

Laboratorium

Technologii Sieciowych

Temat:

Wprowadzenie do wybranych aspektów programów:

„Ping” i „Wireshark”

Autor: Bartosz Banasik
Informatyka, semestr: 4
Prowadzący: dr Łukasz Krzywiecki

1. Wstęp

1.1 Cel pracy.

Celem pracy jest przybliżenie możliwości jakie dają nam programy: „Ping” i „Wireshark” oraz wykorzystanie ich do następujących zadań:

1. Określenie długości ścieżki od komputera do wybranego przez nas hosta.
2. Na podstawie odpowiedzi programu „Ping” ustalić długość ścieżki od hosta do naszego komputera.
3. Punkty 1) i 2) wykonać przy ustawionym bicie niefragmentacji i przy różnych rozmiarach pakietów.
4. Określić jak wyglądają opóźnienia w punktach 1) 2) i 3).
5. Krótki opis programu Traceroute.
6. Krótki opis programu Wireshark.

2. Program Ping

2.1 Określanie długości ścieżki.

Do określenia długości ścieżki pozwoli nam wiedza na temat Time-to-live (TTL).

Wykorzystamy do tego przełączniki odpowiednio -t dla Linuxa i -i dla Windowsa.

```
[aedd@localhost AndroidStudioProjects]$ ping -t 5 -c 4 www.google.pl
PING www.google.pl (216.58.209.67) 56(84) bytes of data.
From ael04-10.ffttr6.Frankfurt.opentransit.net (193.251.249.15) icmp_seq=1 Time to live exceeded
From ael04-10.ffttr6.Frankfurt.opentransit.net (193.251.249.15) icmp_seq=2 Time to live exceeded
From ael04-10.ffttr6.Frankfurt.opentransit.net (193.251.249.15) icmp_seq=3 Time to live exceeded
From ael04-10.ffttr6.Frankfurt.opentransit.net (193.251.249.15) icmp_seq=4 Time to live exceeded

--- www.google.pl ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3003ms

[aedd@localhost AndroidStudioProjects]$
```

Analiza danych otrzymanych przez wpisanie powyższej komendy pozwala stwierdzić, że odległość do hosta www.google.com jest większa niż 5 hopów. (Hopy to kolejne przejścia pakietu przez router). Iteracyjnie zwiększając wartość TTL dojdziemy do granicy przy której dostaniemy odpowiedź z serwera

```
[aedd@localhost ~]$ for i in {1..30}; do ping -t $i -c 1 www.google.pl; done | grep "Time"
From funbox.home (192.168.1.1) icmp_seq=1 Time to live exceeded
From wro-bng2.tpnet.pl (80.50.18.74) icmp_seq=1 Time to live exceeded
From wro-r1.tpnet.pl (80.50.18.73) icmp_seq=1 Time to live exceeded
From poz-r1.tpnet.pl (194.204.175.205) icmp_seq=1 Time to live exceeded
From ael04-10.ffttr6.Frankfurt.opentransit.net (193.251.249.15) icmp_seq=1 Time to live exceeded
From 72.14.214.52 (72.14.214.52) icmp_seq=1 Time to live exceeded
From 72.14.234.168 (72.14.234.168) icmp_seq=1 Time to live exceeded
From 216.239.57.145 (216.239.57.145) icmp_seq=1 Time to live exceeded
From 216.239.57.241 (216.239.57.241) icmp_seq=1 Time to live exceeded
From 209.85.252.29 (209.85.252.29) icmp_seq=1 Time to live exceeded
From 216.239.41.167 (216.239.41.167) icmp_seq=1 Time to live exceeded
```

Teraz z łatwością możemy zliczyć odległość do hosta. W tym przypadku wynosi ona 12 hopów. Jest to minimalna wartość TTL jaką możemy nadać jeśli chcemy otrzymać odpowiedź od serwera.

Kolejną ważną informacją jest TTL zwracany do nas przez serwer. Warto zauważyć, że odpowiedź zostanie wysłana z pewną wartością TTL. Jaką? To zależy od systemu na jakim pracuje serwer. Odpowiednio dla Windows 98, Linux wartość ta wynosi 64, a dla nowszych systemów Windows – 128. Warto zauważyć, że jest to potęga dwójki.

```
[aedd@localhost ~]$ ping -c 4 www.google.pl
PING www.google.pl (46.134.210.49) 56(84) bytes of data.
64 bytes from public102961.xdsl.centertel.pl (46.134.210.49): icmp_seq=1 ttl=60 time=30.9 ms
64 bytes from public102961.xdsl.centertel.pl (46.134.210.49): icmp_seq=2 ttl=60 time=36.2 ms
64 bytes from public102961.xdsl.centertel.pl (46.134.210.49): icmp_seq=3 ttl=60 time=39.1 ms
64 bytes from public102961.xdsl.centertel.pl (46.134.210.49): icmp_seq=4 ttl=60 time=30.9 ms

--- www.google.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 30.920/34.341/39.182/3.548 ms
```

W tym przypadku otrzymaliśmy TTL = 60, więc odległość od hosta do nas to $64 - 60 = 4$ hopy.

2.2 Ustawianie bitu niefragmentacji

Ustawianie bitu niefragmentacji uzyskamy dzięki przełącznikowi „-f” dla Windows i „-M do” dla Linux. Rozmiar pakietu możemy kontrolować dzięki przełącznikom -l (Windows) i -s (Linux).

```
[aedd@localhost ~]$ ping -M do -s 1500 www.wp.pl -c 4
PING www.wp.pl (212.77.98.9) 1500(1528) 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
ping: local error: Message too long, mtu=1500

--- www.wp.pl ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3036ms
```

Jak widzimy w tym przypadku rozmiar pakietu jest za duży i nie można go przesłać bez fragmentacji na mniejsze. Spowodowane jest to ustawieniem MTU (Maximum Transfer Unit). Największy niefragmentowalny pakiet jaki udało mi się przesłać był o rozmiarze 1464 bajtów.

2.3 Wpływ wielkości pakietu na trasy

```
[aedd@localhost ~]$ for i in {1..15}; do ping -t $i -c 1 www.wp.pl; done | grep "Time"
From funbox.home (192.168.1.1) icmp_seq=1 Time to live exceeded
From wro-bng2.tpnet.pl (80.50.18.74) icmp_seq=1 Time to live exceeded
From wro-r1.tpnet.pl (80.50.18.73) icmp_seq=1 Time to live exceeded
From war-r1.tpnet.pl (194.204.175.61) icmp_seq=1 Time to live exceeded
From 80.50.123.52 (80.50.123.52) icmp_seq=1 Time to live exceeded

[aedd@localhost ~]$ for i in {1..15}; do ping -t $i -c 1 -s 20000 www.wp.pl; done | grep "Time"
From funbox.home (192.168.1.1) icmp_seq=1 Time to live exceeded
From wro-bng2.tpnet.pl (80.50.18.74) icmp_seq=1 Time to live exceeded
From wro-r1.tpnet.pl (80.50.18.73) icmp_seq=1 Time to live exceeded
From war-r1.tpnet.pl (194.204.175.61) icmp_seq=1 Time to live exceeded
From 80.50.123.52 (80.50.123.52) icmp_seq=1 Time to live exceeded
```

Sprawdziliśmy trasę dwa razy. Pierwszy raz dla domyślnego pakietu. Za drugim razem ustawiliśmy rozmiar pakietu na 20000 bajtów. Jak widzimy trasa się nie zmieniła.

2.4 Badanie opóźnienia

```
[aedd@localhost ~]$ ping -c 30 -q www.wp.pl
PING www.wp.pl (212.77.98.9) 56(84) bytes of data.

--- www.wp.pl ping statistics ---
30 packets transmitted, 30 received, 0% packet loss, time 29043ms
rtt min/avg/max/mdev = 37.731/39.872/51.494/2.557 ms

[aedd@localhost ~]$ ping -c 30 -s 20000 -q www.wp.pl
PING www.wp.pl (212.77.98.9) 20000(20028) bytes of data.

--- www.wp.pl ping statistics ---
30 packets transmitted, 29 received, 3% packet loss, time 29058ms
rtt min/avg/max/mdev = 82.685/106.732/285.160/46.697 ms
```

```
PING openhost.co.nz (119.47.118.9) 40000(40028) bytes of data.
```

```
--- openhost.co.nz ping statistics ---
5 packets transmitted, 2 received, 60% packet loss, time 4044ms
rtt min/avg/max/mdev = 350.856/381.982/413.108/31.126 ms
```

```
PING openhost.co.nz (119.47.118.9) 56(84) bytes of data.
```

```
--- openhost.co.nz ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 311.061/352.905/397.763/30.732 ms
```

Różnica opóźnienia wynosi 29,077. Wzrosło o zaledwie 8% ($1,082 * 352.905$)

Jak możemy zauważyć średni czas opóźnienia wzrasta razem ze zwiększaniem rozmiaru pakietu.

Przełącznik -q pozwala na wyświetlenie samego podsumowania. Przełącznik -s pozwala na ustawienie rozmiaru pakietu.

2.5 Średnica internetu

Najdłuższa ścieżka jaką udało mi się wyszukać liczyła 25 hopów. Używając strony z Nowej Zelandii.¹

```
Ping statistics for 212.77.98.9:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Control-C
^C
C:\Users\Bartosz>tracert www.openhost.co.nz

Tracing route to openhost.co.nz [119.47.118.9]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    funbox.home [192.168.1.1]
  2  30 ms    29 ms    30 ms    wro-bng2.tpnet.pl [80.50.18.74]
  3  30 ms    29 ms    29 ms    wro-r1.tpnet.pl [80.50.18.73]
  4  32 ms    32 ms    32 ms    poz-r1.tpnet.pl [194.204.175.205]
  5  54 ms    54 ms    54 ms    ae104-10.ffttr6.Frankfurt.opentransit.net [193.251.249.15]
  6  51 ms    54 ms    54 ms    hundredgige0-10-0-1.ffttr4.FrankfurtAmMain.opentransit.net [193.251.133.5]
  7  63 ms    63 ms    64 ms    be5511.agr21.fra03.atlas.cogentco.com [130.117.14.225]
  8  63 ms    63 ms    63 ms    be3119.ccr41.fra03.atlas.cogentco.com [130.117.51.37]
  9  68 ms    67 ms    67 ms    be2813.ccr41.ams03.atlas.cogentco.com [130.117.0.121]
 10 139 ms   140 ms   141 ms    be12194.ccr41.lon13.atlas.cogentco.com [154.54.56.93]
 11 137 ms   137 ms   138 ms    be2317.ccr41.jfk02.atlas.cogentco.com [154.54.30.185]
 12 145 ms   147 ms   145 ms    be2806.ccr41.dca01.atlas.cogentco.com [154.54.40.106]
 13 152 ms   151 ms   152 ms    be2112.ccr41.atl01.atlas.cogentco.com [154.54.7.158]
 14 174 ms   174 ms   174 ms    be2687.ccr41.iah01.atlas.cogentco.com [154.54.28.70]
 15 203 ms   202 ms   204 ms    be2927.ccr21.elp01.atlas.cogentco.com [154.54.29.222]
 16 202 ms   208 ms   204 ms    be2930.ccr22.phx02.atlas.cogentco.com [154.54.42.77]
 17 202 ms   202 ms   204 ms    be2932.ccr22.lax01.atlas.cogentco.com [154.54.45.162]
 18 202 ms   201 ms   202 ms    be2965.ccr41.lax04.atlas.cogentco.com [154.54.45.2]
 19 204 ms   208 ms   204 ms    38.88.197.110
 20 332 ms   334 ms   332 ms    bundle-150.cor01.lax01.ca.vocus.net [49.255.255.8]
 21 326 ms   326 ms   326 ms    bundle-200.cor01.alb01.akl.vocus.net.nz [114.31.202.44]
 22 331 ms   332 ms   332 ms    bundle-11.bdr04.alb01.akl.vocus.net.nz [114.31.202.49]
 23 330 ms   329 ms   329 ms    ip-61.87.45.175.VOCUS.net.au [175.45.87.61]
 24 329 ms   327 ms   326 ms    119.47.127.137
 25 332 ms   333 ms   337 ms    www.openhost.co.nz [119.47.118.9]

Trace complete.
```

3. Program Traceroute

3.1 Jak używać

Narzędzie Traceroute automatycznie wyszukuje nam trasę do danego hosta domyślnie używając protokołu UDP. Czasami używając UDP nie uda nam się zbadać ścieżki gdyż zostaniemy zablokowani. Możemy wtedy spróbować użyć innego protokołu: ICMP, TCP.

¹ Opis programu Traceroute (lub Tracert dla Windows) znajduje się poniżej

```
[aedd@localhost TS]$ traceroute www.wp.pl
traceroute to www.wp.pl (212.77.98.9), 30 hops max, 60 byte packets
 1 funbox.home (192.168.1.1)  2.335 ms  2.320 ms  3.086 ms
 2 wro-bng2.tpnet.pl (80.50.18.74)  31.878 ms  32.323 ms  32.327 ms
 3 wro-r1.tpnet.pl (80.50.18.73)  32.747 ms  33.190 ms  33.192 ms
 4 war-r1.tpnet.pl (194.204.175.61)  43.847 ms  43.388 ms  43.824 ms
 5 80.50.123.52 (80.50.123.52)  42.877 ms  42.970 ms  43.076 ms
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 *^C
[aedd@localhost TS]$ traceroute -I www.wp.pl
You do not have enough privileges to use this traceroute method.
socket: Operation not permitted
[aedd@localhost TS]$ sudo traceroute -I www.wp.pl
traceroute to www.wp.pl (212.77.98.9), 30 hops max, 60 byte packets
 1 funbox.home (192.168.1.1)  3.455 ms  3.493 ms  6.790 ms
 2 wro-bng2.tpnet.pl (80.50.18.74)  43.626 ms  43.650 ms  43.954 ms
 3 wro-r1.tpnet.pl (80.50.18.73)  42.145 ms  43.967 ms  45.633 ms
 4 war-r1.tpnet.pl (194.204.175.61)  70.669 ms  70.980 ms  70.986 ms
 5 80.50.123.52 (80.50.123.52)  55.766 ms  56.619 ms  57.687 ms
 6 www.wp.pl (212.77.98.9)  58.857 ms  38.145 ms  38.453 ms
```

4. Program Wireshark

4.1 Opis Wireshark

Narzędzie umożliwiające przechwytywanie i nagrywanie pakietów danych oraz ich dekodowanie.

4.2 Filtrowanie

Wireshark pozwala na filtrowanie otrzymywanych pakietów. Użyjemy tej opcji aby wyszukać interesujące nasz pakiety. Filtr HTTP.

4.3 Podglądanie strony

Opcja: „follow HTTP stream” pozwala nam na odczytanie treści strony.

Activities Wireshark (GTK+) Tue 22:46 9°C pl

*wlp2s0 [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
757	221.6801545f	192.168.1.15	156.17.7.22	HTTP	419	GET / HTTP/1.1
770	221.7606758f	156.17.7.22	192.168.1.15	HTTP	1881	HTTP/1.1 200 OK (text/html)
1173	268.3899044f	192.168.1.15	54.192.230.179	HTTP	354	GET /success.txt HTTP/1.1
1175	268.4602346f	54.192.230.179	192.168.1.15	HTTP	573	HTTP/1.1 200 OK (text/plain)
1238	269.0265571f	192.168.1.15	178.62.207.82	HTTP	339	GET /data/2.5/weather?lon=16.97819633
1240	269.1044385f	178.62.207.82	192.168.1.15	HTTP	879	HTTP/1.1 200 OK (application/json)
1484	286.1626003f	192.168.1.15	2.16.172.41	OCSP	509	Request
1487	286.2016192f	2.16.172.41	192.168.1.15	OCSP	979	Response
2821	288.2528175f	192.168.1.15	93.184.220.29	OCSP	497	Request
2880	288.2869072f	192.168.1.15	23.42.27.27	OCSP	479	Request
2882	288.2870746f	192.168.1.15	23.42.27.27	OCSP	479	Request
2979	288.3195696f	192.168.1.15	93.184.220.29	OCSP	497	Request

Frame 757: 419 bytes on wire (3352 bits), 419 bytes captured (3352 bits) on interface 0
 Ethernet II, Src: IntelCor_id:5b:6e (48:51:b7:1d:5b:6e), Dst: Sagemcom_2f:7e:5a (a0:1b:29:2f:7e:5a)
 Internet Protocol Version 4, Src: 192.168.1.15, Dst: 156.17.7.22
 Transmission Control Protocol, Src Port: 41862, Dst Port: 80, Seq: 1, Ack: 1, Len: 353
 Hypertext Transfer Protocol

0000 a0 1b 29 2f 7e 5a 48 51 b7 1d 5b 6e 08 00 45 00 .../~ZHQ ..[n..E.
 0010 01 95 bb 7b 40 00 40 06 19 09 c0 a8 01 0f 9c 11 ...{0.0.
 0020 07 16 a3 86 00 50 37 ab 41 83 1b 49 c6 3c 80 18P7. A..I.<..
 0030 00 e5 79 be 00 00 01 01 08 0a be 14 f7 ed 18 b5 ..y.....
 0040 cc 3e 47 45 54 20 2f 20 48 54 50 2f 31 2e 31 ..>GET / HTTP/1.1
 0050 0d 0a 48 6f 73 74 3a 20 63 73 2e 70 77 72 2e 65 ..Host: cs.pwr.e

wlp2s0: <live capture in progress... Packets: 5718 · Displayed: 26 (0.5%)

Mark Packet (toggle)
 Ignore Packet (toggle)
 Set Time Reference (toggle)
 Time Shift...
 Edit Packet
 Packet Comment...
 Manually Resolve Address
 Apply as Filter
 Prepare a Filter
 Conversation Filter
 Colorize Conversation
 SCTP
 Follow TCP Stream
 Follow UDP Stream
 Follow SSL Stream
 Follow HTTP Stream
 Copy
 Protocol Preferences
 Decode As...
 Print...

Follow HTTP Stream (tcp.stream eq 12)

Stream Content

```
<h1>0 Katedrze</h1>
</div>
</div><div class='row'>
<div class='large-6 columns'>
<article>
.<h2>Podstawowe informacje</h2>
.<div class='panel'>
..Pomieszczenia Katedry Informatyki Wydzia..u Podstawowych Problem..w Techniki
(<strong>W11/K2</strong>) znajduj.. sie w budynku D-1 Politechniki Wroc..awskiej (pl.
Grunwaldzki 13).
.</div>
.<div class='panel'>
..G...wnym obszarem naszych zainteresowa.. badawczych s.. zaawansowane technologie
informatyczne. G...wnymi tematami bada.. s... Algorytmika, Kryptografia,
Bezpiecze..stwo Komputerowe i Optymalizacja Dyskretna. Cz..... naszej kadry zajmuje
si.. r..wnie.. Matematyk.. (g...wnie: Teori.. Mnogo..ci, Teori.. Funkcji
Rzeczywistych, Teori.. Miary i Topologi...).
.</div>
.<div class='panel'>
..Opiekujemy si.. studiami informatycznymi pierwszego i drugiego stopnia na Wydziale
Podstawowych Problem..w Techniki. Na studiach drugiego stopnia prowadzimy dwie
specjalno..ci: Algorytmika (w j..zyku polskim) i Bezpiecze..stwo Komputerowe (w j..zyku
angielskim).
.</div>
```

Entire conversation (17688 bytes)

Find Save As Print ☐ ASCII ☐ EBCDIC ☐ Hex Dump ☐ C Arrays ☒ Raw

Help Filter Out This Stream Close