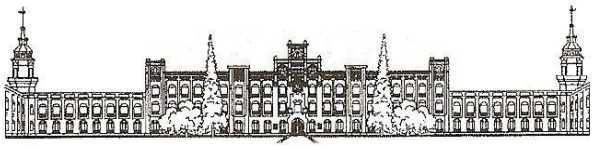

Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут»

Лабораторна робота №6

з дисципліни «Комп'ютерні мережі»

«Засвоєння принципів перетворення DNS-імен в IP-адреси»

Виконав студент групи: КВ-11

ПІБ: Терентьєв Іван Дмитрович

Перевірив: _____

Київ 2024

Мета роботи

Використовуючи програму моделювання комп’ютерних мереж засвоїти принципи адресації на канальному та мережевому рівнях моделі OSI, принципи динамічного призначення IP-адрес і принципів перетворення DNS-імен в IP-адреси.

План виконання лабораторної роботи

Завдання №1. Побудова локальної мережі з двома робочими станціями.

Завдання №2. Засвоєння принципів адресації на канальному і мережевому рівнях.

Завдання №3. Засвоєння принципів динамічного призначення IP-адрес.

Завдання №4. Засвоєння принципів перетворення DNS-імен в IP-адреси.

Завдання №5. Ознайомлення з відомостями про структуру перехресного кабеля.

Завдання

Завдання №1

- Відкрити програму Cisco Packet Tracer, вибрати End Devices і перетягнути мишкою на робоче поле дві робочі станції
- Далі потрібно з’єднати дві робочі станції кабелем. Для цього вибрати Connections і перехресний кабель
- Причини використання перехресного кабелю описані в розділі «Використання перехресного кабелю»
- Мишкою вибрати першу робочу станцію і підключити кабель до FastEthernet0
- Перетягнути мишкою з’єднання на другу робочу станцію і вибрати також FastEthernet0
- В результаті можна побачити, що з’єднання між робочими станціями відбулося – засвітилися зелені індикатори link
- Тепер потрібно вказати статичну IP-адресу комп'ютера. Для цього зробити подвійний клік по першій робочій станції, перейти в меню Desktop і вибрати режим IP Configuration
- Після цього задати IP-адресу і маску.
- На другій робочій станції виконати такі ж дії, але вказати IP-адресу 192.168.1.2
- Тепер на другій робочій станції вибрати режим Command Promt
- Відкривається командний рядок. З командного рядка виконати команду ping 192.168.1.1, в результаті виконання якої видно, що зв’язок між робочими станціями встановлений.
- На станції PC1 створено пакет (конверт), який чекає початку просування його мережею. Запустити просування пакету покроково можна, натиснувши на кнопку «Capture/Forward» (Вперед) у вікні симуляції. Якщо натиснути на кнопку «Auto Capture/Play» (відтворення), то можна спостерігати весь цикл проходження пакету мережт.. В закладці «Event list» (Список подій) можна бачити успішний результат «пінгування»

Завдання №2

- За допомогою програми Packet Tracer побудувати мережу.
- Призначити робочим станціям IP-адреси та маску. Перші три байти IP-адрес збігаються з адресою мережі, а останній байт дорівнює відповідно 1 та 2.
- Визначити MAC-адресу кожної робочої станції за допомогою команди ipconfig /all з командного рядка.
- На робочій станції PC1 з командного рядка виконати команду arp –a. Зафіксувати отриманий результат.
- На робочій чтанції PC1 з командного рядка виконати команду ping на адресу счтанції PC2, після чого знову виконати команду arp –a. Пояснити отриманий результат.
- На робочій станції PC1 з командного рядка виконати команду arp –d. Пояснити призначення ключа –d.
- Перейти в режим "Simulation". Із командного рядка робочої станції PC1 виконати команду ping на IP-адресу станції PC2. На «Simulation panel» натиснути кнопку «CaptureForward». Пояснити призначення пакетів, що відправляються зі станції PC1. Натиснути кнопкою миші на кожному із створених пакетів і переглянути їх вміст. Звернути увагу на адреси відправника та отримувача. Натискаючи на «CaptureForward» прослідкувати за формуванням та передачею створених пакетів мережею, одночасно спостерігаючи за командним рядком.
- Пояснити призначення ARP-пакету.
- Зробити висновки.

Завдання №3

- За допомогою програми Packet Tracer побудувати мережу
- Перейти до режиму «Simulation» .
- Вибрати режим конфігурування сервера. Призначити IP-адресу, перші три байти якої збігаються з адресою мережі, а останній байт дорівнює 100.
- У режимі конфігурування перейти до вкладки DHCP і налаштувати таким чином: у полях Default Gateway та DNS Server ввести адреси, перші три байти яких збігаються з адресою мережі, а останній байт відповідно дорівнює 254 та 253. У полі Start IP Adress ввести адресу, перші три байти якої збігаються з адресою мережі, а останній дорівнює 10. Значення поля Maximum number of Users встановити рівним 15.
- На PC1 включити динамічний режим конфігурування адрес (DHCP). Впевнитись, що поле IP-адреси, маска підмережі, шлюз за замовчуванням та DNS-сервер порожні. Не закриваючи вікна конфігурування PC1 натиснути кнопку «CaptureForward».
- Переглянути вміст пакета, що передав PC1, звернути увагу, що вказано в полі адреси отримувача, порівняти вміст пакетів «Inbound PDU» та «Outbound PDU». Визначити, яку інформацію передав DHCP-сервер станції.
- Послідовно натискаючи на кнопку «CaptureForward» спостерігати за рухом пакетів та аналізувати їх вміст. Дочекатися завершення конфігурування. На робочій станції PC1 переглянути вміст полів: IP- адреса, маска підмережі, шлюз за замовчуванням та DNS- сервер.
- Зробити висновки.

Завдання №4

- За допомогою програми Packet Tracer побудувати мережу. Призначити такі IP-адреси: перші три байти всіх адрес відповідають адресі мережі, останній байт PC1 – 1; DNS- сервера – 253; HTTP-сервера – 252.
- На PC1 в полі DNS вказати відповідну адресу.
- На DNS-сервері в вкладці DNS додати запис, в якому в полі Domain Name вказати ім’я scs.kpi.ua, а в полі IP-Address – адресу HTTP-сервера.
- Перейти до режиму «Simulation».
- На PC1 в командному рядку виконати команду ping, вказавши доменне ім’я scs.kpi.ua та натиснути кнопку «Capture/Forward».
- Натискати кнопку «Capture/Forward», поки на PC1 не буде сформований DNS-запит. Пояснити призначення ARP-пакетів, які були сформовані на попередніх кроках.
- Коли DNS-запит надійде на сервер, переглянути його вміст (Inbound PDU) та вміст відповіді (Outbound PDU). Пояснити інформацію, що міститься в цих пакетах.
- Натиснути кнопку «Capture/Play» та дочекатися завершення виконання команди, пояснити причину утворення всіх пакетів.
- Перейти в режим «Real Time».
- У налаштуваннях DNS-сервера відключити DNS-сервіс. У полі URL веб браузера на PC1 набрати IP-адресу HTTP-сервера. Зафіксувати результат. Замість IP-адреси HTTP-сервера набрати його DNS-ім’я. Пояснити отриманий результат. Не закриваючи вікна веб браузера включити DNS-сервіс. Зафіксувати зміни, що відбулися.

Завдання №5

- Навести теоретичні відомості про кабель типу «вита пара». Використання перехресного кабелю

Теоретичні відомості

Адресація в мережі OSI

Адресація є ключовим елементом роботи мереж. У моделі OSI кожен рівень використовує свій метод і формат адресації:

Канальний рівень використовує MAC-адреси для передачі даних між пристроями в одній мережі.

Мережевий рівень використовує IP-адреси для маршрутизації пакетів між мережами.

DHCP (Dynamic Host Configuration Protocol)

DHCP автоматизує процес призначення IP-адрес, шлюзів і DNS-серверів. Цей протокол працює за схемою DORA:

Discover: клієнт шукає сервер.

Offer: сервер пропонує конфігурацію.

Request: клієнт запитує конфігурацію.

Acknowledge: сервер підтверджує запит.

DNS (Domain Name System)

DNS відповідає за перетворення доменних імен у відповідні IP-адреси. Основні етапи роботи DNS:

Відправка DNS-запиту з клієнта на сервер.

Пошук відповідного запису в зоні домену.

Формування відповіді з IP-адресою.

ARP (Address Resolution Protocol)

ARP використовується для перетворення IP-адрес у MAC-адреси. Цей протокол працює в локальних мережах, де кожен пристрій має унікальну MAC-адресу.

Вита пара та перехресний кабель

Вита пара використовується для передачі даних у мережах Ethernet. Перехресний кабель змінює місця розташування передаючих і приймаючих пар проводів, що дозволяє безпосередньо з’єднувати пристрої одного рівня (наприклад, ПК з ПК).

Хід роботи

Завдання №1

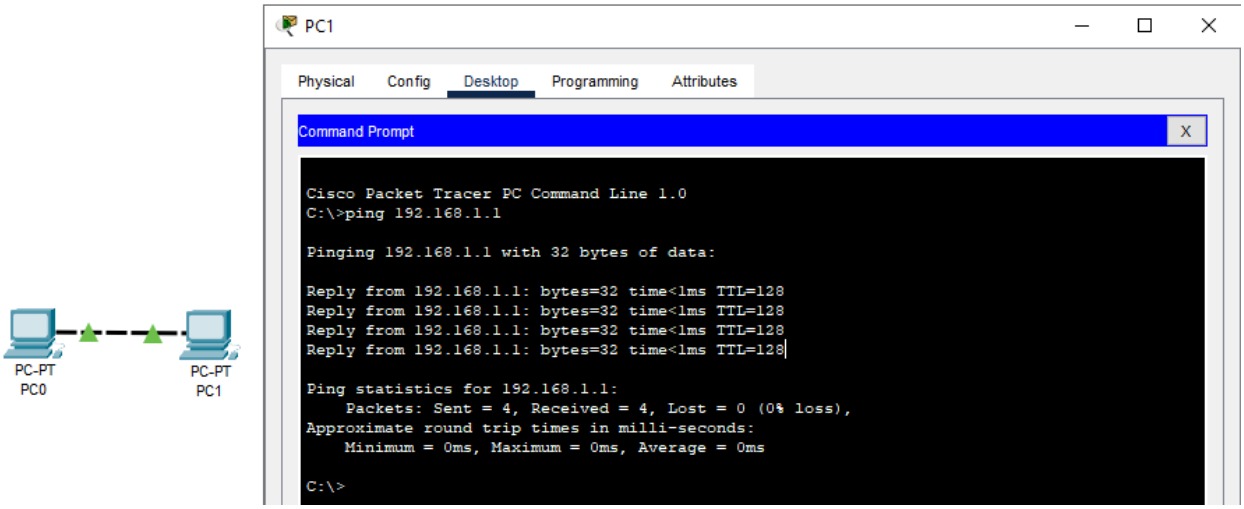

Рис. 1 – Перевірка з'єднання між двома ПК за допомогою команди ping.

Обидва ПК успішно відповідають на запити, що свідчить про правильну конфігурацію мережі.

Завдання №2

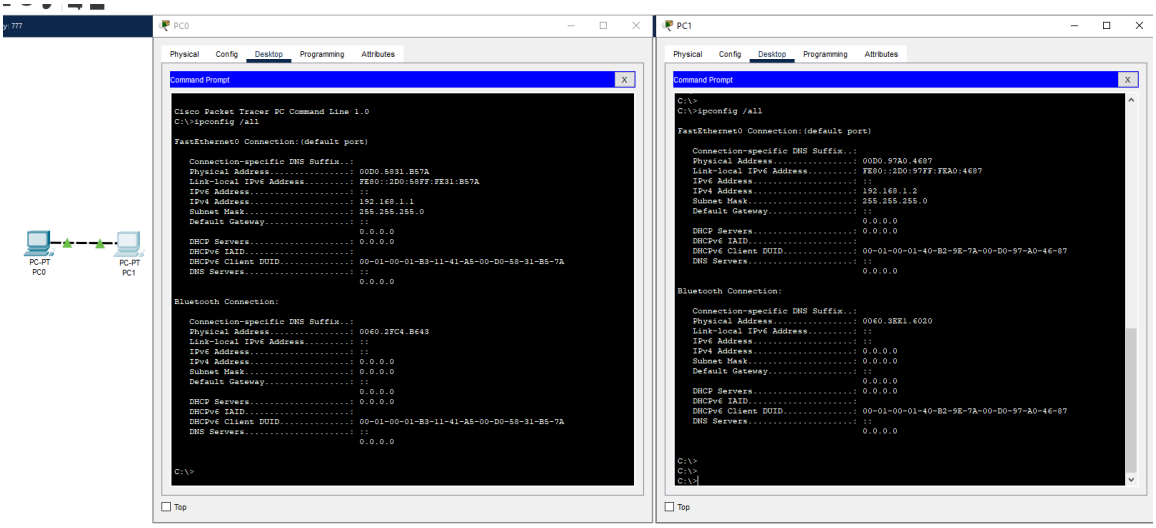

Рис. 2 – Виведення інформації про мережеву конфігурацію за допомогою команди ipconfig /all.

Показано статичні IP-адреси, маски підмережі та MAC-адреси для обох ПК.

До виконання ping команда arp -a показує порожню ARP-таблицю, оскільки інформація про MAC-адреси відсутня. Після виконання ping ARP-таблиця заповнюється відповідним записом, який включає IP-адресу ПК2 та його MAC-адресу. Це відбувається тому, що для успішного надсилання ICMP-запитів (ping) ПК1 виконав ARP-запит для визначення MAC-адреси ПК2.

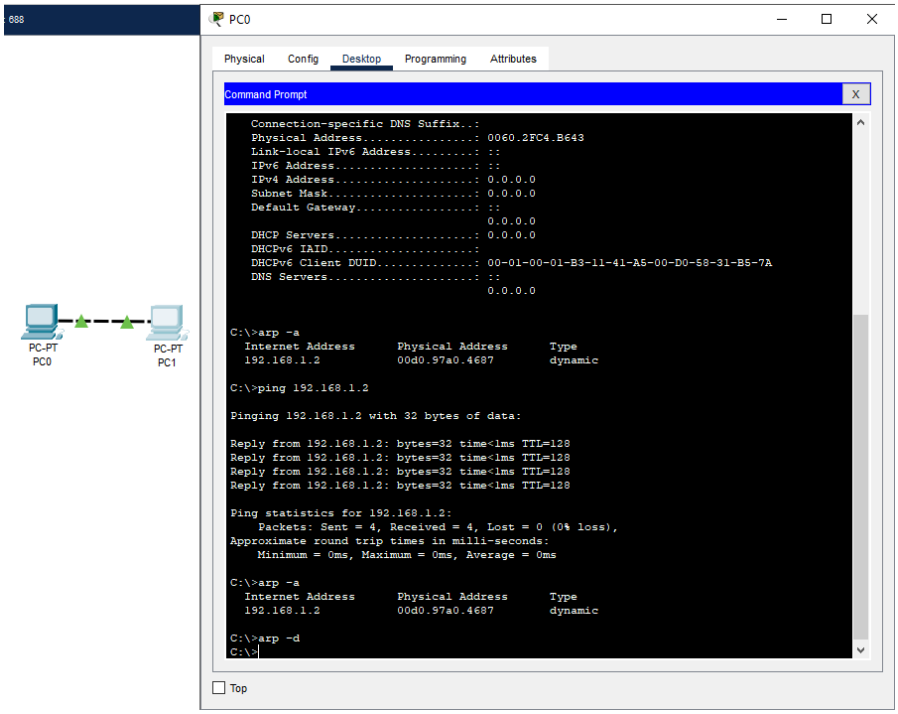

Рис. 3 – Використання команди arp -a для перегляду ARP-таблиці після виконання команди ping.

В таблиці ARP відображені MAC-адреси пристроїв у мережі. Виконано перевірку доступності сусіднього ПК.

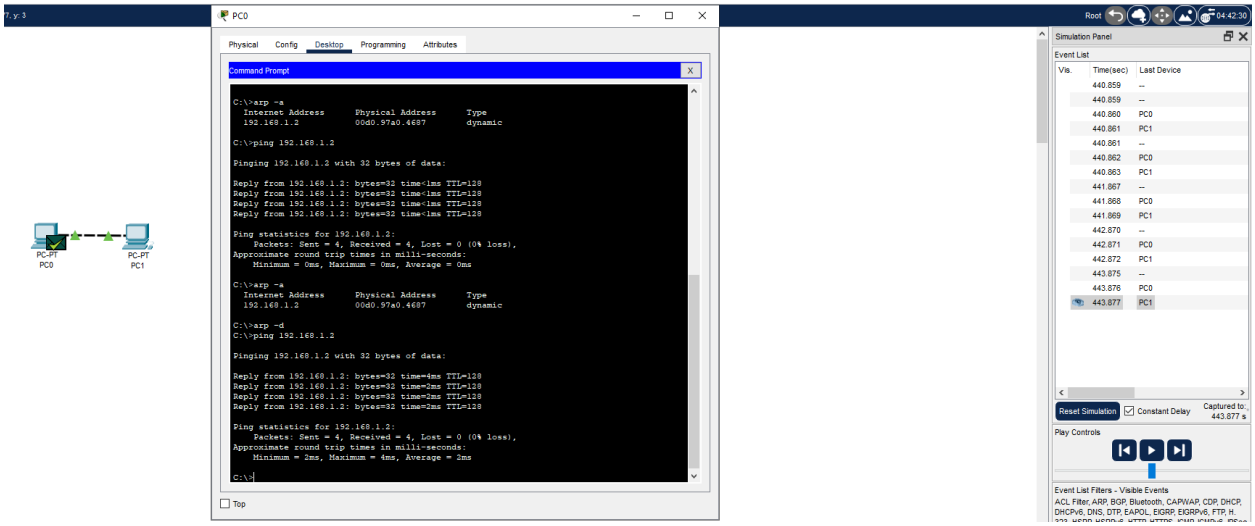

Рис. 4 – Видалення записів з ARP-таблиці за допомогою команди arp -d.

Після очищення ARP-таблиці та повторного ping таблиця заповнюється знову, що підтверджує процес оновлення ARP.

Ключ -d видаляє записи з ARP-таблиці. Це корисно для очищення кешу ARP або примусового оновлення інформації в таблиці.

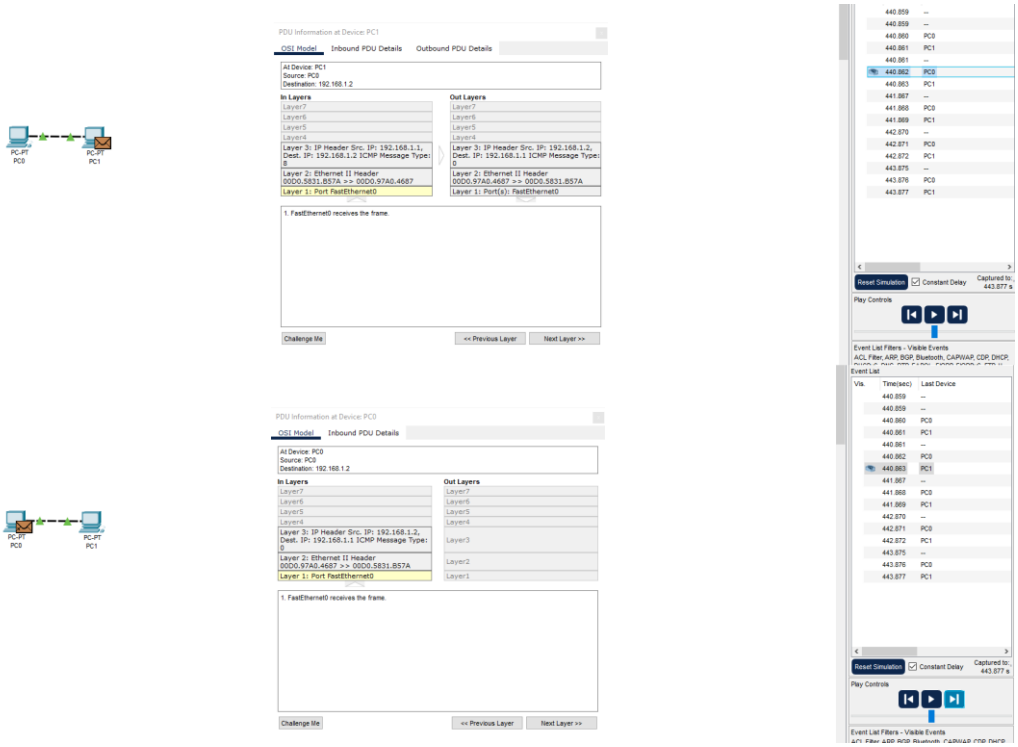

Рис. 5 – Вивчення деталей ICMP-пакетів між ПК0 та ПК1 у режимі симуляції.

На скріншоті показано процес передачі ICMP-пакета від ПК0 до ПК1 та у зворотному напрямку. Відображено структуру Ethernet-заголовка та IP-заголовка, а також рівні обробки пакета у моделі OSI.

Два ПК успішно взаємодіють через мережу. Обмін ARP-запитами дозволив визначити MAC-адреси, необхідні для передачі даних на канальному рівні. Команди ping підтвердили доступність станцій і належну роботу мережі.

Завдання №3

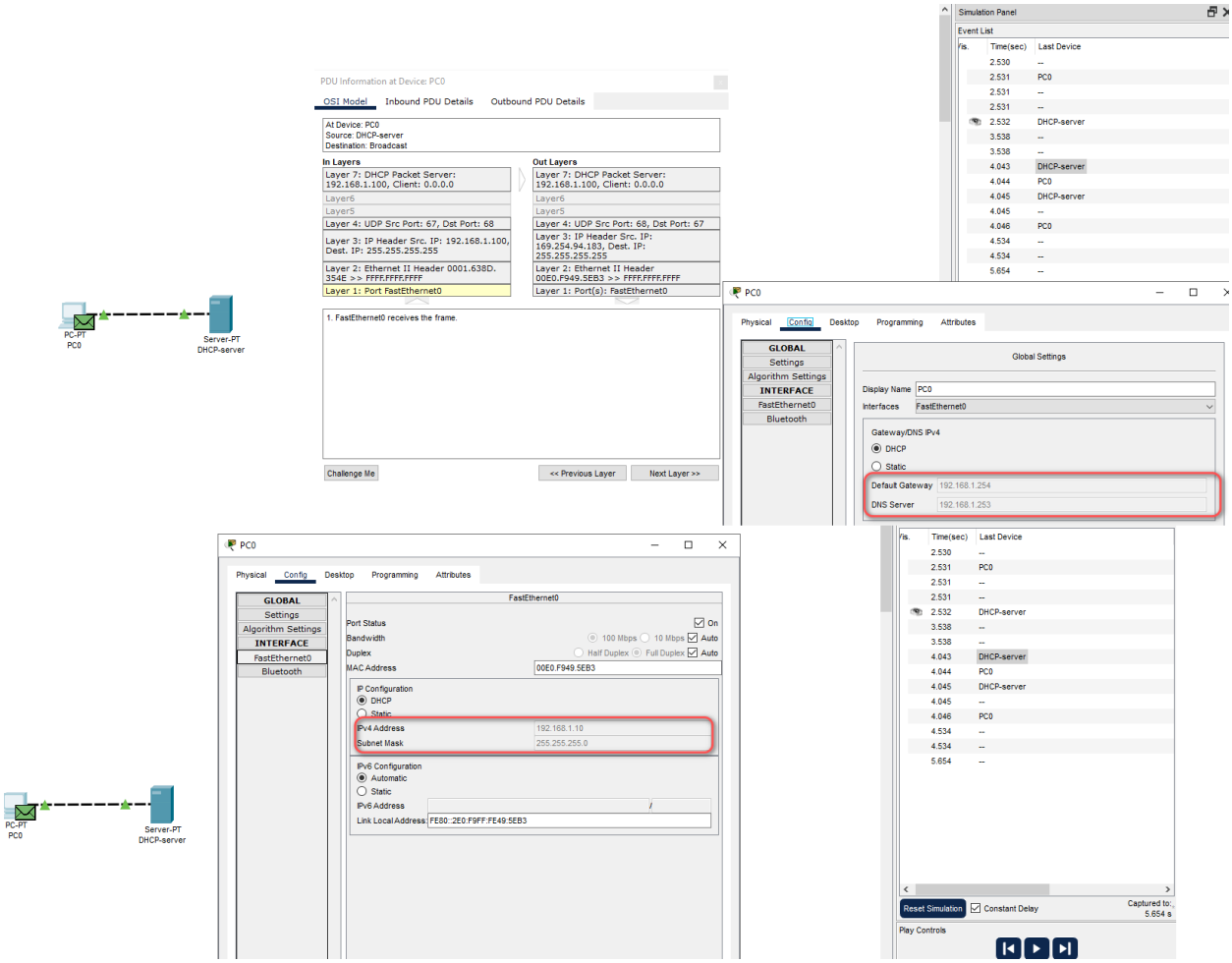

Рис. 6 – Налаштування DHCP-сервера для автоматичного призначення IP-адрес.

У режимі симуляції показано процес взаємодії за схемою DORA (Discover, Offer, Request, Acknowledge).

DHCP-сервер передав таку інформацію: IP-адресу для ПК, маску підмережі, шлюз за замовчуванням та адресу DNS-сервера.

Порівняння пакетів: У Inbound PDU відображена інформація, отримана ПК від DHCP-сервера, тоді як у Outbound PDU показано запит ПК на отримання IP-конфігурації (етап Discover).

DHCP-сервер динамічно призначив IP-адресу та інші параметри мережевої конфігурації для ПК, що автоматизувало процес налаштування мережі. Взаємодія проходила за схемою DORA (Discover, Offer, Request, Acknowledge).

Завдання №4

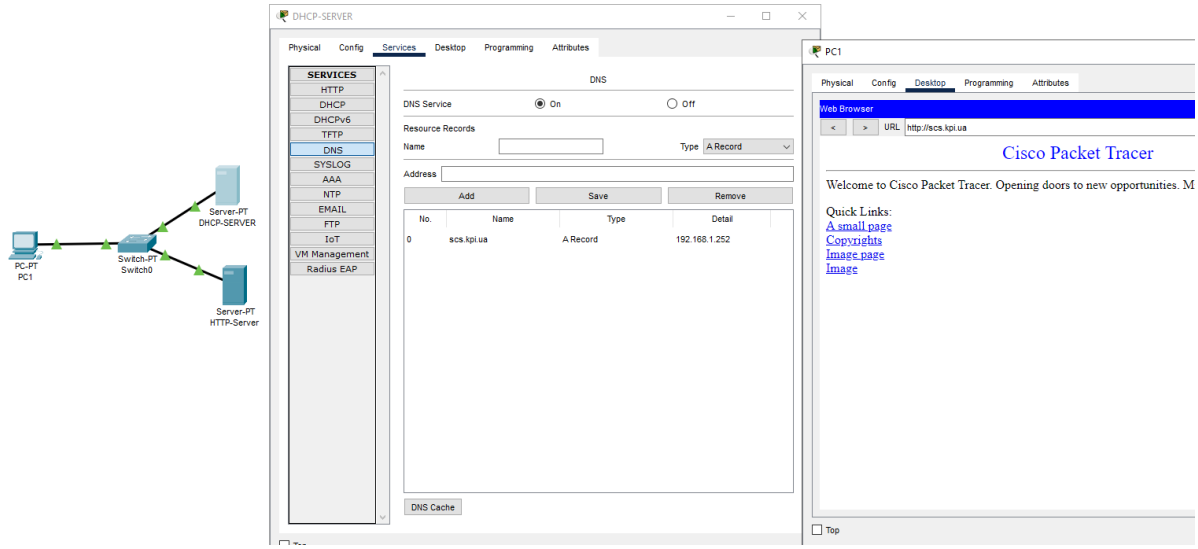

Рис. 7 – Налаштування DNS-сервера для домену scs.kpi.ua.

ARP-пакети використовувалися для визначення MAC-адрес пристроїв у локальній мережі. Це дозволило встановити зв'язок між двома ПК на канальному рівні.

Крім ARP-пакетів, передавалися ICMP-запити та відповіді (для перевірки доступності), а також DHCP-пакети (для отримання IP-адреси) та DNS-запити (для перетворення доменного імені у IP-адресу).

DNS-сервер забезпечує перетворення доменного імені scs.kpi.ua у відповідну IP-адресу. Якщо DNS-сервер вимкнений, браузер не може визначити IP-адресу, і з'єднання не встановлюється.

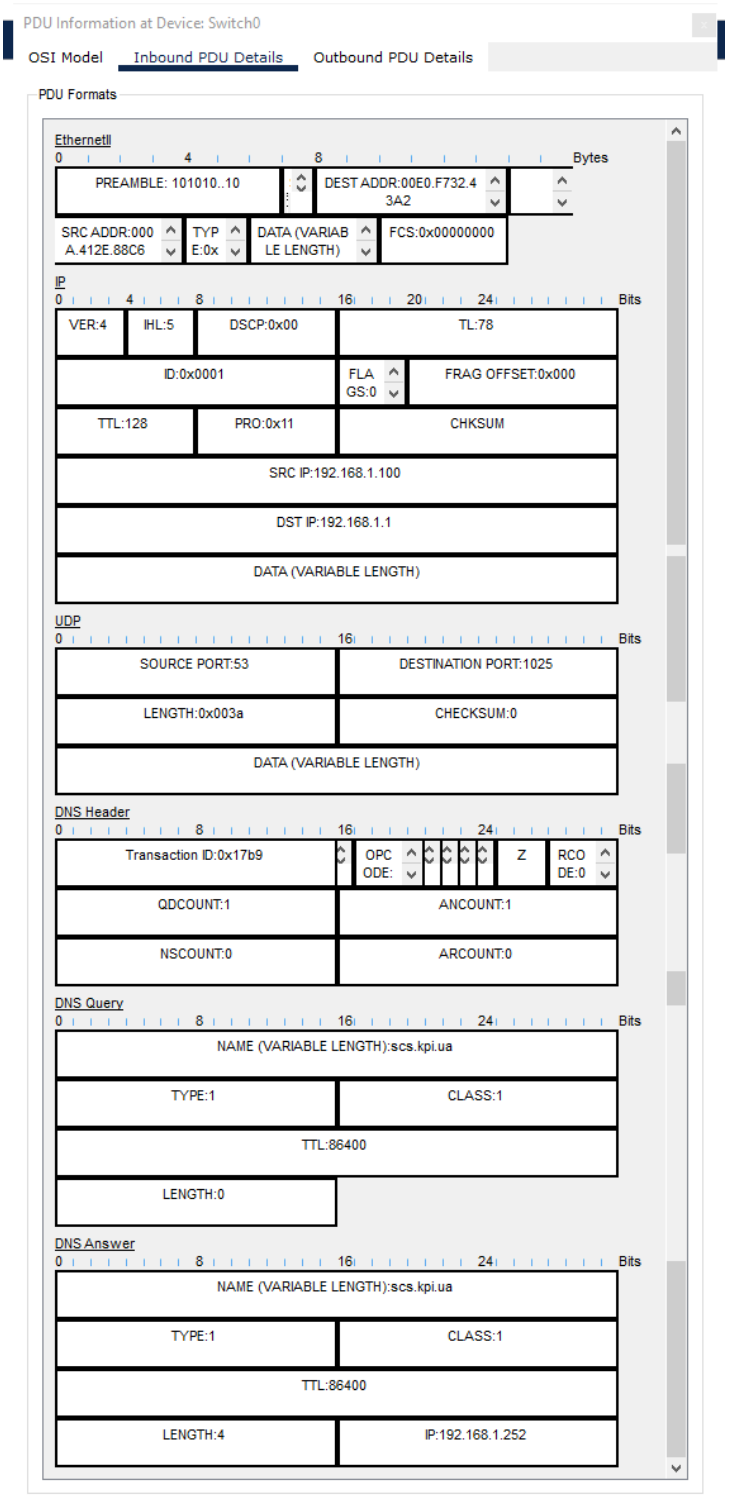

Рис. 8 – Відображення вихідної відповіді DNS-сервера у форматі PDU.

DNS-сервер формує відповідь із відповідною IP-адресою для доменного імені, показано всі рівні обробки пакета.

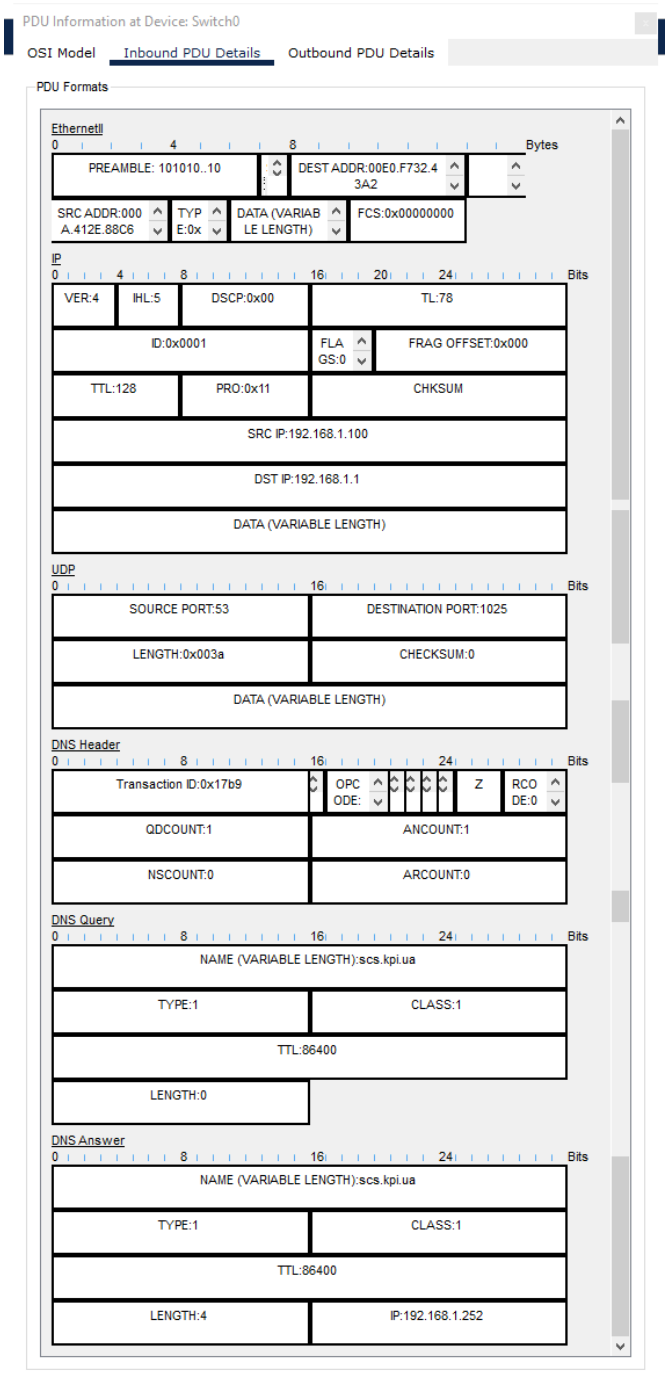

Рис. 9 – Відображення вхідного DNS-запиту в деталях PDU.

Деталізована структура запиту на отримання IP-адреси для доменного імені scs.kpi.ua з зазначенням полів DNS-запиту.

PDU показує структуру пакета, включаючи заголовки Ethernet та IP, які використовуються для передачі даних між станціями. Важливими елементами є IP-адреси джерела та призначення, а також MAC-адреси.

Завдання №5

Перехресний кабель використовується для прямого з'єднання двох пристроїв одного рівня (наприклад, ПК з ПК). Він змінює передачу та прийом даних між пристроями, що дозволяє здійснювати зв’язок без проміжного обладнання.

Висновок

У ході виконання лабораторної роботи було засвоєно основні принципи роботи мережевих протоколів, таких як ARP, DHCP та DNS, а також їх взаємодію у моделі OSI. Було налаштовано локальну мережу з використанням перехресного кабелю, проведено аналіз передачі даних між ПК, і досліджено структуру мережевих пакетів.

- Комунікація між ПК: Встановлено, що для обміну даними між станціями необхідно визначати MAC-адреси за допомогою ARP-запитів. Команди arp -a та arp -d підтвердили правильність роботи ARP-таблиці.
- Робота DHCP: Сервер успішно передав конфігураційні дані, зокрема IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервер. Схема DORA дозволила автоматизувати налаштування мережі.
- DNS: Було продемонстровано, що DNS-запити дозволяють перетворювати доменні імена на IP-адреси. У разі вимкнення DNS-сервера доменне ім'я не може бути розпізнане, що унеможливлює доступ до ресурсу через ім'я.
- Пакети PDU: Порівняння Inbound та Outbound PDU показало структуру мережевих пакетів, що підтверджує роботу протоколів на різних рівнях OSI.
- Перехресний кабель: Використання перехресного кабелю забезпечило пряме підключення між двома станціями, що дозволило здійснити тестування мережі без додаткового обладнання.

Таким чином, було досягнуто поставленої мети — розуміння роботи основних мережевих протоколів і практичне застосування знань для налаштування мережевої взаємодії.