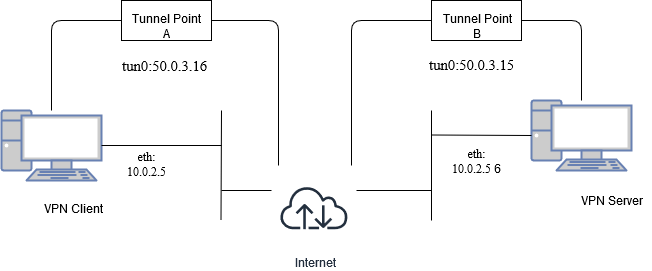
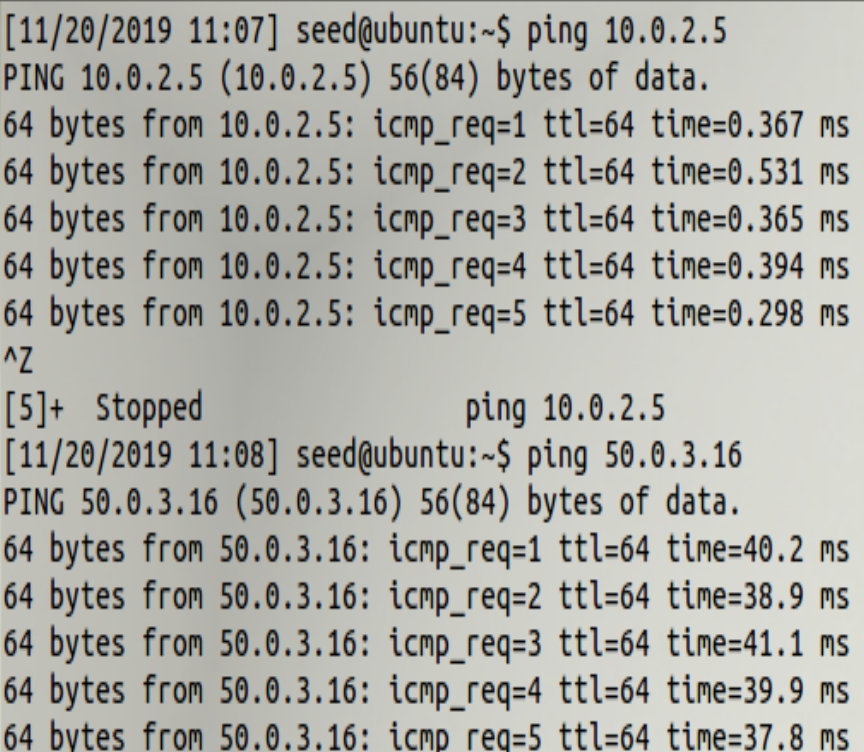
**Network Security**

**Project 2: VPN And It’s Usage**

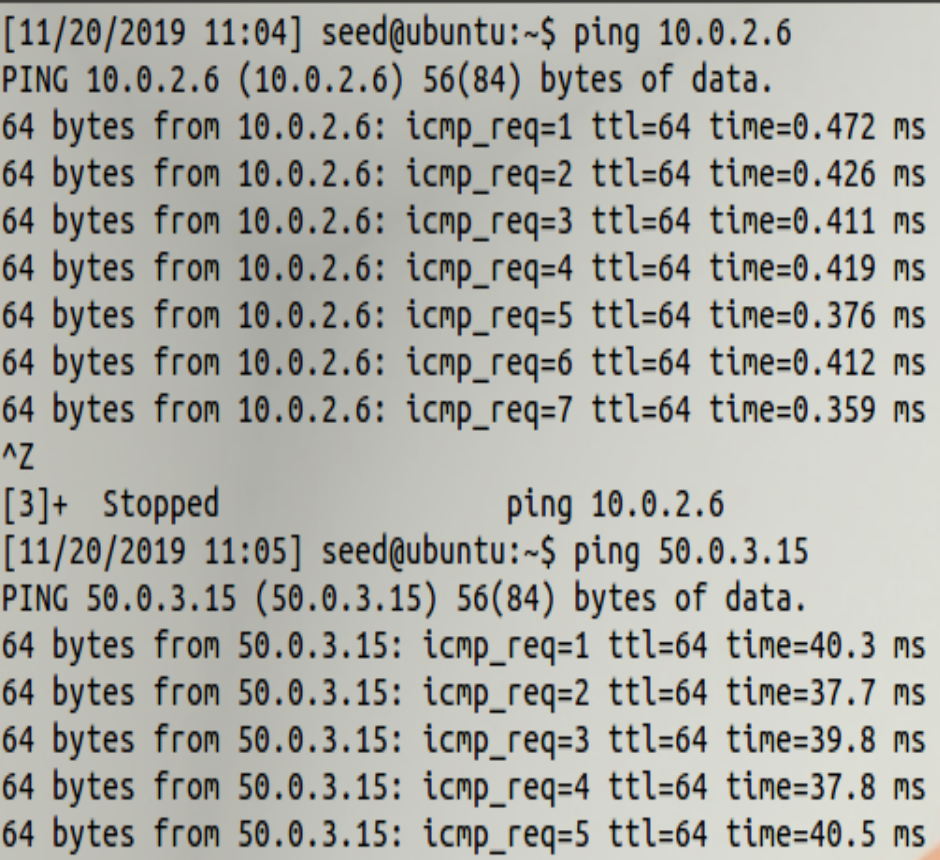
1. Describe and draw a figure to show your network environment including both the eth and tun0 interfaces/addresses on both VMs;  
     
   Eth and Tun0 Interfaces Network Diagram



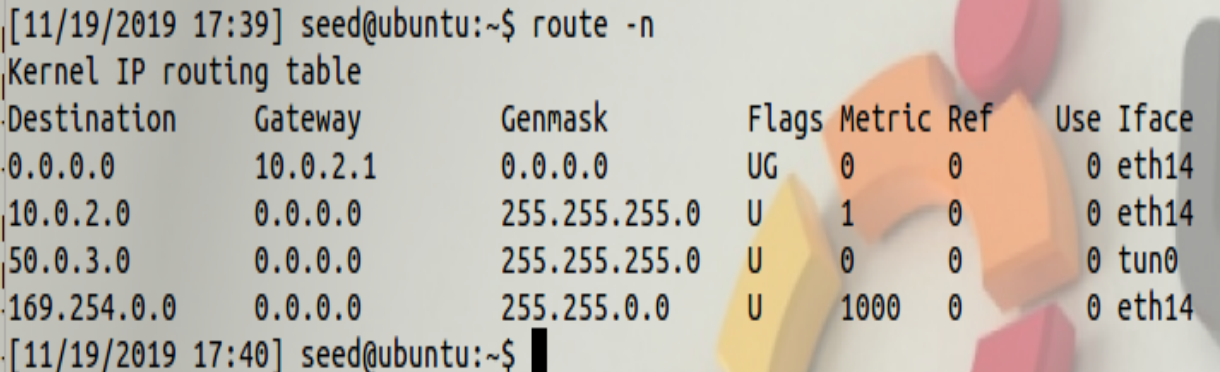
1. Screen capture to show that the two VMs can communicate with each other (ping packets between the eth interfaces and the tun0 interfaces, routing tables of the VMs);  
     
   The below figures display communication between the client and server on both, the eth interfaces and the tun0 interfaces. The VM-1 is the server whose ethernet and Tunnel IP are 10.0.2.6 and 50.0.3.15 respectively. VM-2 is the client whose ethernet and Tunnel IP are 10.0.2.5 and 50.0.3.16 respectively.  
     
   Ping Packets between Server-Client eth and tun0 interfaces:



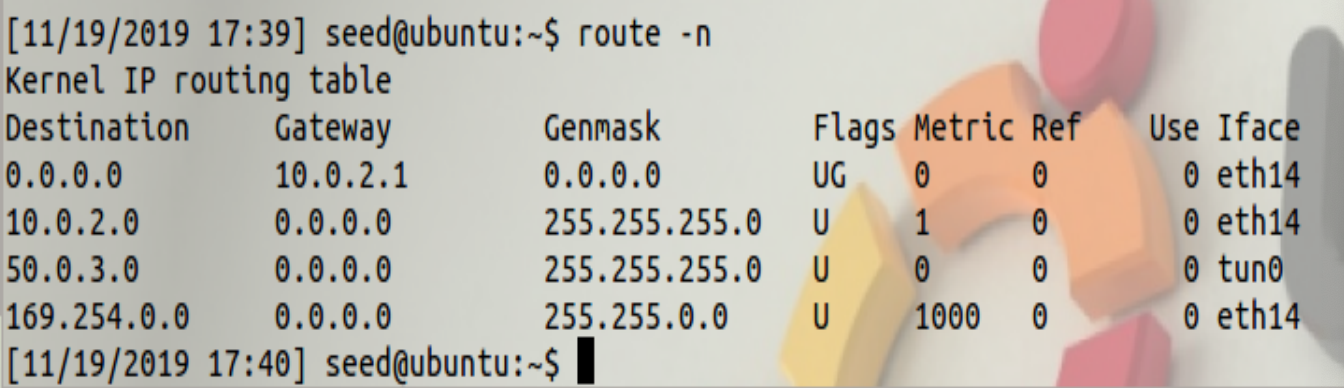
Ping Packets between Client-Server eth and tun0 interfaces:



Server’s (VM 1) Routing Table:

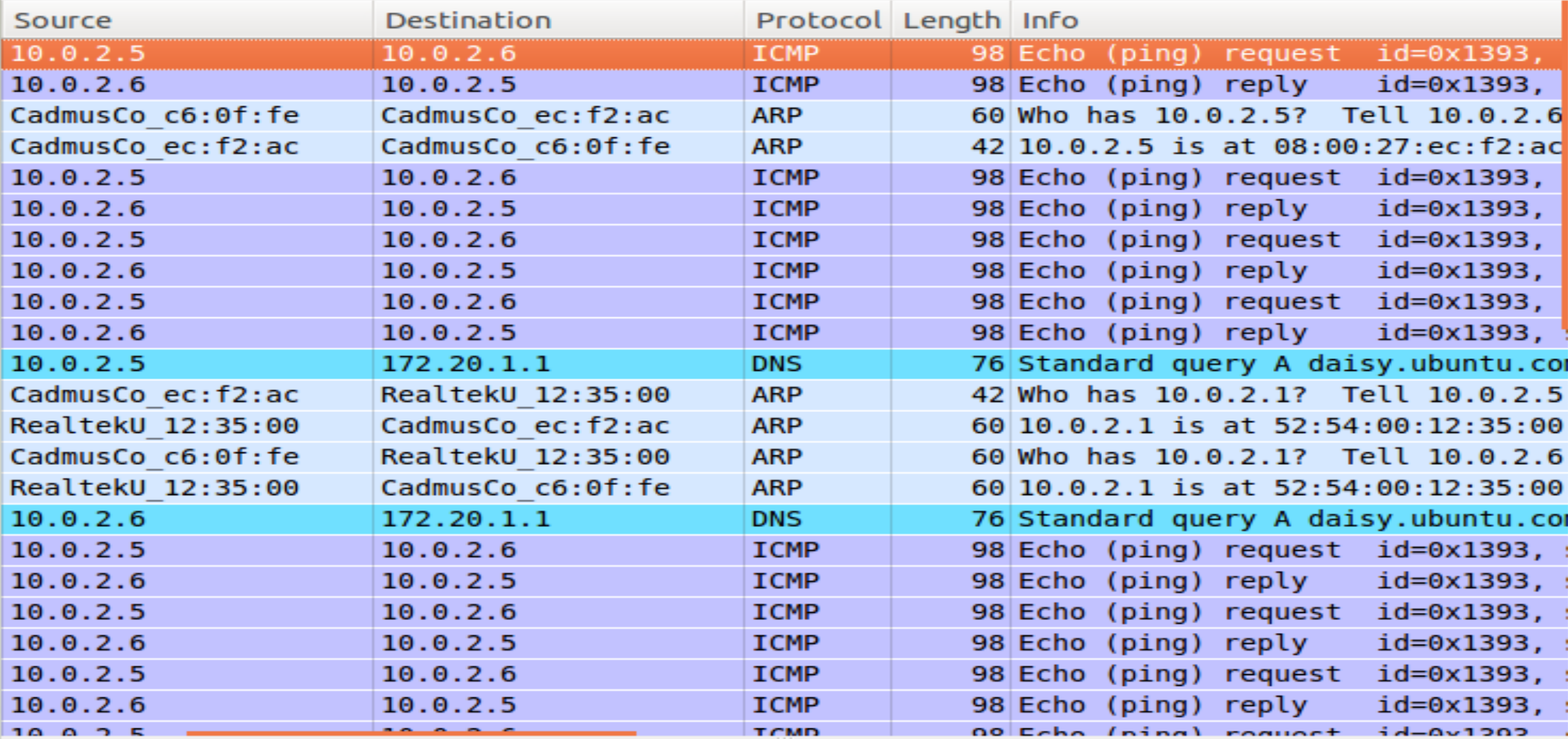


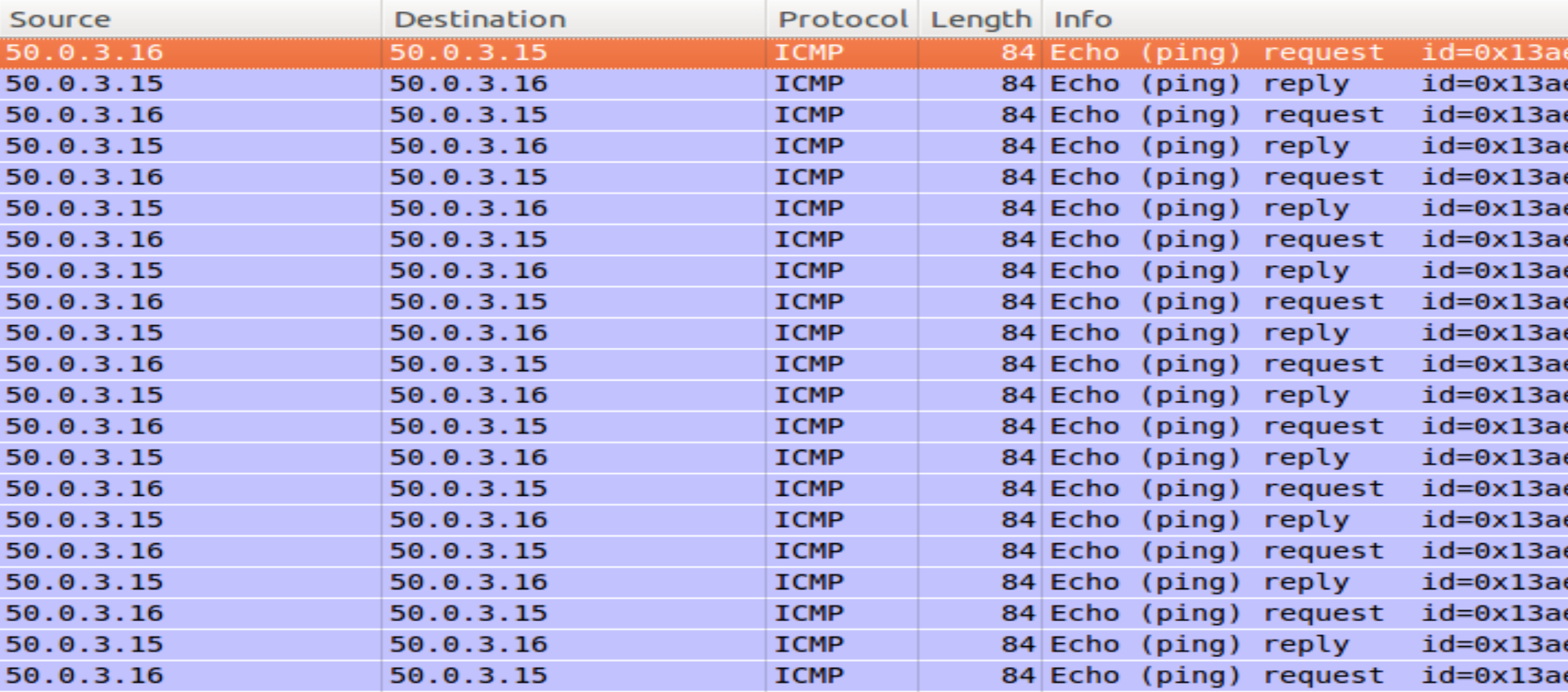
Client’s (VM 2) Routing Table:



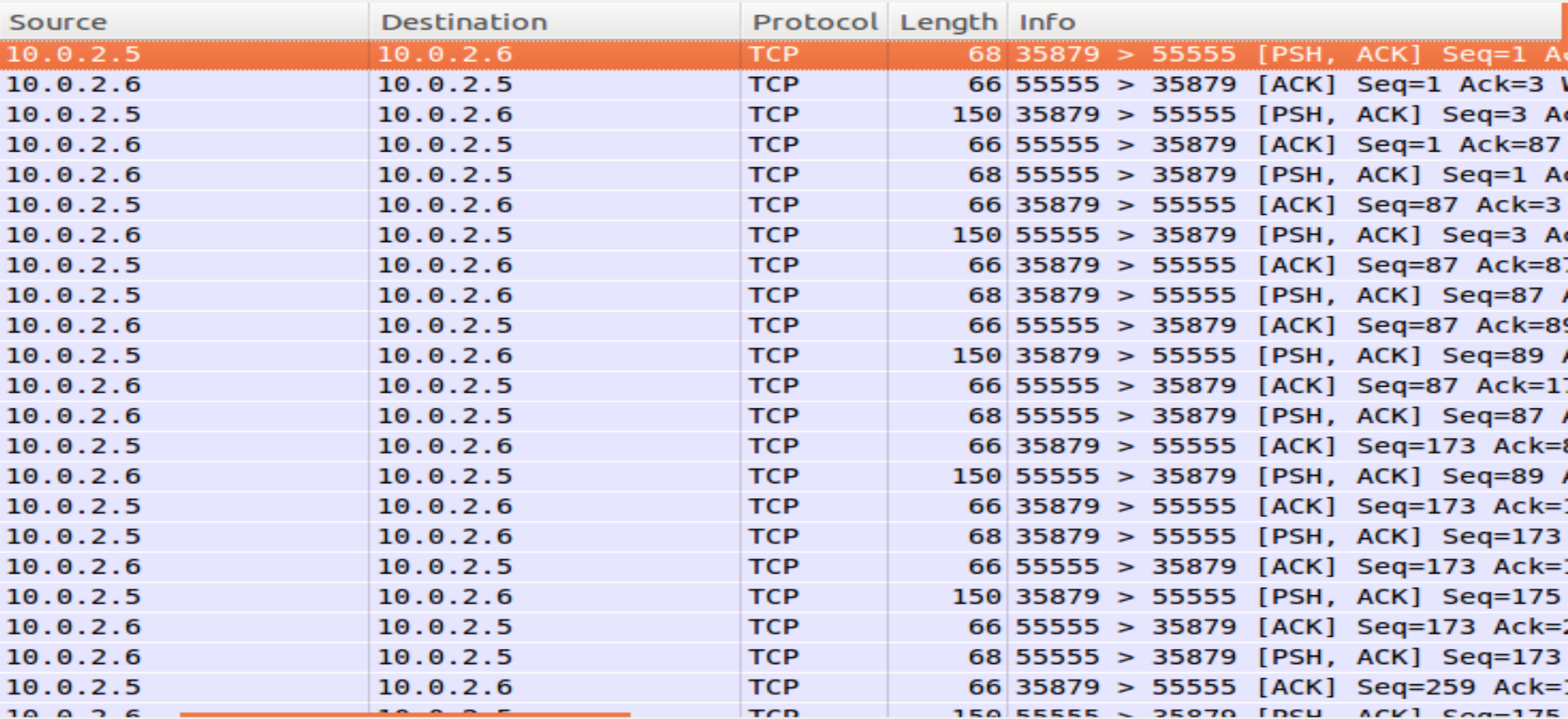
1. Screen capture of the packets that are captured by Wireshark on both VMs. Here you need to capture multiple packets from multiple interfaces (both eth and tun0) on the VMs since you need them in step (4);

Eth-Eth Interface:



Tun0-tun0 Interface:  


Eth-Tun0 Interface:



Explain how VPN uses the “tunneling” technique to hide one IP packet into another IP packet. Use your screen captures to illustrate how the technique is implemented in our experiment environment.

It’s evident from the screenshots provided above that, VPN uses IP tunneling where private leased line between the two hosts are used for communicating instead of having public internet. For instance, a user inside a certain region want to access a website that is blocked by the firewall of that region then the user can overcome this simply setting the VPN outside of the firewall. So, when the user will send a request to access that website, the original web address is encapsulated in VPN packet within normal packet and when the request is sent to firewall, it will point to VPN server that is set up by the user and hence firewall will not discard this request. Finally, when the request will reach VPN server, it will unwrap the packet and send it to that particular address.

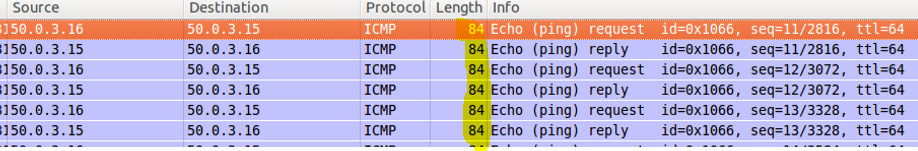
In this project, we created a tunnel called tun0 and implemented host to host tunneling between the two VMs.   
**Capture on client tun0 interface:** When the ICMP request is sent over the tunnel, the VPN will encapsulate the entire frame into the data field. The packet with its data field containing our original packet is sent.   
**Capture on client eth13 interface:** Data field of TCP packet is same as the entire frame in packet capture on eth interface.

Explain what are the IP addresses you see at the eth interfaces even when the two tun0 interfaces are communicating with each other.

The IP addresses we see at the eth interfaces are still the two eth IPs of our client and server i.e. 10.0.2.6 and 10.0.2.5 . The protocol displayed on eth interfaces when two tun0 interfaces are communicating is TCP.

When the two tun0 interfaces ping each other, what is the size of the tun0 packets?

As shown below, the size of the tun0 packets is 84 bytes.

  
  
What is the size of the eth packets?

As evident, the size of the eth packets is 150 bytes

