Here is how traceroute works

```
$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
```

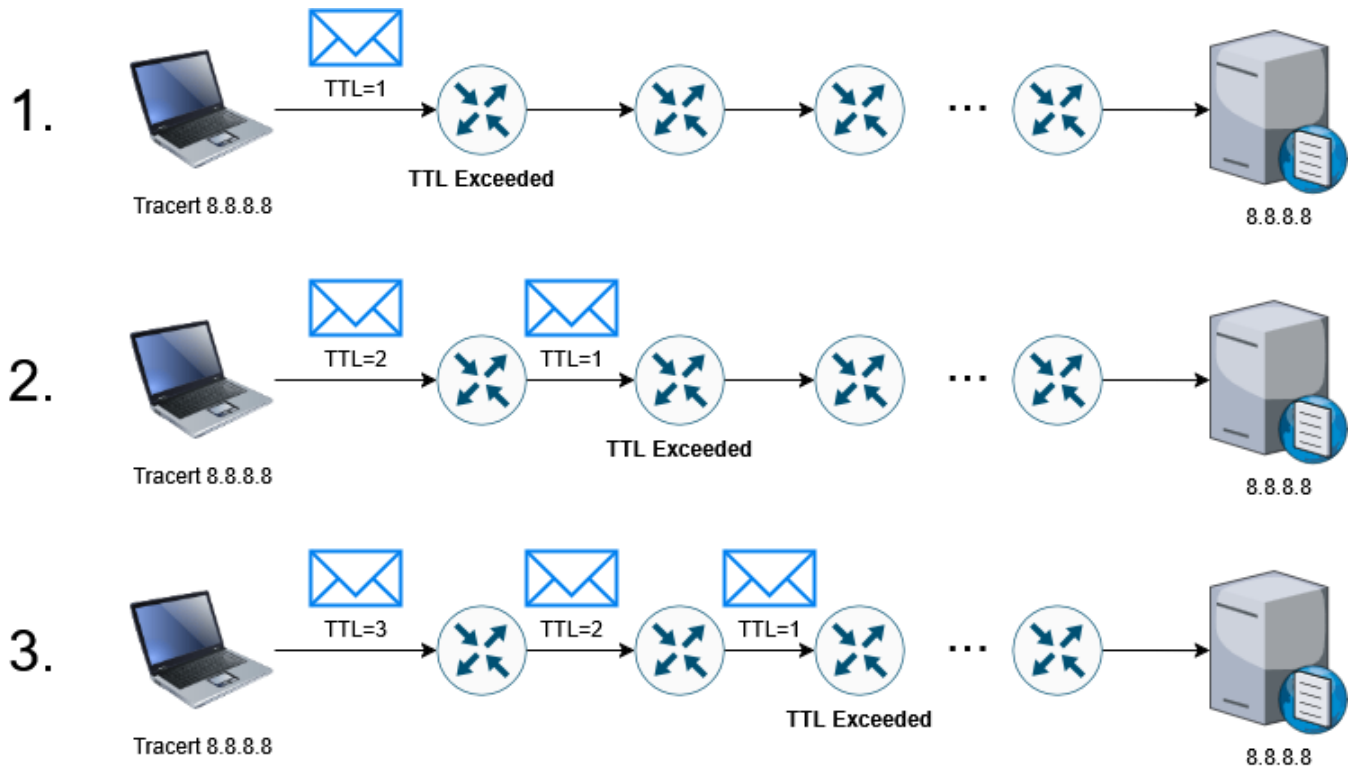
source of illustration: Wikimedia.org

When you send a packet to its destination, it often has to pass through multiple routers or 'hops'.

To prevent packets from endlessly circulating through the network due to routing loops (router A points to router B, which points to router A...), they include a Time-To-Live field that is set to a reasonably high value when the packet is created, and each machine the packet passes through reduces this field by one.

When the field reaches zero, the packet is discarded. As a courtesy, the router that discards the packet has the option of generating a new packet using ICMP with the subtype 'TTL exceeded' and sending it back to the source machine to inform it that something is wrong with the network path.

Those clever people in 1987 realised that by manipulating the TTL value, you could select the router that would send this ICMP message.



Send a packet with the TTL set to 1. The first router you hit will reduce it to zero. The packet is now 'dead', so it drops it and sends back TTL Exceeded. This response will come from the IP address of the router - congratulations, you now have the IP address of the first hop.

Now send another packet with the TTL set to 2. The first router will reduce it to 1 and let it through, and the second router will reduce it to zero and drop it. You now have its IP address.

Repeat, increasing the TTL each time until the last hop replies. You now have a complete path.

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