Traceroute:

Packets contain a time-to-live field (referred to as TTL). The value in this field is decremented by one when it passes through a router and the entire packet is dropped by the router if the counter reaches zero. This mechanism exists in order to prevent packets from being caught in persistent routing loops in the Internet and unnecessarily consuming network bandwidth without being delivered to the appropriate destination. The source typically sets an initial value for the TTL field, which then serves as the upper bound on the number of hops traversed by the packet. If the packet is dropped when the counter reaches zero, a diagnostic packet is sent to the source from the router that drops the packet, and this diagnostic packet contains the identity of the router at which the packet is dropped. The identity is the IP address of the router, and the traceroute tool performs a reverse DNS lookup (i.e., translates the IP address to a human readable name) and reports both the IP address and the DNS name to the user.

Traceroute is a tool devised by Van Jacobson that uses this feature in order to measure the path traversed by a packet from the source to the destination. The tool sends a sequence of packets with increasing TTL values -- first with a TTL value of 1, followed by TTL value of 2, and so on -- and it prints out the identity of the router which is a certain number of hops from the source when it receives the diagnostic message indicating that the packet is dropped at a certain router. This tool also provides additional information such as: (a) it measures and reports the round trip latency from the source to the intermediate router (typically in milliseconds), (b) it issues multiple probes per hop so as to be robust to packet loss and if one of the probes is lost, it reports that with a "*" (unresponsive router hops also result in the same print message), and (c) if the different probes to the same hop reach different routers (e.g., due to path changes or load balancing that is taking place inside the network), it reports the identity of all of the routers reached by the probes. The tool stops when the destination is reached or if the number of hops exceeds a default value (typically 30).

In this exercise, you will use the traceroute tool and learn how to interpret the results reported by it.

1. Perform a traceroute to **www.facebook.com**. You can use the tool from the command line (within the Terminal application) on Linux/Mac OS X by simply running "**traceroute www.facebook.com**" and on Windows machines by issuing the following command from the command prompt: "**tracert www.facebook.com**". Answer the following questions. Add screenshots with highlights for all answers.
    a. What is the IP address associated with "www.facebook.com" (for example, "18.0.1.2")?
    b. What is the IP address and DNS name of the router that is just one hop before the destination?
    c. How many hops did it take for the traceroute to reach from your machine to the destination?
    d. Which link incurs the longest latency (or delay) from the source to the destination?
2. Perform a traceroute to **www.google.com**. Also perform a traceroute to **www.google.co.kr** and **www.google.co.in**

a. What is the IP address associated with "www.google.com"?
b. Where do you think that "www.google.com", "www.google.co.kr", and "www.google.co.in" are physically located?
c. Do you observe any unresponsive router hops (i.e., routers that don't send a diagnostic message when the packet is dropped)?
d. Are the round trip latencies observed to intermediate hops increasing uniformly or are there abrupt jumps? If there are abrupt jumps in measured latencies, can you explain why they occur?

3. www.traceroute.org provides a list of publicly available traceroute servers. Perform a traceroute to your computer from one of these servers. Also traceroute to that server from your computer. Are the same routers observed in both directions?