

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»



ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних технологій та комп'ютерної інженерії

В.Ю. Каштан, Я.В. Панферова, Л.В. Бешта

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра
зі спеціальності F7 Комп'ютерна інженерія

У 2 частинах

Частина 1

Дніпро
НТУ «ДП»
2026

Комп'ютерні мережі [Електронний ресурс] : методичні рекомендації до виконання лабораторних робіт з дисципліни «Комп'ютерні мережі» для здобувачів ступеня бакалавра зі спеціальності F7 Комп'ютерні науки : у 2 ч. / уклад.: В.Ю. Каштан, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро : НТУ «ДП», 2026. – Ч. 1. – 53 с.

Укладачі:

В.Ю. Каштан, канд. техн. наук, доц.;

Я.В. Панферова, асист.;

Л.В. Бешта, асист.

Затверджено науково-методичною комісією зі спеціальності F7 Комп'ютерна інженерія (протокол № 6 від 09.06.2026 р.) за поданням кафедри інформаційних технологій та комп'ютерної інженерії (протокол № 21 від 09.06.2026 р.).

Методичні рекомендації містять опис методики виконання лабораторних робіт з дисципліни «Комп'ютерні мережі» студентами спеціальності F7 Комп'ютерна інженерія.

Орієнтовано на активізацію навчальної діяльності здобувачів ступеня бакалавра спеціальності F7 Комп'ютерна інженерія та закріплення практичних навичок у засвоєнні дисципліни «Комп'ютерні мережі».

Відповідальний за випуск завідувач кафедри інформаційних технологій та комп'ютерної інженерії В.В. Гнатушенко, д-р техн. наук, проф.

ЗМІСТ

Вступ.....	5
1 Лабораторна робота №1. Вивчення інтерфейсу програми Wireshark.....	6
1.1 Мета лабораторної роботи.....	6
1.2 Організація виконання лабораторної роботи	6
1.3 Зміст звіту.....	9
1.4 Питання для підготовки до захисту лабораторної роботи	9
2 Лабораторна робота №2. Отримання відомостей про MAC-адреси і мережні налаштування TCP/IP.....	10
2.1 Мета лабораторної роботи.....	10
2.2 Організація виконання лабораторної роботи	10
2.3 Зміст звіту.....	10
2.4 Питання для підготовки до захисту лабораторної роботи	10
3 Лабораторна робота №3. Дослідження кадру протоколу Ethernet та пропускну здатності Fast Ethernet.....	11
3.1 Мета лабораторної роботи.....	11
3.2 Організація виконання лабораторної роботи	11
3.3 Зміст звіту.....	13
3.4 Питання для підготовки до захисту лабораторної роботи	13
4 Лабораторна робота №4. Мережні пристрої і засоби комунікацій. Середовище моделювання Cisco Packet Tracer.....	15
1.1 Мета лабораторної роботи.....	15
4.1 Організація виконання лабораторної роботи	15
4.2 Зміст звіту.....	20
4.3 Питання для підготовки до захисту лабораторної роботи	21
5 Лабораторна робота №5. Вивчення протоколу ARP	22
5.1 Мета лабораторної роботи.....	22
5.2 Організація виконання лабораторної роботи	22
5.3 Зміст звіту.....	24
5.4 Питання для підготовки до захисту лабораторної роботи	25
6 Лабораторна робота №6. Дослідження моделей TCP/IP і OSI	26
6.1 Мета лабораторної роботи.....	26
6.2 Організація виконання лабораторної роботи	26
6.3 Зміст звіту.....	28
6.4 Питання для підготовки до захисту лабораторної роботи	28
7 Лабораторна робота №7. Розрахунок підмереж.....	29
7.1 Мета лабораторної роботи.....	29
7.2 Організація виконання лабораторної роботи	29
7.3 Зміст звіту.....	33
7.4 Питання для підготовки до захисту лабораторної роботи	34
8 Лабораторна робота №8 Побудова мережі в Cisco Packet Tracer і базове налаштування та захист проміжних пристроїв	35

8.1 Мета лабораторної роботи.....	35
8.2 Організація виконання лабораторної роботи	35
8.3 Зміст звіту.....	42
8.4 Питання для підготовки до захисту лабораторної роботи.....	42
9 Лабораторна робота №9 Впровадження і налаштування сервісів web-серверу, серверу електронної пошти, DHCP, DNS та FTP.....	44
9.1 Мета лабораторної роботи.....	44
9.2 Організація виконання лабораторної роботи	44
9.3 Зміст звіту.....	47
9.4 Питання для підготовки до захисту лабораторної роботи.....	47
Додаток А Мережні та діагностичні команди Windows	49
Додаток Б Розрахунок пропускної здатності мережі Fast Ethernet	50
Список рекомендованих джерел.....	52

ВСТУП

Методичні рекомендації призначені для студентів спеціальності F7 Комп'ютерна інженерія, що вивчають дисципліну «Комп'ютерні мережі».

Методичні рекомендації включають низку частково взаємопов'язаних робіт, під час виконання яких студенти мають можливість отримати досвід роботи з мережним аналізатором Wireshark, командами операційної системи Windows, протоколами Ethernet, ARP, IP, TCP, UDP, HTTP, DHCP, DNS та FTP. Визначати типи IP-адрес та навчитися організовувати підмережі за допомогою маски постійної та змінної довжини.

Перед виконання лабораторної роботи студенти повинні:

- ознайомитися з методичними вказівками;
- повторити лекційний матеріал, пов'язаний з лабораторною роботою;
- підготувати відповіді на питання, які наведені у методичних вказівках наприкінці кожної лабораторної роботи.

Виконавши ці завдання, студент повинен продемонструвати викладачеві роботу на комп'ютері або в зошиті, оформити звіт за результатами даної лабораторної роботи, захистити його та здати викладачеві.

При своєчасному (протягом двох тижнів від дати проведення заняття) та вірному виконанні завдання здобувач отримує оцінку 10. з яких:

- 8 балів: виконання та оформлення лабораторної роботи;
- 2 бали: захист лабораторної роботи.

При несвоєчасному виконанні завдання -1 бал за кожен прострочений тиждень.

Критерії оцінювання лабораторних робіт:

Бали за виконання та оформлення	
8	роботу виконано повністю, налаштування правильні, результати перевірено, звіт оформлено належним чином;
6-7	роботу виконано переважно правильно, але наявні окремі неточності, які не впливають істотно на загальний результат;
4-5	роботу виконано частково, наявні помилки в налаштуваннях або недостатньо представлено результати перевірки;
1-3	виконано лише окремі етапи, мережа працює частково, звіт неповний;
0	роботу не виконано або поданий результат не відповідає завданню.
Бали за захист	
2	здобувач упевнено пояснює виконані налаштування й отримані результати та правильно відповідає на запитання;
1	здобувач розуміє основний зміст роботи, але допускає неточності у відповідях;
0	здобувач не може пояснити виконання роботи та не відповідає на основні запитання.

1 ЛАБОРАТОРНА РОБОТА №1.

ВИВЧЕННЯ ІНТЕРФЕЙСУ ПРОГРАМИ WIRESHARK

1.1 Мета лабораторної роботи

Ознайомитись з програмою Wireshark для аналізу мережних протоколів. Вивчити інтерфейс програми, її основні функціональні можливості, отримати практичні навички з написання фільтрів. Вивчити стек TCP/IP та взаємодію протоколів.

1.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

- робота з командним рядком операційної системи Windows 7;
- діагностичні команди та засоби Windows 7 для роботи в мережі;
- модель OSI та взаємодія протоколів;
- стек протоколів TCP/IP;
- функціональні можливості програми Wireshark;
- правила написання фільтрів для аналізаторів мережних протоколів.

Далі виконати такі дії:

- запустити програму Wireshark;
- відкрити вікно конфігурації захвату (рис. 1.1). Для цього потрібно перейти в меню *Capture->Options* або по комбінації клавіш CTRL+K;
- обрати інтерфейс, на якому буде виконуватися захоплення пакетів;

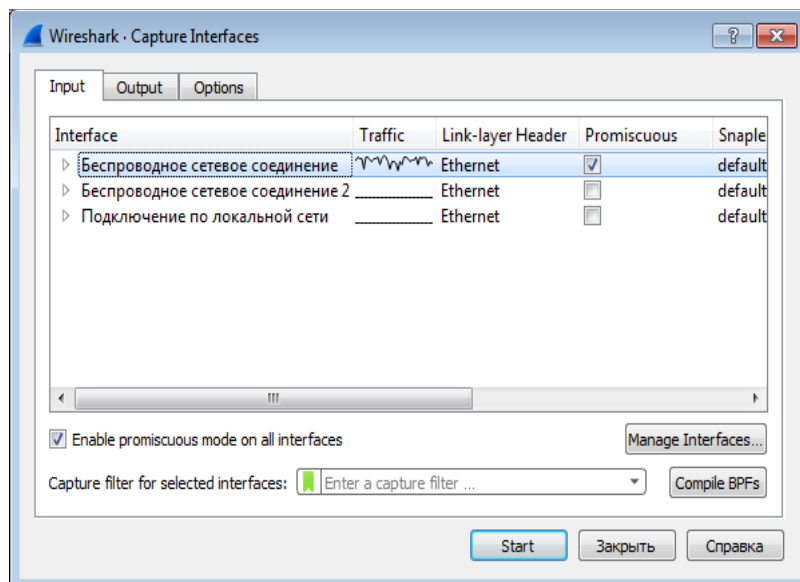


Рисунок 1.1 – Вікно опцій захвату

- відкрити командний рядок (*Пуск->Система Window->Командний рядок*) або на панелі пошуку в Windows ввести *cmd*;
- переглянути список доступних сусідніх вузлів;
`>net view`

– відправити ехо-запити на IP-адреси сусідніх вузлів а за їх відсутності на адресу шлюза, наприклад;

```
>ping 192.168.1.1
```

Щоб дізнатися адресу шлюзу, в командному рядку ввести команду «ipconfig» і знайти параметр *Default Gateway* мережної карти, на якій ведеться передача даних;

```
Connection-specific DNS Suffix . . :  
Link-local IPv6 Address . . . . . : fe80::a590:ab43:2233:423b%10  
IPv4 Address. . . . . : 192.168.0.111  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 192.168.0.1
```

Рисунок 1.2 – Мережні налаштування мережного адаптера

– зупинити захват пакетів в Wireshark (на панелі інструментів  або через меню *Capture->Stop* (Ctrl+E) та використовуючи пункти меню *Statistics->Capture File Properties* (Ctrl+Alt+Shift+C) визначити характеристики отриманого мережного трафіку, а саме:

- 1) які протоколи використовувались в мережі;
- 2) відсоткове співвідношення трафіку різних протоколів в мережі;
- 3) середню швидкість трафіку (кадрів/с, байт/с);
- 4) мінімальний і максимальний розміри кадрів;
- 5) IPv4-адреси и порти TCP та UDP, між якими велася передача даних.

– візуалізувати графік отриманих даних за допомогою пункту меню *Statistics->Io Graphs*;

– візуалізувати інформаційні потоки за допомогою пункту меню *Statistics->Flow Graph*;

– обрати будь-який з захоплених пакетів і перелічити його заголовки та їх розмір;

– визначити IP та MAC-адреси в трафіку через меню *Statistics->Endpoints*;

– налаштувати фільтр на відображення пакетів ARP та ICMP (рис. 1.3);

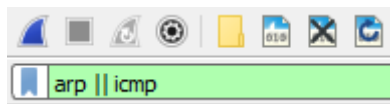


Рисунок 1.3 – Поле фільтру на відображення пакетів ARP та ICMP

– зберегти захоплені пакети в файл *File->Save as...* та разом зі звітом надати викладачу;

– відкрити в Wireshark наданий викладачем файл с захопленими пакетами під час підключення до маршрутизатора по Telnet на ПК. Визначити IP-адреси пристроїв. Визначити пароль, який передавався під час встановлення сеансу до маршрутизатора. Для цього на будь-якому пакеті, в якому велася передача даних по Telnet, натиснути правою кнопкою і вибрати *Follow ->TCP Stream* або на панелі меню *Analyze->Follow ->TCP Stream* (рис.1.4);

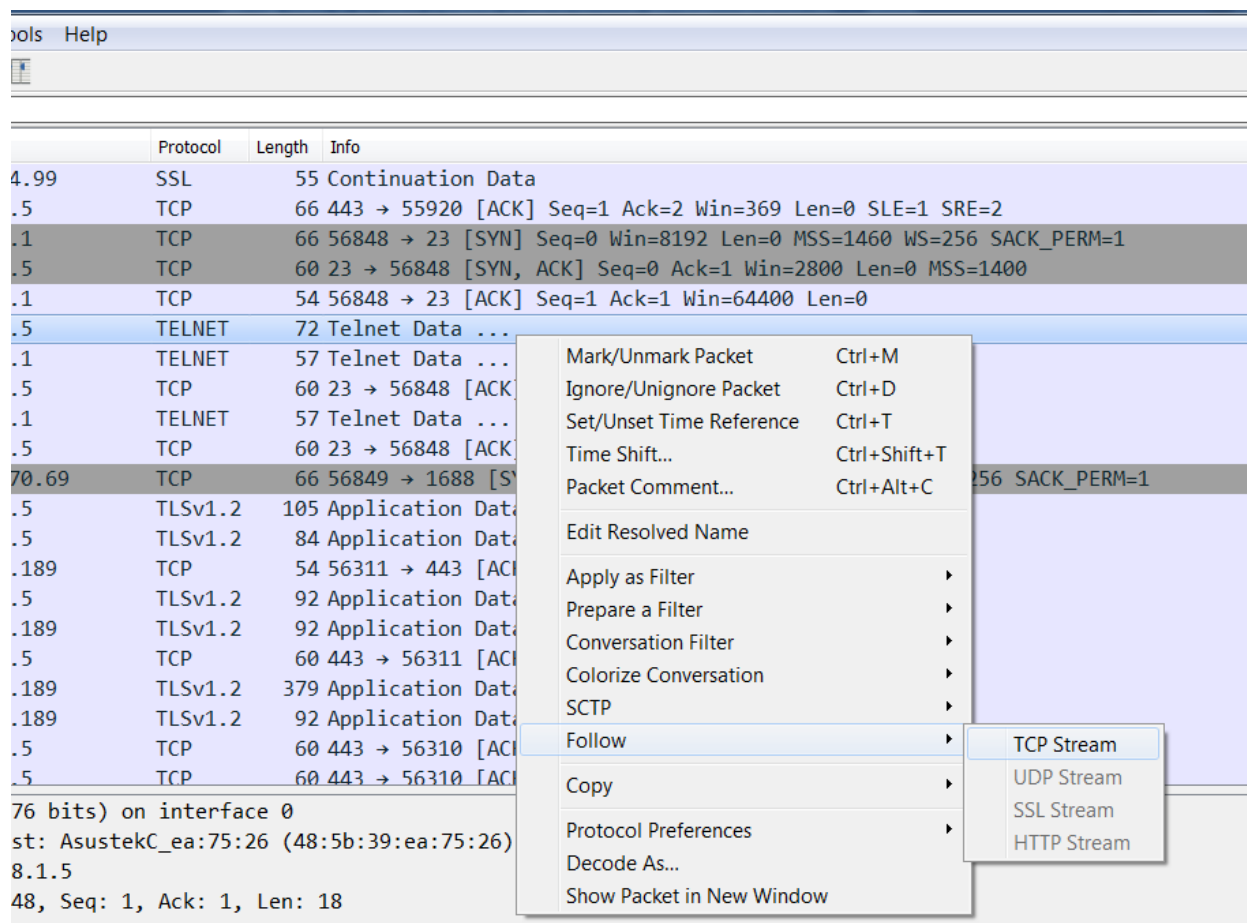


Рисунок 1.4 – Відстеження всього потоку TCP для обраного пакету

– привести приклад написання фільтру відображення по варіанту згідно таблиці 1.1.

Таблиця 1.1 – Варіанти фільтрів відображення

№	Фільтр відображення
1.	Тільки трафік від вузлів з MAC-адресами виробника TP-LINK, які починаються з f4:f2:6d.
2.	Тільки трафік icmp, виключаючи ехо-запити (type=8) та ехо-відповіді (type=0).
3.	IP-пакети від вузла 192.168.0.5 довжиною більше 1450 байт.
4.	Тільки трафік між машинами в локальній підмережі 192.168.30.0/24.
5.	IP-пакети з встановленим прапором фрагментації (mf) від вузла 10.0.0.5.
6.	TCP-пакети з встановленим прапором зняття з'єднання (res) на порт 23.
7.	TCP-пакети з вузла 192.168.10.5 з встановленим прапором встановлення з'єднання (syn).
8.	Весь вхідний трафік, виключаючи трафік SSH (TCP порт 22) генерований вузлом 192.168.5.101.
9.	Тільки трафік від вузла з MAC-адресом f4:f2:6d:54:a0:78, які включали в себе DNS-запити.

Продовження табл. 1.1

№	Фільтр відображення
10.	Широкомовний трафік без ARP-запитів.
11.	Всі HTTP-запити типу GET на адрес 91.198.36.14 .
12.	IGMP-звіти приналежності (Membership Query Message) до групи 224.0.0.113.
13.	Тільки ARP-запити від вузла 192.168.0.10.
14.	Тільки DHCP-запити від вузла з MAC-адресом 6c:f0:49:70:ba:8b.
15.	Тільки DHCP-відповіді від вузла 192.168.0.1 MAC-адрес 6c:f0:49:70:ba:8b.
16.	Тільки пакети з широкомовними адресами 255.255.255.255 на порт призначення 68 протоколу UDP.
17.	IP-пакети між машинами в локальній підмережі 180.15.30.0/24 з довжиною пакету більше 1400 байт.
18.	FTP-пакети с запитамі від клієнта 185.15.1.10.
19.	DNS-пакети від вузла 192.168.15.26
20.	Всі ARP-відповіді крім вузла 192.168.0.10.
21.	Всі telnet-пакети з командою «End of File» від вузла 195.15.2.3.
22.	Всі DHCP-пакети від вузла 192.168.0.5.
23.	Тільки broadcast (ff:ff:ff:ff:ff:ff) і multicast-пакети (починаються з 01:00:5e) мережі 172.16.0.0/16.
24.	Тільки ARP-відповіді від вузла 192.168.0.10
25.	Тільки пакети http, які містили javascript в полі content_type.

1.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- опис завдання з початковими умовами та даними;
- статичні дані захопленого мережного трафіку;
- скріншоти програми Wireshark в ході виконання роботи з описом дій;
- фільтр відображення по варіанту згідно таблиці 1.1.

1.4 Питання для підготовки до захисту лабораторної роботи

1. У якому випадку вузол може бачити всі пакети в сегменті Ethernet?
2. Який протокол канального рівня підтримує мережа учбового класу?
3. Які типи адрес необхідні для взаємодії вузлів в локальній мережі?
4. Дайте визначення терміну “інкапсуляція”, використовуючи як приклад будь-який захоплений пакет.
5. До якого рівню моделі OSI відноситься протокол IP?

2 ЛАБОРАТОРНА РОБОТА №2. ОТРИМАННЯ ВІДОМОСТЕЙ ПРО MAC-АДРЕСИ І МЕРЕЖНІ НАЛАШТУВАННЯ TCP/IP

2.1 Мета лабораторної роботи

Вивчити мережні налаштування комп'ютера шляхом використання командних утиліт Windows.

2.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

- мережні та діагностичні команди Windows (Додаток А);
- синтаксис діагностичних команд «getmac», «ipconfig», «nbtstat» та «route».

Далі виконати такі дії:

- запустити командний рядок;
- відобразити довідку по використанню команди «ipconfig»;
- вивести повну конфігурацію TCP/IP для всіх адаптерів;
- вивести на екран вміст кешу служби розпізнавання імен DNS;
- оновити мережні налаштування, отримані від DHCP-сервера тільки для адаптера локальної мережі;
- відобразити довідку по використанню команди «getmac»;
- отримати детальну інформацію про MAC-адреси всіх існуючих на локальному комп'ютері мережних адаптерів;
- відобразити довідку по використанню команди «route»;
- відобразити таблицю маршрутизації ПК та проаналізувати її записи;
- відобразити довідку по використанню команди «nbtstat»;
- відобразити таблицю NetBIOS-імен на локальному ПК;
- відобразити розв'язання NetBIOS-імен та статистику реєстрації.

2.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- лістинг командного рядку в ході виконання лабораторної роботи.

2.4 Питання для підготовки до захисту лабораторної роботи

1. Як можна з'ясувати MAC-адресу комп'ютера?
2. Як можна з'ясувати IP-адресу комп'ютера?
3. Як можна з'ясувати MAC-адресу комп'ютера в локальній мережі?
4. Як оновити IP-адрес комп'ютера?
5. Як з'ясувати кеш служби розпізнавання імен DNS?

3 ЛАБОРАТОРНА РОБОТА №3.

ДОСЛІДЖЕННЯ КАДРУ ПРОТОКОЛУ ETHERNET ТА ПРОПУСКНОЇ ЗДАТНОСТІ FAST ETHERNET

3.1 Мета лабораторної роботи

Вивчення формату кадру Ethernet, призначень його полів та адресування в локальних мережах. Дослідження залежності пропускної здатності мережі Fast Ethernet від розміру кадру.

3.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

- функції протоколу Ethernet;
- адресація в Ethernet;
- структура заголовку кадру Ethernet;
- часові параметри Fast Ethernet;
- розрахунок пропускної здатності та часу передачі кадру в мережі Fast Ethernet (Додаток Б).

Виконання лабораторної роботи складається з двох частин. В першій частині необхідно дослідити заголовок кадру Ethernet, перехоплюючи і досліджуючи мережний трафік в Wireshark. В другій частині необхідно дослідити залежність часу передачі файлу завданням розміром та пропускної здатності мережі Fast Ethernet від розміру кадру Ethernet.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Вивчення формату кадру Ethernet, призначень його полів та адресування в локальних мережах

Далі виконати такі дії:

- запустити на ПК командний рядок;
- визначити MAC-адрес мережної плати ПК;
`>ipconfig /all`
- відкрити програму Wireshark і запустити захват пакетів тривалістю в кілька хвилин;
- в командному рядку виконати «ping» на сусідні вузли та шлюз;
- для збільшення інтенсивності генерації кадрів відкрити будь-який сайт в браузері;
- зупинити захват пакетів та отримати відомості про MAC-адреси в заголовках кадрів Ethernet, які були захоплені Wireshark, на відповідній вкладці вікна *Endpoints* (рис.3.1) через меню *Statistics->Endpoints*;
- проаналізувати та законспектувати зі вкладки Ethernet (рис. 3.1), які типи MAC-адрес були захоплені Wireshark;

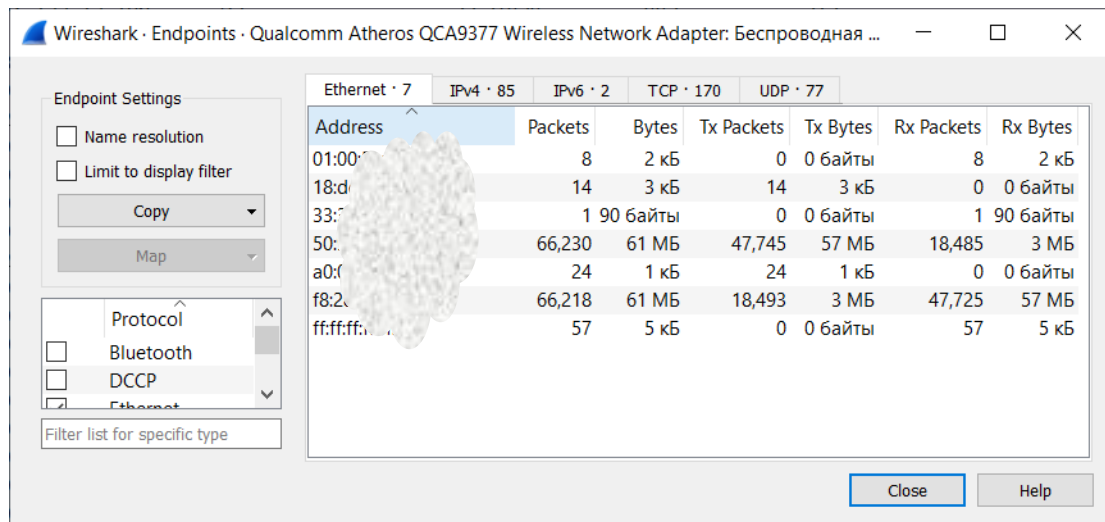


Рисунок 1.1 – Вікно Endpoints

– відфільтрувати MAC-адреси широкомовної розсилки, крім ARP (eth.addr==ff:ff:ff:ff:ff:ff && !arp), проаналізувати та законспектувати всі IP-адреси призначення (рис.3.2);

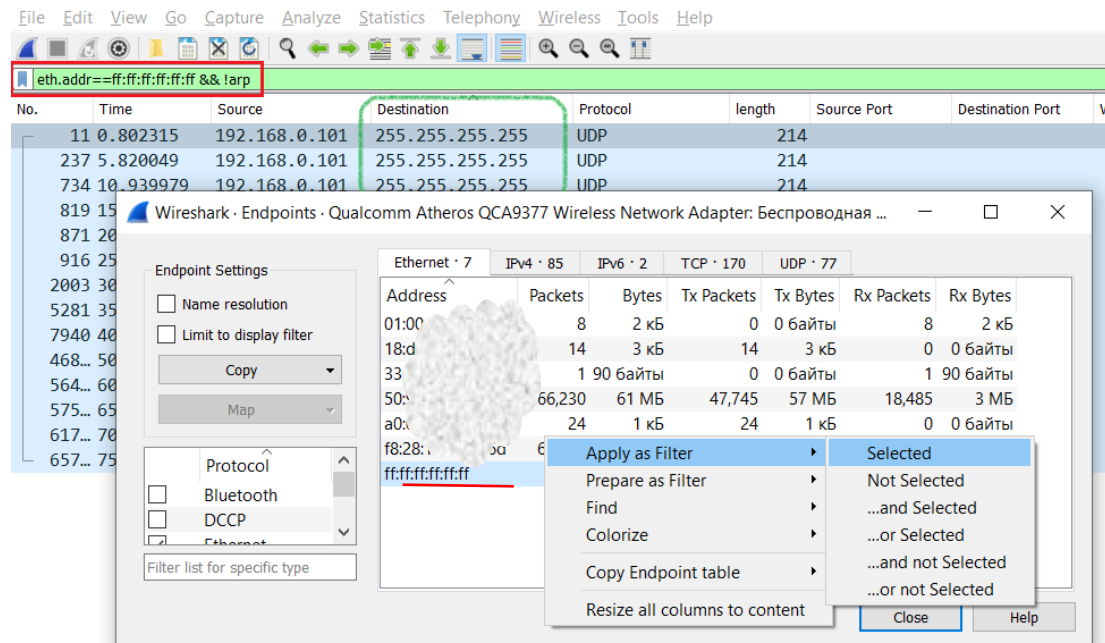


Рисунок 3.1 – Фільтрація широкомовних кадрів

– у вікні захоплених пакетів вибрати будь-який широкомовний пакет і розглянути значення основних полів його заголовку Ethernet II (рис. 3.3). Визначити адреси, на які надходять дані кадри і пакети, для каналного (MAC-адреси) і мережного (IP-адреси) рівня та представити у вигляді таблиці 3.1.

```
> Frame 8: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
[✓] Ethernet II, Src: AsrockIn_a4:57:e6 (bc:5f:f4:a4:57:e6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: AsrockIn_a4:57:e6 (bc:5f:f4:a4:57:e6)
  Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 172.17.29.250, Dst: 172.17.31.255
  > User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
  > NetBIOS Name Service
```

Рисунок 3.2 – Ієрархічна структура заголовків

Таблиця 3.1 – Канальні та мережні адреси в пакеті

MAC Source	
IP Source	
MAC Destination	
IP Destination	

– відфільтрувати MAC-адреси багатоадресної розсилки, якщо вони були захоплені Wireshark. Вибрати будь-який пакет і розглянути значення основних полів його заголовку Ethernet II. Визначити адреси, на які надходять дані кадри і пакети, для канального і мережного рівня у вигляді табл. 3.1.

ЧАСТИНА 2. Дослідження залежності часу передачі файлу та пропускну здатності мережі Fast Ethernet від розміру кадру Ethernet

В цій частині вам необхідно дослідити, як довжина кадру Ethernet впливає на час передачі файлу та на пропускну здатність мережі Fast Ethernet. Використовуючи відомості в Додатку Б необхідно виконати розрахунки для різного значення довжини поля корисних даних кадру Ethernet та побудувати графіки залежності.

Далі виконати такі дії:

– використовуючи відомості в Додатку Б побудувати графік затримки передачі файлу розміром $10 \cdot N_{\text{б}} \text{ Мбайт}$ ($N_{\text{б}}$ - номер за списком в групі) в одному сегменті мережі Fast Ethernet, якщо довжина поля корисних даних кадру N_d буде мати наступні значення: 128, 512, 1000, 1500 та 4096 байт;

– побудувати графік залежності пропускну здатності мережі Fast Ethernet від довжини поля корисних даних кадру N_d , якщо N_d буде мати наступні значення: 128, 512, 1000, 1500 та 4096 байт.

Примітка. Зверніть увагу, що в Додатку Б наведено розрахунок часу передачі для одного кадру довжиною 46 та 1500 байт поля даних, а не всього файлу.

3.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- опис завдання з початковими умовами та даними;
- скрін вікна *Endpoints* з MAC-адресами з визначенням їх типу;
- перелік IP-адрес призначення при фільтрації за широкомовним трафіком;
- перелік IP-адрес призначення при фільтрації багатоадресної розсилки;
- розрахунок та графік затримки передачі файлу;
- розрахунок та графік залежності пропускну здатності мережі.

3.4 Питання для підготовки до захисту лабораторної роботи

1. Чому дорівнюють максимальний та мінімальний розміри кадру Ethernet?
2. Яка частина в MAC-адресі відображає виробника мережної карти?
3. Які типи кадрів Ethernet бувають, в чому їх відмінності?
4. Яка довжина заголовку Fast Ethernet?

5. Як записується широкомовний MAC-адрес Ethernet?

4 ЛАБОРАТОРНА РОБОТА №4. МЕРЕЖНІ ПРИСТРОЇ І ЗАСОБИ КОМУНІКАЦІЙ. СЕРЕДОВИЩЕ МОДЕЛЮВАННЯ CISCO PACKET TRACER

1.1 Мета лабораторної роботи

Ознайомитися з основними мережними пристроями та засобами передачі даних комп'ютерних мереж з використанням середовища моделювання Cisco Packet Tracer.

4.1 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації до даної роботи, наступні питання:

- кінцеві та проміжні пристрої;
- середовище передачі даних;
- топології мереж;
- інтерфейс програми Cisco Packet Tracer.

Необхідно побудувати в Packet Tracer типову модель домашньої мережі, представлену на рисунку 4.1, налаштувати безпечний бездротовий зв'язок, доступ до Internet та IP-адресацію пристрої відповідно до таблиці адресації (табл. 4.1). По завершенні перевірити створену конфігурацію, протестувавши наскрізне з'єднання шляхом звернення до веб-сервера і маршрутизатора провайдера.

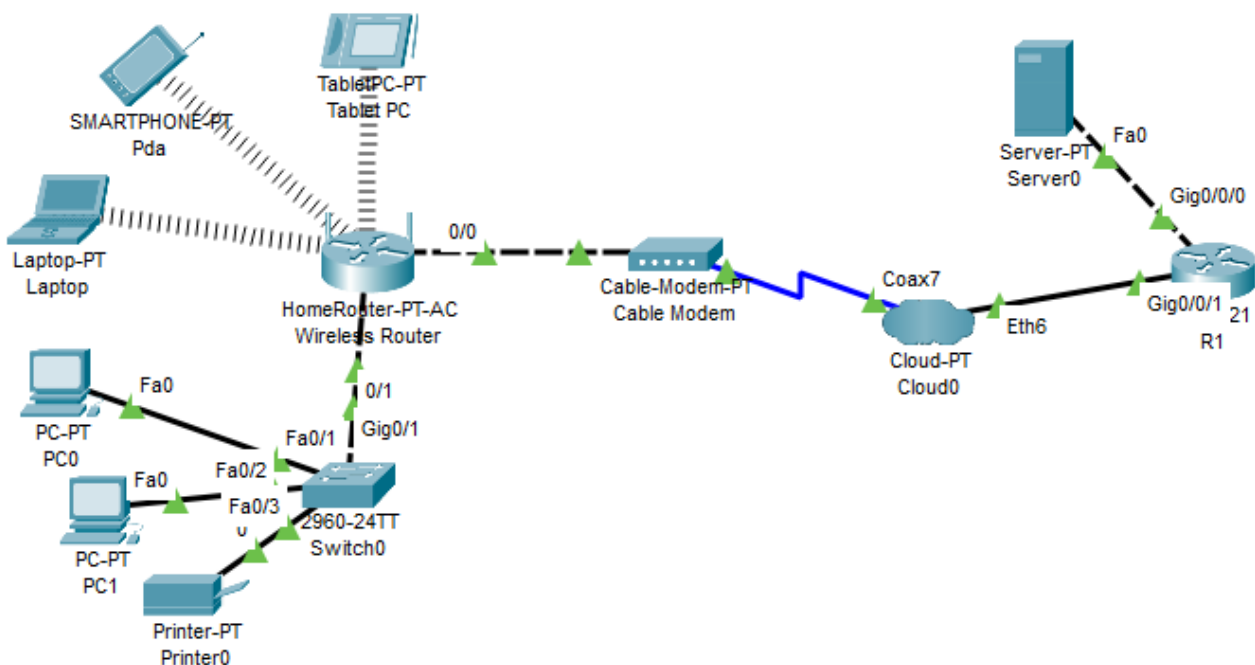


Рисунок 1.1 – Модель мережі

Таблиця 4.1 – Адресація пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	DNS
Wireless Router	LAN	№*10.№.0.1	255.255.255.0	N/A	209.165.201.30
	Internet	209.165.200.226	255.255.255.224	209.165.200.225	
R1	G0/0/1	209.165.200.225	255.255.255.224	N/A	
	G0/0/0	209.165.201.1	255.255.255.224	N/A	
Server0	fe0	209.165.201.30	255.255.255.224	209.165.201.1	
Laptop, Pda Tablet PC	Wireless0	DHCP		№*10.№.0.1	
PC0	fe0	№*10.№.0.3	255.255.255.0	№*10.№.0.1	
PC1	fe0	№*10.№.0.4	255.255.255.0	№*10.№.0.1	
Printer0	fe0	№*10.№.0.10	255.255.255.0	№*10.№.0.1	

де № – номер студента за списком в групі.

Далі виконати такі кроки.

Крок 1. Вибір пристроїв і побудова мережі

1. Запустити програму Packet Tracer.

2. Додати в робочу область пристрої та з'єднати їх між собою, як показано на рис. 4.1. Наприклад, щоб побудувати нижній сегмент мережі, що складається з комутатора, двох ПК та принтера, для цього необхідно додати в робочу область один комутатор серії 2960-24TT з групи елементів *Switches* панелі вибору типових пристроїв і зв'язків (рис.4.2), два комп'ютери PC-PT та принтер Printer-PT з групи *End Device*.



Рисунок 4.1 – Панель вибору типових пристроїв і зв'язків

3. Обрати *Connections* на панелі вибору пристроїв і зв'язків та вибрати прямий кабель (*Copper Straight-Through*), клацнувши по ньому (рис.4.3). Курсор прийме вид роз'єму з кінцем кабелю, що звисає.

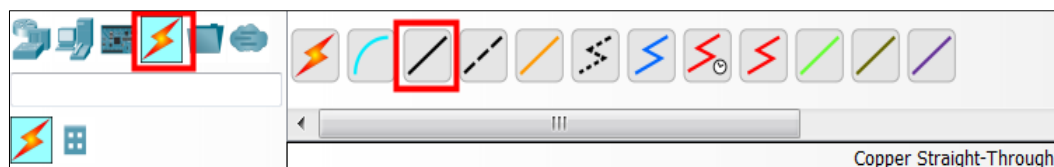


Рисунок 4.2 – Панель вибору з'єднань

4. Клацнути PC0. У вікні вибрати варіант для підключення FastEthernet0. Перетягнути інший кінець підключення до комутатора Switch0 і клацнути на ньому, щоб відкрити список підключень. Вибрати *FastEthernet0/1*, щоб завершити підключення.

Аналогічно зробити підключення другого PC та Printer-PT до комутатора, підключивши до порту *FastEthernet0/2* та *FastEthernet0/3* комутатора Switch0 відповідно.

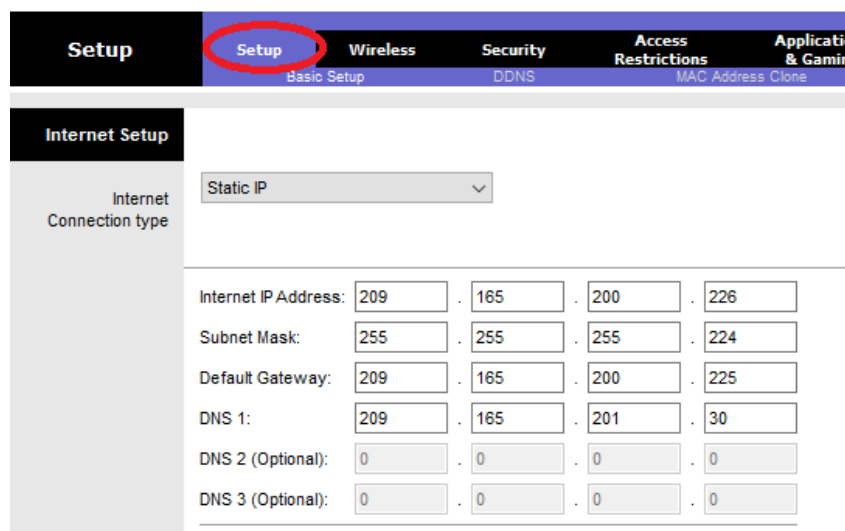
Примітка. Якщо необхідно помістити кілька пристроїв одного і того ж типу на робочий простір, натискання і перетягування може стати дуже виснажливим. Щоб уникнути цього, можна утримувати клавішу CTRL при натисканні на пристрій на панелі вибору пристроїв.

Крок 2. Налаштування Wireless Router та базових функцій безпеки бездротової мережі

Примітка. В методичних рекомендаціях далі всі приклади будуть наведені для 25-го варіанту.

1. Відкрити властивості пристрою Wireless Router, натиснувши на його зображення, та перейти на вкладку GUI.

2. Налаштувати параметри інтерфейсу, підключеного до Інтернету. Для параметра *Internet Connection Type* обрати значення *Static IP* в списку. Ввести дані згідно табл. 4.1 та рис. 4.4.



The screenshot shows the configuration interface of a Wireless Router. The top navigation bar includes 'Setup' (highlighted with a red circle), 'Wireless', 'Security', 'Access Restrictions', and 'Applications & Gaming'. Below this, the 'Internet Setup' section is active. The 'Internet Connection type' is set to 'Static IP'. The following parameters are configured:

Parameter	Value 1	Value 2	Value 3	Value 4
Internet IP Address:	209	165	200	226
Subnet Mask:	255	255	255	224
Default Gateway:	209	165	200	225
DNS 1:	209	165	201	30
DNS 2 (Optional):	0	0	0	0
DNS 3 (Optional):	0	0	0	0

Рисунок 4.3 – IP-налаштування інтерфейсу, підключеного до Інтернету

3. Налаштувати параметри внутрішньої мережі. Прокрутити сторінку вниз до розділу *Network Setup* і налаштувати наступні параметри:

- IP-адреса: №*10.№.0.1, де № – номер студента за списком в групі. Наприклад, для варіанту 25 (№=25) IP-адреса 250.25.0.1;
- маска підмережі: 255.255.255.0;
- початкова IP-адреса: для останнього октету ввести значення 11;
- максимальна кількість користувачів: 25.

Примітка. Зміни в діапазоні IP-адрес пулу DHCP будуть показані тільки після натискання кнопки *Save Settings*.

4. Налаштувати бездротову мережу для бездротових пристроїв. Відкрити параметри *Basic Wireless Settings* на вкладці *Wireless*. Встановити режим мережі *Auto*. Змінити SSID на MyHome (рис. 4.5).

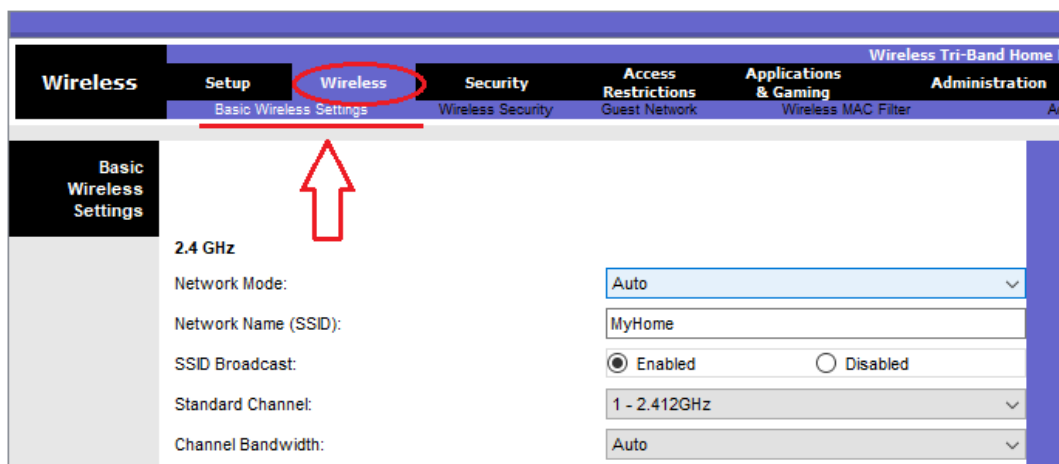


Рисунок 4.4 – Налаштування бездротової мережі для бездротових пристроїв

5. Налаштувати базові функції безпеки бездротової мережі в параметрах *Wireless Security* на вкладці *Wireless*. Змінити режим безпеки на *WPA2 Personal*. В полі *Passphrase* ввести 123Cisco (рис. 4.6).

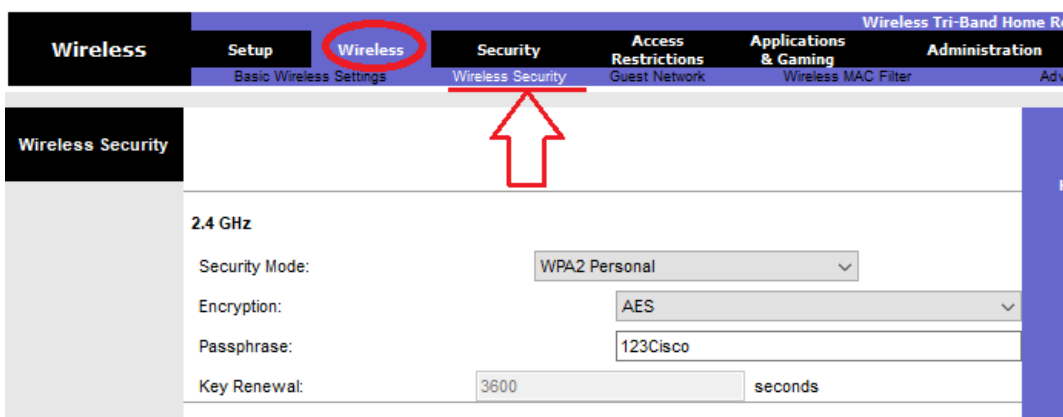


Рисунок 4.5 – Налаштування безпеки бездротової мережі

6. Внизу сторінки клацнути *Save Settings*. Щоб зберегти налаштування.

Крок 3. Налаштування Cloud0

1. Клацнути на Cloud0 та обрати на вкладці *Config* інтерфейс *Ethernet6*. Обрати тип *Cable* для *Provider Network*.

2. На вкладці *Config* в розділі *Connections* для *Cable* додати з'єднання *Coaxial7-Ethernet6*. (рис. 4.7).

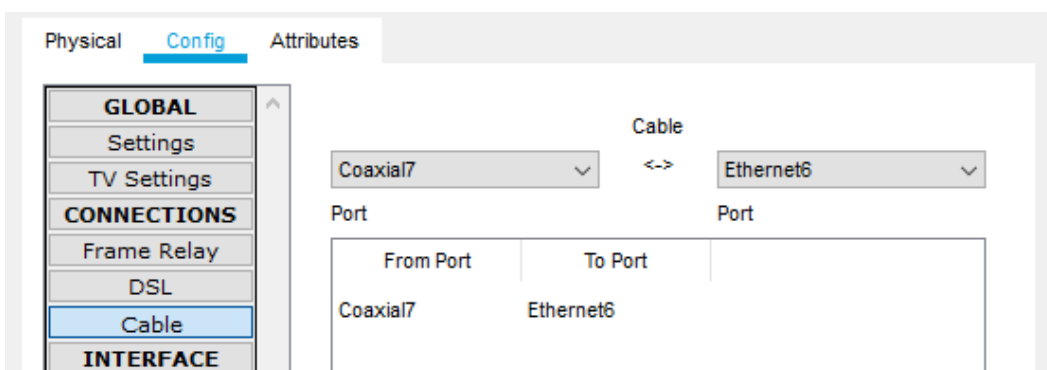


Рисунок 4.6 – Налаштування з'єднання для Cloud

Крок 4. Налаштування маршрутизатора R1

1. Клацнути R1 та обрати вкладку *Config*.
2. Налаштувати IP-адреси інтерфейсів відповідно до таблиці 4.1.
3. Включити інтерфейси, поставивши галочку *Port Status* (рис. 4.8).

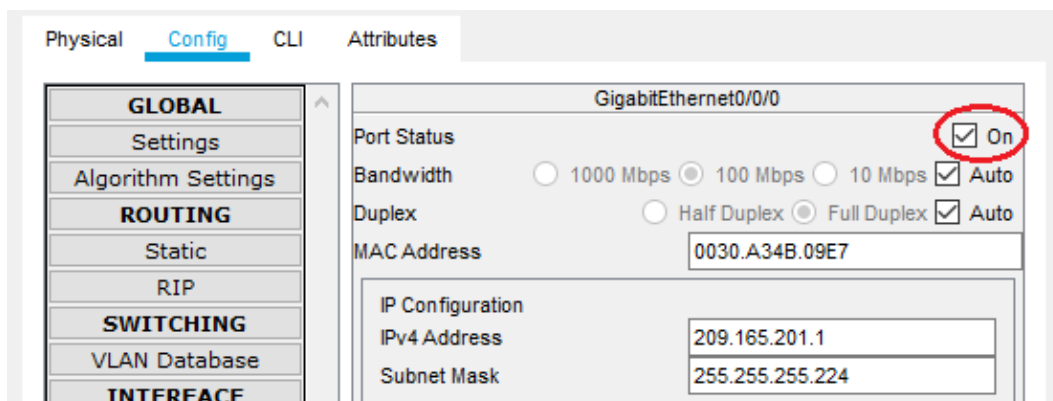


Рисунок 4.7 – Налаштування інтерфейсів на R1

Крок 5. Налаштування бездротових клієнтів для доступу до бездротової мережі

1. Для Laptop необхідно замінити дротову мережну карту на бездротову. Для цього на вкладці *Physical* знайти кнопку на пристрої та вимкнути його. Клацнути на мережній карті на ноутбуці та перемістити її в зону модулів зліва. Обрати модуль *WPC300N* та перемістити в звільнений слот на ноутбуці. Включити ноутбук.

2. Клацнути Laptop і вибрати *Desktop>PC Wireless*. Відкриється вікно графічного користувацького інтерфейсу Linksys для клієнта.

3. Відкрити вкладку *Connect* і натиснути кнопку *Refresh*, якщо необхідно. Повинна з'явитися бездротова мережа MyHome в полі *Wireless Network Name*.

4. Клацнути MyHome і вибрати команду *Connect*.

5. *Pre-shared Key* – пароль, налаштований на кроці 2, пункті 5. Ввести пароль і натиснути кнопку *Connect*.

6. Закрити інтерфейс користувача і клацнути *Command Prompt*. Виконати команду «*ipconfig*», щоб переконатися, що Laptop отримав IP-адресу.

7. Для налаштування смартфона та планшета обрати вкладку *Config* та на інтерфейсі *Wireless0* зробити налаштування відповідно до налаштувань бездротової мережі.

Крок 6. Налаштування PC0, PC1 та принтера

1. Клацнути PC0. У вікні управління відкрити вкладку *Desktop*.
2. Обрати додаток *IP Configuration* і ввести дані з таблиці 4.1 для PC0.
3. Повторити налаштування IP-адреси для PC1 та принтера.

Крок 7. Налаштування Server0

1. Налаштувати IP-адресу сервера відповідно до таблиці 4.1.
2. Відкрити вкладку *Services* і обрати розділ *HTTP*.
3. Обрати варіант *On*, щоб включити HTTP і HTTP Secure (HTTPS).

4. Необов'язковий крок: змінити HTML-код.
5. Відкрити вкладку *Services* і обрати розділ *DNS*.
6. Обрати варіант *On*, щоб включити сервіс *DNS*.
7. Додати запис у відповідних полях:
 - а) Name: labkm.com;
 - б) Address: 209.165.201.30 (IP-адреса Server0).
8. Натиснути кнопку *Add* щоб додати запис.

Крок 8. Перевірка підключення до мережі

Підключення до мережі можна перевірити за допомогою команди «ping». Дуже важливо, щоб з'єднання існувало у всій мережі. У разі збою необхідно вжити відповідні заходи щодо усунення неполадок.

1. Клацнути PC0. На вкладці *Desktop* обрати додаток *Command Prompt*.
2. Надіслати echo-запит на IP-адресу комп'ютера PC1, наприклад:
C:\> ping 250.25.0.4
3. Надіслати echo-запит на IP-адресу Wireless Router, наприклад:
C:\> ping 250.25.0.1
4. З командного рядка надіслати echo-запит на IP-адресу Server0.
C:\> ping 209.165.201.30

Крок 9. Перевірка працездатності веб-серверу

1. На будь-якому вузлі відкрити вкладку *Desktop* та додаток *Web Browser*.
2. В полі URL ввести IP-адресу Server0 і натиснути кнопку *Go*. Повинен відкритися веб-сайт Server0. У разі збою необхідно вжити заходи щодо усунення неполадок.

Крок 10. Перевірка сервісу DNS

1. На будь-якому вузлі відкрити вкладку *Desktop* та вибрати додаток *Command Prompt*.
2. Виконати команду «ping» на IP-адресу Server0, щоб перевірити з'єднання.
3. Виконати команду «nslookup labkm.com», щоб перевірити роботу DNS. Повинні отримати IP-адресу для імені labkm.com.
4. Закрити додаток *Command Prompt* та відкрити *Web Browser*.
5. В полі URL ввести labkm.com і натиснути кнопку *Go*. Відкриється веб-сайт Server0.

4.2 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- опис завдання з початковими умовами та даними;
- скріншот топології мережі та таблиця адресація вузлів згідно варіанту;

- опис значущих виконуваних кроків (з вказівкою їх суті);
- проект мережі з назвою за правилом Surname_Group_lab04.pkt (наприклад, Ivanov_KI-24-1_lab04.pkt) разом зі звітом надати на перевірку в системі Moodle або на корпоративну поштову скриньку викладача.

4.3 Питання для підготовки до захисту лабораторної роботи

1. Які типи мережного середовища ви знаєте?
2. Які є типи витої пари?
3. Як перевірити зв'язок між пристроями?
4. Які типи мережних з'єднань в Packet Tracer ви знаєте?
5. Яка різниця між комутатором та маршрутизатором, та коли їх слід застосовувати?

5 ЛАБОРАТОРНА РОБОТА №5. ВИВЧЕННЯ ПРОТОКОЛУ ARP

5.1 Мета лабораторної роботи

Вивчити роботу протоколу ARP, отримати практичні навички по роботі з командою ARP в командному рядку Windows.

5.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

- функції та робота протоколу ARP;
- синтаксис команди «arp»;
- структура заголовку протоколу ARP.

Виконання лабораторної роботи складається з двох частин. В першій частині необхідно дослідити роботу протоколу ARP в локальній мережі. В другій частині виконується вивчення роботи протоколу ARP в побудованій мережі в Packet Tracer з лабораторної роботи №4.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Вивчення роботи протоколу ARP в локальній мережі

Роботу слід проводити парами з використанням двох комп'ютерів, підключених до одного сегмента локальної мережі та IP-адресами, які належать одній IP-мережі. ПК повинні мати вихід в Інтернет. В разі неможливості наявності в мережі другого ПК, можна використовувати IP-адреси інших пристроїв, наприклад ТВ, ноутбука, принтера або шлюза (роутера).

Далі виконати такі дії:

– відкрити вікно командного рядка на ПК і відобразити довідкову інформацію по команді «arp»;

>arp /?

– відобразити ARP-таблицю;

>arp -a

– запустити програму Wireshark та почати захоплення пакетів;

– в командному рядку очистити ARP-таблицю;

– відобразити ARP-таблицю та переконатися в тому, що вона очищена або має менше записів;

– надіслати echo-запит за допомогою команди «ping» зі свого ПК на інший ПК в мережі (або інший пристрій, наприклад шлюз) для динамічного додавання запису в ARP-таблицю;

– після відправки echo-запиту зупинити захоплення пакетів в Wireshark;

– налаштувати в Wireshark фільтр на відображення тільки пакетів ARP та ICMP;

- на підставі отриманих даних визначити і задокументувати в звіт заголовки ARP-запиту і ARP-відповіді та звернути увагу на інкапсуляцію ARP-повідомлень;
- відобразити ARP-таблицю та визначити MAC-адрес сусіднього ПК (або шлюзу), перевірити ці значення на сусідньому ПК;
- зберегти в файл дамп захоплених пакетів в Wireshark для відправлення зі звітом викладачу;
- почати нове захоплення даних програмою Wireshark;
- надіслати echo-запит за допомогою команди «ping» на кілька IP-адрес в Інтернет;
- визначити, на який MAC-адрес призначення відправлялись echo-запити та якому пристрою він належить.

ЧАСТИНА 2. Вивчення роботи протоколу ARP в Packet Tracer

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи №4. Перед початком виконання перевірте працездатність мережі, виконавши «ping» з PC до Server0. Дуже важливо, щоб з'єднання існувало у всій мережі. У разі збою необхідно вжити відповідні заходи щодо усунення неполадок.

Примітка. Якщо команда «ping» видає повідомлення «Reply from x.y.z.w: Destination host unreachable», збережіть налаштування на Wireless Router, натиснувши кнопку *Save Settings* на вкладці GUI.

Далі виконати такі дії:

- визначити MAC-адреси інтерфейсів маршрутизаторів Wireless Router та R1 та заповнити отриманими відомостями табл. 5.1. Для цього на Wireless Router необхідно зайти в GUI на вкладці *Status* на відповідній мережі, а на R1 на вкладці CLI ввести команду «show interface *interface*», наприклад

```
> show interfaces g0/0/0
```

або інструментом лупа «» обрати опцію *Port Status Summary Table*;

- визначити MAC-адреси всіх PC та бездротових пристроїв та заповнити таблицю 5.1;

- перейти з режиму реального часу *Realtime* до режиму моделювання *Simulation* в правому нижньому кутку програми;

Таблиця 5.1 – IP та MAC-адреси пристроїв мережі

Пристрій	Інтерфейс	IP-адреса	MAC-адреса
Wireless Router	LAN		
	Internet	209.165.200.226	
R1	G0/0/1	209.165.200.225	
	G0/0/0	209.165.201.1	
Server0	fe0	209.165.201.30	
Laptop	Wireless0		
Pda	Wireless0		

Tablet PC	Wireless0		
PC0	fe0		
PC1	fe0		
Printer0	fe0		

Примітка. У нижньому правому куті інтерфейсу Packet Tracer розміщені кнопки перемикавання між режимами *Realtime* і *Simulation*. Packet Tracer завжди запускається у режимі *Realtime*, у якому мережні протоколи оперують у реальних часових проміжках. Проте, можливості Packet Tracer дозволяють користувачеві “зупинити час” за допомогою перемикавання до режиму моделювання *Simulation*. У цьому режимі пакети відображаються у вигляді конвертів, час керується подіями, а користувач може покроково проходити по мережних подіях.

– налаштувати *Event List Filters* лише на відображення повідомлень протоколів ARP та ICMP (рис. 5.1);

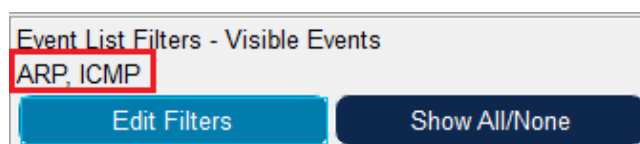


Рисунок 1.1 – Налаштування Event List Filters

– на PC0 на вкладці *Decstop* відкрити додаток *Command Promt* та відправити echo-запити на PC1. Дослідити роботу протоколу ARP, використовуючи інструменти режиму симуляції (рис.5.2);

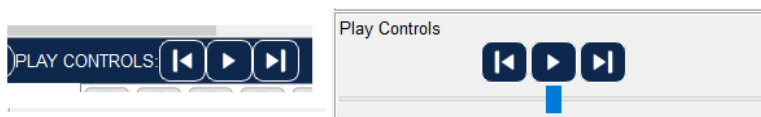


Рисунок 5.1 – Інструменти симуляції

– для заповнення відомостями ARP-таблиці з командного рядка PC0 відправити echo-запити на принтер та всі бездротові пристрої;

– відобразити ARP-таблицю на PC0 та проаналізувати її;

– з командного рядка PC0 відправити echo-запит на Server0 та визначити, на який MAC-адрес призначення відправлялись echo-запити та якому пристрою в мережі він належить;

– відобразити MAC-таблицю на комутаторі Switch0 та проаналізувати її;

>show mac address-table

або інструментом лупа «» ->MAC Table

– відобразити ARP-таблицю на маршрутизаторі R1 та проаналізувати її;

>show arp

або інструментом лупа «» ->ARP Table

Примітка. Інструменту для відображення ARP-таблиці на Wireless Router не розроблено.

5.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- лістинг командного рядка в ході виконання першої частини роботи;
- структура заголовків ARP-запиту та відповідна йому ARP-відповідь, захоплених в Wireshark;
- дамп захоплених пакетів в Wireshark надати разом зі звітом;
- таблиця 5.1 зі значеннями IP та MAC-адрес задіяних інтерфейсів всіх пристроїв в мережі, побудованої в Cisco Packet Tracer;
- вміст ARP-таблиці на PC0 після виконання другої частини роботи;
- вміст MAC-таблиці комутатора Switch0;
- вміст ARP-таблиці на маршрутизаторі R1.

5.4 Питання для підготовки до захисту лабораторної роботи

1. Як і коли видаляються статичні записи в ARP-таблиці?
2. Навіщо додавати статичні записи ARP-таблицю?
3. При виконанні команди «ping» на IP-адреси в Інтернет, який IP-адрес призначення був в ARP-запиті і чому?
4. При виконанні команди «ping» на IP-адреси в Інтернет, на який MAC-адрес призначення відправлялись echo-запити і чому?
5. Коли в мережі виникають ширококомовні ARP-запити?

6 ЛАБОРАТОРНА РОБОТА №6. ДОСЛІДЖЕННЯ МОДЕЛЕЙ TCP/IP І OSI

6.1 Мета лабораторної роботи

Сформувані засади для розуміння стеку протоколів TCP/IP і його взаємозв'язку з моделлю OSI.

6.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

- мережні протоколи та їх взаємодія;
- функції рівнів моделі OSI;
- порівняння моделей TCP/IP та OSI.

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи №4.

В лабораторній роботі буде досліджено процес запиту веб-сторінки з веб-сервера за допомогою браузера на клієнтському ПК. Не зважаючи на те, що більшість поданої інформації детально розглядатиметься пізніше, це завдання дає можливість вивчити функціональність Packet Tracer, стек TCP/IP та дослідити процес інкапсуляції.

Далі виконати такі кроки.

Крок 1. Перевірка працездатності мережі

Перед початком виконання перевірити працездатність мережі, виконавши «ping» з PC0 до Server0. Якщо команда «ping» видає повідомлення «Reply from x.y.z.w: Destination host unreachable», збережіть налаштування на Wireless Router, натиснувши кнопку *Save Settings* на вкладці GUI.

Крок 2. Перехід з режиму реального часу (Realtime) до режиму моделювання (Simulation mode)

1. Перейдіть з режиму реального часу *Realtime* до режиму моделювання *Simulation* в правому нижньому кутку програми.

2. Налаштувати *Event List Filters* лише на відображення повідомлень HTTP.

Крок 3. Створення HTTP-трафіку

На початку моделювання панель *Simulation Panel* порожня. Вгорі на панелі у списку подій вказані п'ять стовпців. У міру того, як трафік генерується і поступово просувається, у списку з'являтимуться події.

1. Натиснути на PC0, потім вкладку *Desktop* і відкрити веб-браузер, обравши додаток *Web Browser*.

2. У полі URL ввести labkm.com і натиснути *Go*.

3. Оскільки час у режимі моделювання залежить від подій, потрібно використовувати кнопку *Capture/Forward* для відображення подій у мережі. Натискати кнопку *Capture/Forward*, поки відповідь з сервера не надійде до PC0. Погляньте на сторінку веб-браузера на PC0. Чи відбулися якісь зміни?

Крок 4. Дослідження вмісту протокольного блоку даних HTTP

1. Натиснути на першому кольоровому квадратному полі у списку подій: *Event List* > колонка *Type*. Можливо знадобиться розгорнути *Simulation Panel* або використати смугу прокрутки безпосередньо під *Event List*.

Відобразиться вікно *PDU Information at Device: PC0*. Оскільки це початок передавання, у вікні є лише дві вкладки: *OSI Model* і *Outbound PDU Details*. При появі більшої кількості подій, з'явиться ще третя вкладка *Inbound PDU Details*.

2. Переконалися, що обрано вкладку *OSI Model*. Під колонкою *Out Layers* натиснути на *Layer 7*.

Яка інформація наведена за допомогою пронумерованих записів нижче полів *In Layers* та *Out Layers* для *Layer 7* в першому і останньому подіях?

Яке значення для *Dst Port* для *Layer 4* міститься у колонці *Out Layers*

Яке значення має *Dest IP* для *Layer 3* у колонці *Out Layers*?

Яка інформація показана на *Layer 2* у колонці *Out Layers*?

3. Натиснути на вкладці *Outbound PDU Details*. Інформація, наведена під *PDU Formats* відповідає рівням моделі TCP/IP.

Яка інформація традиційно міститься у розділі *IP PDU Details*, у порівнянні з інформацією з вкладки *OSI Model*? З яким рівнем вона пов'язана?

Яка інформація традиційно міститься у розділі *TCP PDU Details*, порівняно з інформацією на вкладці *OSI Model*, і з яким рівнем вона пов'язана?

Який *Host* вказаний у розділі *HTTP* деталей PDU?

З яким рівнем пов'язана ця інформація у вкладці *OSI Model*?

4. Натиснути на наступному кольоровому квадраті у *Event List*. Активний лише рівень 1 (незабарвлений). Пристрій переміщує кадри з буфера до мережі.

5. Перейти до 8-ої події HTTP у *Event List*, коли пакет досягає Server0 від R1, і натиснути на кольоровому квадраті. Це вікно містить як вхідні рівні *In Layers* так і вихідні рівні *Out Layers*. Звернути увагу на напрямок стрілки безпосередньо у колонці *In Layers*, вона вказує вгору, у напрямку передавання даних. Перейти по цих рівнях, зважаючи на попередньо розглянуті елементи. Зверху колонки стрілка вказує праворуч. Це означає, що зараз сервер надсилає інформацію назад до клієнта.

Які основні відмінності можна побачити при порівнянні даних, зображених у колонці *In Layers* з даними колонки *Out Layers*?

6. Перейти до вкладки *Inbound* та *Outbound PDU Details*. Переглянути деталі PDU.

7. Натиснути на останню подію HTTP у *Event List*. Скільки вкладок відображається для цієї події? Чому?

Крок 5. Перегляд додаткових подій

1. Закрити усі відкриті вікна з інформацією про PDU.

2. У розділі *Event List Filters > Visible Events*, натиснути на *Show All/None*, щоб відобразити події всіх протоколів.

Які додаткові типи подій *Event Types* відображаються?

Примітка: Ці додаткові записи відіграють різні ролі протоколів у TCP/IP. Протокол ARP надсилає запити про MAC-адреси для вузлів отримувачів. DNS відповідає за визначення IP-адреси для відповідних доменних імен. Додаткові події TCP відповідають за встановлення з'єднання, узгодження параметрів передачі даних і закриття з'єднання (сеансів зв'язку) між пристроями.

3. Натиснути на першій події DNS у вікні *Event List*. Розглянути вкладки *OSI Model* і *PDU Detail* та звернути увагу на процес інкапсуляції. Якщо поглянути на вкладку *OSI Model*, виділивши *Layer 7*, опис того, що відбувається, буде розміщений безпосередньо нижче *In Layers* і *Out Layers* ("1. The DNS client sends a DNS query to the DNS server."). Це дуже важливі дані, які допомагають зрозуміти процеси, які мають місце при передачі даних.

4. Натиснути на вкладці *Outbound PDU Details*. Яка інформація міститься у полі *NAME*: у розділі запиту *DNS QUERY*?

5. Натиснути на останньому кольоровому квадраті DNS у списку подій.

На якому пристрої було захоплено PDU?

Яке значення вказане поряд з *ADDRESS*: у частині *DNS Answer* на вкладці *Inbound PDU Details*?

6. Налаштувати *Event List Filters* на відображення подій HTTP та TCP.

7. Знайти другу подію TCP у переліку *Event List*, коли пакет надходить з R1 до Server0. Обрати *Layer 4* на вкладці *OSI Model*.

Яка інформація відображається у пункті 4 і 5 пронумерованого списку, що міститься безпосередньо під *In Layers* і *Out Layers*?

Окрім інших важливих функцій, TCP керує підключенням і відключенням каналу передавання даних. Саме ця подія відображає, що канал зв'язку налаштовано (ESTABLISHED).

8. Натиснути на останню подію TCP. Обрати *Layer 4* у вкладці *OSI Model*. Ознайомитися з записами, наведеними безпосередньо нижче *In Layers* і *Out Layers*. Яке призначення цієї події, виходячи з інформації в останньому записі списку?

6.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- відповіді на поставленні запитання в ході виконання роботи.

6.4 Питання для підготовки до захисту лабораторної роботи

1. Які переваги використання багаторівневої мережної моделі?
2. Для чого необхідні протоколи при передаванні даних?
3. Які схожості та відмінності між моделлю OSI та моделлю TCP/IP?
4. Які ключові протоколи пов'язані з кожним рівнем моделі TCP/IP?
5. Які організації розробляють стандарти для моделі OSI та TCP/IP?

7 ЛАБОРАТОРНА РОБОТА №7. РОЗРАХУНОК ПІДМЕРЕЖ

7.1 Мета лабораторної роботи

Навчитися розбивати мережу на підмережі за допомогою маски постійної та змінної довжини, визначати адреси підмереж, а також діапазон IP-адрес вузлів для підмереж.

7.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки до даної роботи, наступні питання:

- правила переходу з двійкової системи числення в десяткову та навпаки;
- сегментація мереж;
- використання масок в IP-адресації;
- використання масок змінної довжини (Variable Length Subnet Mask, VLSM) в IP-адресації.

Необхідно розробити схему IP-адресації поділу мережі організації на підмережі для відповідності вимогам топології, представленої на рисунку 9.1.

Кількість вузлів в мережах LAN1-LAN6 та виділений мережний блок для адресації цих вузлів завдана по таблицях 7.1–7.2 згідно з варіантом групи.

Через маршрутизатор Central забезпечується доступ до Internet.

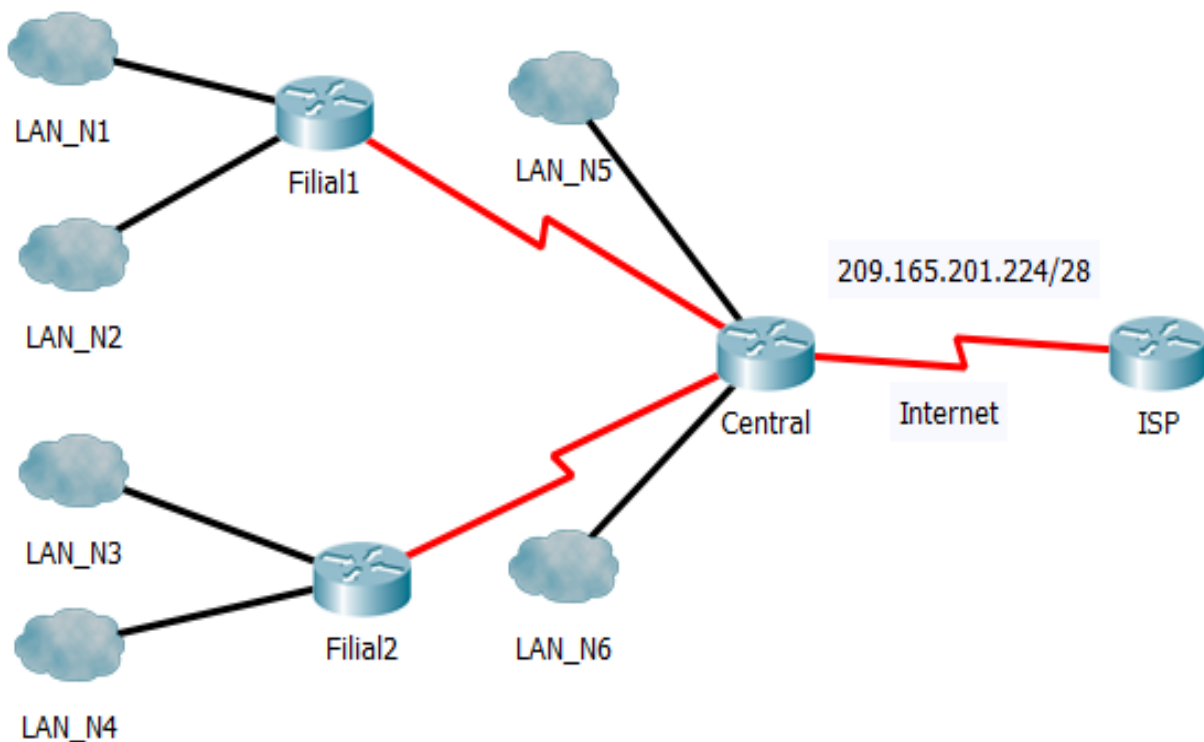


Рисунок 7.1 – Топологія мережі

Таблиця 7.1 – Варіанти завдань для 1-ої групи КІ-1

№ вар.	Адрес мережі	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
1.	10.100+№.0.0/19	250	200	1000	800	20	28
2.	10.100+№.0.0/17	100	120	50	60	400	380
3.	10.100+№.0.0/18	60	55	190	210	110	80
4.	10.100+№.0.0/19	250	180	98	110	60	45
5.	10.100+№.0.0/17	42	50	290	430	70	95
6.	10.100+№.0.0/18	110	90	20	15	450	381
7.	10.100+№.0.0/19	52	60	113	96	451	365
8.	10.100+№.0.0/17	85	78	168	190	560	680
9.	10.100+№.0.0/18	36	60	96	115	260	300
10.	10.100+№.0.0/19	68	92	200	240	20	15
11.	10.100+№.0.0/17	20	18	450	500	800	1000
12.	10.100+№.0.0/18	58	40	620	780	105	98
13.	10.100+№.0.0/19	20	15	103	78	502	362
14.	10.100+№.0.0/17	165	201	30	25	262	368

Продовження табл. 7.1

№ вар.	Адрес мережі	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
15.	10.100+№.0.0/18	86	90	154	160	52	40
16.	10.100+№.0.0/19	69	84	165	205	262	359
17.	10.100+№.0.0/18	57	33	232	155	53	50
18.	10.100+№.0.0/19	198	164	55	60	177	152
19.	10.100+№.0.0/20	149	213	179	168	40	35
20.	10.100+№.0.0/18	184	230	91	87	30	26
21.	10.100+№.0.0/18	11	9	200	150	45	38
22.	10.100+№.0.0/19	52	60	451	365	25	20
23.	10.100+№.0.0/17	850	780	168	190	70	68
24.	10.100+№.0.0/18	30	25	262	368	160	130
25.	10.100+№.0.0/19	68	92	200	240	20	15

Таблиця 7.2 – Варіанти завдань для 2-ої групи КІ-2

№ вар.	Адрес мережі	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
1.	10.200+№.0.0/19	250	200	1000	800	20	28
2.	10.200+№.0.0/17	100	120	50	60	400	380
3.	10.200+№.0.0/18	60	55	190	210	110	80
4.	10.200+№.0.0/19	250	180	98	110	60	45
5.	10.200+№.0.0/17	42	50	290	430	70	95
6.	10.200+№.0.0/18	110	90	20	15	450	381
7.	10.200+№.0.0/19	52	60	113	96	451	365
8.	10.200+№.0.0/17	85	78	168	190	560	680
9.	10.200+№.0.0/18	36	60	96	115	260	300
10.	10.200+№.0.0/19	68	92	200	240	20	15
11.	10.200+№.0.0/17	20	18	450	500	800	1000
12.	10.200+№.0.0/18	58	40	620	780	105	98

13.	10.200+№.0.0/19	20	15	103	78	502	362
14.	10.200+№.0.0/17	165	201	30	25	262	368
15.	10.200+№.0.0/18	86	90	154	160	52	40
16.	10.200+№.0.0/19	69	84	165	205	262	359
17.	10.200+№.0.0/18	57	33	232	155	53	50
18.	10.200+№.0.0/19	198	164	55	60	177	152
19.	10.200+№.0.0/20	149	213	179	168	40	35
20.	10.200+№.0.0/18	184	230	91	87	30	26
21.	10.200+№.0.0/19	100	80	150	130	20	28
22.	10.200+№.0.0/17	1000	1200	50	60	400	380
23.	10.200+№.0.0/18	600	550	190	210	11	8
24.	10.200+№.0.0/19	25	18	98	110	60	45
25.	10.200+№.0.0/17	420	500	190	130	70	95

Виконання лабораторної роботи складається з двох частин. В першій частині виконується сегментація мережі з використанням маски постійної довжини. В другій частині з використанням маски змінної довжини та порівнюються отримані результати.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Розробка схеми адресації сегментів мережі з використанням маски постійної довжини

Необхідно задати схему поділу мережі на підмережі в заданому сценарії враховуючи кількість комп'ютерів в кожній підмережі. При цьому IP-адреси будуть потрібні для кожного інтерфейсу локальної мережі кожного маршрутизатора.

Скласти схему поділу на підмережі, що відповідає зазначеним умовам, допоможуть наступні питання:

- 1) Скільки адрес вузлів необхідно для найбільшої підмережі?
- 2) Яка мінімальна кількість необхідних підмереж?
- 3) Які маски підмереж відповідають максимальній необхідній кількості адрес вузлів?
- 4) Які маски підмереж відповідають мінімальній необхідній кількості підмереж?
- 5) З огляду на відповіді, яка маска підмережі відповідає максимальній необхідній кількості адрес вузлів та мінімальній необхідній кількості підмереж?

З'ясувавши, яка маска підмережі відповідає всім зазначеним вимогам, заповнити наведену нижче таблицю 7.3.

Таблиця 7.3 – Визначення маски підмережі в організації

Вихідна адреса мережі	Вихідна маска мережі в десятковому вигляді	Розрахована маска підмережі в десятковому	Кількість зарезервованих біт для адреси підмережі	Кількість комбінацій підмереж для визначеної
-----------------------	--	---	---	--

		вигляді		маски

Розрахувати підмережі з новою маскою і занести інформацію в таблицю 7.4.

Таблиця 7.4 – Підмережі організації з маскою постійної довжини

Назва підмережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Маска підмережі у десятичному форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса

Дати відповіді на наступні питання:

- кількість необхідних IP-адрес (N);
- кількість IP-адрес, необхідних для кожного каналу WAN між маршрутизаторами;
- кількість IP-адрес, доступних у вихідній мережі ($N_{\text{поч}}$);
- кількість IP-адрес, доступних в розбитій мережі ($N_{\text{роз}}$);
- який відсоток адресного простору використовується в вихідній мережі ($(N/N_{\text{поч}} * 100)$);
- який відсоток адресного простору використовується в розрахованій мережі ($(N/N_{\text{роз}} * 100)$).

ЧАСТИНА 2. Розробка схеми адресації сегментів мережі з використанням маски змінної довжини

Далі розробити схему IP-адресації поділу мережі організації на підмережі за сценарієм, заданому в частині 1, використовуючи маски змінної довжини (метод VLSM).

Для цього спочатку визначити найбільшу підмережу та маску для неї. На звільнених бітах перша допустима комбінація привласнюється цій підмережі. У таблицю 7.5 ввести відповідні дані.

Потім визначити наступну за розмірами підмережу та маску для неї та їй присвоюється наступна комбінація на звільнених бітах.

Так треба продовжувати поділ підмереж відповідного розміру на підмережі до тих пір, поки не буде досягнута потрібна кількість вузлів у кожній підмережі.

Відповідні результати необхідно надати у вигляді таблиці 7.5.

Таблиця 7.5 – Підмережі організації методом VLSM

Назва підмережі	Необхідна кількість вузлів	Виділена кількість вузлів	Адреса підмережі	Маска підмережі у десятичному форматі	Префікс	Діапазон допустимих	Широкомовна адреса

				вому форматі		IP-адрес вузлів	

Призначити підмережу для кожного з каналів між маршрутизаторами. Починати треба з наступної доступної підмережі.

Заповнити таблицю 7.6 відповідними адресами.

Таблиця 7.6 – Підмережі каналів WAN між маршрутизаторами

Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
Канал WAN_N1 між маршрутизаторами Filial1 та Central				
Канал WAN_N2 між маршрутизаторами Filial2 та Central				

Дати відповіді на наступні питання, порівняти з відповідями з частини 1 та дати пояснення в разі отримання різних результатів:

- кількість IP-адрес, доступних у вихідній мережі;
- кількість IP-адрес, доступних в розбитій мережі;
- який відсоток адресного простору використовується в вихідній мережі;
- який відсоток адресного простору використовується в розрахованій мережі.

7.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- тему і мету лабораторної роботи;
- опис завдання з початковими умовами і даними;
- відповіді на зазначені питання;
- розрахунок адресації мережі згідно із завданням, поданий у вигляді таблиць 7.4 – 7.6;
- схеми вирішення адресації заданої мережі методом маски постійної довжини та методом VLSM у вигляді логічної топології згідно з рисунком 7.2 .

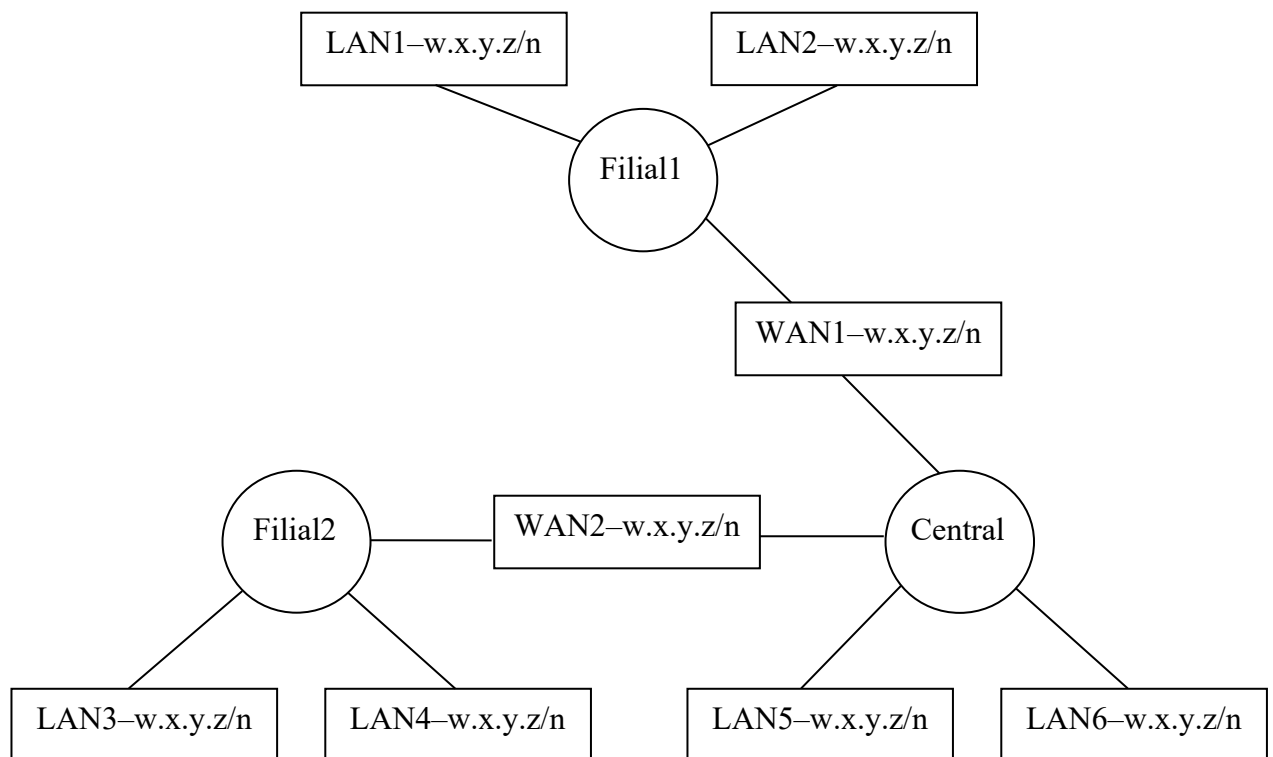


Рисунок 7.2 – Логічна топологія методом маски постійної довжини

7.4 Питання для підготовки до захисту лабораторної роботи

1. Який є запас на випадок появи додаткових мереж?
2. Який є запас на випадок збільшення числа вузлів?
3. Який основний мотив розбиття IP-мереж на підмережі?
4. Який недолік розрахунку мереж за допомогою маски постійної довжини?
5. Яка маска відповідає діапазону IP-адрес від 128.7.64.1 до 128.7.79.254?

8 ЛАБОРАТОРНА РОБОТА №8

ПОБУДОВА МЕРЕЖІ В CISCO PACKET TRACERT І БАЗОВЕ НАЛАШТУВАННЯ ТА ЗАХИСТ ПРОМІЖНИХ ПРИСТРОЇВ

8.1 Мета лабораторної роботи

Побудова мережної інфраструктури в Cisco Packet Tracer, виконання базового налаштування мережних пристроїв та реалізація заходів для забезпечення їхньої безпеки.

8.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні вказівки, такі питання:

- інтерфейс програми Cisco Packet Tracer;
- робота з командним рядком (CLI) операційної системи Cisco IOS;
- робота з контекстною довідкою в CLI;
- базова конфігурація пристроїв Cisco;
- безпечне управління віддаленими підключеннями по протоколу SSH;
- функція безпеки портів на комутаторах Cisco.

В програмі Packet Tracer побудувати розраховану в лабораторній роботі № 7 мережу, виконати налаштування базових параметрів пристроїв і захищене віддалене підключення по протоколу SSH.

Далі виконати такі дії.

Крок 1. Побудова мережі і налаштування ПК

1. Запустити програму Packet Tracer та побудувати модель мережі з лабораторної роботи №7 (рис. 7.1). Кожну мережу (LAN1 – LAN6) представити мінімум двома ПК, за винятком LAN3. Мережу LAN3 представити згідно рисунку 8.1. Для об'єднання ПК в одну мережу використовувати комутатори серії Cisco Catalyst 2960. Для об'єднання мереж використовувати маршрутизатори серії Cisco ISR4331.

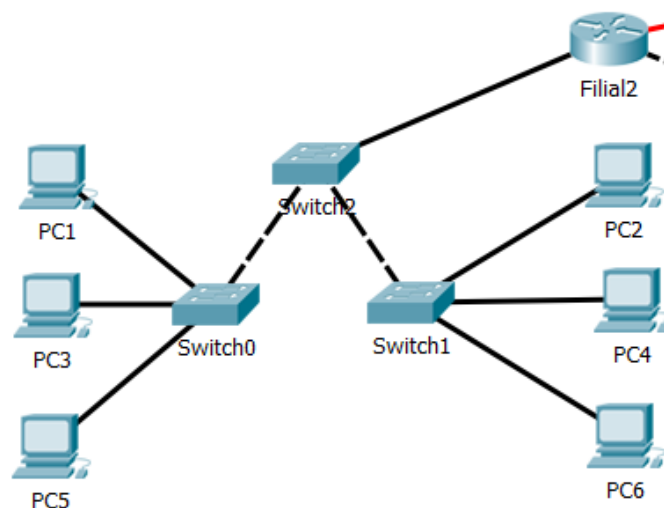


Рисунок 8.1 – Топологія мережі LAN3

2. З'єднати пристрої відповідними інтерфейсами. Так як маршрутизатор ISR4331 має всього 4 вбудованих LAN-порти, з яких G0/0/0 – комбінований (один порт RJ45 и другий порт SFP, які одночасно використовувати не можна), а в порт g0/0/2 не додано інтерфейсний модуль, то розширити інтерфейси для підключення. Для цього при відключеному живленні додати інтерфейси на вкладці *Physical* у вікні властивостей кінцевого пристрою, а саме:

- на Filial1 та Filial2 додати оптичний модуль GLC-TE (рис. 8.2) для під'єднання підмереж організації по Ethernet;

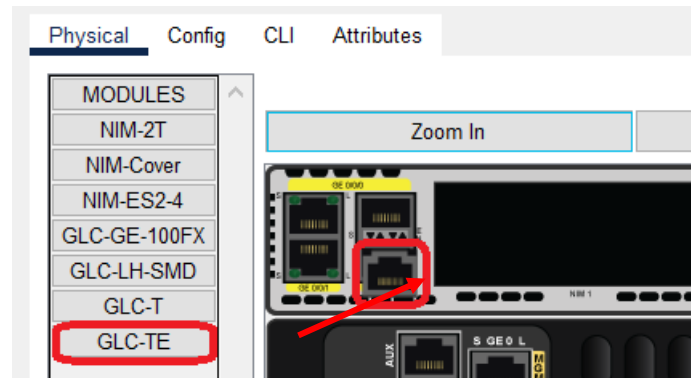


Рисунок 8.2 – Інтерфейсний модуль GLC-TE на Filial1 та Filial2

- на Central додати оптичний модуль GLC-GE-FX для з'єднання з провайдером по оптичному кабелю та 4-портові модулі мережного інтерфейсу комутатора Cisco Gigabit Ethernet LAN NIM-ES2-4 для під'єднання підмереж LAN5 та LAN6 (рис. 8.3);

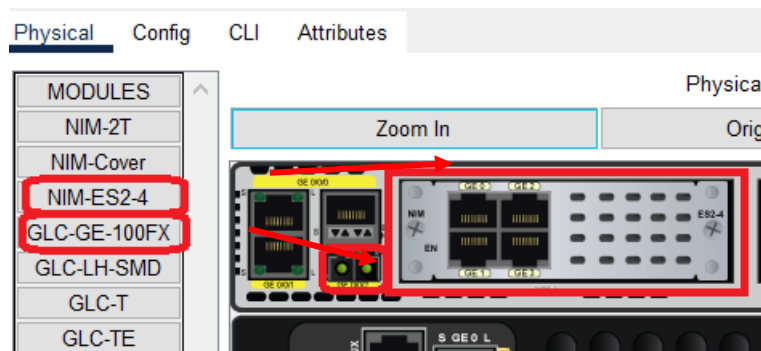


Рисунок 8.3 – Інтерфейсні модулі на Central

- на ISP тільки оптичний модуль GLC-GE-FX для з'єднання з Central та надання організації доступу до Інтернет.

На рис. 8.4 представлено приклад побудованої мережі в Packet Tracer та підключення пристроїв.

3. Для IP-адресації мережі використовувати розрахунки з лабораторній роботі №7 методом VLSM. Задokumentувати схему IP-адресації і підключень пристроїв у вигляді таблиці 8.1 з урахуванням таких вимог:

- перші допустимі IP-адреси призначаються інтерфейсам маршрутизаторів в локальних мережах;
- другі з допустимих IP-адрес призначаються комутаторам;
- останні з використовуваних IP-адрес призначаються ПК.

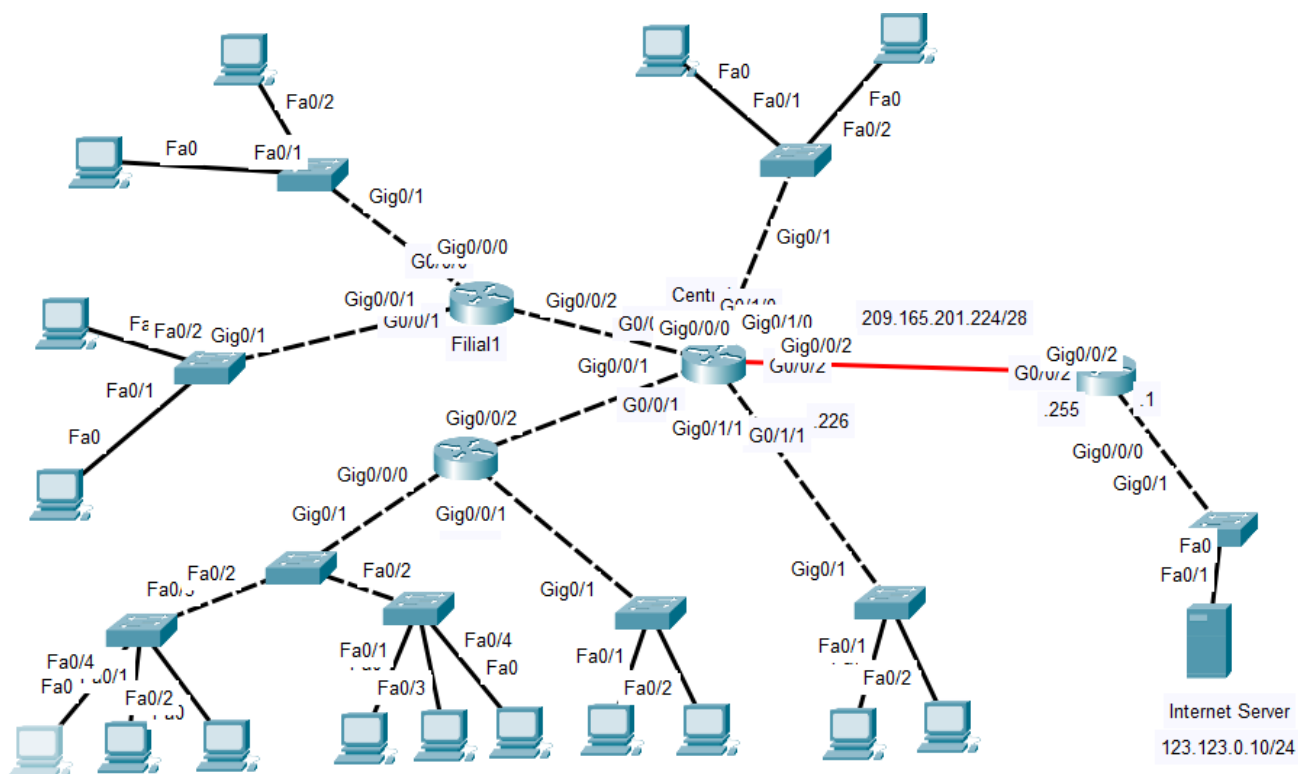


Рисунок 8.4 – Приклад побудованої мережі

Таблиця 8.1 – Адресація пристроїв і їх підключення

Пристрій	Інтерфейс	IP-адрес	Маска мережі	Префікс	Примітка
Filial1	Gig0/0/0				До LAN1
	Gig0/0/1				До LAN2
	Gig0/0/2				До Central G0/0/0
Switch_LAN1	VLAN1				
Switch_LAN2	VLAN1				
Filial2	Gig0/0/0				До LAN3
	Gig0/0/1				До LAN4
	Gig0/0/2				До Central G0/0/1
Switch0_LAN3	VLAN1				
Switch1_LAN3	VLAN1				
Switch2_LAN3	VLAN1				
Switch_LAN4	VLAN1				
Central	G0/0/0				До Filial1 G0/0/0
	G0/0/1				До Filial2 G0/0/1
	G0/1/0 (vlan 5)				До LAN5
	G0/1/1 (vlan 6)				До LAN6
	Serial0/2/0				До ISP s0/2/0
Switch_LAN5	VLAN1				
Switch_LAN6	VLAN1				
ISP	S0/2/0				До Central s0/2/0
	G0/0/1				До Internet Sever

4. Кожному ПК задати IP-адресу, маску і шлюз за замовчуванням. Заповнити таблицю 8.2 відповідними даними для кожної робочої станції.

Таблиця 8.2 – IP-адреси ПК

Назва мережі	IP-адрес ПК1	IP-адрес ПК2	Маска	Адреса шлюзу
LAN1				
LAN2				
LAN3				
LAN4				
LAN5				
LAN6				

5. На каналі підключення граничного маршрутизатора організації Central до Internet-провайдеру ISP назначити першу допустиму адресу мережі 209.165.20.224/28, а маршрутизатору організації наступну.

Крок 2. Налаштування базової конфігурації на маршрутизаторах

Базова конфігурація включає в себе налаштування унікального імені пристрою, заборони пошуку DNS, IP-адресацію інтерфейсів та паролів.

1. На маршрутизаторі Central обрати вкладку *CLI*.

2. Заборонити пошук DNS (DNS lookup), щоб не виконувалось перетворення доменних імен у випадку помилкового введення в командний рядок не інтерпретованих слів замість коректних команд.

```
Router>enable
```

```
Router#configure terminal
```

```
Router(config) # no ip domain-lookup
```

3. Задати унікальне ім'я за правилом *Surname-Central*, наприклад

```
Router(config)#hostname Ivanov-Central
```

4. Задати домену ім'я за правилом *Surname.Group.com*, наприклад:

```
Ivanov-Central(config)# ip domain-name Ivanov.KI-24-1.com
```

5. Для шифрування даних створити ключ RSA довжиною 1024 біт.

```
Ivanov-Central(config)# crypto key generate rsa
```

Після запиту введіть 1024.

6. Створити користувача-адміністратора *admin* з паролем *cisco123*.

```
Ivanov-Central(config)# username admin password cisco123
```

7. Задати пароль до привілейованого режиму *class*.

```
Ivanov-Central(config)#enable secret class
```

8. Задати пароль до консолі *cisco*.

```
Ivanov-Central(config)#line console 0
```

```
Ivanov-Central(config-line)#password cisco
```

```
Ivanov-Central(config-line)#login
```

```
Ivanov-Central(config-line)#exit
```

9. Налаштувати лінії VTU для перевірки реєстраційних даних в локальних базах даних імен користувачів, а також для дозволу віддаленого доступу лише по протоколу SSH.

```
Ivanov-Central(config)#line vty 0 4
Ivanov-Central(config-line)# login local
Ivanov-Central(config-line)# transport input ssh
```

10. Зашифрувати всі паролі, що зберігаються у відкритому вигляді.

```
Ivanov-Central(config)#service password-encryption
```

11. Налаштувати задіяні інтерфейси згідно заповненої таблиці 8.1. Так як на *Central* локальні мережі підключені до інтерфейсної плати NIM-ES2-4, яка має 4 комутованих (не маршрутизованих) порти, то по табл. 10.1 необхідно їх налаштувати з підтримкою маршрутизації через VLAN (Virtual Local Area Network). Приклад налаштувань інтерфейсів на маршрутизаторі Central:

```
Central#vlan database
% Warning: It is recommended to configure VLAN from config
mode,
as VLAN database mode is being deprecated. Please consult
user
documentation for configuring VTP/VLAN in config mode.
Ivanov-Central(vlan)#vlan 5 name LAN5
VLAN 5 added:
Name: LAN5
Ivanov-Central(vlan)#vlan 6 name LAN6
VLAN 6 added:
Name: LAN6
Ivanov-Central(vlan)#exit
APPLY completed.
Exiting....
Central#configure terminal
Ivanov-Central(config)#interface g0/1/0
Ivanov-Central(config-if)# description Connection to LAN5
Ivanov-Central(config-if)#switchport mode access
Ivanov-Central(config-if)#switchport access vlan 5
Ivanov-Central(config-if)#interface g0/1/1
Ivanov-Central(config-if)# description Connection to LAN6
Ivanov-Central(config-if)#switchport mode access
Ivanov-Central(config-if)#switchport access vlan 6
Ivanov-Central(config-if)#exit
Ivanov-Central(config)#interface vlan 5
Ivanov-Central(config-if)#ip address 192.168.5.1 255.255.255.0
Ivanov-Central(config-if)#interface vlan 6
Ivanov-Central(config-if)#ip address 192.168.6.1 255.255.255.0
Ivanov-Central(config)#interface GigabitEthernet0/0/0
Ivanov-Central(config-if)# description Connection to Filial1
Ivanov-Central(config-if)#ip address 192.168.10.1 255.255.255.0
Ivanov-Central(config-if)#no shutdown
Ivanov-Central(config-if)#exit
```

```

Ivanov-Central(config)#interface GigabitEthernet0/0/1
Ivanov-Central(config-if)# description Connection to Filial2
Ivanov-Central(config-if)#ip address 192.168.11.1 255.255.255.0
Ivanov-Central(config-if)#no shutdown
Ivanov-Central(config-if)#exit
Ivanov-Central(config)#interface GigabitEthernet0/0/2
Ivanov-Central(config-if)# description Connection to ISP
Ivanov-Central(config-if)#ip          address          209.165.201.226
255.255.255.240
Ivanov-Central(config-if)#no shutdown
Ivanov-Central(config-if)#exit

```

12. Зберегти конфігурацію.

```
Ivanov-Central#copy running-config startup-config
```

13. На інших маршрутизаторах виконати базові налаштування, змінивши наведений скрипт відповідними даними та налаштуванням адресації відповідних задіяних інтерфейсів. Скопіювати та вставити в командному рядку в режимі користувача.

```

enable
configure terminal
no ip domain-lookup
hostname Ivanov-Filial1
ip domain-name Ivanov.KI-24-1.com
crypto key generate rsa
1024
username admin secret cisco123
enable secret class
line console 0
password cisco
login
line vty 0 4
login local
transport input ssh
service password-encryption
interface GigabitEthernet0/0/0
description Connection to LAN1
ip address 192.168.1.1 255.255.255.0
no shut
interface GigabitEthernet0/0/1
description Connection to LAN2
ip address 192.168.2.1 255.255.255.0
no shut
interface GigabitEthernet0/0/2
description Connection to Central
ip address 192.168.11.1 255.255.255.0
no shut
do copy run start

```

Крок 3. Налаштування базової конфігурації на комутаторах

1. По табл.8.1 виконати базові налаштування на комутаторах в мережах LAN1–LAN4, задавши назву пристрою, паролі до ліній, доступ по SSH, пароль до привілейованого режиму, IP-адресу та шлюз. Змінити наведений скрипт відповідними даними, скопіювати та вставити в командному рядку комутатора в режимі користувача.

```
enable
configure terminal
no ip domain-lookup
hostname SW_LAN1
enable secret class
service password-encryption
line console 0
password cisco
login
username admin secret cisco123
ip domain-name Ivanov.KI-24-1.com
crypto key generate rsa
1024
line vty 0 4
login local
transport input ssh
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
ip default-gateway 192.168.1.1
do copy run start
```

2. На комутаторах в мережах LAN5–LAN6 так як вони під'єднані до комутуваних портів на Central, то необхідно виконати на них додаткові налаштування з відповідними VLAN.

```
vlan 5
vlan 6
int range f0/1-24, g0/1-2
switchport mode access
switchport access vlan 5
interface vlan 5
ip address 192.168.5.2 255.255.255.0
no shutdown
ip default-gateway 192.168.5.1
do copy run start
```

Крок 4. Перевірка і тестування конфігурації

1. Перевірити налаштування конфігурації маршрутизаторів за допомогою команди «show ip interface brief».

2. Для перевірки правильного налаштування ПК і доступності локальних інтерфейсів маршрутизаторів виконати команду «ping» з командного рядка

кожного ПК на його шлюз. Echo-запити повинні бути успішними. При невдалому виконанні echo-запитів виконати пошук і усунення несправностей.

3. Перевірити досяжність мереж, відправивши echo-запити по табл. 8.3, та дайте пояснення.

Примітка. На даному етапі, поки не налаштована маршрутизація, ПК не можуть відправляти echo-запити на ПК в віддалених мережах..

Таблиця 8.3 – Результат перевірки досяжності мереж командою «ping»

ping		Так/ні	Пояснення
Від	До		
LAN1	LAN2		
LAN3	LAN4		
LAN5	LAN6		
LAN1	LAN3		
LAN1	LAN5		
LAN3	LAN5		
LAN1	Internet Server		

Крок 5. Перевірка реалізації протоколу SSH.

1. За допомогою командного рядка з будь-якого вузла підключитися до локального комутатора чи маршрутизатора через Telnet. Спроба повинна завершитися невдачею.

```
> telnet кінцевий_вузол
```

2. Ввести «ssh» і натиснути *Enter*, не додаючи будь-яких параметрів, щоб відобразити інструкції використання команди. Параметр *-l* – це буква «L», а не цифра 1.

3. Увійти до системи через протокол SSH.

```
> ssh -l admin кінцевий_вузол
```

4. Після успішного входу перейти в режим привілейованого доступу і зберігти конфігурацію.

8.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- скрін побудованої мережі в Packet Tracer;
- таблиці призначень IP-адрес (табл. 8.1 і 8.2);
- застосовані команди з налаштувань та їх опис;
- результати перевірки досяжності мереж у вигляді табл. 8.3;
- проект мережі з назвою за правилом *Family.Group_lab8_KM.pkt*.

8.4 Питання для підготовки до захисту лабораторної роботи

1. Що позначає символ # після імені маршрутизатора?
2. При роботі в командному рядку Cisco IOS, які є основні режими введення команд?

3. Що повинні показувати вихідні дані для активних інтерфейсів з правильними налаштуваннями?

4. Що повинні показувати вихідні дані для інтерфейсів, що не налаштовані?

5. Чому не виконується ring до вузлів в віддалених мережах?

9 ЛАБОРАТОРНА РОБОТА №9

ВПРОВАДЖЕННЯ І НАЛАШТУВАННЯ СЕРВІСІВ WEB-СЕРВЕРУ, СЕРВЕРУ ЕЛЕКТРОННОЇ ПОШТИ, DHCP, DNS ТА FTP

9.1 Мета лабораторної роботи

Вивчити призначення та особливості сервісів веб-серверу, серверу електронної пошти, DHCP, DNS та FTP, їх налаштування та перевірку в програмі Packet Tracer.

9.2 Організація виконання лабораторної роботи

Для виконання лабораторної роботи необхідно вивчити, використовуючи рекомендовану літературу, конспект лекцій і методичні рекомендації, такі питання:

- використання портів сервісами веб-серверу, серверу електронної пошти, DHCP, DNS та FTP;
- функції протоколів HTTP, SMTP, POP3, DHCP, DNS та FTP.

Вихідними даними є побудована мережа в Packet Tracer з лабораторної роботи №8.

Виконання лабораторної роботи складається з п'ятих частин. В першій частині необхідно налаштувати веб-сервіс. В другій частині налаштувати сервер електронної пошти. В третій частині виконується налаштування записів на DNS-сервері. В четвертій частині налаштування серверу DHCP та перевірка сервісів DHCP та DNS. В п'ятій частині налаштування FTP-сервісу.

Послідовність виконання окремих частин лабораторної роботи наведена нижче.

ЧАСТИНА 1. Налаштування та перевірка веб-серверу

Крок 1. Налаштування веб-серверу

1. Додати в мережу LAN1 сервер *Server-PT* з групи *End Device*, дати йому назву *MultiServer* та привласнити п'яту IP-адресу з діапазону допустимих IP-адрес цієї підмережі.

2. На *MultiServer* відкрити вкладку *Services* і вибрати розділ *HTTP*.

3. Вибрати варіант *On*, щоб включити HTTP і HTTP Secure (HTTPS).

4. Змінити HTML-код, щоб на головній сторінці сайту відображались відомості про автора роботи.

Крок 2. Перевірка працездатності веб-серверу

1. На будь-якому вузлі в мережі LAN1 відкрити вкладку *Desktop* та вибрати додаток *Web Browser*.

2. В полі URL ввести IP-адресу *MultiServer* і натиснути кнопку *Go*. Відкриється веб-сайт *MultiServer*.

3. Перевірити працездатність веб-серверу з вузлів в підмережах LAN1 або LAN2 через його IP-адресу.

ЧАСТИНА 2. Налаштування та перевірка серверу електронної пошти

Крок 1. Налаштування MultiServer для відправки (SMTP) і отримання (POP3) повідомлень електронної пошти

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *EMAIL*.
2. Вибрати варіант *On*, щоб включити SMTP і POP3.
3. Призначте ім'я домену *surname.pt* і натиснути кнопку *Set*, де *surname* – прізвище розробника проекту, наприклад *ivanov.pt*.
4. Створити користувачів з ім'ям *user1* та *user2* і паролем *cisco*. Натиснути + для додавання користувачів.

Крок 2. Налаштування та перевірка ПК для використання сервісу електронної пошти

1. На будь-якому вузлі в мережі LAN1 відкрити вкладку *Desktop* та вибрати додаток *Email*.
2. Ввести відповідні значення у відповідних полях:
 - а) Your Name: *User1*;
 - б) Email Address: *user1@surname.pt*, наприклад *user1@ivanov.pt*;
 - в) Incoming Mail Server: IP-адреса MultiServer;
 - г) Outgoing Mail Server: IP-адреса MultiServer;
 - д) User Name: *user1*;
 - е) Password: *cisco*;
3. Натиснути кнопку *Save*. З'явиться вікно поштового оглядача.
4. Натиснути кнопку *Receive*. Якщо всі налаштування клієнта і сервера виконані правильно, у вікні поштового оглядача з'явиться повідомлення про підтвердження «Receive Mail Success».
5. Вибрати інший ПК в цій мережі, відкрити вкладку *Desktop* та вибрати додаток *Email*.
6. Виконати відповідні налаштування email для *user2*.

Крок 3. Відправка електронної пошти від user1 до user2

1. У вікні *Mail Browser* на *user1* натиснути кнопку *Compose*.
2. Ввести наступні значення у відповідних полях:
 - а) To: *user2@surname.pt*;
 - б) Subject: вкажіть тему повідомлення;
 - в) Email Body: введіть текст листа.
3. Натиснути *Send*.
4. Натиснути кнопку *Receive* на *user2* і переконатися, що він отримав повідомлення електронної пошти. Двічі клацнути повідомлення електронної пошти.
5. Натиснути кнопку *Reply*, ввести відповідь і натиснути кнопку *Send*.
6. Переконатися, що *user1* отримав відповідь.

ЧАСТИНА 3. Налаштування записів на DNS-сервері

Крок 1. Налаштування записів на DNS-сервері

1. Додати в мережу LAN2 сервер *Server-PT* з групи *End Devise*, дати йому назву *ServerDNS* та привласнити п'яту IP-адресу з діапазону допустимих IP-адрес цієї підмережі.
2. На *ServerDNS* відкрити вкладку *Services* і вибрати розділ *DNS*.
3. Вибрати варіант *On*, щоб включити сервіс *DNS*.
4. Додати запис для *MultiServer* у відповідних полях:
 - а) Name: *labkm.com*;
 - б) Address: IP-адреса *MultiServer*.
5. Натиснути кнопку *Add* щоб додати запис.

ЧАСТИНА 4. Налаштування серверу DHCP та перевірка сервісів DHCP та DNS

Крок 1. Налаштування серверу DHCP

1. На *MultiServer* відкрити вкладку *Services* і вибрати розділ *DHCP*.
2. Вибрати варіант *On*, щоб включити сервіс *DHCP*.
3. Ввести відповідні значення у відповідних полях:
 - а) Default Gateway: IP-адреса шлюза;
 - б) DNS Server: IP-адреса *ServerDNS*;
 - в) Start IP Address: виключити перші 10 адрес;
 - г) Subnet Mask: маска мережі *LAN1*;
4. Натиснути кнопку *Add* щоб додати запис.

Крок 2. Перевірка сервісу DHCP для вузлів в LAN1

1. На кожному вузлі *LAN1* відкрити вкладку *Desktop* і вибрати розділ *IP Configuration*.
2. Вибрати варіант *DHCP* і дочекатися виконання запиту *DHCP*.

Крок 3. Перевірка сервісу DNS

1. На *MultiServer* відкрити вкладку *Desktop* і в розділі *IP Configuration* в полі *DNS Server* вказати IP-адресу *ServerDNS*.
2. На будь-якому вузлі в мережі *LAN1* відкрити вкладку *Desktop* та вибрати додаток *Command Prompt*.
3. Виконати «ping» на IP-адресу *ServerDNS*, щоб протестувати з'єднання.
4. Виконати команду «nslookup labkm.com», щоб перевірити роботу *ServerDNS*. Повинні отримати IP-адрес для імені *labkm.com*.
5. Закрити додаток *Command Prompt* та відкрити *Web Browser*.
6. В полі *URL* ввести *labkm.com* і натиснути кнопку *Go*. Відкриється веб-сайт *MultiServer*.
7. Перевірити працездатність веб-серверу з вузлів в інших підмережах, додавши в налаштуваннях IP-адресу *ServerDNS*.

ЧАСТИНА 5. Налаштування FTP-сервісу на MultiServer

Крок 1. Налаштування FTP-сервісу на MultiServer

1. На MultiServer відкрити вкладку *Services* і вибрати розділ *FTP*.
2. Вибрати варіант *On*, щоб включити сервіс FTP.
3. У розділі *User Setup* створити облікові записи користувачів (табл.9.1).

Натиснути *Add* для додавання облікового запису.

Таблиця 9.1 – Облікові записи на сервері FTP

Ім'я користувача	Пароль	Дозволи
anonymous	anonymous	Read List
administrator	cisco	full permission

Крок 2. Відправка конфігураційного файлу на FTP-сервер

1. На будь-якому вузлі в мережі FTP-сервера відкрити вкладку *Desktop* і вибрати додаток *Text Editor*.

2. Набрати текст в текстовому редакторі та при його закритті зберегти під назвою README.txt.

3. На вкладці *Desktop* відкрити вікно командного рядка і виконати наступні дії.

- а) Ввести «*ftp IP-адреса MultiServer*». Зачекати кілька секунд, поки клієнт підключиться.
- б) Сервер виведе запит для введення імені користувача і пароля. Використати облікові дані для облікового запису administrator.
- в) Рядок зміниться на *ftp>*. Ввести команду «*dir*» для перегляду вмісту каталогу. З'явиться каталог файлів на MultiServer.
- г) Для перенесення файлу README.txt в рядку *ftp>* ввести «*put README.txt*». Файл README.txt буде переданий з вузла на MultiServer.
- д) Ввести команду «*dir*», щоб упевнитися, що файл був переданий. Файл README.txt тепер є в списку файлів каталогу.
- е) Закрити FTP-клієнт, ввівши команду «*quit*». Командний рядок набуде вигляду *PC>*.

9.3 Зміст звіту

Підготувати звіт з виконання лабораторної роботи, який повинен включати:

- номер, тему і мету лабораторної роботи;
- опис застосованих сервісів та їх параметри налаштувань;
- проект мережі в Packet Tracer з назвою за правилом *Surname_Group_lab8.pkt*.

9.4 Питання для підготовки до захисту лабораторної роботи

1. Який протокол перетворює ім'я labkm.com в IP-адресу?

2. Який протокол транспортного рівня використовується для передачі DNS?
3. Які переваги використання DHCP?
4. У чому полягає основне призначення DNS?
5. У чому недолік доступу до FTP з командного рядка?

ДОДАТОК А

МЕРЕЖНІ ТА ДІАГНОСТИЧНІ КОМАНДИ WINDOWS

Команда	Опис
arp	Вивід і редагування таблиці трансляції IP-адрес в фізичні з використанням протоколу дозволу адрес (ARP).
getmac	Вивід MAC-адрес мережних адаптерів комп'ютера. Команда «getmac» може використовуватися для отримання інформації про MAC-адреси віддаленого комп'ютера в мережі, проте необхідно щоб користувач мав право доступу.
ftp	Обмін файлами з комп'ютером, на якому запущена служба сервера FTP.
hostname	Вивід мережної назви комп'ютера. Ця команда доступна тільки після установки підтримки протоколу TCP/IP.
ipconfig	Вивід всіх поточних налаштувань TCP/IP на комп'ютері і поновлення параметрів DHCP і DNS. При виклику команди «ipconfig» без параметрів виводяться IP-адреса, маска підмережі і основний шлюз для кожного мережного адаптера.
nbtstat	Засіб діагностики розпізнавання імен NetBIOS. Вивід статистики протоколу і поточних підключень TCP/IP за допомогою NBT (NetBIOS через TCP/IP).
netstat	Вивід стану TCP-з'єднань та портів, що прослуховуються комп'ютером. Крім цього виводить статистику Ethernet, таблиці маршрутизації, статистику IPv4 (для протоколів IP, ICMP, TCP і UDP) і IPv6 (для протоколів IPv6, ICMPv6, TCP через IPv6 і UDP через IPv6).
nslookup	Діагностична команда для виведення відомостей в базі даних DNS-сервера, які відносяться до вузла або домену.
netsh	Найбільш повна і функціональна команда для керування конфігурацією різних мережних служб на локальному або віддалених комп'ютерах з використанням командного рядка. Можливості «netsh» настільки великі, що важко знайти мережне завдання, яке неможливо було б вирішити за допомогою цієї команди.
ping	Перевірка з'єднань в мережах на основі TCP/IP та служби перетворення імен DNS.
Tracer	Діагностична команда, призначена для визначення маршруту IP-пакетів до точки призначення за допомогою echo-повідомлень протоколу ICMP (Internet Control Message Protocol) та повідомляє час, необхідний для досягнення кожного вузла по шляху до заданого вузла.
pathping	Засіб визначення маршруту, що поєднує функції команд «ping» і «Tracer». Ця команда показує ступінь втрати пакетів на будь-якому маршрутизаторі або каналі та дозволяє визначити, які маршрутизатори або канали викликають неполадки в роботі мережі.
route	Вивід та зміна таблиці маршрутизації на комп'ютері.
net	Управління налаштуваннями мережі в командному рядку Windows. Синтаксис наведено в Додатку В.

ДОДАТОК Б

РОЗРАХУНОК ПРОПУСКНОЇ ЗДАТНОСТІ МЕРЕЖІ FAST ETHERNET

Виконаємо розрахунки пропускної здатності мережі Fast Ethernet для кадру з мінімально ($N_{dmin} = 46$ байт) та максимальною довжиною ($N_{dmax} = 1500$ байт) поля даних в кадрі.

Розмір кадру в байтах визначають за формулою:

$$N_k = N_s + N_d$$

де N_s – службова інформація кадру Fast Ethernet разом з преамбулою, байт;
 $N_s = 26$ байт;

N_d – розмір поля даних кадру.

Розмір мінімального і максимального кадру в байтах:

$$N_{kmin} = 26 + 46 = 72 \text{ (байт)}$$

$$N_{kmax} = 1500 + 26 = 1526 \text{ (байт)}$$

Так як один байт дорівнює восьми бітам, мінімальний і максимальний розмір кадру в бітах:

$$N_{kmin} = 72 * 8 = 576 \text{ (біт)}$$

$$N_{kmax} = 1526 * 8 = 12208 \text{ (біт)}$$

Пропускна здатність Fast Ethernet визначають за формулою:

$$N_{ps} = N_1 * N_2 * K \text{ (біт)}$$

де N_1 - кількість біт в одному кілобіті; $N_1 = 1024$;

N_2 - кількість кілобіт в одному мегабіті; $N_2 = 1024$;

K - коефіцієнт швидкості передачі даних; $K = 100$.

$$N_{ps} = 1024 * 1024 * 100 = 104\,857\,600 \text{ (біт)}$$

Якщо врахувати міжкадровий інтервал, то отримаємо довжину проходження кадрів:

$$L_k = N_{mi} + N_k$$

де N_{mi} – міжкадровий інтервал; $N_{mi} = 96$ біт;

N_k – розмір кадру разом з службовою інформацією.

Тоді період проходження кадрів мінімальної і максимальної довжини:

$$L_{kmin} = 576 + 96 = 672 \text{ (біт)}$$

$$L_{kmax} = 12208 + 96 = 12604 \text{ (біт)}$$

Тоді час проходження кадрів можна визначити за формулою:

$$T = \frac{L_k}{N_{ps}} * K_{mks}$$

де L_k – довжину проходження кадрів, біт;

N_{ps} – пропускна здатність Fast Ethernet, біт;

K_{mks} – кількість мікросекунд в одній секунді; $K_{mks} = 10^6$;

Час проходження мінімального і максимального кадрів:

$$T_{min} = \frac{672}{104857600} * 10^6 = 6,4 \text{ (мкс)}$$

$$T_{max} = \frac{12604}{104857600} * 10^6 = 117,6 \text{ (мкс)}$$

Частоту слідування кадрів, тобто кількість кадрів, що проходять по мережі за 1 секунду можна визначити за формулою:

$$F = \frac{N_{ps}}{L_k}, (\text{кадр/с})$$

Отримуємо частоту слідування кадрів при мінімальному і максимальному розмірі кадру:

$$F_{min} = \frac{104857600}{672} = 156038 (\text{кадр/с})$$

$$F_{max} = \frac{104857600}{12604} = 8522 (\text{кадр/с})$$

Знаючи частоту проходження кадрів F і розмір поля даних кадру N_d в байтах можна розрахувати корисну пропускну здатність мережі:

$$P = F * N_d * 8, (\text{біт/с})$$

$$P_{min} = F_{min} * L_{kmin} * 8 = 156038 * 46 * 8 = 57421984, (\text{біт/с})$$

$$P_{max} = F_{max} * L_{kmax} * 8 = 8522 * 1500 * 8 = 102264000, (\text{біт/с})$$

Або в Мбіт/с:

$$P = \frac{P}{N_1 * N_2} (\text{Мбіт/с})$$

де N_1 - кількість біт в одному кілобіті; $N_1 = 1024$;

N_2 - кількість кілобіт в одному мегабіті; $N_2 = 1024$;

$$P_{min} = \frac{57421984}{1024 * 1024} = 54.76 (\text{Мбіт/с})$$

$$P_{max} = \frac{102264000}{1024 * 1024} = 97.52 (\text{Мбіт/с})$$

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Cisco Networking Academy: Learn Cybersecurity, Python & More. *Networking Academy*. URL: <https://www.netacad.com> (date of access: 15.01.2024).
2. Комп'ютерні мережі : підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. – Вінниця : ВНТУ, 2020. – 378 с.
3. Каштан В.Ю. Комп'ютерні мережі (частина 1): навч. наоч. посіб. / В.Ю. Каштан, М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Електрон. дані. – Дніпро : НТУ «ДП», 2023. – Ч.1.– 371 с.
4. Жураковський Б. Ю. Комп'ютерні мережі. Частина 1. Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 336 с. – Режим доступу до ресурсу: <https://ela.kpi.ua/handle/123456789/36615>.
5. Жураковський Б. Ю. Комп'ютерні мережі. Частина 2 Навчальний посібник [Електронний ресурс] / Б. Ю. Жураковский, І. О. Зенів // КПІ ім. Ігоря Сікорського. – 2020. – 372 с. – Режим доступу до ресурсу: <https://ela.kpi.ua/handle/123456789/36641>
6. Wireshark · Go Deep. *Wireshark*. URL: <https://www.wireshark.org/> (date of access: 15.01.2024).
7. CIDR/VLSM Calculator - subnettingpractice.com. *subnettingpractice.com*. URL: <https://subnettingpractice.com/vlsm.html> (date of access: 15.01.2026).
8. VLSM Calculator. *VLSM Calculator*. URL: <https://vlsmcalc.vercel.app/> (date of access: 15.04.2026).
9. Інформаційні технології та комп'ютерна інженерія. LAB_KM (1 семестр). YouTube. URL: <https://youtube.com/playlist?list=PLYenPXThIsGjtUbFNUmoI046-IY2CZCg-&si=AAjDnhjxdwZwJaUR> (дата звернення: 02.09.2026).
10. Гнатушенко В. В. Словник термінів ІТ і комп'ютерної інженерії / укл.: В. В. Гнатушенко, Г. М. Коротенко, В. І. Олевський, В.Ю. Каштан [та ін.]; під ред. В. В. Гнатушенка, Г. М. Коротенка, Л. І. Цвіркуна. Дніпро:Національний технічний університет «Дніпровська політехніка», 2025. 709 с.

Навчальне видання

Каштан Віта Юріївна
Панферова Яна Володимирівна
Бешта Лілія Валеріївна

КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації до виконання лабораторних робіт
для здобувачів ступеня бакалавра
спеціальності F7 Комп'ютерна інженерія

У 2 частинах

Частина 1

Видано в авторській редакції.

Електронний ресурс.
Підписано до видання 16.07.2026. Авт. арк. 1,9.

Національний технічний університет «Дніпровська політехніка»
49005, м. Дніпро, просп. Дмитра Яворницького, 19