Sieci komputerowe I – laboratorium

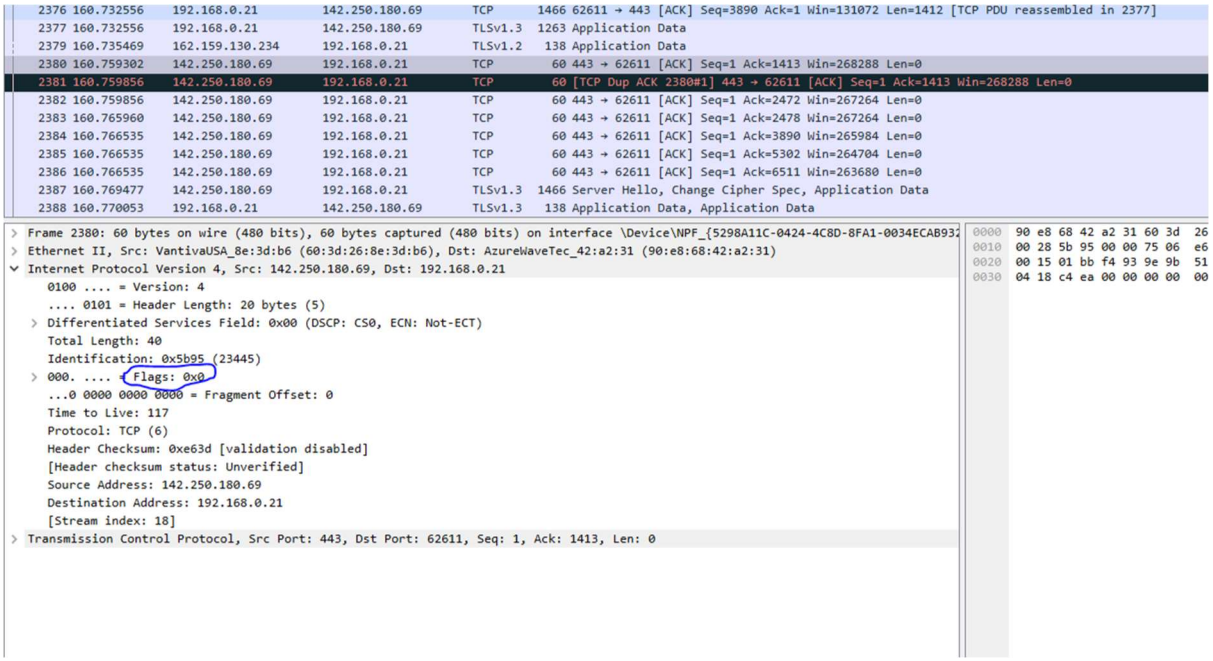
Wiktor Opieliński 157198 Stanowisko: K2

Informatyka, Niestacjonarnie semestr 4, Grupa 1

Warstwa międzysieciowa

Zadanie 1

1.Zaloguj ruch przy pomocy programu wireshark. Jakie zazwyczaj są ustawione flagi w pakietach?



Po przeanalizowaniu pakietów, zazwyczaj flagi są ustawione na 0x0.

- Bit zarezerwowany nie jest ustawiony.

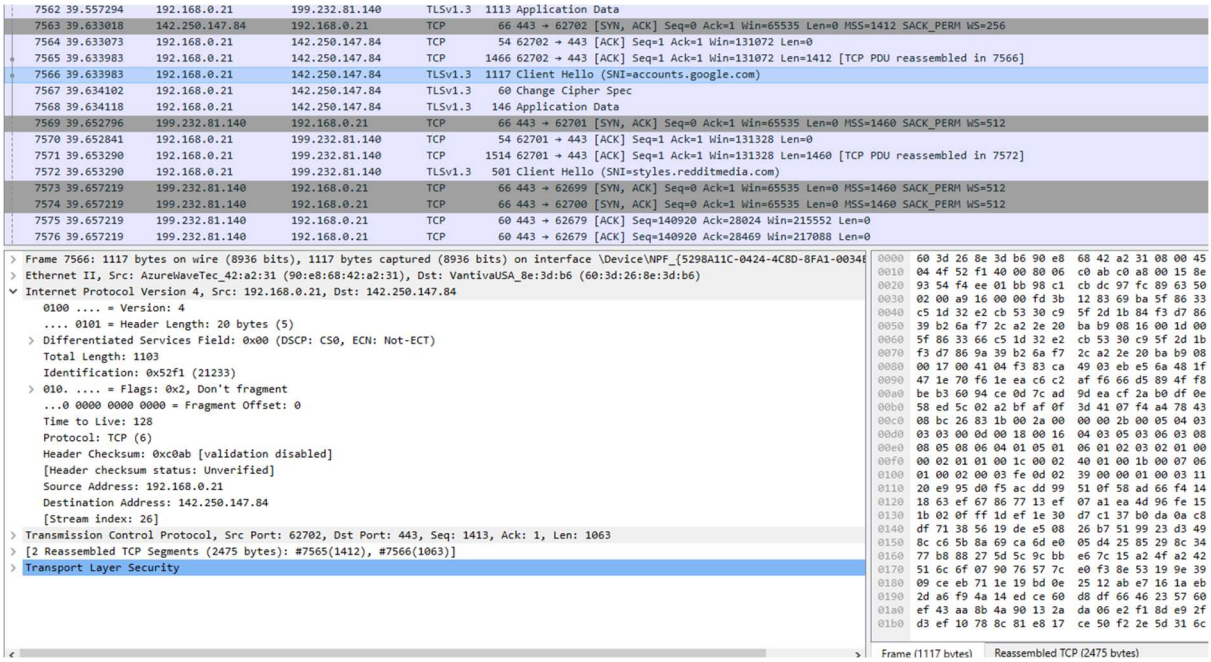
- Pakiet może być fragmentowany, jeśli zajdzie taka potrzeba

- Pakiet nie jest częścią większego pakietu, czyli nie został zfragmentowany

- Fragment Offset: 0 – wskazuje, że jest to pierwszy (i jedyny) fragment pakietu.

Jest to typowe zachowanie dla niewielkich pakietów, które mieszczą się w jednej ramce sieciowej.

2.Powtórz ćwiczenie otwierając w międzyczasie jakąś stronę internetową przy użyciu protokołu https.



Flaga ustawiona jest na 0x2, oznacza to, że tym razem w porównaniu z poprzednim ćwiczeniem pakiet nie może być fragmentowany. Jest to standardowe zachowanie dla współczesnych sieci, gdzie fragmentacja jest niepożądana z powodu bezpieczeństwa i wydajności.

Zamiast fragmentacji protokół TCP z ustawioną flagą 0x2 wykorzystuje Path MTU Discovery, czyli:

- Ustawia DF = 1 i wysyła coraz większe pakiety.

- Gdy pakiet jest za duży, router odrzuca go i odsyła błąd ICMP „Fragmentation needed”.

Dzięki temu nadawca dowiaduje się maksymalnego MTU na trasie i dopasowuje rozmiar.

HTTPS korzysta z tego mechanizmu, aby dobrać optymalny rozmiar segmentów bez fragmentacji.

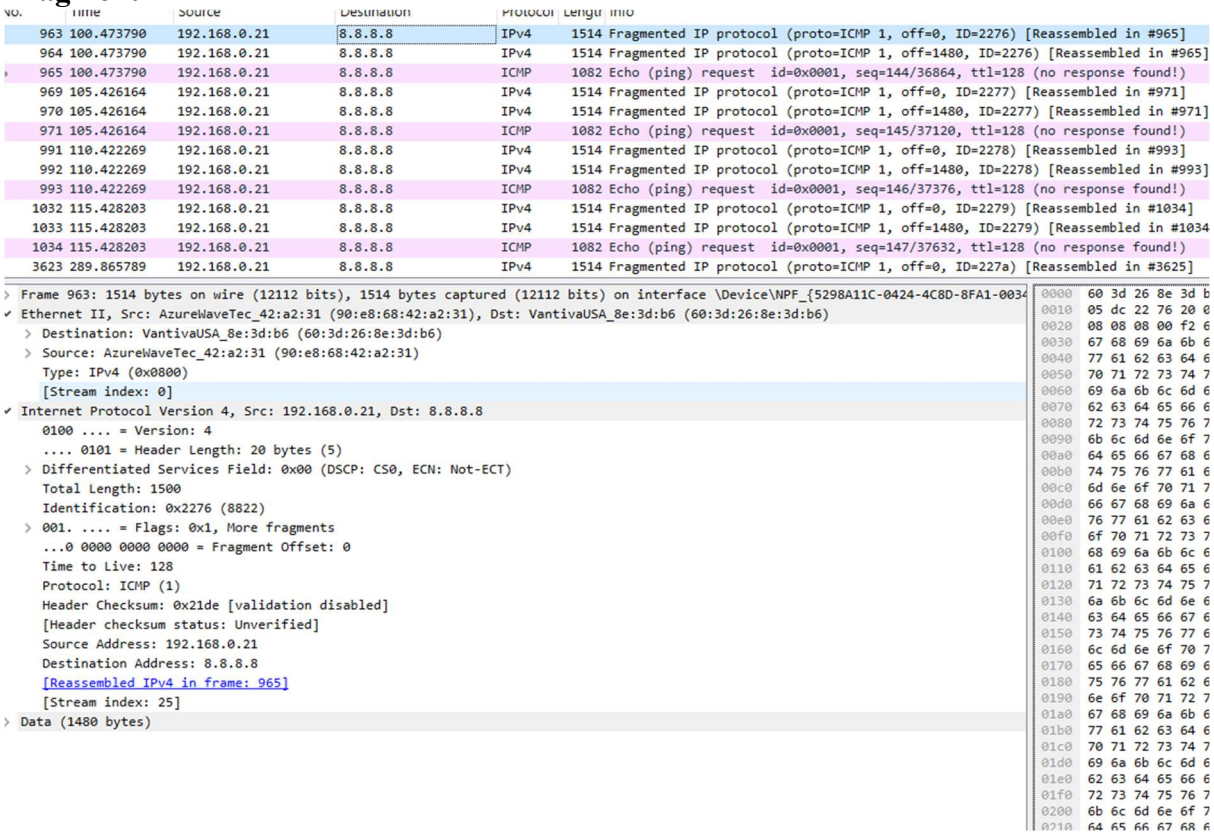
3.Powtórz ćwiczenie w międzyczasie wykonując polecenie ping -s 4000 na wybrany adres IP.

W celu przeanalizowania fragmentacji pakietów IP wykonano polecenie:

ping -s 4000 8.8.8.8

Polecenie to generuje pakiet ICMP o długości 4000 bajtów, który przekracza domyślną wartość MTU (1500 bajtów) dla sieci Ethernet. W efekcie system dzieli pakiet IP na mniejsze fragmenty, które są widoczne w przechwycie Wiresharka.

Fragment 1



Fragment Offset: 0

Flaga MF (More Fragments): 1

Długość (Total Length): 1500

Zawartość: początek nagłówka IP + fragment danych ICMP

Fragment 2

No.	Time	Source	Destination	Protocol	Length	Info
963	100.473790	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2276) [Reassembled in #965]
964	100.473790	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2276) [Reassembled in #96
965	100.473790	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=144/36864, ttl=128 (no response found!)
969	105.426164	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2277) [Reassembled in #971]
970	105.426164	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2277) [Reassembled in #97
971	105.426164	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=145/37120, ttl=128 (no response found!)
991	110.422269	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2278) [Reassembled in #993]
992	110.422269	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2278) [Reassembled in #99
993	110.422269	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (no response found!)
1032	115.428203	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2279) [Reassembled in #1034]
1033	115.428203	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=1480, ID=2279) [Reassembled in #10
1034	115.428203	192.168.0.21	8.8.8.8	ICMP	1082	Echo (ping) request id=0x0001, seq=147/37632, ttl=128 (no response found!)
3623	289.865789	192.168.0.21	8.8.8.8	IPv4	1514	Fragmented IP protocol (proto=ICMP 1, off=0, ID=227a) [Reassembled in #3625]

```
Frame 964: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034
Ethernet II, Src: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)
  > Destination: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)
  > Source: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 192.168.0.21, Dst: 8.8.8.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1500
    Identification: 0x2276 (8822)
  > 001. .... = Flags: 0x1, More fragments
    ...0 0000 1011 1001 = Fragment Offset: 1480
    Time to Live: 128
    Protocol: ICMP (1)
    Header Checksum: 0x2125 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.21
    Destination Address: 8.8.8.8
    [Reassembled IPv4 in frame: 965]
    [Stream index: 25]
Data (1480 bytes)
```

```
0000  60 3d 26 8e 3d
0010  05 dc 22 76 20
0020  08 08 61 62 63
0030  6f 70 71 72 73
0040  68 69 6a 6b 6c
0050  61 62 63 64 65
0060  71 72 73 74 75
0070  6a 6b 6c 6d 6e
0080  63 64 65 66 67
0090  73 74 75 76 77
00a0  6c 6d 6e 6f 70
00b0  65 66 67 68 69
00c0  75 76 77 61 62
00d0  6e 6f 70 71 72
00e0  67 68 69 6a 6b
00f0  77 61 62 63 64
0100  70 71 72 73 74
0110  69 6a 6b 6c 6d
0120  62 63 64 65 66
0130  72 73 74 75 76
0140  6b 6c 6d 6e 6f
0150  64 65 66 67 68
0160  74 75 76 77 61
0170  6d 6e 6f 70 71
0180  66 67 68 69 6a
0190  76 77 61 62 63
01a0  6f 70 71 72 73
01b0  68 69 6a 6b 6c
01c0  61 62 63 64 65
01d0  71 72 73 74 75
01e0  6a 6b 6c 6d 6e
01f0  63 64 65 66 67
0200  73 74 75 76 77
0210  6c 6d 6e 6f 70
0220  65 66 67 68 69
```

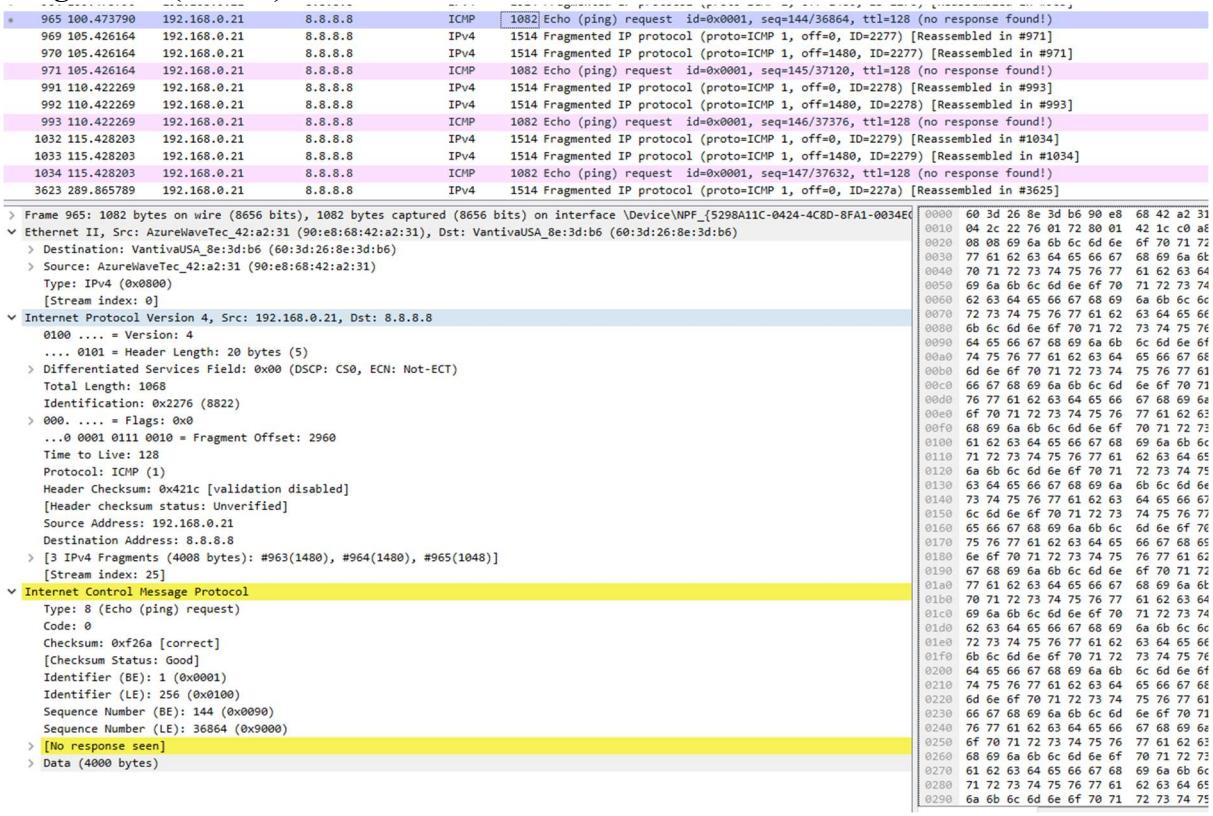
Fragment Offset: 1480

Flaga MF: 1

Długość: 1500

Zawiera kolejną porcję danych ICMP.

Fragment 3 (ostatni)



Fragment Offset: 2960

Flaga MF: 0 (czyli brak — Flags: 0x0)

Długość: 1048

Wireshark scala wszystkie fragmenty i pokazuje je jako pełen pakiet ICMP w ramce końcowej.

Zadanie 2

1. Jak działa program traceroute (ewentualnie skorzystaj z opcji -I lub -T)?

student@lab-sec-2:~> traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
 1 150.254.32.65 (150.254.32.65) 0.480 ms 0.503 ms 0.599 ms
 2 150.254.30.129 (150.254.30.129) 0.579 ms 0.676 ms 0.668 ms
 3 hellfire.put.poznan.pl (150.254.6.36) 1.352 ms 1.216 ms 1.208 ms
 4 PUTNET-BGP-P.put.poznan.pl (150.254.4.66) 2.116 ms 1.970 ms 2.493 ms
 5 237.14.119.185-rev.hti.pl (185.119.14.237) 1.954 ms 1.823 ms 1.691 ms
 6 088156078001.p2p.business.static.vectranet.pl (88.156.78.1) 7.906 ms 7.652 ms 7.480 ms
 7 172.17.64.10 (172.17.64.10) 9.951 ms 9.393 ms 9.437 ms

```
 8  172.17.64.10 (172.17.64.10)  8.852 ms  9.170 ms  9.161 ms
 9  162.158.100.12 (162.158.100.12)  7.899 ms  7.825 ms  8.149 ms
10  162.158.100.17 (162.158.100.17)  8.139 ms 162.158.100.7 (162.158.100.7)  12.670 ms
12.661 ms
11  one.one.one.one (1.1.1.1)  7.402 ms  7.403 ms  7.119 ms
```

Polecenie traceroute służy do śledzenia trasy pakietów IP od źródła (nasz komputer) do hosta docelowego (tu: 1.1.1.1).

Traceroute wykorzystuje mechanizm TTL (Time to Live) w nagłówku IP:

TTL to liczba skoków, jaką pakiet może wykonać.

Każdy router zmniejsza TTL o 1.

Gdy TTL = 0, router odrzuca pakiet i odsyła odpowiedź ICMP Time Exceeded.

Traceroute wysyła pakiety z TTL od 1 w górę, po 3 pakiety dla każdego skoku.

W ten sposób:

- Pakiety z TTL = 1 docierają tylko do pierwszego routera → dostajemy odpowiedź od niego.
- TTL = 2 → odpowiedź od drugiego routera.
- … i tak dalej, aż do hosta docelowego (który odpowiada inaczej – np. ICMP Echo Reply.

2. Zaloguj ruch przy pomocy programu wireshark i zbadaj nagłówki pakietów generowanych przez program traceroute.

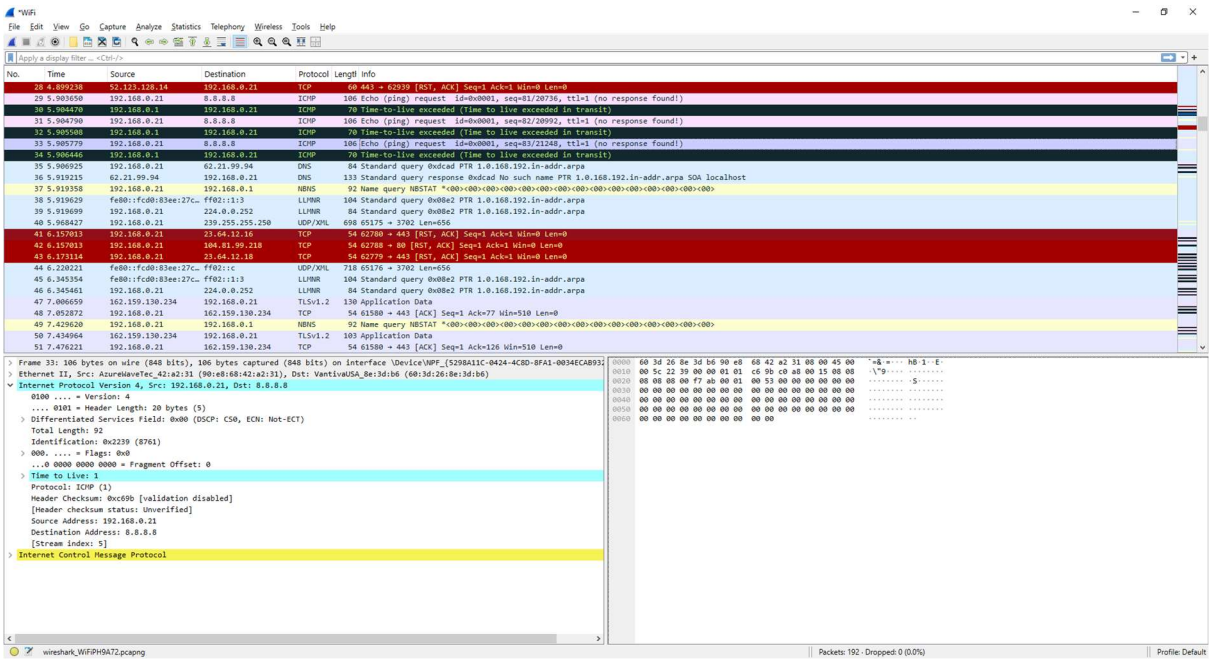
-Traceroute wysyła pakiety z kolejnymi wartościami TTL.

-Każdy router pośredni odrzuca pakiet z TTL = 0 i wysyła ICMP Time Exceeded.

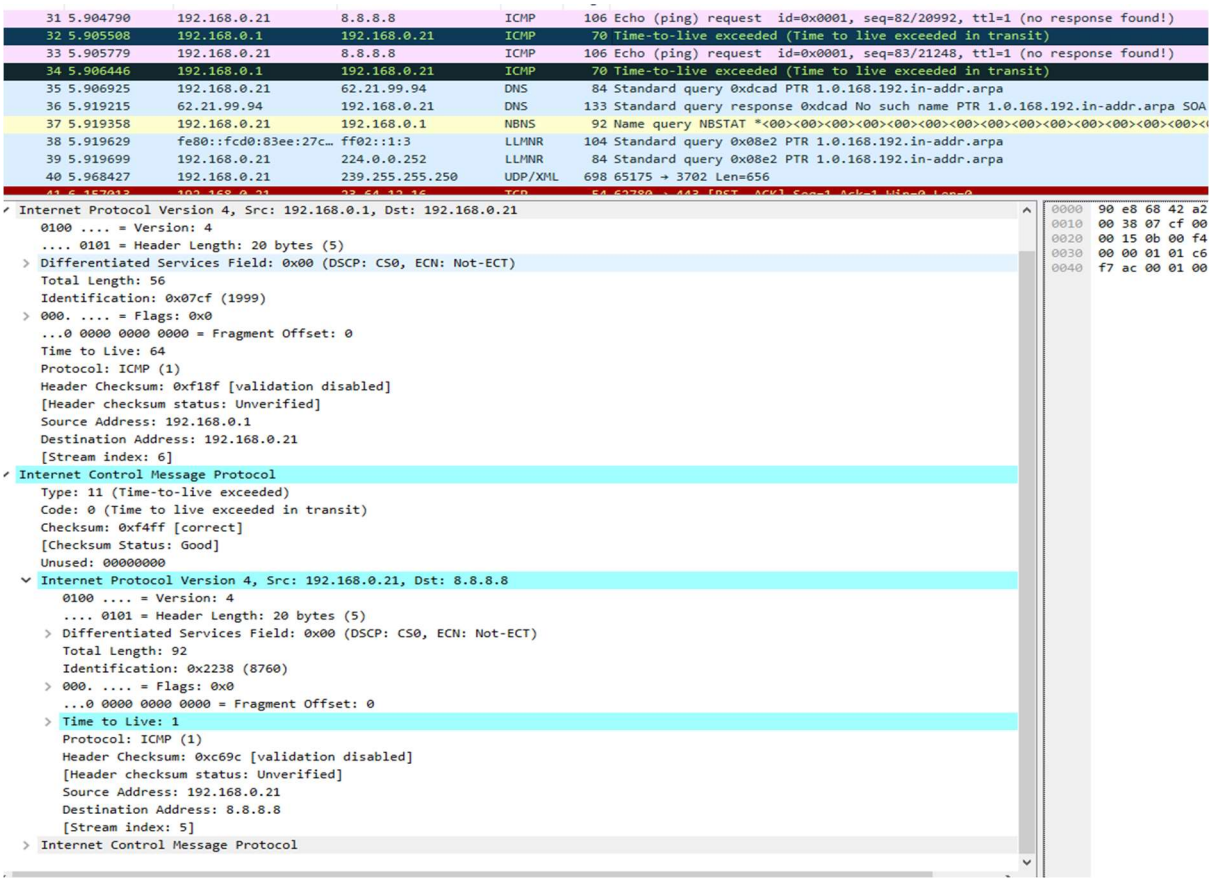
-Dzięki temu traceroute zbiera adresy wszystkich routerów na drodze.

-Ostateczny host może odpowiedzieć Echo Reply (przy ICMP) – tak jak w tym przypadku lub Unreachable (w przypadku UDP).

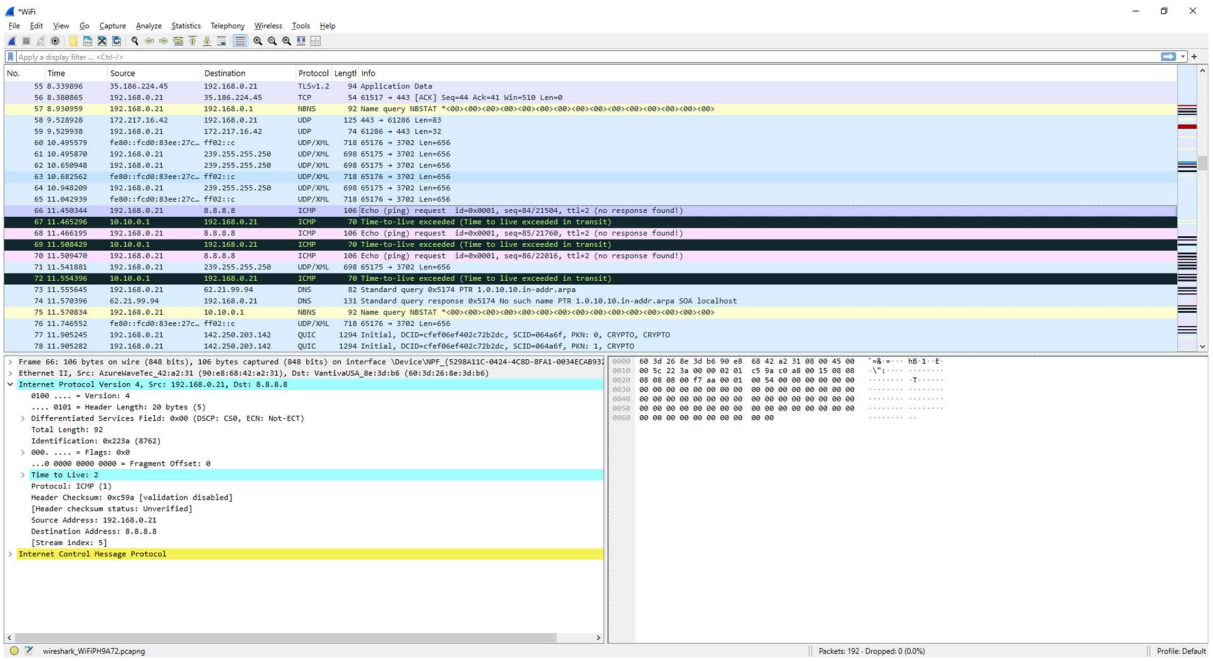
TTL = 1



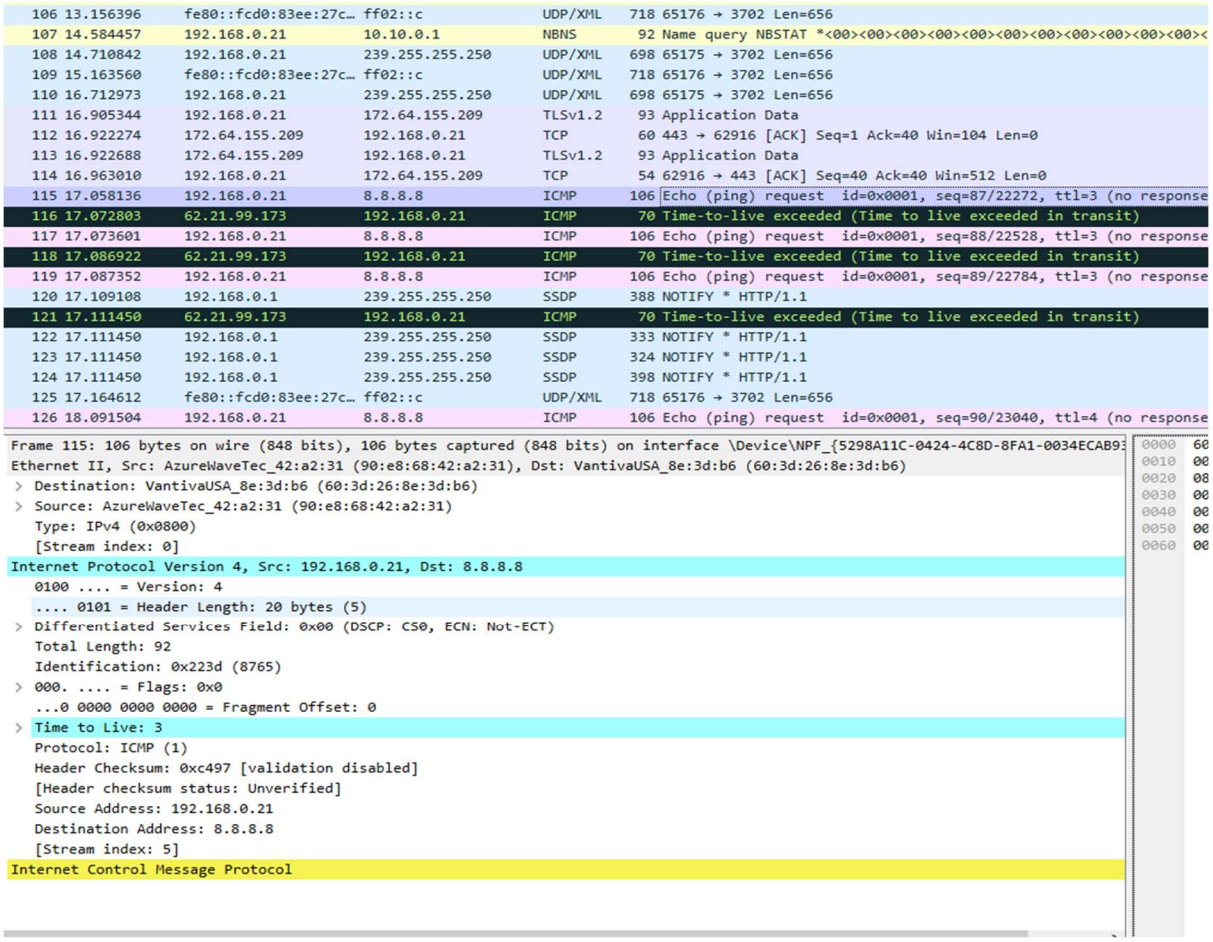
ICMP Time Exceeded



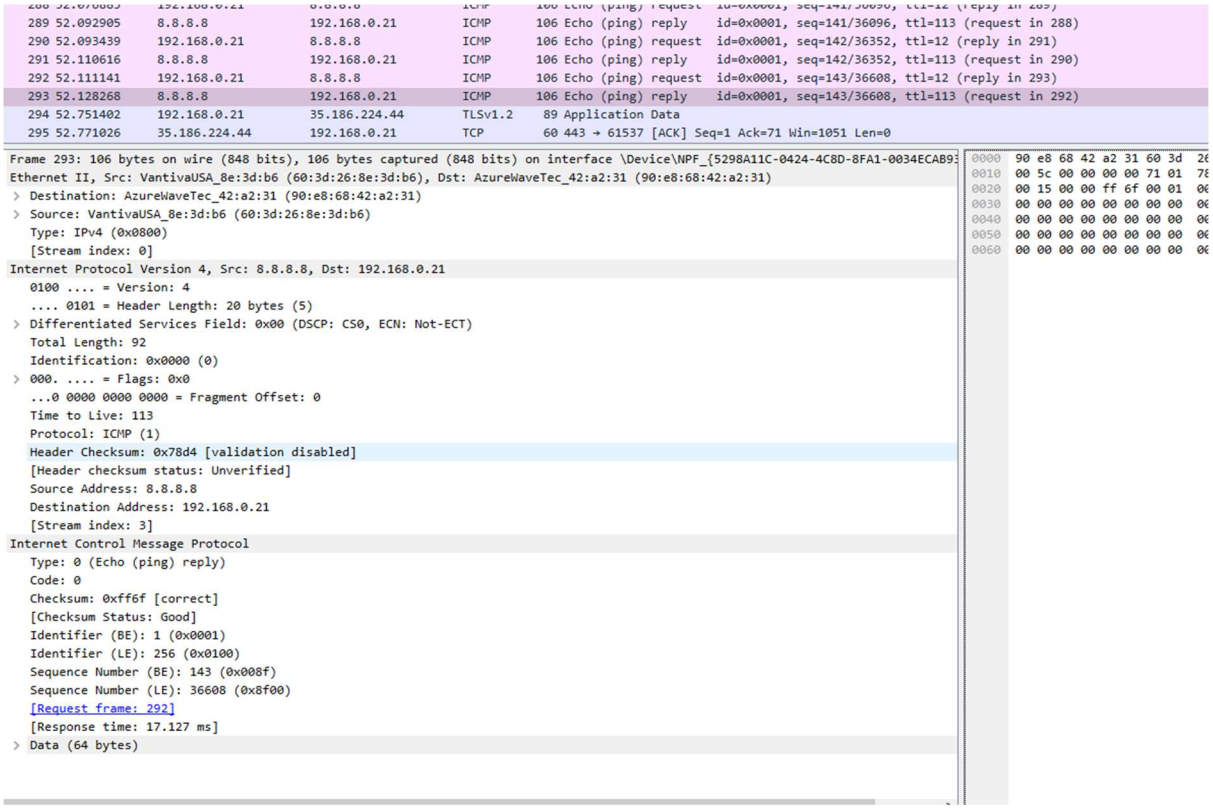
TTL = 2


"WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
55 8.339896 35.186.224.45 192.168.0.21 TLSv1.2 94 Application Data
56 8.380865 192.168.0.21 35.186.224.45 TCP 54 61517 → 443 [ACK] Seq=44 Ack=41 Win=510 Len=0
57 8.930959 192.168.0.21 192.168.0.1 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
58 9.528928 172.217.16.42 192.168.0.21 UDP 125 443 → 61286 Len=83
59 9.529938 192.168.0.21 172.217.16.42 UDP 74 61286 → 443 Len=32
60 10.495579 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
61 10.495870 192.168.0.21 239.255.255.250 UDP/XML 698 65175 → 3702 Len=656
62 10.650948 192.168.0.21 239.255.255.250 UDP/XML 698 65175 → 3702 Len=656
63 10.682562 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
64 10.948209 192.168.0.21 239.255.255.250 UDP/XML 698 65175 → 3702 Len=656
65 11.042939 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
66 11.450344 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=84/21504, ttl=2 (no response found!)
67 11.465296 10.10.0.1 192.168.0.21 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
68 11.466195 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=85/21760, ttl=2 (no response found!)
69 11.508429 10.10.0.1 192.168.0.21 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
70 11.509470 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=86/22016, ttl=2 (no response found!)
71 11.541881 192.168.0.21 239.255.255.250 UDP/XML 698 65175 → 3702 Len=656
72 11.554396 10.10.0.1 192.168.0.21 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
73 11.555645 192.168.0.21 62.21.99.94 DNS 82 Standard query 0x5174 PTR 1.0.10.10.in-addr.arpa
74 11.570396 62.21.99.94 192.168.0.21 DNS 131 Standard query response 0x5174 No such name PTR 1.0.10.10.in-addr.arpa SOA localhost
75 11.570834 192.168.0.21 10.10.0.1 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
76 11.746552 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
77 11.905245 192.168.0.21 142.250.203.142 QUIC 1294 Initial, DCID=cfef06ef402c72b2dc, SCID=064a6f, PKN: 0, CRYPTO, CRYPTO
78 11.905282 192.168.0.21 142.250.203.142 QUIC 1294 Initial, DCID=cfef06ef402c72b2dc, SCID=064a6f, PKN: 1, CRYPTO
Frame 66: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034ECAB93
Ethernet II, Src: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)
Internet Protocol Version 4, Src: 192.168.0.21, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x223a (8762)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 2
Protocol: ICMP (1)
Header Checksum: 0xc59a [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.21
Destination Address: 8.8.8.8
[Stream index: 5]
Internet Control Message Protocol
0000 60 3d 26 8e 3d b6 90 e8 68 42 a2 31 08 00 45 00
0010 00 5c 22 3a 00 00 02 01 c5 9a c0 a8 00 15 08 08
0020 08 08 08 00 f7 aa 00 01 00 54 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00
wireshark_WiFiPH9A72.pcapng
Packets: 192 · Dropped: 0 (0.0%)
Profile: Default

TTL = 3


106 13.156396 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
107 14.584457 192.168.0.21 10.10.0.1 NBNS 92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
108 14.710842 192.168.0.21 239.255.255.250 UDP/XML 698 65175 → 3702 Len=656
109 15.163560 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
110 16.712973 192.168.0.21 239.255.255.250 UDP/XML 698 65175 → 3702 Len=656
111 16.905344 192.168.0.21 172.64.155.209 TLSv1.2 93 Application Data
112 16.922274 172.64.155.209 192.168.0.21 TCP 60 443 → 62916 [ACK] Seq=1 Ack=40 Win=104 Len=0
113 16.922688 172.64.155.209 192.168.0.21 TLSv1.2 93 Application Data
114 16.963010 192.168.0.21 172.64.155.209 TCP 54 62916 → 443 [ACK] Seq=40 Ack=40 Win=512 Len=0
115 17.058136 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=87/22272, ttl=3 (no response
116 17.072803 62.21.99.173 192.168.0.21 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
117 17.073601 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=88/22528, ttl=3 (no response
118 17.086922 62.21.99.173 192.168.0.21 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
119 17.087352 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=89/22784, ttl=3 (no response
120 17.109108 192.168.0.1 239.255.255.250 SSDP 388 NOTIFY * HTTP/1.1
121 17.111450 62.21.99.173 192.168.0.21 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
122 17.111450 192.168.0.1 239.255.255.250 SSDP 333 NOTIFY * HTTP/1.1
123 17.111450 192.168.0.1 239.255.255.250 SSDP 324 NOTIFY * HTTP/1.1
124 17.111450 192.168.0.1 239.255.255.250 SSDP 398 NOTIFY * HTTP/1.1
125 17.164612 fe80::fcd0:83ee:27c… ff02::c UDP/XML 718 65176 → 3702 Len=656
126 18.091504 192.168.0.21 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=90/23040, ttl=4 (no response
Frame 115: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{5298A11C-0424-4C8D-8FA1-0034ECAB93
Ethernet II, Src: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31), Dst: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)
Destination: VantivaUSA_8e:3d:b6 (60:3d:26:8e:3d:b6)
Source: AzureWaveTec_42:a2:31 (90:e8:68:42:a2:31)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.0.21, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x223d (8765)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 3
Protocol: ICMP (1)
Header Checksum: 0xc497 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.0.21
Destination Address: 8.8.8.8
[Stream index: 5]
Internet Control Message Protocol
0000 60
0010 00
0020 08
0030 00
0040 00
0050 00
0060 00

Echo reply od celu



Zadanie 3

1.Podłącz swój komputer (poprzez port p4p1) do koncentratora (na zapleczu).

2. Skonfiguruj interfejs p4p1, tak by wszystkie komputery w rzędzie działały w jednej sieci (unikalne sieci między rzędami).

student@lab-sec-2:~> arp

Address	HWtype	HWaddress	Flags	Mask	Iface
192.168.1.4	ether	00:10:18:aa:a8:b8	C		p4p1
lab-sec-61.cs.put.pozna	ether	00:25:64:3b:c1:d0	C		br0
192.168.1.3	ether	00:10:18:b4:e3:7c	C		p4p1
lab-sec-1.cs.put.poznan	ether	e4:54:e8:a5:98:c6	C		br0
150.254.32.65	ether	00:04:96:9b:9b:f0	C		br0
192.168.1.1	ether	e4:54:e8:a5:98:c6	C		br0
lindev.cs.put.poznan.pl	ether	52:54:00:7d:97:53	C		br0
lab-sec-9.cs.put.poznan	ether	e4:54:e8:a5:98:f0	C		br0

3. Zbadaj jak zmienia się tablica ARP, gdy uruchamiasz program ping z argumentami będącymi adresami IP komputerów z Twojej sieci i adresami komputerów w innych rzędach (należących do innych sieci).

```
student@lab-sec-2:~> ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.503 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.544 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.542 ms
^C
--- 192.168.1.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.503/0.529/0.544/0.018 ms
student@lab-sec-2:~> arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.4              (incomplete)                              p4p1
lab-sec-61.cs.put.pozna  ether   00:25:64:3b:c1:d0   C                     br0
192.168.1.3              ether   00:10:18:b4:e3:7c   C                     p4p1
lab-sec-1.cs.put.poznan  ether   e4:54:e8:a5:98:c6   C                     br0
192.168.1.1              ether   00:10:18:aa:bd:7c   C                     p4p1
150.254.32.65            ether   00:04:96:9b:9b:f0   C                     br0
192.168.1.1              ether   e4:54:e8:a5:98:c6   C                     br0
lindev.cs.put.poznan.pl  ether   52:54:00:7d:97:53   C                     br0
lab-sec-9.cs.put.poznan  ether   e4:54:e8:a5:98:f0   C                     br0
```

Po nadaniu adresu IP, włączeniu interfejsu oraz wykonaniu poleceń ping do komputerów w sieci 192.168.1.0 (2 wiersz), do tablicy ARP zostają dodane powiązania adresów IP z odpowiadającymi im adresami MAC.

Komputery o adresach 192.168.1.1 oraz 192.168.1.3 zostały uwzględnione w poniższej tablicy, natomiast komputer o adresie 192.168.1.4 nie odpowiedział poprawnie – wpis ARP pozostał w stanie incomplete, co może oznaczać, że komputer jest wyłączony, nieosiągalny lub interfejs sieciowy nie działa.