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 sie 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:

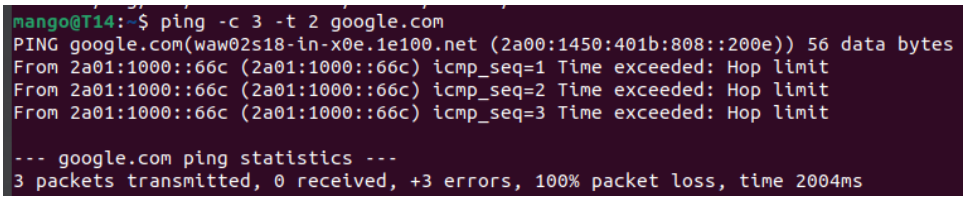
Ping - Packet Internet Groper jest narzędziem diagnostycznym, który pozwala na sprawdzenie łączności pomiędzy dwoma urządzeniami. Polecenie Ping wysyła pakiet danych do urządzenia docelowego, który powinien zostać zwrócony, w ten sposób można określić czy połączenie pomiędzy dwoma urządzeniami istnieje.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

Przykład użycia:

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

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

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

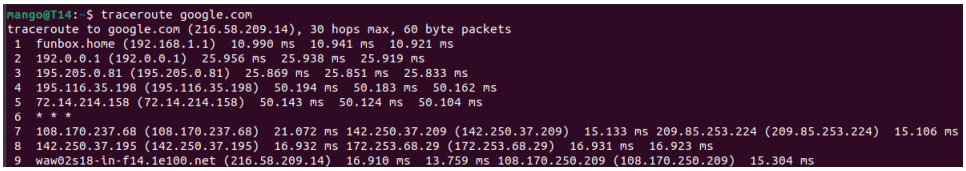


Podstawowe opcje:

- 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 przerwań w transferze danych. Umożliwia ono określenie dokładnego miejsca, w którym owe dane zostały “zgubione”.

Przykład użycia:



Traceroute próbuje ustalić potencjalną drogę jaka 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 unreacheable” (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 bramy 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

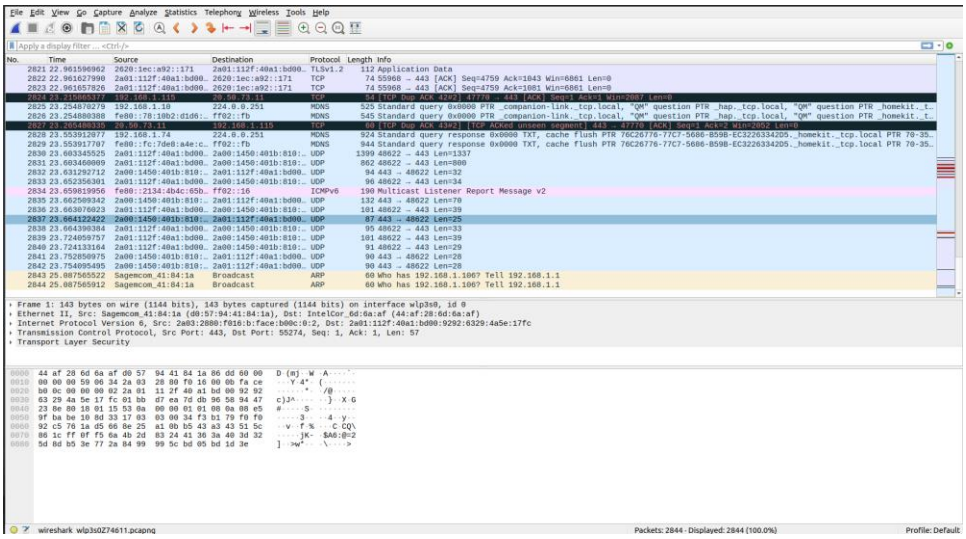
Wireshark – analizator pakietów sieciowych, prezentujący jak najdokładniej dane na temat przechwyconych pakietów. Służy on także do przechwytywania i zapisywania ruchu sieciowego. Jest w stanie rejestrować pakiety przychodzące i wychodzące oraz informacje ich dotyczące.

Zastosowania:

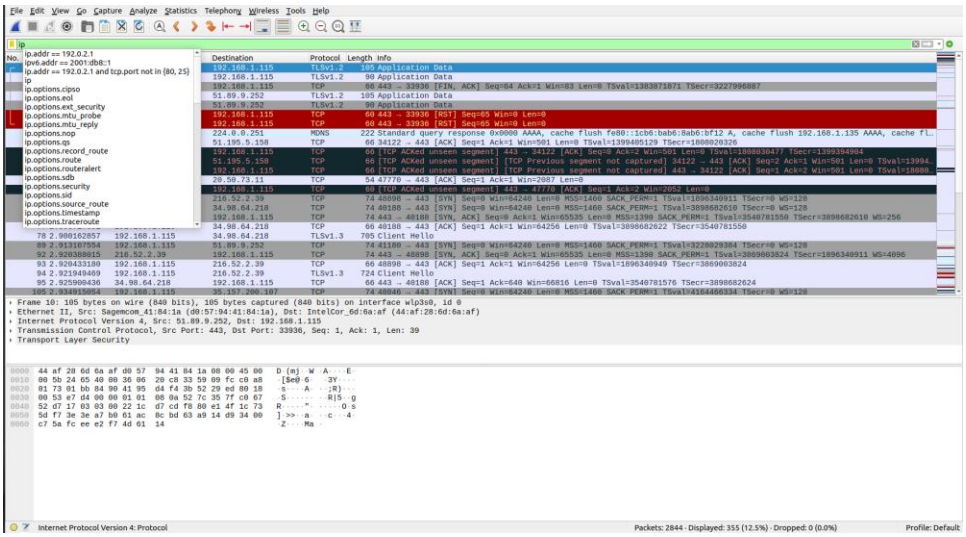
- Rozwiązywanie i diagnostyka problemów sieciowych
- Weryfikowanie aplikacji sieciowych
- Debugowanie implementacji protokołów sieciowych
- Itp.

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 jakaś 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, chodź nie musi być to konieczne. Widać też, że pakiety w drodze do celu poruszają się inna trasą niż w drodze powrotnej, co można wywnioskować z różnej liczby skoków w poszczególne strony.

Wielkość pakietów/fragmentacja a czas propagacji/liczba węzłów

Sprawdzimy 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.de	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)

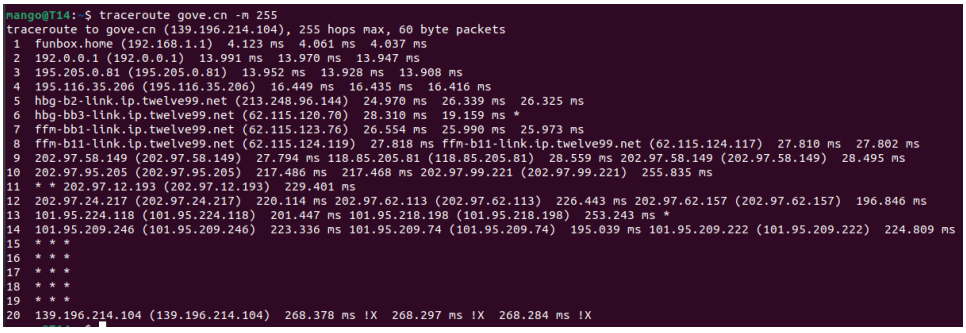
				(bez fragmentacji)	
www.wroclaw.pl	64	8/7	9/7	19.415	29.882
	1208	8/7	8/7	19.964	18.810
	5008	-	-	-	-
Nokiawroclaw.pl	64	8/7	8 lub 9/ 7	17.962	16.193
	1208	8/7	8/7	17.328	21.123
	5008	-	-	-	-

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 Firewallem”. “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.



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 siec 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.