

Sprawozdanie z listy 1. - Technologie sieciowe

Jakub Bachanek

16 marca 2022

1 Ping

1.1 Opis programu

Ping jest programem służącym do badania połączeń sieciowych. Wykorzystuje on protokół ICMP do wysyłania i odbierania pakietów między hostami. Zwracany wynik zawiera informacje o błędach, liczbie wysłanych, otrzymanych i utraconych pakietów, liczbie przeskoków między routerami w sieci, czasach przesyłu pakietu w obie strony (do odbiorcy i z powrotem): minimalnym, maksymalnym, średnim. Przy uruchomieniu można ustawić między innymi następujące flagi:

- -c [count] – wysła [count] pakietów
- -i [interval] – ustawia czas pomiędzy wysłaniem kolejnych pakietów na [interval] sekund
- -s [size] – ustawia rozmiar pakietu na [size] bajtów
- -t [ttl] – ustawia wartość TTL pakietu na [ttl]

Domyślny wynik pracy programu dla *ping google.com* wygląda następująco:

```
PING google.com (142.250.179.142) 56(84) bytes of data.
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=1 ttl=56 time=21.5 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=2 ttl=56 time=21.5 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=3 ttl=56 time=21.7 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=4 ttl=56 time=21.7 ms
64 bytes from ams17s10-in-f14.1e100.net (142.250.179.142): icmp_seq=5 ttl=56 time=21.8 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 21.514/21.648/21.812/0.115 ms
```

Jeżeli cel jest osiągalny, to zwróci odpowiedź, a program *ping* wydrukuje linię, która zawiera:

- rozmiar pakietu
- adres DNS oraz adres IP
- wartość TTL
- całkowity czas dotarcia do celu oraz powrotu

1.2 Odległość serwerów

TTL (Time to live) to parametr, który oznacza dopuszczalną liczbę przeskoków między serwerami zanim pakiet zostanie odrzucony. Każdy serwer, który otrzymuje pakiet zmniejsza tę wartość o 1, po czym podaje go dalej. Aby znaleźć liczbę węzłów na trasie do wybranego serwera będziemy wysyłać pakiety z manualnie ustawioną wartością TTL przy użyciu flagi *-t*. Zaczynamy od 1 i inkrementujemy parametr zawsze kiedy otrzymujemy komunikat "Time to live exceeded". Pierwsza wartość, która nie zwraca tego błędu jest tą, której szukamy. Z kolei, aby znaleźć liczbę przeskoków na trasie z powrotem możemy użyć wartości TTL zwróconej przez *ping*. W tym celu wyznaczamy prawdopodobną liczbę TTL_X (będzie to $2^x - 1$), następnie odejmujemy TTL_X - TTL, co stanowi wynik.

Poniższe tabele przedstawiają uzyskane przeze mnie wyniki.

Miejsce	Adres	średni czas	TTL	Do	Od
Adelaide, Australia	adelaide.edu.au	268.8 ms	237	18	18
Auckland, New Zealand	aut.ac.nz	309.7 ms	38	28	25
Buenos Aires, Argentina	uba.ar	230.6 ms	49	16	14
Shanghai, China	en.sjtu.edu.cn	290.1 ms	232	22	23
Los Angeles, USA	ucla.edu	175.1 ms	42	23	21
Zürich, Switzerland	ethz.ch	37.2 ms	50	13	13
Munich, Germany	tum.de	29.6 ms	244	13	11
Warszawa, Polska	uw.edu.pl	30.8 ms	247	17	8
Wrocław, Polska	edukacja.pwr.wroc.pl	1.3 ms	250	8	5
Gdańsk, Polska	pg.edu.pl	12.9 ms	56	10	7

Wnioski: Czasy propagacji pakietów są najdłuższe dla odległych geograficznie serwerów. Ma to związek z większą liczbą węzłów na trasie, a co za tym idzie z dłuższym przetwarzaniem oraz częstszymi opóźnieniami (większa szansa na trafienie na przeciążony serwer).

1.3 Wielkości pakietów

Ustawiamy rozmiary pakietów za pomocą flagi -s. Będziemy sprawdzać dla 32, 256, 1024, 2048 bajtów.

Miejsce	Adres	rozmiar	średni czas	TTL	Do	Od
Adelaide, Australia	adelaide.edu.au	32	268.0 ms	237	18	18
		256	268.1 ms	237	18	18
		1024	268.4 ms	237	18	18
		2048	Timeout	-	-	-
Auckland, New Zealand	aut.ac.nz	32	309.8 ms	38	28	25
		256	309.8 ms	38	28	25
		1024	310.1 ms	38	28	25
		2048	310.2 ms	38	28	25
Shanghai, China	en.sjtu.edu.cn	32	293.7 ms	232	22	23
		256	290.9 ms	232	22	23
		1024	292.1 ms	232	22	23
		2048	Timeout	-	-	-
Zürich, Switzerland	ethz.ch	32	37.3 ms	50	13	13
		256	37.4 ms	50	13	13
		1024	37.5 ms	50	13	13
		2048	37.8 ms	50	13	13
Wrocław, Polska	edukacja.pwr.wroc.pl	32	1.2 ms	250	8	5
		256	1.5 ms	250	8	5
		1024	1.7 ms	250	8	5
		2048	Timeout	-	-	-
Gdańsk, Polska	pg.edu.pl	32	13.0 ms	56	10	7
		256	13.5 ms	56	10	7
		1024	13.5 ms	56	10	7
		2048	13.6 ms	56	10	7

Wnioski: Różne rozmiary pakietów nie wpłynęły na osiągnięte trasy. Czesy propagacji zazwyczaj nieznacznie rosły ($\sim 1\%$), ale związek jest zbyt słaby, aby można go uznać za ważny. Przy dużych rozmiarach pakiet mógł zostać w pewnym miejscu odrzucony, zatem wtedy *ping* nie drukował odpowiedzi.

1.4 Fragmentacja pakietów

Fragmentacja to proces, który dzieli pakiety na mniejsze części, aby mogły one być przesłane przez połączenia, które mają maksymalny MTU (Maximum Transmission Unit) mniejszy od oryginalnego rozmiaru pakietu. Wartość MTU określa dopuszczalne wielkości pakietów dla danego serwera. Przy domyślnym wywołaniu *ping* ma ustawiony DF (Don't fragment) bit na 0, zatem używa fragmentacji pakietów. Ręcznie można go ustawić przy pomocy flagi -M.

Testując rozmiary z ustawionymi flagami otrzymujemy komunikat:

```
PING aut.ac.nz (156.62.238.90) 4096(4124) bytes of data.
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
ping: local error: message too long, mtu=1500
^C
--- aut.ac.nz ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2045ms
```

Dalej ręcznie szukamy pierwszej wartości, która nie da błędu. Największy niefragmentowany pakiet ma 1472 bajtów.

Nie zauważyłem różnic w czasie propagacji przy różnych ustawieniach fragmentacji dla możliwych rozmiarów.

Wnioski: Z różnych względów routery mają ustawione najbardziej optymalne dla siebie wartości MTU. Każdy pakiet, który przekracza określone rozmiary musi być fragmentowany dla poprawnego przesyłu.

1.5 "Średnica" internetu

Szukając najdłuższych ścieżek trzeba testować różne odległe geograficznie serwery. Niektóre połączenia z Nową Zelandią dają wynik około 27 węzłów. Okolice tego rezultatu należy uznać za "średnicę" internetu. Zdecydowana większość tras posiada poniżej 20 serwerów na swojej drodze.

1.6 Sieci wirtualne

Chcąc wyszukać trasy przebiegające przez sieci wirtualne należy zwracać uwagę na wszelkie nietypowe zachowania przy analizowaniu wyników zwracanych przez *ping*. Używając programu dla serwera *amazon.com* można zauważyć różnice w odpowiedziach:

```
PING amazon.com (205.251.242.103) 56(84) bytes of data.
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=1 ttl=230 time=113 ms
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=2 ttl=230 time=113 ms
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=3 ttl=230 time=113 ms
64 bytes from s3-console-us-standard.console.aws.amazon.com (205.251.242.103): icmp_seq=4 ttl=230 time=113 ms
^C
--- amazon.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 901ms
```

```

PING amazon.com (176.32.103.205) 56(84) bytes of data.
64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=1 ttl=232 time=112 ms
64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=2 ttl=232 time=111 ms
64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=3 ttl=232 time=112 ms
64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=4 ttl=232 time=112 ms
64 bytes from 176.32.103.205 (176.32.103.205): icmp_seq=5 ttl=232 time=111 ms
^C
--- amazon.com ping statistics ---
6 packets transmitted, 5 received, 16,6667% packet loss, time 1505ms

```

Liczby węzłów na trasach są zmienne i wynoszą około 35 dla "do" oraz około 25 dla "od". Są to wartości duże w porównaniu z innymi serwerami, zatem możemy podejrzewać, że może mieć to związek z sieciami wirtualnymi.

2 Traceroute

2.1 Opis programu

Program Traceroute służy do śledzenia trasy pakietów w sieci. Działanie polega na wysyłaniu kolejnych pakietów ze zwiększonym o 1 parametrem TTL (zaczynając od 1). Przechodząc przez trasę TTL jest pomniejszana, a serwer, w którym osiągnie wartość 0 zwraca komunikat o niedotarciu do celu, przy czym zdradza wtedy swoją tożsamość. W ten sposób możliwe jest zbadanie całej ścieżki do hosta docelowego.

Domyślny wynik pracy programu dla *traceroute google.com* wygląda następująco:

```

traceroute to google.com (142.250.179.174), 30 hops max, 60 byte packets
1 adam.t17.ds.pwr.wroc.pl (156.17.234.126) 1.715 ms 1.797 ms 1.745 ms
2 * * *
3 gw.ha.pwr.wroc.pl (156.17.229.253) 0.437 ms 0.441 ms 0.424 ms
4 pwr-zds-centrum3-vprn.wask.wroc.pl (156.17.254.41) 0.509 ms 0.489 ms *
5 pwr-zds-centrum3-vprn.wask.wroc.pl (156.17.254.41) 0.464 ms 0.448 ms 0.475 ms
6 z-Wroclaw-COM.poznan-gw2-amsix.rtr.pionier.gov.pl (212.191.237.121) 4.819 ms sniezka-centrum-rtr.wask.wroc.pl
(156.17.251.166) 0.396 ms z-Wroclaw-COM.poznan-gw2-amsix.rtr.pionier.gov.pl (212.191.237.121) 4.480 ms
7 * z-Wroclaw-COM.poznan-gw2-amsix.rtr.pionier.gov.pl (212.191.237.121) 4.517 ms *
8 core1.ams.net.google.com (80.249.208.247) 24.685 ms 108.170.241.161 (108.170.241.161) 25.770 ms 25.915 ms
9 142.251.48.177 (142.251.48.177) 23.082 ms 108.170.241.161 (108.170.241.161) 25.716 ms 108.170.241.129
(108.170.241.129) 23.329 ms
10 142.251.48.175 (142.251.48.175) 23.399 ms ams15s41-in-f14.1e100.net (142.250.179.174) 22.050 ms 21.963 ms

```

Otrzymywane rezultaty mogą się różnić od tych z *pinga*, zwłaszcza dotyczy

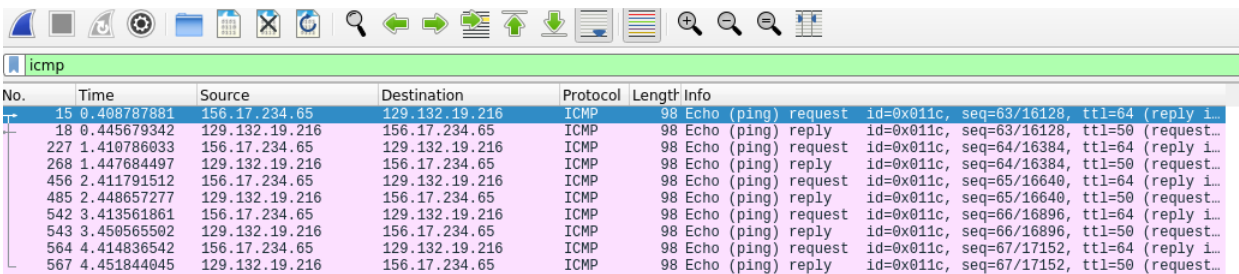
to tego czy cel zostanie osiągnięty. Jest to spowodowane domyślnym używaniem przez program UDP. Można zmienić ustawienie na ICMP poprzez flagę -I, wtedy wyniki są identyczne.

3 WireShark

3.1 Opis programu

Wireshark jest programem służącym do przechwytywania i nagrywania pakietów danych, zarówno wysyłanych, jak i odbieranych. Potrafi rozpoznawać i dekodować wiele protokołów komunikacyjnych, przez co umożliwia szczegółowe zapoznanie się z treścią informacji.

Kiedy program *ping* działa możemy przechwycić i obejrzeć wysłane przez niego pakiety ICMP. Poniżej zamieszczam przykładowe wyniki:



No.	Time	Source	Destination	Protocol	Length	Info
15	0.408787881	156.17.234.65	129.132.19.216	ICMP	98	Echo (ping) request id=0x011c, seq=63/16128, ttl=64 (reply i...
18	0.445679342	129.132.19.216	156.17.234.65	ICMP	98	Echo (ping) reply id=0x011c, seq=63/16128, ttl=50 (request...
227	1.410786033	156.17.234.65	129.132.19.216	ICMP	98	Echo (ping) request id=0x011c, seq=64/16384, ttl=64 (reply i...
268	1.447684497	129.132.19.216	156.17.234.65	ICMP	98	Echo (ping) reply id=0x011c, seq=64/16384, ttl=50 (request...
456	2.411791512	156.17.234.65	129.132.19.216	ICMP	98	Echo (ping) request id=0x011c, seq=65/16640, ttl=64 (reply i...
485	2.448657277	129.132.19.216	156.17.234.65	ICMP	98	Echo (ping) reply id=0x011c, seq=65/16640, ttl=50 (request...
542	3.413561861	156.17.234.65	129.132.19.216	ICMP	98	Echo (ping) request id=0x011c, seq=66/16896, ttl=64 (reply i...
543	3.450565502	129.132.19.216	156.17.234.65	ICMP	98	Echo (ping) reply id=0x011c, seq=66/16896, ttl=50 (request...
564	4.414836542	156.17.234.65	129.132.19.216	ICMP	98	Echo (ping) request id=0x011c, seq=67/17152, ttl=64 (reply i...
567	4.451844045	129.132.19.216	156.17.234.65	ICMP	98	Echo (ping) reply id=0x011c, seq=67/17152, ttl=50 (request...

```

▶ Frame 15: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eno2, id 0
▶ Ethernet II, Src: ASUSTekC_36:df:51 (0c:9d:92:36:df:51), Dst: JuniperN_32:57:81 (78:fe:3d:32:57:81)
▶ Internet Protocol Version 4, Src: 156.17.234.65, Dst: 129.132.19.216
▶ Internet Control Message Protocol

```

```

0000  78 fe 3d 32 57 81 0c 9d 92 36 df 51 08 00 45 00  x.=2W... 6 Q..E.
0010  00 54 f5 97 40 00 00 01 29 62 9c 11 ea 41 81 84  .T..@.. )b..A..
0020  13 d8 08 00 9e 61 01 1c 00 3f b0 20 32 62 00 00  ....a.. ?.. 2b..
0030  00 00 b5 ed 01 00 00 00 00 00 10 11 12 13 14 15  ....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .... !"#%$
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37                                     67

```

4 Wnioski końcowe

Wszystkie analizowane programy są użyteczne w badaniu pracy i struktury sieci. Mogą okazać się również pomocne przy diagnostyce różnych problemów, ponieważ dostarczają sporo informacji, które mogą okazać się w pewnych przypadkach kluczowe. Analiza otrzymywanych wyników daje podstawową dawkę wiedzy na temat funkcjonowania infrastruktury sieciowej.