Warstwa sieciowa

Sprawozdanie nr 4 z przedmiotu Sieci Komputerowe

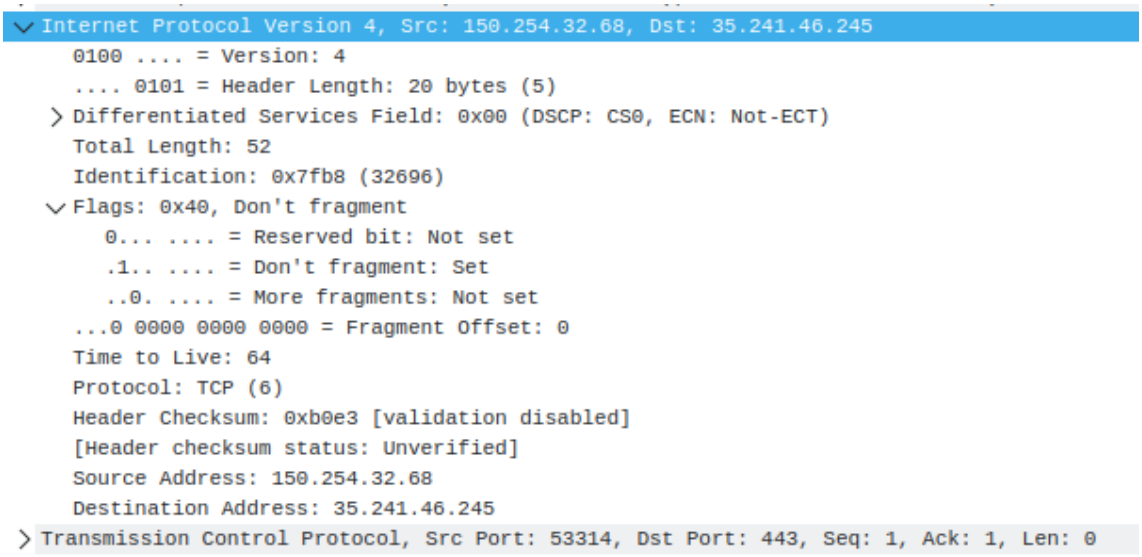
Maciej Kaszkowiak, 151856, zadania wykonane 13 maja 2023

Spis treści

1 Zadanie 1

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

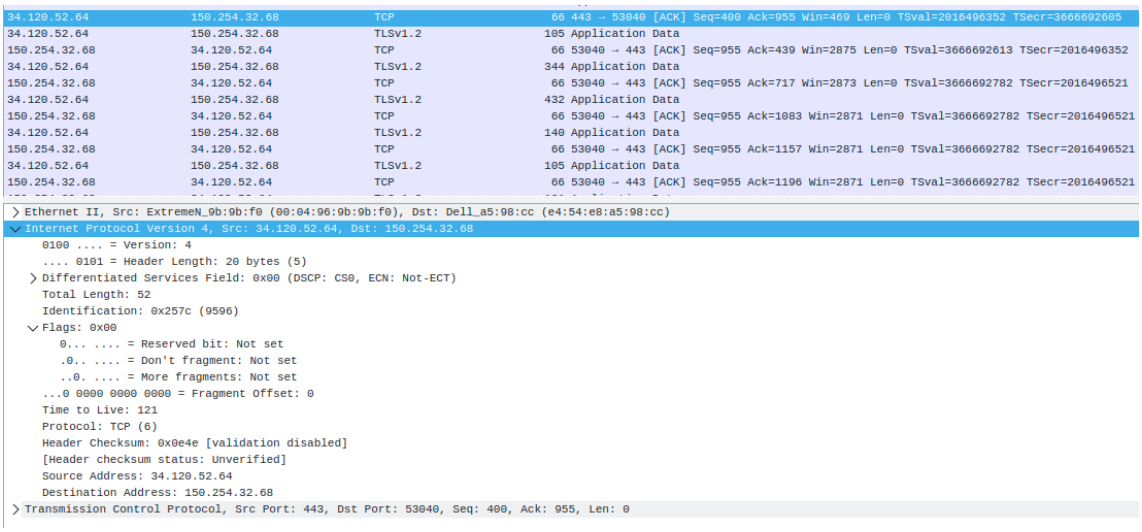
Możemy zaobserwować 2 flagi w pakietach: "Don't fragment"oraz "More fragments".



Rysunek 1: Flagi w pakietach

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

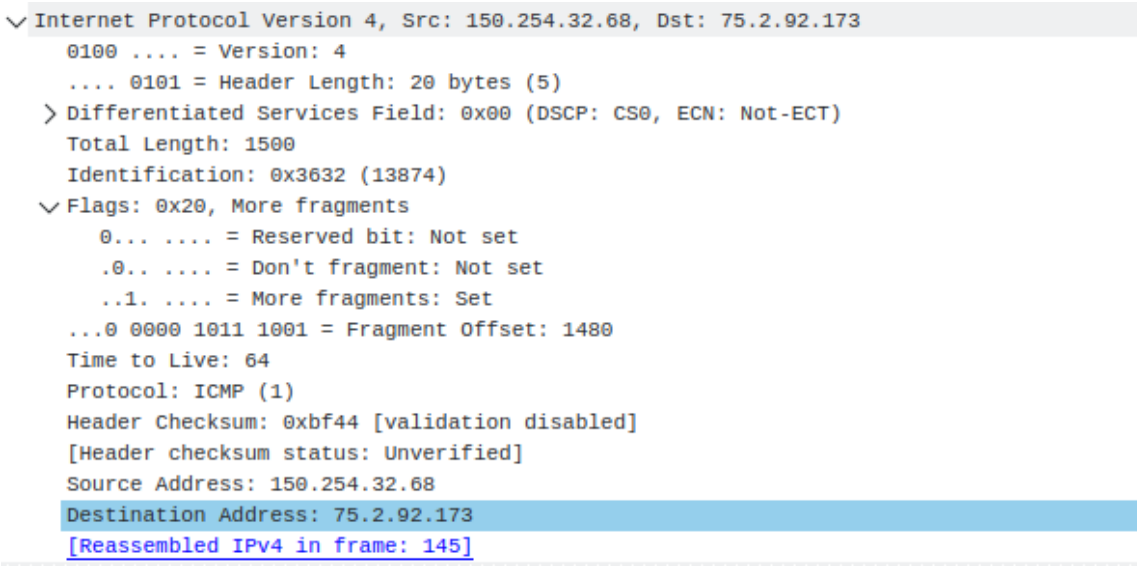
Możemy zauważyć, że flaga Don't fragment w pakiecie została wyłączona.



Rysunek 2: Flagi pozwalające na fragmentację pakietu

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

Możemy zauważyć, że flaga Don't fragment w pakiecie jest wyłączona, a flaga More fragments w niektórych pakietach jest aktywna.

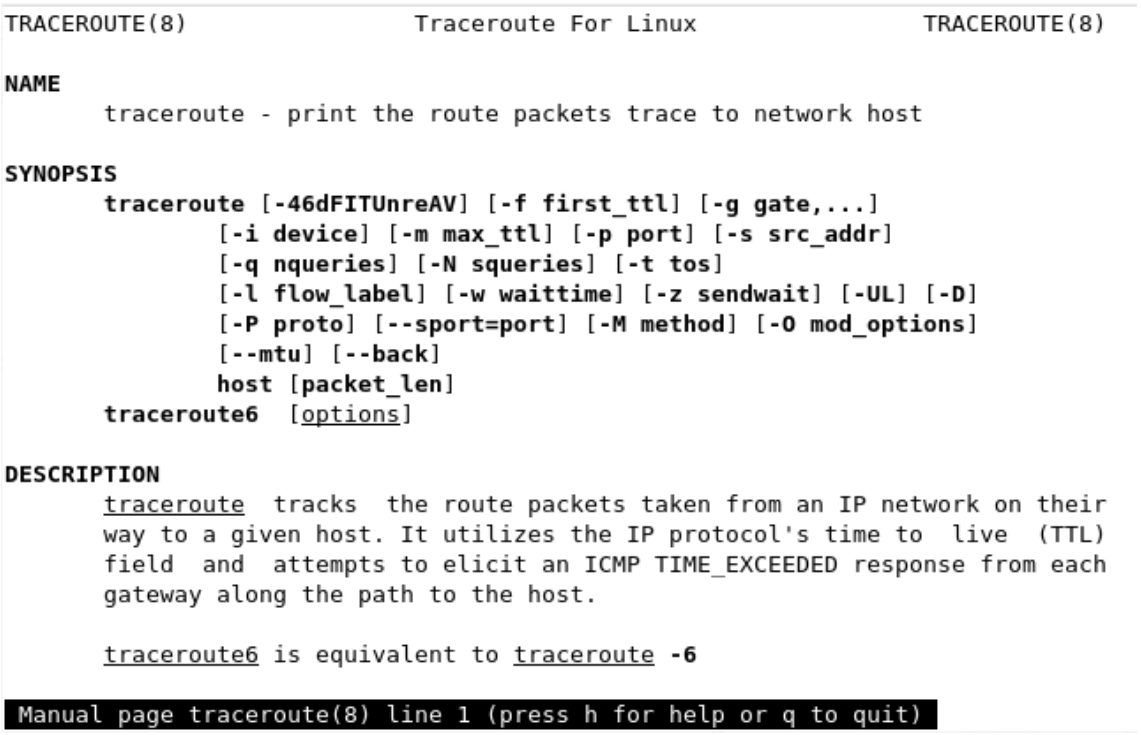


Rysunek 3: Flagi w pofragmentowanym pakiecie

2 Zadanie 2

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

Program traceroute opiera się na mechaniźmie TTL w celu wyznaczenia poszczególnych węzłów na ścieżce pakietu wiodącego do wskazanego przez nas adresu IP. Program nasłuchuje na odpowiedzi ICMP informujące o porzuceniu pakietu ze względu na wyzerowanie jego wartości TTL.



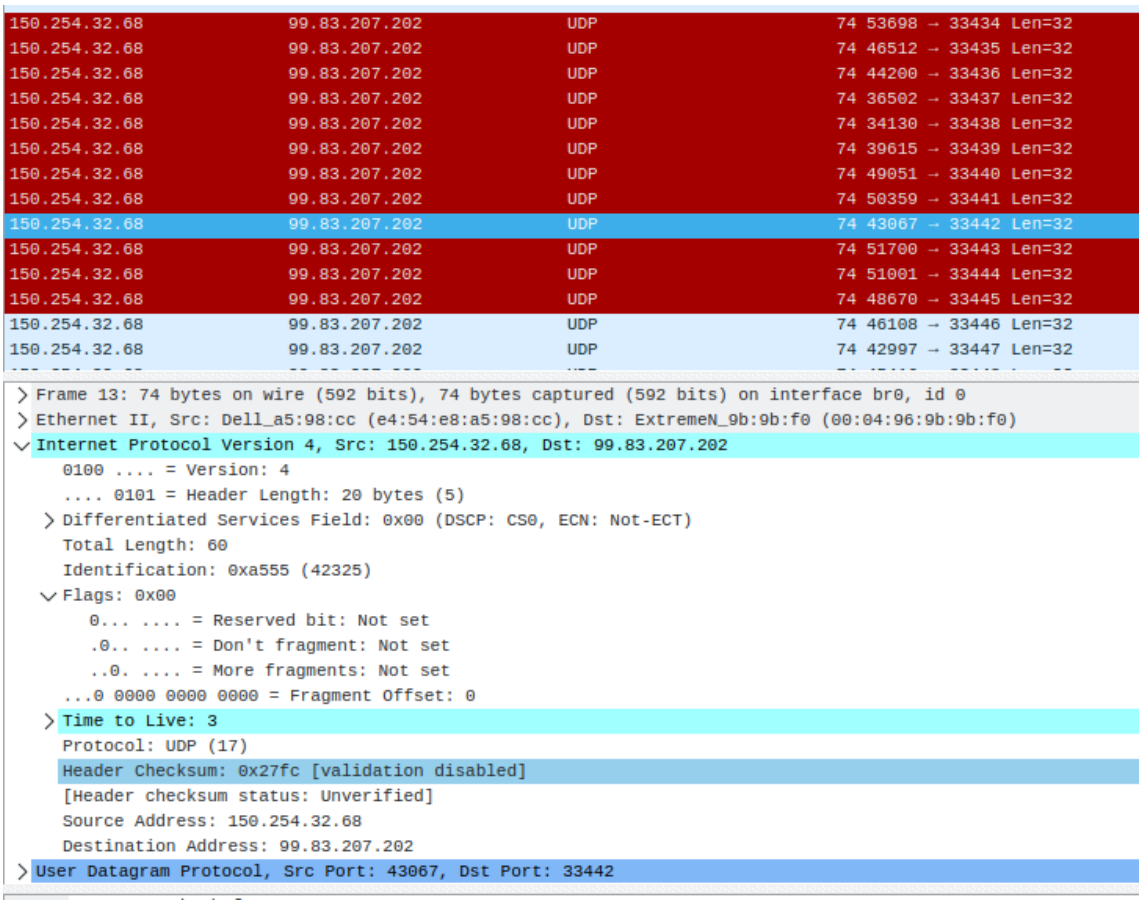
Rysunek 4: Manpages programu traceroute

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

```
student@lab-sec-3:~> traceroute onet.pl
traceroute to onet.pl (99.83.207.202), 30 hops max, 60 byte packets
 1  150.254.32.65 (150.254.32.65)  1.528 ms  1.585 ms  1.681 ms
 2  150.254.30.129 (150.254.30.129)  1.044 ms  1.263 ms  1.501 ms
 3  * * *
```

Rysunek 5: Wykonana komenda

Program generuje pakiety UDP z rosnącymi wartościami TTL, począwszy od TTL = 1. W odpowiedzi otrzymywane są pakiety ICMP informujące o porzuceniu pakietu.



Rysunek 6: Nagłówki pakietów generowanych przez program traceroute

3 Zadanie 3

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

Podłączyłem swój komputer poprzez port o numerze 99 i interfejs p4p1.

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

Połączenie działa:

```
lab-sec-3:/homex/student # ip addr add 192.168.1.3/24 dev p4p1
lab-sec-3:/homex/student # ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.634 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.704 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.496 ms
```

Rysunek 7: Wykonana komenda

3.3 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).

Możemy zaobserwować, ze tablica ARP uzupełnia się po wykonaniu pingu do komputera w naszej sieci.

```
lab-sec-3:/homex/student # arp -d 192.168.1.2
lab-sec-3:/homex/student # arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
150.254.32.65            ether   00:04:96:9b:9b:f0   C                     br0
150.254.32.120           ether   52:54:00:7d:97:53   C                     br0
192.168.1.1              ether   e4:54:e8:a5:98:c6   C                     br0
192.168.1.1                      (incomplete)                              p4p1
150.254.32.126           ether   00:25:64:3b:c1:d0   C                     br0
lab-sec-3:/homex/student # ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.774 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.774/1.104/1.435/0.330 ms
lab-sec-3:/homex/student # arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
150.254.32.65            ether   00:04:96:9b:9b:f0   C                     br0
192.168.1.2              ether   00:10:18:b4:e0:24   C                     p4p1
150.254.32.120           ether   52:54:00:7d:97:53   C                     br0
192.168.1.1              ether   e4:54:e8:a5:98:c6   C                     br0
192.168.1.1                      (incomplete)                              p4p1
150.254.32.126           ether   00:25:64:3b:c1:d0   C                     br0
```

Rysunek 8: Wykonana komenda

Komputery w innych rzędach są nieosiągalne, przez co tablica ARP się nie uzupełnia - nie znamy adresów MAC nieosiągalnych węzłów.

```
lab-sec-3:/homex/student # ping 192.168.5.14
PING 192.168.5.14 (192.168.5.14) 56(84) bytes of data.
From 150.254.4.66 icmp_seq=6 Destination Net Unreachable
^C
--- 192.168.5.14 ping statistics ---
9 packets transmitted, 0 received, +1 errors, 100% packet loss, time 8168ms

lab-sec-3:/homex/student # ping 192.168.5.15
PING 192.168.5.15 (192.168.5.15) 56(84) bytes of data.
From 150.254.4.66 icmp_seq=6 Destination Net Unreachable
From 150.254.4.66 icmp_seq=7 Destination Net Unreachable
^C
--- 192.168.5.15 ping statistics ---
7 packets transmitted, 0 received, +2 errors, 100% packet loss, time 6129ms

lab-sec-3:/homex/student # arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
150.254.32.65            ether   00:04:96:9b:9b:f0   C                     br0
192.168.1.2              ether   00:10:18:b4:e0:24   C                     p4p1
150.254.32.120           ether   52:54:00:7d:97:53   C                     br0
192.168.1.1              ether   e4:54:e8:a5:98:c6   C                     br0
192.168.1.1              ether   00:10:18:aa:bd:7c   C                     p4p1
150.254.32.126           ether   00:25:64:3b:c1:d0   C                     br0
```

Rysunek 9: Wykonana komenda

Zadanie 4 nie zostało wykonane zgodnie z poleceniem prowadzącego.