**Computer Networks – Internet Protocol:**

1a. Find out the IP address of your machine. - 192.168.1.4

b. Identify its CLASS- class C

c. Identify its category – Private or Public-private

2.What is the Network Mask of your machine. Use it to find the Network ID of your machine.

Network Mask-255.255.255.0, Network ID: 192.168.1.0/24

3.The IP address and Mask combination, written in prefix/length notation is given below:

* + 1. Device A: 172.16.17.30/20
    2. Device B: 172.16.28.15/20

Find out if both the devices belong to the same subnet or not?

Both device A and Device B belong to different subnet. They don’t match in the 3rd position and are hence different subnets.

1. What is the need for an IP address? which devices use this address?

IP addresses are the numbers that enable our computers, servers, telephones, cameras, printers and sensors to communicate with each other. Without IP addresses, we would have to copy data from device to device manually, using CDs, DVDs, hard disks or flash storage, such as a USB drive.

1. What is IPv4, IPv6?

IPv4 has a 32-bit address length. It can generate 4.29×109 address space

IPv6 has a 128-bit address length. Address space of IPv6 is quite large it can produce 3.4×1038 address space

1. What is Mac address? What is its length? Which devices use this address?

MAC Address is also known as the Physical Address of a network device. Unique 48-bits hardware number of a computer, which is embedded into a network card (known as a Network Interface Card/Controller device).

1. What are the layer 2 and layer4 protocols?

The Layer2/Data Link layer also defines a lower level addressing structure to be used between end systems as well as the lower level framing and checksums being used to transmit onto the physical medium. Ethernet, Token Ring, and Frame Relay are all examples of Data Link layer or Layer 2 protocols.

The Transport layer is the first at which we see the concept of packets or datagrams of information that will be transported across the network. TCP, UDP, and ICMP are examples of Layer 4 protocols used to provide a delivery mechanism between end stations.

1. Devices below work at which layer?

a. Routers -Network Layer b. Gateways- Network Layer c. Bridge-datalink layer

d. Switches-Data Link layer

1. What is a socket? What are the different types of sockets?

Sockets allow communication between two different processes on the same or different machines. To be more precise, it's a way to talk to other computers using standard Unix file descriptors.

Types: Datagram and Stream sockets

1. Give few eg for applications based on protocols below.
   1. TCP :

* Bootstrap Protocol.
* Connecting to the Internet.
* Dynamic Host Configuration Protocol.
* Domain Name System.
* E-mail.
* File Transfer Protocol.
  1. UDP
* Domain Name System (DNS)
* Simple Network Management Protocol (SNMP)
* Routing Information Protocol (RIP)
* Dynamic Host Configuration Protocol (DHCP).

1. What is the port number used for the following protocols?
   1. tftp: 69 b. smtp: 25 c. dns: 53 d. dhcp: 67 for server, 68 for client

e. telnet: 23 f. ssh: 22

1. Identify the class (A, B, ..) and category (Private or public) of the following ipaddress.
   1. 192.168.1.3 – Class C private
   2. 172.30.5.5 – class B private
2. For the foll. ip address, find the a) network address b) broadcast address (Hint: in node ip address, set all the host bits to 1) c) first usable address d) last usable address
   1. 147.144.1.218/16:

* Network: 147.144.0.0/16
* Broadcast: 147.144.255.255
* First usable: 147.144.0.2
* Last usable: 147.144.255.254
  1. 192.168.1.3/24:
     1. Network: 192.168.1.0/24
* Broadcast: 192.168.1.255
* First usable: 192.168.1.2
* Last usable: 192.168.1.254

1. What is NAT and port forwarding?

NAT - Network address translation is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

Port Forwarding - Port forwarding or port mapping is an application of network address translation that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall