1. The Internet Control Message Protocol (ICMP) is typically used for error reporting and diagnostics used by hosts and routers to communicate network-layer information. As read in the text example of unable to reach a network after a presumed amount of time indicating a certain type of network connection error. It is important for the operator to at least understand that there is some sort of issue if he is not getting the right response along with using the protocol for things like troubleshooting, management, and most importantly for communication.

2. The Ping command is essentially ringing the doorbell of some host on an IP network to see if it can be reached (connected to). On ICMP, the ping command sends an echo request to the destination host and if the host can be reached then it will output the ICMP Echo Reply. If there is a connection, then we can assume at least most things are properly implemented and connected and can now gain further insight and understanding but if not we know there is some sort of error in the network, code, environment, etc.

3. Whether the traceroute command is run on Linux, Windows, or any other applicable OS, the task of identifying the path packets take to a destination remains the same. It sends packets with increasing TTL values starting at 1. Each router lowers the TTL, and when it hits 0, the router drops the packet and sends an ICMP "TTL expired" message (type 11, code 0). This maps the route step by step. Once the packet reaches the destination, it sends back an ICMP "port unreachable" message (type 3, code 3), ending the trace.