

# Exercise: Sending ICMP Messages With Ping & Traceroute

In this lesson, we'll look at real live ICMP packets with ping and traceroute!

## WE'LL COVER THE FOLLOWING ^

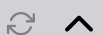
- Ping
- Traceroute
  - How It Works
  - Usage
  - Sample Output #1
  - Sample Output #2

## Ping #

When a client sends ICMP echo messages ( `ping` ), it sets a certain value in the TTL field and starts a timer. An echo server software running on the destination returns an ICMP echo reply message. Since the TTL value is decremented at each hop, the `ping` client can know the number of hops traversed by the packets. Also, when it receives the echo reply, it stops the timer and calculates the round trip time. There is a maximum value for the round trip time and when it's exceeded, the echo message is declared lost. `ping` is also often used by network operators to verify that a given IP address is reachable.

Sample usage of `ping` is shown below.

• Terminal



## Traceroute #

Another very useful debugging tool is `traceroute`. The [traceroute man page](#)

Another very useful debugging tool is `traceroute`. The [traceroute man page](#) describes this tool as “print the route packets take to network host.”

## How It Works #



Traceroute uses the TTL exceeded ICMP messages to discover the intermediate routers on the path towards a destination. The principle behind traceroute is very simple.

- When a router receives an IP packet whose TTL is set to 1, it decrements the TTL and is forced to return a TTL exceeded ICMP message to the sending host.
- To discover all routers on a network path, a simple solution is to first send a packet whose TTL is set to 1, then a packet whose TTL is set to 2, and so on. When the TTL is set to 1, the first router on the path returns a TTL expired packet, which is how its IP address can be discovered. When TTL is set to 2, the second router on the path returns a TTL expired packet, and so on. In this way, we are able to discover IP addresses of all routers on the path to the destination from the sending host. `traceroute` actually sends **three** packets with each TTL value.

Run the following call to `traceroute` to get a traceroute output of a path to [ietf.org](#) from one of Educative’s servers.

## Usage #

● Terminal



## Sample Output #1 #

```
traceroute to www.ietf.org (104.20.1.85), 30 hops max, 60 byte packets
 1  216.239.63.174 27.718 ms  27.838 ms 27.998 ms
 2  108.170.244.16 157.181 ms 157.195 ms 157.714 ms
 3  141.101.73.2
```

Here’s what some simple `traceroute` output may look like. Notice that the output is organized in rows and columns where each hop is represented by one row. Here’s what each column means:

Hop	IP Address	RTT 1	RTT 2	RTT 3
-----	------------	-------	-------	-------

Number	IP Address	R111	R112	R113
1	216.239.63.174	27.718	27.838	27.998
2	108.170.244.16	157.181	157.195	157.714
3	141.101.73.2	11.648	11.650	11.721

The **tracert** output above shows a 3-hop path (in the instance of writing this course - the number of hops and their IP addresses may be different now) between a host at Educative and one IETF's servers. For each hop, traceroute provides the IPv4 address of the router that sent the ICMP message and exactly **three** measured round-trip-times between the source and this router.

## Sample Output #2

```
tracert to www.ietf.org (104.20.1.85), 30 hops max, 60 byte packets
 1  216.239.63.174 (216.239.63.174)  27.718 ms  72.14.232.108 (72.14.232.108)  11.264 ms  216.239.63.174 (216.239.63.174)  27.598 ms
 2  108.170.244.16 (108.170.244.16)  157.181 ms  157.195 ms  108.170.243.196 (108.170.243.196)  11.721 ms
 3  141.101.73.2 (141.101.73.2)  11.648 ms  104.20.1.85 (104.20.1.85)  11.610 ms  141.101.73.2 (141.101.73.2)  11.610 ms
```

You may also get something slightly more complicated like the above. Here, there is more than one next-hop each packet can take. For example, the first hop shows 2 different IP addresses:

```
 1  216.239.63.174 (216.239.63.174)  27.718 ms  72.14.232.108 (72.14.232.108)  11.264 ms  216.239.63.174 (216.239.63.174)  27.598 ms
```

So there are multiple routes towards the destination and probes are sent to each possible next hop.



**Note** Some routers are configured by their administrators not to respond to ICMP messages. In such cases, traceroute shows \* \* \* when it times out waiting for the response. Also, by default, the traceroute utility on our platform goes to a maximum of 30 hops.

on our platform goes to a maximum of 30 hops.

---

In the next lesson, we'll study IPv4 Data Link Layer Address Resolution