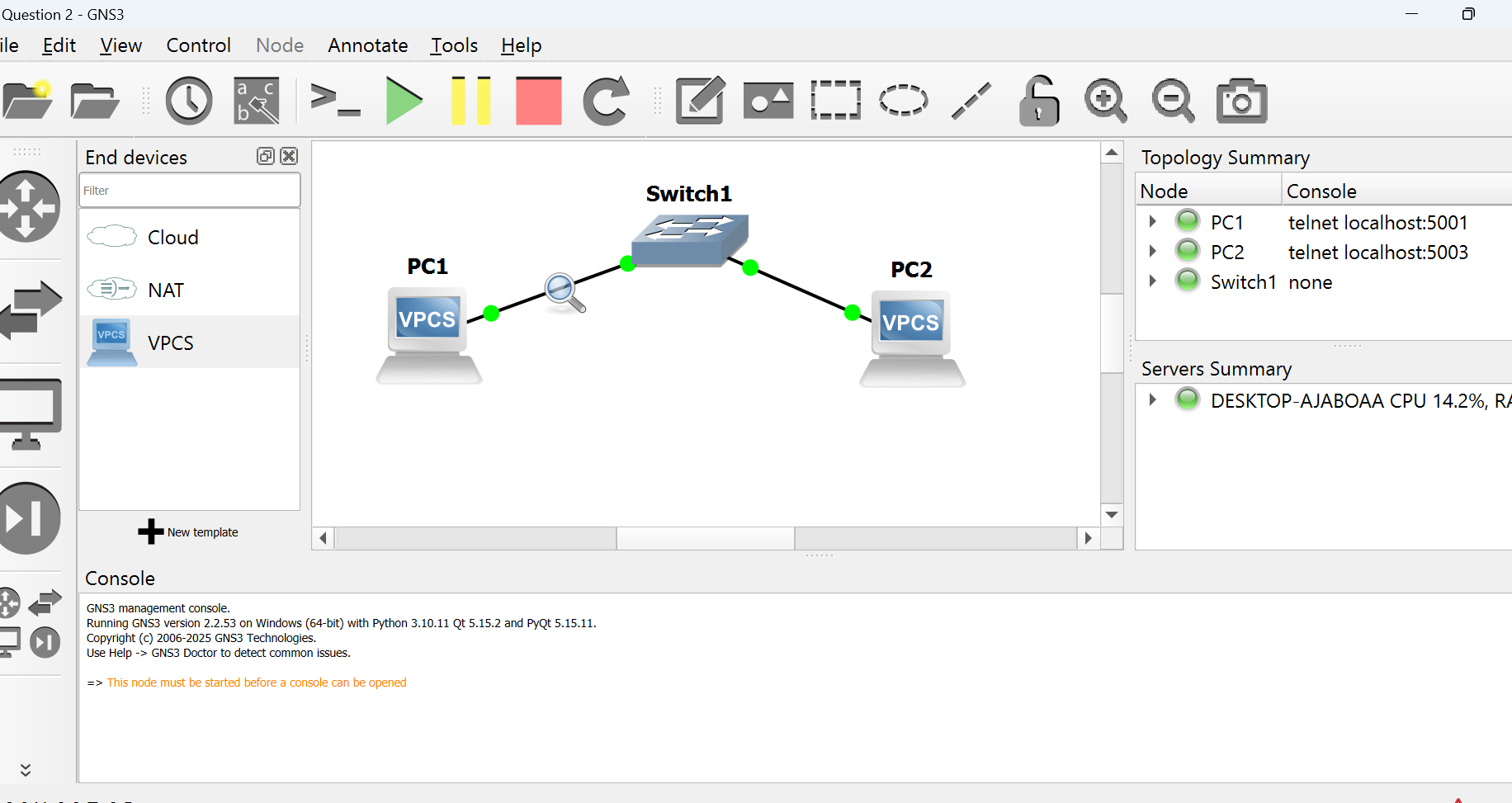
Question 2:

Capture and analyze Ethernet frames using Wireshark. Inspect the structure of the frame, including destination and source MAC addresses, Ethertype, payload, and FCS. Use GNS3 or Packet Tracer to simulate network traffic.

Approach:

We are using GNS3 for this problem because GNS3 directly show the packets in wireshark which is more informative. Cisco is also a best option but there we will get the packet details in the cisco software itself. First we are creating a ground level network with two VPC’s and a switch in GNS3

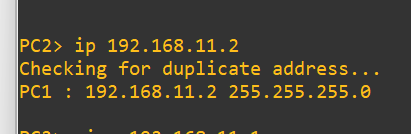
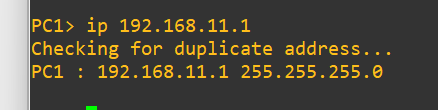
Below is the image attached of the network



Next, set ip for each VPC. Right click VPC and select console and type the command

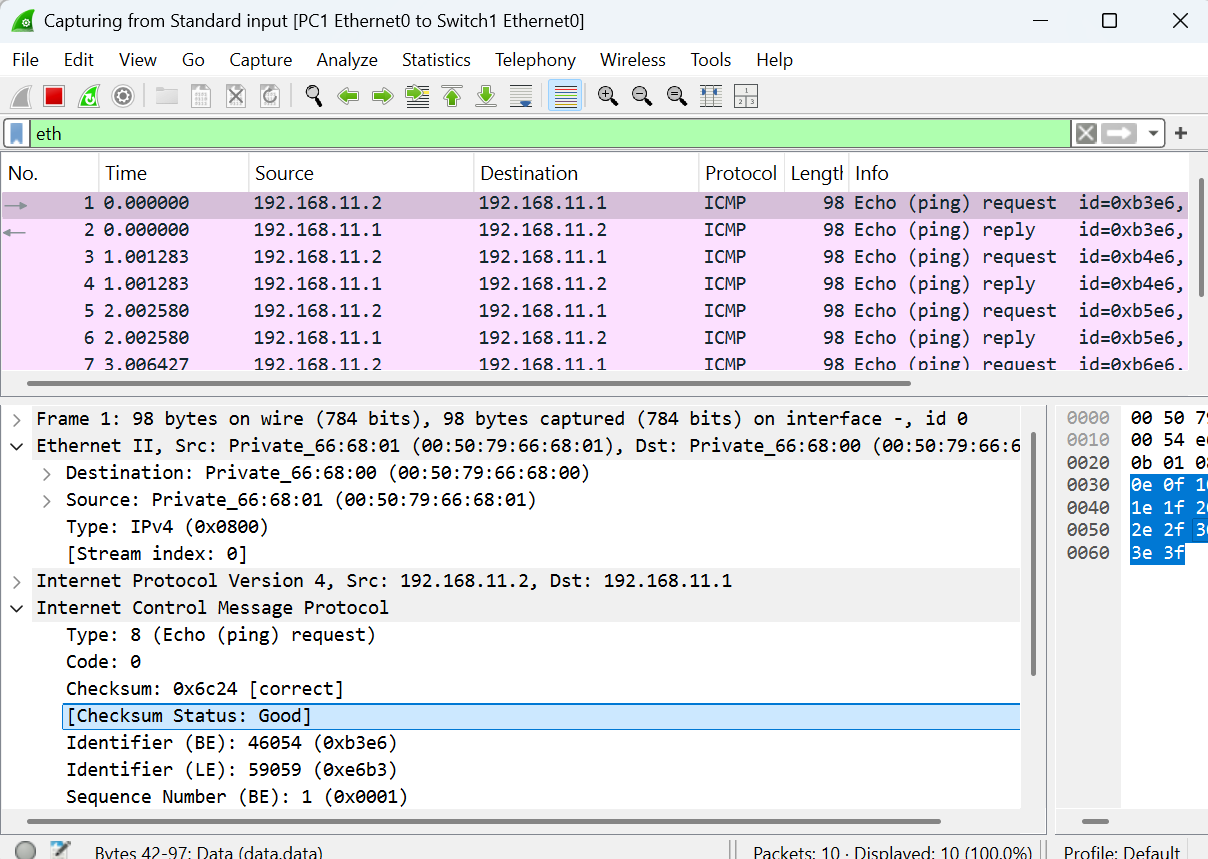
ip 192.168.11.1

follow the same on all vpc’s you have. (you can type any ip but make sure all ip are in same class)



Now right click on any VPC and select start capture option this will open the wireshark software.

Type eth on filter tab to filter all Ethernet frames



A Ethernet frame typically contains

* + **Destination MAC Address:** Where the packet is going.
  + **Source MAC Address**: Where the packet is coming from.
  + **Ethertype:** Identifies the protocol (IPv4 = 0x0800, ARP = 0x0806).
  + **Stream Index:** Helps to identify whether the packet is belong to same communication flow.