технології Wi-Fi та Bluetooth.

6.2.1 Технологія Wi-Fi

Wi-Fi (скорочення від «Wireless Fidelity», «бездротова точність») – популярна у світі технологія, яка забезпечує бездротове підключення мобільних пристроїв до локальної мережі Інтернет (рис 2.11).

Під іменем «Wi-Fi» на справді приховується декілька стандартів, розроблених для бездротових мереж на основі випущеної ще у 1997 р. специфікації IEEE 802.11 (табл. 2.12).

Важливо помітити, що у стандарті 802.11 передбачається використання тільки напівдуплексних передачів, які не можуть одночасно передавати та приймати інформацію. Через це у бездротових мережах 802.11 станція загалом не може виявити зіткнення під час передачі (оскільки в цей час не має можливості приймати дані). Тому у якості методу доступу до середовища у всіх стандартах використовується метод CSMA/CA (із запобіганням колізій), що дозволяє уникати зіткнень. Це призводить до додаткових складнощів при

взаємодії і, як наслідок, до суттєво менших швидкостей передачі даних, ніж, наприклад, у технології Ethernet.

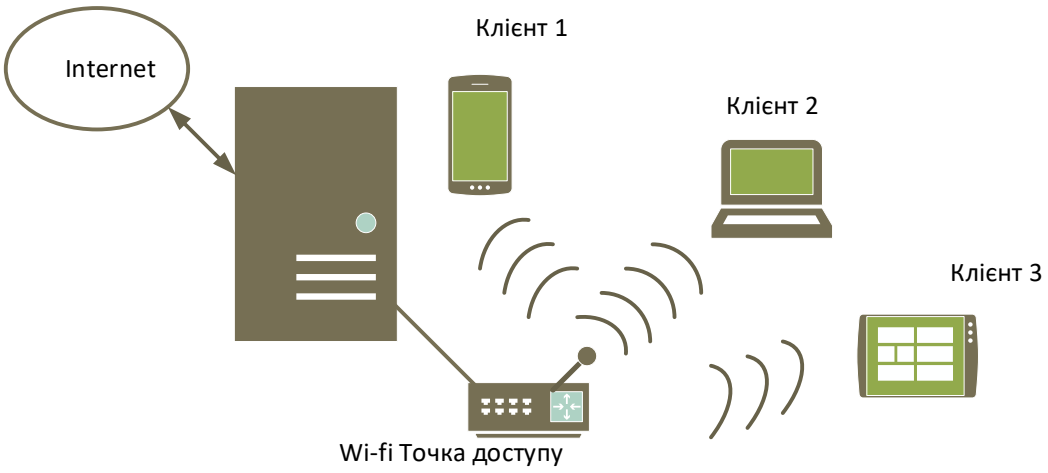


Рисунок 2.10 Бездротові мережі

Таблиця 2.12 – Найбільш важливі стандарти IEEE 802.11x [**Ошибка! Источник ссылки не найден.**]

Стандарт	**Середовище передачі**	**Швидкість передачі, Мбіт/с**	**Примітка**
802.11	Радіосигнал з частотою біля 2,4 ГГц або ІК-сигнал	1 або 2	Базовий стандарт, що визначає взаємодію на фізичному та канальному рівнях моделі OSI
802.11a	Радіосигнал з частотою біля 5 ГГц	До 54	Несумісний на фізичному рівні зі стандартами 802.11b та g;
802.11b	Радіосигнал з частотою 2,4-2,483 ГГц	До 11	Має відносно низьку швидкість та захищеність (захист шифруванням за технологією WEP – Wireless Equivalent Privacy). Забезпечує трохи більшу, у порівнянні з іншими стандартами, дальність передачі даних.

Продовження таблиці 2.12

802.11g	Радіосигнал з частотою 2,4-2,483 ГГц	До 54	Забезпечує сумісність із стандартом 802.11b, але не характеризується більшою швидкістю та захищеністю (окрім WEP, підтримується стандарт захисту WPA – Wi-Fi Protected Access)
802.11n	Радіосигнал з частотою 2,4—2,5 або 5,0 ГГц	До 300	Для досягнення планки 300 Мбіт/с знадобилося використання нової технології передачі даних, якою стала технологія з множинним введенням/виводом (Multiple Input Multiple Output, MIMO). Вона полягає у паралельній передачі даних по різних каналах з застосуванням багатоканальних антенних систем.

Основним недоліком мереж Wi-Fi на сьогодні є досить мала дальність передачі даних, яка не перевищує для більшості пристроїв 150 м (максимум 300 м) на відкритому просторі або усього декількох десятків метрів – у приміщенні.

Рішенням зазначеної проблеми може стати архітектура **WiMAX** (Worldwide Interoperability for Microwave Access), що розробляється у рамках робочої групи IEEE 802.16. Реалізація цієї технології, що також використовує радіосигнали у якості середи передачі, дозволить надати користувачам швидкісний бездротовий доступ на відстанях до декількох десятків кілометрів (рис. 2.11).

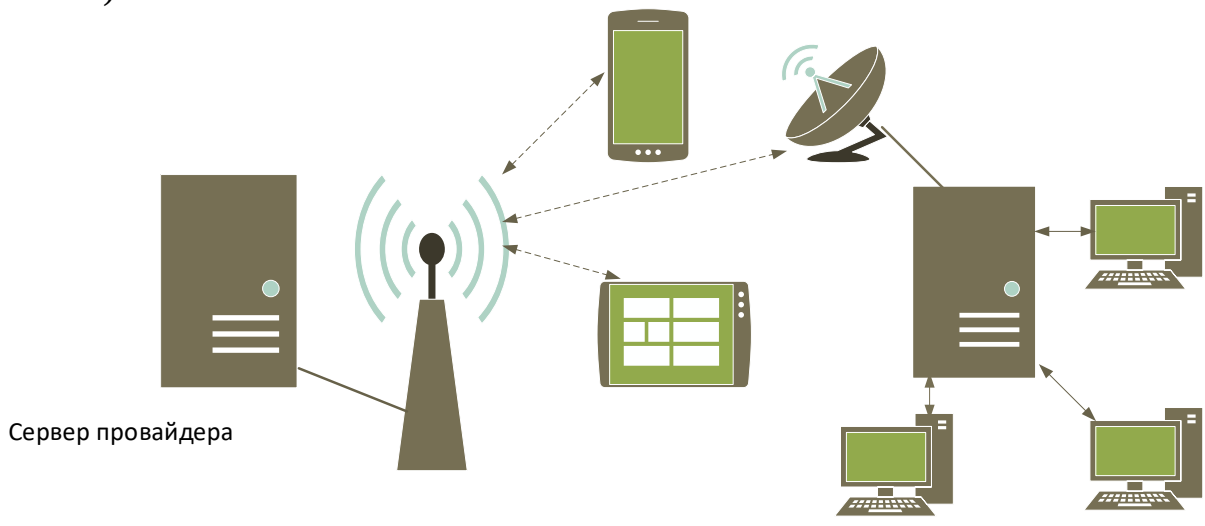


Рисунок 2.11 – Архітектура WiMAX

6.2.2 Технологія Bluetooth

Нарешті, треба пригадати ще про одну з популярних бездротових технологій архітектур – про **технологію Bluetooth** (стандарт IEEE 802.15.1) [**Ошибка! Источник ссылки не найден.**], а також про зовсім нову **технологію ZigBee**.

✎ **Wireless USB – альтернатива Bluetooth: т**ехнологія Wireless USB заснована на використанні нового стандарту бездротового зв'язку – UWB та забезпечує супершвидкісну (до 480 Мбіт/с, а у перспективі – і до 1Гбіт/с) передачу даних на короткі відстані (до 10 км). Вона дозволяє реалізувати бездротове підключення периферійних пристроїв, аналогічних USB 2.0. Перший серійний зразок адаптеру Wireless USB був представлений на Форумі Intel для розробників (IDF-2005).

Як і в Wi-Fi, в Bluetooth використовується радіосигнал з частотою 2,4 ГГц, однак ці стандарти між собою не сумісні. Bluetooth характеризується досить низьким електроспоживанням, що дозволяє з успіхом застосовувати цю технологію у переносних пристроях – ноутбуках, мобільних телефонах (рис. 2.12). До того ж Bluetooth практично не потребує налаштувань – цей стандарт дозволяє пристроям встановлювати взаємодію при мінімальній участі користувача. З іншого боку, у Bluetooth досить низькі показники дальності передачі та пропускної спроможності – не більше 10 метрів та 400-700 Кбіт/с, – що різко обмежує можливості використання технології у локальних мережах.

У технології ZigBee, що з'явилася недавно завдяки зусиллям декількох крупних комунікаційних компаній (стандарт 802.15.4), показники ще «скромніші» – її специфікація передбачає захищену передачу даних у радіусі 10-75 метрів та з максимальною швидкістю до 250 Кбіт/с. Здавалося б, нащо вона потрібна, якщо швидкість передачі у ній ще нижча, ніж для Bluetooth. Однак «родзинкою» пристроїв ZigBee є їх наднизьке електроспоживання та спроможність переходити у «сплячий режим», коли передача даних не потрібна. Тому основною сферою використання ZigBee-пристроїв стануть не локальні мережі, а системи моніторингу та контролю апаратури, у тому числі мережного обладнання.

Основною технологією, що використовується сьогодні у дротових мережах, є Ethernet. Важливо лише визначити конкретний стандарт або набір стандартів, яка використовуються у мережі, та закупити потрібне обладнання. При цьому рекомендації досить прості: намагайтеся обрати найбільш швидкісне та надійне обладнання, що задовольняє вас за ціною. Бажано, щоб це обладнання було максимально функціональним та керованим, однак ці критерії більш значущі для мережних адміністраторів крупних корпоративних мереж.

Для підключення бездротових клієнтів треба зупинитися не технології Wi-Fi, причому обирати треба пристрої, що підтримують стандарт 802.11g, – тільки у ньому забезпечується достатня швидкість передачі даних і, найголовніше, їх надійний захист.

6.2.3 Технологія Mesh Wi–Fi

Mesh мережа [**Ошибка! Источник ссылки не найден.**] – це розподілена, однорангова, комірчаста мережа. Повноцінна Mesh Wi–Fi мережа це така мережа, для підключення до якої не потрібно ніякого додаткового програмного забезпечення окрім DHCP- клієнта.

Об’єднання мереж відбувається в автоматичному режимі – коли пристрій підключений одночасно до двох мереж, вузол який підключений до цих двох мереж стає мостом, який їх об’єднує

Стандартне налаштування мережі не дозволяє виходити в звичайний Інтернет.

Ця технологія вирішує наступні проблеми:

1. Дозволяє бути незалежними від провайдерів
2. Можна самостійно побудувати мережу з Wi-Fi роутерами і маршрутизацією.
3. Для підключення до мережі не треба виконувати ніяких складних дій (за умови, якщо мережа самонастроювана)
4. Кожен новий клієнт, який підключився до мережі, збільшує місткість мережі.
5. Якщо сталося стихійне лихо, то за допомогою Mesh мережі можна швидко побудувати мережу на місці події для зв’язку, за підтримки із зовні – з’єднати її з глобальною мережею.

Достоїнства Mesh мереж:

1. Незалежність від провайдера, режиму, влади
2. При стихійних лихах дозволяє мати мережу на місці події, хоча можливо і відрізану від глобальної частини
3. Деякі сучасні протоколи для будівництва Mesh мереж гарантують шифрування усього трафіку того, що проходить через мережу (CJDNS)
4. Динамічна, маршрутизація, що автоматично конфігурується
5. Можливість об’єднувати mesh мережі через звичайний Інтернет (CJDNS)

Недоліки Mesh мереж:

1. Первинний запуск Mesh мережі дуже складний
2. Ефективна робота досягається коли в мережі багато учасників
3. Негарантована ширина каналу
4. Негарантована якість зв’язку

На сьогодні найпопулярніші протоколи для організації Wi–Fi Mesh мереж це:

– CJDNS
– B.A.T.M.A.N.
– DTN
– Netsukuku
– OSPF

Авто-призначення адреси – клієнт сам вибирає собі адресу і може не міняти її, переходячи з однієї під мережі в іншу, немає єдиного центру видачі адрес.

6.2.4 Покоління бездротових високошвидкісних мереж мобільного зв'язку (1G, 2G, 3G, 4G)

Символ «G» означає «покоління», наприклад, «мережа 4G», означає безпровідну мережу, побудовану на основі технології четвертого покоління [**Ошибка! Источник ссылки не найден.**].

1G – перше покоління безпровідних телефонних технологій і мобільних телекомунікацій. Це аналогові телекомунікаційні стандарти, які були введені в 1980-х, і на початку 90-х були витіснені досконалішою цифровою технологією 2G. Основною відмінністю між системам 1G і 2G є те, що мережі 1G використовують аналогову модуляцію радіосигналів, тоді як в мережі 2G є цифровими, що дозволяло шифрувати розмови і посилати СМС.

Першим стандартом 1G став NMT (Nordic Mobile Telephone), використовуваний в країнах Північної Європи, Швейцарії, Нідерландах, Східній Європі і Росії. Інші стандарти включають AMPS (Advanced Mobile Phone System), застосовують в Північній Америці і Австралії, TACS (Total Access Communications System) у Великобританії, C-450 в Західній Німеччині, Португалії і Південній Африці, Radiocom 2000 у Франції і RtMI в Італії. У Японії було декілька систем. NTT розробила три стандарти (TZ – 801, TZ – 802 і TZ – 803), тоді як конкуруюча система під управлінням DDI використала стандарт JTACS (Japan Total Access Communications System).

У 1G мережах фактична швидкість завантаження складала від 2,9 Кбайт/з до 5,6 Кбайт/с. Попередником 1G технологій являється рухливий радіотелефонний зв'язок (чи стандарт «нульового покоління» 0G).

2G – друге покоління безпровідної телефонної технології.

Було запущено в комерційну експлуатацію за стандартом GSM у Фінляндії компанією Radiolinja (зараз є частиною Elisa Oyj) в 1991. Трьома основними перевагами мереж 2G в порівнянні з попередниками було те, що телефонні розмови були зашифровані за допомогою цифрового шифрування; система 2G була значно ефективнішою; представила послуги передачі даних, починаючи з текстових повідомлень СМС.

Технологія 2G дозволила різним мобільним мережам надавати послуги, такі, як текстові з'єднання, з'єднання із зображеннями і ММС (мультимедійні повідомлення). Технологія 2G досить безпечна як для відправника, так і для одержувача. Цифрове шифрування передає дані таким чином, що тільки той приймач, якому вони призначені, може отримати їх і прочитати.

Після того, як технологія 2G була запущена, попередня технологія була названа 1G. Тоді як радіосигнали мережі 1G є аналоговими, радіосигнали в мережах 2G є цифровими. Обидві системи використовують цифрові сигнали для підключення до базової станції стільникового зв'язку (які прослуховують телефони) до іншої частини телефонної системи. 2G була замінена на нові

технології, такі, як 2.50G, 2.750G, 3.6G, і 4.20G; проте, мережа 2G досі використовується у багатьох частинах світу.

Технологія 2G може бути розділена на TDMA (заснована на тимчасовому розділенні доступу) і CDMA (заснована на кодовому розділенні каналів) залежно від використовуваного типу мультиплексування. Основними стандартами 2g являються:

– GSM (на основі TDMA), родом з Європи, але використовується практично в усіх країнах світу на усіх шести континентах. На сьогодні на цей стандарт доводиться близько 80% усіх абонентів у світі. Більше 60 операторів GSM також використовують CDMA2000 в діапазоні 450 Мгц (CDMA450);

– IS – 95, він же CDMAOne (на основі CDMA, в США називають зазвичай просто CDMA), використовується в Північній і Південній Америці і деяких частинах Азії. На сьогодні на цей стандарт доводиться близько 17 % усіх абонентів по всьому світу. Більше десятка CDMA операторів перейшли на GSM, включаючи операторів Мексики, Індії, Австралії і Південної Кореї;

– PDC (заснований на TDMA), використовується виключно в Японії;

– iDEN (заснований на TDMA), власна мережа, яка використовується компанією Nextel в США і компанією Telus Mobility в Канаді;

– IS – 136, він же D – AMPS (заснований на TDMA, в США – зазвичай просто TDMA), був колись поширений в Північній і Південній Америці, але у більшості мігрував в GSM.

Використання цифрових сигналів між гарнітурами і базовими станціями зв’язку збільшує пропускну спроможність системи в двох ключових напрямах:

– цифрові голосові дані можуть бути стислі і мультиплексовані набагато ефективніше, ніж аналогове кодування голосу за рахунок використання різних кодеків, що дозволяє передавати більшу кількість дзвінків в одній смузі радіочастот;

– цифрові системи були розроблені, щоб мобільні телефони мали менше радіовипромінювання. Це стало можливим завдяки базовим станціям стільникового зв’язку і тому, що відповідне устаткування стало дешевше.

3G (від англ. third generation – третє покоління), технології мобільного зв’язку 3 покоління – набір послуг, який об’єднує як високошвидкісний мобільний доступ з послугами мережі Інтернет, так і технологію радіозв’язку, який створює канал передачі даних. Під цим терміном найчастіше мається на увазі технологія UMTS з надбудовою HSPA.

Мобільний зв’язок третього покоління будується на основі пакетної передачі даних. Мережі третього покоління 3G працюють на межі дециметрового і сантиметрового діапазону, як правило, в діапазоні близько 2 ГГц, передаючи дані зі швидкістю до 3,6 Мбіт/с. Вони дозволяють організовувати відеотелефонний зв’язок, дивитися на мобільному телефоні фільми і різний контент.

3G включає 5 стандартів сімейства IMT – 2000 (UMTS/WCDMA, CDMA2000/IMT – MC, TD – CDMA/TD – SCDMA (власний стандарт Китаю), DECT і UWC – 136).

Найбільше поширення у світі отримали два стандарти: UMTS (чи W – CDMA) і CDMA2000 (IMT – MC), в основі яких лежить одна і та ж технологія – CDMA (Code Division Multiple Access – множинний доступ з кодовим розділенням каналів).

Технологія CDMA2000 забезпечує еволюційний перехід від вузькосмугових систем з кодовим розділенням каналів IS – 95 (американський стандарт цифрового стільникового зв'язку другого покоління) до систем CDMA «третього покоління» і отримала найбільше поширення на Північноамериканському континенті, а також в країнах Азіатсько-тихоокеанського регіону.

Технологія UMTS (Universal Mobile Telecommunications System – універсальна система мобільного електрозв'язку) розроблена для модернізації мереж GSM (європейського стандарту стільникового зв'язку другого покоління), і отримала широке поширення не лише в Європі, але і у багатьох інших регіонах світу.

Робота за стандартизацією UMTS координується міжнародною групою 3GPP (Third Generation Partnership Project), а за стандартизацією CDMA2000 – міжнародною групою 3GPP2 (Third Generation Partnership Project 2), створеними і такими, що співіснують у рамках ITU.

У мережах 3G забезпечується надання двох базових послуг : передача даних і передача голосу. Згідно з регламентами ITU (InterNATional Telecommunications Union – Міжнародний Союз Електрозв'язку) мережі 3G повинні підтримувати наступні швидкості передачі даних :

– для абонентів з високою мобільністю (до 120 км/год) – не більше 144 Кбіт/з;

– для абонентів з низькою мобільністю (до 3 км/год) – 384 Кбіт;

– для нерухомих об'єктів – 2048 Кбіт/с.

У мережах з кодовим розділенням каналів, у тому числі і 3G, є важлива перевага – поліпшений захист від обривів зв'язку в процесі руху, за рахунок використання так званого «м'якого хендовера». По мірі видалення від однієї базової станції клієнта «підхоплює» інша. Вона починає передавати все більше і більше інформації, тоді як перша станція передає усе менше і менше, поки клієнт взагалі не покине її зону обслуговування. При хорошому покритті мережі вірогідність обриву повністю виключається системою подібних " підхоплень".

4G (від англ. fourth generation – четверте покоління) – покоління мобільного зв'язку з підвищеними вимогами. До четвертого покоління прийнято відносити перспективні технології, що дозволяють здійснювати передачу даних зі швидкістю, що перевищує 100 Мбіт/с, – рухливим і 1 Гбіт/с – стаціонарним абонентам.

Передові міжнародні мобільні телекомунікаційні системи (IMT – Advanced), визначені сектором радіозв'язку MCE, повинні відповідати деяким вимогам, щоб вважатися мережами покоління 4G:

– ґрунтуються на комутації пакетів, використовуючи протоколи IP;

– пікові швидкості передачі даних від 100 Мбіт/с для користувачів з високою мобільністю (від 10 км/год до 120 км/год) і від 1 Гбіт/с для користувачів з низькою мобільністю (до 10 км/год);

– використовуються мережні ресурси, що динамічно розділяються, для підтримки більшої кількості одночасних підключень до однієї соте;

– їх масштабована смуга частот каналу 40 Мгц;

– мінімальні значення для пікової спектральної ефективності 15 біт/с/Гц в низхідному каналі і 6,75 біт/с/Гц у висхідному каналі (мається на увазі, що швидкість передачі інформації 1 Гбіт/с в низхідному каналі має бути можлива при смузі пропускання радіоканалу менше 67 Мгц);

– спектральна ефективність на сектор в низхідному каналі від 1,1 до 3 біт/с/Гц/сектор і у висхідному каналі від 0,7 до 2,25 біт/с/Гц/сектор;

– плавний хендовер через різні мережі;

– висока якість мобільних послуг.

Технології LTE Advanced (LTE – A) і WiMAX 2 (WMAN – Advanced, IEEE 802.16m) (сим-карта не потрібно) були офіційно визнані безпровідними стандартами зв’язку четвертого покоління 4G (IMT – Advanced) Міжнародним союзом електрозв’язку на конференції в Женеві в 2012 році

LTE (буквально з англ. Long – Term Evolution – довготривалий розвиток, часто позначається як 4G LTE) – стандарт безпровідної високошвидкісної передачі даних для мобільних телефонів і інших терміналів, працюючих з даними. Він ґрунтований на GSM/EDGE і UMTS/HSPA мережних технологіях, збільшуючи пропускну спроможність і швидкість за рахунок використання іншого радіоінтерфейсу разом з поліпшенням ядра мережі стандарт був розроблений 3GPP і визначений в серії документів Release 8, з незначними поліпшеннями, описаними в Release 9.

LTE є природним оновленням як для операторів з мережею GSM/UMTS, так і для операторів з мережею CDMA2000. У різних країнах використовуються різні частоти і смуги для LTE, що робить можливим підключати до LTE мереж по всьому світу тільки багатодіапазонні телефони.

Хоча маркування 4G використовується мобільними операторами і виробниками телефонів, LTE (як вказано в серії документів консорціуму 3GPP Release 8 і Release 9) не задовольняє технічним вимогам, які консорціум 3GPP прийняв для нового покоління мобільного зв’язку, а також вимогам, які були спочатку встановлені Міжнародним союзом електрозв’язку (у специфікації IMT Advanced).

LTE є стандартом безпровідної передачі даних і розвитком стандартів GSM/UMTS. Метою LTE було збільшення пропускної спроможності і швидкості з використанням нового методу цифрової обробки сигналів і модуляції, які були розроблені на рубежі тисячоліть. Ще однією метою було реконструювати і спростити архітектуру мереж, ґрунтованих на IP, значно зменшивши затримки при передачі даних в порівнянні з архітектурою 3G мереж. Безпровідною інтерфейс LTE є несумісним з 2G і 3G, тому він повинен працювати на окремій частоті.

Специфікація LTE дозволяє забезпечити швидкість завантаження до 326,4 Мбіт/с, швидкість віддачі до 172,8 Мбіт/с, а затримка в передачі даних може бути понижена до 5 мілісекунд. LTE підтримує смуги пропускання частот від 1,4 Мгц до 20 Мгц і підтримує як частотне розділення каналів (FDD), так і тимчасове розділення (TDD).

Радіус дії базової станції LTE залежить від потужності випромінювання і теоретично не обмежений, а максимальна швидкість передачі даних залежить від радіочастоти і віддаленості від базової станції. Теоретична межа для швидкості в 1 Мбіт/сікла – від 3,2 км (2600 Мгц) до 19,7 км (450 Мгц).

Велика частина стандарту LTE розглядає модернізацію 3g UMTS на те, що зрештою буде технологією 4g. Велика частина роботи спрямована на спрощення архітектури системи : вона переходить з існуючих UMTS ланцюги + комутації пакетів об'єднаної мережі до єдиної IP-інфраструктури (all – IP). E – UTRA є безпровідним інтерфейсом LTE. Його основні особливості:

– максимальна швидкість завантаження з мережі до 299,6 Мбіт/с і максимальна швидкість завантаження в мережу від абонента до 75,4 Мбіт/с залежно від категорії устаткування;

– низька затримка при передачі даних (5 мс затримка для маленьких IP пакетів в оптимальних умовах), нижча затримка при установці з'єднання;

– OFDMA для вхідної лінії зв'язку, SC – FDMA для вихідної лінії зв'язку з метою економії енергії.

– підтримка і FDD і TDD систем зв'язку, а також напівдуплексною FDD з однією і тією ж технологією радіодоступу;

– підвищення гнучкості. Спектр: 1,4 МГц, 3 Мгц, 5 МГц, 10 МГц, 15 МГц і 20 МГц для ширини стільники стандартизовані;

– підтримка співіснування із старими стандартами (наприклад, GSM/EDGE, UMTS і CDMA2000). Користувачі можуть почати виклик або передачу даних в області з наявністю LTE і, покинувши область покриття, продовжити роботу без яких-небудь спеціальних дій з його боку в мережах GSM/GPRS;

– радіоінтерфейс комутації пакетів.

? Контрольні запитання:

1. Які ви знаєте мережні архітектури? Які їх переваги та недоліки?
2. Чому архітектура Ethernet сьогодні отримала найбільше розповсюдження?
3. Які ви знаєте різновиди архітектури Ethernet? Чим вони відрізняються?
4. Які ви знаєте бездротові мережні технології?
5. Які мережні технології, на ваш погляд, краще за все використовувати:

– при створенні локальної мережі у крупному офісі;

– при розгортанні домашньої мережі у міській квартирі (з телефоном);

– при розгортанні домашньої мережі у сільському домі (не телефонізованому);

– при об’єднанні у мережу мобільних комп’ютерів (КПК) на території торгового центру чи складу;

– при організації систем збору даних у польових умовах на території селищ у сільській місцині?

✍Практичні завдання:

Завдання 1.

1. У Packet Tracer створити топологію локальної мережі, зображеної на рис.2.13.

2. Для приватної (зліва від маршрутизатора) та публічної (справа від маршрутизатора) підмереж визначити номер мережі.

3. Налаштувати DHCP-сервер вказавши пул від номера вузла, вказаного у варіанті, до максимально можливої адреси мережі, шлюз та адресу сервера DNS (адреса DNS-server з публічної мережі).

4. Присвоїти невикористані у пулі DHCP адреси серверам та інтерфейсам маршрутизатора власноруч.

5. Налаштувати робочі станції мережі для автоматичного отримання IP- адреси.

6. Протестувати взаємний зв’язок між хостами приватної та публічної підмереж.

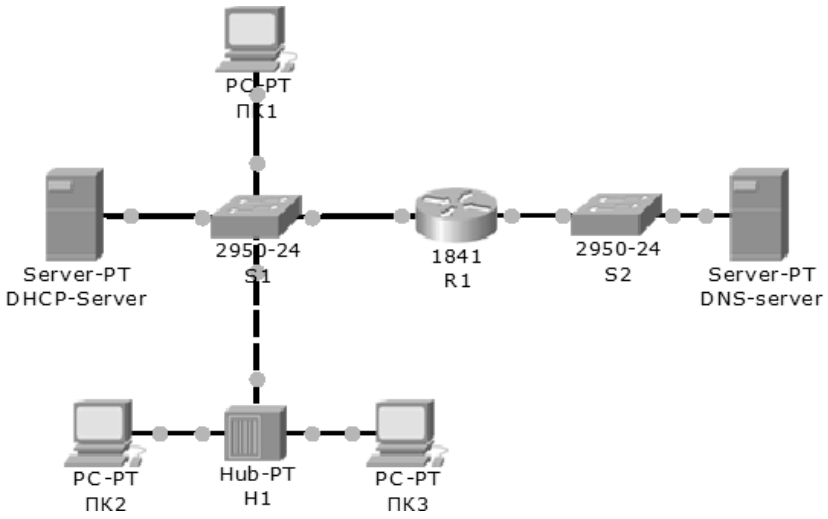


Рисунок 2.12 – Топологія мережі

Завдання 2.

1. У Packet Tracer створити мережну топологію, представлену на рис.2.14.

2. Використовуючи графічний інтерфейс користувача бездротового маршрутизатора, виконати наступні налаштування:

– призначити IP-адресу у локальній мережі 192.168.X.1 (X – тут і надалі номер студента у журналі академічної групи);

– встановити логін та пароль доступу до веб-інтерфейсу admin/admin;

– змінити SSID за замовченням на «LAB_9_X»;

– налаштувати параметри аутентифікації у бездротовій мережі, обравши тип аутентифікації WPA2-personal, шифрування AES та ключ «111111111»;

– увімкнути сервер DHCP та призначити необхідні параметри для його роботи (шлюз, сервер DNS, стартову адресу);

– для порта «Internet» обрати автоматичне отримання IP-адреси.

3. Сервер DHCP_WEB налаштувати за наступними вимогами:

– встановити статичну адресу мережного адаптера 150.1.X.1/24;

– увімкнути сервер DHCP для видачі IP-адрес глобальної мережі 150.1.X.100/24 – 150.1.X.256/24, шлюза та DNS 150.1.X.1;

– увімкнути сервер DNS та додати запис «webserver – 150.1.X.1» типу «A-record»;

– увімкнути HTTP-сервер.

4. Підключити та налагодити роботу бездротових клієнтів.

5. Перевірити працездатність мережних ресурсів (перехресне тестування з'єднання, доступ до серверів DHCP, DNS, HTTP).

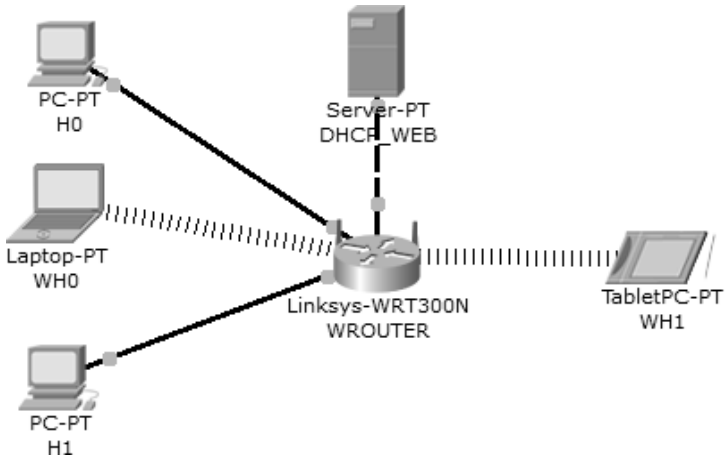


Рисунок 2.13 – Топологія мережі

Тести з теми «Базові мережні архітектури»

1. Як називається метод доступу, вживаних в мережах Ethernet?

A. Маркерний
B. CSMA/CD
C. Пріоритетний

2. Максимальна кількість вузлів в мережі Ethernet :

A. 1000
B. 1024
C. необмежено

3. Вкажіть загальну довжину мережі в Ethernet 10base-5 :

A. 5*185 м = 925 м
B. 5*500 м = 2500 м
C. 3*185 м = 555 м

4. Перерахуйте стандарти фізичного рівня для мереж Ethernet 100 Мбіт/с (Fast Ethernet)

_____

_____

5.Технологія Gigabit Ethernet працює в повнодуплексному режимі:

A. так, на кабелях UTP cat.5
B. так, на оптоволокні
C. так, на коаксіальному кабелі
D. ні

6. Максимальна довжина пакету даних в кадрі Gigabit Ethernet складає:

A. 4096 біт
B. 512 біт
C. 46 біт

7. Технологія Fast Ethernet може працювати в повнодуплексному режимі:

A. так, згідно із стандартом 100base – TX/FX
B. так, згідно із стандартом 100base – T4
C. ні

8. Стандарт Ethernet 10Мбит/з називається:

A. 802.3
B. 802.3z
C. 802.2
D. 802.3ab

9.Яка технологія сімейства xDSL використовує метод розділення смуги пропускання мідної телефонної лінії на декілька частотних смуг?

A. HDSL.
B. ADSL.
C. IDSL.
D. SDSL.
E. VDSL.

Які з перелічених технологій xDSL є симетричними?

A. HDSL.
B. ADSL.
C. IDSL.
D. SDSL.
E. VDSL.

РОЗДІЛ 3 ТЕХНОЛОГІЇ ПЕРЕДАВАННЯ ДАНИХ У ГЛОБАЛЬНИХ МЕРЕЖАХ

Тема 7 Мережний рівень. IP-адресація

Ключові поняття: IP-адреса, масштабованість, мережний рівень, підмережа, маска підмережі, класова адресація, IP-протокол

7.1 Призначення мережного рівня моделі OSI

Мережний рівень потрібен для створення великої складної мережі на основі окремих мереж, кожна з яких побудована за різними технологіями. Це можуть бути технології Ethernet, Wi-Fi, мережі мобільного зв'язку різних поколінь, мультисервісні мережі MPLS.

Ідея створення окремого мережного рівня для об'єднання мереж, побудованих на основі різних технологій канального рівня, була вперше запропонована Вінтоном Серфом і Робертом Каном у 1974 році. За цю ідею вони отримали премію Тьюринга — еквівалент Нобелівської премії в інформаційних технологіях і комп'ютерних науках. Оскільки мережний рівень широко використовується в Інтернеті і фактично є основою Інтернету, Вінтон Серф і Роберт Кан отримали звання «батьків Інтернету».

Але перед тим, як розглядати мережний рівень, розберемось навіщо він потрібний, адже на канальному рівні мережне обладнання вже вміє передавати дані різними способами: через дротові технології, як Ethernet, або бездротові, як Wi-Fi. Колись існувало багато інших технологій. Проте, якщо потреба у побудові мережі, яка охоплює весь світ, із використанням лише технологій канального рівня, виникає низка проблем.

Основними з них є:

1. Відмінності між технологіями канального рівня, що ускладнює їхнє об'єднання.
2. Обмеження масштабованості технологій канального рівня, які добре підходять для локальних мереж, але не для глобальних.

Технології канального рівня відрізняються за:

- **Рівнем сервісу.** В Інтернеті використовується сервіс без гарантії доставки. У Wi-Fi є гарантія доставки: відправник чекає підтвердження прийому кадру і повторно передає його за відсутності підтвердження.
- **Типом адресації.** Ethernet і Wi-Fi використовують MAC-адреси, стільникові мережі — IMEI-адреси, а інші технології можуть мати свої типи адресації.
- **Максимальним розміром кадру.** Наприклад, Ethernet підтримує кадри до 1500 байтів, Wi-Fi — до 2304 байтів.

На мережному рівні вводяться глобальні адреси, що не залежать від локальних адрес канального рівня. Для визначення локальної адреси за глобальною використовується протокол ARP.

Щоб вирішити проблему максимального розміру пакету, на мережному рівні використовується фрагментація. Якщо дані перевищують максимальний розмір кадру в певній мережі, вони розбиваються на фрагменти, які передаються окремо. На кінцевих пристроях ці фрагменти знову збираються в єдиний пакет.

Технології Ethernet і Wi-Fi, хоч і схожі, не можуть забезпечити глобальну масштабованість через такі обмеження:

- **Таблиці комутації.** У комутаторах Ethernet таблиці зберігають MAC-адреси всіх пристроїв мережі. Для глобальних мереж із мільярдами пристроїв це неможливо.
- **Відсутність дублюючих шляхів.** Протокол STP (Spanning Tree Protocol) забезпечує уникнення утворення кілець у мережі, але обмежує кількість активних з'єднань.

Мережний рівень вирішує ці проблеми через:

1. **Агрегацію адрес.** Працює не з окремими адресами, а з групами адрес, об'єднаними в блоки (мережі).
2. **Фільтрацію пакетів.** Пакети без відомого шляху доставки відкидаються, щоб уникнути перевантаження мережі.

Таким чином, мережний рівень дозволяє об'єднувати локальні мережі в єдину глобальну мережу — Інтернет.

7.2 IP-адресація

У мережах використовуються два типи адрес: локальні та глобальні.

✎**Локальні адреси** – це адреси на рівні канального рівня, вони прив'язані до конкретної технології. Наприклад, це можуть бути **MAC-адреси** в Ethernet або **адреси в мережах мобільного зв'язку**. Такі адреси не можуть використовуватися для створення великої об'єднаної мережі, яка поєднує різні технології.

Щоб це стало можливим, у **моделі взаємодії відкритих систем** вводиться **мережний рівень**, де використовуються глобальні адреси.

✎**Глобальні адреси** – це адреси мережного рівня. У стеку протоколів TCP/IP це **IP-адреси**.

Глобальні адреси не прив'язані до канального рівня, і завдяки їм можна створити мережу, яка об'єднує підмережі, побудовані на різних технологіях канального рівня.

Тип глобальних адрес – це **IP-адреси**. Саме ці адреси використовуються у стеку протоколів TCP/IP і, зокрема, в Інтернеті. IP-адреси застосовуються для **унікальної ідентифікації комп'ютерів** у великій об'єднаній мережі, яка може охоплювати весь світ, як це робить мережа Інтернет.

Різні частини Інтернету побудовані на різних технологіях канального рівня. Наразі існують дві версії IP-протоколу: **версія 4** та **версія 6**. Ми будемо вивчати **IPv4**, а IPv6 буде розглянуто в окремих лекціях.

Основна відмінність між цими протоколами – **довжина IP-адреси**. У IPv4 вона становить **4 байти** (32 біти), а в IPv6 – **16 байтів** (128 біт).

IP-адреса версії 4 складається з **32 біт** (4 байти). Для зручності роботи з такими адресами їх ділять на **4 частини по 8 біт**. Кожна частина називається **октетом**. Октети записуються в десятковому форматі, розділені крапками, наприклад: **192.168.0.1**.

Одне із завдань мережного рівня – забезпечити **масштабованість**, тобто створити таку мережу, яка може працювати в масштабах усього світу. Для цього мережний рівень працює не з окремими комп'ютерами, а з так званими **підмережами**, які об'єднують кілька комп'ютерів.

У підмережах об'єднуються комп'ютери з однаковою старшою частиною IP-адреси. Наприклад, у діапазоні адрес **192.168.1.0 – 192.168.1.255** перші три октети однакові, а відрізняється лише останній.

7.2.1 Маска підмережі

Щоб визначити, яка частина IP-адреси відповідає підмережі, а яка – хосту (комп'ютеру), використовується **маска підмережі**.
Маска підмережі також складається з **32 біт**. Вона вказує, де в IP-адресі знаходиться адреса підмережі:

- У частині, що належить підмережі, маска містить **1**.
- У частині, що належить хосту, – **0**.

Наприклад, для підмережі з адресою **192.168.1.0/24** маска в десятковому форматі записується як **255.255.255.0**. У нотації префікса вона записується як **/24**, де 24 означає кількість біт, що належать підмережі.

7.2.2 Класова адресація

Раніше IP-адреси поділялися на **класи** (A, B, C, D, E). У кожному класі жорстко визначалося, яка частина IP-адреси відповідає підмережі, а яка – хосту. Сьогодні класова адресація вважається застарілою, але її іноді згадують у літературі та документах.

IP-адреси – це **глобальні адреси мережного рівня**, що використовуються в стеку протоколів TCP/IP та в Інтернеті.

Маска підмережі дозволяє визначити, де в IP-адресі знаходиться адреса мережі, а де – адреса хоста.
Завдяки використанню маски підмережі забезпечується масштабування мереж, включаючи глобальну мережу Інтернет, яка охоплює весь світ.

В IPv4 використовується 3 типи адрес:

1. Індивідуальний (unicast);
2. Груповий (multicast);
3. (broadcast).

- Індивідуальна адреса — це адреса комп'ютера, саме такі адреси ми розглядали вище.

– Групова адреса — це адреса, яка використовується кількома комп'ютерами. Якщо ви відправите дані на цю адресу, його отримає кілька комп'ютерів у мережі, які входять до цієї групи.

– Широкомовна адреса — це така адреса, яка використовується для отримання даних усіма комп'ютерами мережі.

7.2.3 Широкомовна адреса

Широкомовна адреса в IP має такий формат: частина яка відноситься до адреси мережі залишається без змін, а в тій частині, що відноситься до адреси хоста, записуються в бітові одиниці.

Ми вже зустрічалися з широкомовними. Важливою відмінністю широкомовних адрес у мережному рівні від адрес технології канального рівня Ethernet є те, що широкомовні адреси використовуються тільки в межах однієї підмережі.

Маршрутизатори не передають широкомовні пакети в іншу мережу, інакше можна дуже швидко завалити всю глобальну мережу, у тому числі весь Інтернет, сміттєвими пакетами.

В IP використовується 2 типи широкомовних адрес, що підходять для двох різних сценарій (рис.3.1).

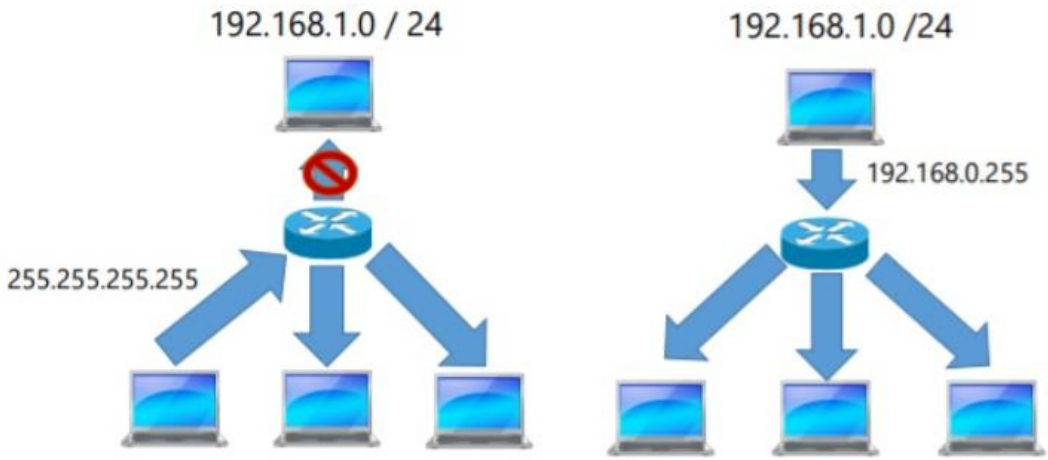


Рисунок 3.1 – Типи широкомовних адрес

Припустимо, що у нас є 2 підмережі об'єднані між собою маршрутизатором. Якщо ми хочемо відправити широкомовний пакет у межах однієї мережі, це називається обмежене широкомовлення. У цьому випадку ми можемо використовувати спеціальну широкомовну адресу, яка складається з усіх бітових одиниць (255.255.255.255). У цьому випадку дані отримають усі комп'ютери в мережі, а через маршрутизатор дані не пройдуть.

Інший сценарій, коли комп'ютер, який знаходиться за межами нашої мережі, хоче передати широкомовний пакет всім комп'ютерам, які знаходяться в нашій мережі, це називається спрямоване широкомовлення. У цьому випадку широкомовна IP-адреса буде виглядати 192.168.0.255, адреса підмережі, в яку

ми хочемо відправити широкомовний пакет і бітові одиниці в тій частині, яка відноситься до адреси хоста. Як відбудеться обробка такого пакета? Пакет передається маршрутизатору і маршрутизатор вже розішле цей пакет у широкомовному режимі, але тільки передах однієї підмережі, для якої призначається цей широкомовний пакет.

Спеціальні типи IP-адрес

Які бувають спеціальні типи IP-адрес:

У номері хоста не можна використовувати лише бітові 0, і лише бітові 1. Якщо ми вкажемо тільки бітові 0, це вийде не адреса хоста, а адреса підмережі 213.180.193.0.

А якщо вкажемо лише бітові 1, то це буде широкомовна адреса. 213.180.193.255.

Часто, маршрутизатору за умовчанням у мережі, чи шлюзу, якими всі комп'ютери мережі потрапляють до інтернету, присвоюють адресу з номером 1. Проте чітких правил немає, так робити необов'язково 213.180.193.1.

Адреса, яка складається з усіх 0.0.0.0, це адреса поточного хоста. Він використовується, коли комп'ютер ще не отримав IP-адресу.

Адреса з усіх бітових одиниць, 255.255.255.255 це все хости в поточній підмережі (обмежена широкомовна адреса).

127.0.0.0/8 це зворотна петля, спеціальний діапазон адрес, який виділено для того, щоб налагоджувати мережні програми, якщо у вас немає мережного обладнання або воно налаштоване не так як вам потрібно, в цьому випадку дані не відправляються в мережу, а приходять назад на комп'ютер. Часто з цієї мережі використовується адреса 127.0.0.1 це поточний комп'ютер (localhost). Однак не обов'язково для цієї мети використовувати адресу з хостом 1, можна використовувати 2, 3 або будь-яку іншу IP-адресу з цього діапазону.

IP-адреси з підмережі 169.254.0.0/16 називаються Link- local адреси. Якщо ви не налаштували IP-адресу на своєму ПК вручну або якимось іншим способом, наприклад за допомогою протоколу DHCP, то операційна система сама може призначити комп'ютеру адресу з цього діапазону. Такі адреси можуть використовуватися лише в межах підмережі та не проходять через маршрутизатор.

7.2.4 Розподіл IP-адрес

Так як IP-адреси є глобальними адресами і використовуються для побудови мереж, які можуть потенційно об'єднувати всі комп'ютери в світі, такі як мережа інтернет, то кожен комп'ютер повинен мати унікальну IP-адресу в усьому світі.

Якщо у нас буде кілька комп'ютерів з однією IP-адресою, то ми не зможемо зрозуміти до якого комп'ютера повинні відправити наші дані . IP-адреси в Internet Assigned Number Authority (IANA), зараз функції IANA реалізуються корпорацією ICANN (Internet Corporation for Assigned Names and Numbers) — Корпорація Інтернет для розподілу імен та номерів. Саме ця організація відповідає за розподіл IP-адрес у всьому світі.

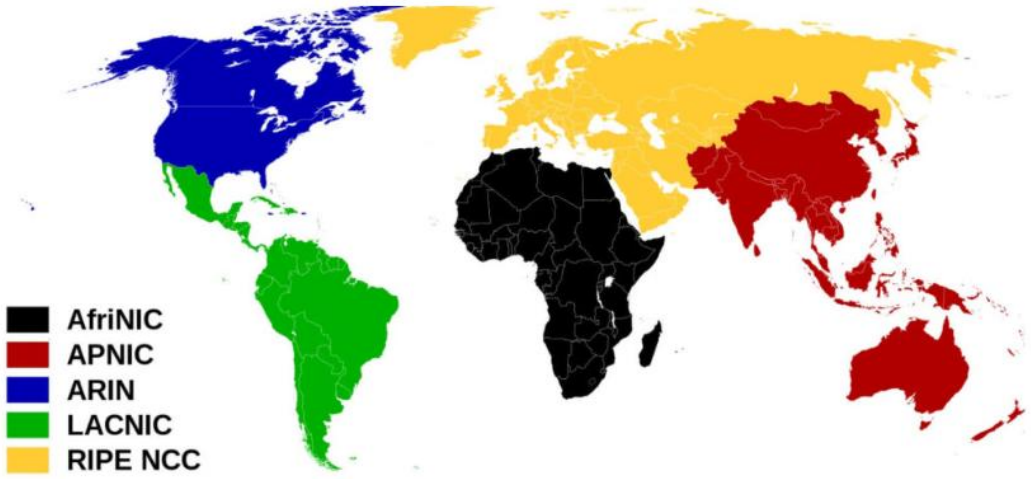


Рисунок 3.2 – Регіональні реєстратори ICANN

Проте організація робить це безпосередньо, а з допомогою регіональних реєстраторів. У кожному регіоні є свій реєстратор, який взаємодіє з компанією ICANN та розподіляє IP-адреси. Європа належить до регіонального реєстратора RIPE.

7.2.5 Приватні IP-адреси

Однак є такі випадки, коли ви створюєте мережу, яка використовує IP-адреси, але при цьому вона не підключена до Інтернету. Наприклад, внутрішня мережа організації або внутрішня мережа класу, де ви просто тестуєте якісь мережні технології. Було б дуже незручно звертатися до регіонального реєстратора для того, щоб просити IP-адреси для такої мережі. Спеціально для цього випадку виділено кілька діапазонів приватних IP-адрес, це такі IP-адреси, які можна використовувати в підмережах, які не підключаються до інтернету. При цьому звертатися до ICANN для отримання IP-адреси не потрібно. Діапазон приватних IP-адрес визначений у документі RFC 1918 і він включає наступне:

- 10.0.0.0/8
- 172.168.0.0/12
- 192.168.0.0/16

Особливість цих адрес у тому, що вони не маршрутизуються до Інтернету. Однак, є можливість підключити мережу, побудовану на основі приватних адрес до Інтернету, для цього використовується технологія Трансляція мережних адрес NAT (Network Address Translation) . У цьому випадку адреса приватної підмережі замінюється на реальну IP-адресу.

7.3 Протокол IP

IP-протокол (від англ. **I**nternet **P**rotocol — Інтернет-протокол, міжмережний протокол) — це основний протокол **мережного рівня**, який

відповідає за **адресацію** та **маршрутизацію** пакетів даних (дейтаграм) між мережами.

Протокол IP виник задовго до того, як з'явилася і стала набирати популярність мережа, яку ми називаємо Internet, означає об'єднання мереж.

Мета протоколу IP якраз об'єднати мережі побудовані за допомогою різних технологій канального рівня в цій термінології словом інтернет називалася об'єднана мережа, а subnet підмережа або окрема мережа. Словом інтернет з великої літери зараз називається найбільша об'єднана мережа побудована за протоколом IP.

У моделі взаємодії відкритих систем і у моделі tcp IP ротокол IP знаходиться на одному й тому ж рівні мережному. Мережний рівень стека протоколів tcpip включає також і інші протоколи крім IP, це ARP, DHCP та icmp. Але для передавання даних використовується тільки протокол IP, інші протоколи служать для забезпечення коректної роботи великої складеної мережі.

IP забезпечують передавання даних без гарантії доставки, не гарантується як доставка так і порядок проходження повідомлень. Протокол IP, так само як і Ethernet, використовує передавання даних без встановлення з'єднання. IP пакет просто відправляється в мережу в надії, що він дійде до одержувача, якщо пакет з якихось причин не дійшов, не робиться жодних спроб сповістити відправника і також не робиться спроб запросити цей пакет знову. Вважається, що помилка має бути виправлена протоколами, які знаходяться на вищих рівнях. Завдання IP є об'єднання мереж побудованих на основі різних технологій канального рівня, які можуть значно відрізнятися одна від одної в одну велику об'єднану мережу, в якій комп'ютери можуть вільно спілкуватися один з одним не зважаючи на відмінність конкретної мережної технології. Друге важливе завдання протоколу IP - це маршрутизація, тобто пошук маршруту від відправника до одержувача. Також IP забезпечує необхідну якість обслуговування.

Для того щоб зрозуміти, як протокол IP реалізує ці завдання ми розглянемо формат заголовка IP пакета. Перше поле - номер версії. Зараз використовуються дві версії протоколу IP, четверта і шоста. В полі довжина заголовка записується повна довжина, як обов'язкової частини так і опцій. Наступне поле тип сервісу - це поле потрібне для забезпечення необхідної якості обслуговування, але зараз на практиці використовується дуже рідко. Наступне поле - загальна довжина загальна довжина містить довжину всього IP пакета включно з заголовком і даними.

Максимальна довжина пакета 65535 байт але на практиці такі великі пакети не використовуються, а максимальний розмір обмежений розміром кадру канального рівня для Ethernet це 1500 байт. В іншому випадку для передачі одного IP пакета необхідно було б кілька кадрів канального рівня, що незручно. Поля ідентифікатор пакета. прапори та зміщення фрагмента використовуються для реалізації фрагментації. Далі йде поле час життя час Time to Life або ТЛ - це максимальний час протягом, якого пакет може переміщатися мережі, воно впроваджене для того, щоб пакети не гуляли по

мережі нескінченно, якщо в конфігурації мережі виникла якась помилка, наприклад, в результаті неправильного налаштування маршрутизаторів у мережі може утворитися петля. Раніше час життя вимірювався в секундах, але зараз маршрутизатори обробляють пакет значно швидше ніж за секунду, тому час життя зменшується на одиницю на кожному маршрутизаторі і він вимірюється в кількостях проходження через маршрутизатори, по-англійськи хоп від слова стрибок. Після часу життя вказується тип протоколу наступного рівня, це поле необхідне для функції мультиплексування та демультиплексування. Якщо при перевірці контрольної суми виявлено помилки, то пакет відкидається, ніякої інформації відправнику пакета не надсилається, контрольна сума розраховується тільки за заголовком IP пакета і вона перераховується на кожному маршрутизаторі, через те що дані в заголовку змінюються, як мінімум змінюється час життя пакета, а також можуть змінитися деякі опції. Після контрольної суми йдуть IP-адреса відправника та IP-адреса одержувача.

? Контрольні запитання:

1. Яке основне завдання Мережного рівня в загальному розумінні, і для чого він був створений?
2. Назвіть дві основні проблеми, які виникають при спробі побудувати глобальну мережу, використовуючи лише технології Канального рівня.
3. Наведіть три приклади, чим саме відрізняються технології канального рівня, що ускладнює їхнє об’єднання (наприклад, рівень сервісу, тип адресації тощо).
4. Яким чином Мережний рівень вирішує проблему обмеження максимального розміру кадру в різних мережах?
5. Які два механізми використовує Мережний рівень для вирішення проблеми масштабованості глобальних мереж?
6. Що таке глобальні IP-адреси і чим вони принципово відрізняються від локальних адрес, таких як MAC-адреси?
7. Скільки біт має IP-адреса у версії IPv4 та у версії IPv6?
8. Яка функція маски підмережі і що конкретно означає число у нотації префікса (наприклад, /24)?
9. Назвіть три типи IP-адрес за призначенням (типи передачі), що використовуються в IPv4.
10. Чому маршрутизатори не передають широкомовні пакети (broadcast) в іншу мережу?
11. Яку функцію виконує поле «Час життя» (Time to Live, TTL) у заголовку IP-пакета?
12. Назвіть три діапазони приватних IP-адрес згідно з RFC 1918.

✍Практичні завдання:

Завдання 1:

Вам надано опис підмережі та IP-адресу комп'ютера в ній.

Дано: IP-адреса хоста: 192.168.10.150, маска підмережі (префікс): /24

Необхідно:

1. Записати маску підмережі у десятковому форматі (наприклад, 255.x.x.x).
2. Визначити адресу самої підмережі (Network Address).
3. Визначити широкомовну адресу (Broadcast Address) для цієї підмережі.
4. Який діапазон IP-адрес можуть використовувати хости у цій підмережі?
5. Чи є IP-адреса 192.168.10.150 приватною, і якщо так, до якого діапазону (за RFC 1918) вона належить?

Завдання 2:

Вам надано перелік IP-адрес. Визначте, **яка це спеціальна адреса** (за текстом) і **яке її призначення**.

IP-адреса	Назва спеціальної адреси	Призначення
0.0.0.0		
255.255.255.255		
127.0.0.1		
169.254.10.5		

Тести з теми «Мережний рівень. IP-адресація»

1. Який протокол відповідає за адресацію та маршрутизацію пакетів даних (дейтаграм) на Мережному рівні?

A. TCP
B. IP
C. Ethernet

2. Яка з наведених проблем виникає при спробі побудувати глобальну мережу з мільярдами пристроїв, використовуючи лише технології Канального рівня (наприклад, Ethernet/Wi-Fi)?

A. Занадто швидка передача даних
B. Обмеження масштабованості через розмір таблиць комутації
C. Невідповідність між довжиною хвилі сигналу

3. Скільки біт використовується для представлення IP-адреси у версії IPv4?

A. 16 біт

B. 64 біти
C. 32 біти

4. Яка частина IP-адреси у масці підмережі (Subnet Mask) позначається бітовими одиницями (1)?

A. Частина, що належить хосту (комп'ютеру)
B. Частина, що належить підмережі
C. Частина, що належить шлюзу

5. Яка з наведених IP-адрес є обмеженою широкомовною адресою (Limited Broadcast Address) в межах поточної підмережі?

A. 192.168.1.1
B. 127.0.0.1
C. 255.255.255.255

Тема 8 Маршрутизація в IP-мережах

Ключові поняття: маршрутизація, маршрутизатор, метрика, маршрут за замовчуванням,

8.1 Маршрутизація

Маршрутизація працює на мережному рівні модель взаємодії відкритих систем OSI.

Маршрутизація — це пошук маршруту доставки пакета у великій складовій мережі через транзитні вузли, які називаються маршрутизатори.

Маршрутизація складається з двох етапів:

1. На першому етапі відбувається вивчення мережі, які підмережі є в цій складовій мережі, які маршрутизатори і як ці маршрутизатори об'єднані між собою.
2. Другий етап маршрутизації виконується коли мережа вже вивчена і на маршрутизатор надійшов пакет, для цього пакета потрібно визначити куди саме його відправити. Іноді для другого етапу маршрутизації використовується окремий термін "просування" англійською *forwarding*.

Як приклад, розглянемо схему структурованої мережі (рис.3.3), тут показано окремі підмережі, для кожної підмережі є її адреса і маска, а також маршрутизатори, які об'єднують ці мережі.

Розглянемо маршрутизатор D, на нього прийшов пакет, і маршрутизатор має вирішити, що йому робити з цим пакетом. Почнемо з того, які взагалі можливі варіанти дій у маршрутизатора. Перший варіант — мережа, якій призначений пакет, підключена безпосередньо до маршрутизатора. У маршрутизатора D таких мереж 3, у цьому випадку маршрутизатор передає пакет безпосередньо в цю мережу.

Другий варіант: потрібна мережа підключена до іншого маршрутизатора (A), і відомо, який маршрутизатор потрібен. У цьому випадку маршрутизатор D передає пакет на наступний маршрутизатор, який може передати пакет у потрібну мережу, такий маршрутизатор називається шлюзом.

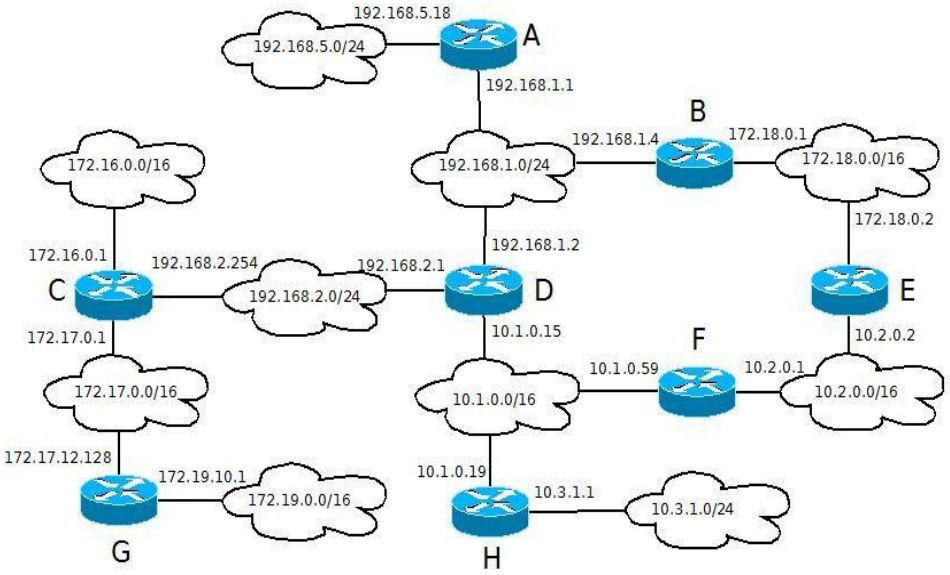


Рисунок 3.3 – Схема IP-мережі

Третій варіант: прийшов пакет для мережі, маршрут якої не відомий, у цьому разі маршрутизатор відкидає пакет. У цьому відмінність роботи маршрутизатора від комутатора, комутатор відправляє кадр, який він не знає, куди доставити, на всі порти, маршрутизатор так не робить. В іншому разі складова мережа дуже швидко може переповнитися сміттєвими пакетами, для яких не відомий маршрут доставки.

Часто виникає питання, що робити, якщо мережа, для якої прийшов пакет, знаходиться не за одним маршрутизатором? Щоб у неї потрапити, потрібно пройти не через один, а через кілька маршрутизаторів, що в цьому випадку потрібно вписати в таблицю маршрутизації.

У таблицю маршрутизації записуємо тільки перший крок, адресу наступного маршрутизатора, все, що знаходиться далі, нас не цікавить.

Адреса	Маска	Шлюз	Інтерфейс	Метрика
192.168.1.0	255.255.255.0	Під'єднаний	192.168.1.2	276
192.168.2.0	255.255.255.0	Під'єднаний	192.168.2.1	276
10.1.0.0	255.255.0.0	Під'єднаний	10.1.0.15	276
172.16.0.0	255.255.0.0	192.168.2.254	192.168.2.1	306
10.2.0.0	255.255.0.0	10.1.0.59	10.1.0.15	306

Рисунок 3.4 – Таблиця маршрутизації

Вважаємо, що наступний маршрутизатор має знати правильний маршрут до потрібної мережі, він знає краще за наступний маршрутизатор, той знає наступний крок і так далі, поки не доберемося до потрібної нам мережі.

8.1.1 Метрика

Можна помітити, що в нашій схемі в одну й ту саму мережу, наприклад ось у цю (10.2.0.0/16), можна потрапити двома шляхами, перший шлях проходить через один маршрутизатор F, а другий шлях — через два маршрутизатори B та E.

У цьому відмінність мережного рівня від канального. На канальному рівні у нас завжди має бути тільки одне з'єднання, а на мережному рівні допускаються і навіть заохочуються для забезпечення надійності кілька шляхів до однієї і тієї ж мережі.

Який шлях обрати? Для цього використовуються поле метрика таблиці маршрутизації.

Метрика — це деяке число, яке характеризує відстань від однієї мережі до іншої. Якщо є кілька маршрутів до однієї і тієї самої мережі, то обирається маршрут із меншою метрикою.

Раніше метрику вимірювали в кількості маршрутизаторів, тож відстань через маршрутизатор F була б одна, а через маршрутизатори B і E — дві.

Однак зараз метрика враховує не тільки кількість проміжних маршрутизаторів, а й швидкість каналів між мережами, бо іноді буває вигідніше пройти через два маршрутизатори, але швидкісними каналами. Також може враховуватися завантаженість каналів, тому зараз метрика — це число, яке враховує всі характеристики. Ми обираємо маршрут із мінімальною метрикою в цьому прикладі вище, буде обрано перший маршрут через маршрутизатор F.

8.1.2 Записи в таблиці маршрутизації

Звідки з'являються записи в таблиці маршрутизації? Є два варіанти: статична маршрутизація та динамічна маршрутизація.

За статичної маршрутизації, записи в таблиці маршрутизації налаштовуються вручну, це зручно робити, якщо у вас мережа невелика і змінюється рідко, але якщо мережа велика, то вигідніше використовувати динамічну маршрутизацію, в якій маршрути налаштовуються автоматично. У цьому випадку маршрутизатори самі виявляють мережу за допомогою протоколів маршрутизації RIP, OSPF, BGP та інших.

Перевага динамічної маршрутизації в тому, що зміни в мережі можуть автоматично відзначатися в таблиці маршрутизації. Наприклад, якщо вийшов з ладу один із маршрутизаторів, то маршрутизатори за протоколами маршрутизації про це дізнаються й приберуть маршрут, який проходить через цей маршрутизатор. З іншого боку, якщо з'явився новий маршрутизатор, то це також відобразиться в таблиці маршрутизації автоматично.

8.1.3 Маршрут за замовчуванням

Якщо маршрутизатор не знає куди відправляти пакет, то такий пакет відкидається. Таким чином виходить, що маршрутизатор має знати маршрути до всіх підмереж у складному мережі. На практиці для великих мереж, наприклад для інтернету, це неможливо, тому використовуються такі рішення.

У таблиці маршрутизації призначається спеціальний маршрутизатор за замовчуванням, на який надсилаються всі пакети для невідомих мереж, як правило це маршрутизатор, який підключений до інтернету.

Передбачається, що цей маршрутизатор краще знає структуру мережі, і здатний знайти маршрут у складній мережі. Для позначення маршруту за замовчуванням в таблиці маршрутизації використовують чотири нулі в адресі підмережі та чотири нулі в масці (0.0.0.0, маска 0.0.0.0), а іноді також пишуть default.

IP-адреса і маска дорівнюють нулю, в адресу і шлюз вказуються IP-адреса маршрутизатора за замовчуванням.

8.1.4 Довжина маски підмережі

Розглянемо приклад. Маршрутизатор прийняв пакет на IP-адресу (192.168.100.23). У таблиці маршрутизації є 2 записи (192.168.100.0/24 і 192.168.0.0/16), який підходить цій IP-адресі, але в них різна довжина маски. Який із цих записів вибрати? Вибирається той запис, де маска довша, відповідно цей запис із довшою маскою містить найкращий маршрут мережі, яка нас цікавить.

Щоб зрозуміти чому так відбувається, давайте розглянемо складову мережу гіпотетичного університету. Університет отримав блок IP-адрес, розділив цей блок IP-адрес на дві частини, і кожну частину виділив окремому кампусу.

На кампусі знаходяться свої маршрутизатори, на яких мережа була далі розділена на частини призначені для окремих факультетів. Поділ мереж проводиться за допомогою збільшення довжини маски, весь блок адрес має маску /16, блоки кампусів мають маску /17, а блоки факультетів /18.

Нижче показано фрагмент таблиці маршрутизації на маршрутизаторі першого кампусу. Він містить шлях до мережі першого факультету, 2 факультету, до загально університетської мережі, який проходить через університетський маршрутизатор, а також маршрут за замовчуванням до інтернету, який теж проходить через загально університетський маршрутизатор.

Припустимо, що на цей маршрутизатор прийшов пакет, призначений для другого факультету, що має зробити маршрутизатор? Він може вибрати запис, який відповідає другому факультету й відправити безпосередньо в мережу цього факультету, або може вибрати запис, який відповідає всій університетській мережі, тоді відправить на університетський маршрутизатор, що буде явно неправильним.

І так виходить, що обирається завжди маршрут із маскою максимальної довжини. Загальні правила вибору маршруту такі:

– Найдовша маска — це маршрут конкретному хосту, якщо в таблиці маршрутизації є такий маршрут, то обирається він.

– Потім обирається маршрут до мережі з маскою максимальної довжини.

– І тільки після цього використовується маршрут за замовчуванням, де маска /0, під яку підходять усі IP-адреси.

– Слід зазначити, що таблиця маршрутизації є тільки у мережних пристроїв маршрутизатора, у звичайних комп'ютерів у мережі, хоча в них таблиця маршрутизації набагато менша.

– Зазвичай така таблиця містить опис приєднаної мережі, до якої під'єднано цей комп'ютер.

– Адреса маршрутизатора за замовчуванням (шлюз або gateway), через який виконується підключення до інтернету або до корпоративної мережі підприємства.

– А також можуть бути додаткові маршрути до деяких знайомих мереж, але це швидше виключення.

Для того щоб переглянути таблицю маршрутизації, можна використовувати команду route або ip route (route print — Windows; route і ip route — Linux).

? Контрольні запитання:

1. Що таке маршрутизація і з яких двох основних етапів вона складається?
2. Назвіть три можливі варіанти дій маршрутизатора, коли він отримує пакет, призначений для певної мережі (наприклад, мережа підключена безпосередньо, мережа віддалена тощо).
3. Що таке метрика в контексті маршрутизації? Як маршрутизатор використовує метрику при наявності декількох шляхів до однієї і тієї ж мережі?
4. Яка основна відмінність між статичною та динамічною маршрутизацією?
5. Як маршрутизатор обирає маршрут, якщо в таблиці маршрутизації є кілька записів, що підходять для однієї IP-адреси, але мають різну довжину маски (наприклад, /16 та /24)? Який маршрут має найвищий пріоритет?

✍Практичні завдання:

Завдання 1:

Уявіть, що маршрутизатор має доставити пакет до віддаленої мережі. У його таблиці маршрутизації знайдено два можливих шляхи:

Маршрут	Шлюз (Next Hop)	Метрика

Маршрут А	10.10.1.1	5
Маршрут Б	10.10.2.1	2

1. Який маршрут вибере маршрутизатор для надсилання пакета?
2. На основі чого (якої характеристики) приймається це рішення?
3. Наведіть приклад, що може означати це число (метрика), якщо вона вимірюється за старим стандартом?

Завдання 2:

Маршрутизатор отримав пакет, призначений для IP-адреси 172.16.50.25. У його таблиці маршрутизації (Router Table) є наступні записи, які відповідають цій IP-адресі:

Номер запису	Адреса Підмережі та Маска	Шлюз
1	0.0.0.0 / 0 (За замовчуванням)	R1
2	172.16.0.0 / 16	R2
3	172.16.50.0 / 24	R3

1. Який із трьох записів обере маршрутизатор для маршрутизації цього пакета?
2. Сформулюйте правило.

Тести з теми «Маршрутизація в IP-мережах»

1. Маршрутизація складається з двох етапів. Як називається другий етап, що виконується, коли мережа вже вивчена і маршрутизатор визначає, куди саме відправити пакет?

A. Інкапсуляція
B. Просування (Forwarding)
C. Фрагментація

2. Яку дію виконує маршрутизатор, коли отримує пакет, призначений для мережі, маршрут до якої йому не відомий?

A. Надсилає пакет на всі порти, крім того, звідки він прийшов.
B. Запитує протокол ARP, щоб знайти MAC-адресу одержувача.
C. Відкидає пакет, щоб уникнути переповнення мережі сміттєвими пакетами.

3. Що таке метрика в таблиці маршрутизації?

A. Максимальний розмір пакета.
B. Число, що характеризує відстань від однієї мережі до іншої.

C. Кількість активних з'єднань, що підтримується протоколом STP.

4. Який запис у таблиці маршрутизації використовується, коли маршрутизатор не знає точного маршруту до цільової мережі?

A. Маршрут до мережі з найдовшою маскою.
B. Маршрут за замовчуванням (0.0.0.0 / 0).
C. Маршрут з найменшим значенням TTL.

5. Якщо до однієї IP-адреси підходять два записи в таблиці маршрутизації, який запис буде обрано, згідно з правилом «найдовша маска»?

A. Запис із найменшим значенням метрики.
B. Запис, який відповідає маршруту за замовчуванням.
C. Запис із маскою максимальної довжини.

РОЗДІЛ 4 АВТОМАТИЗАЦІЯ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

Тема 9 Технології автоматизації

Ключові поняття: ARP, ARP-запит, ARP-відповідь, мережний рівень.

9.1 Протокол ARP

ARP-протокол (Address Resolution Protocol) — це мережний протокол, який використовується для визначення фізичної (MAC) адреси пристрою за його IP-адресою в локальній мережі.

Дані передаються за допомогою якоїсь технології канального рівня , наприклад Ethernet . Комутатори Ethernet нічого не знають про IP-адреси і для передачі даних використовують MAC-адреси. Отже, необхідний засіб, який дозволяє за IP-адресою комп'ютера визначити його MAK-адресу.

9.1.1 Таблиця відповідності ARP

Найпростіший засіб це таблиця відповідності. Ми створюємо таблицю, в якій пишемо IP-адресу та відповідну їй MAC-адресу.

Такий засіб дійсно використовується на практиці, наприклад, у Linux така табличка зберігається у файлі / etc / ethers . Однак у великій мережі такий підхід не працює.

Протокол ARP дозволяє автоматично визначити MAK-адресу комп'ютера за його IP-адресою. Протокол працює в режимі запит-відповідь.

Комп'ютер, який хоче дізнатися MAK-адресу за відомою IP-адресою, надсилає ARP запит "У кого IP 192.168.10.43?" Запит надсилається на широкомовну MAK-адресу (FF:FF:FF:FF:FF:FF).

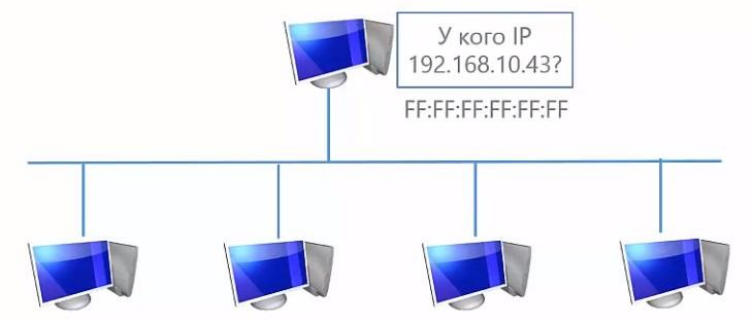


Рисунок 4.1 – ARP-запит

І цей запит отримують усі комп'ютери в мережі. Той комп'ютер, який дізнався у запиті свою IP-адресу готує та надсилає ARP відповідь. У відповідь включається IP-адреса комп'ютера (IP:192.168.10.43) та її MAK-адреса (MAC: 54:BE:F7:88:15:47).

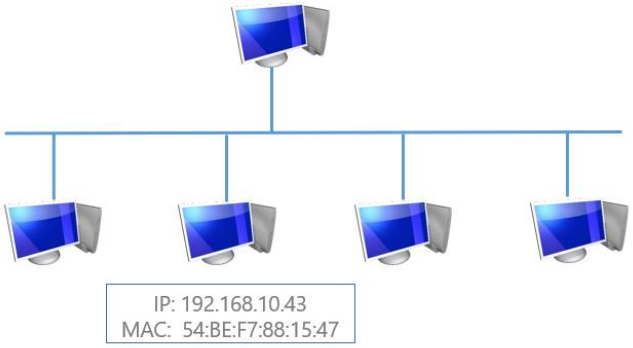


Рисунок 4.2 – ARP-відповідь

Відправник ARP запиту отримує відповідь, витягує з нього МАК-адресу та використовує її для передачі даних за технологією канального рівня .

ARP розроблявся як протокол загального призначення з можливістю застосовувати його не тільки в Ethernet і не тільки для IP-адрес. Тому на початку ARP пакету (рис.4.3) йде службова інформація, яка дозволяє визначити з яким типом мережного обладнання та з яким протоколом мережного рівня ми працюємо.

- Перше поле “тип мережі” говорить про те, яке обладнання ми використовуємо в мережі, 1 - відповідає Ethernet.
- Друге поле "тип протоколу" в ньому вказується протокол мережного рівня 2048 означає IP.
- Далі йде “довжина локальної адреси”, у разі МАК-адреси 6 байт, “довжина глобальної адреси у разі IP-адреси” 4 байта.
- Наступне поле код операції, 1 відповідає ARP запиту, а 2 - ARP відповіді.
- Потім йде корисна інформація про локальні (1C:75:08:D2:49:45) та глобальні адреси (192.168.10.15). Вказується МАК-адреса та IP-адреса відправника, щоб одержувач знав, кому надсилати відповідь.
- Глобальна адреса одержувача (192 168 10 43).
- Локальна адреса одержувача невідома (00:00:00:00:00:00)

Поле	Значення
Тип мережі	1
Тип протоколу	2048
Довжина локальної адреси	6
Довжина глобальної адреси	4
Операція	1
Локальна адреса відправника	1C:75:08:D2:49:45
Глобальна адреса відправника	192.168.10.15
Локальна адреса одержувача	00:00:00:00:00:00
Глобальна адреса одержувача	192.168.10.43

Рисунок 4.3 – Формат ARP – запиту

Формат ARP відповіді (рис.4.4) такий самий, тільки в полі “операція” стоїть значення 2 та адреса, яку ми шукаємо знаходиться в полі локальну адресу відправника.

Поле	Значення
Тип мережі	1
Тип протоколу	2048
Довжина локальної адреси	6
Довжина глобальної адреси	4
Операція	2
Локальна адреса відправника	54:BE:F7:88:15:47
Глобальна адреса відправника	192.168.10.43
Локальна адреса одержувача	1C:75:08:D2:49:45
Глобальна адреса одержувача	192.168.10.15

Рисунок 4.4 – Формат ARP – відповіді

У моделі взаємодії відкритих систем OSI протокол ARP знаходиться між канальним та мережним рівнем .

Через те, що ARP знаходиться нижче мережного рівня, пакети ARP не проходять через маршрутизатори. Таким чином, за допомогою ARP можна дізнатися лише MAK-адреси комп'ютерів, які знаходяться в одній підмережі, а адреси комп'ютерів, які знаходяться в іншій підмережі, відокремлені маршрутизатором не можна.

Чому так відбувається? ARP запит надсилається на широкомовну адресу, яку отримують всі комп'ютери всередині мережі, але широкомовний трафік не проходить через маршрутизатори, тому комп'ютери в іншій підмережі за маршрутизатором ARP запит не отримають і не зможуть відправити на нього відповідь.

Після того, як MAK-адреса одержувача знайдена, вона кешується на комп'ютери відправника в ARP-таблиці (рис.4.5) для того, щоб не вимагати MAK-адресу кожного разу за протоколом ARP.

IP-адреса	MAC-адреса	Тип
172.16.10.253	00:1C:C5:34:B3:01	Динамічний
172.16.10.88	1C:75:08:D2:49:45	Статичний

Рисунок 4.5 – ARP– таблиця

Таблиця складається з 3-х полів — IP-адреса, MAC-адреса і Тип запису в ARP таблиці.

Подивитися ARP таблицю на комп'ютері можна за допомогою команди arp -a .

9.1.2 Оптимізація ARP

ARP запит відправляється на широкомовну адресу і його отримують всі комп'ютери в мережі, крім ip -адреси для якого необхідно отримати мак-адресу ARP запит. Відправник також включає свою ip- адресу та свою мак-адресу, ці дані можуть бути записані всіма комп'ютерами в мережі в ARP-таблицю, щоб використовувати коли вони знадобляться.

ARP-запит (Gratuitous ARP) - це запит по ARP власної IP -адреси, він використовується для двох цілей. Перша мета, швидке оповіщення всіх комп'ютерів у мережі від того, що у комп'ютера з'явився новий IP- адреса.

Інша мета - перевірка використання даної ip -адреси іншим комп'ютером. Якщо на добровільний ARP запит надійшла відповідь, це означає, що якийсь комп'ютер у мережі вже використовує цю ip- адресу і призначати його комп'ютеру відправника не можна.

? Контрольні запитання:

1. Для чого використовується протокол ARP та яку проблему він вирішує в локальній мережі?
2. Чому в Ethernet-мережах необхідно визначати MAC-адресу пристрою, навіть якщо відома його IP-адреса?
3. Чому ARP-запити не можуть пройти через маршрутизатор і як це обмежує пошук MAC-адрес?
4. Яку інформацію містять основні поля ARP-пакету та які значення відповідають ARP-запиту і ARP-відповіді?
5. Що таке Gratuitous ARP, у яких випадках він використовується і яку проблему допомагає виявити?

✍Практичні завдання:

Завдання 1.

1. Відкрити командний рядок (Windows: *cmd*, Linux/MacOS: *terminal*).
2. Виконати команду:
   - Windows: arp -a
   - Linux: ip neigh або arp -n
3. Зробити скриншот або переписати фрагмент таблиці.
4. Проаналізувати отриману інформацію:
   - Які IP-адреси представлені в таблиці?
   - Які відповідні до них MAC-адреси?
   - Який тип запису (dynamic/static) мають елементи таблиці?

5. Зробити висновок: як ARP-таблиця допомагає оптимізувати обмін даними між пристроями?

Завдання 2.

1. Запустити програму для аналізу трафіку (наприклад, *Wireshark*).
2. У фільтрі ввести: arp → щоб бачити лише ARP-пакети.
3. На іншому комп'ютері в мережі виконати команду ping <IP вашого ПК>.
4. Відстежити появу ARP-запиту та ARP-відповіді.
5. Проаналізувати:
- Хто відправив ARP-запит?
- На яку MAC-адресу він був націлений?
- Яка MAC-адреса була повернута у відповіді?
6. Зробити висновок: як працює механізм «запит–відповідь» у ARP?

Тести з теми «Технології автоматизації»

1. Для чого використовується протокол ARP?

A. Для шифрування пакетів у мережі
B. Для визначення MAC-адреси за IP-адресою
C. Для призначення IP-адрес клієнтам
D. Для маршрутизації між підмережами

2. На яку адресу надсилається ARP-запит?

A. На адресу відправника
B. На уніфіковану адресу шлюзу
C. На широкомовну MAC-адресу
D. На довільну MAC-адресу

3. Чому ARP-запит не проходить через маршрутизатор?

A. Тому що ARP забороняє маршрутизаторам пересилати пакети
B. Тому що маршрутизатори працюють лише з DNS
C. Тому що ARP знаходиться нижче мережного рівня
D. Тому що ARP-пакети надто великі

4. Яке значення в полі «операція» відповідає ARP-відповіді?

A. 0
B. 1
C. 2
D. 3

5. Для чого використовується Gratuitous ARP?

A. Для перевірки канального рівня
B. Для оповіщення мережі про нову IP-адресу та виявлення конфлікту IP
C. Для шифрування ARP-пакетів
D. Для прискорення маршрутизації між підмережами

Тема 10 Технологія NAT

Ключові поняття: Network Address Translation, внутрішні та зовнішні IP-адреси, динамічний NAT, статичний NAT, порт.

10.1 Network Address Translation

Трансляція мережних адрес (Network Address Translation) (NAT) – це технологія заміни IP-адрес і портів в заголовку ір пакета. Найчастіше NAT використовується, щоб замінити IP-адресу внутрішньої мережі на IP-адресу із зовнішньої мережі. Це робиться, щоб подолати брак IPv4 адрес.

Зовнішні IP-адреси – це звичайні адреси, які можна застосовувати в інтернет. Вони мають бути унікальними у всьому світі, їх не можна використовувати просто так. Потрібно отримувати дозвіл корпорації ICANN, в одного з її регіональних реєстраторів.

Проблема із зовнішніми адресами у протоколі IPV4 у тому, що їх не вистачає для сучасного масштабу інтернету. Адреса IPV4 приблизно 4 млрд., а зараз пристроїв в інтернеті набагато більше.

Внутрішні IP-адреси це три спеціальні, діапазони IP-адрес, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 які можна використовувати для створення внутрішніх або приватних мереж. Діапазони визначені в документі RFC 1918. Ці адреси не можуть використовуватися в інтернеті, проте їх можна застосовувати у своїй мережі без звернення до ICANN. Різні приватні мережі можуть використовувати одні й самі діапазони внутрішніх IP-адрес.

Приклад використання NAT

Припустимо, у нас є мережа організації, в якій використовуються внутрішні адреси з діапазону 192.168.1.0. Є Інтернет, в якому такі адреси використовувати не можна і внутрішня мережа, що підключається до інтернету через пристрій NAT.

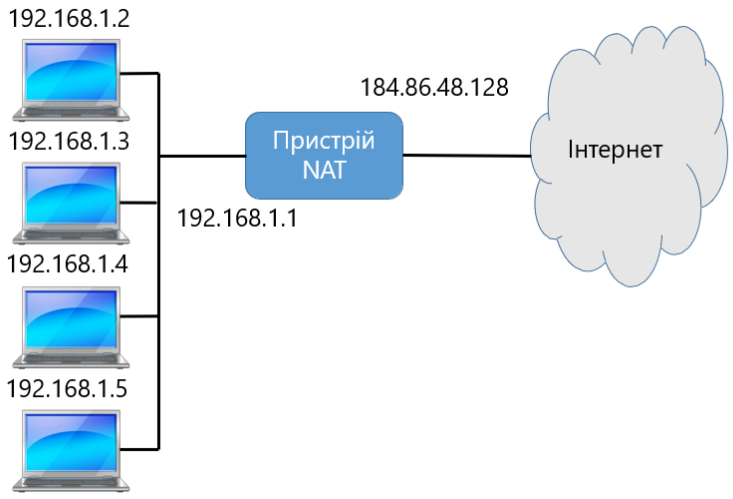


Рисунок 4.6 – Робота мережі за технологією NAT

Пристрій NAT має одну зовнішню IPV4 адресу 184.86.48.128 (рис.4.6) і коли комп'ютери з внутрішньої мережі хочуть підключитися до інтернету, пристрій NAT перетворює IP-адреси з внутрішньої мережі на IP-адресу зовнішньої мережі.

Є багато різних варіантів технології NAT. Ми розглянемо 3 типи, які найчастіше використовуються. Однак, крім них, є й інші можливі варіанти.

10.1.1 Статичний NAT

Перший тип це статичне відображення IP-адрес один до одного. У цьому випадку нам потрібно мати стільки ж зовнішніх адрес, скільки і комп'ютерів у внутрішній мережі. тобто. 4 комп'ютери та 4 IP-адреси в нашому випадку. І у нас фіксоване відображення внутрішніх адрес у зовнішні IP-адреси (рис.4.7).

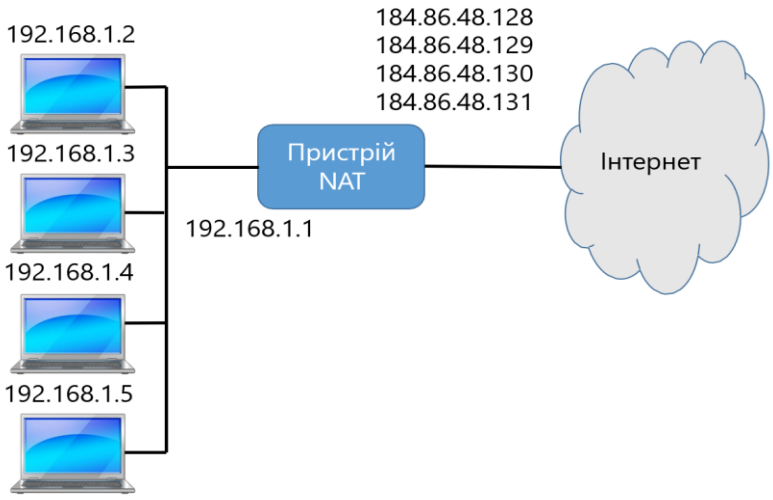


Рисунок 4.7 – Статичне перетворення адрес

Така схема використовується рідко і вона можлива, коли Ви підключаєте мережу організації не до інтернету, а до якоїсь іншої організації, де теж використовуються внутрішні IP-адреси і можливий конфлікт IP-адрес.

10.1.2 Динамічний NAT

Другий варіант це динамічне перетворення, коли набір внутрішніх IP-адрес відображається на групу зовнішніх IP-адрес. У разі динамічного NAT у нас є кілька зовнішніх IP-адрес, які по черзі використовуються різними комп'ютерами з внутрішньої мережі. Наприклад, спочатку комп'ютер 1 використовує першу адресу, а комп'ютер 3 другий адресу.

Через деякий час, другий комп'ютер може використовувати другу адресу, а третій комп'ютер – першу адресу. Отже, перетворення виконується динамічно.

Один до багатьох (masquerading)

Третій варіант, який найчастіше використовується це, коли всі адреси з внутрішньої мережі, відображаються на один зовнішній IP-адресу.

Розглянемо, як працює варіант NAT one-to-many , тому що за його допомогою, можна підключати до інтернету великі мережі організацій, використовуючи одну зовнішню IP-адресу (184.86.48.128) (рис.4.8). Саме це дозволяє частково пом'якшити проблему нестачі адрес IPv4.

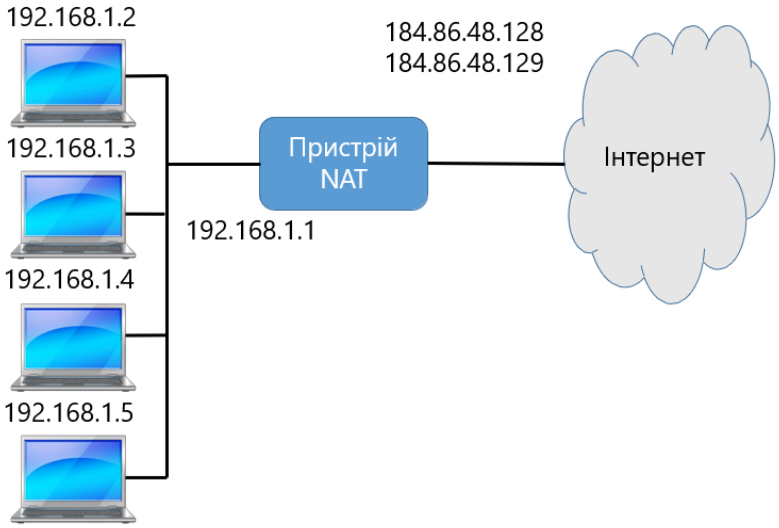


Рисунок 4.8 – Динамічне перетворення адрес

Перетворення або трансляція мережних адрес реалізується за допомогою таблиці NA (рис. 4.9)Т, яка знаходиться всередині пристрою NAT.

Внутрішній IP	Внутрішній порт	Зовнішній IP	Зовнішній порт
192.168.1.2	50300	184.86.48.128	49127
192.168.1.3	52001	184.86.48.128	49128
192.168.1.2	49238	184.86.48.128	49129

Рисунок 4.9 – Таблиця NAT

10.1.3 Робота NAT

Як працює NAT в режимі masquerading ? Припустимо, перший комп'ютер вирішив зайти на сайт. Він відправляє пакет, в IP- адресі вказується IP- адреса комп'ютера з внутрішньої мережі (192.168.1.2), в полі порт вказується динамічний порт, виданий браузеру операційною системою (57160). І пакет призначений для 80 портів адреси Веб-сайту.

Але, оскільки адреси із внутрішньої мережі не можуть використовуватися в інтернеті, то пристрою NAT потрібно замінити IP-адресу з внутрішньої мережі в заголовку пакета на адресу відправника (192.168.1.1), на IP-адресу із зовнішньої мережі (184.86.48.128).

Як це робить пристрій NAT? Після того, як пристрій NAT отримав пакет, воно записує внутрішній IP-адресу та внутрішній порт у таблицю і генерує пару зовнішню адресу та зовнішній порт для заміни в пакеті. Так як у нас лише одна зовнішня адреса, то саме він записується в полі зовнішній ip . Зовнішній порт генерується випадковим чином. Пристрій нат згенерував адресу поту 48202 (рис.4.10).

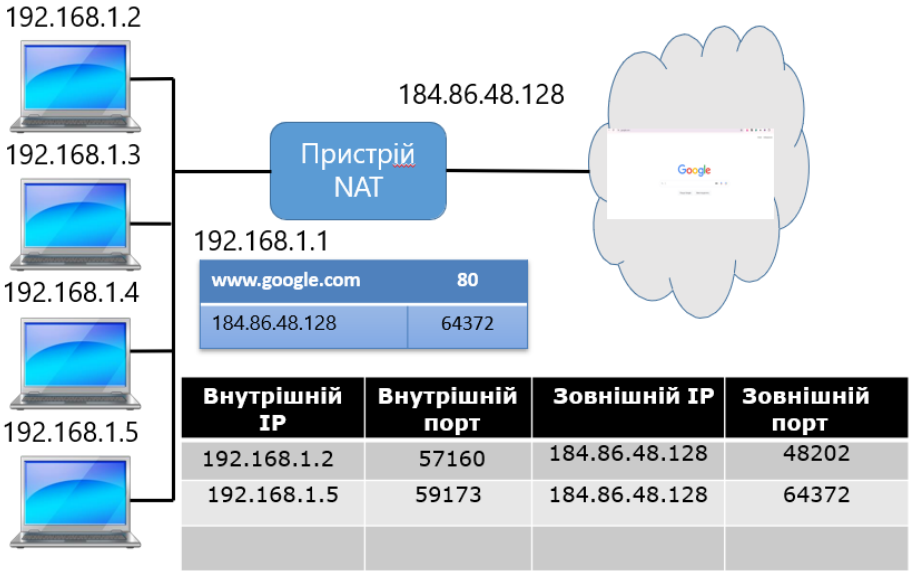


Рисунок 4.10 – Процес захаповнення таблиці NAT

Наступного етапі відбувається трансляція, тобто. заміна IP-адреси та порту. IP-адреса і порт відправника видаляються з пакета і їх місце записуються нові дані з таблиці NAT . Зовнішній IP-адресу пристрою NAT і зовнішній порт, який пристрій NAT згенерував випадковим чином.

У такому вигляді пакет передається на веб-сервер. Коли надходить відповідь від веб-сервера, там як одержувач, вказується IP-адреса пристрою NAT і порт на цьому пристрої.

Але насправді ці дані призначені задля пристрою NAT , а комп'ютера внутрішньої мережі. Тому пристрій нат повинен зрозуміти якого комп'ютера у внутрішній мережі призначені дані. Потім змінити IP-адресу та порт, передати дані потрібному комп'ютеру. Це робиться за допомогою таблиці NAT .

У таблиці NAT шукається запис в якій зовнішній IP-адресу і зовнішній порт, такі ж як у пакеті, що надійшов. Поки у нас у таблиці один запис, тому пристрій NAT бере з цього запису внутрішню IP-адресу комп'ютера, що цікавить нас, і його порт. Пристрій NAT знову робить заміну IP-адреси і порту в пакеті і в такому вигляді передає пакет у внутрішню мережу.

Що відбувається якщо в інтернет захоче зайти якийсь інший комп'ютер, припустимо, що комп'ютер 4 теж хоче зайти на веб-сайт zvondozvon.ru. Пристрій NAT працює аналогічно, витягує IP-адресу і порт, записує в таблицю NAT . Як зовнішній IP-адреса вказується єдиний зовнішній IP-адресу пристрою NAT і номер зовнішнього порту знову генерується випадковим чином.

Адреса та порт із внутрішньої мережі змінюються на адресу та порт із зовнішньої мережі. І в такому вигляді пакет передається до інтернету.

Коли надходить відповідь від веб-сервера, знову виконується пошук пари зовнішню IP-адресу та зовнішній порт. У таблиці NAT шукається відповідні їм внутрішній адресу ір і внутрішній порт. Замінюється в заголовку пакета і пакет передається у внутрішню мережу. Можете подивитись відео, якщо щось було не зрозуміло.

10.1.4 Переваги NAT

Ця технологія довго дозволяла справлятися з нестачею IPv4 адрес. Ви можете підключити до інтернет мережу великої організації, де багато комп'ютерів, за допомогою лише однієї зовнішньої адреси IPv4.

Цю технологію легко розгорнути та використовувати, Вам потрібно лише один пристрій NAT та адреси для внутрішньої мережі. Ви можете вільно використовувати з діапазону приватних адрес не звертаючись до ICANN.

Додаткова перевага у безпеці, технологія NAT приховує внутрішню структуру мережі від зовнішнього світу. Для зовнішнього світу є лише одна адреса IPv4, а що встановлено всередині мережі, з внутрішніми адресами ніхто не бачить.

10.1.5 Недоліки NAT

Однак NAT має низку істотних недоліків. Перший теоретичний недолік, полягає в тому, що порушення фундаментального принципу побудови IP - мереж, в яких кожен комп'ютер повинен мати можливість з'єднуватися з будь-яким іншим комп'ютером.

Наслідком цього теоретичного недоліку є ряд практичних. Наприклад, немає можливості підключитися із зовнішнього світу до комп'ютерів у внутрішній мережі. З зовнішнього світу видно лише одну IP-адресу і неможливо зрозуміти, що насправді за цією IP-адресою знаходиться велика кількість інших пристроїв.

Деякі протоколи, які розроблялися в ранні роки створення інтернету, і розраховані на те, що кожен пристрій може з'єднатися з кожним, у випадку з NAT працюють погано. Наприклад, погано працює протокол FTP, який використовує два з'єднання, одне керування, інше передачі даних. З'єднання даних зазвичай встановлюється сервером, якщо клієнт перебуває за пристроєм NAT , то сервер FTP неспроможна встановити з ним з'єднання передачі даних.

Погано працюють протоколи, які не встановлюють з'єднання. Для яких немає можливості зберегти запис у таблиці NAT на весь час з'єднання.

Додатковий недолік у тому, що немає єдиного стандарту NAT , а є багато різних варіантів, які підтримуються різними виробниками обладнання та їхнього ПЗ, все це вносить плутанину і призводить до несумісності.

10.1.6 Вирішення проблем з NAT

Як можна вирішити проблеми з NAT ? Якщо Ви хочете мати можливість потрапити із зовнішнього світу до внутрішньої мережі, то для цього можна використовувати статичне відображення, яке ми вже розглядали вище.

Можна використовувати відображення один до одного, але для цього потрібно мати декілька зовнішніх адрес ip .

Також можна використовувати статичне відображення портів. Наприклад, порт 80 на пристрої NAT відображається у внутрішню адресу сервера і порт 80. Порт 25, який використовується для електронної пошти відображається у внутрішню адресу поштового сервера і порт 25. У цьому випадку ми маємо одну IP-адресу, але різні його порти відображаються в різні пари, IP-адреса і порт, у внутрішній мережі.

Є технологія NAT Traversal , яка дозволяє встановлювати з'єднання з комп'ютерами у внутрішній мережі без Інтернету. Вона визначена у стандарті RFC 3489. Є й інші варіанти такої технології. Така технологія часто використовується в програмах передачі відео та голосу, наприклад Skype.

❓Контрольні запитання:

1. Що таке технологія NAT і для чого вона застосовується в комп’ютерних мережах?
2. Чим відрізняються внутрішні IP-адреси, визначені в RFC 1918, від зовнішніх IP-адрес?
3. У чому полягає різниця між статичним NAT, динамічним NAT та режимом one-to-many (masquerading)?
4. Як таблиця NAT допомагає пристрою правильно обробляти пакети, що повертаються з інтернету у внутрішню мережу?
5. Назвіть два основних недоліки NAT і поясніть, як вони впливають на роботу деяких мережевих протоколів (наприклад, FTP).

✍Практичні завдання:

Завдання 1.

У таблиці NAT записані такі відповідності:

Внутрішня IP	Внутрішній порт	Зовнішня IP	Зовнішній порт
192.168.1.10	54231	184.86.48.128	40012
192.168.1.12	49800	184.86.48.128	50133

1. Який внутрішній комп’ютер має отримати пакет, якщо з інтернету прийшов пакет на IP **184.86.48.128:50133**?

2. Поясніть, чому пристрій NAT може мати одну зовнішню IP-адресу, але обслуговувати багато комп’ютерів.

Завдання 2.

У мережі використовується NAT. Відомо, що:

- в організації є **20 комп’ютерів**;
- зовнішніх IP-адрес є **2**;
- при кожному новому з’єднанні внутрішній комп’ютер може отримати будь-яку з доступних зовнішніх адрес, і це не завжди одна й та сама адреса.

1. Визначте, який тип NAT використовується (статичний NAT, динамічний NAT чи one-to-many).
2. Поясніть, чому саме цей тип відповідає описаній ситуації.

Тести з теми «Технологія NAT»

1. Для чого найчастіше використовується технологія NAT?

A. Для прискорення передачі файлівB. Для заміни внутрішніх IP-адрес на зовнішні
C. Для шифрування мережевого трафіку
D. Для збільшення швидкості роботи роутера

2. Які IP-адреси належать до приватних (внутрішніх)?

A. 8.8.8.8
B. 172.16.0.0 – 172.31.255.255
C. 150.10.0.0 – 150.10.255.255
D. 1.1.1.1

3. Який тип NAT потребує стільки ж зовнішніх IP-адрес, скільки комп’ютерів у внутрішній мережі?

A. One-to-many (masquerading)
B. Динамічний NAT
C. Статичний NAT
D. Порт форвардинг

4. Який механізм дозволяє багатьом комп’ютерам використовувати одну зовнішню IP-адресу?

A. ICMP Redirect
B. Маскування (masquerading)
C. ARP трансляція
D. PPP

5. Який недолік пов’язаний з NAT?

A. Підвищення продуктивності серверів
B. Складність маршрутизації всередині приватних мереж
C. Неможливість встановити деякі типи з’єднань із зовнішнього світу
D. Неможливість використання RFC-адрес

ПРЕДМЕТНИЙ ПОКАЖЧИК

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Tanenbaum A., Wetherall D. Computer Networks, Global Edition 6th Edition. Pearson, 2021.
2. Peterson L., Davie B. Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition. Morgan Kaufmann, 2021. 848 p.
3. Worley R. Computer Networking Bible. Paperback, 2023. 161 p.
4. Scott R.Networking for Beginners. Independently published, 2019. 111 p.
5. Gaber H.Understanding Computer Networks. Paperback, 2020. 355 p.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі : навч. посіб. Ч. 1. Київ : КПІ ім. І. Сікорського, 2020. 328 с.

2. Жураковський Б. Ю., Зенів І. О. Комп’ютерні мережі : навч. посіб. Ч. 2. Київ : КПІ ім І. Сікорського, 2020. 372 с.

3. Комп'ютерні мережі, інтернет-технології : курс лекцій / уклад.: В. М. Русскін, Н. А. Хміль. Харків : ХГПА, 2022. 120 с.

4. Gaber H.Understanding Computer Networks. Paperback, 2020. 355 p.

5. Lowe D. Networking All-in-One For Dummies, 2021. 1056 p.

ЗМІСТ

Навчальне видання
(українською мовою)

Решевська Катерина Сергіївна

КОМП’ЮТЕРНІ МЕРЕЖІ

Навчальний посібник
для здобувачів ступеня вищої освіти бакалавра
спеціальності «Комп’ютерні науки»
освітньо-професійної програми «Комп’ютерні науки»

Рецензент С.Ю. Борю
Відповідальний за випуск О. С. Пшенична
Коректор К. С. Решевська