Szymon Głąb 05.03.2019, Wrocław

Sprawozdanie 1

PING

Opis

Narzędzie służące do sprawdzenia czy dane urządzenie jest dostępne w naszej sieci. Innymi słowy umożliwia nam sprawdzenie czy istnieje połączenie pomiędzy naszym komputerem, a serwerem.

Wybrane z możliwych parametrów (dla systemu Windows):

- ***-t*** - sprawia, że polecenie ping ponawia wysyłanie komunikatów do obiektu docelowego do momentu przerwania danej operacji,
- ***-n liczba*** - określa liczbę wysyłanych żądań,
- ***-f*** - powoduje, że żądania są wysyłane z flagą zapobiegającą fragmentacji,
- ***-w limit_czasu*** - określa w milisekundach czas oczekiwania na odebranie komunikatu odpowiedzi. Domyślnie są to 4 sekundy,
- ***-l rozmiar*** – pozwala wysłać pakiet określonego rozmiaru,
- ***-i TTL*** – pozwala ustawić początkową wartość TTL.

Sprawdzanie ilości węzłów

Do sprawdzenia długości trasy używamy wartości wyświetlanej przy TTL (Time To Live), Wydawać by się mogło że są to sekundy, lecz jest to liczba możliwych skoków na trasie pakietu. Dla różnych systemów operacyjnych mamy różne wartości początkowe TTL, od których następnie odejmujemy wynik który został nam zwrócony.

Wartości początkowe:

- **32** – Windows 95 i NT 3.51
- **64** – Windows 98, Linux
- **128** – Nowsze systemy Windows

Przykładowe wywołanie

```
C:\Users\Szymon>ping help-plock.pl

Pinging help-plock.pl [188.128.195.229] with 32 bytes of data:
Reply from 188.128.195.229: bytes=32 time=11ms TTL=59
Reply from 188.128.195.229: bytes=32 time=11ms TTL=59
Reply from 188.128.195.229: bytes=32 time=12ms TTL=59
Reply from 188.128.195.229: bytes=32 time=11ms TTL=59

Ping statistics for 188.128.195.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 12ms, Average = 11ms
```

Jak widać na powyższym zrzucie ekranu TTL wynosi 59 z tego wynika, że nasz pakiet wracając „pokonał” na swojej drodze 64 – 59 = 5 routerów.

Do sprawdzenia drogi do serwera używamy parametru ***-i TTL,*** gdzie sami możemy ustawić wartość początkową TTL dla danego pakietu, w ten sposób doświadczalnie znajdujemy drogę. Dla przykładu powyżej, droga do serwera wynosi 6 hopów.

```
C:\Users\Szymon>ping -i 5 help-plock.pl

Pinging help-plock.pl [188.128.195.229] with 32 bytes of data:
Reply from 195.182.218.21: TTL expired in transit.
Reply from 195.182.218.21: TTL expired in transit.
Reply from 195.182.218.21: TTL expired in transit.
Reply from 195.182.218.21: TTL expired in transit.

Ping statistics for 188.128.195.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
C:\Users\Szymon>ping -i 6 help-plock.pl

Pinging help-plock.pl [188.128.195.229] with 32 bytes of data:
Reply from 188.128.195.229: bytes=32 time=11ms TTL=59
Reply from 188.128.195.229: bytes=32 time=12ms TTL=59
Reply from 188.128.195.229: bytes=32 time=11ms TTL=59
Reply from 188.128.195.229: bytes=32 time=14ms TTL=59

Ping statistics for 188.128.195.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 14ms, Average = 12ms
```

Wielkość pakietu, a ilość skoków

Podczas wykonywanych prób nie zaobserwowałem, aby wielkość pakietu miała jakikolwiek wpływ na ich trasę, poniżej umieszczam kilka przykładowych wywołań.

Adres	1000b	5000b
wikipedia.org	TTL = 57	TTL = 57
miejski.pl	TTL = 56	TTL = 56
dnc.org.nz	TTL = 43	TTL = 43

Dane w tabeli to średnia 5 pomiarów

Przykładowe odpowiedzi dla serwisu *wikipedia.org*

```
Pinging wikipedia.org [91.198.174.192] with 1000 bytes of data:
Reply from 91.198.174.192: bytes=1000 time=31ms TTL=57
```

```
Pinging wikipedia.org [91.198.174.192] with 5000 bytes of data:
Reply from 91.198.174.192: bytes=5000 time=48ms TTL=57
```

Maksymalny rozmiar niefragmentowanego pakietu

Maksymalny rozmiar jest zależny od MTU (Maximum Transfer Unit), która określa rozmiar największego pakietu, jaki możemy wysłać i nie ulegnie on fragmentacji. W moim przypadku największym możliwym pakietem jest ***1472b danych +28b nagłówek ramki, czyli 1500b.*** Niezależnie od tego, czy wysyłamy ping na adres o krótkiej, czy długiej trasie.

Czas propagacji

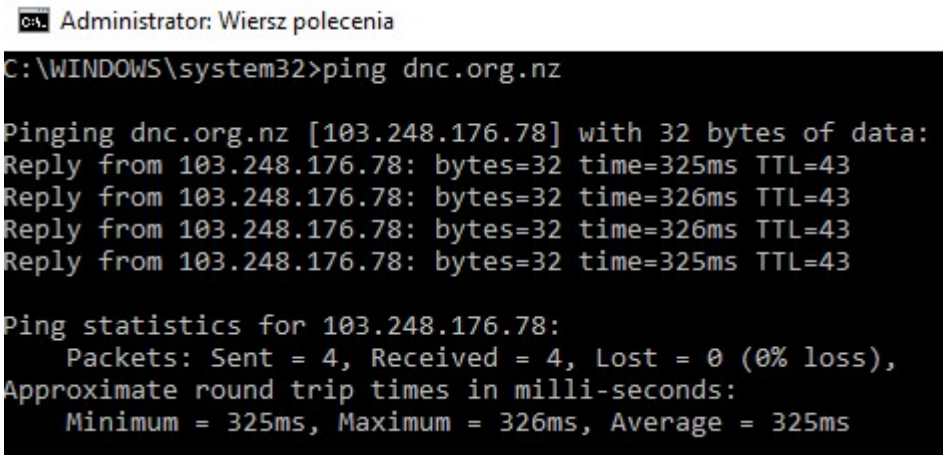
Adres	1000b	1000b bez fragmenatcji	2500b	5000b
wikipedia.org	36ms	32ms	37ms	40ms
miejski.pl	30ms	28ms	30ms	40ms
dunedin.govt.nz	380ms	359ms	385ms	410ms

Dane w tabeli to średnia 5 pomiarów

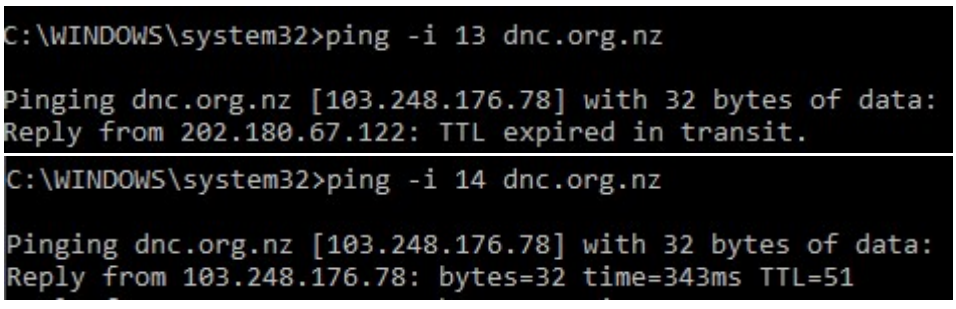
Jak widać z powyższej tabelki wynika że wraz ze ***wzrostem wielkości pakietu, rośnie także czas propagacji.***

Średnica Internetu

Średnica internetu to najdłuższa ścieżka jaką udało mi się otrzymać (mierzona przy pomocy TTL). W moim przypadku był to ping do serwisu znajdującego się w Nowej Zelandii **dnc.org.nz.** Jak widać na załączonym zrzucie najdłuższą ścieżką jaką udało mi się osiągnąć jest **21.**



Natomiast podczas drogi do serwera nie była ona aż tak długa bo wynosiła **14** hopów.



Sieci Wirtualne

Sieci wirtualne modyfikują wartość wskaźnika TTL, przez co utrudnione jest śledzenie pakietów. To że nasz pakiet na swojej drodze przechodzi przez sieć wirtualną można

rozpoznać po tym, że pingując kilka razy (z odstępami czasowymi) dostajemy znaczne różnice TTL, lub odpowiedź uzyskujemy z różnych adresów IP.

TRACEROUTE

Polecenie systemowe umożliwiające sprawdzenie przez jakie komputery przepływają pakiety danych wysłane przez nasz komputer do wybranego serwera. Polecenie *traceroute* wypisze też czasy przechodzenia danych na poszczególnych odcinkach ich sieciowej drogi.

Polecenie *traceroute* ma swój odpowiednik w systemach z rodziny Microsoft Windows – *tracert*. Ma ono podobną funkcjonalność.

Przykładowe wywołanie

```
C:\WINDOWS\system32>tracert wikipedia.org

Tracing route to wikipedia.org [91.198.174.192]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  192.168.0.254
  2    10 ms     6 ms     4 ms  10.10.200.1
  3     9 ms     5 ms     7 ms  87.239.41.6
  4     8 ms     4 ms     6 ms  91.198.97.22
  5     8 ms     5 ms     6 ms  94-75-96-197.home.aster.pl [94.75.96.197]
  6    44 ms    38 ms    33 ms  pl-ktw01a-rc1-ae5-1408.aorta.net [84.116.193.50]
  7    35 ms     *       33 ms  pl-waw04a-rc1-ae40-0.aorta.net [84.116.133.33]
  8    32 ms    40 ms    32 ms  nl-ams17b-rc1-lag-22-0.aorta.net [84.116.136.141]
  9    35 ms    33 ms    31 ms  nl-ams04a-rb2-ae1-0.aorta.net [84.116.139.130]
 10    46 ms    33 ms    33 ms  213.46.186.10
 11    31 ms    30 ms    31 ms  ae1-403.cr2-esams.wikimedia.org [91.198.174.254]
 12    31 ms    34 ms    30 ms  text-lb.esams.wikimedia.org [91.198.174.192]

Trace complete.
```

Z powyższego obrazka można wywnioskować, że na trasie do serwera wikipedia.org pakiet wykonał 12 hopów.

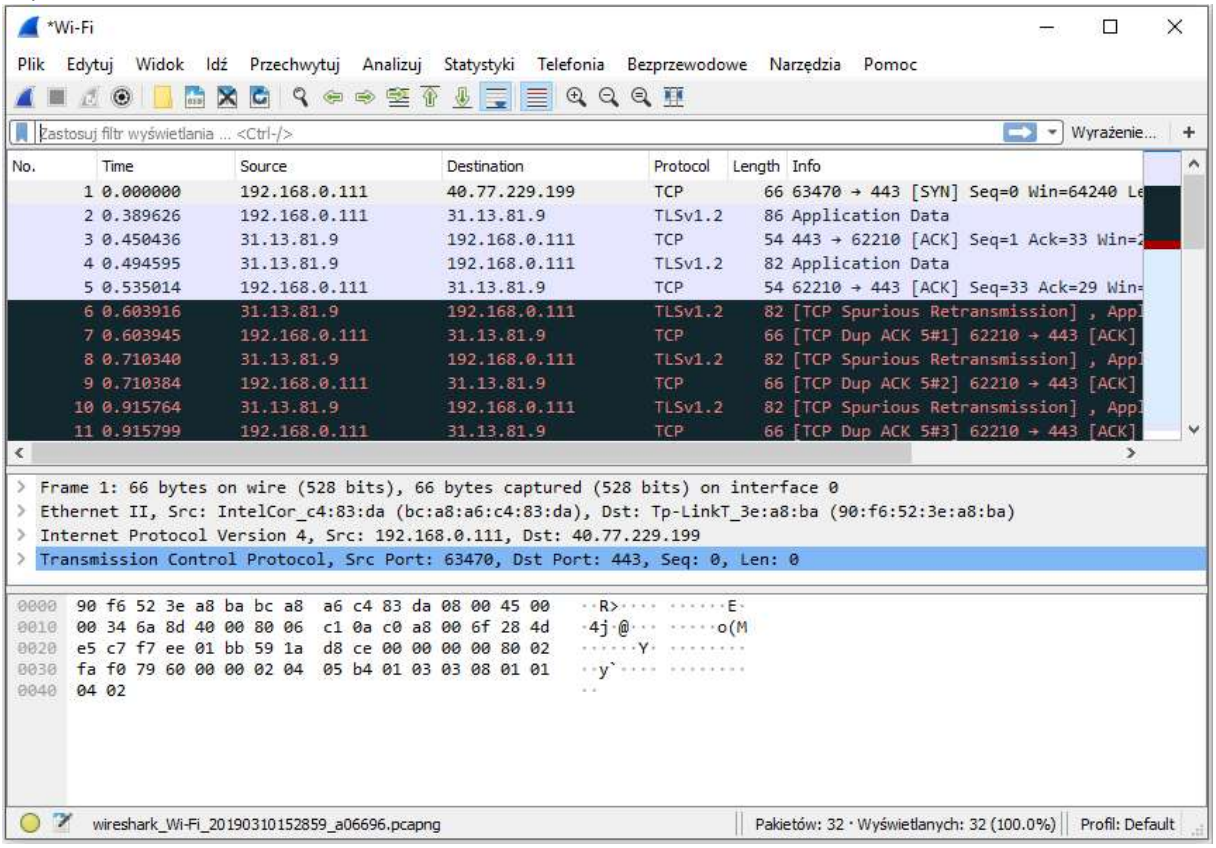
WIRESHARK

Darmowe oprogramowanie open-source służące do analizowania pakietów. Działa w sposób pasywny, tzn. nie wysyła żadnych informacji, a tylko przechwytuje dane docierające do interfejsu sieciowego. Nie wpływa także w żaden sposób na działanie aplikacji przesyłających dane przez sieć. W aplikacji możemy używać różnych filtrów które ułatwiają nam odczytywanie przechwyconych danych. Dzięki temu programowi można łatwo odczytać informacje o zastosowanych protokołach oraz ich budowę.

Na załączonym poniżej zdjęciu widać przechwycone informacje. Kolejno:

- Numer ramki
- Czas przechwyconej ramki (od uruchomienia przechwytywania) w sekundach
- Adres źródła ramki
- Adres adresata ramki
- Rodzaj użytego protokołu
- Długość ramki

Przykład uruchomienia



Wnioski

Każdy z powyższych programów zajmuje się czymś innym, lecz łączy je jedno zadanie – analiza sieci. Programów tych używamy aby dowiedzieć się czy istnieje połączenie pomiędzy serwerami, jak przekazywane są dane, do kogo trafiają wysłane przez nas dane lub aby dowiedzieć się w jaki sposób dany pakiet trafił do wybranego serwera. Programy te często wykorzystywane są do wstępnej analizy problemów z połączeniem oraz mogą ułatwić nam rozwiązanie tego problemu.

Na podstawie wyżej przeprowadzonych doświadczeń możemy dojść do następujących wniosków:

- ➔ Wielkość pakietu nie ma wpływu na jego trasę, niezależnie od tego gdzie znajduje się serwer,
- ➔ Jeżeli trasa jest dłuższa to czas propagacji jest większy, więc połączenia z serwerami znajdującymi się w większej odległości geograficznej zajmują więcej czasu
- ➔ Czym większy pakiet, tym większy czas propagacji,
- ➔ Największy możliwy do pingowania nie fragmentowany pakiet to 1500b (1472b danych + 28b nagłówka)
- ➔ Średnica internetu wynosi 21 hopów.