Міністерство освіти і науки України
Національний технічний університет України «КПІ» імені Ігоря Сікорського
Кафедра обчислювальної техніки ФІОТ

ЗВІТ
з лабораторної роботи №1
з навчальної дисципліни «Тестування та контроль якості (QA) вбудованих систем»

Тема:
НАЛАШТУВАННЯ МЕРЕЖНОГО ОТОЧЕННЯ ТА ТЕСТУВАННЯ ПРОТОКОЛУ ARP

Виконав:
студент IV курсу ФІОТ
групи ІВ-93
Залікова №9325
Варіант – 1

Перевірила:
Клименко І.А.

Київ 2022

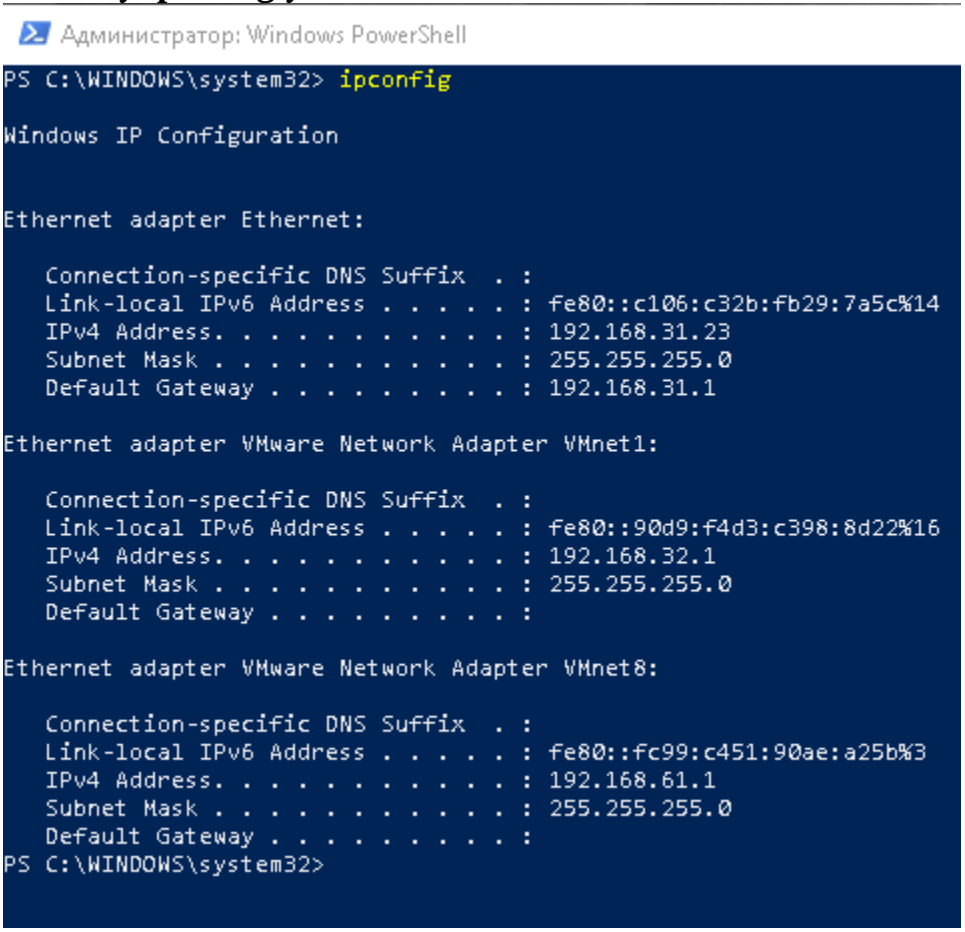
I. Мета: Навчитися налаштовувати мережне оточення для тестування вбудованих
систем та пристроїв IoT. Навчитися використовувати утиліту wireshark для аналізу трафіка в комп'ютерній мережі. Протестувати мережне оточення на канальному рівні моделі OSI.

II. Завдання:

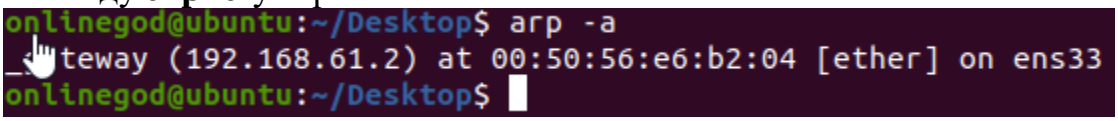
▪ налаштувати оточення для експериментального дослідження основних процесів та артефактів канального рівня моделі OSI, зокрема форматів фреймів Ethernet, формату MAC адрес, протоколу ARP;
▪ експериментально ознайомитися з протоколом передавання службових повідомлень ICMP;
▪ навчитися користуватися мережною утілітою ping;
▪ з використанням програми wireshark дослідити основні етапи отримання MAC адрес протоколом ARP на канальному рівні моделі OSI.
QA завдання: QA Embedded Testing на прикладі протоколу ARP
Розроблення ARP Test Cases.

По варіанту:
1)Переконатися в тому, що arp-таблиця оновлюється при отриманні arp-reply.

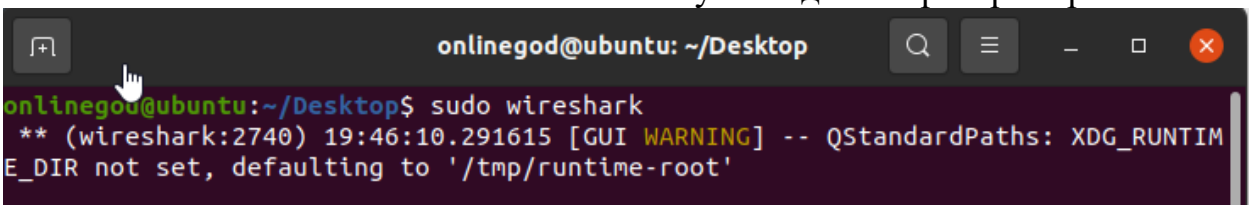
1. На PC2 куди мы будемо відсилати пакети дізнаемося IP адрессу через команду **ipconfig** у Windows Power Shell

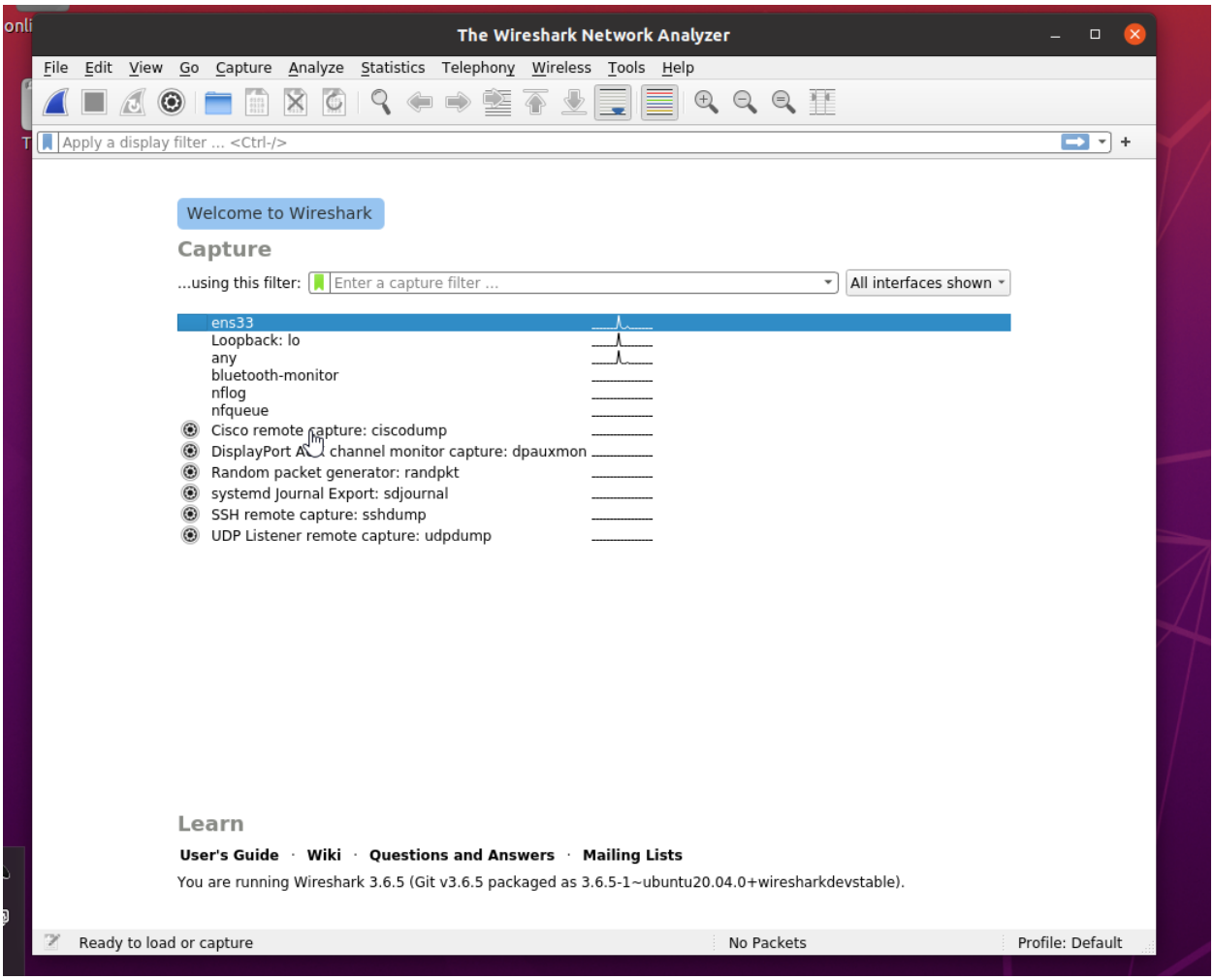


2. Перевіряємо на PC1 **arp** таблицю щоб там не було кешу про PC2 через команду **arp -a** у терміналі

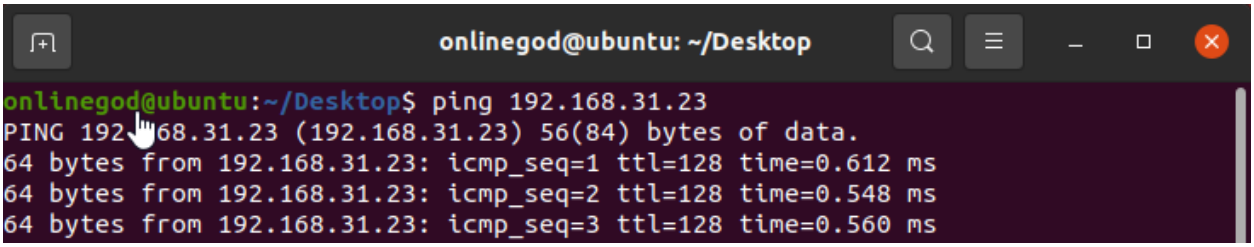


3.Запускаємо Wireshark на PC1 командою **sudo wireshark** попердньо його встановивши там обновивиши як показано у звіті до лабораторної роботи

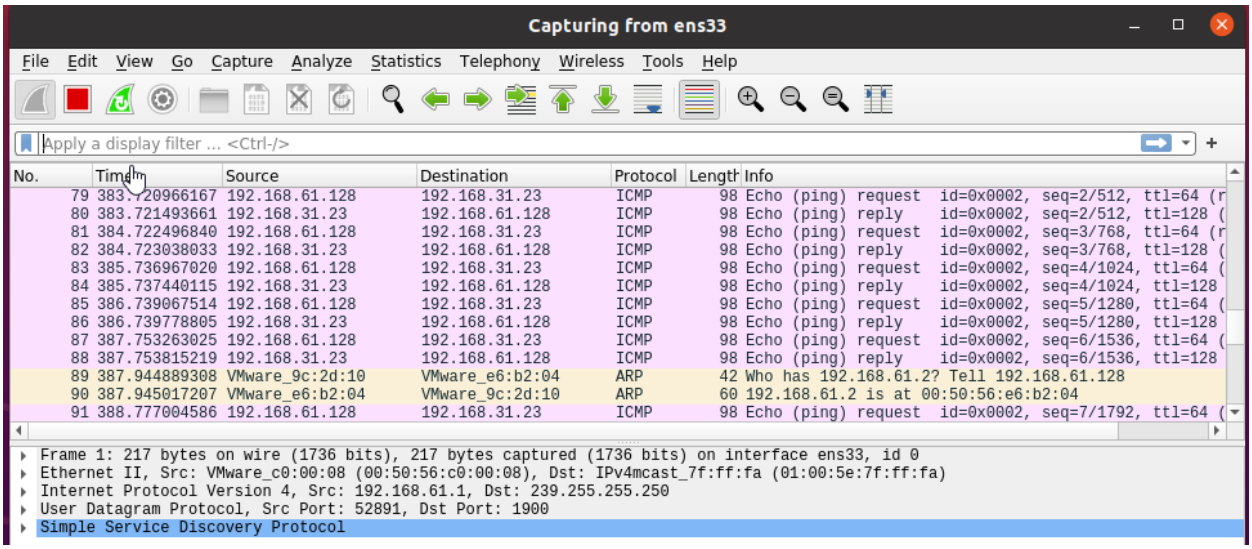




4.Знаючи IP адрессу PC2 посилаємо пакети на PC1 командою **ping 192.168.31.23**

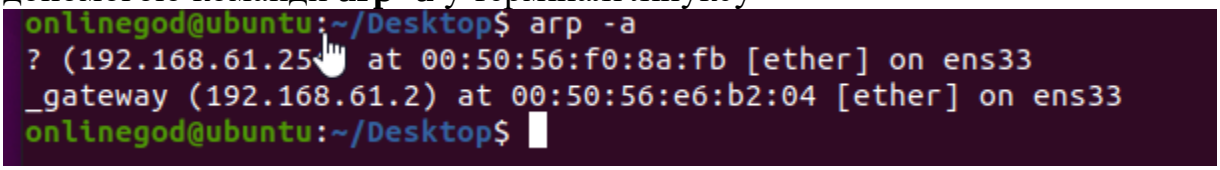


5.Обираємо **ens33** та починаємо відстежувати пакети



6. Бачимо що Wireshark відстежує наш ping та як працює ARP протокол а саме питає хто це(IP адреса) та наш PC2 відповідає на це своєю MAC адресою(00:50:56:e6:b2:04)

7. Також перевіряємо після цих взаємодій з іншим PC нашу arp таблицю за допомогою команди **arp -a** у терміналі лінуксу



Тепер у нас є кеш про PC2.(його можна видалити командою **arp -d [IP адреса]**)

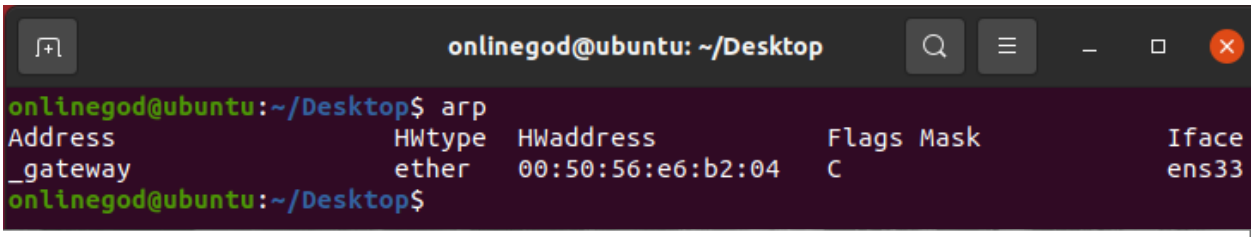
Завдання по варіанту виконано arp-таблиця оновлюється при отриманні arp-reply та на це зроблен Test Case.

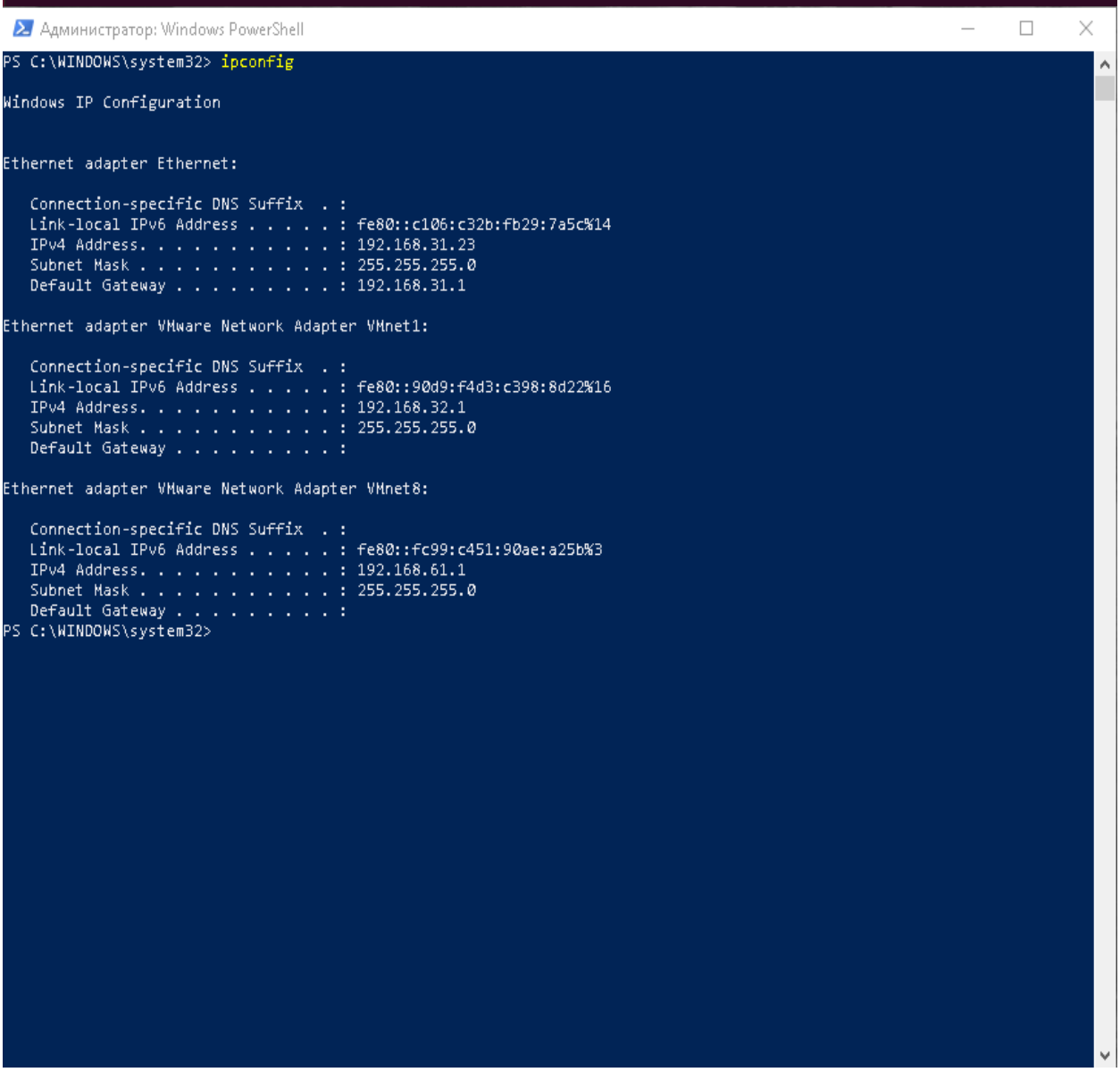
Summary: ARP Functionality

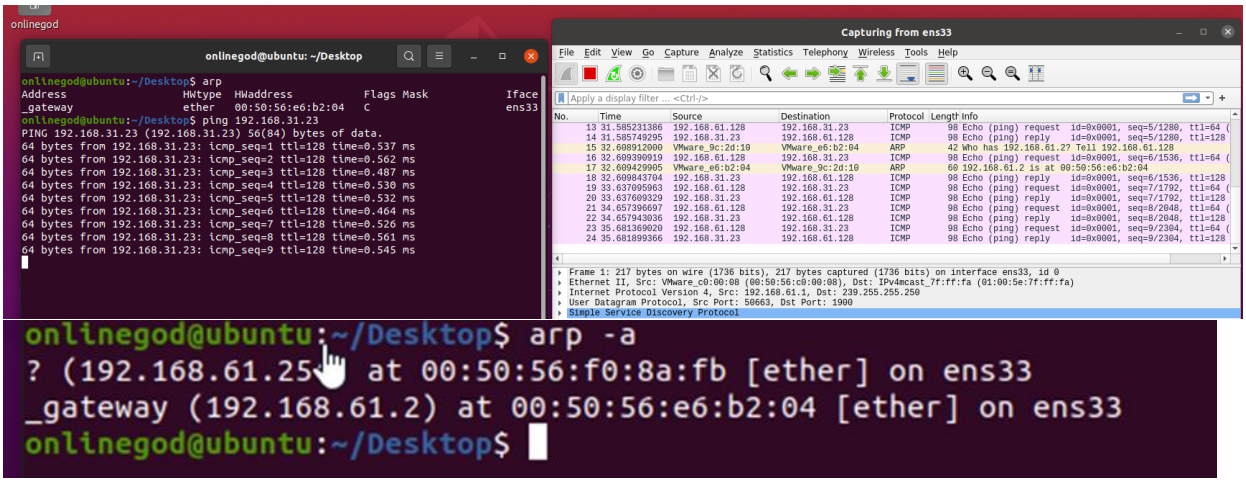
Test designed by Rustamov Arsen from IB-93 on 01.10.2022

Description: Verify that **ARP** protocol update arp table

Attachments:


onlinegod@ubuntu: ~/Desktop
onlinegod@ubuntu:~/Desktop$ arp
Address HWtype HWaddress Flags Mask Iface
_gateway ether 00:50:56:e6:b2:04 C ens33
onlinegod@ubuntu:~/Desktop$


Администратор: Windows PowerShell
PS C:\WINDOWS\system32> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c106:c32b:fb29:7a5c%14
IPv4 Address. . . . . : 192.168.31.23
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.31.1
Ethernet adapter VMware Network Adapter VMnet1:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::90d9:f4d3:c398:8d22%16
IPv4 Address. . . . . : 192.168.32.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
Ethernet adapter VMware Network Adapter VMnet8:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::fc99:c451:90ae:a25b%3
IPv4 Address. . . . . : 192.168.61.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
PS C:\WINDOWS\system32>



Version: **ARP** v1

Setup Description:

PC1-----ethernet1-----PC2

PC1: 192.168.61.128

PC2: 192.168.31.23

Steps (with ER):

1. Check arp table

   arp -a <for PC1>

   ER: verify that arp table (cache) has no information about PC2

2. Check IP address of PC2

   ipconfig <for PC2>

   ER: ip of PC2 is shown in PowerShell

3. Run Wireshark for ethernet1

4. Run ping from PC1 to PC2

   ER: ping is running

5. Verify that ARP request and ARP reply are present for IP and MAC of PC2 in Wireshark

6. Check arp table one more time

   arp -a <for PC1>

   ER: verify that arp table now has information about PC2

Висновок: Ми зрозуміли як працює ARP протокол, що таке MAC адреса, навчилися з'єднувати системи через Ethernet ,посилати пакети командою ping

та відстежувати трафік через утіліту Wireshark. Також написали ARP Test Case.