[4 marks] What is the maximum number of available host IP addresses that can be used by the group? Briefly explain your answer

'IPv4 network address 133.166.199.0/24'
Addresses and masks have 32 bits.
On a /24 network, the length of the network part in the IP addresses for this network is 24 bits which means eight bits represent the host ID (32-24)
With eight host bits available, this ranges from 0 to 255, encompassing 256 possible host Ip addresses (2^8 = 256)

Application:
we have a range of 256 host ids, ranging from 133.166.199.2 to 133.166.199.254

we have three reserved addresses as followed:
Network Address: 133.166.199.0/24
Default Gateway: 133.166.199.1
Network broadcast address: 133.166.199.255

The number of available host IP addresses is 253 (256-3).

[6 marks] The DREAMING group leader envisaged that there will be SIX subgroups and wants each group to have an IP subnet with as many host IDs as possible within each subnet. Consider how you would further partition the given network address to achieve this. How many bits would each subgroup's network ID be and therefore what is the corresponding netmask, e.g. /25 or /26 or /27 or … ? Briefly explain your answer listing the possible subnetwork addresses in CIDR format, i.e., /<network address>/<netmask>.

Network IP Address = 133.166.199.0 / 24
Number of Subnets Required = 6

Addresses and masks have 32 bits.
We are given 8 bits (2^8 = 256) since our network is /24 (32 - 24 = 8).
The required number of subnets is 6, this not a power of 2 so we need to pick the next higher power of 2 (8) which is 8 is 2^3. This implies that 3 bits are needed to denote subnets.
The 24 bits you already have plus the 3 bits borrowed from the host bits for the subnets is 27 bits. These 27 bits denote the Network and Subnet.
That leaves 5 bits (32-27) for the number of addresses (2^5 = 32) per subnet.

Therefore, the net-mask = 255.255.255.224 or /27. A max of 32 IP addresses are available in each Subnet.

Subnet No.	First IP Add	Last IP Add	CIDR
1	133.166.199.0	133.166.199.31	/27
2	133.166.199.32	133.166.199.63	/27
3	133.166.199.64	133.166.199.95	/27
4	133.166.199.96	133.166.199.127	/27
5	133.166.199.128	133.166.199.159	/27
6	133.166.199.160	133.166.199.191	/27
7	133.166.199.192	133.166.199.223	/27
8	133.166.199.224	133.166.199.255	/27

[8 marks] During the first week of operation, with only FIVE staff working in the lab, everything seemed fine. Later, as increasingly more students started working in the lab, everyone complained that the network was slow even though they were just working on their "local server", e.g., users on n14, n15 and n16 connecting to S1 only, users on n18, …, n20 connecting to S2 only, etc. What is the reason for the network to be slow?

<u>It is likely due to the use of hubs:</u>

>Network hubs can only send or receive data at any given time (half-duplex mode). A hub in a network situation is constantly switching between sending and receiving data, which creates an inefficient data flow process.
>Network hubs share all their bandwidth between every connected device. If one computer is sending a large file to another computer, it's going to occupy all the bandwidth and give the other two computers slow network access.
>Hubs are unable to differentiate between the devices on the network. If one computer is trying to reach another on a hub-based network, the computer will send the message to every other computer on the network, consuming bandwidth for each transfer.
>Hub can't support collision domain as well as re-transmission of frames so due to this, to increase the probability of collision.

<u>4. The two postgraduate students who set up the network were called to explain. With only minimal networking knowledge that they acquired from unreliable online sources, they were clueless. Coincidentally, one of the undergraduate students working in the lab was also taking NWEN243 and recalled something she learnt from the lectures on link layer addressing and forwarding. She explained the likely cause of the slowness and suggested replacing the hubs with switches. After listening to her explanation, the DREAMING group leader agreed to purchase switches to replace the hubs. The network topology remained the same, as shown below. The network became "faster" and everyone was happy.</u>

(a) <u>[6 marks] Explain how switches improved the network performance. You should include details like which layer of the protocol stack switches operate on, how they forward traffic, what information they collect/store, etc.</u>

Switches interact with the link layer to forward incoming traffic to the correct media access control address. Each switch has a routing table which is either manually set up or automatically created based on a trial and error self-learning system. With this forwarding table, switches can forward the outgoing frames to the correct/next destination based on the frame's media access control address. The outcome of replacing hubs with switches is less bandwidth being consumed as unnecessary frame broadcasts are not occurring.

(b) <u>[8 marks] The network was restarted after the switches were installed and all the switches' memory/tables were empty. The undergraduate student working on n8 executed the ping command to check connectivity with the web server S4, i.e., n8$ ping -c 1 133.166.199.S4 Explain, step-by-step, how the ping (echo request) packet is switched/forwarded from n8 to S4 and, similarly, how the ping reply (echo response) packet is switched/ forwarded back from S4 to n8. You may assume that n8 and S4 were not powered off and their ARP caches still contain the MAC addresses S4 and n8 respectively. [Hint: see lecture notes on switch forwarding.]</u>

Assuming switches have not been filled once the server is pinged:
When the server is pinged, S1 will look for an entry corresponding to the destination MAC address (S4). Finding none, S1 will forward the packet to SW1. SW1 has no routing table, therefore it will temporarily act as a hub and broadcast the packet to all connected devices. SW2 will receive this broadcast and the same event will occur again. SW2 will broadcast and be received by SW3; SW3 will broadcast and be received by SW4. SW4 will then forward the packet to the webserver (destination MAC address). For returning the packet, the routing tables will now follow the same path backwards as the self-learning system has filled in the forwarding table.

<u>(c) [6 marks] Thinking that the network problem has been solved, the two postgraduate students connected 14 more PCs/workstations to the network using TWO hubs without realizing that the switches have very limited memory and could only store up to 32 MAC /</u>

link layer addresses each. When all the PCs/workstations were being used by students to work on their projects, the network became very slow again. Briefly explain the cause of the poor network performance when all the workstations were being used.

There are a total of 25 devices on the network initially.
If 14 PCs are added and are connected to the 2 hubs (1 hub is connected to a switch), each switch will have to store a total of 39 addresses. Switches forwarding table's have limited space due to low memory, as they are only able to store 32 MAC / link-layer addresses each. As there are more MAC addresses than available slots in the forwarding tables, the switches cannot hold the forwarding instructions for all PC's/workstations. The limited memory space means when an address which is not in the forwarding table (Due to limited space) is broadcast, the switch will act as a hub (broadcast out to all connected device). This causes slowdowns and additional bandwidth costs.

5. [12 marks] The address resolution protocol (ARP) is used to translate a host's IPv4 address to the corresponding MAC address. With reference to the figure below, state and briefly explain which IPv4 address the respective sender should indicate in the ARP request in order to transmit a datagram to the receiver:

(a) **Node N1 sends a datagram to Node N2**
172.16.0.21
N1 looks for destination 172.16.0.21 in its routing table to check if the source 172.16.0.22 is in the same subnet. As they are, it indicates N2's IP address inside of the ARP request.

(b) **Node N1 sends a datagram to Server**
172.16.0.1
N1 looks for the destination 172.16.4.10 in its routing table to check if the source I172.16.0.22 is in the same subnet. As they aren't, it indicates R1's IP address inside of the ARP request.

(c) **Node N2 sends a datagram to Node N3**
17.16.0.1
N2 looks for the destination 172.16.1.2 in its routing table to check if the source 172.16.0.21 is in the same subnet. As they are not, it indicates R1's IP address inside of the ARP request.

(d) **Node N3 sends a datagram to Server**
172.16.1.1
N3 looks for the destination 172.16.4.10 in its routing table to check if the source 172.16.0.21 is in the same subnet. Since they aren't, it indicates R1's IP address inside of the ARP request.