Politechnika Wrocławska
Wydział Podstawowych Problemów Techniki

TECHNOLOGIE SIECIOWE
SPRAWOZDANIE Z LABORATORIUM

Lista 1

Autor:
Jakub Duda
II rok Inf.
indeks: 236778

Prowadzący:
dr inż. Łukasz Krzywiecki

Wrocław, 21 luty 2018

1. Cel

Celem zajęć laboratoryjnych jest przetestowanie działania i analiza programów Traceroute oraz WireShark oraz dokładne zapoznanie się z programem Ping poprzez badanie wyników wywołań. Sprawdzenie ilości węzłów na trasie do odległych i bliskich geograficznie serwerów, zbadanie jaki wpływ na to ma konieczność fragmentacji pakietów i wielkość pakietu.

2. Realizacja

Zadanie będziemy realizować w systemie linuxowym wpisując odpowiednie polecenia do terminala i analizując przychodzące odpowiedzi dla programów takich jak ping i tracerout. W przypadku programu WireShark korzystać będziemy z graficznego interfejsu.

2.1 PING

- **TTL – węzły**

Sprawdzenie ilości węzłów na trasie do (i od) odległego serwera znajdującego się w Nowej Zelandii odbywa się za pomocą wywołania polecenia „ping **www.tvnz.co.nzco.nz”**. Liczbę węzłów na trasie możemy odczytać dzięki ttl(Time to live) w naszym przypadku wynosi on 236, więc na trasie od pakiet przebywa 20 węzłów ponieważ najbliższą potęgą dwójki jest 256 i z taki ttl został nadany pakiet Echo Replay z każdym węzłem ttl zostało zmniejszane o 1. Następnie wywołujemy to samo tylko z flagą -t <liczba ttl> ustawiając odpowiednią liczbę ttl w przypadku odpowiedzi serwera zmniejszamy ttl a gdy otrzymamy odpowiedz „Time to live exceeded” zwiększamy ttl. W moim przypadku odpowiedz dostałem gdy ustawiłem ttl=18. Dzięki czemu możemy wnioskować że droga do wynosi 18 węzłów a droga z wynosi o 2 węzły więcej. Następnie badamy wpływ wielkości wysyłanego pakietu na czas propagacji i drogę do i z.

ping www.tvnz.co.nz						-s 24			-s 16376		
Bytes	From	IP	SEQ	TTL	TIme	Bytes	ttl	time	Bytes	ttl	time
64	cmsprod2.tvnz.co.nz	103.231.157.164	1	236	326	32	236	312	16384	236	1023
64	cmsprod2.tvnz.co.nz	103.231.157.164	2	236	328	32	236	336	16384	236	1003
64	cmsprod2.tvnz.co.nz	103.231.157.164	3	236	331	32	236	346	16384	236	1011
64	cmsprod2.tvnz.co.nz	103.231.157.164	4	236	324	32	236	361	16384	236	938
64	cmsprod2.tvnz.co.nz	103.231.157.164	5	236	324	32	236	321	16384	236	1021

Analizując powyższe wyniki możemy dojść do wniosku że wielkość pakietu nie ma wpływu na długość drogi ponieważ dla różnych wielkości pakietu liczba ttl była taka sama zmieniał się natomiast czas propagacji, a dokładnie zwiększył się on dla większych pakietów.

Następnie podobnie sprawdzaliśmy programem ping serwery bliskich geograficznie.

ping www.wp.pl						-s 24			-s 16376		
Bytes	From	IP	SEQ	TTL	TIme	Bytes	ttl	time	Bytes	ttl	time
64	www.wp.pl	212.77.98.9	1	57	32.2	32	57	32.1	16384	57	51.8
64	www.wp.pl	212.77.98.9	2	57	28.7	32	57	24.0	16384	57	58.3
64	www.wp.pl	212.77.98.9	3	57	27.4	32	57	22.5	16384	57	54.4
64	www.wp.pl	212.77.98.9	4	57	31.1	32	57	34.1	16384	57	88.3
64	www.wp.pl	212.77.98.9	5	57	30.4	32	57	24.8	16384	57	52.4

- **Fragmentacja**

Największy niedefragmentowany pakiet jaki udało mi się wysłać miał rozmiar 55850b.

```
 ping -c 10 -s 55842 www.checkpoint.com
PING e14576.dscg.akamaiedge.net (104.81.226.207) 55842(55870) bytes of data.
55850 bytes from a104-81-226-207.deploy.static.akamaitechnologies.com
(104.81.226.207): icmp_seq=6 ttl=58 time=70.6 ms

--- e14576.dscg.akamaiedge.net ping statistics ---
10 packets transmitted, 1 received, 90% packet loss, time 9161ms
rtt min/avg/max/mdev = 70.617/70.617/70.617/0.000 ms
```

```
 ping -c 5 -s 1000 -M do eska.pl
PING eska.pl (212.180.238.58) 1000(1028) bytes of data.
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=1 ttl=56 time=17.7 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=2 ttl=56 time=17.7 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=3 ttl=56 time=16.8 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=4 ttl=56 time=18.8 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=5 ttl=56 time=15.8 ms

--- eska.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 15.846/17.398/18.839/1.022 ms
```

```
 ping -c 5 -s 1000 -l 1 eska.pl
PING eska.pl (212.180.238.55) 1000(1028) bytes of data.
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=1 ttl=57 time=16.8 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=2 ttl=57 time=17.5 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=3 ttl=57 time=16.4 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=4 ttl=57 time=18.6 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=5 ttl=57 time=18.9 ms

--- eska.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 16.487/17.698/18.984/0.987 ms
```

```
ping -c 5 -s 1000 -l 3 eska.pl
PING eska.pl (212.180.238.55) 1000(1028) bytes of data.
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=1 ttl=57 time=31.7 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=2 ttl=57 time=31.8 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=3 ttl=57 time=31.8 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=4 ttl=57 time=33.1 ms
1008 bytes from 212.180.238.55 (212.180.238.55): icmp_seq=5 ttl=57 time=15.7 ms

--- eska.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 15.798/28.863/33.136/6.556 ms, pipe 3
```

```
 ping -c 5 -s 1000 -l 5 eska.pl
PING eska.pl (212.180.238.58) 1000(1028) bytes of data.
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=1 ttl=56 time=39.2 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=2 ttl=56 time=40.4 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=3 ttl=56 time=40.7 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=4 ttl=56 time=40.7 ms
1008 bytes from 212.180.238.58 (212.180.238.58): icmp_seq=5 ttl=56 time=31.0 ms

--- eska.pl ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 31.095/38.467/40.790/3.738 ms, pipe 4
```

W pierwszej próbie wysłane zostały pakiety wielkości 1000 bajtów z zastrzeżoną fragmentacją, średni czas przesyłu w tej próbie wynosi 17.39 ms. W drugiej próbie wymuszona została fragmentacja pakietów na 1, średni czas propagacji wyniósł:17.69 ms. Trzecia próba to fragmentacja na 3, gdzie średni czas to 28.86 .Ostatnia próba to fragmentacja na 5, średni czas przesyłu to 38.46 ms. Obserwacje: Czas przesyłu pojedynczego pakietu rośnie wraz ze zwiększeniem liczby pakietów po fragmentacji. Wniosek: Podział pakietu ma wpływ na czas jego przesyłu, na im więcej elementów jest dzielony tym czas większy, ponieważ dużo czasu zabiera samo fragmentowanie większych pakietów.

- ## Cloud Computing

Sieci wirtualne Większe wartości uzyskano tylko na stronach chińskich, gdzie wartości te mogą sięgać nawet 45 węzłów. Większość stron z Chin napotkanych podczas testów jest tak odległa, może to wskazywać na to że w Chinach istnieje sieć wirtualna gdzie droga jaką pokonują pakiety może być celowo wydłużana. Kolejną rzeczą która wskazuje na istnienie takiej sieci w Chinach jest to, że tamtejsze strony najszybciej blokowały możliwość wysyłania pakietów („pingowanie”), zdarzyło się to już nawet przy 4-5 próbach.

2.2 Tracerout

Jest programem służącym do badania tras pakietów, przetestuje działanie trasy na podstawie strony cs.pwr.pl wpisując w terminal następujące polecenie traceroute cs.pwr.edu.pl

```
 $ 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)  0.942 ms  5.174 ms  5.467 ms
 2  10.10.57.1 (10.10.57.1)  5.892 ms  12.319 ms  13.588 ms
 3  ws-zlot6-brze39.siec.internetunion.pl (188.121.30.237)  7.484 ms  7.861 ms
12.023 ms
 4  188.121.31.51 (188.121.31.51)  7.798 ms ws-gajo1-
zlot6.siec.internetunion.pl (188.121.31.49)  11.931 ms  11.918 ms
 5  fo-zlot-cg2-30-253.net.internetunion.pl (188.121.30.253)  7.732 ms  7.716
ms  11.645 ms
 6  v210.core1.waw1.he.net (216.66.87.145)  22.495 ms  26.044 ms  27.511 ms
 7  100ge11-2.core1.vie1.he.net (184.105.65.73)  37.825 ms  30.635 ms  36.665
ms
 8  vie-ix.geant.net (193.203.0.172)  34.599 ms  35.833 ms  35.515 ms
 9  ae3.mx1.poz.pl.geant.net (62.40.98.48)  62.428 ms  59.519 ms  58.380 ms
10  pionier-ias-pionier-gw-1.poz.pl.geant.net (83.97.88.122)  59.080 ms  59.068
ms  59.399 ms
11  z-poznan-gw3.wroclaw.10Gb.rtr.pionier.gov.pl (212.191.224.106)  62.342 ms
64.065 ms  63.628 ms
12  rolnik2-centrum.wask.wroc.pl (156.17.254.65)  74.544 ms  76.304 ms  74.351
ms
13  wazniak-rolnik.wask.wroc.pl (156.17.254.140)  73.990 ms  72.768 ms  73.243
ms
14  z-wask2-do-pwr2.pwrnet.pwr.wroc.pl (156.17.18.244)  62.377 ms  69.324 ms
63.393 ms
15  156.17.33.1 (156.17.33.1)  69.585 ms  63.633 ms  69.502 ms
16  informatyka.im.pwr.wroc.pl (156.17.7.22)  69.087 ms  69.395 ms  69.036 ms
```

Wynik ukazuję drogę jaką przebywa pakiet z wysyłanego komputera (dostawca sieci internetunion) do serwerów pwr .
Analizując wyniki uzyskujemy informacje przez jakie drogę przechodzi pakiet. Program korzysta z programu ping. Czasami możemy uzyskać następujący wynik który jest znakiem * oznacza to brak odpowiedzi na zadany pakiet i może wynikać z przeciążenia sieci, routera bądź z celowej konfiguracji urządzeń (ustawienia firewalla). W takim przypadku możemy korzystać z z czasu między kolejnymi krokami i na ich podstawie możemy wywnioskować większe odległości geograficzne takie jak np. Oceany. Jeśli router zostanie tak skonfigurowany żeby nie zmniejszać wartości ttl przetwarzanych pakietów, to nie będzie widoczny przez traceroute ponieważ program ten korzysta z programu ping w następujący sposób pinguję stronę z ttl=1 router zmniejsza wartość do 0 i wysyła komunikat ICMP "Time Exceeded" następnie powtarzamy czynność ale tym razem z ttl=2 gdy pakiet dotrze do kolejnego routera sytuacja się powtórzy.

2.3 WireShark

Wireshark- jest snifferem, umożliwia więc on na przechwytywanie i nagrywanie pakietów danych a także ich dekodowanie.



Przyciskając który znajduje się w górnym prawym rogu zaczynamy nadsłuchiwanie obok pojawi się ikonka zakończenia nadsłuchiwania oraz ikonka restartowania nadsłuchiwania. W polu poniżej możemy wpisać filtry czyli możemy wyświetlić protokoły które nas interesują w moim przypadku będzie to protokół ICMP następnie w konsoli uruchomiłem poleceniem ping cs.pwr.edu.pl -c 4 program ping w Wiresharku pojawiły się wyszukane protokoły ICMP liczba ich jest równa 8 ponieważ zostały wysłane 4 protokoły Echo request i cztery powrotne Echo Replay. Ważne jest aby logując się lub gdziekolwiek wpisując jakieś dane wrażliwe zwracać uwagę na to strona używa (https) ponieważ w innym wypadku nasze dane będą łatwo dostępne jeśli ktoś je przechwyci. Https mówi nam czy strona używa protokołu ssl co jest bezpieczne dla naszych danych ponieważ przesyłane dane są zaszyfrowane.

3 Wnioski

Zaprezentowane programy służą do śledzenia pakietów, dzięki czemu możemy badać sieć to jak jest zbudowana. W głównej mierze powyższe programy są wykorzystywane przez administratorów sieci, służby specjalne oraz hakerów do śledzenia pakietów i zbierania informacji o routerach.