Oto jak działa traceroute

```
$traceroute wikipedia.org
traceroute to wikipedia.org (66.230.200.100), 64 hops max, 44 byte packets
 1  124.ae0.xr1.3d12.xs4all.net (194.109.21.1)  0.305 ms  0.360 ms  0.405 ms
 2  0.so-6-0-0.xr1.tc2.xs4all.net (194.109.5.10)  0.634 ms  0.716 ms  0.673 ms
 3  ams-ix-c00.wvfiber.net (195.69.145.58)  0.638 ms  0.601 ms  0.551 ms
 4  lon-c00-pos-4-0.OC48-ams-pos11-0.wvfiber.net (63.223.28.201)  7.512 ms  7.427 ms  7.494 ms
 5  nyc60-pos-1-0.OC48-lon-c00-pos-3-0.wvfiber.net (63.223.28.145)  84.108 ms  83.804 ms  83.995 ms
 6  66.216.1.181 (66.216.1.181)  83.435 ms  83.278 ms  83.348 ms
 7  ash-c01-tge-3-3.TG-nyc-c01-1-1.wvfiber.net (66.216.1.161)  89.563 ms  89.554 ms  89.551 ms
 8  atl-c01-tge-3-1.TG-ash-c01-3-1.wvfiber.net (66.216.1.157)  103.701 ms  103.606 ms  103.596 ms
 9  cpp-hostway.wvfiber.net (63.223.8.26)  103.678 ms  103.609 ms  103.630 ms
10  e1-12.co2.as30217.net (64.156.25.105)  113.014 ms  113.044 ms  113.084 ms
11  10ge5-1.csw5-pmtpa.wikimedia.org (84.40.25.102)  113.153 ms  113.251 ms  113.180 ms
12  rr.pmtpa.wikimedia.org (66.230.200.100)  113.069 ms  113.172 ms  113.003 ms
```

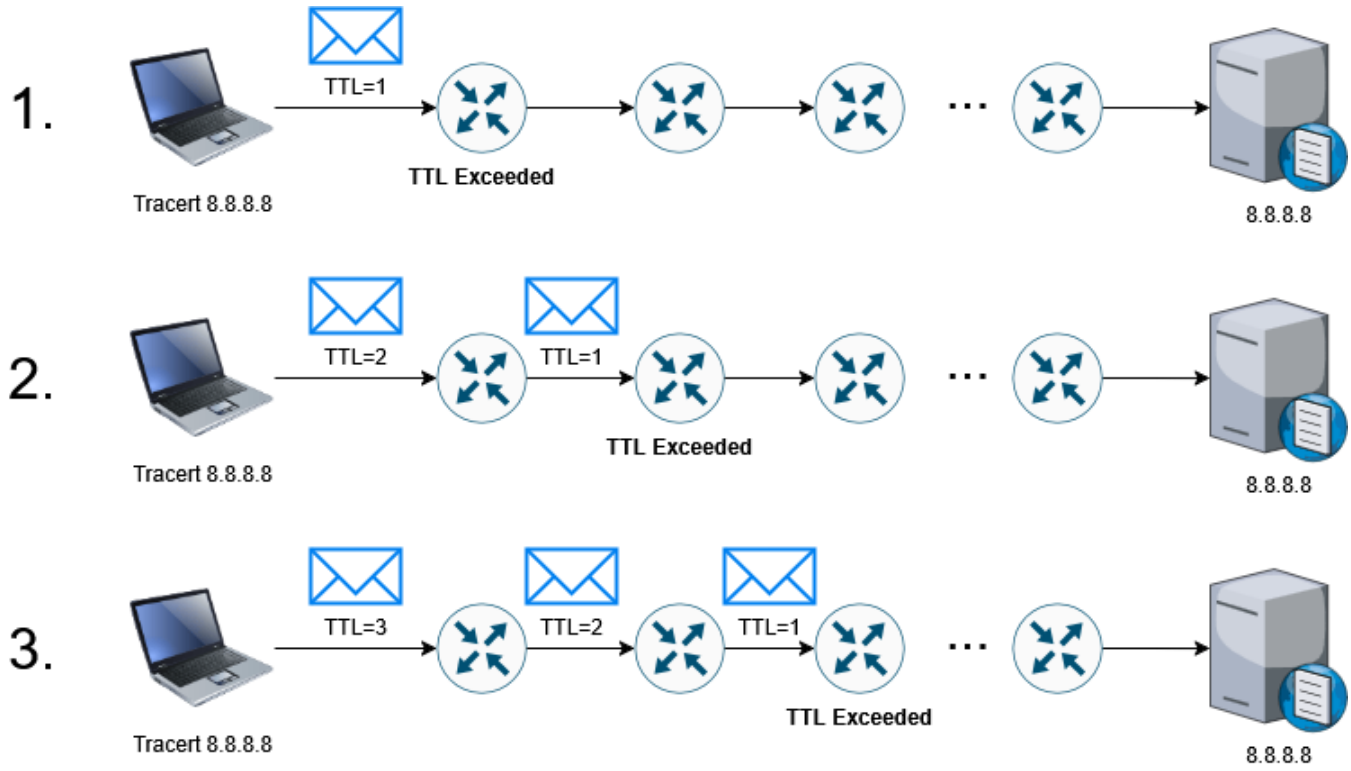
źródło ilustracji: Wikimedia.org

Kiedy wysyłasz pakiet do miejsca docelowego, często musi on przejść przez wiele routerów lub „przeskoków”.

Aby zapobiec nieskończonemu obiegowi pakietów w sieci z powodu pętli routingu (router A wskazuje na router B, który wskazuje na router A...), zawierają one pole Time-To-Live, które jest ustawiane na rozsądnie wysoką wartość, gdy pakiet jest tworzony, a każda maszyna, przez którą pakiet przechodzi, zmniejsza to pole o jeden.

Gdy pole osiągnie zero, pakiet jest odrzucany. W ramach uprzejmości router, który odrzuca pakiet, ma możliwość wygenerowania nowego pakietu przy użyciu protokołu ICMP z podtypem „Przekroczono TTL” i odesłania go z powrotem do maszyny źródłowej, aby poinformować ją, że coś jest nie tak ze ścieżką sieciową.

Ci sprytni ludzie w 1987 roku zdali sobie sprawę, że manipulując wartością TTL, można wybrać router, który wyśle tę wiadomość ICMP.



Wyślij pakiet z TTL ustawionym na 1. Pierwszy router, na który trafisz, zmniejszy go do zera. Pakiet jest teraz „martwy”, więc porzuca go i wysyła z powrotem TTL Exceeded. Ta odpowiedź będzie pochodzić z adresu IP routera - gratulacje, masz teraz adres IP pierwszego przeskoku.

Teraz wyślij kolejny pakiet z TTL ustawionym na 2. Pierwszy router zmniejszy go do 1 i przepuści, a drugi zmniejszy go do zera i porzuci. Teraz masz jego adres IP.

Powtarzaj, zwiększając TTL za każdym razem, aż ostatni przeskok odpowie. Masz teraz kompletną ścieżkę.

źródło: https://gekk.info/articles/traceroute.htm