PING

Komenda **ping** służy do wysłania żądania ECHO_REQUEST protokołu ICMP w celu otrzymania komunikatu ICMP ECHO_RESPONSE od hosta lub bramy. **Ping** posiada wiele przydatnych opcji, w tym sprawozdaniu będe używać **-s** (ustala wielkość pakietu), **-t**(ustala wartość pola ttl).

Sprawdzanie ilości węztów
ttl to parametr,który określa czas życia pakietu. Każdy router, obniża wartość ttl w nagłówku o 1.Po osiągnięcu wartości 0 pakiet jest kasowany. Takie działanie zapobiega istnieniu pakietu, który krążyłby w nieskończoność bez celu.Standardowo wartość ttl w różnych systemach wynosi 64,128,255.

ilość węztów do celu

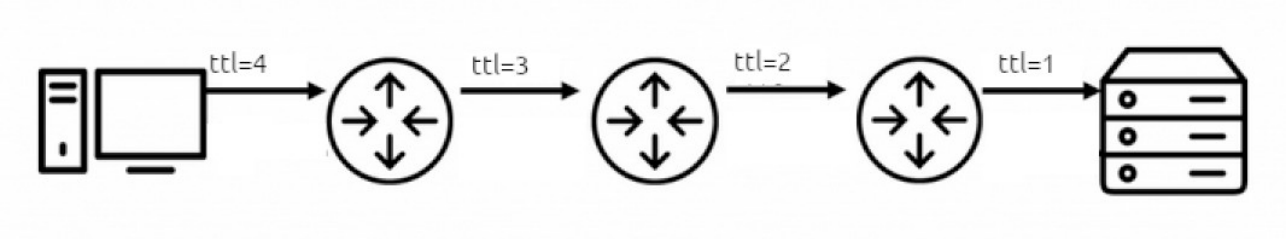
```
➜ ~ ping -c 2 -t 6 wcss.pl
PING wcss.pl (156.17.193.248) 56(84) bytes of data.
From fw1-vsys3-backup.wcss.wroc.pl (156.17.252.138) icmp_seq=1 Time to live exceeded
From fw1-vsys3-backup.wcss.wroc.pl (156.17.252.138) icmp_seq=2 Time to live exceeded

--- wcss.pl ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1002ms

➜ ~ ping -c 2 -t 7 wcss.pl
PING wcss.pl (156.17.193.248) 56(84) bytes of data.
64 bytes from www.wcss.pl (156.17.193.248): icmp_seq=1 ttl=247 time=2.92 ms
64 bytes from www.wcss.pl (156.17.193.248): icmp_seq=2 ttl=247 time=3.66 ms

--- wcss.pl ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.918/3.289/3.661/0.371 ms
➜ ~
```

W tym przypadku liczba węztów wynosi 6, faktyczna liczba ttl musi być o 1 większa niż liczba routerów przez, która przechodzi, żeby ostatni router nie zniszczył pakietu



ilość węztów od celu

```
➜ ~ ping -c 2 wcss.pl
PING wcss.pl (156.17.193.248) 56(84) bytes of data.
64 bytes from www.wcss.pl (156.17.193.248): icmp_seq=1 ttl=247 time=3.35 ms
64 bytes from www.wcss.pl (156.17.193.248): icmp_seq=2 ttl=247 time=3.65 ms

--- wcss.pl ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.350/3.497/3.645/0.147 ms
```

W tym przypadku zakładamy że wartość początkowa ttl wynosiła 255, co nam daje 255-247=8 węztów, przez które pakiet przeszedł po drodze z serwera do hosta.

lokalizacja	adres	węzły do	węzły od
wrocław	www.wcss.pl	6	8
Niemcy	www.stadtmuseum.de	11	11
Chiny	www.cnnic.com.cn	15	17
Nowa Zelandia	www.govt.nz	12	11

wpływ wielkości pakietu na ttl

adres	1 000B	20 000B	40 000B
www.wcss.pl	ttl=8	* (MAX=1500)	*
www.stadtmuseum.de	ttl=11	ttl=11	ttl=11
www.cnnic.com.cn	ttl=17	*(MAX=1500)	*
www.govt.nz	*(MAX=100)	*	*

Wielkość pakietu nie ma wpływu na trase pakietu, jedynie może zostać odrzucony przez zbyt duży rozmiar.Maximum Transmit Unit, defaultowo ma wartość 1500 (powyzej wcss.pl), jednak na każdym routerze można ustawić różną wartość.

wpływ wielkośći pakietu na czas propagacji

adres	1 000B	20 000B	40 000B
www.stadtmuseum.de	29.5	30.4	30.7

Wraz ze wzrostem pakietu rośnie czas propagacji.Na linuxie defaultowo flaga DF jest ustawiona.Więc rzadko pakiet o wiekszym rozmiarze niz 1500 dojdzie do celu bez fragmentacji.

sieci wirtualne

sieci wirtualne modyfikują prawdziwą wartość pola ttl, przez co utrudnione jest śledzenie pakietu.Sieci wirtualne charakteryzują sie tym, że pingując cel w odstępach czasowych dostajemy różne wartości pola ttl

TRACEROUTE

Jest to program służacy do śledzenia trasy pakietów w sieci.Pokazuje nam przez jakie routery pakiet przeszedł w drodze do celu. Tak samo jak w poleceniu ping możemy modyfikować np. ttl.Ponadto wypisze czas przesyłu pakietu do konkretnych routerów.

```
➜ ~ traceroute wcss.pl
traceroute to wcss.pl (156.17.193.248), 30 hops max, 60 byte packets
 1  funbox.home (192.168.1.1)  0.609 ms  0.648 ms  0.690 ms
 2  wro-bng2.neo.tpnet.pl (83.1.5.3)  2.804 ms  3.770 ms  3.880 ms
 3  wro-r11.tpnet.pl (80.50.18.73)  3.635 ms  3.625 ms wro-r12.tpnet.pl (80.50.122.73)  3.616 ms
 4  wro-ar1.tpnet.pl (213.25.5.102)  3.606 ms wro-ar1.tpnet.pl (213.25.12.102)  3.713 ms  3.704 ms
 5  Wroclaw.tpeix.rtr.pionier.gov.pl (212.191.243.14)  3.814 ms  3.804 ms  3.795 ms
 6  fw1-vsys3-backup.wcss.wroc.pl (156.17.252.138)  5.018 ms  3.112 ms  4.066 ms
 7  www.wcss.pl (156.17.193.248)  4.056 ms  3.842 ms  3.999 ms
➜ ~
```

Tak jak w poleceniu ping, widzimy że do celu mamy 6 węzłów

```
➜ ~ traceroute www.govt.nz
traceroute to www.govt.nz (45.60.16.237), 30 hops max, 60 byte packets
 1  funbox.home (192.168.1.1)  0.683 ms  0.760 ms  0.793 ms
 2  wro-bng2.neo.tpnet.pl (83.1.5.3)  3.526 ms  3.569 ms  3.560 ms
 3  wro-r11.tpnet.pl (80.50.18.73)  7.567 ms  7.557 ms wro-r12.tpnet.pl (80.50.122.73)  3.420 ms
 4  195.116.35.206 (195.116.35.206)  5.921 ms  6.901 ms  6.888 ms
 5  hbg-b2-link.ip.twelve99.net (213.248.96.144)  28.559 ms  28.550 ms  28.614 ms
 6  hbg-bb3-link.ip.twelve99.net (62.115.120.70)  28.604 ms  26.440 ms  26.555 ms
 7  ffm-bb1-link.ip.twelve99.net (62.115.123.76)  26.397 ms  25.357 ms ffm-bb2-link.ip.twelve99.net (62.115.127.91)  26.213 ms
 8  ffm-b11-link.ip.twelve99.net (62.115.124.117)  26.132 ms  26.174 ms ffm-b11-link.ip.twelve99.net (62.115.124.119)  27.157 ms
 9  * * *
10  * * *
11  195.122.180.66 (195.122.180.66)  26.648 ms  27.564 ms  26.253 ms
```

Dodatkowo znakiem “*”, pokazuje że nie dostał odpowiedzi od routera

WIRESHARK

Jest to program, który umożliwia przechwytywanie pakietów docierające do interfejsu sieciowego.Przechwycone pakiety można zapisać, oraz poddać analizie.

tls handshake

za pomocą wiresharka, możemy podejrzeć jak odbywa się proces rozpoczęcia komunikacji, oraz w jaki sposób komunikacja jest zabezpieczana

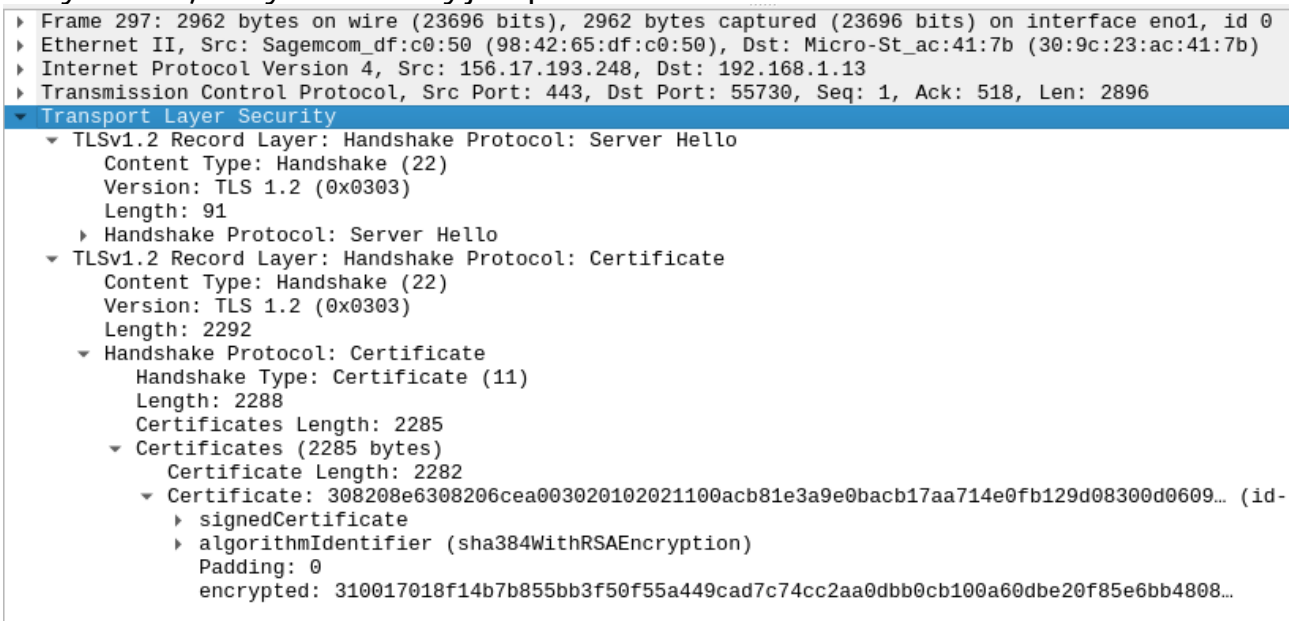
1.client hello

klient rozpoczyna komunikacje, przesyła serwerowi wersje tls, oraz wersje algorytmów szyfrujących

```
▾ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  ▾ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 508
      Version: TLS 1.2 (0x0303)
    ▸ Random: c10dfe545998d552d658cb43553fbee4fd9e81059d3319d7694f771024a0df60
      Session ID Length: 32
      Session ID: 1b28267ad36b409268c08bce23622004019f2025c2f50ee54e9d142448e8c727
      Cipher Suites Length: 34
    ▸ Cipher Suites (17 suites)
      Compression Methods Length: 1
    ▸ Compression Methods (1 method)
      Extensions Length: 401
    ▸ Extension: server_name (len=12)
    ▸ Extension: extended_master_secret (len=0)
    ▸ Extension: renegotiation_info (len=1)
    ▸ Extension: supported_groups (len=14)
    ▸ Extension: ec_point_formats (len=2)
    ▸ Extension: session_ticket (len=0)
    ▸ Extension: application_layer_protocol_negotiation (len=14)
    ▸ Extension: status_request (len=5)
    ▸ Extension: delegated_credentials (len=10)
    ▸ Extension: key_share (len=107)
    ▸ Extension: supported_versions (len=5)
    ▸ Extension: signature_algorithms (len=24)
    ▸ Extension: psk_key_exchange_modes (len=2)
    ▸ Extension: record_size_limit (len=2)
    ▸ Extension: padding (len=143)
      [JA3 Fullstring: 771,4865-4867-4866-49195-49199-52393-52392-49196-49200-49162-
      [JA3: 579ccef312d18482fc42e2b822ca2430]
```

2.server hello, certificate

serwer wysyła wersje tls oraz wersje algorytmów, które może używać I odeśle je wraz z certyfikatem, który walidowany jest przez klienta



3.Server Key Exchange

serwer wysyła, klucz publiczny oraz podpis.Klucz publiczny jest używany do ustalenia wspólnego tajnego klucza (**Protokół Diffiego-Hellmana**)

4.Client Key Exchange

klient wysyła swój klucz publiczny, żeby serwer ustalił ten sam wspólny tajny klucz

Dd tego momentu cała komunikacja jest zaszyfrowana.dodatkowo istnieją jeszcze protokoły:
Change Cipher Spec – wiadomośc wysyłana przez obie strony, że od tej pory komunikacja jest chroniona przez wczesniej ustalone wersje, oraz klucze
Encrypted Handshake Message – wiadomość wysyłana przez obie strony, potwierdzająca działanie wspólnego tajnego klucza

WNIOSKI

Wszystkie użyte tutaj programy służą do analizy sieci.Użyteczność tych programów znajdujemy w diagnozowaniu problemów działania sieci.

- Wielkośc pakietu nie ma wpływu na pole ttl.
- Dłuższa trasa => Większy czas propagacji
- Większy rozmiar pakietu => Większy czas propagacji
- Największy możliwy pakiet (defaultowo) do wysłania to 1472(+28)B
- W rzeczywistości **PING** pozwala na wysłanie pakietu o wielkości **65 527 B**
- Większa odległośc geograficzna nie oznacza większej liczby skoków, (Chiny>NZ)