Marcel Jerzyk

Technologie Sieciowe

08.03.2019

Wstęp do Technologii Sieciowych

1. *Wprowadzenie*

Celem jest przetestowanie trzech programów: ping, wireshark oraz traceroute. Ich wspólną cechą jest możliwość analizowania pakietów wychodzących i przychodzących. Między innymi zajmiemy się wątkiem określania „średnicy Internetu", sprawdzenia, co się dzieje przy próbie kontaktu z siecią w Chińskiej Republice Ludowej oraz wpływem wielkości pakietu i ich fragmentacji na czas propagacji.

2. *Ping*

Narzędzie systemowe ping, które można wywołać w command prompt'cie głównie wykorzystywane jest w celu sprawdzenia czy komputer jest w stanie dostać sygnał zwrotny z wybranego serwera, czyli innymi słowy – czy jest w stanie się z nim połączyć. Działanie programu jest „genialne w swej prostocie", a mianowicie wysyła sygnał ICMP („Internet Control Message Protocol"), tzw. Echo Request i czeka na odpowiedź. To jak wiele z nich wróci oraz to jak długo im zajmuje powrót do komputera wysyłającego sygnał to dwie najważniejsze informacje, które ten program dostarcza użytkownikowi.

Zaczynając testowanie narzędzia pierwsze, co przychodzi do głowy to wybranie prawdopodobnie najbardziej znanego wszystkim serwera – „ping *google.com"*.

```
C:\Users\Luzkan>ping google.com

Pinging google.com [172.217.20.78] with 32 bytes of data:
Reply from 172.217.20.78: bytes=32 time=40ms TTL=53
Reply from 172.217.20.78: bytes=32 time=41ms TTL=53
Reply from 172.217.20.78: bytes=32 time=37ms TTL=53
Reply from 172.217.20.78: bytes=32 time=36ms TTL=53

Ping statistics for 172.217.20.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 36ms, Maximum = 41ms, Average = 38ms
```

Obrazek 1: ping google.com

Zauważyć można, że uzyskaliśmy 4 odpowiedzi z adresu 172.217.20.78, który krył się pod wybraną nazwa serwera. Nie zostały użyte, żadne sufixy, a także „-l”, który odpowiada za żądaną wielkość (w bajtach) odpowiedzi zwrotnej z serwera. Największa możliwa wartość, którą można ustawić to 65,527, a najmniejszą, a zarazem domyślną, jest 32, którą widać na *„Obrazek 1”*. Następną wartością jest time, która informuje, jaki czas zajął pakietom powrót. W tym wypadku widać, że zajęło to średnio 38ms, czego podsumowanie mamy na dole konsoli wraz z innymi statystykami. Ostatnią wartość jest TTL, czyli Time to Live – jest to liczba skoków, po której przekroczeniu router, który otrzyma pakiet po prostu do odrzuci..., ale jaki router?

Sieć ma ograniczony zasięg i na obecną chwilę nie ma kabla, który połączyłby cały glob dając możliwość bezpośredniego dostępu od hosta A do hosta B bez pośrednictwa innych routerów. Dlatego TTL informuje nas jak wiele routerów „dzieli” Hosta A od Hosta B.

Obrazek 2: TTL

To prowadzi do ciekawego pytania „jak długi jest Internet”. Zbadajmy to pingując różne serwery na globie (naszą lokacją jest Wrocław) używając domyślnej konfiguracji ping’a.

Serwer	Czas	TTL	Miejsce Serwera*
gov.lk	Timed out.	ND	Colombo (Sri Lanka)
falklandislands.com	Timed out.	ND	Falklandy (Malwiny)
statssa.gov.za	Timed out.	ND	Cape Town (RPA)
argentina.gob.ar	Timed out.	ND	Buenos Aires (Argentyna)
gov.sg	Timed out.	ND	Singapur (Singapur)

Tabela 1: próby połączeń z różnymi serwerami

Request timed out informuje nas, że nie otrzymaliśmy w ogóle odpowiedzi zwrotnej z serwera. Może to oznaczać kilka rzeczy: serwer stoi za zaporą sieciową, która odrzuca pakiety, opcja ping została wyłączona na serwerze przez administratora systemu albo po prostu serwer jest akurat wyłączony. Potestujmy dalej w poszukiwaniu serwerów, które kwapią się wysłać odpowiedź zwrotną.

Serwer	Czas	TTL	Miejsce Serwera*
Christchurchnz.com	325ms	110	Auckland (Nowa Zelandia)
gov.ph	184ms	42	Montreal (Kanada)
chinhphu.vn	371ms	44	Ho Chi Minh (Wietnam)
argentina.gob.ar	410ms	39	Asunción (Paragwaj)
uchile.cl	481ms	45	Santiago (Chile)

Tabela 2: udane próby połączeń

Po ciężkich poszukiwaniach znalazło się parę serwerów rozlokowanych całkiem daleko na globie w stosunku do Wrocławia. Najwięcej skoków wystąpiło podczas połączenia z serwerem w Paragwaju – aż 25, lecz jak widać wcale to nie oznacza, że właśnie tam pakiety musiały odbyć najdłużej trwającą podróż, ponieważ pakiety z Chile musiały iść aż (albo raczej tylko) prawie 0,5s. Należy pamiętać, że pakiety nie muszą wędrować w obie strony tą samą drogą – mogą wybrać inną drogę, a co za tym idzie – przejść przez inną liczbę routerów DO, a inną Z.

Można powiedzieć, że tak, jak aby skontaktować się z dowolnym człowiekiem na Ziemi wystarczy około 7 wymian telefonów w relacji <znajomy-znajomy znajomego>, tak by połączyć się z dowolnym punktem na Ziemi potrzeba około 25 routerów pośredniczących.

Wróćmy do googlowskiego serwera z początku tego rozdziału (*obrazek 1*). Zbadajmy jak wielkość pakietu jak i fragmentacja wpływa na to, co się wydarzy. Komenda –l odpowiada za pierwsze, a –f za fragmentacje. Dodam, że z racji przeniesienia lokalizacji komputera i korzystaniu z LTE zamiast światłowodu czasy będą inne niż na początku.

Zmienna	Wartość	Czas z Fragmentacji	Czas bez Fragmentacji
-l	32	84	156
-l	128	98	174
-l	1024	200	260
-l	2048	Timed out	Packets need to be fragmented.
-l	4096	Timed out.	Packets need to be fragmented.

Tabela 3: pingowanie google.com [LTE]

W celu usystematyzowania wyników ponowne pomiary na łączu kablowym.

Zmienna	Wartość	Czas z Fragmentacją	Czas bez Fragmentacji
-l	32	17	19
-l	128	18	20
-l	1024	18	20
-l	2048	Timed out	Packets need to be fragmented.
-l	4096	Timed out.	Packets need to be fragmented.

Tabela 4: pingowanie google.com [Ethernet]

Ostatnim serwerem, który poddamy testom, będzie ten zlokalizowany w Chile.

Zmienna	Wartość	Czas z Fragmentacją	Czas bez Fragmentacji
-l	32	264	266
-l	128	266	264
-l	1024	264	266
-l	2048	Timed out	Packets need to be fragmented.
-l	4096	Timed out.	Packets need to be fragmented.

Tabela 5: pingowanie uchile.cl [Ethernet]

Jak widać, na kablu o szybkim łączu światłowodowym wielkość pakietu oraz fragmentacja nie ma żadnego wpływu (granica błędu statystycznego) na czas, czy to na serwerze względnie bliskim (Frankfurt, Niemcy – google.com), czy też na serwerze położonym bardzo daleko geograficznie. Ciekawiej wygląda sprawa, gdy łączymy się za pomocą LTE, w miejscu, w którym jednocześnie z niego korzysta lekko tysiące osób w r < 1km. Podwójny test wskazał, że brak fragmentacji znacząco wydłużał czas (około 1.5 razy). Zaobserwowane zostało także wydłużenie czasu przy większej ilości bajtów.

Warto zaznaczyć, że maksymalna wartość „–l", na którą odpowiadał serwer to 1472 (bytes) – pofragmentowany jak i nie.

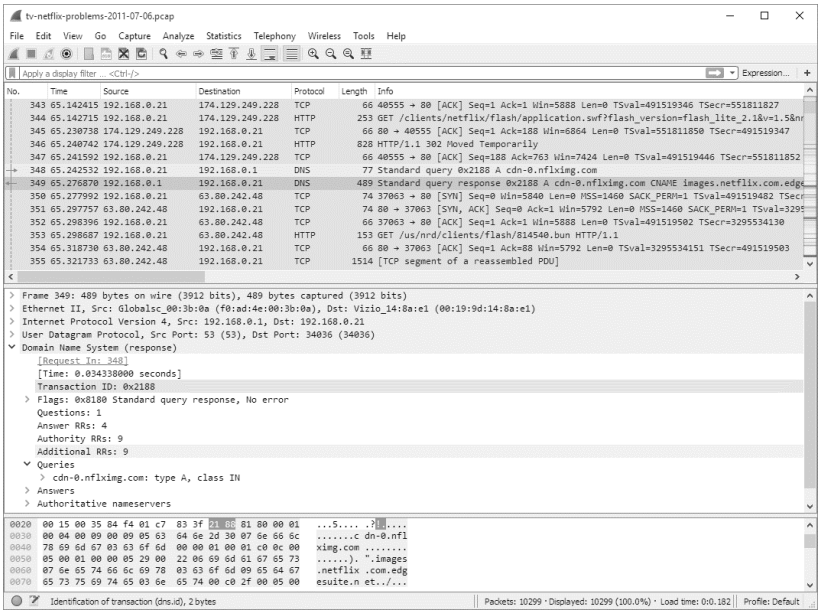
Ostatnim wartym sprawdzenia zagadnieniem jest próba ping'u na serwerach należących do Chińskiej Federacji Ludowej, które używają sieci wirtualnych do pokazywania „przyfalszowanych" TTL dzięki nabijaniu skoków na „wirtualnych routerach". Nie zadziała to na stronie rządowej, ponieważ ta jest umieszczona na serwerach we Francji, ale już na popularnym w chinach sklepie internetowym taobao.com. Utrudnia to badanie infrastruktury Internetowej tamtejszego państwa.

*W celu analizy położenia lokalizacji serwerów geograficznie została użyta strona https://check-host.net/, dzięki temu nie ma pomyłek w tekście typu jak test na stronie rządowej jakiegoś państwa, która ma serwery daleko poza granicami swojego kraju.

3. *Wireshark*

Wireshark jest jednym z popularniejszych narzędzi do analizy sieci. Ma bardzo dużą funkcjonalność, a więc szereg zastosowań, dzięki czemu z chęcią wykorzystywany jest przez sysadminów, służby, hackerów czy zwykłych użytkowników. Tak szerokie spektrum grup, które używają tego programu Wireshark zawdzięcza poza swoją funkcjonalnością także dzięki prostocie obsługi, łatwości instalacji, interfejsie graficznym jak i konsolowym.

Program ten analizuje ruch sieciowy i konwertuje go w łatwy do przeanalizowania przez człowieka format. Łatwo jest przez to zidentyfikować cały ruch w sieci, częstotliwość, wielkość, czasy oczekiwań (ang. latency) pomiędzy skokami itd. Dodatkowo wbudowane są filtry,



Obrazek 3: WireShark GUI

które jeszcze bardziej ułatwiają analizę np.: w dużych korporacjach, czy też gdy np. użytkownik chce przeanalizować pracę jakiegoś danego programu.

Zbiera on wszystkie pakiety wychodzące i przychodzące „na żywo”, ale również potrafi posłużyć się już takimi zebranymi wcześniej.

W moim przypadku Wireshark przydał się, w celu przeanalizowania pracy programu, który był według mnie był podejrzany ze względu na spowolnienie łącza, jak i komputera. Prostym sposobem dało się sprawdzić, że program wysyła gigantyczną ilość pakietów do serwera

nieznanego mi pochodzenia i to prawie, że natychmiastowo podczas startu aplikacji aż do jej wyłączenia. To na pewno nie było zadaniem tego programu, więc w ten sposób dowiedziałem się, że to nie komputer czy Internet nie jest w stanie utrzymać jakiegoś przeciążenia, a po prostu program tworzył z mojego PC coś w stylu bota, który wykonywał niechciane akcje.

4. Traceroute

Powrót do korzystania z konsoli systemowej. Traceroute to kolejny program do badania pakietów – tym razem do śledzenia ich trasy w sieci IP. W systemach Windowsowych znajdziemy go pod nazwą „tracert". Główna zasada działania polega na stopniowym zwiększeniu TTL o jeden w celu identyfikacji wszystkich routerów na trasie (zaczynając od 1 każdy kolejny router będzie odrzucał i wysyłał informację zwrotną - w ten sposób uzyskuje się jego adres IP). W skrócie to narzędzie pokaże przegląd drogi, jaką pokona komputer do danego serwera.

```
C:\Users\Luzkan>tracert 185.40.65.1

Tracing route to 185.40.65.1 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  192.168.0.1
  2    10 ms    13 ms     8 ms  89-79-100-1.dynamic.chello.pl [89.79.100.1]
  3    14 ms     7 ms    10 ms  89-75-12-1.infra.chello.pl [89.75.12.1]
  4    32 ms    32 ms    29 ms  pl-wro02a-ra2-ae0-1430.aorta.net [84.116.253.210]
  5    26 ms    33 ms    28 ms  pl-ktw01a-rc1-ae17-2120.aorta.net [84.116.253.206]
  6    26 ms    29 ms    34 ms  de-fra04d-rc1-ae30-0.aorta.net [84.116.137.41]
  7    33 ms    26 ms    29 ms  de-fra04c-ri1-ae9-0.aorta.net [84.116.140.190]
  8     *       29 ms    30 ms  213.46.177.58
  9     *        *       31 ms  104.160.142.44
 10     *       38 ms    36 ms  ae-30.br02.ams02.riotdirect.net [104.160.159.54]
 11    36 ms    39 ms    37 ms  104.160.141.103
 12    37 ms    35 ms    35 ms  104.160.141.107
 13     *       38 ms    38 ms  104.160.141.107
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
```

Obrazek 4: tracert

Z tym narzędziem korzysta się w celu diagnostyki trasy. Jest to bardzo proste:

- Pierwsza linijka tekstu opisuje efekt polecenia „śledzenie połączenia do <IP>".
- Każda kolejna linia wyświetla 3 wartości, które opisują czas potrzebny na dostarczenie pakietu danych do punktu przeskoku i z powrotem (tzw. Round Trip time). Każdy przeskok wykonywany jest trzy razy

- Jeżeli wartość oznaczona jest gwiazdką „*”, oznacza to, że pakiet danych nie wrócił do komputera w wyznaczonym czasie. Jedna lub dwie gwiazdki nie oznaczają jeszcze utraty całego pakietu, ale już trzy – informują o przekroczonym czasie oczekiwania (np.: połączenie jest blokowane przez zaporę albo zabezpieczenie sieciowe).

5. Podsumowanie

Zadania wykonane przy tych programach dają pojęcie na temat tego jak wygląda wymiana pakietów pomiędzy komputerami podłączonymi do sieci oraz w jaki sposób komputery/serwery są połączone pomiędzy sobą; to, w jaki sposób są w stanie między sobą się komunikować i jak można badać połączenie na własną ręką z pomocą w/w programów.