

# Technologie Sieciowe

## Lista 1

Autor: Jakub Jaśków

Data: 14.03.2023

### Treść listy:

1. Przetestuj działanie programów:
  - A) Ping: Sprawdź za jego pomocą, ile jest węzłów na trasie do (i od) wybranego, odległego geograficznie, serwera. Uwaga: trasy tam i z powrotem mogą być różne. Zbadaj jaki wpływ ma na to wielkość pakietu. Zbadaj jak wielkość pakietu wpływa na obserwowane czasy propagacji. Zbadaj jaki wpływ na powyższe ma konieczność fragmentacji pakietów. Jaki największy niefragmentowany pakiet uda się przesłać. Przeanalizuj te same zagadnienia dla krótkich tras (do serwerów bliskich geograficznie). Określ "średnicę" Internetu (najdłuższą ścieżkę, którą uda się wyszukać). Czy potrafisz wyszukać trasy przebiegające przez sieci wirtualne (zdalne platformy "cloud computing"). Ile węzłów mają ścieżki w tym przypadku.
  - B) Traceroute,
  - C) WireShark.
2. Napisz sprawozdanie zawierające: opis programów, wywołania dla powyższych zagadnień z analizą wyników, wnioski dotyczące przydatności tych programów.

### Opisy programów:

Ping - Packet Internet Groper jest narzędziem diagnostycznym, który pozwala na sprawdzenie łączności pomiędzy dwoma urządzeniami. Polecenie Ping wysyła pakiet danych do urządzenia docelowego, który powinien zostać zwrócony, w ten sposób można określić czy połączenie pomiędzy dwoma urządzeniami istnieje. Dodatkowo otrzymujemy informację jak długo zajęło pakietowi danych przebycie drogi od naszego komputera do serwera i z powrotem.

### Przykład użycia:

```
mango@T14:~$ ping -c 5 google.com
PING google.com(waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e)) 56 data bytes
64 bytes from waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e): icmp_seq=1 ttl=116 time=15.6 ms
64 bytes from waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e): icmp_seq=2 ttl=116 time=18.2 ms
64 bytes from waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e): icmp_seq=3 ttl=116 time=18.5 ms
64 bytes from waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e): icmp_seq=4 ttl=116 time=15.9 ms
64 bytes from waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e): icmp_seq=5 ttl=116 time=27.8 ms

--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 15.610/19.187/27.782/4.449 ms
```

W powyższym przykładzie pomyślnie wysłaliśmy oraz otrzymaliśmy 5 64 bitowych pakietów (56 + 8-nagłówek). Otrzymaliśmy informację dotyczące adresu IP domeny. Przy każdym wysłanym pakiecie PING informuje nas o:

- Rozmiarze pakietu
- Kolejności przyjscia (icmp seq)
- Pozostałym czasie życia (ttl)
- Czasie, który upłynął od wysłania pakietu do jego otrzymania

Jeżeli pakiet nie dotarłby do celu zostaniemy o tym poinformowani wiadomością na dole ekranu.

```
mango@T14:~$ ping -c 3 -t 2 google.com
PING google.com(waw02s18-in-x0e.1e100.net (2a00:1450:401b:808::200e)) 56 data bytes
From 2a01:1000::66c (2a01:1000::66c) icmp_seq=1 Time exceeded: Hop limit
From 2a01:1000::66c (2a01:1000::66c) icmp_seq=2 Time exceeded: Hop limit
From 2a01:1000::66c (2a01:1000::66c) icmp_seq=3 Time exceeded: Hop limit

--- google.com ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2004ms
```

Podstawowe opcje:

- c-ilość wysłanych pakietów
- i-ustal interwał wysyłania pakietów (w sekundach)
- s-ustal wielkość pakietów
- t-ustal ttl

Tracerout - narzędzie wykorzystujące pakiety ICMP do prześledzenia drogi przebytej przez Internet z jednego urządzenia do drugiego. Jest w stanie zmierzyć czas potrzebny do przeskoku z jednego węzła na drugi. Aby zapewnić dokładność każdy skok wykonywany jest parę razy. Narzędzie to najczęściej wykorzystywane jest do diagnostyki przerw w transferze danych. Umożliwia ono określenie dokładnego miejsca, w którym owe dane zostały "zgubione".

Przykład użycia:

```
mango@T14:~$ traceroute google.com
traceroute to google.com (216.58.209.14), 30 hops max, 60 byte packets
 1 funbox.home (192.168.1.1)  10.990 ms  10.941 ms  10.921 ms
 2 192.0.0.1 (192.0.0.1)  25.956 ms  25.938 ms  25.919 ms
 3 195.205.0.81 (195.205.0.81)  25.869 ms  25.851 ms  25.833 ms
 4 195.116.35.198 (195.116.35.198)  50.194 ms  50.183 ms  50.162 ms
 5 72.14.214.158 (72.14.214.158)  50.143 ms  50.124 ms  50.104 ms
 * * *
 7 108.170.237.68 (108.170.237.68)  21.072 ms  142.250.37.209 (142.250.37.209)  15.133 ms  209.85.253.224 (209.85.253.224)  15.106 ms
 8 142.250.37.195 (142.250.37.195)  16.932 ms  172.253.68.29 (172.253.68.29)  16.931 ms  16.923 ms
 9 waw02s18-in-f14.1e100.net (216.58.209.14)  16.910 ms  13.759 ms  108.170.250.209 (108.170.250.209)  15.304 ms
```

Traceroute próbuje ustalić potencjalną drogę jaką obrałby pakiet przesłany do ustalonego celu (w tym przypadku domeny google.com) poprzez wysyłanie pakietów o małym ttl i nasłuchiwanie na sygnał "time exceeded". Zaczynamy od małego ttl stopniowo je zwiększając, aż w pewnym momencie otrzymamy sygnał "port unreachable" (lub TCP reset), co pozwala nam stwierdzić, że dotarliśmy do "hosta" lub dotarliśmy do maksimum (standardowo 30 skoków). Przy każdej wartości ttl wysyłane są 3 (standardowo) próbki, po czym wypisywany jest ttl, adres bramki oraz całkowity czas próbki. Jeżeli odpowiedź nadejdzie z innej bramki zostanie wypisany adres każdego poszczególnego punktu z której nadeszła odpowiedź. Jeżeli w danym czasie odpowiedź nie nastąpi - "\*" zostanie wypisana na ekranie.

Podstawowe opcje:

- f-ustalenie początkowego ttl
- F-nie fragmentuj pakietów

- m-ustalenie maksymalnego ttl
- q-ustalenie ilości próbek
- w-ustalenie czasu oczekiwania na odpowiedź

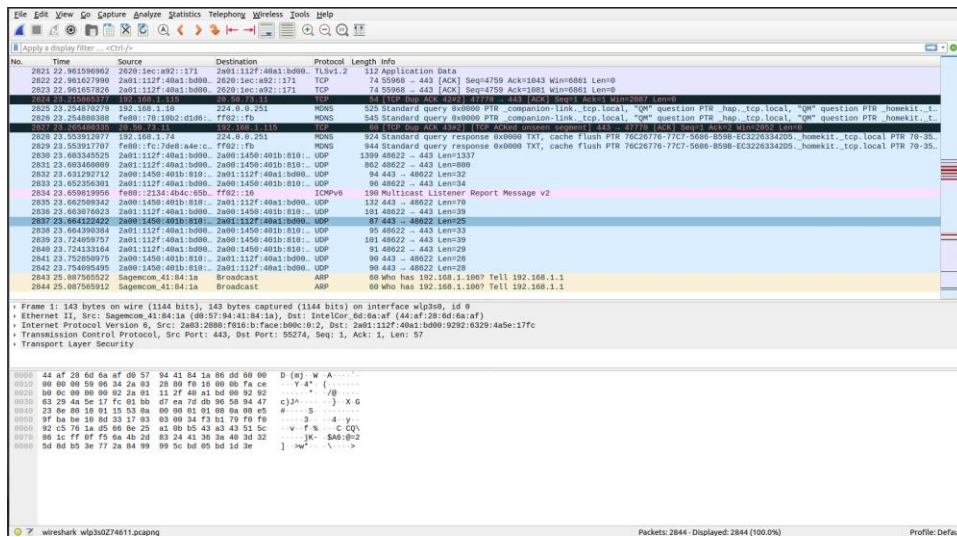
Wireshark – analizator pakietów sieciowych, prezentujący jak najdokładniej dane na temat przechwytych pakietów. Służy on także do przechwytywania i zapisywania ruchu sieciowego. Jest w stanie rejestrować pakiety przychodzące i wychodzące oraz informacje ich dotyczące.

Zastosowania:

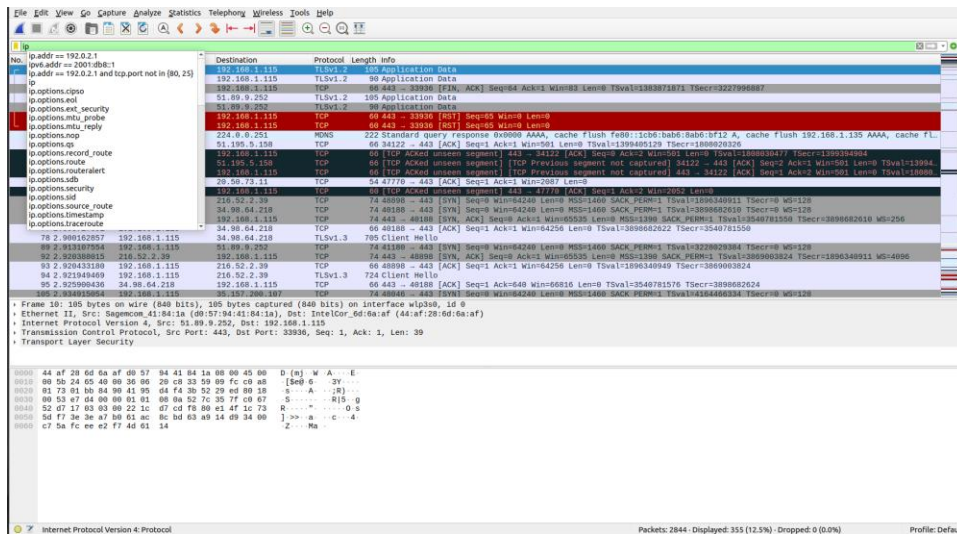
- Rozwiązywanie i diagnostyka problemów sieciowych
- Weryfikowanie aplikacji sieciowych
- Debugowanie implementacji protokołów sieciowych
- Itp.

Przykład użycia:

- Bez filtrów



- Z filtrami



## Wywołania programów:

## Odległość a liczba węzłów na trasie

Aby otrzymać liczbę skoków pomiędzy serwerami wystarczy zwrócić uwagę na ttl.

Jeśli chcemy uzyskać liczbę skoków do jakiegoś miejsca ustalamy najpierw jakąś małą wartość ttl a następnie zwiększamy, dopóki nie uzyskamy odpowiedzi.

Jeśli natomiast chcemy uzyskać liczbę skoków “w drugą stronę” wystarczy, że odejmiemy uzyskane ttl od najbliższej z popularnych wartości (32, 64, 128, 255)

Domena	L. skoków “do”	L. skoków “od”	Przybliżona odległość
gove.au	15	64-53 = 11	15000 km
google.com	9	128-116 = 12	1100 km
deutschland.de	13	64-57 = 7	295 km
gove.cn	20	64-49 = 25	7200 km

Z wyników można wywnioskować, że wraz ze wzrostem odległości wzrasta liczba skoków, choć nie musi być to konieczne. Widać też, że pakiety w drodze do celu poruszają się inną trasą niż w drodze powrotnej, co można wywnioskować z różnej liczby skoków w poszczególne strony.

## Wielkość pakietów/fragmentacja a czas propagacji/liczba węzłów

Sprawdźmy teraz jaki wpływ na liczbę węzłów przebytą przez pakiet ma jego rozmiar. Do tego celu przyda nam się opcja `-s ping’a`.

domena	Rozmiar pakietu	Skoki od/do (fragmentacja)	Skoki od/do (brak fragmentacji)	Średni czas propagacji pakietu (fragmentacja)	Średni czas propagacji pakietu (bez fragmentacji)

Google.com	64 bytes	12/11	12/11	18.647 ms	19.792 ms
	1208 bytes	12/11	12/11	18.791 ms	19.769 ms
	5008 bytes	-	-	-	-
Gove.cn	64 bytes	25/20	25/20	238.660 ms	252.888 ms
	1208 bytes	25/20	25/20	263.330 ms	266.478 ms
	5008 bytes	-	-	-	-
Deutschland.d e	64 bytes	7/13	7/13	31.913 ms	41.417 ms
	1208 bytes	7/13	7/13	34.922 ms	35.341
	5008 bytes	-	-	-	-

Przykładowe wywołanie programu PING bez fragmentacji, wielkość pakietu = 1208, ilość próbek = 10:

```
mango@T14:~$ ping -M do -s 1200 -c 10 google.com
PING google.com (216.58.215.110) 1200(1228) bytes of data:
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=1 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=2 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=3 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=4 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=5 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=6 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=7 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=8 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=9 ttl=115 (truncated)
76 bytes from waw02s17-in-f14.1e100.net (216.58.215.110): icmp_seq=10 ttl=115 (truncated)

--- google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 65.901/97.474/227.014/44.264 ms
```

Wnioski:

Fragmentacja:

- Zmniejsza czas propagacji pakietów
- Nie wpływa na ilość skoków

Wielkość pakietów:

- Nie wpływa na czas propagacji pakietów
- Nie wpływa na ilość skoków

Największy niefragmentowany pakiet jaki udało się przesłać to 1500 bajtów, czyli 1472 bajtów danych oraz 28 bajtów nagłówka. Dzieje się tak ponieważ MTU (maximum transmission unit) ma wielkość 1500 bajtów.

Dla małych odległości geograficznych:

Domena	Rozmiar pakietu	Skoki od/do (bez fragmentacji)	Skoki od/do (fragmentacja)	Średni czas propagacji pakietu	Średni czas propagacji pakietu (fragmentacji)

				(bez fragmentacji)	
www.wroclaw.pl	64	8/7	9/7	19.415	29.882
	1208	8/7	8/7	19.964	18.810
	5008	-	-	-	-
Nokiawroclaw.pl	64	8/7	8 lub 9/ 7	17.962	16.193
	1208	8/7	8/7	17.328	21.123
	5008	-	-	-	-

## Średnica Internetu

Największą odległość w węzłach jaką udało mi się znaleźć jest trasa kera.co.nz. “Od” trasa ma długość 20 węzłów, natomiast “do” aż 23. Strona ta zdaje się być stroną jakiegoś Nowo Zelandzkiego rezerwatu przyrody.

## Sieci wirtualne

Bardzo dobrym przykładem użycia sieci wirtualnych są ścieżki prowadzące do domen za tak zwanym “Wielkim Chińskim Firewalllem”. “Nienaturalna” ilość węzłów na ścieżce do gove.cn bardzo dobrze prezentuje politykę zaciemniania sieci Chińskich. Dzięki temu nie jesteśmy w stanie dokładnie poznać infrastruktury Chińskich sieci.

```
mango@T14:~$ traceroute gove.cn -m 255
traceroute to gove.cn (139.196.214.104), 255 hops max, 60 byte packets
 1 funbox.home (192.168.1.1)  4.123 ms  4.061 ms  4.037 ms
 2 192.0.0.1 (192.0.0.1)  13.991 ms  13.970 ms  13.947 ms
 3 195.205.0.81 (195.205.0.81)  13.952 ms  13.928 ms  13.908 ms
 4 195.116.35.206 (195.116.35.206)  16.449 ms  16.435 ms  16.416 ms
 5 hbg-b2-link.ip.twelve99.net (213.248.96.144)  24.970 ms  26.339 ms  26.325 ms
 6 hbg-bb3-link.ip.twelve99.net (62.115.120.78)  28.310 ms  19.159 ms *
 7 ffm-bb1-link.ip.twelve99.net (62.115.123.76)  26.554 ms  25.990 ms  25.973 ms
 8 ffm-b11-link.ip.twelve99.net (62.115.124.119)  27.818 ms  ffm-b11-link.ip.twelve99.net (62.115.124.117)  27.810 ms  27.802 ms
 9 202.97.58.149 (202.97.58.149)  27.794 ms  118.85.205.81 (118.85.205.81)  28.559 ms  202.97.58.149 (202.97.58.149)  28.495 ms
10 202.97.95.205 (202.97.95.205)  217.486 ms  217.468 ms  202.97.99.221 (202.97.99.221)  255.835 ms
11 * * 202.97.12.193 (202.97.12.193)  229.401 ms
12 202.97.24.217 (202.97.24.217)  220.114 ms  202.97.62.113 (202.97.62.113)  226.443 ms  202.97.62.157 (202.97.62.157)  196.846 ms
13 101.95.224.118 (101.95.224.118)  201.447 ms  101.95.218.198 (101.95.218.198)  253.243 ms *
14 101.95.209.246 (101.95.209.246)  223.336 ms  101.95.209.74 (101.95.209.74)  195.039 ms  101.95.209.222 (101.95.209.222)  224.809 ms
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 139.196.214.104 (139.196.214.104)  268.378 ms IX  268.297 ms IX  268.284 ms IX
```

## Podsumowanie

Przeprowadzone testy pozwoliły nam określić, że:

- wielkość pakietów nie ma zbytniego wpływu na czas propagacji ani na długość ścieżki
- fragmentacja pakietów ma wpływ na czas propagacji, lecz nie na długość ścieżki
- średnica Internetu wynosi przynajmniej 23 węzły, lecz nie jesteśmy w stanie tego dokładnie określić
- nienaturalnie wysoka ilość węzłów prowadzących do połączenia z serwerami Chińskimi wskazuje na użycie sieć wirtualnych
- Ping, wireshark oraz traceroute pozwalają nam na zbadanie sieci oraz analizę danych przez nią przechodzących. Są one potrzebne do zdobycia choćby podstawowej wiedzy na temat funkcjonowanie sieci i pakietów.