

Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Факультет інформатики та обчислювальної техніки  
Кафедра обчислювальної техніки

«Тестування та контроль якості (QA) вбудованих систем»

Лабораторна робота №1

**НАЛАШТУВАННЯ МЕРЕЖНОГО ОТОЧЕННЯ ТА ТЕСТУВАННЯ  
ПРОТОКОЛУ ARP**

Виконала:  
студентка групи ІО-91  
Тимошенко Діана

Київ  
2022 р.

**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 каналному рівні моделі OSI.

### Завдання на лабораторну роботу

Для налаштування мережного оточення вивчити теоретичні відомості та виконати кроки, що описані в розділі 1.2, врахувати рекомендації, що запропоновані в пункті 1.2.1.

#### QA завдання:

Згідно з визначеними варіантами описати Test-case.

Визначення варіанту: Останні дві цифри номеру залікової книжки розділити на три. Остача від ділення і буде номером варіанту.

$$28 \bmod 3 = 1$$

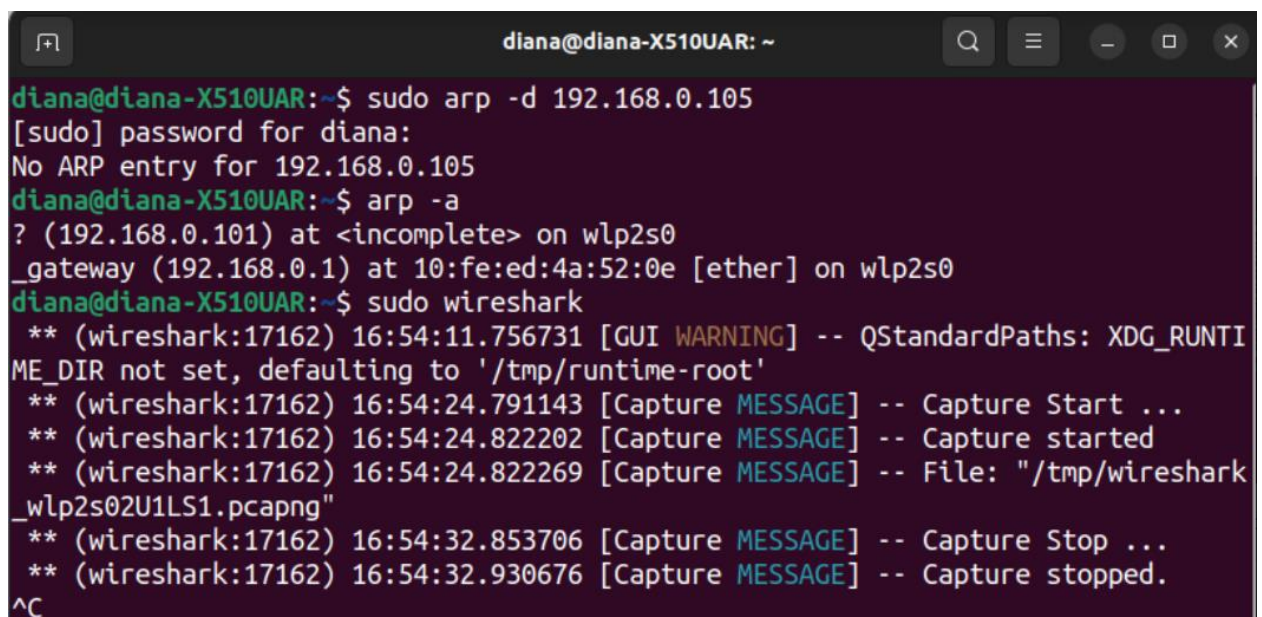
1) Переконатися в тому, що arp-таблиця оновлюється при отриманні arp-reply.

#### Посилання на репозиторій:

<https://github.com/diana-tym/qa-labs>

#### Виконання

- 1) Видаляємо з ARP-таблиці запис з IP-адресою, яку будемо пінгувати.
- 2) Перевіряємо таблицю.
- 3) Відкриваємо wireshark.



```
diana@diana-X510UAR: ~  
diana@diana-X510UAR:~$ sudo arp -d 192.168.0.105  
[sudo] password for diana:  
No ARP entry for 192.168.0.105  
diana@diana-X510UAR:~$ arp -a  
? (192.168.0.101) at <incomplete> on wlp2s0  
_gateway (192.168.0.1) at 10:fe:ed:4a:52:0e [ether] on wlp2s0  
diana@diana-X510UAR:~$ sudo wireshark  
** (wireshark:17162) 16:54:11.756731 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'  
** (wireshark:17162) 16:54:24.791143 [Capture MESSAGE] -- Capture Start ...  
** (wireshark:17162) 16:54:24.822202 [Capture MESSAGE] -- Capture started  
** (wireshark:17162) 16:54:24.822269 [Capture MESSAGE] -- File: "/tmp/wireshark_wlp2s02U1LS1.pcapng"  
** (wireshark:17162) 16:54:32.853706 [Capture MESSAGE] -- Capture Stop ...  
** (wireshark:17162) 16:54:32.930676 [Capture MESSAGE] -- Capture stopped.  
^C
```

- 4) Пінгуємо IP-адресу телефону.

```
diana@diana-X510UAR: ~  
diana@diana-X510UAR:~$ ping 192.168.0.105  
PING 192.168.0.105 (192.168.0.105) 56(84) bytes of data.  
64 bytes from 192.168.0.105: icmp_seq=1 ttl=64 time=246 ms  
64 bytes from 192.168.0.105: icmp_seq=2 ttl=64 time=69.3 ms  
64 bytes from 192.168.0.105: icmp_seq=3 ttl=64 time=93.3 ms  
64 bytes from 192.168.0.105: icmp_seq=4 ttl=64 time=209 ms  
64 bytes from 192.168.0.105: icmp_seq=5 ttl=64 time=37.9 ms  
^C  
--- 192.168.0.105 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4003ms  
rtt min/avg/max/mdev = 37.860/131.134/246.308/81.570 ms  
diana@diana-X510UAR:~$
```

## 5) Дивимось трафік у wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_73:b1	Broadcast	ARP	42	Who has 192.168.0.105? Tell 192.168.0.106
2	0.045492	96:83:c8:8c:30...	IntelCor_73:b1	ARP	42	192.168.0.105 is at 96:83:c8:8c:30:e5
3	0.045514	192.168.0.106	192.168.0.105	ICMP	98	Echo (ping) request id=0x0009, seq=1/256, ttl=64 (reply in 6)
4	0.238781	96:83:c8:8c:30...	Broadcast	ARP	42	Who has 192.168.0.106? Tell 192.168.0.105
5	0.238806	IntelCor_73:b1	96:83:c8:8c:30...	ARP	42	192.168.0.106 is at 14:4f:8a:73:b1:30
6	0.246264	192.168.0.105	192.168.0.106	ICMP	98	Echo (ping) reply id=0x0009, seq=1/256, ttl=64 (request in 3)
7	0.754092	149.154.167.51	192.168.0.106	SSL	171	Continuation Data
8	0.754162	192.168.0.106	149.154.167.51	TCP	66	50054 → 443 [ACK] Seq=1 Ack=106 Win=7523 Len=0 TSval=1528511192 TSecr
9	1.000685	192.168.0.106	192.168.0.105	ICMP	98	Echo (ping) request id=0x0009, seq=2/512, ttl=64 (reply in 10)
10	1.069971	192.168.0.105	192.168.0.106	ICMP	98	Echo (ping) reply id=0x0009, seq=2/512, ttl=64 (request in 9)
11	2.002456	192.168.0.106	192.168.0.105	ICMP	98	Echo (ping) request id=0x0009, seq=3/768, ttl=64 (reply in 12)
12	2.095684	192.168.0.105	192.168.0.106	ICMP	98	Echo (ping) reply id=0x0009, seq=3/768, ttl=64 (request in 11)
13	3.002858	192.168.0.106	192.168.0.105	ICMP	98	Echo (ping) request id=0x0009, seq=4/1024, ttl=64 (reply in 14)
14	3.211731	192.168.0.105	192.168.0.106	ICMP	98	Echo (ping) reply id=0x0009, seq=4/1024, ttl=64 (request in 13)
15	4.002789	192.168.0.106	192.168.0.105	ICMP	98	Echo (ping) request id=0x0009, seq=5/1280, ttl=64 (reply in 16)
16	4.040609	192.168.0.105	192.168.0.106	ICMP	98	Echo (ping) reply id=0x0009, seq=5/1280, ttl=64 (request in 15)
17	4.403877	192.168.0.106	149.154.167.51	SSL	443	Continuation Data
18	4.442732	149.154.167.51	192.168.0.106	TCP	68	443 → 50054 [ACK] Seq=106 Ack=378 Win=32768 Len=0 TSval=4254386030 TSe
19	4.443296	149.154.167.51	192.168.0.106	SSL	155	Continuation Data
20	4.443330	192.168.0.106	149.154.167.51	TCP	66	50054 → 443 [ACK] Seq=378 Ack=195 Win=7523 Len=0 TSval=1528514881 TSe

## Test case

Test ID: TC\_ARP\_1

Summary: Перевірити, що arp-таблиця оновлюється при отримати arp-reply

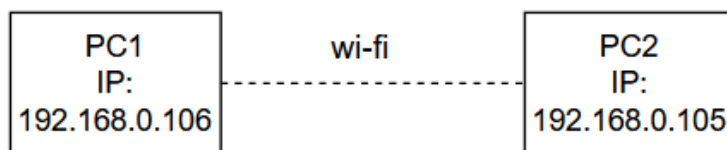
Attachments: capture – wireshark.png

ping – ping.png

arp – arp.png

Version: ARIPv1

Setup description:



Steps:

1. Видалити з arp-таблиці PC1 запис з IP-адресою PC2.

arp -d IP\_PC2

ER: в arp-таблиці немає запису з IP-адресою PC2

2. Відкрити wireshark для відповідного інтерфейсу.

sudo wireshark

3. Пропінгувати з PC1 PC2.

ping IP\_PC2

ER: з PC1 відправляються ехо-запити і з PC2 приходять ехо-відповіді.

4. Перевірити, що arp-таблиця оновилася.

arp -a

ER: в arp-таблиці з'явився новий запис з IP-адресою PC2.

## Висновок

В цій лабораторній роботі ми ознайомились з протоколом ICMP та ARP, командою ping, програмою wireshark. Оскільки, не було можливості з'єднати комп'ютери за допомогою Ethernet, завдання було виконано через Wi-Fi. Також як QA завдання був написаний test case на перевірку, що arp-таблиця оновлюється при отриманні arp-reply.