Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

Звіт до комп’ютерного практикуму № 1

з дисципліни «Тестування та контроль якості (QA) вбудованих систем»

на тему: Налаштування мережевого оточення та тестування протоколу ARP

|  |  |
| --- | --- |
| Прийняв:  \_\_\_Гайдай А.\_\_\_\_\_\_\_\_\_\_\_\_ | Виконав:  студент гр. ІК-92  \_\_\_\_\_Кравець М.О.\_\_\_\_\_ |

Київ – 2022р.

**Мета роботи**: ознайомитись з базовою еталонною моделлю взаємодії відкритих систем, зрозуміти важливість декомпозиції у комп’ютерних мережах, ознайомитись з існуючим мережевим обладнанням та технологіями передачі сигналів.

**Структура лабораторної роботи:**

▪ налаштувати оточення для експериментального дослідження основних

процесів та артефактів канального рівня моделі ОSI, зокрема форматів

фреймів Ethernet, формату MAC адрес, протоколу ARP;

▪ експериментально ознайомитися з протоколом передавання службових

повідомлень ІCMP;

▪ навчитися користуватися мережною утілітою ping;

▪ з використанням програми wireshark дослідити основні етапи отримання

MAC адрес протоколом ARP на канальному рівні моделі OSI.

**Хід роботи**

**Встановлення та запуск wireshark:**

1) Додано офіційний PPA, щоб завантажити останню стабільну версію (рис.1)

$ sudo add-apt-repository ppa:wireshark-dev/stable

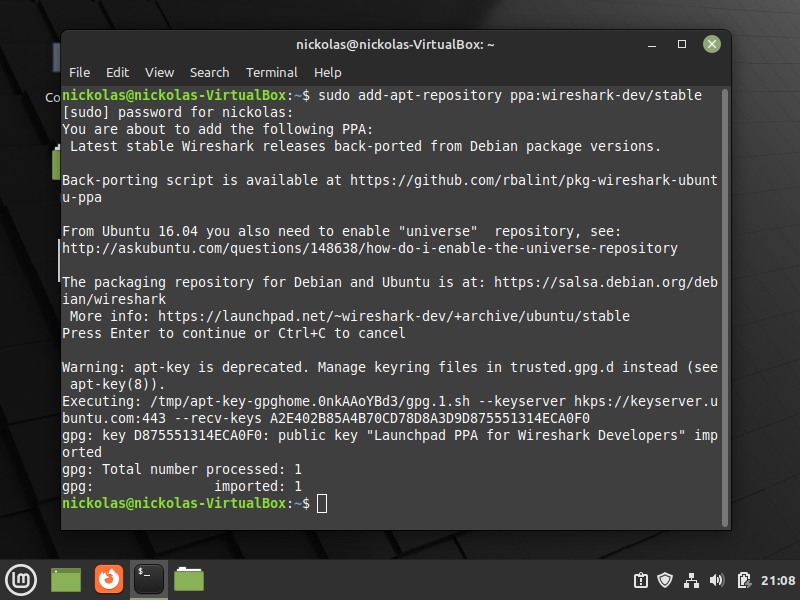


Рис.1. Додання офіційного PPA

2) Оновлено списки пакетів з репозиторіїв для оновлення пакетів (рис.2)

$ sudo apt-get update

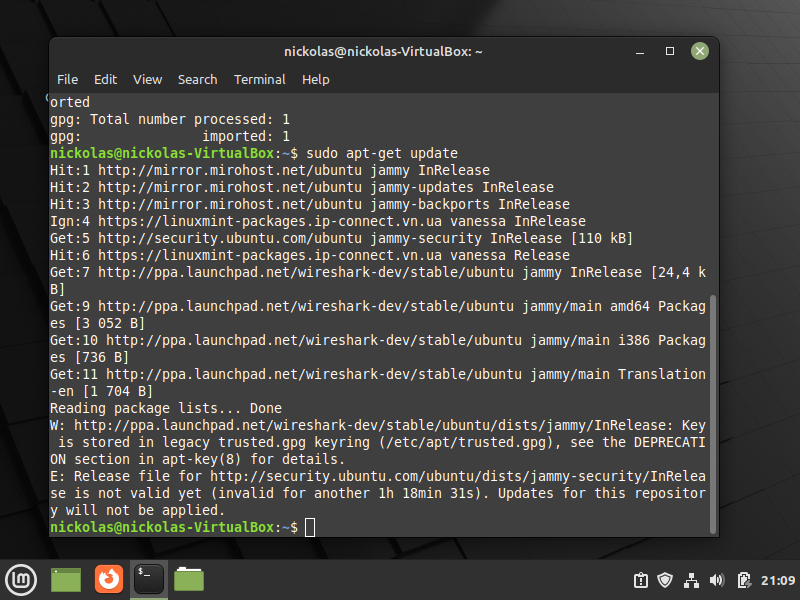


Рис.2. Оновлення списків пакетів

3) Завантажено wireshark (рис.3-4)

$ sudo apt-get install wireshark

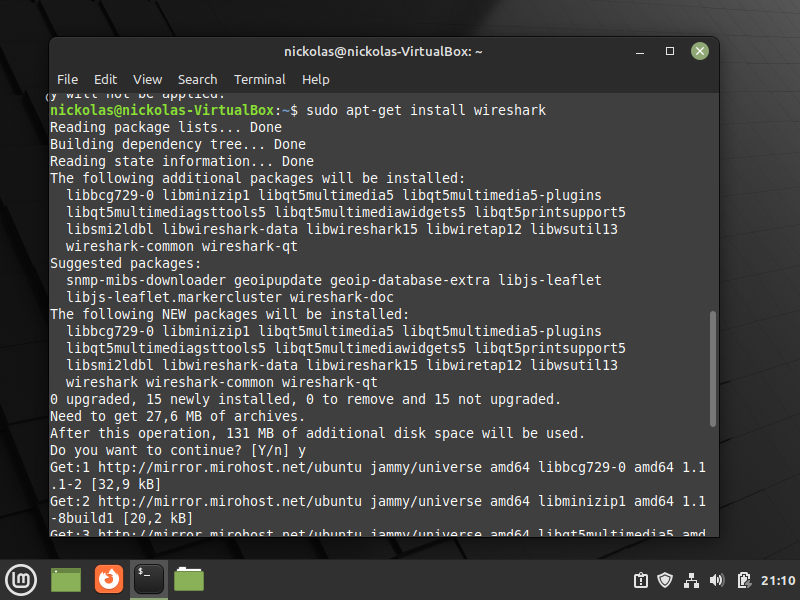


Рис.3. Встановлення wireshark

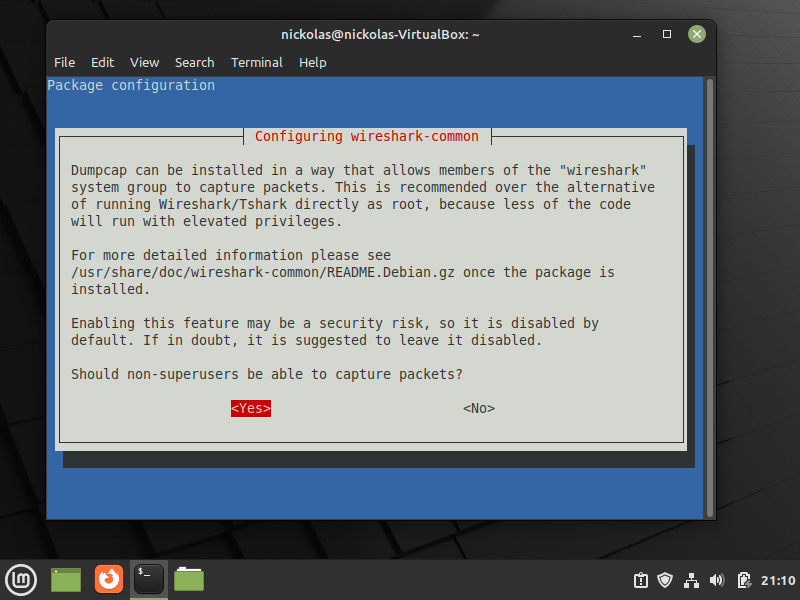


Рис.4. Вікно для конфігурації

4) Запустіть wireshark

$ sudo wireshark

Оскільки було дозволено не-суперкористувачу (nonsuperuser) перехоплювати пакети, то необхідно додати користувача в групу wireshark наступною командою:

$ sudo adduser $USER wireshark

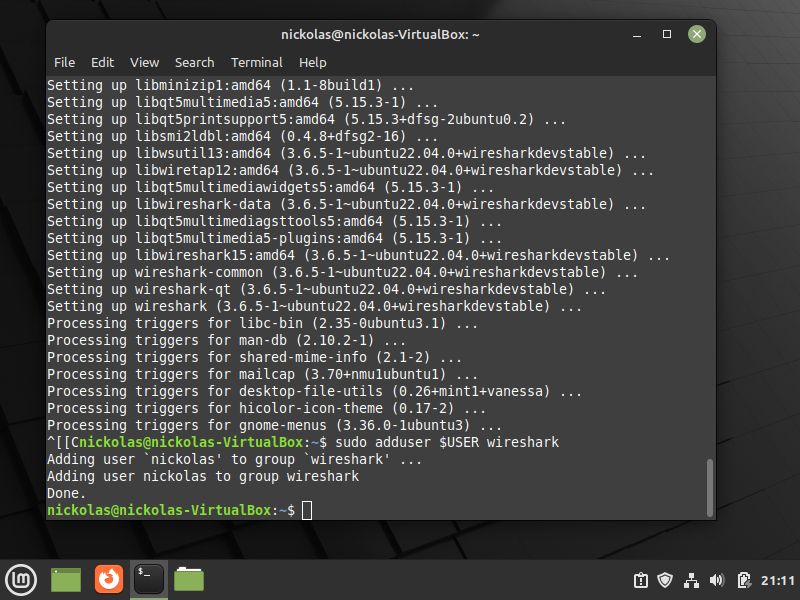


Рис.5. Додавання користувача в групу wireshark

**Захоплення пакетів у Wireshark.**

Після запуску Wireshark, можна побачити список доступних інтерфейсів, які

Можуть бути використані для захоплення пакетів (рис. 6). Для захоплення пакетів, було обрано бажаний інтерфейс та натиснуто на піктограму Почати захоплення пакетів.

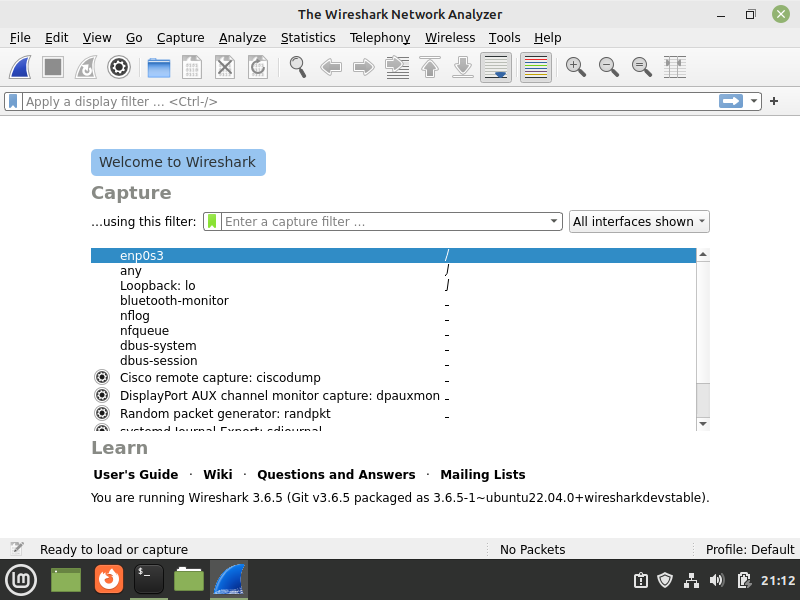


Рис.6. Перелік інтерфейсів для аналізу трафіка

В іншому терміналі введено $ ping google.com та відстежено трафік, який передається через обраний інтерфейс – захоплення пакетів програмою Wireshark (рис. 7).

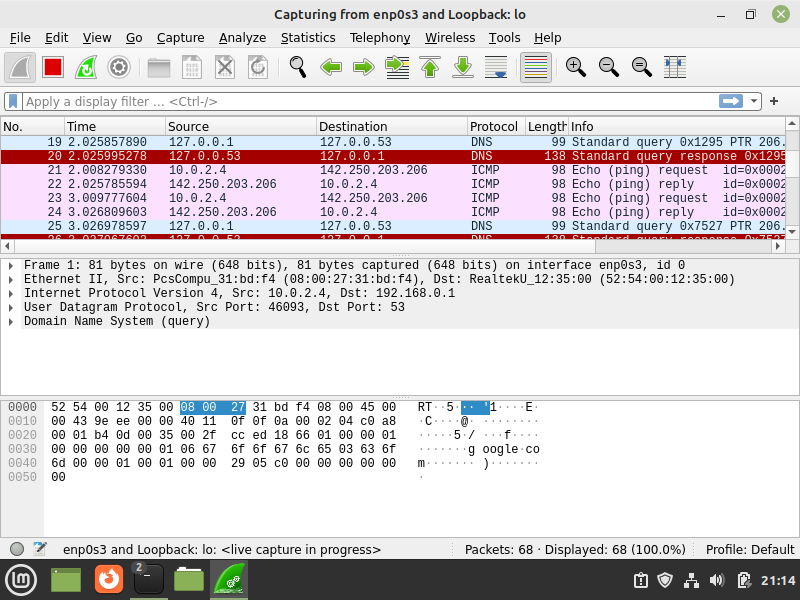


Рис.7. Перегляд інформації про захоплення пакетів

**Налаштування фільтрів у Wireshark**

Це дуже потужна можливість. За допомогою фільтрів можна прибрати

трафік, який нас не цікавить, та залишити тільки потрібний. Трафік можна

фільтрувати по МАС-адресі, ІР-адресі, підмережі або протоколу.

Приклад фільтрів по ІР-адресі зображено на рис.8.

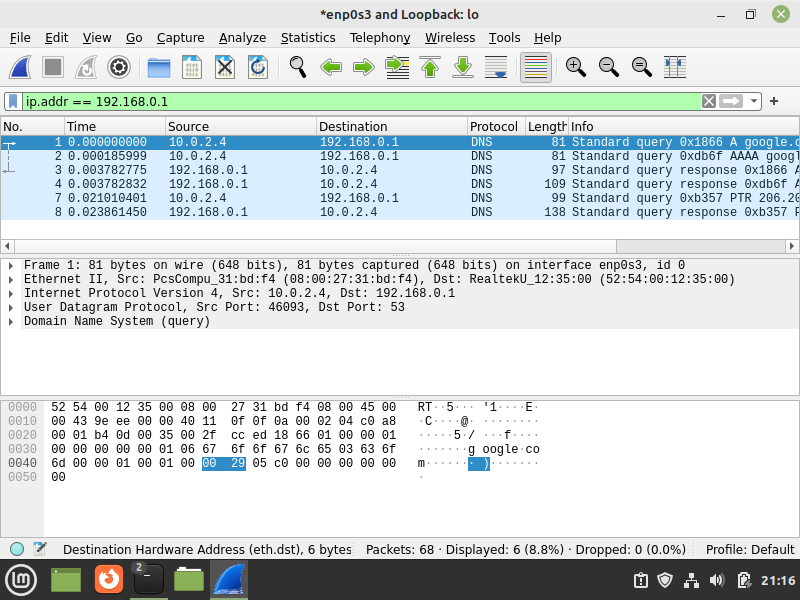


Рис.8. Приклади фільтрів по ІР-адресі

**Порядок виконання завдання лабораторної роботи:**

Для виконання лабораторного завдання необхідно два комп’ютери, з’єднані за допомогою ethernet. У даному випадку будуть використовуватися 2 віртуальні машини з’єднані в одну мережу.

Переконаємося, що arp таблиця не має даних про інший комп’ютер (рис.9):

$ arp -a

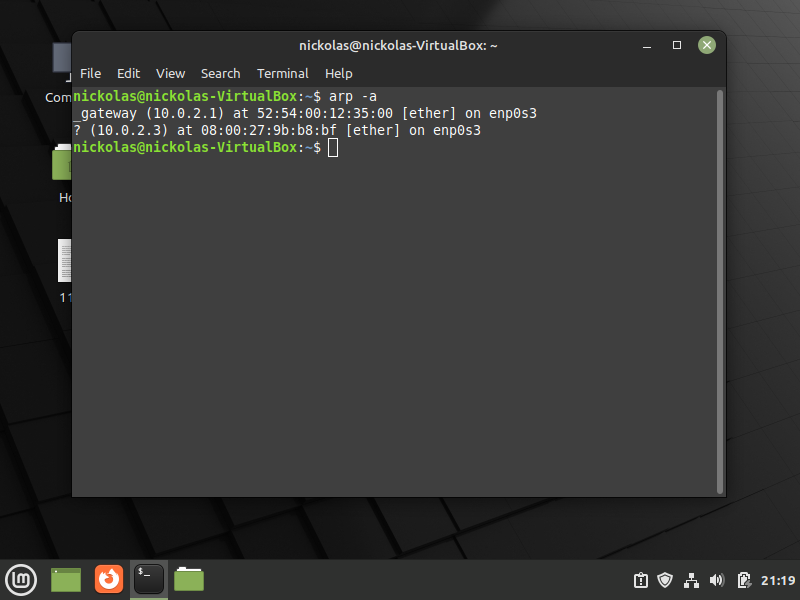


Рис.9. Перевірка arp таблиці на наявність другого комп’ютера

Запуск wireshark:

$ sudo wireshark

Відкрито для аналізу трафіку відповідний інтерфейс (у даному випадку enp0s3)

Після цього відкрийто другий термінал та пропінговано другий пристрій:

$ ping 10.0.2.15

Проаналізовано отриманий трафік у Wireshark (рис.10).

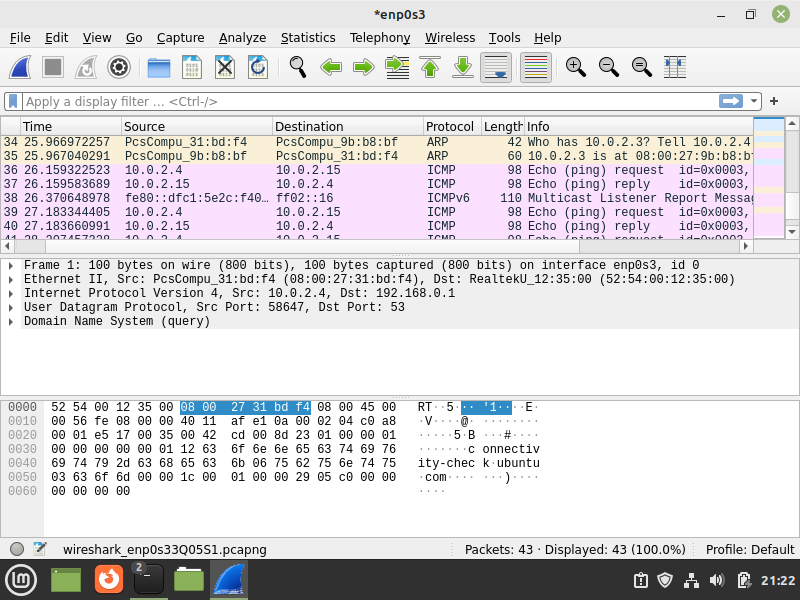


Рис.10. Аналіз отриманого трафіку у Wireshark

Перевірено arp таблицю командою (рис.11):

$ arp -a

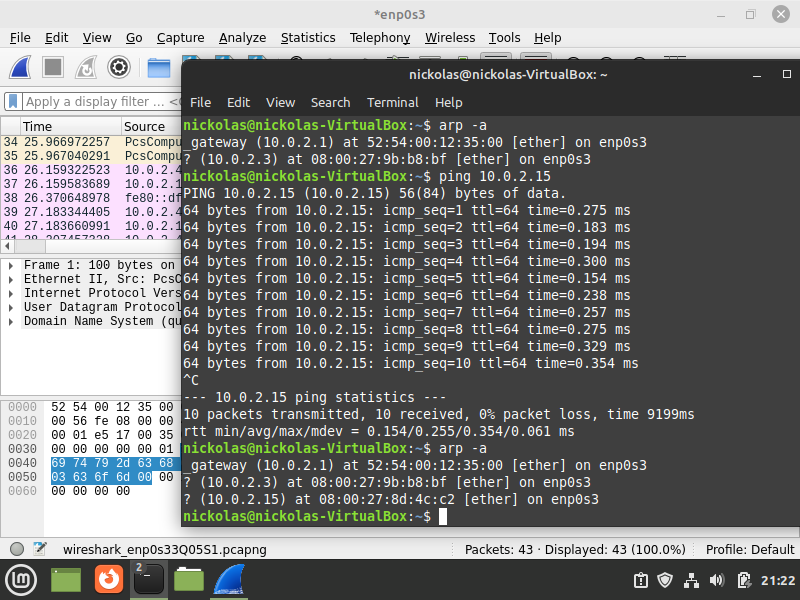


Рис.11. Перевірка arp таблиці

З’явився рядок з ІР-адресою та МАС-адресою 2 комп’ютера (ip 10.0.2.15).

У Wireshark прибрано трафік, який нас не цікавить, та виділено рядки з arp-протоколом, використовуючи фільтри (рис.12).

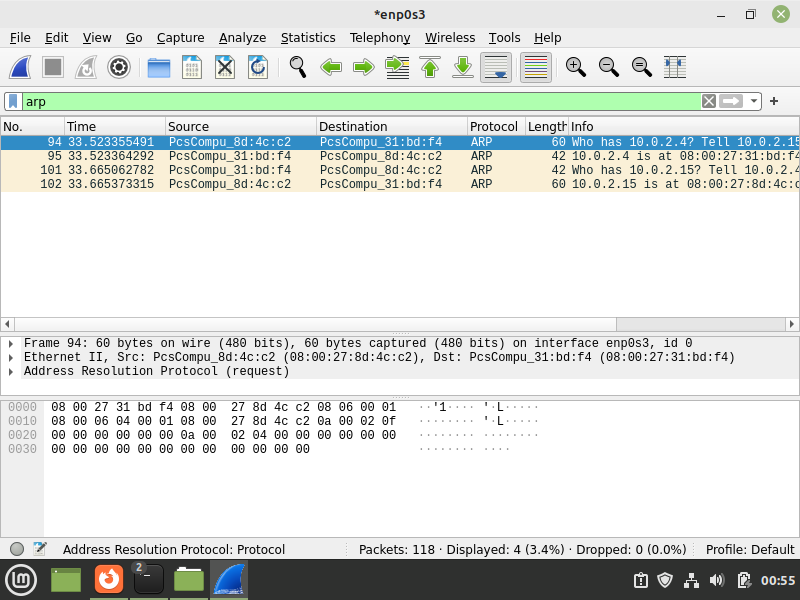


Рис.12. Виділення рядків з arp-протоколом, використовуючи фільтри

**Test-case:**

Варіант 1

Test case ID: TC\_AT\_1

Test priority: high

Test designed by: Mykola Kravets

Date of test designed: 26.09.2022

Test executed by: Mykola Kravets

Summary: ARP-table updates after receiving ARP-reply

Description: Ensure that the arp-table is updated when an arp-reply is received

Version: ARPv1

Setup Descriptions:

PC1 ---- Ethernet1 ---- PC2

PC1: 10.0.2.4

PC2: 10.0.2.15

Steps(With ER)

1. Clean ARP-table

arp -d 10.0.2.15

ER: verify that value for PC2 is absent

2. Run Wireshark from PC1 for ethernet1

3. Run ping from PC1 to PC2

ER: ping is running

4. Verify that in Wireshark ARP-request and ARP-reply are present for ip and Mac of PC1 and PC2

ER: ARP-request and ARP-reply are present

5. Verify that ARP-table is updated after receiving ARP-reply

arp -a

ER: verify that after receiving ARP-reply ARP-table was updated with the value for PC2.

**Висновок**

У даній лабораторній роботі я ознайомився з базовою еталонною моделлю взаємодії відкритих систем, зрозумів важливість декомпозиції у комп’ютерних мережах, ознайомився з існуючим мережевим обладнанням та технологіями передачі сигналів. Також я виконав лабораторні завдання та описав test-case за вказаним варіантом.