

Лабораторна робота №1

Основи комп'ютерних мереж

Виконав:

Студент 3 курсу ФТІ
групи ФІ-92
Поночевний Назар Юрійович
Версія тестової лабораторії: v1.0

Завдання:

Метою даної лабораторної роботи є отримання розуміння роботи базових мережніх протоколів канального та мережного рівня (Ethernet, ARP, ICMP, IP), отримання розуміння роботи атаки ARP-spoofing, а також отримання навичок роботи з розповсюдженими утилітами для аналізу і конфігурування у комп'ютерних мережах: ifconfig, ip, netstat, ping, tcpdump, wireshark.

- 1) Отримайте SSH доступ до машини client_pc1

```
Creating client_pc3 ... done
Creating ftp_server ... done
Creating ftilabs_comnetworks_wordpress_1 ... done
Creating ftilabs_comnetworks_https-portal_1 ... done

CURRENT INFRASTRUCTURE VERSION: v1.0
ubuntu@ip-172-31-95-189:~/ftilabs_comnetworks$ ssh -i ./assets/pc1_access root@127.0.0.1 -p 8022
The authenticity of host '[127.0.0.1]:8022 ([127.0.0.1]:8022)' can't be established.
ECDSA key fingerprint is SHA256:cAyxvGF3mN4kLb7+NIIEEE2vqcnhHfQN3+WqkJrt7mq4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[127.0.0.1]:8022' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.13.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@fd9504d8d51c:~#
```

- 2) Зберіть інформацію про налаштування мережі, адреси, маршрути тощо

```

root@fd9504d8d51c:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.16.238.10 netmask 255.255.255.0 broadcast 172.16.238.255
          ether ea:e7:b2:4e:88:58 txqueuelen 0 (Ethernet)
            RX packets 2613 bytes 11163970 (11.1 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 2765 bytes 493495 (493.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
          loop txqueuelen 1000 (Local Loopback)
            RX packets 243 bytes 32515 (32.5 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 243 bytes 32515 (32.5 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@fd9504d8d51c:~#

```

- 3) Перейдіть за SSH на вузол https-portal (172.11.15.71). Очистіть arp кеш (та упевнітесь в цьому) та спробуйте пінгувати вузли corp_gateway, corp1, corp2, http_server, ftp_server, проаналізуйте зміни в arp кеші та дайте оцінку отриманому результату

```

root@fd9504d8d51c:~# ssh root@172.11.15.71
The authenticity of host '172.11.15.71 (172.11.15.71)' can't be established.
ED25519 key fingerprint is SHA256:ESk7GQtBcjvBZ0nUNBUr/R0qdnqOZNcG2MEk7h3p95I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.11.15.71' (ED25519) to the list of known hosts.
root@172.11.15.71's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@55df5f83c1c8:~# arp -e
Address           HWtype  HWaddress          Flags Mask   Iface
corp1.ftilabs_comnetwor  ether   02:42:ac:0b:0f:11  C      eth0
corp2.ftilabs_comnetwor  ether   02:42:ac:0b:0f:21  C      eth0
ftilabs_comnetworks_wor  ether   02:42:0a:0a:0f:0f  C      eth1
dockerhost          ether   (incomplete)          C      eth0
root@55df5f83c1c8:~# ip -s neigh flush all

*** Round 1, deleting 3 entries ***

*** Round 2, deleting 1 entries ***

*** Round 3, deleting 1 entries ***

*** Round 4, deleting 1 entries ***

```

```

*** Round 4, deleting 1 entries ***

*** Round 5, deleting 1 entries ***

*** Round 6, deleting 1 entries ***

*** Round 7, deleting 1 entries ***

*** Round 8, deleting 1 entries ***

*** Round 9, deleting 1 entries ***

*** Round 10, deleting 1 entries ***
*** Flush not complete bailing out after 10 rounds
root@55df5f83c1c8:~# arp -e
Address          HWtype  HWaddress          Flags Mask   Iface
corp1.ftilabs_comnetwor ether   02:42:ac:0b:0f:11  C      eth0
corp2.ftilabs_comnetwor ether   02:42:ac:0b:0f:21  C      eth0
ftilabs_comnetworks_wor ether   02:42:0a:0a:0f:0f  C      eth1
dockerhost          (incomplete)
root@55df5f83c1c8:~#

```

```

root@55df5f83c1c8:~# ping -c 4 172.11.15.220
PING 172.11.15.220 (172.11.15.220): 56 data bytes
64 bytes from 172.11.15.220: icmp_seq=0 ttl=64 time=0.087 ms
64 bytes from 172.11.15.220: icmp_seq=1 ttl=64 time=0.068 ms
64 bytes from 172.11.15.220: icmp_seq=2 ttl=64 time=0.067 ms
64 bytes from 172.11.15.220: icmp_seq=3 ttl=64 time=0.068 ms
--- 172.11.15.220 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.067/0.073/0.087/0.000 ms
root@55df5f83c1c8:~# ping -c 4 172.11.15.53
PING 172.11.15.53 (172.11.15.53): 56 data bytes
64 bytes from 172.11.15.53: icmp_seq=0 ttl=64 time=0.117 ms
64 bytes from 172.11.15.53: icmp_seq=1 ttl=64 time=0.098 ms
64 bytes from 172.11.15.53: icmp_seq=2 ttl=64 time=0.075 ms
64 bytes from 172.11.15.53: icmp_seq=3 ttl=64 time=0.066 ms
--- 172.11.15.53 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.066/0.089/0.117/0.000 ms
root@55df5f83c1c8:~# ping -c 4 172.11.15.61
PING 172.11.15.61 (172.11.15.61): 56 data bytes
64 bytes from 172.11.15.61: icmp_seq=0 ttl=64 time=0.083 ms
64 bytes from 172.11.15.61: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 172.11.15.61: icmp_seq=2 ttl=64 time=0.099 ms
64 bytes from 172.11.15.61: icmp_seq=3 ttl=64 time=0.102 ms
--- 172.11.15.61 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.066/0.088/0.102/0.000 ms

```

```

root@55df5f83c1c8:~# ping -c 4 172.11.15.17
PING 172.11.15.17 (172.11.15.17): 56 data bytes
64 bytes from 172.11.15.17: icmp_seq=0 ttl=64 time=0.048 ms
64 bytes from 172.11.15.17: icmp_seq=1 ttl=64 time=0.062 ms
64 bytes from 172.11.15.17: icmp_seq=2 ttl=64 time=0.068 ms
64 bytes from 172.11.15.17: icmp_seq=3 ttl=64 time=0.074 ms
--- 172.11.15.17 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.048/0.063/0.074/0.000 ms
root@55df5f83c1c8:~# ping -c 4 172.11.15.33
PING 172.11.15.33 (172.11.15.33): 56 data bytes
64 bytes from 172.11.15.33: icmp_seq=0 ttl=64 time=0.052 ms
64 bytes from 172.11.15.33: icmp_seq=1 ttl=64 time=0.069 ms
64 bytes from 172.11.15.33: icmp_seq=2 ttl=64 time=0.064 ms
64 bytes from 172.11.15.33: icmp_seq=3 ttl=64 time=0.065 ms
--- 172.11.15.33 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.052/0.062/0.069/0.000 ms
root@55df5f83c1c8:#

```

```

root@55df5f83c1c8:~# arp -e
Address          HWtype  HWaddress          Flags Mask           Iface
corp1.ftilabs_comnetwor ether   02:42:ac:0b:0f:11  C      eth0
corp2.ftilabs_comnetwor ether   02:42:ac:0b:0f:21  C      eth0
ftp_server.ftilabs_comn ether   02:42:ac:0b:0f:35  C      eth0
ftilabs_comnetworks_wor ether   02:42:0a:0a:0f:0f  C      eth1
corp_gateway.ftilabs_co ether   02:42:ac:0b:0f:dc  C      eth0
http_server.ftilabs_com ether   02:42:ac:0b:0f:3d  C      eth0
dockerhost        ether   (incomplete)
root@55df5f83c1c8:~

```

- 4) Відкрийте дві SSH сесії на client_pc1. В одній з них запустіть tcpdump, а у іншій – очистіть arp кеш та спробуйте пінгувати сусідні машини client_pc2-client_pc4. Вивантажте дамп трафіку та проаналізуйте за допомогою wireshark. Відфільтруйте трафік за ICMP та ARP. Опишіть функціонування цих протоколів на прикладі перехоплених пакетів

Time	Source	Destination	Protocol	Length	Info
1 0. 0.000000	d6:db:84:e4:8d:90	Broadcast	ARP	42	Who has 172.16.238.30? Tell 172.16.238.10
2 0. 0.000024	172.16.238.10	172.16.238.30	ICMP	98	Echo (ping) request id=0x0060, seq=0/0, ttl=64 (no re)
3 1. 001143	172.16.238.10	172.16.238.30	ICMP	98	Echo (ping) request id=0x0060, seq=1/256, ttl=64 (no re)
4 2. 0.002382	172.16.238.10	172.16.238.30	ICMP	98	Echo (ping) request id=0x0060, seq=2/512, ttl=64 (no re)
5 3. 0.003074	172.16.238.10	172.16.238.30	ICMP	98	Echo (ping) request id=0x0060, seq=3/768, ttl=64 (no re)
6 5. 139370	d6:db:84:e4:8d:90	56:5c:a5:92:9b:35	ARP	42	172.16.238.10 is at d6:db:84:e4:8d:90
7 8. 9.000051	172.16.238.10	172.24.118.16	ICMP	98	Echo (ping) request id=0x0061, seq=0/0, ttl=64 (no re)
8 9. 9.001208	172.16.238.10	172.24.118.16	ICMP	98	Echo (ping) request id=0x0061, seq=1/256, ttl=64 (no re)
9 10. 9.002483	172.16.238.10	172.24.118.16	ICMP	98	Echo (ping) request id=0x0061, seq=2/512, ttl=64 (no re)
10 11. 9.003404	172.16.238.10	172.24.118.16	ICMP	98	Echo (ping) request id=0x0061, seq=3/768, ttl=64 (no re)
11 31. 518178	172.16.238.10	172.24.118.15	ICMP	98	Echo (ping) request id=0x0062, seq=0/0, ttl=64 (no re)
12 32. 519356	172.16.238.10	172.24.118.15	ICMP	98	Echo (ping) request id=0x0062, seq=1/256, ttl=64 (no re)
13 33. 520633	172.16.238.10	172.24.118.15	ICMP	98	Echo (ping) request id=0x0062, seq=2/512, ttl=64 (no re)
14 34. 521886	172.16.238.10	172.24.118.15	ICMP	98	Echo (ping) request id=0x0062, seq=3/768, ttl=64 (no re)

- 5) Відкрийте у дампі будь-який TCP пакет та проаналізуйте кожен рівень стеку TCP/IP: опишіть на прикладі перехопленого пакета, які поля містяться у заголовках кожного рівня, яке їх призначенння

102 4.106127	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=7502 Win=614 Len=0
103 4.106142	172.11.15.61	172.16.238.10	TCP	7306 80 → 53698 [PSH, ACK] Seq=7502 Ack=370 Win=506 Len=0
104 4.106147	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=14742 Win=727 Len=0
105 4.106171	172.11.15.61	172.16.238.10	TCP	10202 80 → 53698 [PSH, ACK] Seq=14742 Ack=370 Win=506
106 4.106175	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=24878 Win=886 Len=0
107 4.106181	172.11.15.61	172.16.238.10	TCP	4410 80 → 53698 [PSH, ACK] Seq=24878 Ack=370 Win=506
108 4.106183	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=29222 Win=954 Len=0
109 4.106191	172.11.15.61	172.16.238.10	TCP	14546 80 → 53698 [PSH, ACK] Seq=29222 Ack=370 Win=506
110 4.106194	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=43702 Win=1180 Len=0
111 4.106202	172.11.15.61	172.16.238.10	TCP	2962 80 → 53698 [PSH, ACK] Seq=43702 Ack=370 Win=506
112 4.106204	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=46598 Win=1225 Len=0
113 4.106209	172.11.15.61	172.16.238.10	TCP	24682 80 → 53698 [PSH, ACK] Seq=46598 Ack=370 Win=506
114 4.106214	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=71214 Win=1610 Len=0
115 4.106235	172.11.15.61	172.16.238.10	HTTP	188 HTTP/1.1 200 OK
116 4.106237	172.16.238.10	172.11.15.61	TCP	66 53698 → 80 [ACK] Seq=370 Ack=71336 Win=1610 Len=0
117 4.686606	172.11.15.61	172.16.238.10	TCP	66 80 → 53694 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0
118 4.728951	172.16.238.10	172.11.15.61	TCP	66 53694 → 80 [ACK] Seq=1 Ack=2 Win=524 Len=0 TSval
119 4.740465	52:c7:9b:a9:c9:96	e6:e9:1c:ce:9f:b0	ARP	42 172.16.238.22 is at 52:c7:9b:a9:c9:96

Frame 102: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 ▶ Ethernet II, Src: 52:c7:9b:a9:c9:96 (52:c7:9b:a9:c9:96), Dst: 02:42:ac:10:ee:16 (02:42:ac:10:ee:16)
 ▶ Internet Protocol Version 4, Src: 172.16.238.10, Dst: 172.11.15.61
 ▶ Transmission Control Protocol, Src Port: 53698, Dst Port: 80, Seq: 370, Ack: 7502, Len: 0
 Source Port: 53698
 Destination Port: 80
 [Stream index: 1]
 [TCP Segment Len: 0]
 Sequence number: 370 (relative sequence number)
 Sequence number (raw): 3824663226
 [Next sequence number: 370 (relative sequence number)]
 Acknowledgment number: 7502 (relative ack number)
 Acknowledgment number (raw): 4039807022
 1000 = Header Length: 32 bytes (8)
 ▶ Flags: 0x010 (ACK)

Бачимо відправлений Acknowledge-пакет (ACK) від 172.16.238.10:53698 (source) про прийняття пакета з 172.11.15.61:80 (destination)

- 6) Знову відкрийте дві сесії на client_pc1 і запустіть tcpdump. Одночасно, запустіть wireshark для перехоплення трафіку зі сторони хосту, на мостовому інтерфейсі з контейнером corg_gateway. У другій SSH сесії спробуйте дістатися до зовнішнього ресурсу (наприклад, через команду curl google.com). Поясніть роботу механізму NAT на прикладі порівняння двох дампів трафіків – зовнішнього і внутрішнього

Source	Destination	Protocol	Length	Info
92.168.0.110	52.97.174.66	TCP	66 47702 → 443 [ACK] Seq=2737 Ack=720 Win=49	
2.97.174.66	192.168.0.110	TLSv1.2	97 Application Data	
92.168.0.110	52.97.174.66	TCP	66 47702 → 443 [ACK] Seq=2737 Ack=751 Win=49	
Tp-LinkT_fb:4e:64	14:85:7f:ff:b4:14	ARP	42 Who has 192.168.0.110? Tell 192.168.0.1	
4:85:7f:ff:b4:14	Tp-LinkT_fb:4e:64	ARP	42 192.168.0.110 is at 14:85:7f:ff:b4:14	
5.174.127.31	192.168.0.110	TLSv1.2	98 Application Data	
92.168.0.110	35.174.127.31	TCP	66 47020 → 443 [ACK] Seq=416 Ack=358 Win=501	
e80::1c4b:2ec6:322...	ff02::1:fff1:5929	ICMPv6	86 Neighbor Solicitation for fe80::8d90:6e85	
92.168.0.110	52.97.174.66	TLSv1.2	2733 Application Data	
92.168.0.110	52.97.174.66	TLSv1.2	97 Application Data	
2.97.174.66	192.168.0.110	TCP	66 443 → 47702 [ACK] Seq=751 Ack=5404 Win=16	
2.97.174.66	192.168.0.110	TCP	66 443 → 47702 [ACK] Seq=751 Ack=5435 Win=16	
92.168.0.103	255.255.255.255	UDP	230 36461 → 6667 Len=188	
2.97.174.66	192.168.0.110	TLSv1.2	2532 Application Data	
92.168.0.110	52.97.174.66	TCP	66 47702 → 443 [ACK] Seq=5435 Ack=3217 Win=4	
2.97.174.66	192.168.0.110	TLSv1.2	97 Application Data	
92.168.0.110	52.97.174.66	TCP	66 47702 → 443 [ACK] Seq=5435 Ack=3248 Win=4	
e80::1c4b:2ec6:322...	ff02::1:fff1:5929	ICMPv6	86 Neighbor Solicitation for fe80::8d90:6e85	
e80::1c4b:2ec6:322...	ff02::1:fff1:5929	ICMPv6	86 Neighbor Solicitation for fe80::8d90:6e85	
92.168.0.105	192.168.0.255	UDP	77 58651 → 15600 Len=35	
92.168.0.110	185.4.64.197	TCP	66 [TCP Dup ACK 36#5] 41776 → 443 [ACK] Seq=85.4.64.197	
92.168.0.103	255.255.255.255	UDP	230 36461 → 6667 Len=188	

Бачимо зі скріншота з Wireshark для зовнішнього трафіку, що роутер шле ARP-запити для пошуку фізичної адреси того, кому буде повертати запити "зовні", тобто від google.com

Time	Source	Destination	Protocol	Length	Info	No.	Time	Source	Destination	Protocol	Length	Info
93.0 365449	172.16.238.18	172.11.15.61	TCP	66	33934 - 88 [ACK]	270	66.034484434	192.168.0.1	192.169.0.110	DNS	109	Standard query response
94.0 630508	172.11.15.220	172.16.238.19	SSH	142	Server: Encrypted	271	66.036691434	192.168.0.110	142.250.186.206	TCP	74	39164 - 80 [SYN]
95.0 631122	172.16.238.19	172.11.15.220	SSH	142	Client: Encrypted	272	66.04455972	52.97.174.66	192.168.0.110	TLSv1.2	185	Application Data
96.0 631157	172.11.15.220	172.16.238.19	TCP	66	22 - 57250 [ACK]	273	66.044697457	192.168.0.110	52.97.174.66	TCP	66	47762 - 443 [ACK]
97.0 668505	172.11.15.61	172.16.238.19	TCP	66	80 - 33932 [FIN]	274	66.054847481	192.250.186.206	192.168.0.110	TCP	74	88 - 39164 [SYN]
98.0 668432	172.16.238.18	142.250.186.206	TCP	74	39164 - 80 [SYN]	275	66.054996832	192.168.0.110	142.250.186.206	TCP	66	39164 - 80 [ACK]
99.0 782767	142.250.186.206	172.16.238.19	TCP	74	80 - 39164 [SYN]	276	66.055195282	192.168.0.110	142.250.186.206	HTTP	140	GET / HTTP/1.1
100.0 872752	172.16.238.18	142.250.186.206	HTTP	167	39164 - 80 [ACK]	277	66.057137396	192.168.0.110	142.250.186.206	TCP	66.00	39164 - 80 [ACK]
101.0 872753	172.16.238.18	142.250.186.206	HTTP	167	39164 - 80 [ACK]	278	66.057137396	192.168.0.110	142.250.186.206	HTTP	66.00	39164 - 80 [ACK]
102.0 872755	172.16.238.19	172.11.15.61	TCP	66	80 - 33932 [FIN]	279	66.0578476749	192.168.0.110	142.250.186.206	TCP	66.00	39164 - 80 [ACK]
103.0 8719032	142.250.186.206	172.16.238.18	TCP	66	80 - 33914 [ACK]	280	66.055212945	192.168.0.110	142.250.186.206	TCP	66	39164 - 80 [ACK]
104.0 8719032	142.250.186.206	172.16.238.19	HTTP	594	HTTP/1.1 301 Moved	281	66.078795728	192.168.0.110	142.250.186.206	TCP	66.00	88 - 39164 [FIN]
105.0 8962621	172.16.238.18	142.250.186.206	TCP	66	39164 - 80 [ACK]	282	66.0788654527	192.168.0.110	142.250.186.206	TCP	66	39164 - 80 [ACK]
106.0 9002966	172.16.238.19	142.250.186.206	TCP	66	39164 - 80 [FIN]	283	66.0696518705	192.168.0.1	224.0.0.1	IGMPv2	46	Membership Query
107.0 9063238	172.16.238.18	172.11.15.220	SSH	366	Client: Encrypted	284	66.072112085	f8e0: 1:4c:b:ec:32:32::	f8e0: 1::ffff:1:5929	ICMPv6	88	Neighbor Solicit
108.0 9033279	172.11.15.220	172.16.238.19	TCP	66	22 - 57250 [ACK]	285	61.783532359	192.168.0.102	224.0.0.1	IGMPv2	46	Membership Report
109.0 0056975	172.16.238.18	172.11.15.220	SSH	199	Client: Encrypted	286	61.79553205	f8e0: 1:4c:b:ec:32:32::	f8e0: 1::ffff:1:5929	ICMPv6	88	Neighbor Solicit
110.0 0056975	172.16.238.19	172.11.15.220	TCP	66	80 - 33932 [FIN]	287	61.79553205	192.168.0.102	224.0.0.1	IGMPv2	77	53932 - 80 [ACK]
111.0 9185777	142.250.186.206	172.16.238.19	TCP	66	80 - 33934 [FIN]	288	66.054005081	52.97.174.66	192.168.0.110	TLSv1.2	107	Application Data
112.0 9185777	172.16.238.19	142.250.186.206	TCP	66	39164 - 80 [ACK]	289	66.055475764	192.168.0.110	52.97.174.66	TCP	66	47762 - 443 [ACK]
113.0 891949	172.16.238.19	172.11.15.61	TCP	66	33932 - 80 [FIN]	290	66.17981667	f8e0: 1:4c:b:ec:32:32::	f8e0: 1::ffff:1:5929	ICMPv6	88	Neighbor Solicit
114.0 892017	172.11.15.61	172.16.238.19	TCP	66	80 - 33932 [FIN]	291	66.035784382	192.168.0.103	225.255.255.255	UDU	230	364631 - 6676 Len
115.0 892112	172.16.238.19	172.11.15.61	TCP	74	33933 - 80 [SYN]	292	65.849663429	192.168.0.110	194.44.229.242	TCP	54	[TCP Dup ACK 354]
116.0 892162	172.11.15.61	172.16.238.19	TCP	74	80 - 33933 [SYN]	293	66.067856263	194.44.229.242	194.168.0.110	TCP	54	[TCP Dup ACK 374]
117.0 892182	172.16.238.18	172.11.15.61	TCP	66	33933 - 80 [ACK]	294	66.30671614	f8e0: 1:4c:b:ec:32:32::	f8e0: 1::ffff:ba:8ie2	ICMPv6	88	Neighbor Solicit

Порівнюючи внутрішній (зліва) та зовнішній (справа) трафіки, бачимо, що source-адреса однаакова - 142.250.186.206 (google.com), проте destination-адреси різні (всередині це адреса pc_1, а зовні це локальна адреса хоста - 192.168.0.110).

Взагалі, NAT це такий "хак", коли під одною білою IPv4 адресою роутера, насправді може бути декілька окремих девайсів, які відправляють запити в мережу, а NAT розкриває пакет, вписує свою адресу і запам'ятовує що він замінив, щоб потім розкрити пакет відповіді, вписати туди справжнього адресата з локальної мережі та передати пакет далі. Таким чином, маскується справжня адреса відправника + якщо підмінити TTL, то можна маскувати навіть сам факт наявності роутера. Це призводить до економії IPv4 адрес, які вже закінчилися і збільшує безпеку внутрішніх девайсів локальної мережі.

- 7) На вузлі client_pc1 запустіть tcpdump та збирайте трафік впродовж 1-2 хвилин. Проведіть arp spoofing атаку на вузли client_pc2 client_pc3, ftp_server, під час кожної з них зберіть трафік впродовж 1- 2 хвилин. Порівняйте отримані дампи та надайте їм оцінку, поясніть, який результат дала атака в кожному випадку і чому саме такий

Time	Source	Destination	Protocol	Length	Info
191 48.968022	172.11.15.220	172.16.238.10	TCP	66 22	→ 57250 [ACK] Seq=77 Ack=241 Win=24555 Len=0 TSval=
192 48.968394	172.16.238.10	172.11.15.220	SSH	150	Client: Encrypted packet (len=84)
193 48.968431	172.11.15.220	172.16.238.10	TCP	66 22	→ 57250 [ACK] Seq=77 Ack=325 Win=24555 Len=0 TSval=
194 48.968681	172.16.238.10	172.11.15.220	SSH	190	Client: Encrypted packet (len=124)
195 48.968709	172.11.15.220	172.16.238.10	TCP	66 22	→ 57250 [ACK] Seq=77 Ack=449 Win=24555 Len=0 TSval=
196 49.000452	72:d6:79:f6:80:9d	Broadcast	ARP	42	Who has 172.16.238.30? Tell 172.16.238.10
197 49.000481	22:b3:b7:c4:96:2f	72:d6:79:f6:80:9d	ARP	42	172.16.238.30 is at 22:b3:b7:c4:96:2f
198 49.000485	172.16.238.10	172.16.238.30	UDP	42 42648	→ 67 Len=0
199 49.000526	172.16.238.30	172.16.238.10	ICMP	70	Destination unreachable (Port unreachable)
200 49.829411	172.16.238.10	172.11.15.61	TCP	66 36140	→ 80 [FIN, ACK] Seq=200 Ack=196 Win=64128 Len=0 TSval=
201 49.829464	172.11.15.61	172.16.238.10	TCP	66 80	→ 36140 [ACK] Seq=196 Ack=201 Win=65024 Len=0 TSval=
202 49.829545	172.16.238.10	172.11.15.61	TCP	74 36142	→ 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_Pkts=0 TSval=
203 49.829575	172.11.15.61	172.16.238.10	TCP	74 80	→ 36142 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_Pkts=0 TSval=
204 49.829585	172.16.238.10	172.11.15.61	TCP	66 36142	→ 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2988
205 49.829605	172.16.238.10	172.11.15.61	HTTP	256	HEAD /aesifft HTTP/1.1
206 49.829637	172.11.15.61	172.16.238.10	TCP	66 80	→ 36142 [ACK] Seq=1 Ack=191 Win=65024 Len=0 TSval=5400
207 49.829832	172.11.15.61	172.16.238.10	HTTP	260	HTTP/1.1 404 Not Found
208 49.829838	172.16.238.10	172.11.15.61	TCP	66 36142	→ 80 [ACK] Seq=191 Ack=195 Win=64128 Len=0 TSval=
209 50.001101	72:d6:79:f6:80:9d	22:b3:b7:c4:96:2f	ARP	42	172.11.15.53 is at 72:d6:79:f6:80:9d
210 50.358866	172.16.238.10	172.11.15.61	TCP	327 36138	→ 80 [PSH, ACK] Seq=4261 Ack=73125 Win=64128 Len=0 TSval=
211 50.358888	172.11.15.61	172.16.238.10	TCP	66 80	→ 36138 [ACK] Seq=73125 Ack=4522 Win=64128 Len=0 TSval=
212 50.358907	172.16.238.10	172.11.15.61	HTTP	1224	HEAD /common?page=1 HTTP/1.1 (application/x-www-form-urlencoded)
213 50.358915	172.11.15.61	172.16.238.10	TCP	66 80	→ 36138 [ACK] Seq=73125 Ack=5680 Win=64128 Len=0 TSval=
214 50.359076	172.11.15.61	172.16.238.10	HTTP	327	HTTP/1.1 200 OK
215 50.359080	172.16.238.10	172.11.15.61	TCP	66 36138	→ 80 [ACK] Seq=5680 Ack=73386 Win=64128 Len=0 TSval=
216 52.001244	72:d6:79:f6:80:9d	22:b3:b7:c4:96:2f	ARP	42	172.11.15.53 is at 72:d6:79:f6:80:9d
217 54.001501	72:d6:79:f6:80:9d	22:b3:b7:c4:96:2f	ARP	42	172.11.15.53 is at 72:d6:79:f6:80:9d
218 54.008426	22:b3:b7:c4:96:2f	72:d6:79:f6:80:9d	ARP	42	Who has 172.16.238.10? Tell 172.16.238.30
219 54.008434	72:d6:79:f6:80:9d	22:b3:b7:c4:96:2f	ARP	42	172.16.238.10 is at 72:d6:79:f6:80:9d

Неможливо провести arp spoofing атаку на pc_3 та ftp-server, бо pc_3 знаходитьться в іншій мережі. Тому утиліта arpspoof не може зробити arp-запит на 172.24.118.15 (pc_3)

```
root@fd9504d8d51c:~# arpspoof -i eth0 -t 172.24.118.15 172.11.15.53
arpspoof: couldn't arp for host 172.24.118.15
root@fd9504d8d51c:~# arp -e
Address          HWtype  HWaddress          Flags Mask      Iface
corp1.ftilabs_comnetwor  ether   02:42:ac:10:ee:16  C        eth0
root@fd9504d8d51c:~# ping -c 4 172.24.118.15
PING 172.24.118.15 (172.24.118.15): 56 data bytes
^C--- 172.24.118.15 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
root@fd9504d8d51c:~#
```