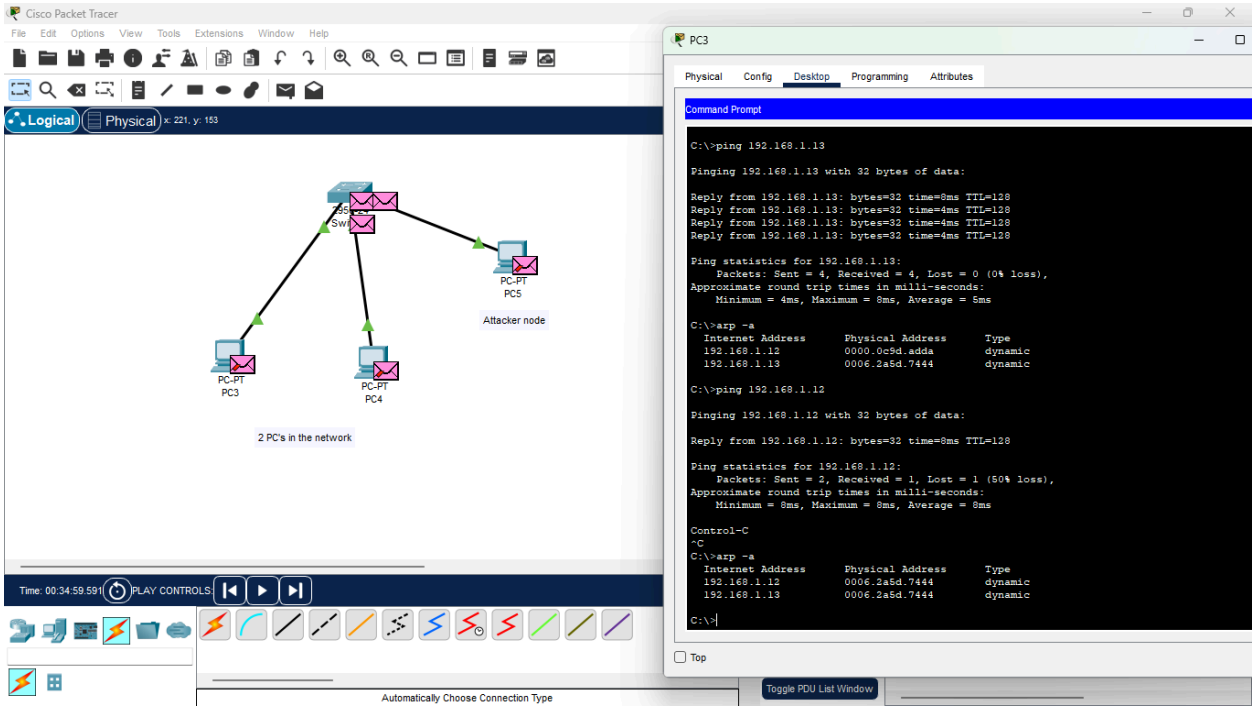
ARP Spoofing

In packet tracer , “ arp -s “ couldnt be used due to security permissions in the application hence I have used changing IP of attacker PC to the IP of another PC in the network.



Here first we passed ping to both PCs from PC3 as source to ping commands in PC4 and PC 5

Arp -a command provides the mac address of the devices in the network

C:\>ping 192.168.1.13
Pinging 192.168.1.13 with 32 bytes of data:
Reply from 192.168.1.13: bytes=32 time=8ms TTL=128
Reply from 192.168.1.13: bytes=32 time=4ms TTL=128
Reply from 192.168.1.13: bytes=32 time=4ms TTL=128
Reply from 192.168.1.13: bytes=32 time=4ms TTL=128
Ping statistics for 192.168.1.13:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -a
Internet Address Physical Address Type
192.168.1.12 0000.0c9d.adda dynamic
192.168.1.13 0006.2a5d.7444 dynamic

C:\>ping 192.168.1.12
Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=8ms TTL=128
Ping statistics for 192.168.1.12:
Packets: Sent = 2, Received = 1, Lost = 1 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms, Maximum = 8ms, Average = 8ms

C:\>arp -a
Internet Address Physical Address Type
192.168.1.12 0006.2a5d.7444 dynamic
192.168.1.13 0006.2a5d.7444 dynamic

Packets which was checking to ping PC4 but due to IP address change same as it. The packets are sent to PC5 (attacker) spoofing / pretending as someone in the network and stealing the data packets