Politechnika Wrocławska

Anna Modrzejewska

Sprawozdanie nr 1

Technologie Sieciowe

16 października 2018

1 Cel

Przetestowanie działania programów Ping, Traceroute, WireShark. Za pomocą programu Ping: sprawdzenie liczby węzłów do i od geograficznie odległego serwera; zbadanie wpływu wielkości oraz konieczności fragmentacji pakietów; znalezienie największego niefragmentowanego pakietu, który uda się przesłać; przeanalizowanie tych samych rzeczy dla serwerów bliskich geograficznie; znalezienie tras przebiegających przez sieci wirtualne oraz określenie długości ścieżek w tym przypadku.

2 Realizacja

2.1 Ping

Ping to program służący do badania połączeń sieciowych. Wysyła zapytania echo do serwera i oczekuje na odpowiedź. Umożliwia on sprawdzenie, czy istnieje połączenie między użytkownikiem a testowanym serwerem. Ponadto można zmierzyć liczbę zgubionych pakietów oraz opóźnienie w ich przesyłaniu. Jako parametr dla programu należy podać adres IP lub nazwę badanego serwera oraz opcjonalnie flagi:

$-n$ ustawienie liczby wysłanych pakietów

$-l$ wyznaczenie rozmiaru pakietu

$-f$ ustawienie w pakiecie flagi „Nie fragmentuj”

$-i$ ustalenie początkowej wartości TTL wychodzących pakietów

Przykładowe wywołanie:

```
C:\Users\Damian>ping pl.wikipedia.org -n 3

Badanie pl.wikipedia.org [91.198.174.192] z 32 bajtami danych:
Odpowiedź z 91.198.174.192: bajtów=32 czas=50ms TTL=52
Odpowiedź z 91.198.174.192: bajtów=32 czas=48ms TTL=52
Odpowiedź z 91.198.174.192: bajtów=32 czas=48ms TTL=52

Statystyka badania ping dla 91.198.174.192:
    Pakiety: Wysłane = 3, Odebrane = 3, Utracone = 0
             (0% straty),
Szacunkowy czas błądzenia pakietów w millisekundach:
    Minimum = 48 ms, Maksimum = 50 ms, Czas średni = 48 ms
```

Można dzięki temu dowiedzieć się między innymi: jaki jest numer IP badanego serwera, łączny czas wysłania i odebrania pakietu oraz ile routerów pakiet przeszedł. To ostatnie można policzyć na podstawie wartości TTL - w tym przypadku początkowa wartość TTL ustawiona jest na 63 (taka procedura zapobiega błądzeniu pakietu w sieci w przypadku błędów połączeń). Podczas przechodzenia pakietu przez router wartość TTL zmniejszana jest o 1. W tym wywołaniu końcowa wartość TTL wynosi 52, co oznacza, że pakiet przeszedł przez $63 - 52 = 11$ routerów.

2.1.1 Liczba skoków od odległego miejsca

120.138.22.174 - numer IP serwera położonego w Australii

```
Odpowiedź z 120.138.22.174: bajtów=32 czas=303ms TTL=39
```

TTL odbieranych pakietów wynosi 39, początkowa wartość wynosiła 63. Zatem odległość od serwera wynosi $63 - 39 = 24$ węzłów.

2.1.2 Liczba skoków do odległego miejsca

95.141.39.238 - numer IP serwera położonego w Nowej Zelandii

```
C:\Users\Damian>ping 95.141.39.238
Odpowiedź z 95.141.39.238: bajtów=32 czas=51ms TTL=50

C:\Users\Damian>ping 95.141.39.238 -i 10
Odpowiedź z 95.141.39.238: bajtów=32 czas=49ms TTL=50

C:\Users\Damian>ping 95.141.39.238 -i 9
Upłynął limit czasu żądania.
```

W tym przypadku długość drogi od serwera wynosi 13 węzłów. Natomiast długość do serwera można stwierdzić za pomocą ustawienia flagi $-i$ (ustawienie początkowej wartości TTL). Przy wartości $TTL = 10$ pakiet zostanie odebrany, a przy $TTL = 9$ nie. Zatem długość do serwera to 10 węzłów. Wynika z tego, że pakiety mogą być wysyłane i odbierane różnymi ścieżkami, w tym przypadku różnią się długością o 3 węzły.

2.1.3 Wpływ rozmiaru pakietu na drogę pakietu od odległego miejsca

Największy możliwy rozmiar pakietu do wysłania wynosi $65500B$, próba przesłania większego pakietu nie zostanie zrealizowana:

```
C:\Users\Damian>ping 120.138.22.174 -l 65500
Odpowiedź z 120.138.22.174: bajtów=65500 czas=412ms TTL=39

C:\Users\Damian>ping 120.138.22.174 -l 65501
Zła wartość dla opcji -l, właściwy zakres: od 0 do 65500.
```

Można zauważyć, że w przypadku przesyłania maksymalnie dużego pakietu wartość TTL pozostała taka sama, jak przy standardowym rozmiarze ($32B$), zatem rozmiar nie wpłynął na długość drogi pakietu od odległego miejsca.

2.1.4 Wpływ blokady fragmentacji pakietu na drogę pakietu od odległego miejsca

Największy możliwy rozmiar niefragmentowalnego pakietu do wysłania wynosi $1472B$, próba przesłania większego pakietu nie zostanie zrealizowana z opcją blokowania fragmentacji:

```
C:\Users\Damian>ping 120.138.22.174 -f
Odpowiedź z 120.138.22.174: bajtów=32 czas=310ms TTL=39

C:\Users\Damian>ping 120.138.22.174 -f -l 1472
Odpowiedź z 120.138.22.174: bajtów=1472 czas=369ms TTL=39

C:\Users\Damian>ping 120.138.22.174 -f -l 1473
Pakiet musi być podzielony na fragmenty, ale ustawiono opcję DF.
```

Można zauważyć, że blokada fragmentacji, podobnie jak rozmiar pakietu, nie wpływa na wartość TTL, czyli na długość drogi pakietu od serwera.

2.1.5 Odczyty dla bliskiego geograficznie miejsca

onet.pl, pl.wikipedia.org - domeny internetowe z serwerami położonymi w Polsce

```
C:\Users\Damian>ping onet.pl
Odpowiedź z 213.180.141.140: bajtów=32 czas=15ms TTL=55
```

```
C:\Users\Damian>ping pl.wikipedia.org
Odpowiedź z 91.198.174.192: bajtów=32 czas=54ms TTL=52
```

W obu przypadkach pakiety mają większą wartość TTL niż w przypadku wysyłania pakietu do odległego serwera. Oznacza to, że pokonały krótszą drogę od serwera, w pierwszym przypadku długość 8 węzłów, w drugim - 11.

```
C:\Users\Damian>ping onet.pl -i 10
Odpowiedź z 213.180.141.140: bajtów=32 czas=12ms TTL=55

C:\Users\Damian>ping onet.pl -i 9
Odpowiedź z 213.180.152.129: Limit czasu wygaśnięcia (TTL) upłynął
podczas tranzytu.
```

Długość drogi pakietu do serwera onet.pl wyniosła 10 węzłów, czyli różniła się o 2 węzły od drogi z powrotem.

```
C:\Users\Damian>ping onet.pl -l 65500
Odpowiedź z 213.180.141.140: bajtów=65500 czas=114ms TTL=55
```

TTL nie zmienił się w przypadku dużego pakietu.

2.1.6 Wpływ blokady fragmentacji pakietu na drogę pakietu do bliskiego miejsca

```
C:\Users\Damian>ping onet.pl -f
Odpowiedź z 213.180.141.140: bajtów=32 czas=15ms TTL=55

C:\Users\Damian>ping onet.pl -f -l 1472
Odpowiedź z 213.180.141.140: bajtów=1472 czas=15ms TTL=55

C:\Users\Damian>ping onet.pl -f -l 1473
Pakiet musi być podzielony na fragmenty, ale ustawiono opcję DF.
```

TTL nie zmienił się w przypadku blokady fragmentacji. Rozmiar maksymalnego niefragmentowalnego pakietu również nie uległ zmianie.

2.1.7 Great FireWall of China

"Wielka Zapora Chińska" to termin stosowany do działań Chińskiej Republiki Ludowej, by kontrolować Internet. Ich celem jest zablokowanie dostępu do niektórych zagranicznych stron oraz opóźnienie ruchu w Internecie np. poprzez blokowanie adresów IP, filtrowanie URL czy pakietów. Po wysłaniu pakietu do chińskiego serwera otrzymamy daleką od normy wartość TTL:

```
C:\Users\Damian>ping www.jiayuan.com
Odpowiedź z 59.151.22.120: bajtów=32 czas=1024ms TTL=221
```

Nie ma pewności, czy te wartości to rzeczywista liczba przebytych węzłów, czy TTL zostało sztucznie zmnienione.

2.2 TraceRoute

Traceroute to program, za pomocą którego można badać trasę pakietu w sieci. Flaga:
$-h$ ustawienie maksymalnej liczby przeskoków w poszukiwaniu celu
Przykładowe wywołanie:

```
C:\Users\Damian>tracert 120.138.22.174

Śledzenie trasy do dns-nz-02.getflix.com.au [120.138.22.174]
z maksymalną liczbą 30 przeskoków:

  1     1 ms    <1 ms    <1 ms  netiaspot.home [192.168.1.254]
  2     *        *        *     Upłynął limit czasu żądania.
  3     6 ms     5 ms    14 ms  host-87-99-33-89.internetia.net.pl

  4     2 ms     2 ms     3 ms  83.238.251.117
  5     7 ms     6 ms     6 ms  katoh001rt02.inetia.pl [87.204.225.2]
  6     7 ms     7 ms     6 ms  87.204.225.163
  7     *        *        *     Upłynął limit czasu żądania.
  8    26 ms    23 ms    23 ms  100ge11-2.core1.vie1.he.net
  9    48 ms    50 ms    48 ms  100ge13-1.core1.par2.he.net
 10   116 ms   115 ms   123 ms  100ge10-2.core1.ash1.he.net
 11   172 ms   171 ms   171 ms  100ge13-1.core1.lax1.he.net
 12   173 ms   173 ms   174 ms  100ge14-1.core1.lax2.he.net
 13   175 ms   189 ms   174 ms  vocus.10gigabitethernet5-8.lax2.he.net
 14   296 ms   296 ms   296 ms  bundle-153.cor02.lax01.ca.vocus.net
 15   294 ms   294 ms   294 ms  100g-0-1-0-0.cor01.lax01.ca.vocus.net
 16   296 ms   296 ms   296 ms  bundle-200.cor01.alb1.akl.vocus.net.nz
 17   294 ms   294 ms   294 ms  bundle-50.cor01.akl05.akl.vocus.net.nz
 18   305 ms   296 ms   305 ms  bundle-10.bdr02.akl05.akl.VOCUS.net.nz
 19   302 ms   296 ms   293 ms  as9790.bdr02.akl05.akl.VOCUS.net.nz
 20   295 ms   297 ms   296 ms  202.180.65.0
 21   315 ms   313 ms   305 ms  default-rdns.vocus.co.nz
 22   306 ms   305 ms   306 ms  ae2-11.dist1-nct1.sitehost.co.nz
 23   303 ms   307 ms   311 ms  dns-nz-02.getflix.com.au
```

Program pozwala dokładnie prześledzić, przez jakie węzły przechodzi pakiet. W tym przypadku, dążąc do nowozelandzkiego serwera, przebył trasę przez Katowice (pkt 5.), Stany Zjednoczone (pkt 8. - 13.) i Australię (pkt 14., 15.).

2.3 WireShark

WireShark to program umożliwiający przechwytywanie oraz śledzenie pakietów, a także odczytanie ruchu w sieci. Za jego pomocą można na przykład przechwycić (z tej samej sieci) dane do logowania na stronie używającej protokołu HTTP. Należy w tym celu uruchomić w programie WireShark przechwytywanie pakietów, zalogować się na niezabezpieczonej stronie, zatrzymać przechwytywanie i znaleźć pakiet z danymi do logowania - można w tym celu odfiltrować wyniki wyrażeniem *http.request.method == "POST"*.
Wynik:

No.	Source	Destination	Protocol	Info
51	192.168.1.2	91.220.17.214	HTTP	POST /personalizacja/logowanie

Następnie, po kliknięciu prawym przyciskiem myszy w otrzymany wynik, wybrać "Podążaj" → "Strumień TCP". W otworzonym dokumencie znaleźć fragment z danymi do logowania:

```
email=ania@helena.pl&password=alohomora&login=HTTP/1.1 200 OK
```

WireShark jest również użyteczny, by zobaczyć zasadę działania programu TraceRoute. Po rozpoczęciu przechwytywania pakietów w WireShark i wywołaniu programu TraceRoute z IP nowozelandzkiego serwera otrzymamy:

Source	Destination	Info
192.168.1.2	120.138.22.17	Echo (ping) request id=0x0001, seq=279/5889, ttl=1 (no response found!)
192.168.1.2	120.138.22.174	Echo (ping) request id=0x0001, seq=280/6145, ttl=1 (no response found!)
192.168.1.2	120.138.22.174	Echo (ping) request id=0x0001, seq=281/6401, ttl=1 (no response found!)
192.168.1.2	120.138.22.174	Echo (ping) request id=0x0001, seq=282/6657, ttl=2 (no response found!)
...	...	...
192.168.1.2	120.138.22.174	Echo (ping) request id=0x0001, seq=286/7681, ttl=3 (no response found!)
192.168.1.2	120.138.22.174	Echo (ping) request id=0x0001, seq=288/8193, ttl=4 (no response found!)
...	...	...
192.168.1.2	120.138.22.174	Echo (ping) request id=0x0001, seq=345/22785, ttl=23 (reply in 673)
120.138.22.174	192.168.1.2	Echo (ping) reply id=0x0001, seq=345/22785, ttl=39 (request in 672)

Można wnioskować na tej podstawie, że program TraceRoute wysyła po 3 pakiety z początkową wartością $TTL = 1$, a następnie wysyła ze zwiększoną o 1 wartością TTL, aż do czasu, gdy pakiet zostanie skutecznie wysłany do docelowego serwera. W każdym przypadku TraceRoute stwierdza, dokąd dotarł pakiet i na tej podstawie ustala jego trasę do celu.

3 Wnioski

- Ping jest przydatny do badania łączności między użytkownikiem a wybranym serwerem. Podaje informacje takie jak IP wybranego serwera, czas wysłania i odebrania pakietu, końcową wartość TTL.
- Systemy operacyjne ustawiają początkową wartość TTL, żeby zapobiec za długiemu błądzeniu pakietów w sieci.
- Liczba węzłów od serwera to różnica początkowego i końcowego TTL.
- Liczba węzłów do serwera to minimalna poczatkowa wartość TTL, przy której pakiet dotrze.
- Największy rozmiar pakietu do przesłania to 65500B, wtedy zostanie on wysłany fragmentami.
- Największy rozmiar fragmentu do wysłania to 1472B.
- Rozmiar pakietu lub zablokowanie fragmentacji nie wpływają na długość trasy pakietu od serwera.
- Pakiety wysyłane do bliskiego geograficznie serwera mają do pokonania mniej węzłów niż te wysyłane do odległych miejsc.
- TraceRotue pozwala na prześledzenie trasy pakietu.
- WireShark umożliwia przechwycenie danych z sieci, zwłaszcza niezaszyfrowane loginy i hasła, jeśli są podawane na niezabezpieczonych stronach.