PING (PACKET INTERNET GROPPER)

1. ICMP (Internet Control Message Protocol) is a network layer protocol used for error reporting, diagnostics, and operational queries in an IP network.
2. It operates at Layer 3 (Network Layer) of the OSI model and is encapsulated within IP packets.
3. There are five common icmp message types. They are echo response (Sent to check if a host is reachable (used in Ping)), echo reply (Response to a Ping request), Destination Unreachable, Redirects the sender to use a better route, TTL expired.
4. Ping (Packet Internet Groper) is a network utility that uses ICMP Echo Request and Echo Reply messages to test connectivity between devices.
5. The sender sends an ICMP Echo Request (Type 8) to a target IP.
6. If the target is online, it responds with an ICMP Echo Reply (Type 0).
7. Sender calculates RTT and packet loss.
8. Many firewalls and security policies disable ICMP to prevent DDoS attacks (e.g., Ping of Death).

OPTIONS IN PING COMMAND :

1. ping <host/ip> (continuously pings until ctrl+C)
2. ping -c 5 <host/ip> (sends only 5 packets and analyses)
3. ping -s <pkt size> <host/ip> (to change the icmp echo packet size)
4. ping -6 <host/ip> (to use ipv6)
5. sudo ping -f <host/ip> (used for diagnosis purposes – creates ping flood)
6. ping -w <time in seconds> <host/ip> (total duration to ping)
7. ping -q <host/ip> (quiet output – releases only summary of pinging)
8. ping -i <host/ip> (Set interval between ping packets (default: 1 sec))

TRACEROUTE :

1. Traceroute is a network diagnostic tool used to track the path that packets take from a source to a destination. It helps identify network delays, routing loops, and points of failure by displaying each hop (intermediate router) that the packet traverses.

2. Traceroute works by using TTL of packets. that is, at first, source sends packet with TTL = 1 thus, probably default gateway receives and decrements TTL to 0. thereby discarding it. Due to this, router sends ICMP time exceeded message to source and traceroute records the RTT and router's IP. traceroute sends ICMP echo requests or udp packets in 33434 - 33534 port range.

3. Now, it increments TTL by 1 and repeats the above step until 30 hops are achieved.

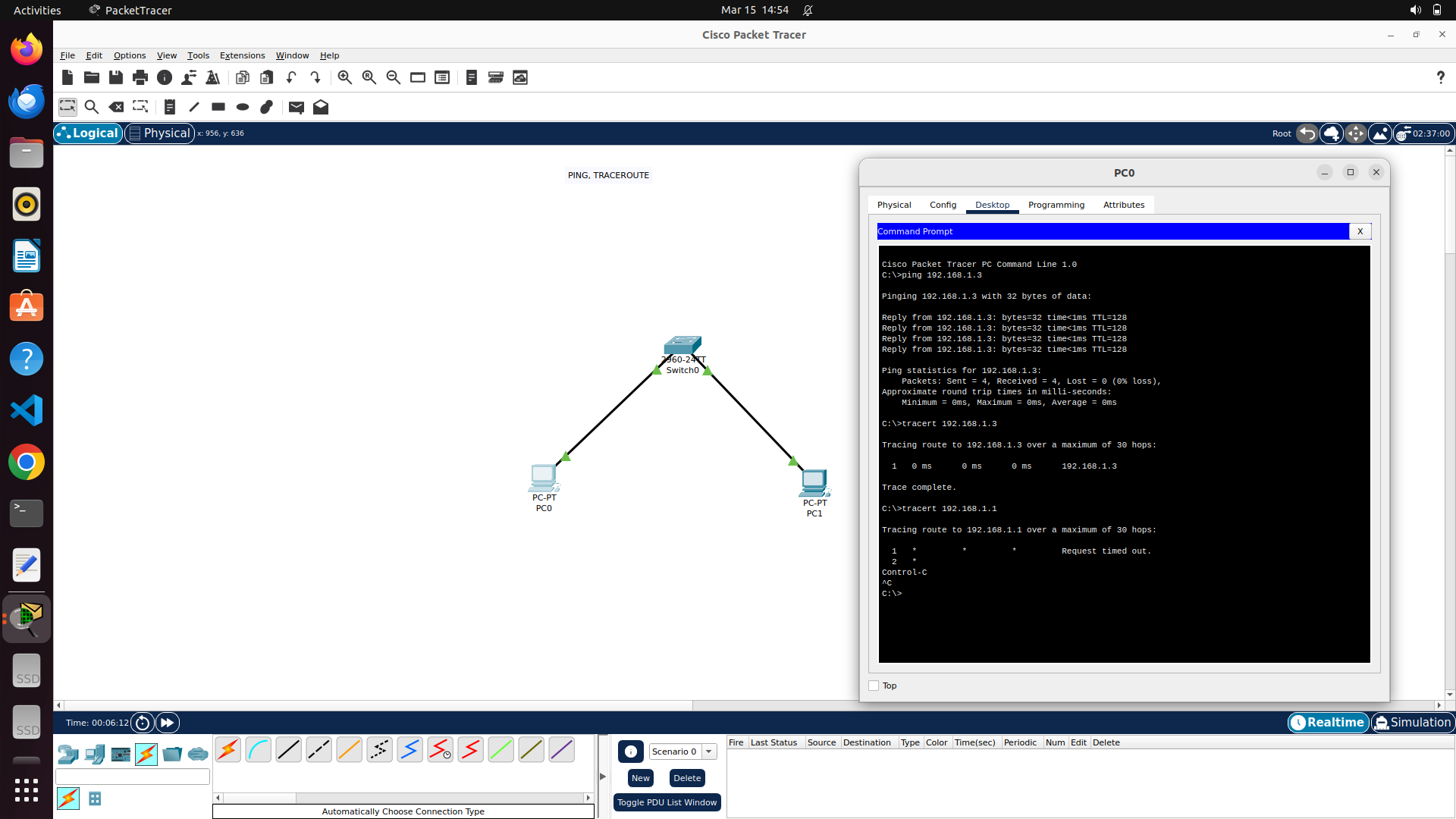
4. \* \* \* -> in traceroute means that packet got lost or firewall blocks packet.

5. !<N/H/P> -> Network/Host/Protocol is unreachable.

6. !X -> administratively prohibited.

OPTIONS IN TRACEROUTE COMMAND :

1. traceroute <host/ip> (for max. of 30 hops, it tries to find out the path of destination IP)
2. traceroute -n <host/ip> (don’t resolve IP addresses – for faster execution)
3. traceroute -I <host/ip> (use icmp packets and not udp)
4. traceroute -T <host/ip> (uses tcp packets for traceroute to avoid icmp/udp block in intermediate firewall)
5. traceroute -m <#hops> <host/ip> (limits max. number of hops)
6. traceroute -w <count> <host/ip> (set timeout per hop in seconds)
7. image showing simple LAN setup with only 2 PCs connected to switch and ping and traceroute commands got executed.



1. image showing another network constructed which gives two hopss of traceroute outputs as shown.

