

Державний вищий навчальний заклад
«Запорізький національний університет»
Міністерства освіти і науки України

А.О. Лісняк, С.В. Чопоров, О.С. Козлова, К.С. Решевська

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Методичні вказівки до лабораторних занять для студентів
освітньо-кваліфікаційного рівня «бакалавр» напрямку
підготовки «Програмна інженерія»

Затверджено
вченою радою ЗНУ
Протокол № 3 від 28.10.2014

Запоріжжя
2014

УДК: 004.7(076.6)

ББК: 3973.202-Д18.2я73

О -751

Лісняк А.О. Організація комп'ютерних мереж: методичні вказівки до лабораторних занять для студентів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки «Програмна інженерія» / А.О. Лісняк, С.В. Чопоров, О.С. Козлова, К.С. Решевська. – Запоріжжя: ЗНУ, – 2014. – 60 с.

Методичні вказівки до лабораторних занять з дисципліни «Організація комп'ютерних мереж» пропонуються студентам, що навчаються за програмою освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050103 – «Програмна інженерія» містять теоретичні матеріали, приклади, лабораторні роботи, завдання, контрольні питання та тести для самоконтролю. Увага студентів акцентується на розширенні теоретичних знань та набутті практичних навичок створення, налагодження та тестування сучасних комп'ютерних мереж.

Методичні вказівки призначені для студентів та будуть корисними для викладачів, а також усіх, хто цікавиться питаннями зазначеної тематики.

Рецензент

С.М. Гребенюк

Відповідальний за випуск

А.О. Лісняк

Зміст

Вступ	4
Загальні вказівки.....	5
Лабораторна робота №1. Мережеві інструменти операційних систем	6
Лабораторна робота №2. Використання протоколів	10
прикладного рівня	10
Лабораторна робота №3. Детальний огляд основних рівнів OSI та стека протоколів TCP/IP	15
Лабораторна робота №4. Мережеві пристрої.....	20
Лабораторна робота №5. Кодування цифрових сигналів.....	25
Лабораторна робота №6. Логічна адресація	30
Лабораторна робота №7. Створення підмереж	34
Лабораторна робота №8. Локальна мережа з динамічною адресацією	39
Лабораторна робота №9. Налаштування бездротового	43
маршрутизатора.....	43
Лабораторна робота №10. Статична маршрутизація.....	48
Контрольні завдання та тести	51
Предметний покажчик	57
Рекомендована література	59

Вступ

Комп'ютерні мережі є результатом еволюції двох важливих науково-технічних галузей – комп'ютерних та телекомунікаційних технологій і у сучасному світі є одним з найпоширеніших засобів обміну інформацією. Саме завдяки комп'ютерним мережам можливі такі явища, як інформаційні ресурси Інтернет, соціальні мережі, IP-телефонія, IP-телебачення, сервіси електронної пошти, голосовий та відеозв'язок тощо. Роботу різних підприємств, навчальних та наукових закладів складно уявити без використання сучасних мережевих технологій. Кількість користувачів локальних та глобальних мереж активно збільшується, що вимагає відповідного рівня апаратного та програмного забезпечення, захисту інформації й, звичайно, кваліфікованих спеціалістів.

Мета курсу: сформувати теоретичні та практичні знання в галузі організації комп'ютерних мереж у студентів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050103 – «Програмна інженерія», які можуть бути використані при подальшому навчанні, професійній, виробничій та науковій діяльності. Курс «Організація комп'ютерних мереж» базується на дисциплінах «Архітектура комп'ютера», «Основи програмування та інформаційна культура студента» та «Організація і функціонування ЕОМ». Отримані теоретичні та практичні знання можуть бути використані у професійній, виробничій та науковій діяльності, є базовими для опанування курсів «Інтернет-технології», «Технології та протоколи Інтернет», «Web-технології програмування» та інших дисциплін, що викладаються на математичному факультеті

Методичні вказівки містять 10 лабораторних робіт, контрольні питання та тести для самостійного контролю.

Завдання навчальної дисципліни: ознайомити студента з історичними аспектами виникнення та розвитку обчислювальних мереж; допомогти засвоїти основні поняття та теоретичні основи функціонування сучасних комп'ютерних мереж; навчити механізмам роботи мережевих пристроїв. Студенти повинні опанувати принципи мережевої адресації; набути практичного досвіду проектування, тестування й аналізу роботи локальних та глобальних мереж передачі даних.

Загальні вказівки

1. Лабораторні роботи виконуються в години, зазначені в розкладі і для кожного студента присутність на занятті є обов'язковою. Студенту, що пропустив лабораторне заняття без поважних причин і не захистив лабораторну роботу на наступному занятті, виставляється незадовільна оцінка з відповідної лабораторної роботи.

2. У комп'ютерний клас дозволяється входити тільки після дзвінка на заняття й у присутності викладача.

3. Вхід у комп'ютерний клас дозволяється тільки за наявності документа, що засвідчує особу і завірений відповідальним органом ЗНУ.

4. Лабораторну роботу припиняють виконувати за дзвінком.

5. Забороняється виходити з аудиторії без дозволу викладача.

Вимоги до виконання лабораторних робіт

1. Ознайомитися із загальними теоретичними відомостями.

2. За номером варіанта¹ обрати завдання.

3. Уважно прочитати завдання.

4. Кожну роботу виконувати відповідно до завдання.

5. Оформити друкований звіт з виконання лабораторної роботи, який повинен містити:

- титульний лист;
- тему роботи;
- схеми основних моделей та алгоритмів;
- опис виконання роботи;
- висновки.

6. При необхідності захистити результати, відповісти на контрольні та додаткові питання.

¹ Номер варіанта визначає викладач.

Лабораторна робота №1. Мережеві інструменти операційних систем

Мета: навчитися використовувати основні мережеві інструменти операційних систем сімейства Windows та Linux.

Теоретичні відомості

Комп'ютерна мережа – сукупність об'єктів, що створена пристроями для передачі та обробки даних.

Для фізичного підключення до мережі необхідним є **мережевий адаптер** – частина апаратного забезпечення, яка дозволяє комп'ютеру підключатися до мережі. Кожен мережевий адаптер має **MAC-адресу** – 6 дворозрядних шістнадцяткових чисел, розділених тире або двокрапкою які є обов'язковими для будь якого порту або пристрою, що під'єднаний до локальної комп'ютерної мережі (наприклад: 15-EF-A3-45-9B-57).

На додаток до фізичного підключенню для ідентифікації кожного комп'ютера в мережі використовується мережева IP-адреса. Щоб комп'ютер зміг обмінюватися даними через IP-мережу, необхідно правильно налаштувати наступні параметри:

- **ім'я комп'ютера** – зручна назва, яка полегшує користувачам доступ до загальних ресурсів;
- **IP-адреса** – унікальний ідентифікатор комп'ютера в мережі;
- **маска підмережі** – параметр, що дозволяє визначити адресу локальної підмережі;
- **шлюз за замовченням** – IP-адреса пристрою в локальній підмережі, через який локальна підмережа і комп'ютер підключаються до Інтернету або інший IP-мережі.

Зазвичай ці параметри налаштовують власноруч, але деякі з них можна привласнити автоматично. При ручному конфігуруванні мережевий адміністратор (як правило) вводить в комп'ютер необхідні значення з клавіатури. При автоматичному – параметри отримуються за спеціальним запитом від сервера динамічної роздачі мережевих адресів(DHCP).

Перевірка мережевого зв'язку, отримання та встановлення мережевих параметрів, визначення проблем у роботі є поширеними завданнями при роботі у локальній комп'ютерній мережі. Сучасні мережеві операційні системи мають вбудовані інструменти, які дозволяють вирішувати подібні завдання з використання командної стрічки або графічного інтерфейсу.

Основні утиліти для роботи у командній стрічці сімейства операційних систем Windows представлено у таблиці 1.1.

Таблиця 1.1 – Основні утиліти ОС Windows

Команда	Опис команди
ping	перевіряє коректність конфігурації протоколу TCP/IP і доступність іншого хоста
ipconfig	відображає конфігурацію протоколу TCP/IP включаючи адреси серверів DHCP, DNS і WINS.
hostname	повертає ім'я локального комп'ютера для аутентифікації
nslookup	дозволяє переглядати записи в базі даних сервера DNS, що відносяться до того чи іншого вузла або домену
route	переглядає або змінює локальну таблицю маршрутизації
tracert	простежує маршрут від локального до віддаленого вузла
net view	використовується для перегляду списку ресурсів комп'ютера або мережі; виводить список доменів, комп'ютерів або загальних ресурсів, доступних на певному комп'ютері.
arp	відображає локальний кеш відповідностей IP-адрес адресам мережевих адаптерів

Завдання 1

- Визначити ім'я локального комп'ютера, використовуючи команду *hostname*.
- За допомогою утиліти *ipconfig* для вашого комп'ютера знайти:
 - MAC-адресу;
 - IP-адресу;
 - IP-адресу шлюзу;
 - IP-адреси сервера DNS;
 - IP-адресу сервера DHCP;
 - ім'я хоста;
 - DNS-ім'я локального комп'ютера.
- Використовуючи команду *net view*, визначити:
 - перелік доступних доменів мережі;
 - доступні мережеві ресурси (комп'ютери та інші доступні пристрої мережі);
 - доступні ресурси вашого комп'ютера (мережеві папки, принтери та інше);
 - доступні ресурси п'яти хостів локальної мережі.
- Використовуючи команди утиліти *nslookup*, отримати всі записи DNS сервера _____.

5. Виконати команду *ping* для перевірки з'єднання з п'ятьма сусідніми вузлами мережі.

6. Для п'яти хостів (з попереднього пункту) у комп'ютерному залі знайти MAC-адреси. Для перегляду інформації в локальному кеші використати команду *arp -a*

7. Отримати таблицю мережевих маршрутів використовуючи команду *route* та команди утиліти *nbtstat*.

8. Простежити маршрут від локального до віддалених вузлів (п'ять довільних пошукових систем), використовуючи команду *tracert*.

9. За результатами виконаної роботи оформити звіт і заповнити в ньому таблицю 1.2.

Таблиця 1.2. – Результати виконання роботи

Команда	Результат роботи
Завдання 1	
<i>Опис команди / утиліти</i>	
Копія командної стрічки	Результат роботи команди
Завдання 2	
<i>Опис команди / утиліти</i>	
Копія командної стрічки	Результат роботи команди
...	

Завдання 2

1. Самостійно ознайомитися та проаналізувати мережевий інструментарій операційної системи Linux.

2. Виконати всі пункти завдання 1 в операційній системі Linux.

Контрольні питання

1. Як визначити ім'я комп'ютера в мережі?
2. Як протестувати з'єднання хоста з довільним вузлом комп'ютерної мережі?
3. Як отримати фізичну (MAC) адресу будь-якого доступного вузла мережі?

4. Чи можливо використовувати вивчені мережеві команди та утиліти у глобальній мережі Інтернет?
5. Скільки MAC-адресів може мати хост?
6. Наведіть приклад IP-адреса.
7. Які параметри має команда *ipconfig*?

Лабораторна робота №2. Використання протоколів прикладного рівня

Мета: отримання практичних навичок роботи з протоколами прикладного рівня еталонної моделі OSI.

Теоретичні відомості

Протокол – це сукупність правил, які визначають формат і процедури обміну інформацією між двома або кількома пристроями.

Telnet – мережевий протокол, який використовується в Інтернеті та локальних мережах для підключення до віддалених пристроїв. Як правило, застосовується з метою налагодження та діагностики.

У таблиці 2.1 наведено перелік та опис найнеобхідніших команд Telnet.

Таблиця 2.1 – Основні команди Telnet

Команда	Дія
<i>open</i> або <i>o</i>	Встановити підключення Telnet до головного комп'ютера або віддаленого сервера.
<i>close</i> або <i>c</i>	Закрити наявне підключення Telnet.
<i>quit</i> або <i>q</i>	Завершити сеанс Telnet.
<i>CTRL+]</i>	Перейти до командного рядка Telnet із сеансу підключення.
<i>enter</i>	Перейти до підключеного сеансу (якщо такий є).
<i>?</i> / <i>help</i>	Переглянути довідку.

FTP (File Transfer Protocol) – протокол передачі файлів який працює на рівні додатків еталонної моделі OSI і дає можливість обмінюватися бінарними та текстовими файлами з будь-якими комп'ютерами мережі, що підтримують даний протокол.

Особливість FTP в тому, що він використовує два TCP з'єднання.

1. Керуюче з'єднання встановлюється як звичайне з'єднання клієнт-сервер. Сервер здійснює пасивне відкриття на заздалегідь відомий порт FTP (21) і очікує запиту на з'єднання від клієнта. Клієнт здійснює активне відкриття на TCP порт 21, щоб встановити керуюче з'єднання. Керуюче з'єднання існує весь час, поки клієнт спілкується з сервером. Це з'єднання використовується

для передачі команд від клієнта до сервера і для передачі відповідей від сервера.

2. З'єднання даних відкривається щоразу, коли здійснюється передача даних (файли, список вмісту директорії) між клієнтом і сервером.

На рис. 2.1 показано взаємодія клієнта та сервера за двома варіантами.

При створенні з'єднання для передачі даних використовується два режими:

- *пасивний* – клієнт буде з'єднуватись з портом, що пропонується сервером;
- *активний* – сервер буде з'єднуватись з 20 портом клієнта.

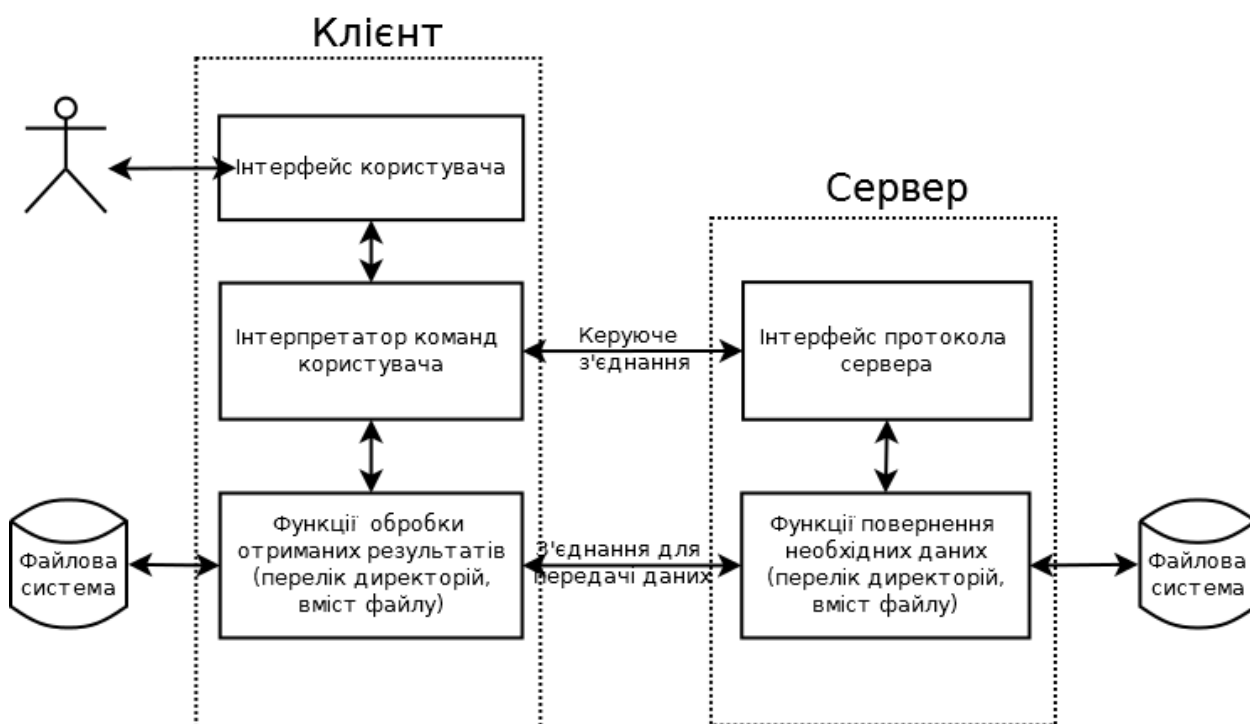


Рисунок 2.1 – Взаємодія клієнта та сервера за протоколом FTP

Існує три способи використання з'єднання даних:

- відправка файлів від клієнта до сервера;
- відправка файлів від сервера до клієнта;
- відправка списку файлів або директорій від сервера до клієнта.

Основні команди протоколу FTP наведено у таблиці 2.2.

Таблиця 2.2 – Основні команди FTP

Команда	Опис
ABOR	Перервати передачу файлу.
CDUP	Змінити директорію на один рівень вище.
CWD	Змінити директорію.
DELE	Видалити файл (DELE filename).

EPSV	Увійти в розширений пасивний режим. Застосовується замість PASV.
HELP	Виводить список команд, прийнятих сервером.
LIST	Повертає список файлів директорії. Список передається через з'єднання даних.
MDTM	Повертає час модифікації файлу.
MKD	Створити директорію.
NLST	Повертає список файлів директорії в більш короткому форматі, ніж LIST. Список передається через з'єднання даних.
NOOP	Порожня операція.
PASV	Увійти в пасивний режим. Сервер поверне адресу і порт, до якого потрібно підключитися, щоб забрати дані. Передача почнеться при введенні таких команд як: RETR, LIST.
PORT	Увійти в активний режим. Наприклад PORT 12,34,45,56,78,89. На відміну від пасивного режиму для передачі даних сервер сам підключається до клієнта.
PWD	Повертає поточну директорію.
QUIT	Від'єднатися.
REIN	Реініціалізувати підключення.
RETR	Завантажити файл. Перед RETR має бути команда PASV або PORT.
RMD	Видалити директорію.
RNFR і RNT0	Перейменувати файл. RNFR – що перейменувати, RNT0 – в що.
SIZE	Повертає розмір файлу.
STOR	Відправити файл. Перед STOR має бути команда PASV або PORT.
SYST	Повертає тип системи (UNIX, WIN, ...).
TYPE	Встановити тип передачі файлу (бінарний, текстовий).
USER	Ім'я користувача для входу на сервер.

Після виконання команди сервер повертає код відповіді – тризначне число. Перша цифра відповідає за один з трьох результатів: успіх, відмова або вказівка на помилку чи неповну відповідь (табл. 2.3). Друга цифра визначає тип помилки, а третя – остаточно визначає помилку.

Таблиця 2.3 Основні коди відповідей FTP.

Перша цифра	
Код	Опис
2xx	Успішна відповідь.

4xx / 5xx	Команда не може бути виконана.
1xx / 3xx	Помилка або неповна відповідь.
Друга цифра – визначає тип помилки	
Код	Опис
x0z	Синтаксична.
x1z	Інформаційне повідомлення.
x2z	Повідомлення відноситься до керуючого з'єднання або до з'єднання даних.
x3z	Повідомлення про аутентифікацію користувача і його права.
x4z	Не визначено.
x5z	Повідомлення файлової системи.

Приклад. Отримати список файлів кореневої директорії FTP сервера використовуючи telnet-клієнт та пасивний режим передачі даних.

На рис. 2.2 наведено перелік команд керуючого з'єднання та список файлів отриманий у з'єднанні для передачі даних.

Керуюче з'єднання

```
C:>telnet 192.168.1.4 21
220 (vsFTPD 3.0.2)
USER ftpuser
331 Please specify the password.
PASS ftpuser
30 Login successful.
PASV
227 Entering Passive Mode
(192,168,1,4,181,135).
LIST
150 Here comes the directory listing.
226 Directory send OK.
QUIT
221 Goodbye.
```

З'єднання для передачі даних

```
C:>telnet 192.168.1.4 46471 (=181*256+135)
-rw----- 1 1001 1001 29 Sep 23 17:18 filename.txt
drwxr-xr-x 3 1001 1001 4096 Sep 23 16:45 students
drwxr-xr-x 2 1001 1001 4096 Sep 23 14:28 documents
drwxr-xr-x 2 1001 1001 4096 Sep 23 14:28 books
drwxr-xr-x 2 1001 1001 4096 Sep 23 14:28 install
```

Рисунок 2.2 – Приклад роботи за протоколом FTP

Завдання

1. За допомогою telnet-клієнта з'єднатися з доступним FTP сервером (сервер: _____, користувач: _____, пароль користувача _____)

_____), та використовуючи команди протоколу передачі файлів виконати наступні операції:

- отримати перелік директорій та файлів кореневої папки FTP-сервера²;
- перейти до папки з номером групи;
- створити а потім перейти до папки з ім'ям, що відповідає Вашому прізвищу англійською мовою;
- створити декілька текстових файлів (first.txt, second.txt, about.txt) вміст яких відповідає їх назвам;
- перейменувати файл about.txt на файл info.txt;
- завантажити файли info.txt та second.txt;
- створити та видалити директорію з ім'ям test.

2. За результатами виконання роботи скласти та захистити звіт, що відображає всі етапи виконання завдання: команди та відповіді протоколу керуючого з'єднання і з'єднання для передачі даних.

Контрольні питання

1. Що називають протоколом?
2. Які режими роботи FTP-сервером вам відомі?
3. Яка команда FTP призначена для визначення поточної директорії?
4. Який порт призначений для керуючого з'єднання FTP за замовченням?
5. Як отримати порт для встановлення з'єднання та передачі даних при пасивному типі роботи з сервером FTP?

² Тут і надалі для передачі потоку даних використовувати пасивний режим роботи FTP

Лабораторна робота №3. Детальний огляд основних рівнів OSI та стека протоколів TCP/IP

Мета: вивчити рівні еталонної моделі OSI та стека протоколів TCP/IP, процес інкапсуляції та декапсуляції даних.

Теоретичні відомості

Основне завдання будь-якої комп'ютерної мережі – передача інформації.

У загальному вигляді процес обміну інформацією у сучасних комунікаційних мережах можна зобразити у вигляді схеми на рис. 3.1.

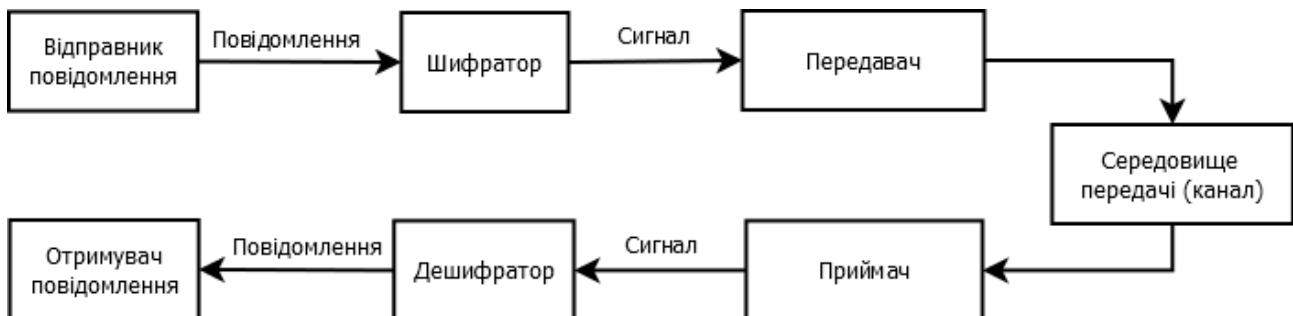


Рисунок 3.1 – Загальна схема процесу обміну повідомленнями.

При відправці повідомлення від джерела повідомлення до адресата необхідно використовувати певний формат або структуру. Наприклад, при листуванні між людьми потрібно не тільки скласти текст листа в правильному форматі, але й запакувати його в конверт для доставки. На конверті, в спеціально відведеному місці, пишеться адреса відправника і одержувача. Подібний процес відбувається і при відправці повідомлення в комп'ютерній мережі.

Процес розміщення одного формату повідомлення (лист) всередині іншого (конверт) називається **інкапсуляцією**. Зворотний процес, або отримання повідомлення (листа) з іншого повідомлення (конверта) називається **декапсуляцією**.

Для кожного повідомлення використовується особливий формат, який називається **кадром**. Кадр діє подібно конверту; в ньому зазначені адреси вузла-відправника та одержувача.

Якщо повідомлення занадто велике, його необхідно поділити на частини. Кожна частина інкапсулюється в окремий кадр та передається у мережі. Вузол-адресат розпаковує повідомлення і збирає їх разом для обробки та інтерпретації.

У сучасних комп'ютерних мережах формування кадрів та передача даних по каналам зв'язку регламентується технологією Ethernet.

Ethernet – сукупність технологій пакетної передачі даних для комп'ютерних мереж, які визначають проводові з'єднання та електричні сигнали на фізичному рівні, формат кадрів та протоколи управління доступом до середовища.

Для будь-якого обміну даними необхідний спосіб ідентифікації відправника та отримувача. У мережі Ethernet у кожного підключеного вузла існує фізична адреса, яку називають адресою управління доступом до середовища або **MAC-адресою**. MAC-адреси присвоюють в процесі виробництва всім мережевим інтерфейсам Ethernet.

Структура кадру Ethernet представлена у табл. 3.1.

Таблиця 3.1 – Поля кадру стандарту IEEE 802.3 Ethernet

Назва поля	Довжина, байт	Опис
<i>Преамбула</i>	7	Певна послідовність бітів з інформацією, що ідентифікує початок кадру.
<i>Ознака початку кадру (Start of Frame Delimiter - SFD)</i>	1	Утворює окреме поле пакета з інформацією про початок кадру.
<i>MAC-адреса одержувача</i>	6	MAC-адреса одержувача може бути одноадресною та багатоадресною
<i>MAC-адреса відправника</i>	6	MAC-адреса відправника може бути одноадресною та багато адресною.
<i>Довжина / тип</i>	2	Виконує дві функції: визначає тип протоколу, містить інформацію про довжину поля даних.
<i>Інкапсульовані дані</i>	64–1518	Поле даних містить пакет даних, що пересилаються.
<i>Поле контрольної суми (Frame Check Sequence-FCS)</i>	4	Містить 4-байтове значення, створене пристроєм-відправником і перераховується пристроєм-одержувачем для перевірки правильності даних.

Однак передача даних за допомогою кадрів не забезпечує достатнього рівня абстрагування сучасним програмам та сервісам (HTTP-клієнти, офісні програми, клієнти електронної пошти і т.п.). Для успішної взаємодії між вузлами необхідна ефективна взаємодія цілого ряду протоколів. Ці протоколи реалізовані на рівні обладнання та програмного забезпечення кожного мережевого пристрою. Взаємодію між ними можна представити у вигляді стека протоколів. Протоколи стека представляють собою багаторівневу ієрархію, в якій протокол верхнього рівня залежить від сервісів та протоколів на більш низьких рівнях.

Для опису взаємодій між різними протоколами зазвичай застосовують багаторівневу модель, яка описує взаємодію протоколів всередині кожного рівня, а також взаємодію з верхніми і нижніми рівнями. Існує дві мережеві

моделі: стек протоколів TCP/IP та еталонна модель мережевої взаємодії OSI (рис. 3.2).

Модель OSI			Назва PDU	Стек TCP/IP
Верхній рівень	7	Прикладний	<i>Дані / Data</i>	Прикладний
	6	Представлення		
	5	Сеансів		
Нижній рівень	4	Транспортний	<i>Сегмент / Segment</i>	Транспортний
	3	Мережевий	<i>Пакет / Packet</i>	Інтернет
	2	Канальний	<i>Кадр / Frame</i>	Доступ до мережі
	1	Фізичний		

Рисунок 3.2 – Модель OSI та стек TCP/IP

У моделі TCP/IP, для опису інкапсульованих даних різних рівнів, використовуються такі терміни, як **сегмент**, **пакет** та **фрейм** або **кадр**. У моделі OSI використовується більш загальний термін – **протокольний блок даних** або **PDU**.

Процес інкапсуляції даних при передачі від сервера до клієнта з відповідними назвами протокольних блоків даних представлено на рис 3.3.

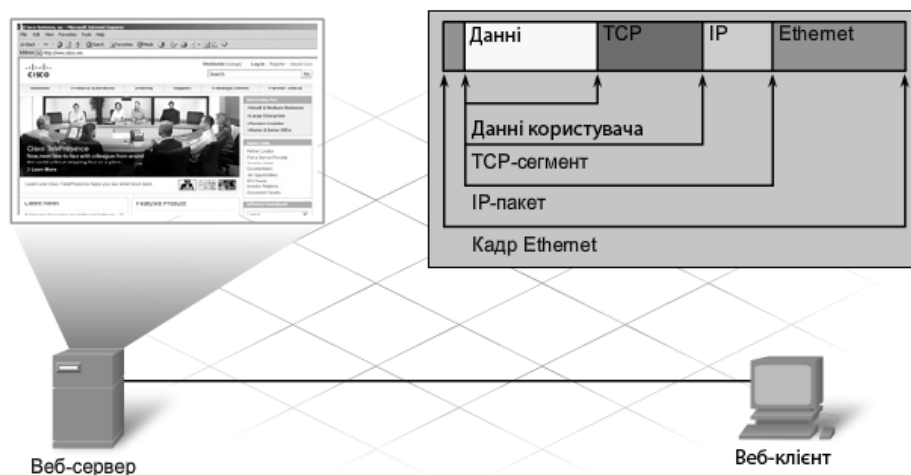


Рисунок 3.3 – Інкапсуляція даних стеку TCP/IP

Завдання 1

Опанувавши теоретичний матеріал за темою, заповнити таблицю 3.2.

Таблиця 3.2 – Опис основних протоколів мережевої 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

Опанувавши теоретичний матеріал та за результатами заповнення таблиці 3.2, заповнити таблицю 3.3

Таблиця 3.3 – Опис основних протоколів відповідних рівнів OSI

№	Протокол	Перелік загальних протоколів та технологій
7	Прикладний	
6	Представлення	
5	Сеансів	
4	Транспортний	

3	Мережевий	
2	Канальний	
1	Фізичний	

Завдання 3

Використовуючи таблицю 3.1, сформувати кадр для передачі даних згідно топології мережі на рис. 3.4. Як дані кадру використати Ваше ПІБ. Значення MAC-адрес X та Y визначити за наступною схемою:

X: $[(A+N) \bmod 16]:[(N+N) \bmod 16]:[N \bmod 16]:[(3*N) \bmod 16]:DF:FF;$

Y: $[(E+N) \bmod 16]:[(2*N+N) \bmod 16]:[(N+3) \bmod 16]:3F:AD:E3.$

N – ваш номер у журналі академічної групи.

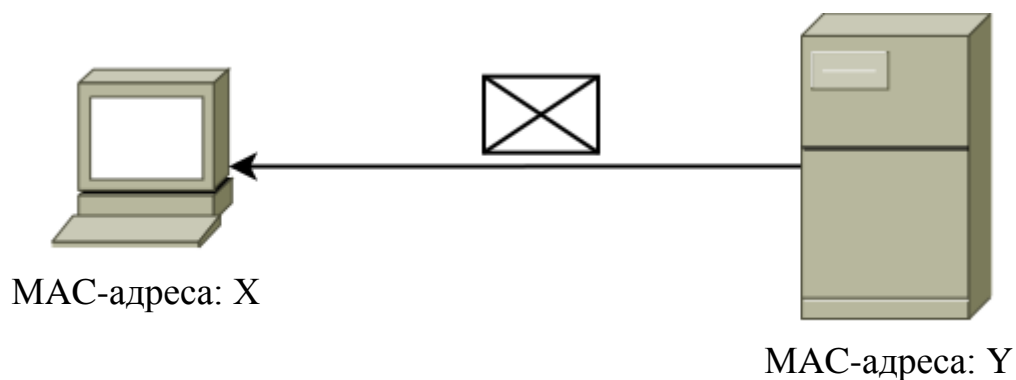


Рисунок 3.4 – Топологія мережі

Контрольні питання

1. Що називають інкапсуляцією?
2. PDU якого рівня OSI називають пакетом?
3. Які рівні стеку протоколів TCP/IP та OSI співпадають?
4. Для чого використовують протокол ICMP?
5. Які порти використовуються для роботи протоколу FTP?

Лабораторна робота №4. Мережеві пристрої

Мета: використання мережевих пристроїв та аналіз їх роботи з огляду на еталонну модель взаємодії відкритих систем.

Теоретичні відомості

Комп'ютерна мережа складається з різних компонентів (персональні комп'ютери, сервери, мережеві пристрої, фізичні лінії передачі). Ці компоненти можна розділити на чотири основні категорії:

- вузли;
- пристрої для спільного використання;
- мережеві пристрої;
- мережеві носії.

Вузли – це пристрої, які безпосередньо відправляють і приймають повідомлення в мережі.

Пристрої для спільно використання, як правило, підключаються до мережі не безпосередньо, а через вузли.

Мережеві пристрої, як і **мережеві носії**, з'єднують вузли між собою.

Більшість сучасних локальних комп'ютерних мереж як канал зв'язку (мережевий носій) використовують кабельні з'єднання (стандарти 10BASE5 та 10BASE2 – коаксіальний кабель; 10BASE-T, 100BASE-TX, 1000BASE-T – вита пара). Інколи, при перевищенні певної довжини кабельної мережі, каналам властиве затухання сигналу. Для підсилення сигналу використовують **повторювач**.

Повторювач – мережевий пристрій, який з'єднує кілька кабельних сегментів, отримує електричний сигнал з одного порту, а потім генерує новий, очищений від шумів та посилений, сигнал на інший порт. Оскільки повторювач НЕ інтерпретує значення бітів, а тільки виконує його регенерацію він відноситься до пристроїв, які працюють на *першому рівні еталонної моделі OSI*.

Характерною рисою стандартів, які використовують кабель типу вита пара, є під'єднання кожного вузла до централізованої точки. Як така точка у стандарті 10BASE-T використовується концентратор.

Концентратор (hub) – багатопортовий повторювач.

Через концентратор Ethernet можна одночасно відправляти тільки одне повідомлення. Якщо два або більше вузлів, підключених до одного концентратора, спробують одночасно відправити повідомлення виникає колізія.

Колізія – зіткнення електронних сигналів у комп'ютерній мережі, що призводить до спотворення повідомлення.

Оскільки концентратор НЕ декодує повідомлення, він не виявляє спотворені колізією повідомлення і повторює його всім портам. Область мережі, в якій вузол може отримати викривлене при зіткненні повідомлення, називається **доменом колізій**. Всередині цього домену вузол, що отримав спотворене повідомлення, виявляє, що відбулося зіткнення. Кожен вузол, що відправляє повідомлення, якийсь час чекає і потім намагається знову відправити повідомлення, що зі збільшенням кількості вузлів призводить до перевантаження мережі та зменшення швидкості передачі даних.

Для обмеження потоку даних та зменшення кількості колізій, як правило, локальну мережу розділяють на окремі сегменти.

Сегмент – окрема частина чого-небудь.

Для з'єднання між собою мережевих сегментів, можуть бути використані мости, комутатори, маршрутизатори та шлюзи.

Мережевий міст (Bridge) – мережевий пристрій, що працює на канальному рівня моделі OSI, призначений для об'єднання сегментів (підмереж) комп'ютерної мережі в єдину мережу.

Коли міст отримує фрейм, він порівнює MAC-адресу відправника з наявною у нього адресної таблицею для визначення того, чи слід відфільтрувати цей фрейм (відкинути), розіслати його лавинним способом або скопіювати фрейм в інший сегмент. Прийняття такого рішення відбувається наступним чином:

- якщо пристрій-одержувач знаходиться в тому ж сегменті, з якого цей фрейм був отриманий, то міст запобігає його передачі в інший сегмент (цей процес називається фільтрацією);
- якщо пристрій-одержувач знаходиться в іншому сегменті і його адреса присутня в адресній таблиці, то міст пересилає фрейм у відповідний сегмент;
- якщо пристрій-одержувач відсутній в таблиці адрес (тобто "невідомий" мосту), то міст розсилає фрейм в усі сегменти за винятком того, звідки був отриманий фрейм (лавинна розсилка повідомлень).

Встановлення мережевого моста збільшує кількість доменів колізій. Для обміну даними з усіма доменами колізій використовують ширококомвні та багатоадресатні фрейми канального рівня еталонної моделі OSI.

Якщо якомусь вузлу потрібно звернутися до всіх вузлів мережі, то він посилає фрейм з адресою одержувача FF:FF:FF:FF:FF:FF (**широкомовна MAC-адреса**). Ця адреса приймається мережевими адаптерами (NIC) всіх пристроїв мережі. Пристрої другого рівня повинні передавати всі ширококомвні і багатоадресні фрейми методом лавинної розсилки, тобто передавати їх усім пристроям, які до них приєднані.

Комутатор (Switch) – багатопортовий мережевий міст, у якого на кожен порт доводиться по одному вузлу. Такий пристрій зменшує домени колізій до мінімуму і колізії практично не виникають. Маленькі фізичні сегменти, які створює комутатор, називають **мікросегментами**.

Мікросегментація сприяє створенню виділених сегментів, що забезпечує паралельну взаємодію з мінімальною кількістю колізій.

Завдання

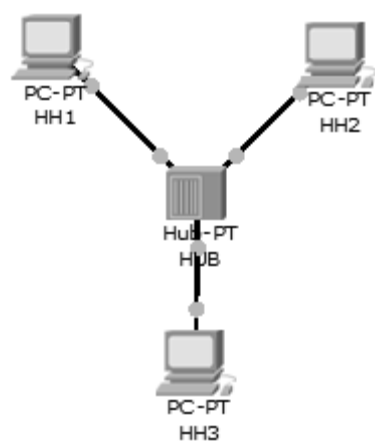
1. Використовуючи програму Cisco Packet Tracer, створити мережеві топології зображені на рис. 4.1.
2. Налаштувати мережеві пристрої згідно таблиці 4.1 (N – номер у списку академічної групи, I – номер пристрою).
3. Виконати імітацію передачі пакетів у кожній з топологій, вказавши у фільтрі протоколів ARP та ICMP.
4. Переглянути PDU пакетів на різних рівнях еталонної моделі OSI.
5. У кожній з топологій спробувати створити колізію та проаналізувати роботу мережевого обладнання при її виникненні.
6. Проаналізувати результат роботи різних мережевих пристроїв та мереж побудованих на їх основі.
7. Для кожної з мереж заповнити таблицю 4.2 та письмово відповісти на контрольні питання.

Таблиця 4.1 – Налаштування IP – адрес

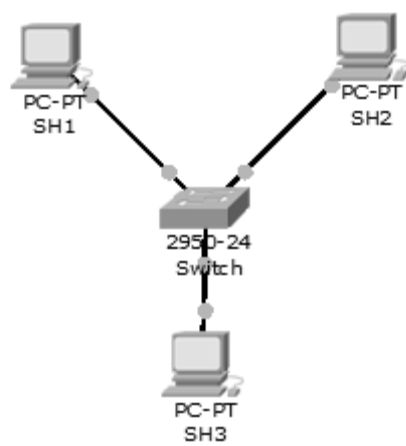
Пристрій	IP Address	Subnet Mask
HH _I	192.168.N.I	255.255.255.0
SH _I	192.168.N+1.I	255.255.255.0
H _I	192.168.N+2.I	255.255.255.0
BH _I	192.168.N+3.I	255.255.255.0
SHH _I	192.168.N+4.I	255.255.255.0

Таблиця 4.2 – Переваги та недоліки комутаційних пристроїв.

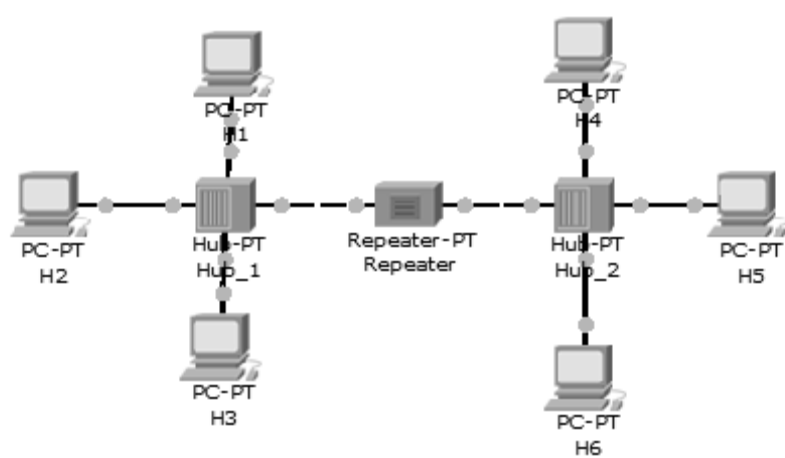
Назва мережі	Переваги та недоліки	Кількість вузлів, які отримають пошкоджені кадри	Кількість доменів колізій	Чи можлива колізія, так/ні
HH				
SH				
H				
BH				
SHH				



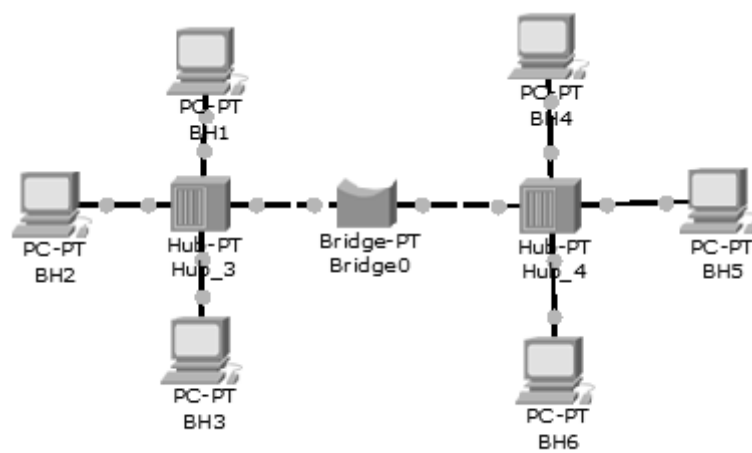
a



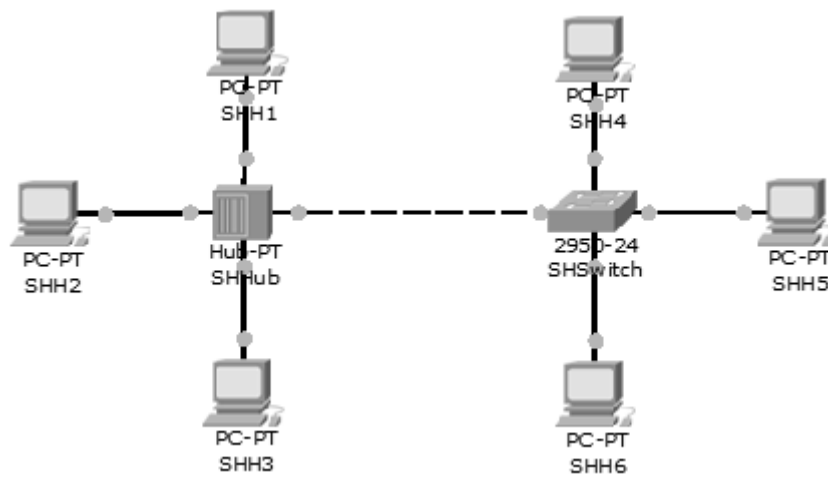
б



B



Г



Д

Рисунок 4.1 – Різні варіанти з'єднання мережевих пристроїв

Контрольні питання

1. Що таке колізія?
2. На якому рівні еталонної моделі OSI працює мережевий міст?
3. Чи існує мережева топологія з варіантів, зображених на рисунку 4.1, у якій неможливе виникнення колізії?
4. Чим відрізняється принцип роботи концентраторів та комутаторів?
5. Які функції виконує повторювач?

Лабораторна робота №5. Кодування цифрових сигналів

Мета: вивчити особливості функціонування фізичного рівня еталонної моделі OSI.

Теоретичні відомості

При передачі дискретних даних по каналах зв'язку застосовуються два основні типи фізичного кодування – на основі несучого синусоїдального сигналу та на основі послідовності прямокутних імпульсів. Перший спосіб називають **модуляцією** або **аналоговою модуляцією**, а другий спосіб – **цифровим кодуванням**.

Аналогова модуляція застосовується для передачі дискретних даних по каналах з вузькою полосою частот, наприклад, суспільні телефонні мережі. Амплітудно-частотна характеристика каналу тональної частоти представлена на рис 5.1.

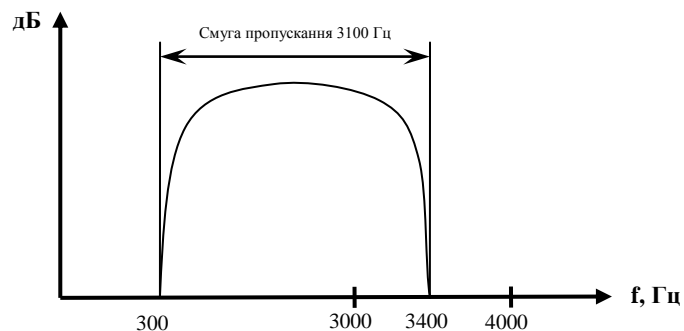


Рисунок 5.1 – Смуга пропускання стандартного телефонного каналу

Представлений канал передає частоти в діапазоні від 300 до 3400 Гц, таким чином, його смуга пропускання дорівнює 3100 Гц. Хоча людський голос має ширший спектр (приблизно від 100 Гц до 10 кГц), для прийнятної якості передачі мови, діапазон в 3100 Гц є хорошим рішенням. Жорстке обмеження полоси пропускання тонального каналу пов'язане з використанням апаратури ущільнення та комутації каналів в телефонних мережах.

Пристрій, який виконує функції модуляції несучої синусоїди на стороні, що виконує передачу, і демодуляції на приймаючій стороні, має назву **модем** (модулятор-демодулятор).

При фізичному кодуванні способом аналогової модуляції інформація кодується зміною амплітуди, частоти або фази синусоїдального сигналу несучої частоти. Основні способи аналогової модуляції показані на рис. 5.2.

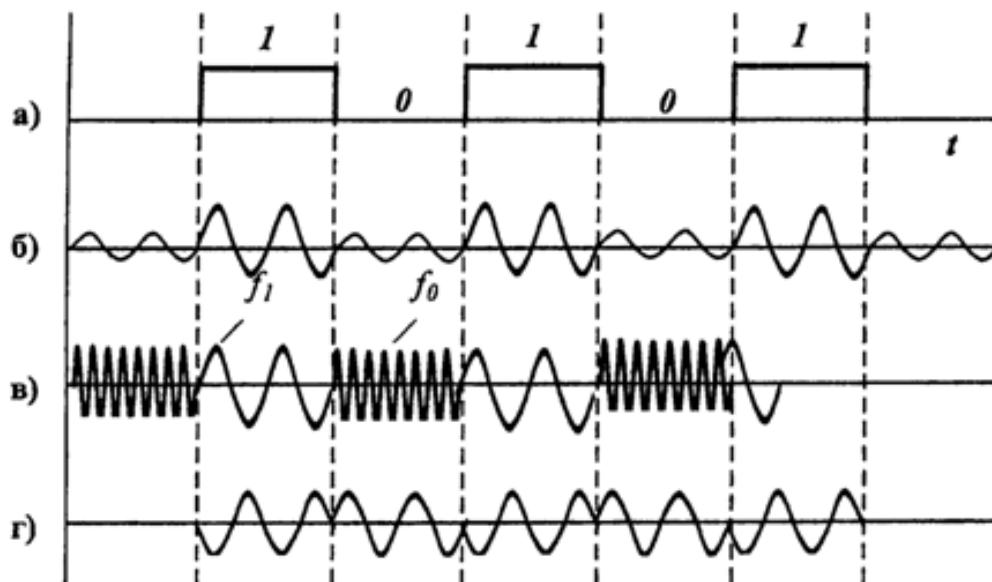


Рисунок 5.2 – Типи модуляції

На діаграмі (рис. 5.2 а) показана послідовність біт вихідної інформації, яка представлена потенціалами високого рівня для логічної одиниці і потенціалами нульового рівня для логічного нуля. Такий спосіб кодування називається **потенційним кодом**, який часто використовується при передачі даних між блоками комп'ютера.

При **амплітудній модуляції** (рис 5.2 б) для логічної одиниці вибирається один рівень амплітуди синусоїди несучої частоти, а для логічного нуля – інший. Цей спосіб рідко використовується через низьку завадостійкості, але часто застосовується в поєднанні з фазовою модуляцією.

При **частотній модуляції** (рис 5.2 в) значення 0 та 1 вихідних даних передаються синусоїдами з різною частотою – f_0 та f_1 . Цей спосіб модуляції досить простий і зазвичай застосовується в модемах, що працюють на швидкостях від 300 до 1200 біт/с.

При **фазовій модуляції** (рис. 5.2 г) значенням даних 0 та 1 відповідають сигнали однакової частоти, але різної фази, наприклад 0 та 180, або 0 та 90 градусів.

При цифровому кодуванні дискретної інформації застосовують потенційні та імпульсні коди. У **потенційних кодах** для представлення логічних одиниць та нулів використовують лише значення потенціалу сигналу, а його перепади, що формують закінчені імпульси, до уваги не приймаються. **Імпульсні коди** дозволяють представити двійкові дані або імпульсами певної полярності, або частиною імпульсу – перепадом потенціалу певного напрямку.

При використанні прямокутних імпульсів для передачі дискретної інформації обирають такий спосіб кодування, який забезпечує виконання таких умов:

- при одній і тій же бітовій швидкості найменшу ширину спектра результуючого сигналу;

- забезпечення синхронізації між передавачем і приймачем;
- здатність розпізнавати помилки;
- низька вартість реалізації.

Такі вимоги є взаємно суперечливими, тому кожен з наступних методів цифрового кодування має свої переваги та недоліки.

Потенціальний код без повернення до нуля (Non return to Zero, NRZ) – метод потенційного кодування (рис. 5.3 а), у якому при передачі послідовності одиниць сигнал не повертається до нуля під час такту. Метод NRZ простий в реалізації, дає можливості розпізнавання помилок, але не має властивості самосинхронізації. При високих швидкостях обміну даними і довгих послідовностях одиниць або нулів невелике розузгодження тактових частот може призвести до помилки в цілий такт і, відповідно, читання некоректного значення біта. У чистому вигляді код NRZ в мережах не використовується.

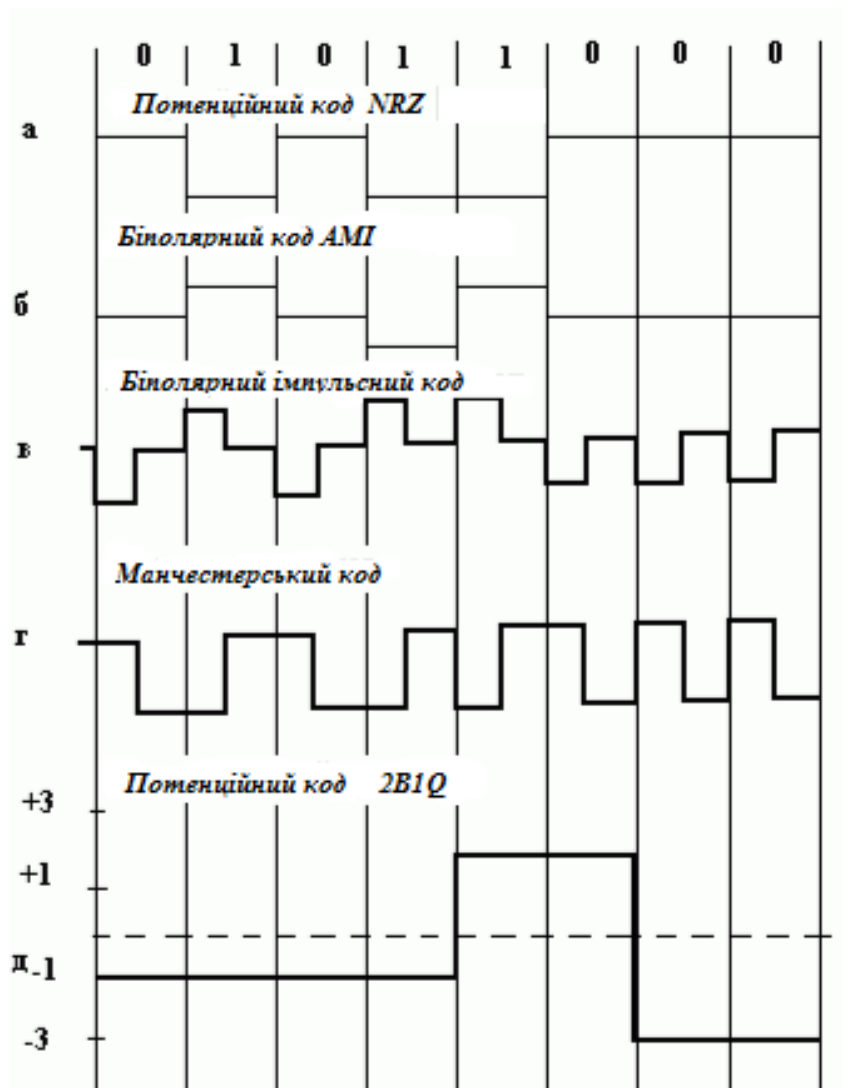


Рисунок 5.3 – Різні типи цифрового кодування

Метод біполярного кодування з альтернативною інверсією (Bipolar Alternate Mark Inversion, AMI) – є однією з модифікацій методу NRZ, у якій використовуються три рівні потенціалу – від’ємний, нульовий і додатний (рис. 5.3 б). Для кодування логічного нуля використовується нульовий потенціал, а логічна одиниця кодується або додатним потенціалом, або від’ємним, при цьому потенціал кожної нової одиниці протилежний до потенціалу попередньої. Використання AMI призводить до більш вузького спектра сигналу, ніж для коду NRZ, і, таким чином, до вищої пропускної спроможності лінії.

Потенціальний код з інверсією при одиниці (Non return to Zero with ones Inverted, NRZI) – метод потенційного кодування схожий на AMI, але лише з двома рівнями сигналу. При передачі нуля він передає потенціал, який був встановлений в попередньому такті (тобто не міняє його), а при передачі одиниці потенціал інвертується на протилежний. Зручний в тих випадках, коли наявність третього рівня сигналу вельми небажана, наприклад в оптичних кабелях, де стійко розрізняються два стани сигналу – світло та темрява.

Окрім потенційних кодів в мережах використовуються й імпульсні коди, в яких дані представлені повним імпульсом або ж його частиною – **фронтом**.

Біполярний імпульсний код – метод імпульсного кодування в якому одиниця представлена імпульсом однієї полярності, а нуль – іншої (рис. 5.3 в). Кожен імпульс триває половину такту. Такий код має відмінні самосинхронізуючі властивості, але через широкий спектр використовується рідко.

Манчестерський код – метод імпульсного кодування, у якому для кодування нулів і одиниць використовується перепад потенціалу, тобто фронт імпульсу. Одиниця кодується перепадом від низького рівня сигналу до високого, а нуль – зворотним перепадом. На початку кожного такту може відбуватися службовий перепад сигналу, якщо потрібно представити декілька одиниць або нулів підряд (рис. 5.3 г). До недавнього часу, манчестерський код був найпоширенішим методом кодування в технологіях Ethernet та Token Ring. Ширина його спектру в півтора рази вужча, ніж в біполярному імпульсному коді, а для передачі даних використовуються два рівні сигналу.

Потенціальний код 2B1Q – метод потенційного кодування з чотирма рівнями сигналу для кодування даних. Назва відображає суть метода. Кожні два біта (2B) передаються за один такт сигналом, що має чотири стани (1Q). Парі біт 00 відповідає потенціал -2,5 В; парі біт 01 – потенціал -0,833 В; парі 11 – потенціал +0,833; парі 10 – потенціал +2,5 В. Метод додатково потребує заходів по боротьбі з довгими послідовностями однакових пар бітів. При випадковому чередуванні бітів спектр сигналів в два рази вужчий, ніж у NRZ, тому як при тій же бітовій швидкості, тривалість такту збільшується в два рази. За допомогою коду 2B1Q можна по одній і тій же лінії передавати дані в два рази швидше, ніж за допомогою коду AMI або NRZI. Проте реалізація цього методу вимагає більш потужного передавача і складнішого приймача, який повинен розрізняти чотири рівні сигналу.

Завдання

1. Ознайомитися з основними типами цифрового кодування сигналів.
2. Реалізувати програму, яка автоматично переводить байти даних у поширені системи обчислення (двійкова, восьмирічна, шістнадцятирічна).
3. Реалізувати програму, яка кодує довільні вісім біт інформації основними способами аналогової модуляції: амплітудна, частотна, фазова.
4. Реалізувати програму, яка кодує довільні вісім біт інформації, використовуючи методи цифрового кодування сигналів:
 - потенціальний код без повернення до нуля (NRZ);
 - метод біполярного кодування з альтернативною інверсією (AMI);
 - потенціальний код з інверсією при одиниці (NRZI);
 - біполярний імпульсний код;
 - манчестерський код;
 - потенціальний код 2B1Q.
5. Для демонстрацій завдань 2-4 створити єдиний графічний інтерфейс користувача.
6. За результатами виконання роботи оформити звіт.

Контрольні питання

1. Які з вивчених методів кодування сигналів мають тільки два рівні сигналу?
2. Які переваги має потенційний код 2B1Q?
3. У чому полягає суть амплітудної модуляції?
4. Як називають пристрій для модуляції та демодуляції сигналів?
5. Перерахуйте основні методи аналогового кодування цифрових сигналів.

Лабораторна робота №6. Логічна адресація

Мета: засвоїти основні поняття IP – адресації та принципи ділення адрес на базі класів та масок.

Теоретичні відомості

IP-адреса – адреса мережевого рівня, що позначає логічний, а не фізичний мережевий пристрій. Всі мережеві пристрої певної локальної комп'ютерної мережі повинні мати унікальні адреси. Якщо вузол IP-мережі має кілька мережевих інтерфейсів, кожному з них присвоюється окрема IP-адреса.

IP-адреса являє собою 32-бітове число. Зручною формою запису IP-адреси є запис у вигляді чотирьох десяткових чисел значенням від 0 до 255.

IP-адреса складаються з двох частин – номера мережі та номера вузла. Номер мережі ідентифікує підмережу, до якої належить вузол, номер вузла – однозначно визначає вузол всередині підмережі. Слід зазначити, що адреса мережі завжди має двійкові нулі у вузловій частині адреси.

Для ділення IP-адрес на частини використовують дві схеми:

- на основі класів адресів;
- на основі масок.

Розподіл IP-адрес на номер мережі та номер вузла, що базується на класах, приведено у таблиці 6.1.

Таблиця 6.1 – Класи логічних адрес

Клас адреси	Біти першого октету (виділені не змінюються)	Мережева (М) та вузлова (В) частина адреси	Маска	Діапазон адрес
A	00000000 – 01111111	М.В.В.В	255.0.0.0	1.0.0.0 – 126.255.255.255
B	10000000 – 10111111	М.М.В.В	255.255.0.0	128.0.0.0 – 191.255.255.255
C	11000000 – 11011111	М.М.М.В	255.255. 255.0	192.0.0.0 – 223.255.255.255
D	11100000 – 11101111	–	–	224.0.0.0 – 239.255.255.255
E	11110000 – 11111111	–	–	240.0.0.0 – 255.255.255.255

Практичний досвід показує, що виділення мережам блоків адрес на основі класів не забезпечує оптимальне використання адресного простору.

Маска – це чотирьохбайтове число, двійковий запис якого містить одиниці в розрядах, що відповідають номеру мережі, і нулі в розрядах, що

відповідають номеру вузла, яке використовується спільно з IP-адресою. Одиниці маски починаються з першого розряду адреси і не можуть чергуватися з нулями.

За допомогою маски можна виділяти довільну кількість розрядів для номера мережі, що дозволяє відмовитися від понять класів адрес і зробити систему адресації більш гнучкою.

Для зазначення кількості розрядів, виділених для номера мережі, також використовується **префікс** адреси. Запис адреси з префіксом має вигляд: IP-адреса/префікс, де **префікс** – число розрядів маски, виділених для номера мережі.

Наприклад, запис 192.168.75.64/26 означає, що в адресі 192.168.75.64 під номер мережі відведено 26 двійкових розрядів, відповідна маска 255.255.255.192.

Для адресації вузлів у локальних комп'ютерних мережах, відповідно до стандарту RFC 1918, рекомендується використовувати наступні адреси:

- 10.0.0.0 (блок адрес класу A);
- 172.16.0.0 – 172.31.0.0 (блок адрес класу B);
- 192.168.0.0 – 192.168.255.0 (блок адрес класу C).

Адреси з цих блоків називають **приватними адресами**. IP-пакети з приватними адресами знищуються магістральними маршрутизаторами Інтернет. Усі інші адреси називають **відкритими**, і вони повинні бути унікальними при роботі у глобальній мережі Інтернет.

Крім того існує перелік IP-адрес спеціального призначення.

Пакет з адресою 255.255.255.255 повинен розсилатися всім вузлам, що знаходяться в тій же підмережі, що і джерело пакета. Такий спосіб розсилки називається **обмеженим широкомовленням** (limited broadcast).

Якщо розряди адреси, що відповідають номеру вузла, містять тільки одиниці, то пакет розсилається всім вузлам мережі з заданим номером. Такий спосіб розсилки називається **широкомовним** (broadcast).

Якщо в адресі одержувача в полі номера мережі містяться тільки нулі, то вузол-одержувач належить тій самій підмережі, що і вузол, який відправив пакет.

Блок адрес 127.0.0.0/8 використовується для тестування і взаємодії мережевих процесів у межах окремого комп'ютера.

Завдання

Виконати по два варіанти з кожного завдання. Номер першого варіанта у завданнях $N \bmod 10$, другого – $3 \cdot N \bmod 10$ (N – номер студента у журналі академічної групи).

Визначити клас IP-адреси:

1. 172.219.112.245
2. 144.125.208.62
3. 172.51.251.146
4. 147.102.112.115
5. 174.150.24.36
6. 181.114.149.46
7. 154.228.92.125
8. 173.78.30.27
9. 150.35.21.27
10. 179.229.16.178

Визначити номер мережі, номер вузла, широкомовну адресу для заданих IP-адрес та маски (або без неї):

1. 148.141.32.138/19
2. 183.126.32.14/18
3. 136.73.79.103./23
4. 156.169.93.140
5. 145.41.144.123
6. 180.60.211.145
7. 180.101.59.143
8. 185.35.82.241/16
9. 183.177.20.72/21
10. 181.234.27.92/24

Для заданих адрес та маски визначити номер мережі та вузла, першу та останню доступні адреси вузла у двійковому та десятковому вигляді:

1. 10.208.205.107 / 255.255.255.240
2. 10.9.237.10 / 255.255.240.0
3. 10.229.136.23 / 255.255.255.254
4. 10.161.182.146 / 255.255.192.0
5. 10.181.73.164 / 255.255.254.0
6. 10.237.115.109 / 255.255.255.224
7. 10.112.124.230 / 255.255.224.0
8. 10.241.188.186 / 255.255.240.0
9. 10.67.178.135 / 255.255.240.0
10. 10.152.184.191 / 255.255.224.0

У перліку мереж знайти мережу, яка включає в собі всі інші мережі:

- | | |
|----------------|-----------------|
| 1. | 91.5.192.0 / 19 |
| 91.5.64.0 / 18 | 91.5.128.0 / 18 |

91.5.0.0 / 18
91.5.224.0 / 19
2.
122.47.0.0 / 17
122.46.0.0 / 17
122.47.192.0 / 18
122.46.128.0 / 17
122.47.128.0 / 18
3.
2.30.42.0 / 25
2.30.43.192 / 26
2.30.43.128 / 26
2.30.42.128 / 25
2.30.43.0 / 25
4.
103.192.0.0 / 11
103.128.0.0 / 11
103.240.0.0 / 12
103.160.0.0 / 11
103.224.0.0 / 12

5.
32.202.228.0 / 22
32.202.238.0 / 23
32.202.232.0 / 22
32.202.224.0 / 22
32.202.236.0 / 23

6.
177.210.120.0 / 21
177.210.64.0 / 20
177.210.112.0 / 21
177.210.96.0 / 20
177.210.80.0 / 20
7.
122.47.0.0 / 17
122.46.0.0 / 17
122.47.192.0 / 18
122.46.128.0 / 17
122.47.128.0 / 18
8.
2.30.42.0 / 25
2.30.43.192 / 26
2.30.43.128 / 26
2.30.42.128 / 25
2.30.43.0 / 25
9.
103.192.0.0 / 11
103.128.0.0 / 11
103.240.0.0 / 12
103.160.0.0 / 11
103.224.0.0 / 12

10.
32.202.228.0 / 22
32.202.238.0 / 23
32.202.232.0 / 22
32.202.224.0 / 22
32.202.236.0 / 23

Контрольні питання

1. Що таке маска?
2. Скільки вузлів може бути у мережі класу С?
3. Які переваги використання масок?
4. Які адреси відносять до класу В?
5. Які адреси називають широкомовними?
6. Які діапазони адрес називають приватними?

Лабораторна робота №7. Створення підмереж

Мета: закріпити теоретичні відомості та отримати практичні навички створення підмереж, проаналізувати їх роботу з огляду на еталонну модель OSI.

Теоретичні відомості

Одним із способів економії IP-адрес є використання підмереж (subnetting). Цей метод дозволяє розбивати повні класові блоки мережевих адрес на менші і допомагає уникнути повного використання всіх IP-адрес. На рис. 7.1 зображена мережа класу В (131.108.0.0), яка розбита на три підмережі. Необхідність подрібнення невеликої мережі виникає досить рідко, але у разі використання великих блоків адрес і дуже великих мереж такий розподіл є практично обов'язковим.

Створення підмереж означає використання маски підмережі для поділу її на більш дрібні, більш ефективні та легші у керуванні сегменти.

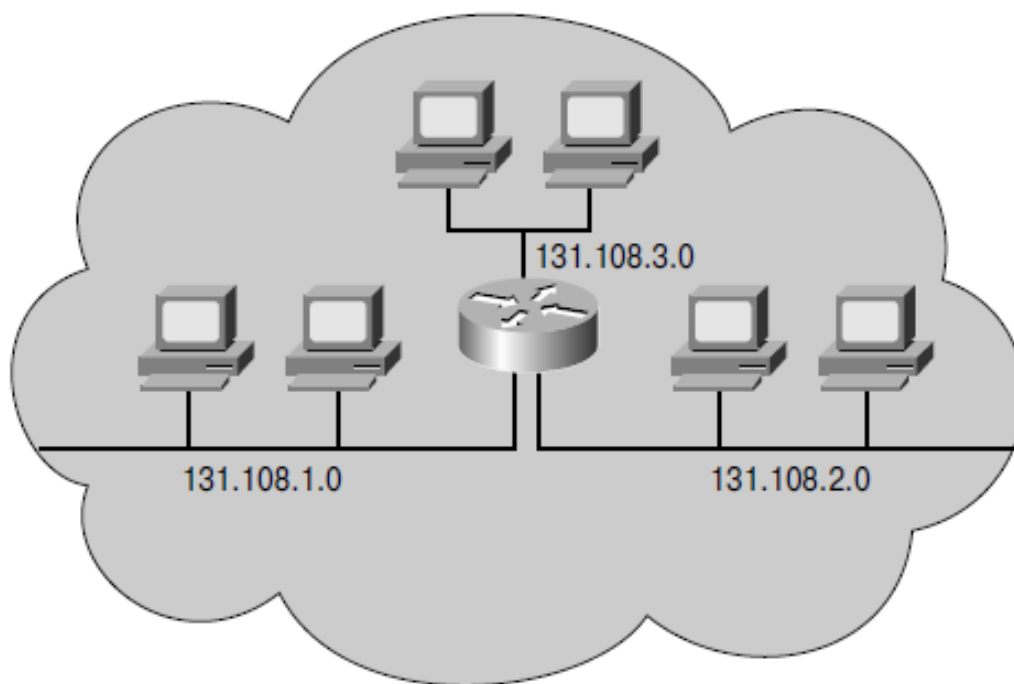


Рисунок 7.1 – Схема адресації з використанням підмереж

Наприклад, механізм ділення визначеної мережі (213.59.30.0/24) на чотири підмережі наведено на рис 7.2.

Кожна з підмереж є окремою локальною мережею. Щоб пристрої з однієї підмережі змогли обмінюватися даними з пристроями з іншої, необхідний маршрутизатор.

Маршрутизатор – це мережевий пристрій, що з'єднує локальні мережі та працює на третьому рівні еталонної моделі OSI.

Кожен порт, або інтерфейс, маршрутизатора пов'язаний зі своєю локальною мережею. У кожного маршрутизатора є таблиця локально підключених мереж і їх інтерфейсів на основі якої приймається рішення про можливість та напрям передачі даних. Приймавши кадр, маршрутизатор декодує його і отримує пакет з IP-адресою одержувача. Цю адресу він порівнює з даними всіх мереж з таблиці маршрутизації. Якщо адреса мережі одержувача є в таблиці, маршрутизатор інкапсулює пакет в новий кадр і відправляє. Цей новий кадр прямує в мережу одержувача через інтерфейс, що відноситься до обраного шляху (рис 7.3). Процес перенаправлення пакетів в мережу одержувача називається **маршрутизацією**.

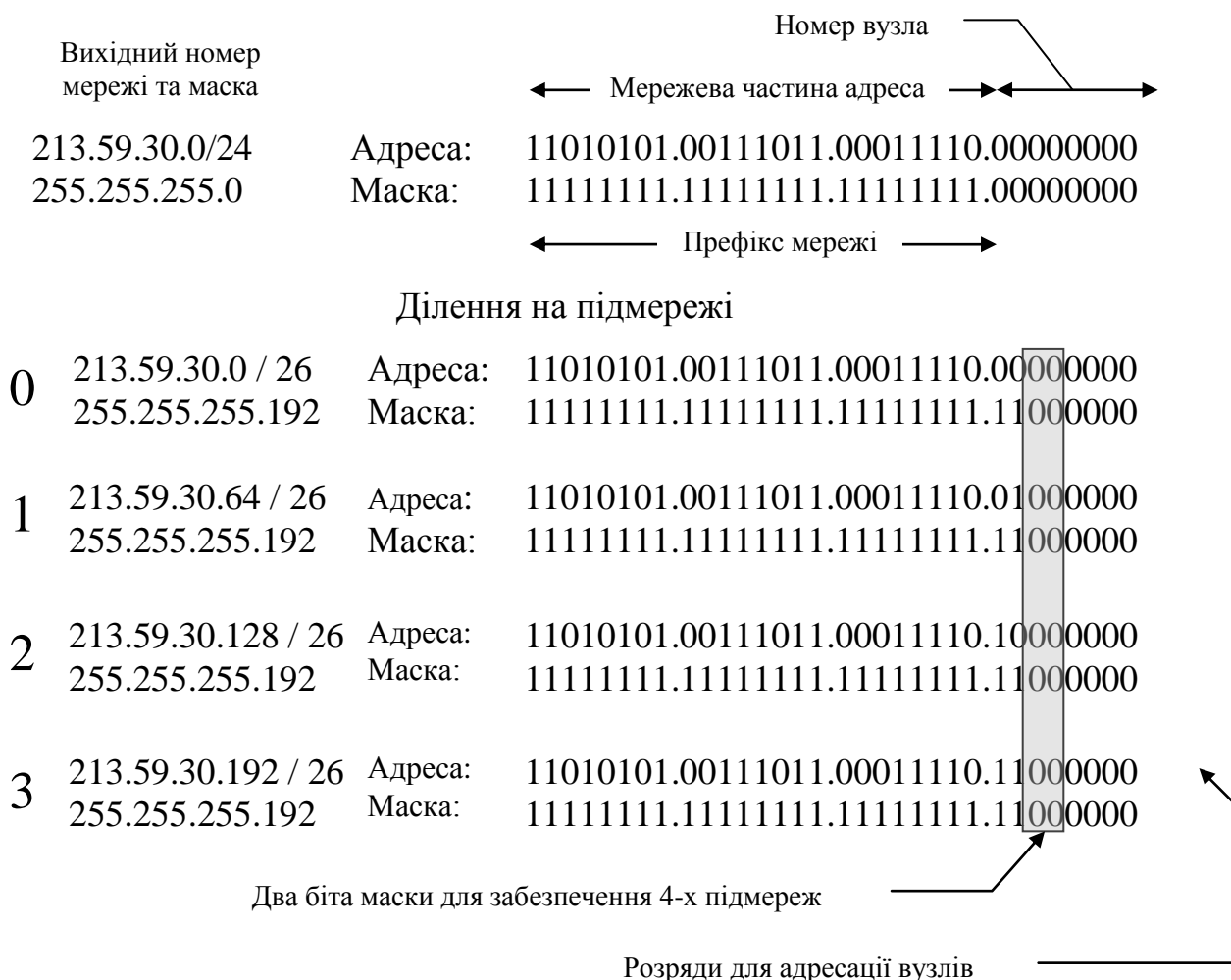


Рисунок 7.2 – Ділення мережі на підмережі

Інтерфейси маршрутизатора не пересилають повідомлення за широкомовною MAC-адресою. Тому розсилки локальної мережі не потрапляють в інші мережі через маршрутизатор

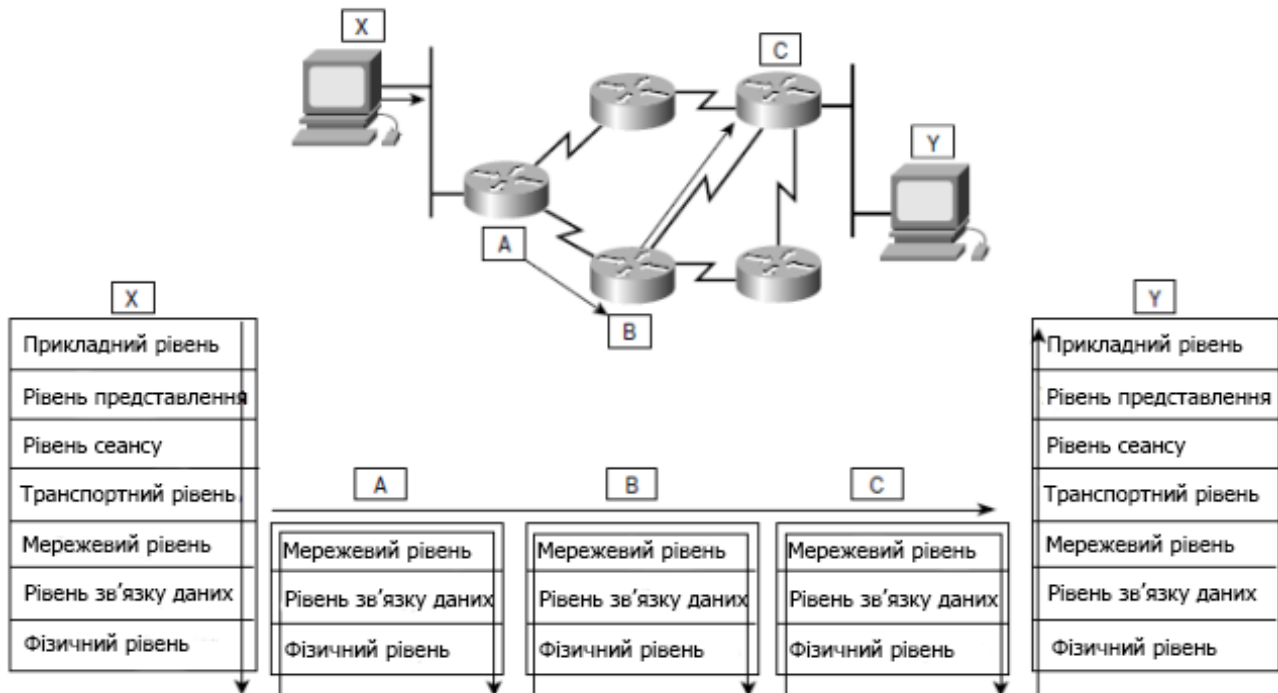


Рисунок 7.3 – Передача даних між підмережами

Розглянемо механізми відправки повідомлень адресату з тієї ж та з іншої локальної мережі.

При відправці вузлу, підключеному до тієї ж мережі, повідомлення надсилається безпосередньо, визначивши перед цим MAC-адресу вузла призначення за допомогою протоколу ARP.

При наявності IP-адреси вузла ARP визначає і зберігає MAC-адресу вузла в локальній мережі в три етапи.

1. Відправляючий вузол створює і відправляє кадр з MAC-адресою широкомовної розсилки. У кадрі знаходиться повідомлення з IP-адресою вузла призначення.

2. Кожен мережевий вузол отримує цей кадр і порівнює IP-адресу отримувача зі своєю. Вузол з відповідною IP-адресою посилає відправникові свою MAC-адресу.

3. Відправник отримує повідомлення і зберігає MAC-адресу та IP-адресу в таблиці ARP.

Коли MAC-адреса одержувача є в таблиці ARP відправника, кадр відправляється безпосередньо адресату.

Якщо вузлу потрібно відправити повідомлення у віддалену мережу, використовується маршрутизатор. Вузол включає в пакет IP-адресу вузла призначення, а у кадр як адресу одержувача вказується MAC-адреса

маршрутизатора. Таким чином, маршрутизатор отримує і приймає кадр за MAC-адресою.

Вузол отримує IP-адресу маршрутизатора на основі адреси шлюзу, що вказаний в налаштуваннях протоколу TCP/IP.

Адреса шлюзу – це адреса інтерфейсу маршрутизатора, підключеного до тієї ж локальної мережі, що і вузол-відправник повідомлення.

Завдання

1. Змоделювати мережеву топологію, зображену на рис. 7.1.
2. Налаштувати мережеві пристрої згідно таблиці 7.1. (X – номер у списку академічної групи).
3. Протестувати роботу мережі, передаючи пакети командою *ping* між хостами мережі.
4. Проаналізувати роботу протоколу ARP при передачі даних у локальній мережі та між окремими мережами.
5. Проінспектувати PDU 2-го та 3-го рівнів моделі OSI при передачі пакетів у локальній мережі та між окремими мережами.
6. Проаналізувати зміни PDU другого рівня при передачі пакета маршрутизатором.
7. Написати звіт.

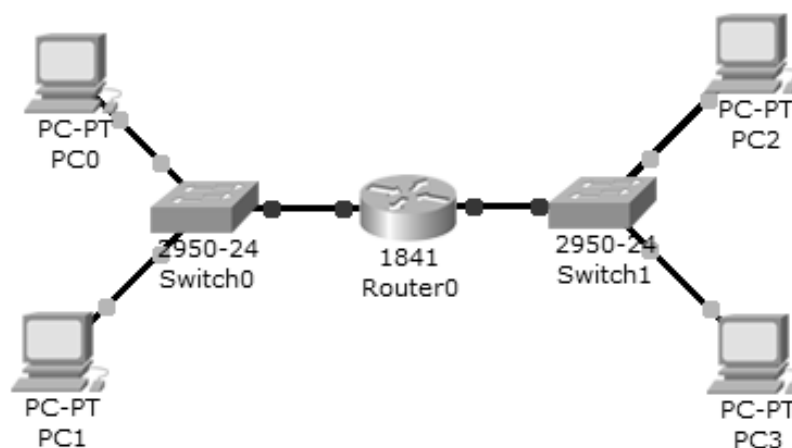


Рисунок 7.4 – Топологія локальної мережі

Таблиця 7.1 – Схема адресації пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз за замовченням
1841 Router	Fa0/0	150.X.1.1	255.255.255.0	N/A
	Fa0/1	150.X.2.1	255.255.255.0	

PC0	NIC	150.X.1.2	255.255.255.0	150.X.1.1
PC1	NIC	150.X.1.3	255.255.255.0	150.X.1.1
PC2	NIC	150.X.2.2	255.255.255.0	150.X.2.1
PC3	NIC	150.X.2.3	255.255.255.0	150.X.2.1

Контрольні питання

1. У якому випадку локальна мережа обов'язково повинна містити маршрутизатор?
2. Які пакети відправляються до найближчого маршрутизатора (шлюза)?
3. Чи залишається незмінним PDU 2-го рівня моделі OSI при передачі пакета у рамках однієї підмережі?
4. За яким протоколом визначається канална адреса (MAC-адреса) хоста до якого потрібно відправити пакет?
5. Чи проходять широкомовні кадри крізь маршрутизатор?

Лабораторна робота №8. Локальна мережа з динамічною адресацією

Мета: вивчити основні методи розподілу IP-адрес, опанувати ділення блоків адрес на номер мережі та номер вузла з використанням класів та масок.

Теоретичні відомості

Кількість робочих станцій локальної мережі іноді сягає декількох тисяч, список користувачів постійно змінюється, з'являються нові користувачі з ноутбуками та мобільними пристроями. Присвоєння кожному пристрою IP-адреси власноруч є складною проблемою, тому доцільно це зробити автоматично. Для цього використовується протокол під назвою DHCP.

Dynamic Host Configuration Protocol (DHCP) – протокол, який передбачає механізм автоматичного присвоєння інформації про IP-адресу, маску, шлюз та перелік адрес DNS-серверів.

Це найбільш бажаний спосіб привласнення IP-адрес вузлам у великій мережі, оскільки він полегшує роботу фахівців служби підтримки і практично усуває можливість помилки. Крім того, адреси присвоюються вузлам тимчасово і якщо вузол вимикається або йде з мережі, його адреса повертається в пул для повторного використання.

При першому налаштуванні як клієнта DHCP у вузла немає IP-адреси, маски підмережі та стандартного шлюзу. Він отримує ці дані за наступною схемою (рис 8.1):

- клієнт, якому потрібна IP-адреса, посилає повідомлення про пошук DHCP у вигляді широкомовної розсилки з IP-адресою одержувача 255.255.255.255 (32 одиниці) та MAC-адресою одержувача FF-FF-FF-FF-FF-FF (48 одиниць);

- кадр DHCP отримують всі вузли в мережі, але відповідає тільки сервер DHCP який відправляє клієнту запропоновану IP-адресу;

- клієнт у відповідь посилає на вказаний сервер запит DHCP з підтвердженням використання IP-адреси;

- сервер надсилає підтвердження.

DHCP-сервер може знаходитися в іншій мережі, якщо проміжні маршрутизатори сконфігуровані на пересилку DHCP-запитів.



Рисунок 8.1 – DHCP повідомлення для отримання мережевих параметрів

Завдання

1. Створити топологію локальної мережі, зображеної на рис. 8.2.
2. Для приватної (зліва від маршрутизатора) та публічної (справа від маршрутизатора) підмереж визначити номер мережі згідно з вимогами варіанта.
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.
7. Заповнити таблицю 8.1.
8. Проаналізувати та зафіксувати у звіті PDU різних рівнів моделі OSI при автоматичному отриманні IP-адреси.
9. За результатами виконання роботи скласти звіт.

Таблиця 8.1 – Адресація пристроїв локальної мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз

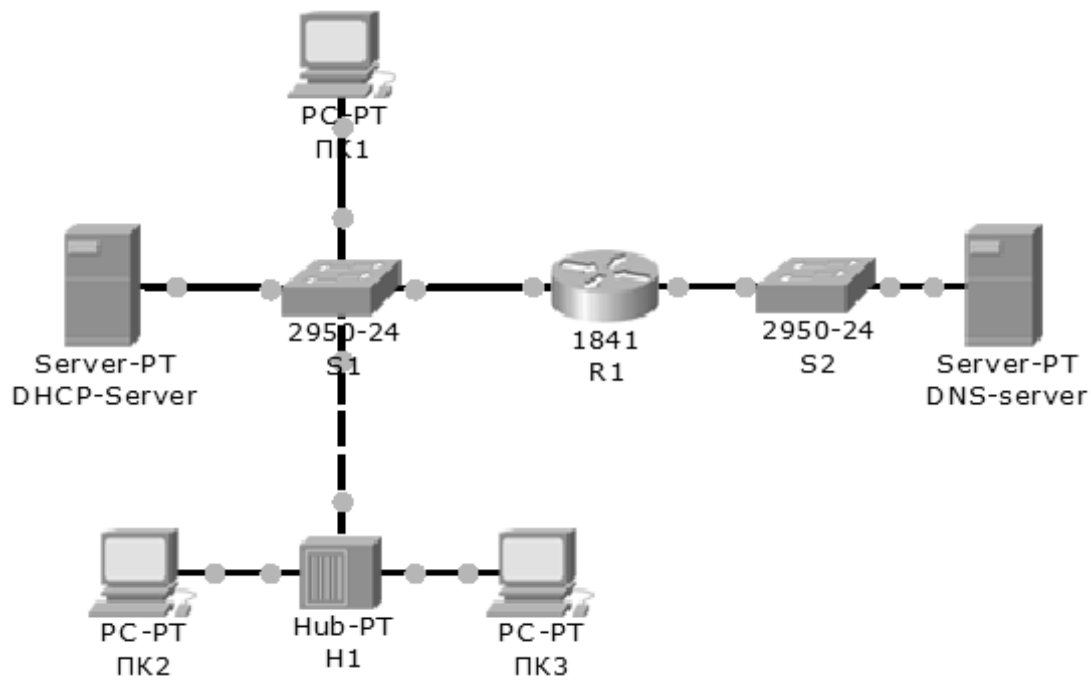


Рисунок 8.2 – Топологія мережі

Варіанти

На базі номера мережі для приватної та публічної мереж (табл 8.2) визначити адресні блоки для адресацій заданої кількості вузлів, розділивши її на необхідну кількість підмереж. Серед отриманих блоків вибрати адресні блоки з визначеними номерами підмереж.

Таблиця 8.2 – Варіанти завдань

№	Приватна			Публічна		
	Номер мережі	Кількість вузлів	Номер підмережі	Номер мережі	Кількість вузлів	Номер підмережі
1	10.14.251.0/25	25	4	150.125.231.0/25	58	3
2	172.240.251.0/24	58	3	180.240.251.0/24	28	2
3	192.168.247/26	28	2	153.168.247/26	25	4
4	10.14.251.0/25	25	4	135.14.251.0/25	58	3
5	172.240.251.0/24	58	3	37.240.251.0/24	58	3
6	192.168.247/26	28	2	95.168.247/26	28	2
7	10.14.251.0/25	25	4	58.14.251.0/25	25	4
8	172.240.251.0/24	58	3	39.240.251.0/24	58	3
9	192.168.247/26	28	2	113.168.247/26	28	2
10	172.240.251.0/24	58	3	140.240.251.0/24	58	3

Контрольні питання

1. Для чого призначений протокол DHCP?
2. Які порти використовує протокол DHCP за замовчуванням?
3. Чи можливе звернення до DHCP – сервера який знаходиться у іншій підмережі?
4. У яких випадках ручне налаштування є обов'язковим, а у яких майже неможливе?
5. Що таке пул адрес?

Лабораторна робота №9. Налаштування бездротового маршрутизатора.

Мета: ознайомитися з основними стандартами бездротових мереж, методами аутентифікації та шифрування, опанувати основні параметри налаштування бездротових маршрутизаторів.

Теоретичні відомості

Поширеним способом організації комп'ютерних мереж є бездротові технології. Основними перевагами їх використання є:

- мобільність;
- масштабованість;
- гнучкість;
- зменшення фінансових витрат;
- швидкість розгортання;
- надійність.

У бездротових технологіях для обміну інформацією між пристроями використовуються електромагнітні хвилі, які переносять радіосигнали через ефір.

До спектра електромагнітних хвиль входять смуги радіо частот, інфрачервоне та видиме світло, рентгенівське випромінювання й гамма-випромінювання. Кожній з цих смуг відповідає конкретний діапазон довжин хвиль і потужностей. Деякі області спектра виділені для мереж загального користування та можуть використовуватися без обмежень і без необхідності отримання спеціальних дозволів. Для бездротових мереж загального користування зазвичай використовується інфрачервоний спектр і частина радіочастотного діапазону.

Робота бездротових мережевих пристроїв базується на використанні випромінювання радіочастот у діапазонах 900 МГц, 2,4 ГГц і 5 ГГц.

Bluetooth – технологія, що використовує певну смугу в діапазоні частот 2,4 ГГц. Швидкість передачі даних і радіус дії цієї технології обмежений, але її перевага полягає в тому, що вона дозволяє обмінюватися даними між декількома пристроями одночасно.

Смуги частот близько 2,4 ГГц та 5 ГГц також використовують більш потужні, відносно Bluetooth, сучасні технології бездротових мереж, що відповідають вимогам ряду стандартів IEEE 802.11.

Бездротові мережі діляться на три основні категорії:

- бездротові персональні мережі (Wireless Personal Area network, WPAN);
- бездротові локальні мережі (Wireless Local Area network, WLAN);

– бездротові глобальні мережі (Wireless Wide Area network, WWAN).
Основні характеристики цих мереж наведено у таблиці 9.1

Таблиця 9.1 Характеристики бездротових мереж

Стандарт	Швидкість	Радіус дії	Примітка
Bluetooth v2.0+ EDR	< 3 Мбіт/с	Малий	Одноранговий зв'язок між пристроями
IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	1-540 Мбіт/с	Середній	Домашні мережі, мережі малих підприємств та корпоративні мережі
GSM, GPRS, CDMA	10-384 Кбіт/с	Великий	PDA, мобільні телефони

Стандарт IEEE 802.11 регламентує роботу пристроїв у мережах WLAN. З урахуванням різних характеристик бездротового зв'язку в стандарт IEEE 802.11 було внесено чотири поправки (802.11a, 802.11b, 802.11g та 802.11n). Всі ці технології віднесені до категорії Wi-Fi (Wireless Fidelity).

У мережі WLAN має бути кілька обов'язкових компонентів, до яких належать:

- бездротовий клієнт;
- точка доступу;
- бездротовий міст;
- антена.

Сота – зона покриття однієї точкою доступу.

Для того, щоб бездротові компоненти були підключені до відповідної мережі використовується ідентифікатор набору послуг (SSID).

SSID – це ім'я бездротової мережі, що представляє собою чутливий до регістру, довжиною до 32 символів рядок. Цей ідентифікатор пересилається у заголовку всіх кадрів, переданих по мережі WLAN. Ідентифікатор SSID повідомляє бездротовим пристроям до якої мережі WLAN вони належать.

Застосовуються два основних види конфігурування мереж WLAN: **спеціальний** та **інфраструктурний режими**.

Спеціальний режим (Ad-hoc) – найпростіша бездротова мережа, яка створюється за допомогою об'єднання двох або більше бездротових клієнтів у тимчасову мережу. Бездротова мережа, побудована таким чином, не має жодної точки доступу, а клієнти в ній рівноправні.

Інфраструктурний режим (Hot-spot) – бездротова мережа з точкою доступу, яка бере на себе функції управління взаємодією в соті. При такій формі організації бездротової локальної мережі окремі пристрої не можуть взаємодіяти між собою безпосередньо, для цього їм необхідний дозвіл від точки доступу.

Для отримання доступу до обраної бездротової мережі та забезпечення безпеки передачі даних використовується шифрування й аутентифікація.

Аутентифікація – видача певних прав доступу абоненту на основі наявного в нього ідентифікатора.

Відкрита аутентифікація (Open Authentication) – аутентифікація в якій використовується тільки MAC-адреса клієнта, на основі якого точка доступу відповідає або відмовою, або підтвердженням аутентифікації. При такому режимі аутентифікація можна працювати без шифрування або використовувати такі шифри як статичний WEP та SKIP.

Аутентифікація із загальним ключем (Shared Key Authentication) – аутентифікація в якій необхідно налаштувати статичний ключ шифрування алгоритму WEP. Схема роботи наступна:

- клієнт виконує запит;
- точка доступу відправляє підтвердження, яке містить 128 байт випадкової інформації;
- клієнт шифрує отримані дані алгоритмом WEP (проводиться побітове додавання за модулем 2 даних повідомлення з послідовністю ключа) і відправляє зашифрований текст разом із запитом на асоціацію (підключення);
- точка доступу розшифровує текст і порівнює з вихідними даними, у разі збігу, відсилає підтвердження асоціації, і клієнт вважається підключеним до мережі.

Аутентифікація за MAC-адресою – виконує аутентифікацію шляхом порівняння MAC-адреси клієнта з таблицею дозволених MAC-адрес, що зберігається на точці доступу. Як правило, використовується як додатковий заходу захисту.

Wi-Fi Protected Access (WPA) і WI-FI Protected Access2 (WPA2) – оновлена система аутентифікації бездротових пристроїв, що прийшла на зміну застарілому WEP. Як основний шифр використовується стійкий блоковий шифр AES. В WPA та в WPA2 є два варіанти аутентифікації WPA2-Enterprise з аутентифікацією на RADIUS сервері та WPA2-PSK з передвстановленим ключем.

Завдання

1. Створити мережеву топологію, представлену на рис. 9.1.
2. Використовуючи графічний інтерфейс користувача бездротового маршрутизатора Linksys, 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 «11111111»;
 - 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 мережевого 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 мережевих ресурсів (перехресне тестування з'єднання, доступ до серверів DHCP, DNS, HTTP).
6. Заповнити таблицю 9.1.
7. Заповнити таблицю 9.2 описом стандартів, що регламентують роботу бездротових мереж.

Таблиця 9.1 – Таблиця комутації

Ім'я пристрою	Порт	IP-адреса	Маска

Таблиця 9.2 – Опис стандартів бездротових мереж

Стандарт	Дата виходу	Частота	Швидкість	Радіус дії
802.11				
802.11a				
802.11b				
802.11g				
802.11n				

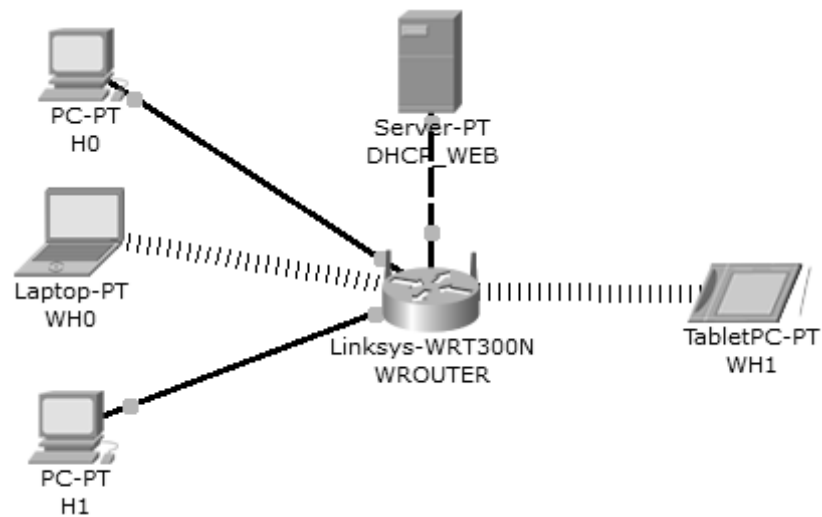


Рисунок 9.1 – Топологія мережі

Контрольні питання

1. Які переваги використання бездротових комп'ютерних мереж?
2. Наведіть приклади технологій та стандартів для організації роботи бездротових мереж.
3. Які особливості роботи технології Bluetooth?
4. Що таке сота?
5. Наведіть приклади методів аутентифікації у бездротових мережах.

Лабораторна робота №10. Статична маршрутизація

Мета: закріпити теоретичні основи та здобути практичні навички налаштування статичної маршрутизації.

Теоретичні відомості

При розширенні комп'ютерних мереж, зазвичай, доводиться ділити одну локальну мережу на декілька підмереж. Причини та критерії ділення можуть бути різними:

- фізичне місце розташування;
- логічна функція;
- вимоги безпеки;
- вимоги програм.

Маршрутизатор є основним мережевим пристроєм, що зв'язує локальні мережі, направляє трафік (виконує передачу пакетів) та виконує інші важливі для ефективної роботи мережі функції.

Маршрут – послідовність маршрутизаторів, через які повинен пройти пакет.

Протоколи маршрутизації – це правила, за якими здійснюється обмін інформацією про шляхи передачі пакетів між маршрутизаторами.

Одна з головних задач маршрутизатора полягає у визначенні найкращого шляху до заданого адресату. Маршрутизатор визначає шляхи (маршрути) до адресатів або зі **статичної** конфігурації, введеної адміністратором, або **динамічно** на підставі маршрутної інформації, отриманої від інших маршрутизаторів.

Маршрутизатори передають дані тільки **між різними мережами** і для цього використовують таблиці маршрутів, які зберігаються в оперативній пам'яті. У більшості ОС таблиці маршрутизації містять наступні поля:

- **адреса призначення** – адреса мережі (вузла), для якої призначений маршрут;
- **маска** – маска, що відповідає адресі, вказаній в полі адреса призначення;
- **шлюз** – IP-адреса інтерфейсу маршрутизатора, якому має бути переданий пакет;
- **інтерфейс** – ідентифікатор інтерфейсу, через який має бути переданий пакет.

Маршрутизатор використовує цю таблицю для прийняття рішення куди направляти пакет за декілька кроків.

1. Для визначення маршруту з кожним рядком таблиці проводяться наступні дії (рядок для маршрутизатора за замовчуванням обробляється останнім):

- виконується операція накладення значення поля "Маска" на IP-адресу одержувача;
- отримане значення порівнюється зі значенням поля "Адреса призначення", якщо значення збігаються, то система запам'ятовує рядок таблиці.

2. Якщо на попередньому кроці було знайдено один рядок, то з поля "Шлюз" цього рядка обирається адреса шлюзу, який буде використаний для передачі пакета. Якщо знайдено кілька рядків, то використовують рядок з найбільшою кількістю одиниць у масці. Якщо рядків не виявлено, пакет знищується і відправнику надсилається повідомлення про помилку за допомогою протоколу ICMP.

Якщо на маршрутизаторі не налагоджена маршрутизація, то він будує таблицю маршрутів для безпосередньо приєднаних до нього мереж, наприклад, для мережі, зображеної на рис. 10.1, вона має наступний вигляд:

```
192.168.1.0/24 is directly connected, FastEthernet0/0
192.168.2.0/24 is directly connected, FastEthernet0/1
```

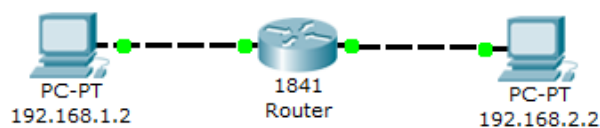


Рисунок 10.1 – Приклад мережі з маршрутизатором

Таблиці маршрутизації комп'ютерів і маршрутизаторів можуть містити записи для маршрутизатора за замовчуванням.

Маршрутизатор за замовчуванням (default router) – це маршрутизатор, якому буде передано пакет в тому випадку, коли інші рядки таблиці маршрутизації не описують шлях до вузла-одержувача.

Завдання

1. Створити мережеву топологію, наведену на рисунку 10.2.
2. Розбити наявний пул (діапазон) адрес 192.168.X.0 / 24 на 4 підмережі з необхідною кількістю адрес вузлів з урахуванням того, що в кожній підмережі буде не більше десяти хостів (X – номер студента в журналі академічної групи).
3. Призначити кожній з підмереж відповідні IP-адреси, визначивши при цьому як шлюз, максимально можливу адресу в заданій підмережі.
4. Для «нульового - першого» і «нульового - другого» маршрутизаторів визначити статичні маршрути необхідні для пересилки пакетів між будь-якими кінцевими вузлами з'єднаних з ними підмереж.

5. Організувати передачу пакетів між першим і другим маршрутизаторами використовуючи маршрути за замовчуванням.

6. Підготувати звіт, до якого включити:

- скріншот топології, створеної при виконанні роботи;
- Таблицю 10.1 з адресами свого варіанта.

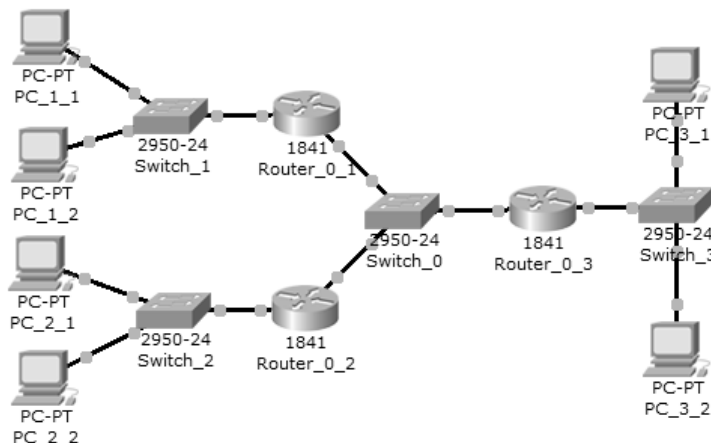


Рисунок 10.1 – Топологія мережі

Таблиця 10.1 – Таблиця комутації

	Підмережа №1 (192.168.X.Y)	Підмережа №2 (192.168.X.Y)	Підмережа №3 (192.168.X.Y)	Підмережа №4 (192.168.X.Y)
Router_0_1	E0: 192.168.X.Y	—	—	E1: 192.168.X.Y
...				
PC_0_1	E0: 192.168.X.Y
PC_0_2				
...				

Контрольні питання

1. Як відправник дізнається MAC-адресу одержувача?
2. Як подивитися ARP таблицю?
3. Коли в ARP таблиці з'являються нові рядки?
4. Що таке таблиця маршрутів?
5. Що містить таблиця маршрутизації, якщо адміністратор не налаштовував ніяких маршрутів?

Контрольні завдання та тести

Модульний тест №1. Стек протоколів TCP/IP та еталонна модель OSI

1. Який з перерахованих нижче протоколів відноситься до транспортного (transport) рівня моделі TCP / IP?

- a) Ethernet
- b) HTTP
- c) IP
- d) UDP
- e) SMTP
- f) TCP

2. Який з перерахованих нижче протоколів працює на рівні доступу до мережі (network access) моделі TCP/IP?

- a) Ethernet
- b) HTTP
- c) IP
- d) UDP
- e) SMTP

3. Коли протокол HTTP використовує TCP для передачі будь-яких даних та контролю доставки, такий процес буде прикладом:

- a) взаємодії двох систем на однаковому рівні
- b) взаємодії двох суміжних рівнів
- c) еталонної моделі OSI
- d) усі зазначені вище відповіді правильні

4. Прикладом якої саме технології є процес, коли протокол TCP вузла відправника маркує сегмент порядковим номером рівним 1, а приймаючий вузол відправляє у відповідь підтвердження прийому з порядковим номером 1?

- a) інкапсуляція даних
- b) взаємодія двох систем на однаковому рівні
- c) взаємодія двох суміжних рівнів
- d) еталонна модель OSI
- e) жодна із зазначених вище відповідей не правильна

5. Прикладом якої саме технології є процес, коли служба веб-сервера додає до поля даних, в яке поміщена веб-сторінка, заголовок протоколу TCP, далі додає заголовок протоколу IP, а потім додає заголовок і кінцевик канального рівня?

- a) інкапсуляція даних
- b) взаємодія двох систем на однаковому рівні
- c) еталонна модель OSI
- d) жодна із зазначених вище відповідей не правильна

6. Який з рівнів моделі OSI відповідає за логічну адресацію в рамках всієї мережі та маршрутизацію?

- a) рівень 1
- b) рівень 2
- c) рівень 3
- d) рівень 4
- e) рівень 5
- f) рівень 6
- g) рівень 7

7. Скільки доменів колізій у мережі, зображеній на рис. 11.1?

- a) 1 домен колізій
- b) 2 домени колізій
- c) 8 доменів колізій
- d) доменів колізій немає

8. Якщо H3 відправляє повідомлення H6 (рис. 11.1), які вузлові пристрої отримають повідомлення?

- a) тільки H6
- b) тільки вузли, що підключені до концентратору А
- c) тільки вузли, що підключені до концентратору В
- d) усі вузли мережі

9. Скільки доменів колізій у мережі, представлений на рисунку 11.2?

- a) 1 домен колізій
- b) 2 домени колізій
- c) 3 домени колізій
- d) 10 доменів колізій
- e) 12 доменів колізій

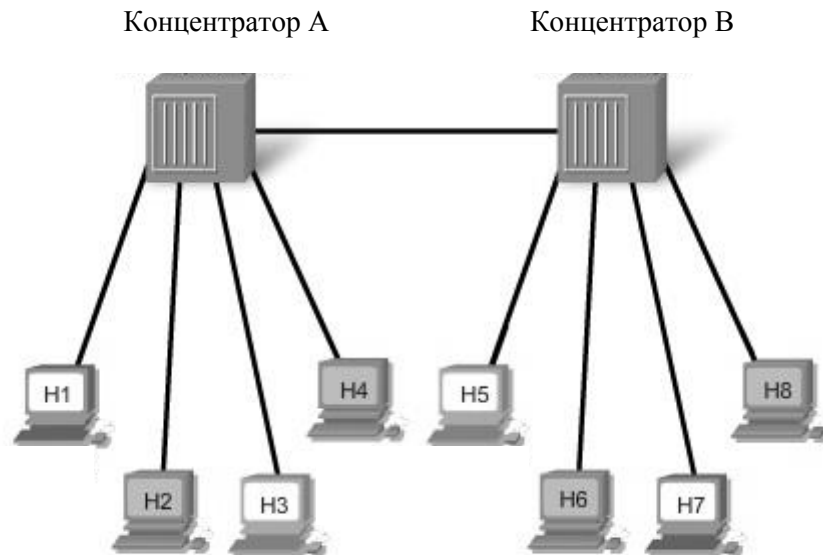


Рисунок 11.1. – Комп'ютерна мережа з концентраторами

10. Якщо вузол 8 (рис 11.2) відправляє повідомлення вузлу 1 і MAC-адреса призначення знаходиться в MAC-таблиці, які вузлові пристрої отримають повідомлення?

- а) тільки У1
- б) усі вузли, підключені до концентратора
- в) усі вузли, підключені до комутатора 1
- г) усі вузли, підключені до концентратора, і всі вузли, підключені до комутатора 1
- д) усі вузли мережі

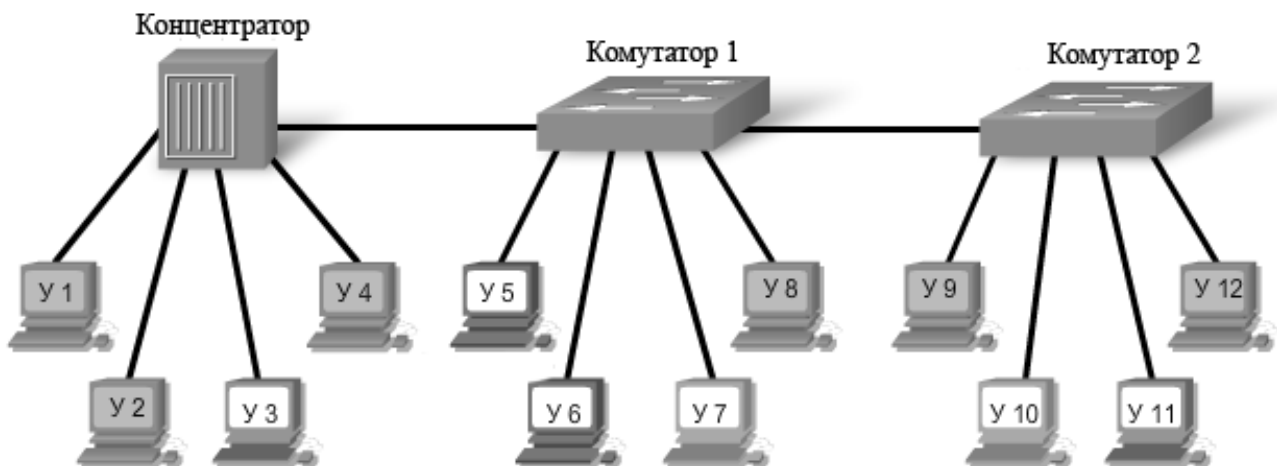


Рисунок 11.2. – Комп'ютерна мережа з концентратором та комутаторами

Модульний тест №2. Підключення до комп'ютерної мережі

1. Технік налаштовує обладнання. Яким трьома пристроями знадобляться IP-адреси?

- a) принтер з платою Ethernet
- b) веб-камера, напряму з'єднана з хостом
- c) сервер з двома NIC адаптерами
- d) IP-телефон
- e) автономна робоча станція
- f) кишеньковий ПК, з'єднаний з робочою станцією, підключеною до мережі

2. Співставте значення першого октету з класом адреси (А, В, С). Зауважте, що будуть використані не всі значення першого октету, показані зліва.

- a) значення першого октету 0
- b) значення першого октету 126
- c) значення першого октету 130
- d) значення першого октету 200
- e) значення першого октету 224
- f) значення першого октету 240

3. Яке твердження є правильним стосовно адрес у приватній мережі?

- a) вони завжди передаються через інтернет
- b) вони можуть одночасно використовуватися тільки однією компанією;
- c) вони забезпечують легкий доступ зовнішніх користувачів до внутрішніх веб-серверів
- d) вони є більш захищеними, оскільки вони видимі тільки для локальної мережі

4. Скільки мереж класу С зарезервовані для простору приватних адрес?

- a) 1
- b) 16
- c) 128
- d) 256

5. Яка кінцева MAC-адреса широкошовного кадру Ethernet?

- a) 255.255.255.255

- b) 1.1.1.1;
- c) AA-AA-AA-AA-AA-AA;
- d) FF-FF-FF-FF-FF-FF.

6. Які твердження відповідають статичній IP-адресації?

- a) корисна для принтерів і серверів
- b) дозволяє краще контролювати мережеві ресурси
- c) ймовірність помилок введення
- d) корисна для мобільних користувачів
- e) обмежує час використання адреси
- f) адреса надаються сервером
- g) автоматично вилучає адреси з пулу
- h) адреси не присвоюються повторно іншому пристрою

7. Оберіть твердження, які відповідають динамічній IP-адресації.

- a) корисна для принтерів і серверів
- b) дозволяє краще контролювати мережеві ресурси
- c) ймовірність помилок введення
- d) корисна для мобільних користувачів
- e) обмежує час використання адреси
- f) адреса надаються сервером
- g) автоматично вилучає адреси з пулу
- h) адреси не присвоюються повторно іншому пристрою

8. Розмістіть дані повідомлення DHCP в порядку отримання хостом IP-адреси від сервера DHCP.

- a) DHCP-запит
- b) пошук DHCP
- c) пропонування DHCP
- d) підтвердження DHCP

9. Що станеться, якщо у топології, представлений на рис. 1, H3 та H4 одночасно відправляти повідомлення через концентратор А?

- a) станеться колізія двох кадрів, і концентратор передасть викривлене повідомлення всім вузлам мережі
- b) станеться колізія двох кадрів, і концентратор передасть викривлене повідомлення тільки вузлу-джерелу і вузлу призначення
- c) два кадри будуть передані потрібному пристрою без виникнення колізії

d) два вузли не можуть відправляти інформацію через концентратор одночасно, оскільки вони повинні спочатку дочекатися кадру «запиту» даних від концентратора

10. Що відбудеться, якщо у топології, представлений на рис. 2, Н9 і Н12 одночасно відправлять повідомлення через комутатор 2?

a) відбудеться колізія двох кадрів, і комутатор передасть викривлене повідомлення всім вузлам мережі

b) відбудеться колізія двох кадрів, і комутатор передасть викривлене повідомлення тільки вузлу джерела та передбачуваному вузлу призначення.

c) два кадри будуть передані відповідному вузлу призначення без виникнення колізії.

d) два вузли не можуть відправляти інформацію через комутатор одночасно, оскільки вони повинні спочатку дочекатися кадру запиту даних від комутатора.

Предметний покажчик

Ad-hoc, 46

AMI, 28

Bluetooth, 45

DHCP, 41

Ethernet, 16

FTP, 10

Hot-spot, 46

IP-адреса, 6, 31

MAC-адреса, 6

NRZ, 27

NRZI, 28

PDU, 17

SSID, 46

Telnet, 10

WPA, 47

WPA2, 47

Амплітудна модуляція, 26

Аналогова модуляція, 25

Аутентифікація, 47

Аутентифікація за MAC-адресою, 47

Аутентифікація із загальним ключем, 47

Біполярний імпульсний код, 29

Відкрита аутентифікація, 47

Декапсуляція, 15

Доменом колізій, 21

Імпульсний код, 26

Інкапсуляція, 15

Кадр, 15

Колізія, 21

Комп'ютерна мережа, 6

Комутатор, 21

Концентратор, 20

Манчестерський код, 29

Маршрут, 50

Маршрутизатор, 37

Маршрутизатор за замовчуванням, 51

Маска, 32

Мережевий адаптер, 6

Мережевий міст, 21

Мережеві носії, 20

Мережеві пристрої, 20

Модем, 25

Модуляція, 25

Обмежене широкомовлення, 32

Повторювач, 20

Потенціальний код 2B1Q, 29

Потенційний код, 26

Префікс, 32

Приватні адреси, 32

Протокол, 10

Протокольний блок даних, 17

Сегмент, 21

Сота, 46

Фазова модуляція, 26

Фронт, 29

Цифрове кодування, 25

Частотна модуляція, 26

Шлюз, 39

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

1. Программа сетевой академии Cisco CCNA 1 и 2 : вспомогательное руководство / Корпорация Cisco Systems, Inc. – М. : Вильямс, 2008. – 1170 с.
2. Программа сетевой академии Cisco CCNA 3 и 4 : вспомогательное руководство / Корпорация Cisco Systems, Inc. – М. : Вильямс, 2008. – 900 с.
3. Одом У. Компьютерные сети. Первый шаг / У. Одом. – М. : Вильямс, 2006. – 403 с.
4. Одом У. Официальное руководство по подготовке к сертификационным экзаменам CCENT/CCNA ICNDI / У. Одом. – М. : Вильямс, 2010. – 670 с.
5. Олифер В.Г. Компьютерные сети: Принципы, технологии, протоколы: учебник для вузов. / В.Г. Олифер, Н.А. Олифер. – СПб.: Питер, 2010. – 672с.
6. Столлингс В. Компьютерные сети, протоколы и технологии Интернета / В. Столлингс. – СПб.: Петер, 2005. – 780 с.
7. Таненбаум. Э. Компьютерные сети. / Э. Таненбаум. – СПб.: Питер, 2003 – 993 с.

Додаткова:

1. Закер К. Компьютерные сети. Модернизация и поиск неисправностей / К. Закер. – СПб: Петер, 2004. – 1008с.
2. Джеймс Ф.К. Компьютерные сети: Многоуровневая архитектура Интернета / Ф. К. Джеймс, В. Р Кит. – СПб: Питер, 2004. – 731 с.
3. Стивенс У. Протоколы TCP/IP: В подлиннике / У. Стивенс – СПб.: Питер, 2003. – 672 с.
4. Стерн М. Сети предприятий на основе Windows NT для профессионалов. / М. Стерн. Г. Монти, В. Бэчманн. – СПб: Питер, 1999. – 448 с.

Навчально-методичне видання
(українською мовою)

Лісняк Андрій Олександрович
Чопоров Сергій Вікторович
Козлова Ольга Станіславівна
Решевська Катерина Сергіївна

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНИХ МЕРЕЖ

Методичні вказівки до лабораторних занять для студентів
освітньо-кваліфікаційного рівня «бакалавр» напрямку
підготовки «Програмна інженерія».

Рецензент *С.М. Гребенюк*
Відповідальний за випуск *А.О. Лісняк*
Коректор *О.С. Козлова*