Sprawozdanie z listy 1 na laboratorium   
 Technologie Sieciowe

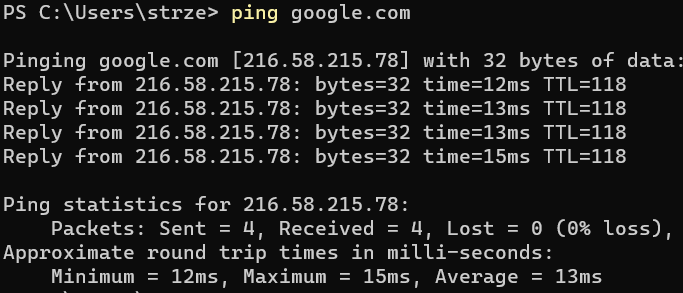
Wojciech Strzelecki (254618)

1. **Wstęp  
   1.1. Polecenie**

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 przesłac. Przeanalizuj te same zagadnienia dla krótkich tras (do serwerów bliskich geograficznie). Określ "średnicę" internetu (najdłuższą sćieżkę którą uda sie wyszukać). Czy potraficz wyszukać trasy przebiegające przez sieci wirtualne (zdalne platformy "cloud computing"). Ile węzłów mają scieżki w tym przypadku.  
b) Traceroute,  
c) WireShark.

**1.2 . Ping**  
  
Ping to program pozwalający na diagnozowanie połączeń sieciowych. Pozwala na sprawdzanie istnienia połączenia między hostami. Pokazuje też liczbę zgubionych pakietów po przesłaniu oraz opóźnienie transmisji.  
 **1.2.1 Przykładowe użycie na Windowsie**



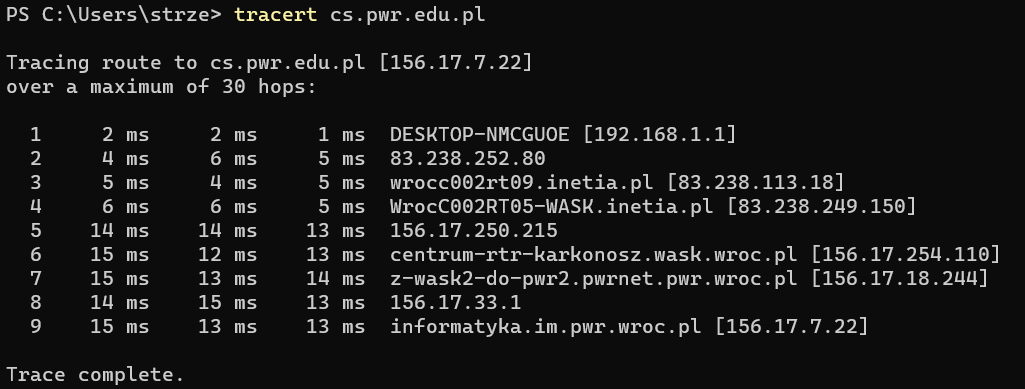
**1.2.2 Najważniejsze opcje**

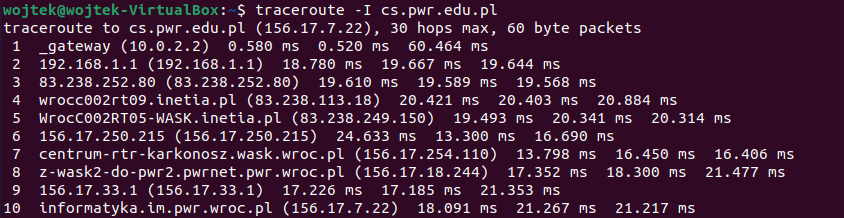
* -l <<wartość>> - ustawienie rozmiaru wysyłanego pakietu
* -4 – wymusza użycie protokołu IPv4
* -i <<wartość>> - wartość pola TTL (Time To Live) (na Linux -t)
* -f – brak fragmentacji (na Linux -M do)

**1.3 Traceroute**

Traceroute to program służący do badania trasy pakietów w sieci IP. Jego odpowiednikiem w systemach Windows jest Tracert.

* + 1. **Przykładowe użycie na Windowsie i Linuxie**

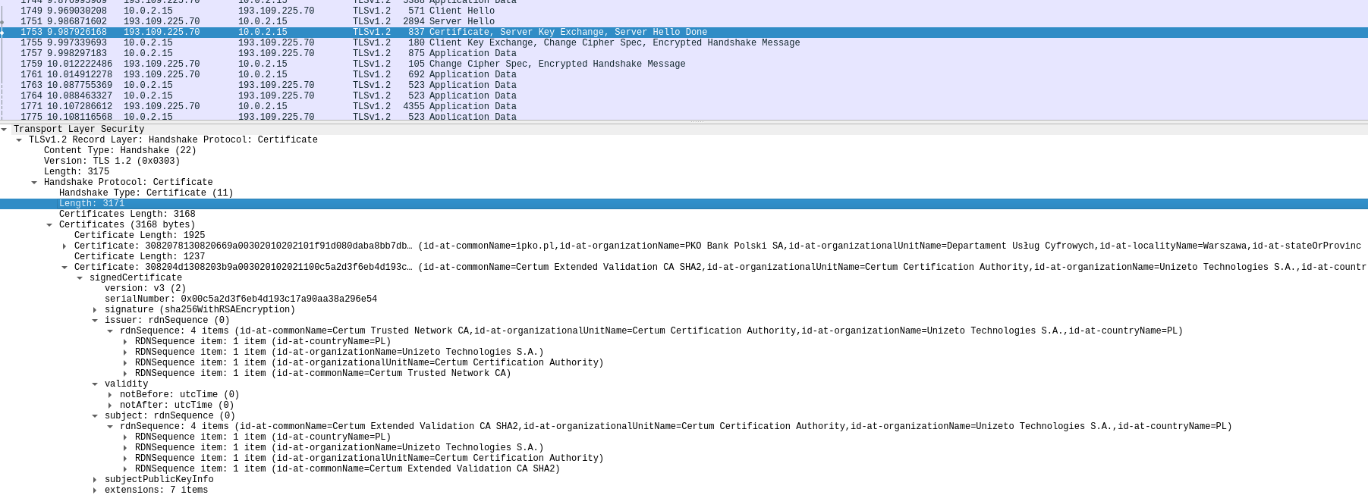




**1.4 WireShark**

WireShark to bezpłatny program opensource. Używany do kontrolowania i dekodowania pakietów danych. Potrafi zdekodować wiele protokołów komunikacyjnych. Wykorzystywany głównie przez administratorów sieci. WireShark wyposażony jest we własny interfejs graficzny.

**1.4.1 Przykładowe użycie do dekodowania pakietu strony PKO B.P.**



**2. Testy**

**2.1 Odległości**

Testy polegały na „pingowaniu” serwerów w różnych odległościach geograficznych. Skoki do ustalamy poprzez odpowiednie nadanie wartości pola TTL i zwiększanie jej do momentu otrzymania odpowiedzi. Skoki z to różnica pomiędzy początkową wartością TTL (64, 128 lub255) a wartością zwracaną.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adres | Położenie | Skoki do | Skoki z | Średni czas [ms] |
| cs.pwr.edu.pl | Polska | 9 | 10 | 14 |
| mof.gov.sg | Singapur | 9 | 11 | 16 |
| sydney.edu.au | Australia | 15 | 25 | 294 |
| tokyo-icc.jp | Japonia | 25 | 27 | 332 |

Można wywnioskować, że *średnica Internetu* ma zatem około 27 węzłów.

**2.2 Wielkość pakietu, a liczba węzłów**

Sprawdzimy, czy rozmiar pakietów wpłynie na ilość węzłów potrzebnych do przebycia. Z wykorzystaniem flagi *-l* podam 4 różne rozmiary pakietów (128, 256,   
512 i 1024) i sprawdzę, przy jakiej minimalnej liczbie skoków otrzymamy informację zwrotną.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adres | 128 | 256 | 512 | 1024 |
| cs.pwr.edu.pl | 9 | 9 | 9 | 9 |
| government.nl | 10 | 10 | 10 | 10 |
| sydney.edu.au | 15 | 15 | 15 | 15 |

Wniosek: Rozmiar pakietu nie wpływa na liczbę węzłów potrzebnych do przebycia.

**2.3 Wielkość pakietu, a czas propagacji [ms]**

Sprawdzimy jak wielkość pakietu wpłynie na czas propagacji dla różnej wielkości pakietów. W poniższej tabeli przedstawiłem jak wyglądały średnie czasy propagacji dla różnych adresów i rozmiarów pakietów.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adres | 128 | 256 | 512 | 1024 |
| cs.pwr.edu.pl | 13 | 14 | 14 | 14 |
| government.nl | 38 | 39,5 | 41 | 38 |
| sydney.edu.au | 330 | 331 | 331 | 332 |

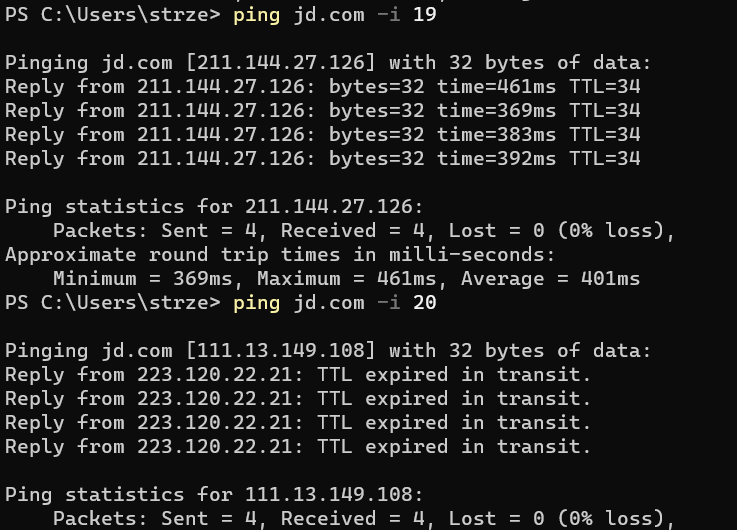
**2.4 Fragmentacja**

Sprawdzimy, jaki jest maksymalny rozmiar niefragmentowanego pakietu. Użyjemy do tego wywołania ping, flagi DF (*Don’t Fragment*) *-f* oraz flagi ustawiającej rozmiar pakietu *-l*. Okazuje się, że maksymalny rozmiar niefragmentowanego pakietu możliwego do wysłania wynosi 1472 bajty. W poniższej tabeli przedstawiłem wpływ zastosowania flagi DF na liczbę węzłów oraz średni czas dla pakietu 512 bajtów.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Adres | TTL | TTL z DF | Czas [ms] | Czas z DF [ms] |
| cs.pwr.edu.pl | 9 | 9 | 14 | 14 |
| government.nl | 10 | 10 | 39 | 40 |
| sydney.edu.au | 15 | 15 | 330 | 336 |

**3. Sieci wirtualne**

Trasy przebiegające przez sieci wirtualne będziemy szukać poprzez „pingowanie” adresów stron z flagą *-i* ustawiającą wartość TTL. Trasy przebiegające przez sieci wirtualne będą miały zmienną liczbę hopów.



Jak widzimy początkowo dla wartości 19 otrzymaliśmy informację zwrotną, a następnie przy wartości 20 pakiet wygasł w trakcie przesyłania (wartość TTL była zbyt mała).

**4. Podsumowanie**

Wyniki doświadczeń zgadzają się z intuicją. Do serwerów dalszych geograficznie potrzebujemy więcej skoków niż do serwerów znajdujących się w Polsce. Jak pokazały testy rozmiar oraz fragmentacja pakietu nie wpłynęły znacząco na czas propagacji.   
Przydatność powyższych programów zależy niewątpliwie od potrzeb i wiedzy użytkownika. Z pewnością można stwierdzić, że są to dobre narzędzia do diagnostyki i analizy sieci.