Technologie Sieciowe - lista 1

Bartosz Olszewski

marzec 2025

1 Wstęp

Opis narzędzi

PING – narzędzie diagnostyczne używane do sprawdzania dostępności hosta w sieci oraz mierzenia czasu odpowiedzi. Wysyła pakiety ICMP (Echo Request) do docelowego adresu IP i oczekuje na odpowiedź (Echo Reply), podając statystyki dotyczące opóźnień i utraconych pakietów.

Przykład wywołania:

```
ping -c 1 google.com
PING google.com (142.250.186.206) 56(84) bytes of data.
64 bytes from waw07s05-in-f14.1e100.net (142.250.186.206):
    icmp_seq=1 ttl=114 time=9.50 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.496/9.496/9.496/0.000 ms
```

Otrzymujemy dane o adresie, czasie przesyłu oraz parametrze TTL pakietów zwrotnych. TTL (Time To Live) określa maksymalną liczbę węzłów, przez które może przejść pakiet – podstawowe wartości to zazwyczaj 64, 128 lub 255. Po każdym przekaźniku wartość ta jest dekrementowana, a po osiągnięciu zera pakiet nie jest już przesyłany. Dzięki poleceniu `ping` można oszacować trasę pakietu oraz zdiagnozować opóźnienia.

TRACEROUTE – narzędzie do śledzenia trasy pakietów w sieci. Pokazuje kolejne węzły (routery), przez które przechodzi pakiet od nadawcy do odbiorcy, oraz mierzy czasy odpowiedzi z każdego z nich. Używa pakietów ICMP lub UDP z rosnącym TTL, wymuszając odpowiedzi od pośrednich urządzeń.

Przykład wywołania:

```
traceroute google.com
traceroute to google.com (142.250.186.206), 30 hops max, 60 byte packets
 1  _gateway (10.138.0.1)  1.720 ms  1.631 ms  1.563 ms
 2  * * *
 3  88.220.36.153 (88.220.36.153)  4.811 ms  4.757 ms  5.874 ms
 4  88.220.196.247 (88.220.196.247)  9.734 ms  9.683 ms  10.777 ms
```

```
5  209.85.168.100 (209.85.168.100)  21.536 ms  21.477 ms  21.410 ms
6  142.251.225.169 (142.251.225.169)  13.491 ms 108.170.234.167
   (108.170.234.167)  6.839 ms 142.251.225.169 (142.251.225.169)
   10.682 ms
7  142.250.239.81 (142.250.239.81)  9.555 ms 209.85.252.117
   (209.85.252.117)  9.452 ms 142.251.239.81 (142.251.239.81)
   9.407 ms
8  waw07s05-in-f14.1e100.net (142.250.186.206)  9.371 ms  9.212 ms  11.711 ms
```

WIRESHARK – zaawansowany program służący do monitorowania ruchu sieciowego, umożliwiający przechwytywanie i szczegółową analizę pakietów. Program pozwala filtrować ruch, diagnozować problemy sieciowe i wyświetlać szczegółowe informacje, takie jak czas, źródło, cel, protokół oraz zawartość pakietów.

2 Testy praktyczne

2.1 a) Odległości serwerów

Używając metodologii opisanej w sekcji `ping` sprawdziłem odległości do różnych serwerów (dla pakietów o standardowym rozmiarze 64 bajty). Liczba skoków od serwera do nas została oszacowana na podstawie wartości TTL, a od nas do serwera przy użyciu `traceroute`. Poniższa tabela przedstawia wyniki:

Serwer	**Lokalizacja**	**Od nas**	**Od nich**	**Opóźnienie**
wcss.pl	Wrocław	9	9	4 ms
pg.edu.pl	Gdańsk	7	6	12 ms
fu-berlin.de	Niemcy	16	14	30 ms
harvard.edu	USA	5	5	32 ms
victoria.ac.nz	Nowa Zelandia	15	13	282 ms
aarnet.edu.au	Australia	29	28	323 ms

2.2 b) Wielkość pakietów a opóźnienia

Testowałem wpływ rozmiaru pakietu na opóźnienia oraz poprawność transmisji. Wyniki przedstawiono w poniższej tabeli:

Serwer	Rozmiar	Odpowiedź	TTL	Czas (średni)	Dodatkowe info
wcss.pl	64	64	9	3.7 ms	–
wcss.pl	256	256	9	3.8 ms	–
wcss.pl	1468	1468	9	12.2 ms	–
wcss.pl	1469	timeout	timeout	timeout	–
harvard.edu	64	64	5	32 ms	–
harvard.edu	256	256	5	33 ms	–
harvard.edu	1499	1499	5	33 ms	–
harvard.edu	15000	15000	5	38 ms	–
harvard.edu	65500	65500	5	46 ms	–
harvard.edu	65525	local error	local error	local error	–
harvard.edu	65550	timeout	timeout	timeout	–
google.com	64	64	12	20 ms	–
google.com	256	256	12	21 ms	–

2.3 c) Fragmentacja

Test fragmentacji został przeprowadzony na serwerze `harvard.edu` (tam możliwe było przesyłanie pakietów większych niż 1472 bajtów). Poniższa tabela prezentuje liczbę fragmentów uzyskiwanych dla różnych rozmiarów pakietów:

Rozmiar pakietu	Liczba fragmentów
1400	1
2000	2
3200	3
15000	11
17000	15
25000	17
26000	18
27000	19
28000	19 (truncated)
30000	21 (truncated)
45000	31 (truncated)
65000	44 (truncated)

Według Wireshark pakiety są dzielone na fragmenty o rozmiarze 1480 bajtów. W przypadku polecenia `ping` rozmiar danych wynosi 1472 bajtów (1472 + 28 bajtów nagłówków = 1500 bajtów). Oznaczenie *truncated* wskazuje, że przy bardzo dużych pakietach (np. powyżej 27000 bajtów) fragmentacja nie przebiega prawidłowo – nie wszystkie fragmenty są przesyłane lub poprawnie zrekonstruowane, co może być wynikiem ograniczeń sieciowych lub mechanizmów ochronnych.

3 Wnioski

a) Odległości

Testy wykazały, że liczba skoków między nadawcą a serwerami jest zróżnicowana i zależy od trasy, jaką wybiera ruch sieciowy. Różnice te wynikają z zastosowanych tras, polityki routingu, obecności NAT oraz firewalli, co wpływa również na rzeczywiste opóźnienia.

b) Wielkość pakietów a opóźnienia

Analiza wykazała, że zwiększenie rozmiaru pakietu nie powoduje drastycznego wzrostu opóźnień, jednak przekroczenie określonych limitów (np. MTU = 1500 bajtów) skutkuje błędami transmisji (timeout, local error). Pokazuje to, że sieci mają ustalone limity dla maksymalnego rozmiaru przesyłanych pakietów.

c) Fragmentacja

Fragmentacja pakietów następuje automatycznie, gdy rozmiar pakietu przekracza wartość MTU. Przy standardowym MTU 1500 bajtów, fragmenty mają rozmiar około 1480 bajtów (po odjęciu 20 bajtów nagłówka IPv4 oraz 8 bajtów nagłówka ICMP). Przy bardzo dużych pakietach (np. powyżej 27000 bajtów) obserwuje się, że fragmenty są oznaczane jako *truncated*, co wskazuje na przerwanie procesu fragmentacji lub przekroczenie limitów sieciowych.

d) Dodatkowe obserwacje

Różnice między wynikami `ping` i `traceroute` sugerują, że trasy przesyłu pakietów są asymetryczne. Dodatkowo, niektóre serwery (np. Google, Harvard) stosują mechanizmy ochronne, które ograniczają przesyłanie bardzo dużych pakietów, co objawia się fragmentacją lub oznaczeniem fragmentów jako *truncated*.

e) Wnioski ogólne i podsumowanie

Narzędzia diagnostyczne, takie jak `ping`, `traceroute` i `Wireshark`, dostarczają cennych informacji o charakterystyce sieci. Na podstawie przeprowadzonych testów można wyciągnąć następujące wnioski:

- Sieci często wykorzystują wielopoziomowe trasy, które mogą być znacznie dłuższe niż wynikałoby to z fizycznej odległości między punktami.
- Rozmiar pakietu ma wpływ na stabilność transmisji – przekroczenie limitu MTU skutkuje fragmentacją lub błędami transmisji.
- Mechanizmy ochronne stosowane przez niektóre serwery ograniczają przesyłanie bardzo dużych pakietów, co objawia się fragmentacją lub oznaczeniem fragmentów jako *truncated*.

f) Dodatkowe wnioski z testu niestandardowego wzorca

Test niestandardowy został przeprowadzony przy użyciu polecenia:

```
ping -c 1 -s 11 -p 68656c6c6f20776f726c64 192.168.9.94
```

Dane z Wireshark (Frame 57) zawierają następujące szczegółowe informacje:

- **Długość ramki:** 53 bajty (424 bity) – dokładnie 53 bajty zostały przechwycone, co odpowiada całkowitej długości ramki na łączu.
- **Interfejs:** Ramka została przechwycona na interfejsie `wlp1s0`.
- **Czas przybycia:** Ramka dotarła 11 marca 2025 r. o 17:59:30.513811725 CET (16:59:30.513811725 UTC), co umożliwia dokładną synchronizację czasową.
- **Skład ramki:**
  - **Ethernet II:** Nagłówek Ethernet (14 bajtów) zawiera adres źródłowy (Intel_cc:61:4a, 60:67:20:cc:61:4a) oraz adres docelowy (Intel_db:47:2d, 84:ef:18:db:47:2d).
  - **IPv4:** Nagłówek IP (20 bajtów) wskazuje, że wersja to 4, a długość nagłówka wynosi 20 bajtów. Całkowita długość pakietu IP to 39 bajtów, co wynika z sumy nagłówka (20 bajtów) oraz danych ICMP (19 bajtów).
  - **ICMP:** Nagłówek ICMP (8 bajtów) oraz dane (11 bajtów). Dane (11 bajtów) odpowiadają ciągowi znaków `"hello world"` (przekonwertowanemu z zapisu szesnastkowego: 68 65 6c 6c 6f 20 77 6f 72 6c 64).
- **Pozostałe parametry:**
  - **TTL:** 64 – standardowa wartość dla systemów opartych na systemie Unix/Linux.
  - **Identification:** 0x8401, co umożliwia śledzenie pakietu w przypadku fragmentacji (tu brak fragmentacji, ponieważ flaga i offset są zerowe).
  - **Czas transmisji:** Między ramkami odnotowano ~6.386 ms, co wskazuje na bardzo niskie opóźnienie w sieci lokalnej.
- **Wnioski:**
  - Konstrukcja ramki jest zgodna z oczekiwaniami – łączna długość 53 bajty wynika z sumowania: 14 bajtów (Ethernet) + 20 bajtów (IPv4) + 8 bajtów (ICMP) + 11 bajtów (dane).
  - Dane przekazane w pakiecie ICMP (11 bajtów) reprezentują poprawnie zakodowany tekst `"hello world"`.
  - Precyzyjne znaczniki czasowe oraz minimalne opóźnienie potwierdzają prawidłowe działanie sieci lokalnej oraz dokładność narzędzi przechwytujących.