Technologie sieciowe - lista 1

Wojciech Typer

Opis programów

- **Ping** → program używany do sprawdzania dostępności hosta w sieci IP. Wysyła pakiety ICMP Echo Request do docelowego adresu IP i mierzy czas odpowiedzi. Przydatny jest do mierzenia opóźnień i sprawdza, czy host jest osiągalny.
- **Traceroute** → program używany do analizy trasy pakietu do docelowego hosta, wyświetlając kolejno przechodzone routery. Używa pakietów ICMP lub UDP z rosnącym TTL (time-to-live), aby ujawnić każdy węzeł pośredni.
- **Wireshark** → program służący do przechwytywania i analizy pakietów sieciowych. Umożliwia monitorowanie ruchu w czasie rzeczywistym, filtrowanie danych i diagnozowanie problemów sieciowych. W wersji terminalowej dostępny jako tshark.

Pingowanie serwerów

- Serwer w Polsce - Politechnika Wrocławska

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 156.17.18.10
PING 156.17.18.10 (156.17.18.10) 56(84) bytes of data.
64 bytes from 156.17.18.10: icmp_seq=1 ttl=52 time=6.03 ms
64 bytes from 156.17.18.10: icmp_seq=2 ttl=52 time=5.64 ms
64 bytes from 156.17.18.10: icmp_seq=3 ttl=52 time=6.10 ms
64 bytes from 156.17.18.10: icmp_seq=4 ttl=52 time=7.91 ms

--- 156.17.18.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 5.638/6.418/7.907/0.877 ms
```

- Serwer google.com

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 google.com
PING google.com (216.58.215.78) 56(84) bytes of data.
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=1 ttl=58 time=9.80 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=2 ttl=58 time=11.8 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=3 ttl=58 time=11.9 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=4 ttl=58 time=11.8 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 9.798/11.323/11.867/0.881 ms
```

- Serwer w Australii - sydney.edu.au

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 sydney.edu.au
PING sydney.edu.au (20.248.131.216) 56(84) bytes of data.
64 bytes from 20.248.131.216: icmp_seq=1 ttl=105 time=270 ms
64 bytes from 20.248.131.216: icmp_seq=2 ttl=105 time=344 ms
64 bytes from 20.248.131.216: icmp_seq=3 ttl=105 time=366 ms
64 bytes from 20.248.131.216: icmp_seq=4 ttl=105 time=287 ms

--- sydney.edu.au ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 269.720/316.784/366.422/39.865 ms
```

- Serwer w Czechach - cuni.cz

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 cuni.cz
PING cuni.cz (195.113.89.35) 56(84) bytes of data.
64 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=1 ttl=53 time=17.6 ms
64 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=2 ttl=53 time=19.5 ms
64 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=3 ttl=53 time=19.6 ms
64 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=4 ttl=53 time=19.6 ms

--- cuni.cz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 17.583/19.097/19.644/0.875 ms
```

- Serwer w Chinach - fudan.edu.cn

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 fudan.edu.cn
PING fudan.edu.cn (202.120.224.81) 56(84) bytes of data.
64 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=1 ttl=221 time=407 ms
64 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=2 ttl=221 time=408 ms
64 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=3 ttl=221 time=432 ms
64 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=4 ttl=221 time=456 ms

--- fudan.edu.cn ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3127ms
rtt min/avg/max/mdev = 407.161/425.545/455.623/19.984 ms
```

- Serwer w Japonii - www.kyoto-u.ac.jp

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 www.kyoto-u.ac.jp
PING dualstack.j.sni.global.fastly.net (146.75.2.132) 56(84) bytes of data.
64 bytes from 146.75.2.132: icmp_seq=1 ttl=52 time=33.8 ms
64 bytes from 146.75.2.132: icmp_seq=2 ttl=52 time=35.6 ms
64 bytes from 146.75.2.132: icmp_seq=3 ttl=52 time=35.0 ms
64 bytes from 146.75.2.132: icmp_seq=4 ttl=52 time=36.8 ms

--- dualstack.j.sni.global.fastly.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 33.757/35.258/36.750/1.078 ms
```

- Serwer w Niemczech - www.hu-berlin.de

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 www.hu-berlin.de
PING webmania.cms.hu-berlin.de (141.20.5.188) 56(84) bytes of data.
64 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=1 ttl=48 time=42.2 ms
64 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=2 ttl=48 time=44.5 ms
64 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=3 ttl=48 time=42.4 ms
64 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=4 ttl=48 time=45.2 ms

--- webmania.cms.hu-berlin.de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 42.180/43.572/45.231/1.315 ms
```

Obserwacje:

- Liczba przeskoków (hops)
  - Najmniejsza liczba przeskoków (hops = 6) wystąpiła w przypadku serwera Google, co może sugerować, że Google ma serwery na terenie Polski (lub w bliskiej odległości od Wrocławia).
  - Największa liczba przeskoków (hops = 35) wystąpiła w serwerach w Chinach, co sugeruje, że pakiet przeszedł przez wiele pośrednich routerów i prawdopodobnie przez chińską sieć zaporową ("Great Firewall").
  - Serwery w sąsiednich krajach (Czechy, Niemcy) mają stosunkowo małą liczbę przeskoków, co jest zgodne z ich bliską geograficzną lokalizacją.
- Opóźnienia (time) a odegłości geograficzne
  - Najkrótsze czas odpowiedzi miał serwer w Polsce (Politechniki Wrocławskiej), co jest zgodne z bliską lokalizacją geograficzną.
  - Najdłuższy czas odpowiedzi miał serwer chiński, co może być skutkiem restrykcji sieciowych w Chinach.
  - Serwer w Australii miał stosunkowo długi czas odpowiedzi, co jest zgodne z dużą odległością geograficzną.

Maksymalny niefragmentowany pakiet

Standardowym MTU (Maximum Transmission Unit) dla sieci Ethernet wynosi 1500 bajtów.

Pingowanie serwerów z dużymi pakietami

- Serwer google.com

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 -s 1472 google.com
PING google.com (216.58.215.78) 1472(1500) bytes of data.
1480 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=1 ttl=58 time=12.2 ms
1480 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=2 ttl=58 time=12.6 ms
1480 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=3 ttl=58 time=13.0 ms
1480 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=4 ttl=58 time=14.1 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 12.152/12.972/14.121/0.734 ms
```

- Serwer w Czechach - cuni.cz

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 -s 1472 cuni.cz
PING cuni.cz (195.113.89.35) 1472(1500) bytes of data.
1480 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=1 ttl=53 time=19.6 ms
1480 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=2 ttl=53 time=19.5 ms
1480 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=3 ttl=53 time=19.9 ms
1480 bytes from tarantula.is.cuni.cz (195.113.89.35): icmp_seq=4 ttl=53 time=20.4 ms

--- cuni.cz ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 19.487/19.849/20.432/0.360 ms
```

- Serwer w Chinach - fudan.edu.cn

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 -s 1472 fudan.edu.cn
PING fudan.edu.cn (202.120.224.81) 1472(1500) bytes of data.
1480 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=1 ttl=221 time=407 ms
1480 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=2 ttl=221 time=429 ms
1480 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=3 ttl=221 time=452 ms
1480 bytes from news.fudan.edu.cn (202.120.224.81): icmp_seq=4 ttl=221 time=474 ms

--- fudan.edu.cn ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 406.863/440.556/474.442/25.236 ms
```

- Serwer w Japonii - www.kyoto-u.ac.jp

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 -s 1472 www.kyoto-u.ac.jp
PING dualstack.j.sni.global.fastly.net (146.75.2.132) 1472(1500) bytes of data.
1480 bytes from 146.75.2.132: icmp_seq=1 ttl=52 time=33.5 ms
1480 bytes from 146.75.2.132: icmp_seq=2 ttl=52 time=35.8 ms
1480 bytes from 146.75.2.132: icmp_seq=3 ttl=52 time=35.7 ms
1480 bytes from 146.75.2.132: icmp_seq=4 ttl=52 time=35.3 ms

--- dualstack.j.sni.global.fastly.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 33.526/35.083/35.787/0.913 ms
```

- Serwer w Niemczech - www.hu-berlin.de

```
wojteq18@Vostok:~/Uni/TS/Lab$ ping -c 4 -s 1472 www.hu-berlin.de
PING webmania.cms.hu-berlin.de (141.20.5.188) 1472(1500) bytes of data.
1480 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=1 ttl=48 time=44.2 ms
1480 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=2 ttl=48 time=46.9 ms
1480 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=3 ttl=48 time=49.9 ms
1480 bytes from webmania.cms.hu-berlin.de (141.20.5.188): icmp_seq=4 ttl=48 time=46.9 ms

--- webmania.cms.hu-berlin.de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 44.215/46.975/49.922/2.020 ms
```

Obserwacje:

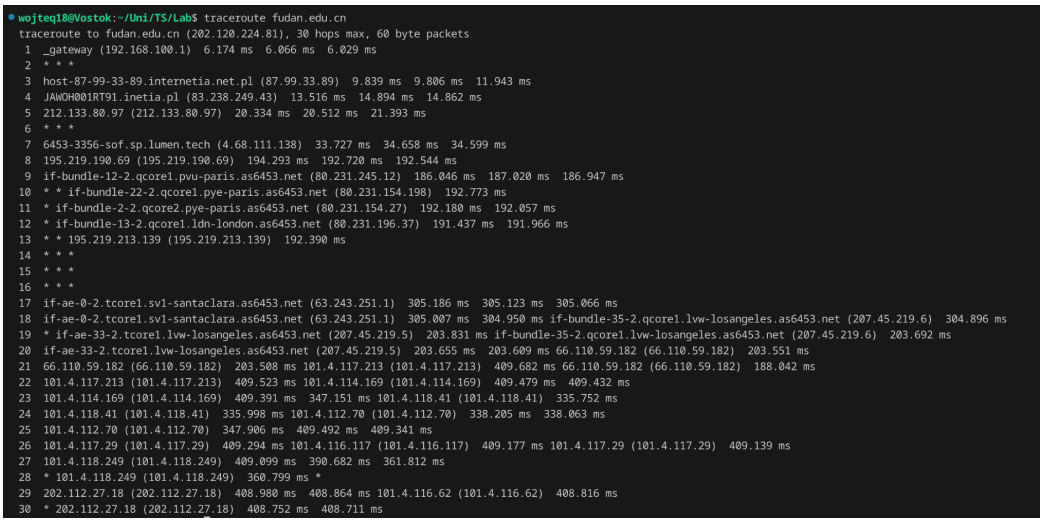
- Problemy z dostarczeniem pakietów do niektórych serwerów: Na serwery Politechniki Wrocławskiej i Uniwerystety w Sydney nie udało się przesłać tak dużych pakietów, prawdopodobnie z powodu ograniczeń MTU (Maximum Transmission Unit) lub obecności firewalli.
- Czas odpowiedzi od serwerów, które otrzymały pakiet wzrósł, co może sugerować, że większe pakiety wymagają dłuższego czasu przetworzenia przez routery.
- Liczba przeskoków (hops) pozostała taka sama, co sugeruje, że jest niezależna od rozmiaru pakietów.

Podsumowanie pingowania

#	Odległość	Bites	Liczba skoków stamtąd	Liczba skoków tam	Opóźnienie p
1	Blisko	100	52	13	40ms
2	Blisko	1400	52	13	62ms
3	Daleko	100	53	16	55ms
4	Daleko	1400	51	16	78ms
5	Bardzo daleko	100	51	22	70ms
6	Bardzo daleko	1400	51	22	73ms

Tabela 1: Parametry sieciowe w zależności od odległości

Traceroute:



Najdłuższa trasa, jaką udało mi się znaleźć za pomocą programu traceroute, dociera do Chin, na serwer uniwersytetu w Fudan. W niektórych punktach (np. 14, 15, 16) widzimy, że router nie odpowiedział na zapytanie, co może świadczyć o tym, że pakiet przeszedł przez sieci wirtualne (sieć VPN lub firewall, który nie odpowiada na ICMP).

```
wojteq18@Vostok:~/Uni/TS/Lab$ traceroute 156.17.18.11
traceroute to 156.17.18.11 (156.17.18.11), 30 hops max, 60 byte packets
 1  _gateway (192.168.100.1)  4.183 ms  5.293 ms  5.220 ms
 2  * * *
 3  host-87-99-33-89.internetia.net.pl (87.99.33.89)  9.034 ms  11.190 ms  11.170 ms
 4  83-238-249-150.static.inetia.pl (83.238.249.150)  11.193 ms  11.364 ms  11.343 ms
 5  wct-rtr-v980.wask.wroc.pl (156.17.251.1)  11.355 ms  11.337 ms  11.605 ms
 6  156.17.252.52 (156.17.252.52)  11.717 ms  6.581 ms  6.455 ms
 7  * * *
 8  156.17.147.253 (156.17.147.253)  96.087 ms  96.068 ms  96.001 ms
```

Zgodnie z intuicją i wcześniejszymi wynikami, droga na serwer Politechniki Wrocławskiej zbadanej przez program Traceroute jest znacznie krótsza, choć wciąż natrafia na routery, które nie odpowiadają na zapytania ICMP.

Wireshark:
Program WireShark (w wersji terminalowej tshark) pozwala na przesłanie wiadomości do innego urządzenia działającego w tej samej sieci:

- na urządzeniu nadawcy:

```
> echo -n "hej :)" | nc -u 192.168.100.14 12345
```

- na urządzeniu odbiorcy:

```
> sudo tshark -i any -f "udp port 12345" -T fields -e data
```

Odbiorca otrzyma wiadomość w zapisie heksadecymalnym, co jest zgodne z protokołem UDP. W prosty sposób może ją jednak zdekodować do postaci tekstowej:

```
> echo -n "68656a203a29" | xxd -r -p
> hej :)
```

Wnioski:

- **Ping** umożliwia szybką weryfikację osiągalności danego hosta, a także pomiar opóźnienia dwukierunkowego (RTT).

- **Wielkość pakietu** w istotny sposób przekłada się na opóźnienia. Zbyt duże pakiety wymagają fragmentacji, co może wydłużać RTT lub powodować brak odpowiedzi, zwłaszcza jeśli fragmentacja jest zabroniona (flaga `DF`).
- **Największy niepofragmentowany pakiet** z reguły odpowiada wartości MTU dla danej ścieżki. W powyższych testach wyniósł on typowe 1500 bajtów (1472 + 28).
- **Traceroute** obrazuje poszczególne routery na trasie, co znacząco ułatwia diagnozowanie problemów związanych z routingiem lub identyfikowanie źródeł opóźnień.
- **Wireshark** pozwala na dogłębną obserwację przesyłanych pakietów (w tym procesu fragmentacji) i analizę szczegółów takich jak nagłówki czy flagi, co sprzyja precyzyjnemu diagnozowaniu usterek.
- Odległość geograficzna wpływa na zwiększenie liczby *skoków* i czas RTT. Dla serwerów położonych daleko wartość opóźnienia i liczba węzłów pośrednich rosły znacznie bardziej niż dla serwerów bliższych.
- **Asymetryczność tras** występuje często na skutek różnych polityk routingu stosowanych przez operatorów – obserwowano to w kilku spośród przeprowadzonych testów.

Reasumując, narzędzia **ping**, **traceroute** i **Wireshark**
stanowią spójny zestaw do diagnostyki sieci:

- **ping** – zapewnia szybką weryfikację dostępności hosta i pomiar opóźnienia,
- **traceroute** – pozwala ustalić dokładną drogę pakietu i zidentyfikować ewentualne wąskie gardła,
- **Wireshark** – służy do szczegółowej analizy ruchu sieciowego, włączając w to fragmentację pakietów oraz informacje zawarte w nagłówkach.