Lista 1
Technologie sieciowe

Patryk Majewski

14 marca 2020

1 Opis zadania

Celem zadania jest zapoznanie się z działaniem programów Ping, Traceroute, WireShark, a następnie wykorzystanie programu Ping do przeprowadzenia następujących testów:

- zależność liczby węzłów na trasie od odległości,
- zależność liczby węzłów na trasie od rozmiaru pakietu, określenie maksymalnego rozmiaru pakietu,
- zależność czasu propagacji od rozmiaru pakietu,
- wpływ fragmentacji pakietów na dwa poprzednie testy,
- wpływ sieci wirtualnych na liczbę węzłów.

Na postawie wykonanych testów należy następnie spróbować określić "średnicę" internetu, czyli najdłuższą znalezioną ścieżkę.

2 Działanie programów

2.1 Ping

Ping jest programem umożliwiającym sprawdzenie połączenia z danym serwerem. Wysyła "sygnał echo" – pakiet o określonych parametrach. Następnie oczekuje na odpowiedź, a po jej otrzymaniu informuje użytkownika o szczegółach:

```
$ ping cs.pwr.edu.pl
PING cs.pwr.edu.pl (156.17.7.22) 56(84) bytes of data.
64 bytes from informatyka.im.pwr.wroc.pl (156.17.7.22): icmp_seq=1 ttl=52 time=6.54 ms
64 bytes from informatyka.im.pwr.wroc.pl (156.17.7.22): icmp_seq=2 ttl=52 time=8.35 ms
64 bytes from informatyka.im.pwr.wroc.pl (156.17.7.22): icmp_seq=3 ttl=52 time=8.84 ms
64 bytes from informatyka.im.pwr.wroc.pl (156.17.7.22): icmp_seq=4 ttl=52 time=7.70 ms
64 bytes from informatyka.im.pwr.wroc.pl (156.17.7.22): icmp_seq=5 ttl=52 time=9.37 ms

--- cs.pwr.edu.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 6.542/8.162/9.374/0.986 ms
```

W powyższym przykładzie z powodzeniem wysłaliśmy i otrzymaliśmy pięć pakietów. Rozmiar wysłanego przez nas pakietu to 64 bajty (56 + 8 na nagłówek). Otrzymaliśmy informację o adresie IP wybranej przez nas domeny. Przy każdym z odebranych pakietów program informuje o:

- jego rozmiarze,
- kolejności jego przyjścia (icmp_seq),
- pozostałym czasie życia (ttl),
- czasie, który upłynął od wysłania pakietu do uzyskania odpowiedzi (time).

Szczególnie wartą uwagi jest tutaj wartość ttl. Mechanizm jej działania umożliwia określenie liczby węzłów na trasie między serwerami. Nadawca pakietu ustala dla niego początkową wartość (zalecana to 64, maksymalna – 255, często występuje także 128). Każdy węzeł – router na trasie – dekrementuje ttl pakietu, a w przypadku wartości 0 nie przekazuje go dalej. Wiedzę tę wykorzystamy dalej podczas testów.

Wiadomość końcowa informuje nas o ewentualnych niepowodzeniach i całkowitym czasie operacji (biorąc pod uwagę również czas pomiędzy wysyłaniem kolejnych pakietów). Znajdują się tam również statystyki dla wartości time.
Opcje programu Ping, które wykorzystamy podczas wykonywania testów:

- -t – ustalenie początkowego ttl wysyłanych pakietów
- -c – ustalenie liczby pakietów do wysłania
- -s – ustalenie rozmiaru pakietu
- -i – ustalenie czasu między wysłaniem kolejnych pakietów
- -M do – zakazanie fragmentacji

2.2 Traceroute

Traceroute jest programem umożliwiającym śledzenie trasy wysłanego przez nas pakietu do określonego serwera. W tym celu wysyła próbki o inkrementowanym ttl (domyślnie zaczynając od 1), oczekując odpowiedzi "time exceeded". W ten sposób uzyskuje informacje o adresach kolejnych kroków na trasie. Przykładowe wywołanie:

```
$ traceroute cs.pwr.edu.pl
traceroute to cs.pwr.edu.pl (156.17.7.22), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.1)  6.348 ms  6.551 ms  6.466 ms
 2  10.10.10.1 (10.10.10.1)  6.495 ms  6.538 ms  6.625 ms
 3  78.11.75.145 (78.11.75.145)  6.657 ms  6.715 ms  7.309 ms
 4  wrocr013rt01.inetia.pl (213.17.151.165)  11.162 ms  15.387 ms  18.087 ms
 5  wrocr022rt01.inetia.pl (87.204.226.207)  9.287 ms  14.092 ms  16.582 ms
 6  wrocc002rt04.inetia.pl (87.204.226.38)  17.622 ms  7.401 ms  7.469 ms
 7  wask-do-pkptelekom.wask.wroc.pl (212.127.66.242)  5.085 ms  6.902 ms  7.006 ms
 8  156.17.250.215 (156.17.250.215)  13.011 ms  13.383 ms  14.252 ms
 9  centrum-rtr-karkonosz.wask.wroc.pl (156.17.254.110)  18.611 ms  23.372 ms  23.680 ms
10  rolnik2-centrum.wask.wroc.pl (156.17.254.65)  24.726 ms  25.214 ms  25.425 ms
11  wazniak-rolnik.wask.wroc.pl (156.17.254.140)  26.281 ms  27.717 ms  28.511 ms
12  z-wask2-do-pwr2.pwrnet.pwr.wroc.pl (156.17.18.244)  24.652 ms  23.361 ms  23.768 ms
13  156.17.33.1 (156.17.33.1)  6.046 ms  4.804 ms  5.649 ms
14  informatyka.im.pwr.wroc.pl (156.17.7.22)  5.974 ms  6.161 ms  6.835 ms
```

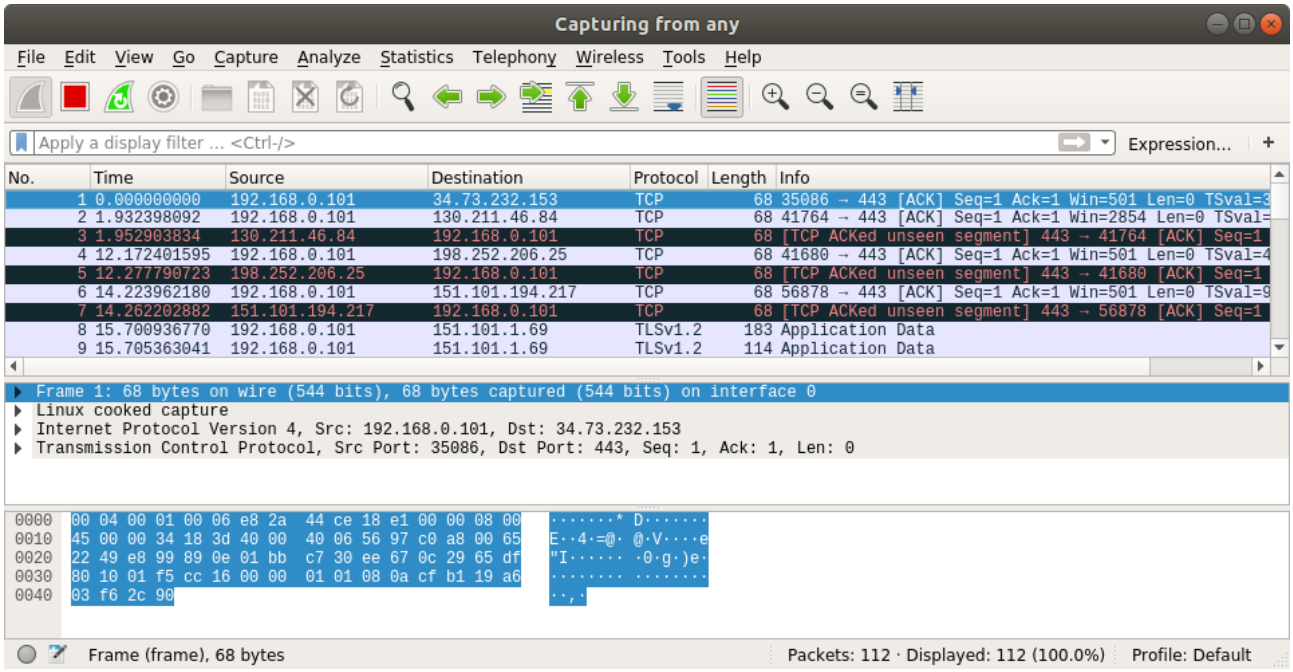
Domyślnie wysyłane są pakiety 60-bajtowe, po trzy na każdą wartość ttl, a maksymalna liczba skoków to 30 – wartości te możemy modyfikować z użyciem opcji programu:

- -f – ustalenie początkowego ttl
- -m – ustalenie maksymalnego ttl (maksymalnej liczby skoków)
- -q – ustalenie liczby pakietów wysyłanych dla każdej wartości ttl
- -w – ustalenie timeoutu oczekiwania na odpowiedź

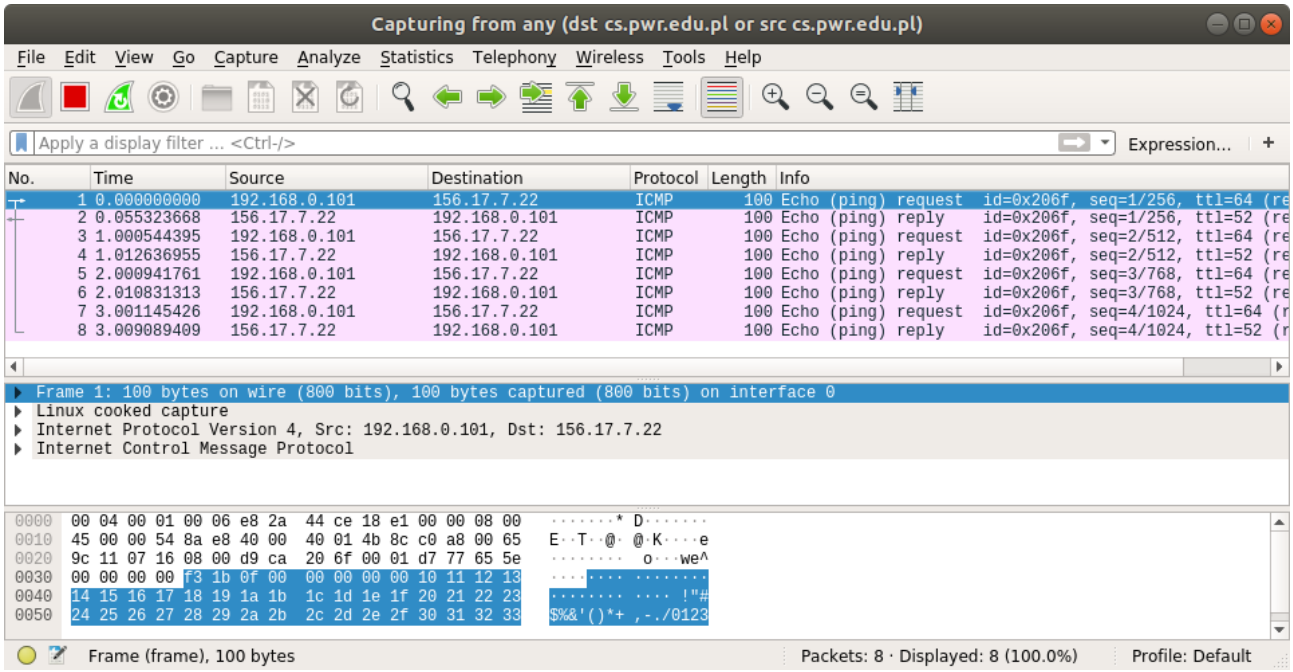
Może się zdarzyć, że w wywołaniu programu pojawi się symbol '*'. Oznacza to, że został przekroczony czas oczekiwania na odpowiedź. Czasami dzieje się tak, ponieważ dany serwer nie wysyła "time exceeded" albo nie zmienia ttl wysłanego przez nas pakietu, przez co odpowiedź nie ma szans na dotarcie.

2.3 WireShark

WireShark to tzw. "sniffer" – program służący do przechwytywania i zapisywania ruchu sieciowego. Rejestruje wszystkie pakiety wychodzące i przychodzące wraz z informacjami o nich (takimi jak czas, źródło, cel, protokół). Ponadto pozwala na użycie filtrów, dzięki czemu możemy przechwycić tylko te pakiety, które interesują nas w danym momencie. Przykładowe użycie programu:



Rysunek 1: Uruchomienie przechwytywania bez filtrów.



Rysunek 2: Przechwytywanie z filtrem "dst cs.pwr.edu.pl or src cs.pwr.edu.pl" – pakiety przechwycone po wywołaniu *ping cs.pwr.edu.pl*.

3 Testy

3.1 Odległość a liczba węzłów na trasie

Korzystając z wiedzy o zasadach zmian wartości ttl, liczbę skoków między serwerami wyznaczać będziemy w następujący sposób:

- *"do"* – wywołanie programu z ustaloną niewielką wartością ttl, inkrementacja wartości do momentu uzyskania odpowiedzi – w poniższym przykładzie otrzymujemy 14
- *"od"* – otrzymana wartość ttl odjęta od najbliższej z popularnych wartości startowych (32, 64, 128, 255) – w poniższym przykładzie: 64 - 52 = 12

```
$ ping -t 13 cs.pwr.edu.pl
PING cs.pwr.edu.pl (156.17.7.22) 56(84) bytes of data.
From 156.17.33.1 (156.17.33.1) icmp_seq=1 Time to live exceeded

$ ping -t 14 cs.pwr.edu.pl
PING cs.pwr.edu.pl (156.17.7.22) 56(84) bytes of data.
64 bytes from informatyka.im.pwr.wroc.pl (156.17.7.22): icmp_seq=1 ttl=52 time=6.84 ms
```

Domena	Skoki do	Skoki od	Lokalizacja	Odległość od Wrocławia
cs.pwr.edu.pl	14	12	Wrocław, PL	0 km
uw.edu.pl	14	12	Warszawa, PL	293 km
derspiegel.de	21	16	Köln, GE	709 km
vk.ru	18	14	Moskwa, RU	1462 km
publico.pt	19	18	Lizbona, PT	2281 km
canada.ca	24	24	Ottawa, CA	6417 km
digitimes.com.tw	22	29	Taipei, TW	8813 km
sfchronicle.com	18	27	San Francisco, US	9360 km
g1.globo.com	17	25	Rio de Janeiro, BR	10100 km
sydney.edu.au	26	32	Sydney, AU	15900 km
aut.ac.nz	24	28	Auckland, NZ	17660 km

Na podstawie wyników testu możemy wnioskować, że z reguły ze wzrostem odległości rośnie też liczba węzłów, chociaż udało się znaleźć też wyjątki. Zauważamy też, że w większości przypadków liczby skoków "od" i "do" różnią się.

3.2 Wielkość pakietu a liczba węzłów

Sprawdzimy teraz, jak na liczbę skoków na trasie wpływa rozmiar wysłanego przez nas pakietu. W tym celu posłużymy się opcją -s programu ping.

Domena	Rozmiar pakietu	Skoki do/od (fragmentacja)	Skoki do/od (bez fragmetacji)
cs.pwr.edu.pl	64 bajty	14/12	14/12
	512 bajtów	14/12	14/12
	1 452 bajty	14/12	14/12
	16 384 bajty	14/12	–
sfchronicle.com	64 bajty	18/27	18/27
	512 bajtów	18/27	18/27
	1 452 bajty	18/27	18/27
	16 384 bajty	18/27	–
sydney.edu.au	64 bajty	26/32	26/32
	512 bajtów	26/32	26/32
	1 452 bajty	26/32	26/32
	16 384 bajty	26/32	–

Uwaga:
3.2 i 3.3 nie są do końca dobrze. Pasowałoby sprawdzić różne rozmiary, nie tylko parzyste czy potęgi dwójki. Wnioski mogą być podobne, ale testy będą wiarygodniejsze.

Zauważamy, że rozmiar pakietu w żadnym stopniu nie wpływa na liczbę skoków. Podobnie ustawienie flagi zabraniającej fragmentacji nie zmienia wyników (o ile oczywiście uda się wysłać pakiet o danym rozmiarze – ustawienie -s na więcej niż 1452 skutkowało uzyskaniem błędu "message too long").

3.3 Wielkość pakietu a czas propagacji

Sprawdzimy teraz zależność czasu propagacji od rozmiaru pakietu. Wyślemy po sto pakietów danej wielkości do każdego z serwerów, a następnie za czas przyjmiemy średnią umieszczoną w wiadomości końcowej wywołania programu.

Domena	Rozmiar pakietu	Czas (fragmentacja)	Czas (bez fragmentacji)
cs.pwr.edu.pl	64 bajty	45.565 ms	58.455 ms
	512 bajtów	53.677 ms	45.472 ms
	1 452 bajty	48.390 ms	47.651 ms
sfchronicle.com	64 bajty	215.622 ms	199.210 ms
	512 bajtów	211.589 ms	206.818 ms
	1 452 bajty	214.031 ms	220.717 ms
sydney.edu.au	64 bajty	403.729 ms	398.371 ms
	512 bajtów	412.794 ms	399.178 ms
	1 452 bajty	408.332 ms	408.240 ms

Wyniki wskazują na to, że czas propagacji nie jest zależny od rozmiaru pakietu. Również fragmentacja zdaje się nie wpływać na czas propagacji. Warto podkreślić, że mimo stu prób wyniki takiego samego wywołania potrafiły znacząco się różnić, co tym bardziej sugeruje, że z fragmentacją i wielkością pakietu nie wiąże się żadna tendencja zmiany czasu.

3.4 Sieci wirtualne a liczba węzłów na trasie

Przykładem tras prowadzących przez sieci wirtualne są na przykład połączenia z serwerami ulokowanymi w Chinach, umieszczonymi za tzw. Wielkim Firewallem. Takie trasy mogą charakteryzować się nienaturalnie dużą liczbą węzłów w stosunku do odległości. Dla domeny taobao.com zlokalizowanej w Hangzhou – około 8200 km od Wrocławia – uzyskaliśmy minimalnie 38 skoków "do" (natomiast w kolejnej próbie, dzień później, nawet 43), a ttl uzyskanej odpowiedzi wynosił 1 – jest to zjawisko raczej niespotykane w przypadku "normalnych" tras. Próba odkrycia ścieżki z pomocą programu Traceroute okazała się wątpliwym sukcesem – od pewnego momentu w wywołaniu figurują głównie znaki '*'. Tego typu sposób działania serwerów może mieć na celu ukrycie struktury topologicznej chińskiej sieci.

```
$ ping -t38 taobao.com
PING taobao.com (140.205.94.189) 56(84) bytes of data.
64 bytes from 140.205.94.189 (140.205.94.189): icmp_seq=1 ttl=1 time=351 ms

$ traceroute taobao.com
traceroute to taobao.com (140.205.220.96), 30 hops max, 60 byte packets
    (...) // poczatek podobny do typowego wywolania programu
 7  GM-FF-FRK-F-1.163.chinatelecomeurope.com (80.81.194.33)  56.837 ms
    ancotel.GM-FF-FRK-F-2.163.chinatelecomeurope.com (80.81.195.33)  61.127 ms
    GM-FF-FRK-F-1.163.chinatelecomeurope.com (80.81.194.33)  67.834 ms
    (...) // ciag adresow ip bez domen, ale dalej uzyskujemy odpowiedzi
16  116.251.117.181 (116.251.117.181)  306.790 ms
    116.251.117.177 (116.251.117.177)  309.605 ms
    140.205.58.13 (140.205.58.13)  408.959 ms
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

4 Podsumowanie

Wykonane testy pozwalają ustalić, że wielkość pakietu nie wpływa znacząco na liczbę węzłów ani czas propagacji. Podobnie znikomy wpływ na te wartości wykazuje fragmentacja. Na podstawie testu odległości możemy zatem wywnioskować, że "fizyczna" średnica internetu wynosi przynajmniej 32 węzły (ale prawdopodobnie niewiele więcej). Test połączenia z serwerem w Chinach sugeruje, że nienaturalnie wysokie liczby węzłów mogą implikować przebieg trasy przez sieci wirtualne.
Wykorzystane programy umożliwiają zdobycie podstawowej wiedzy na temat mechanizmów działania sieci komputerowych i zarządzania pakietami. Z całą pewnością stanowią także użyteczne narzędzia do ich kontroli i analizy.