Technologie Sieciowe
Lista 1

Illia Azler
239537

Ping

Polecenie ping jest poleceniem używanym do testowania zdolności komputera źródłowego do dotarcia do określonego komputera docelowego. Zwykle jest używany do sprawdzenia, czy może komputer komunikować się przez sieć z innym komputerem lub urządzeniem sieciowym(serwerem).

Czas potrzebny na odpowiedź sieci zwany jest opóźnieniem.

Przykład użycia polecenia "ping" Windows OS

Sprawdzić możemy za pomocą polecenia **ping** w konsoli cmd

```
ping google.com
```

Polecenie ping wysyła żądania do sieci, a gdy odpowiedź zostanie odebrana, otrzymujemy informację wyjściową z następującymi informacjami (standardowo 4 wysłanych pakietów po 32 bajty):

- liczba odebranych bajtów
- adres IP
- numer porządkowy
- czas potrzebny na odpowiedź

Również możemy sprawdzić połączenie za pomocą IP adresu

```
ping 192.168.0.1
```

Flagi:

- ping -a 142.250.186.206 — nazwa hostu
- ping -4 google.com — format tylko IPv4
- ping -6 google.com — format tylko IPv6
- ping -n 4 google.com — liczba wysłanych pakietów(default bez flagi 4)
- ping -w 10 google.com — czas w milisekundach pomiędzy próbami
- ping -f google.com — wysyłanie z flagą zapobiegającą fragmentacji oraz wyświetla IP
- ping -i 15 google.com — TTL(Time to live)
- ping -l 1452 google.com — wielkość wysłanego pakietu(>1512 brak odpowiedzi)

Jak sprawdzić ile jest węzłów na trasie?

Dobierając odpowiednią ilość TTL **do** podanego adresu. W przypadku niewystarczającej ilości dostajemy wiadomość: „TTL expired in transit”.
W podanym przykładzie:

```
ping -i 15 google.com
```

Dostajemy odpowiedź od serwera.
W przypadku poniższego polecenia dostajemy odpowiedź: „TTL expired in transit”.

```
ping -i 14 google.com
```

Więc mamy 15 węzłów do google.com.
Żeby dowiedzieć się ile węzłów mamy **od** serwera, odejmujemy otrzymany TTL przy zwykłym poleceniu ping od najbliższej ilości bajtów(64, 128, 255)

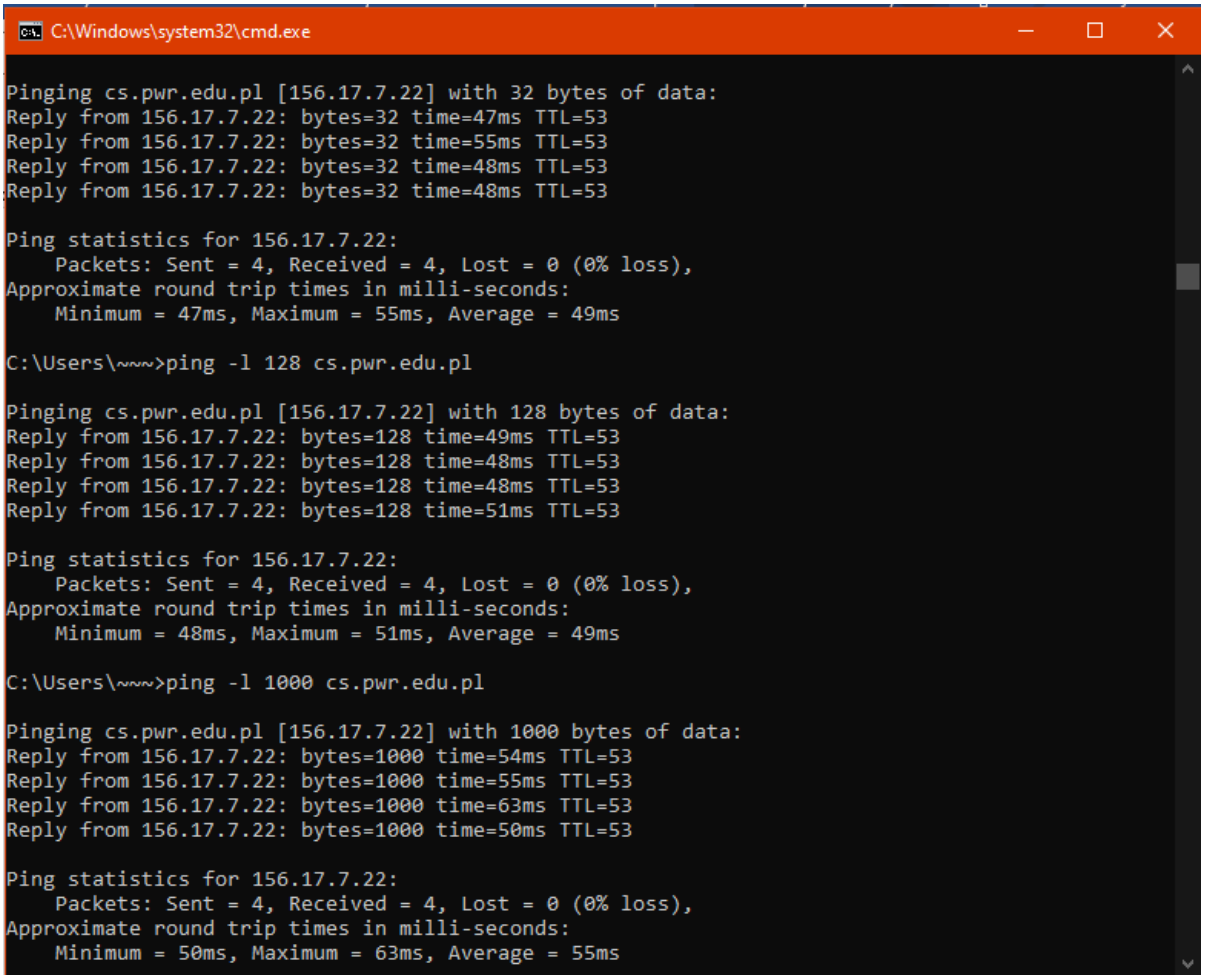
Odległość geograficzna

Domen	Do	Od	Lokalizacja serwera docelowego
onet.pl	8	8	United States
cs.pwr.edu.pl	13	11	Poland
play.pl	9	8	Poland
automobile.fr	15	12	Netherlands
cbsnews.com	8	7	United States
foxnews.com	9	9	United Kingdom

Patrząc na tabele możemy wywnioskować, że odległość geograficzna zależy od trasy do serwera, im dalej, tym więcej węzłów, ale nie jest tak zawsze. Co ciekawie, trasa w jednej lokalizacji może być dłuższa niż przy odległości w 10000 km między serwerami. Moim zdaniem, zależy to od złożoności systemu.
Geograficznie: Mój IP - Bydgoszcz, Kujawsko-Pomorskie, Poland
cs.pwr.edu.pl - Wroclaw, Lower Silesia, Poland

Wielkość pakietów

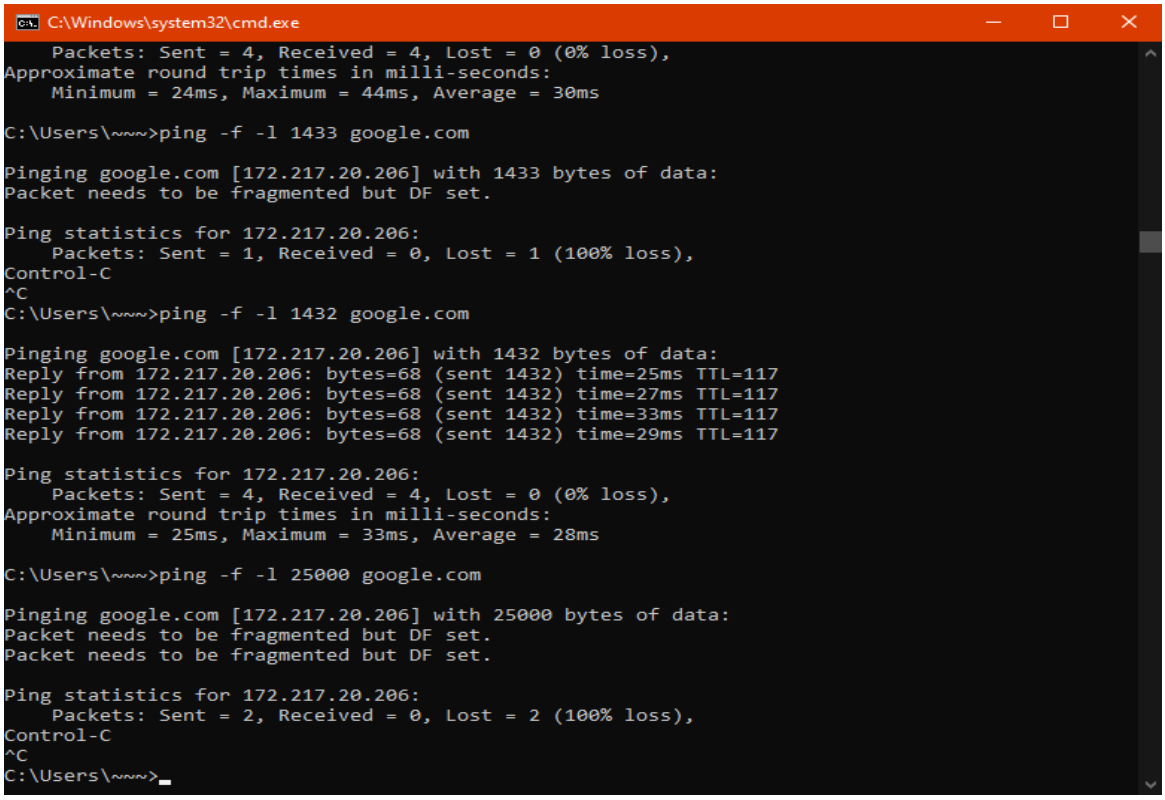
Rozmiar(bajty)	32		128		1000	
Domen	Min	Max	Min	Max	Min	Max
cs.pwr.edu.pl	47ms	55ms	48ms	51ms	50ms	63ms
onet.pl	23ms	25ms	22ms	36ms	25ms	33ms
automobile.fr	41ms	57ms	40ms	42ms	40ms	52ms



Możemy wywnioskować: 1) ilość węzłów pozostaje stałą; 2) wielkość wysłanego pakietu wpływa na czas, lecz niezbyt znacznie, im większy rozmiar, tym dłużej trwa proces.

Niefragmentowane pakiety

Największy niefragmentowany pakiet, który można wysłać dla google.com w moim przypadku wynosi 1432 bajty. Sprawdzimy to za pomocy flagi -f (niefragmentowany pakiet) oraz -l (wielkość pakietu).



„Średnica" internetu

Średnicę internetu można określić za pomocą ilości węzłów. Geograficznie do Polski najdalszy punkt znajduje się w Nowej Zelandii(17.465,40km). Największą ilość węzłów od Polski trudno określić. Zgodnie z najdalszym od nas geograficznym punktem, zaczyna ona od 16 węzłów przy adresie iponz.govt.nz. Fakt, różnica w ilości węzłów pomiędzy najdalszym punktem od Polski a adresem cs.pwr.edu.pl wynosi 3 węzły ;) Adres cs.pwr.edu.pl geograficznie znajduję się w 233,38km od mojego IP. Przypuśćmy, że średnica internetu wacha się w przedziale od 16 do 25 węzłów.

Sieci wirtualne

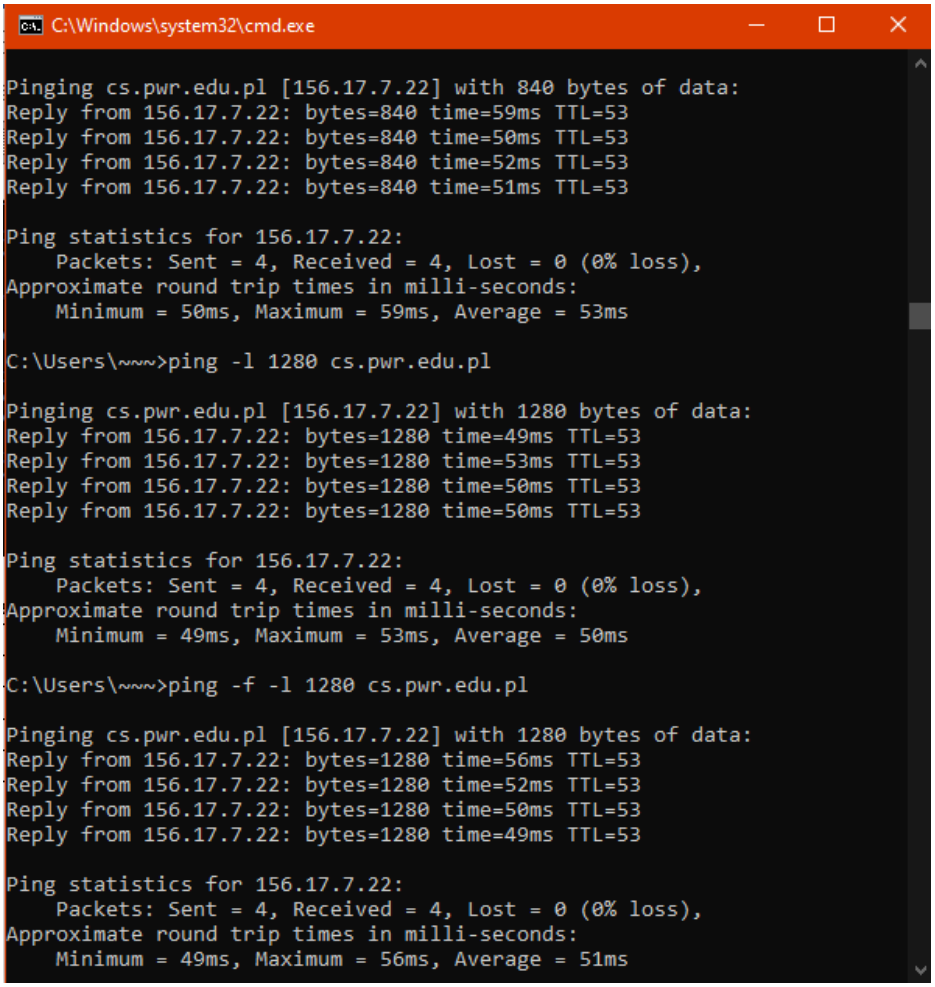
Sieci wirtualne modyfikują ilość węzłów, na tej podstawie przy pingowaniu tego samego adresu dostajemy różną ilość węzłów lub odpowiedź od innego IP. To znaczy, że przechodzimy prze sieć wirtualną. Śledzenie pakietów w takim przypadku będzie utrudnione.

Wpływ fragmentacji na czas

Rozmiar(bajty)	**128**		**840**		**1280**	
Domen	**F(avg)**	**DF(avg)**	**F(avg)**	**DF(avg)**	**F(avg)**	**DF(avg)**
cs.pwr.edu.pl	49ms	49ms	51ms	53ms	50ms	51ms
onet.pl	25ms	25ms	24ms	24ms	27ms	27ms
foxnews.com	40ms	42ms	40ms	43ms	46ms	43ms

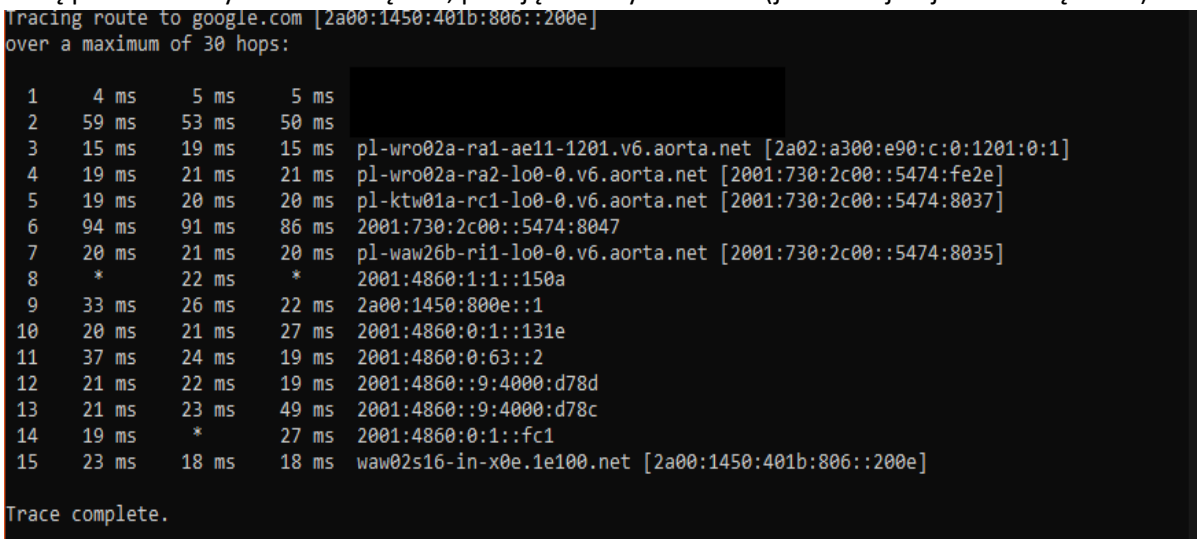
F – fragmentowany
DF – niefragmentowany
Dość trudno określić różnice w czasie opóźnienia pomiędzy pakietami fragmentowanymi a niefragmentowanymi. Wielkość pakietu oraz fragmentacja zgodnie ze sprawdzeniem nie wykazuje dużej różnicy. Fragmentowany ma trochę mniejszy czas opóźnienia niż niefragmentowany, ale nie koniecznie.

Poniższy zrzut ekranu to udowadnia:



TraceRoute(tracert)

W przypadku flagi ping -i musieliśmy dobierać odpowiednią ilość węzłów. TraceRoute wylicza dokładną trasę przez serwery oraz ilość węzłów, podając adresy serwerów(jednak zajmuje to trochę czasu).



WireShark

To sniffer(przechwytuje i ewentualnie analizuje dane przepływające w sieci) będący wolnym oprogramowaniem. Umożliwia przechwytywanie i nagrywanie pakietów danych w wybranie sieci, a także ich dekodowanie. Dzięki dużej ilości dodatków potrafi rozpoznać i zdekodować wiele protokołów komunikacyjnych. W głównej mierze jest wykorzystywany przez administratorów sieci, służby specjalne oraz hakerów do śledzenia pakietów. Zaletą jest obecność GUI.

Wnioski

W przypadku odległości zaskoczeniem była ilość węzłów od Bydgoszcza do Wrocławia, chociaż fizycznie znajduję się we Wrocławiu, UPC Polska ma tam swoje serwerze(zgodnie z położeniem mojego IP). Jednak to bardziej „wyjątki", w zasadzie im geograficznie bliżej do lokalizacji, tym mniej węzłów. „Średnica" internetu ma w zasadzie 20-25 węzłów, wydaję mi się, że może być na kilka więciej.
Co dotyczy realizowanych programów, najciekawszy okazał się Wireshark, ponieważ może przechwycić dane oraz ich dekodować. Każdy z programów ma swoje przeznaczenie oraz swoją analizę sieci. Wielkość pakietów nie wpływa na ilość węzłów i niezbyt dużo na czas opóźnienia. Ciekawym faktem był wpływ lokalizacji na ilość węzłów, a niefragmentowane i fragmentowane dane niezbyt się różnią w czasie opóźnienia, tylko różnią się pod katem wielości wysłanego pakietu, fragmentowane dane mogą mieć większy rozmiar niż niefragmentowane. W przypadku google.com - 1452 bajtów fragmentowanego pakietu w porównaniu do 1432 bajtów niefragmentowanego pakietu.