Computer Networks

Question 1: What is computer network?

Answer: A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.

Question 2: What is a protocol?

Answer: A communication protocol is a system of rules that allow two or more entities of a communications system to transmit information via any kind of variation of a physical quantity. The protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods.

Question 3: What is OSI Model?

Answer: The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other.

There are 7 OSI layers

- **Application Layer:** At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
    - Example: Application – Browsers, Skype Messenger etc.
    - Describes the application over which the data is transmitted at application level like HTTP, HTTPS, SSH etc.
- **Presentation Layer:** The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
    - **Translation:** For example, ASCII to EBCDIC
    - **Encryption:** Presenetation layer is responsible for encrypting the data.
    - **Compression:** Presenetation layer is responsible for compressing the number of bits to be tranmitted over network.
- **Session Layer:** In computer science and networking in particular, a session is a temporary and interactive information interchange between two or more

communicating devices, or between a computer and user. This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
    - **Session Handling**: Session establishment, maintenance and termination happens here
    - **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
    - **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.
- **Transport Layer:** Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as **Segments**.
    - **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
    - **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service **point address** or **port address**. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.
    - **Sets Connection Type:** Adds if TCP or UDP connection.
- **Network Layer:** Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.
    - **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
    - **Logical Addressing**: In order to identify each device on inter-network uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.
- **Data Link Layer:** The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
    - **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can

be accomplished by attaching special bit patterns to the beginning and end of the frame.
    - **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
    - **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames
    - **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
    - **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.
- **Physical Layer:** The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits.
    - **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
    - **Bitrate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
    - **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
    - **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Question 4: Explain what is happening practically in OSI layer.

Answer:

- Router here does not mean the one we see in home, they are actually combination of router and switch
- All layer other than physical layers are providing some logical calculations only Here is my logic
- Application Layer, Presentation Layer and Session Layers are work of browser (or application) only that is why it is merged in TCP/IP model
- Transport Layer is also browser work which tell from which port it will read the data but is actually solving logic for OS-software connection and getting it ready in boxes (called segments) to be loaded on truck.
- Network Layer is actually solving logic for where data should go next (or which turn truck needs to take next).

- Now Network Layer is just telling a logical or refferential address known as IP address so it makes it difficult to communicate with physical layer.
- Data Link Layer is like a friend who tells cab driver your correct address when you ask driver to go your home.
- Once Data Link Layer gives physical address, Physical layer drives the data physically.
- All this communication has happened between two routers only and happens multiple times so it reach its final destination.

Question 5: What is Access Point?

Answer: Access Point(AP) is a wireless LAN base station that can connect one or many wireless devices simultaneously to internet.

Question 6: What is Circuit Switching and Packet Switching?

Answer:

- **Circuit Switching-** This switching happens in physical layer. What happens is that once connection is created, then data flows continuously.
  - There is a dedicated path
  - Contiguous Flow is there
  - Data is always in an order
  - Less Efficiency
  - There is less delay
- **Packet Switching-** We send data in packets, as discussed for OSI layer. All logics happens as discussed in OSI or TCP/IP model.
  - There is a store and forward switching, data is stored and then forwarded so in case data is lost, then it can resend.
  - No order of packets
  - More efficiency
  - There is more delay as if resources are not free, then packet waits in queue.

Question 7: What is a firewall?

Answer:
A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.

A firewall can be hardware, software, or both.

- **Host based Firewalls:** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
- **Network based Firewalls:** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

Question 8: What is the difference between private IP address and public IP address?

Answer:

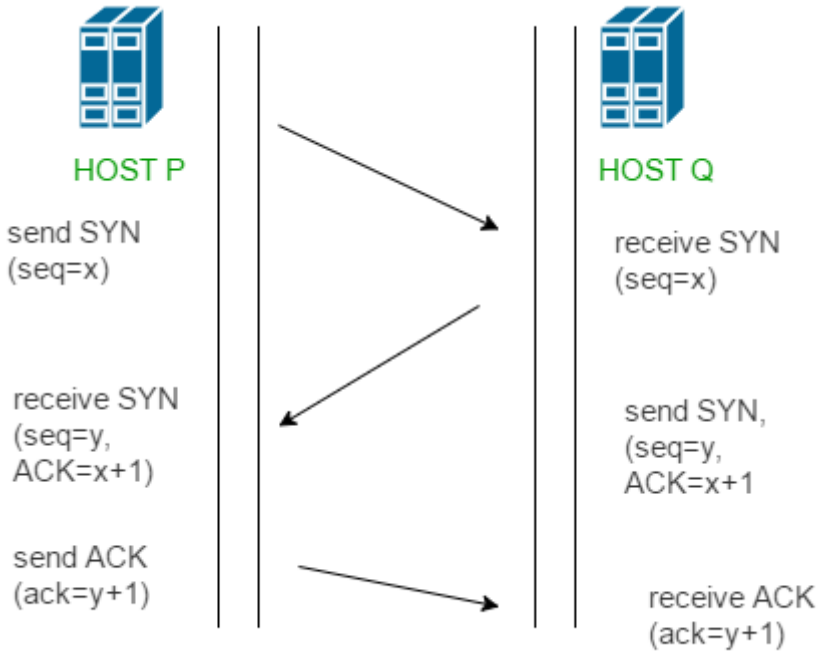
Key	Private	Public
Scope	Private IP address scope is local to present network.	Public IP address scope is global.
Provider	Local Network Operator creates private IP addresses using network operating system.	ISP, Internet Service Provider controls the public IP address.
Cost	Private IP Addresses are free of cost.	Public IP Address comes with a cost.
Range	Limited	Anything other than Private range is available for public

Question 9: What is a 3 way handshake?

Answer: It is how TCP establishes connection.

- **Step 1 (SYN):** In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with

- **Step 3 (ACK):** In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start the actual data transfer



Question 10: What is cryptography?

Answer: Cryptography is the science of secret writing with the intention of keeping the data secret. Cryptography can be classified into 2 categories

- **Encryption-** Encryption is a process that encodes a message or file so that it can be only be read by certain people. Encryption uses an algorithm to scramble, or encrypt, data and then uses a key for the receiving party to unscramble, or decrypt, the information. The message contained in an encrypted message is referred to as plaintext. In its encrypted, unreadable form it is referred to as ciphertext. Encryption is of 2 types
  - **Symmetric Encryption-** Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys.
    - **Public Key-** This key is given to public and data can be encrypted using this key.
    - **Private Key-** This key is kept with the receiver and is used for decryption of data.
  - **Asymmetric Encryption-** Asymmetric Encryption uses two distinct, yet related keys. One key, the Public Key, is used for encryption and the other, the Private Key, is for decryption. As implied in the name, the Private Key is intended to be private so that only the authenticated recipient can decrypt the message.

- **Hashing-** Hashing is the process of converting a given key into another value. A hash function is used to generate the new value according to a mathematical algorithm. The result of a hash function is known as a hash value or simply, a hash. A good hash function uses a one-way hashing algorithm, or in other words, the hash cannot be converted back into the original key.

Question 11: Explain classes in IP addressing.

Answer: IP addresses are globally managed by **Internet Assigned Numbers Authority(IANA)** and **regional Internet registries(RIR)** There are 5 classes of IP addresses

1. **Class A-**
   - 0 (7-bit Network ID) (24 bit Host ID)
   - $2^7 - 2 = 126$ network ids (0.x.y.x and 127.x.y.z are reserved)
   - $2^{24} - 2$ host ids (x.0.0.0 is subnet mask and x.255.255.255)
2. **Class B-**
   - 1 0 (14-bit Network ID) (16 bit Host ID)
   - 2^{14} network ids
   - $2^{16} - 2$ host ids (x.y.0.0 is subnet mask and x.y.255.255)
3. **Class C-**
   - 1 1 0 (21-bit Network ID) (8 bit Host ID)
   - 2^{21} network ids
   - $2^8 - 2$ host ids (x.y.z.0 is subnet mask and x.y.z.255)
4. **Class D-**
   - 1 1 1 0 (28 bit Host ID)
   - IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
5. **Class E-**
   - 1 1 1 1 (28 bit Host ID)
   - Reserved special IP addresses

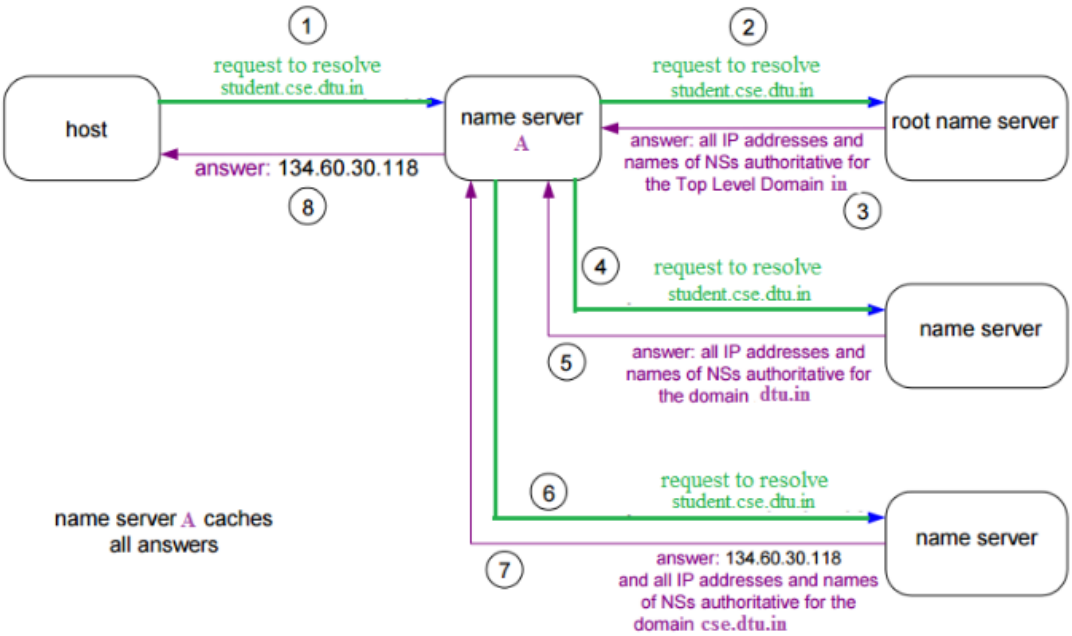
Question 12: What is classless IP addressing?

Answer: To reduce the wastage of IP addresses in a block, we use sub-netting. What we do is that we use host id bits as net id bits of a classful IP address. We give the IP address and define the number of bits for mask along with it (usually followed by a '/' symbol), like, 192.168.1.1/28. Here, subnet mask is found by putting the given number of bits out of 32 as 1, like, in the given address, we need to put 28 out of 32 bits as 1 and the rest as 0, and so, the subnet mask would be 255.255.255.240.

Question 13: Explain domain name system.

Answer: DNS is a hostname to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

1. **Root name servers–** It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
2. **Top level server–** It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.
3. **Authoritative name servers-** This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.



Question 14: Explain SMTP server.

Answer: SMTP stands for Simple Mail Transfer Protocol. SMTP is a push protocol and is used to send the mail whereas **POP (post office protocol)** or **IMAP (internet message access protocol)** are used to retrieve those emails at the receiver's side.

The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is the always-on listening

mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

Question 15: What is port number?

Answer: A port is basically a physical docking point which is basically used to connect the external devices to the computer or we can say that A port act as an interface between computer and the external devices, e.g., we can hard drives, printers to the computer with the help of ports.

Question 16: What is the difference between hub, switch and router?

Answer:

1. **Hub-** When a data packet comes to one of the port, then hub rebroadcasts data to all other
2. **Switch-** Switch can store MAC address of the devices and then ship the data as per MAC requirment
3. **Router-** Router checks the logical address and if selects the IP to send data to and send this information to switch to make it physically transfer data.

Question 17: What is TCP and UDP?

Answer:

TCP	UDP
TCP stands for Transmission Control Protocol	UDP is stands for User Datagram Protocol
Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol	UDP is connectionless, simple protocol. Using UDP, messages are sent as packets
The speed of TCP is slower than UDP	UDP is faster compared to TCP
TCP is used for the application where time is not critical part of data transmission	UDP is suitable for the applications which require fast transmission of data and time is crucial in this case.
TCP tracks the data sent to ensure no data loss during data transmission	UDP does not ensure whether receiver receives packets are not. If packets are misses then they are just lost

Question 18: What is domain and workgroup?

Answer:

- **Domain** is a client/server network where user can login from any device of the office. Also known as Remote login. It has a centralized administration and all devices can be managed from a centralized device. It prefers a centralized storage and all the users data is stored at a centralized storage device which can be NAS or SAN.
- **Workgroup** is a peer to peer windows computer network, where users can use his login credentials only on his or her system and not others. It holds an distributed administration wherein each user can manage his machine independently. Most storage is distributed. Each device has its own dedicated storage.

Question 19: What are proxy servers.

Answer: Proxy server refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources.

Question 20: What is DHCP server?

Answer: DHCP server stands for Dynamic Host Configuration Server.

DHCP is a service. It allows devices to acquire their IP configuration dynamically. It is defined in RFC 2131 and 2939. It works in the server/clients model. The server offers and delivers IP configuration. Clients request and acquire an IP configuration.

When a host (DHCP client) needs an IP configuration, it connects to a DHCP server and requests for an IP configuration. DHCP server contains several pre-configured IP configurations. DHCP server, upon receiving a request from the DHCP client, offers an IP configuration from all available IP configurations.

This entire process goes through the four steps: Discover, Offer, Request, and Acknowledgment. The following image shows these steps