Computer Networks

1. Define network

   A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes. A network is a collection of devices connected to each other to allow the sharing of data.

2. What do you mean by network topology and explain types of them

   Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other

   Types of network topology : Ring, Bus, Mesh, Tree , Hybrid
   i) Star :
   ● Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
   ● Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only disconnect a specific computer connected to this cable.
   ● If the central device is damaged, then the whole network fails.
   ● Star topology is very easy to install, manage and troubleshoot. It is commonly used in office and home networks.

   ii) Ring :
   1. Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.
   2. It does not need any central server to control the connectivity among the nodes.
   3. If the single node is damaged, then the whole network fails.
   4. Ring topology is very rarely used as it is expensive, difficult to install and manage.
   5. Examples of Ring topology are SONET network, SDH network, etc.

   iii) Bus :
   1. Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
   2. It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.
   3. Bus topology is useful for a small number of devices.
   4. As if the bus is damaged then the whole network fails.
   (This topology is no longer used. But there was a time when this topology used to be the first choice among the network administrators.)

   iv)Mesh :
   1. Mesh topology is a network topology in which all the nodes are individually

connected to other nodes.
2. It does not need any central switch or hub to control the connectivity among the nodes.
3. Mesh topology is categorised into two parts: Fully connected mesh topology: In this topology, all the nodes are connected to each other. Partially connected mesh topology: In this topology, all the nodes are not connected to each other.
4. It is robust as a failure in one cable will only disconnect the specified computer connected to this cable.
5. Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
6. Cabling cost is high as it requires bulk wiring.
(Mesh topology is commonly used in the WAN network for backup purposes. This topology is not used in the LAN network implementations.)

v)Tree :
1. Tree topology is a combination of star and bus topology. It is also known as the expanded star topology.
2. In tree topology, all the star networks are connected to a single bus.
3. Ethernet protocol is used in this topology.
4. In this, the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged, there is no effect on other segments.
5. Tree topology depends on the "main bus," and if it breaks, then the whole network gets damaged
(Tree topology is suitable for large networks, spread into many branches. Example: Big university campuses, hospitals etc. Main disadvantage of tree topology is that the connectivity between tree branches are dependent on main backbone switches)

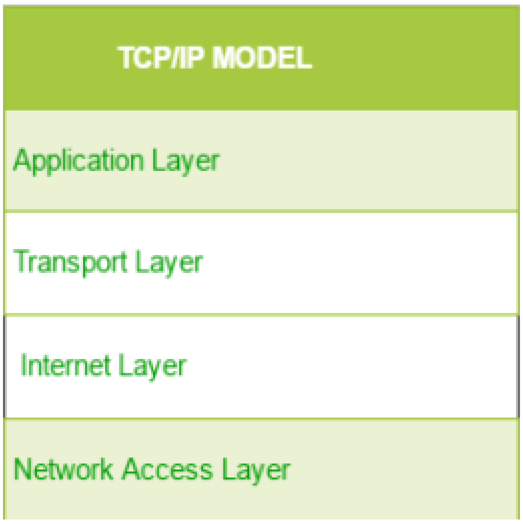
vi)Hybrid :
1. A hybrid topology is a combination of different topologies to form a resulting topology.
2. If star topology is connected with another star topology, then it remains a star topology. If star topology is connected with different topology, then it becomes a Hybrid topology.
3. It provides flexibility as it can be implemented in a different network environment

3. Define bandwidth, node and link ?

Bandwidth is the data transfer capacity of a computer network in bits per second (Bps). The term may also be used colloquially to indicate a person's capacity for tasks or deep thoughts at a point in time.

A network is a connection setup of two or more computers directly connected by some physical mediums like optical fibre or coaxial cable. This physical medium of connection is known as a link, and the computers that it is connected to are known as nodes

4. Explain TCP model

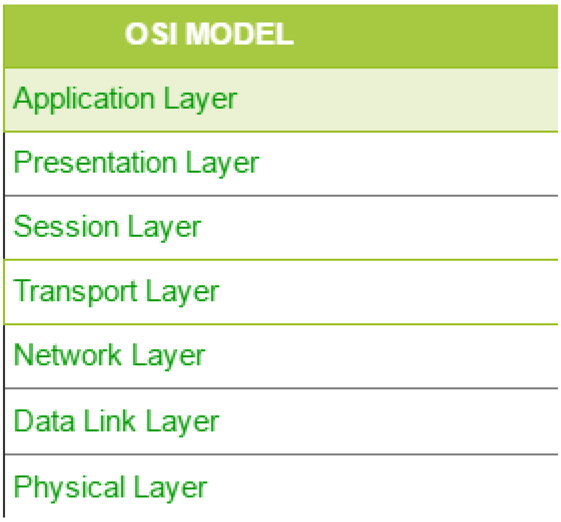


TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer

It is a compressed version of the OSI model with only 4 layers. It was developed by the US Department of Defence (DoD) in the 1860s. The name of this model is based on 2 standard protocols used i.e. TCP (Transmission Control Protocol) and IP (Internet Protocol).

1. Network Access/Link layer : Decides which links such as serial lines or classic Ethernet must be used to meet the needs of the connectionless internet layer. Ex - Sonet, Ethernet
2. Internet : The internet layer is the most important layer which holds the whole architecture together. It delivers the IP packets where they are supposed to be delivered. Ex - IP, ICMP.
3. Transport : Its functionality is almost the same as the OSI transport layer. It enables peer entities on the network to carry on a conversation. Ex - TCP, UDP (User Datagram Protocol)
4. Application : It contains all the higher-level protocols. Ex - HTTP, SMTP, RTP, DNS

5. Layers of OSI model



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

It is a network architecture model based on the ISO standards. It is called the OSI model as it deals with connecting the systems that are open for communication with other systems. The OSI model has seven layers.

The principles used to arrive at the seven layers can be summarised briefly as below:

1. Create a new layer if a different abstraction is needed.
2. Each layer should have a well-defined function.
3. The function of each layer is chosen based on internationally standardised protocols.

● Seven Layers :

1. Physical Layer

● It is the lowest layer of the OSI reference model.

● It is used for the transmission of an unstructured raw bit stream over a physical medium.

● Physical layer transmits the data either in the form of electrical/optical or mechanical form.

● The physical layer is mainly used for the physical connection between the devices, and such physical connection can be made by using twisted-pair cable, fibre-optic or wireless transmission media.

2. DataLink Layer

● It is used for transferring the data from one node to another node.

● It receives the data from the network layer and converts the data into data frames and then attaches the physical address to these frames which are sent to the physical layer.

● It enables the error-free transfer of data from one node to another node.

Functions of Data-link layer:

● Frame synchronisation: Data-link layer converts the data into frames, and it ensures that the destination must recognize the starting and ending of each frame.

● Flow control: Data-link layer controls the data flow within the network.● Error control: It detects and corrects the error occurred during the transmission from source to destination.

● Addressing: Data-link layers attach the physical address with the data frames so that the individual machines can be easily identified.

● Link management: Data-link layer manages the initiation, maintenance and termination of the link between the source and destination for the effective exchange of data.

3. Network Layer

● Network layer converts the logical address into the physical address.

● The routing concept means it determines the best route for the packet to travel from source to the destination.

Functions of network layer :

● Routing: The network layer determines the best route from source to destination. This The function is known as routing.

● Logical addressing: The network layer defines the addressing scheme to identify each device uniquely.

● Packetizing: The network layer receives the data from the upper layer and converts the data into packets. This process is known as packetizing.

● Internetworking: The network layer provides the logical connection between the different types of networks for forming a bigger network.

● Fragmentation: It is a process of dividing the packets into fragments..

4. Transport Layer

● It delivers the message through the network and provides error checking so that no error occurs during the transfer of data.

● It provides two kinds of services:

○ Connection-oriented transmission: In this transmission, the receiver sends the acknowledgement to the sender after the packet has been received.○ Connectionless transmission: In this transmission, the receiver does not send
the acknowledgement to the sender.

5. Session Layer

● The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.

● Session layer also reports the error coming from the upper layers.

● Session layer establishes and maintains the session between the two users.

6. Presentation Layer

● The presentation layer is also known as a Translation layer as it translates the data from one format to another format.

● At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.

Functions of presentation layer:

○ Character code translation

○ Data conversion

○ Data compression

○ Data encryption

7. Application Layer

● Application layer enables the user to access the network.

● It is the topmost layer of the OSI reference model.

● Application layer protocols are file transfer protocol, simple mail transfer protocol, domain name system, etc.

● The most widely used application protocol is HTTP(Hypertext transfer protocol). A user sends the request for the web page using HTTP.

6. Significance of Data Link Layer
   (discussed in the previous question)

7. Define gateway, difference between gateway and router ..
   A node that is connected to two or more networks is commonly known as a gateway. It is also known as a router. It is used to forward messages from one network to another. Both the gateway and router regulate the traffic in the network. Differences between gateway and router: A router sends the data between two similar networks while gateway sends the data between two dissimilar networks

8. What does ping command do ?
   The "ping" is a utility program that allows you to check the connectivity between the network devices. You can ping devices using its IP address or name.

9. What is DNS, DNS forwarder, NIC, ?
   DNS (Imp) :
   1. DNS is an acronym that stands for Domain Name System.DNS was introduced by Paul Mockapetris and Jon Postel in 1983.
   2. It is a naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate resources easily over a network.
   3. DNS is an internet which maps the domain names to their associated IP addresses.4. Without DNS, users must know the IP address of the web page that you wanted
   to access.
   ● Working of DNS (Imp): If you want to visit the website of "shaurya", then the user will
   type "https://www.shaurya.com" into the address bar of the web browser. Once the domain name is entered, then the domain name system will translate the domain name
   into the IP address which can be easily interpreted by the computer. Using the IP address, the computer can locate the web page requested by the user.
   ● DNS Forwarder : A forwarder is used with a DNS server when it receives DNS queries
   that cannot be resolved quickly. So it forwards those requests to external DNS servers
   for resolution. A DNS server which is configured as a forwarder will behave differently than the DNS server which is not configured as a forwarder.
   NIC stands for Network Interface Card. It is a peripheral card attached to the PC to connect to a network. Every NIC has its own MAC address that identifies the
   PC on the network. It provides a wireless connection to a local area network. NICs were
   mainly used in desktop computers.

10. What is a MAC address ?
    A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

MAC address and IP address (Imp) :
1. Both MAC (Media Access Control) Address and IP Address are used to uniquely define a device on the internet. NIC Card’s Manufacturer provides the MAC Address, On the other hand, Internet Service Providers provide IP Addresses.
2. The main difference between MAC and IP address is that MAC Address is used to ensure the physical address of a computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely identify the connection of a network
with that device taking part in a network.

11. What is IP address, private IP address, public IP address, APIPA ?
An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Private IP Address - There are three ranges of IP addresses that have been reserved for IP addresses. They are not valid for use on the internet. If you want to access the internet on these private IPs, you must use a proxy server or NAT server.

Public IP Address - A public IP address is an address taken by the Internet Service Provider which facilitates communication on the internet.

APIPA stands for Automatic Private IP Addressing (APIPA). It is a feature or characteristic in operating systems (eg. Windows) which enables computers to self-configure an IP address and subnet mask automatically when their DHCP(Dynamic Host Configuration Protocol:A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol) server isn't reachable

12. Difference between IPv4 and IPv6

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
It can generate 4.29×10^9 address space	Address space of IPv6 is quite large it can produce 3.4×10^38 address space
It Supports Manual and DHCP address	It supports Auto and renumbering

configuration	address configuration
IPv4 sites load less faster compared to IPv6	

13. What is subnet ?
    A subnet is a network inside a network achieved by the process called subnetting which helps divide a network into subnets. It is used for getting a higher routing efficiency and enhances the security of the network. It reduces the time to extract the host address from the routing table.

14. Firewalls
    The firewall is a network security system that is used to monitor the incoming and outgoing traffic and blocks the same based on the firewall security policies. It acts as a wall between the internet (public network) and the networking devices (a private network). It is either a hardware device, software program, or a combination of both. It adds a layer of security to the network

15. Different type of delays
    The delays, here, means the time for which the processing of a particular packet takes place. We have the following types of delays in computer networks:

    1)Transmission Delay:
    The time taken to transmit a packet from the host to the transmission medium is called Transmission delay.
    Let B bps is the bandwidth and L bit is the size of the data then transmission delay is,

    Tt = L/B

    2) Propagation delay:

After the packet is transmitted to the transmission medium, it has to go through the medium to reach the destination. Hence the time taken by the last bit of the packet to reach the destination is called propagation delay. Tp = Distance / Velocity

3) Queueing delay:

If the packet is received by the destination, the packet will not be processed by the destination immediately. It has to wait in a queue in something called a buffer. So the amount of time it waits in queue before being processed is called queueing delay.

In general, we can’t calculate queueing delay because we don’t have any formula for that.

4.)Processing delay:
Now the packet will be taken for the processing which is called processing delay.

Time is taken to process the data packet by the processor, that is the time required by intermediate routers to decide where to forward the packet, update TTL, and perform header checksum calculations.

It also doesn’t have any formula since it depends upon the speed of the processor and the speed of the processor varies from computer to computer.

Note: Total = Tt + Tp + Tq + Tpro

Total = Tt+Tp
(when taking Tq(queuing delay) and Tpro(processing delay) equals to 0)

16. 3 way handshaking
    Three-Way HandShake or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronisation and acknowledgment packets before the real data communication process starts.

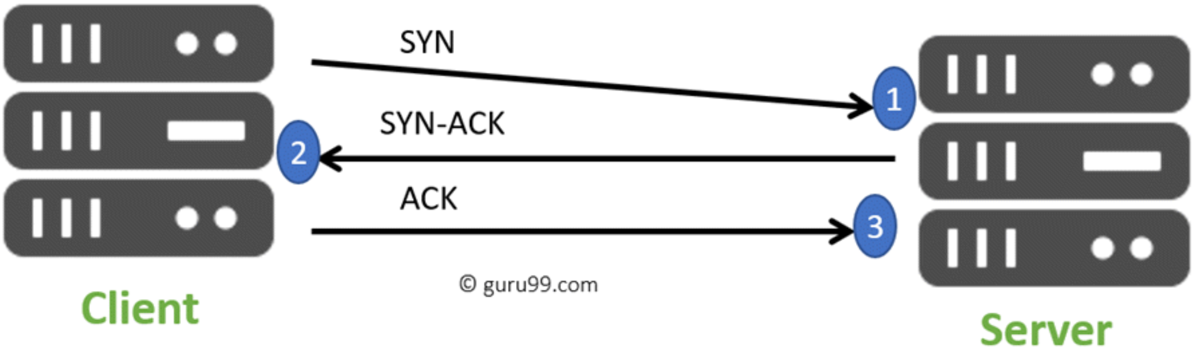
    Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. It allows you to transfer multiple TCP socket connections in both directions at the same time.

TCP message types

Message	Description
Syn	Used to initiate and establish a connection. It also helps you to synchronise sequence numbers between devices.
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

TCP Three-Way Handshake Process

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server:



3 way Handshake Diagram

- **Step 1:** In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server that the client should start communication, and with what should be its sequence number.
- **Step 2:** In this step **s**erver responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of the segment that is received and SYN signifies what sequence number it should be able to start with the segments.
- **Step 3:** In this final step, the client acknowledges the response of the Server, and they both create a stable connection and begin the actual data transfer process.

17. Server-side load balancer

    Q. Why do we need load balancing?

    Ans. When using scalable microservices, a client needs to be able to route its requests to one of the multiple backend server instances. Multiple requests from the client(s) need to be load-balanced across the backend servers so that no single backend server gets overloaded.

    There are 2 approaches for load balancing:

    1. Server-side load-balancing: All backend server instances are registered with a central load balancer. A client requests this load balancer which then routes the request to one of the server instances using various algorithms like round-robin. AWS ELB(Elastic Load Balancing) is a prime example of server-side load-balancing that registers multiple EC2 instances launched in its auto-scaling group and then routes the client requests to one of the EC2 instances.

    Advantages of server-side load balancing:

Simple client configuration: only need to know the load-balancer address.
Clients can be untrusted: all traffic goes through the load-balancer where it can be looked at.Clients are not aware of the backend servers.

2. Client-side load-balancing: The load balancing decision resides with the client itself. The client can take the help of a naming server (eg. Netflix Eureka) to get the list of registered backend server instances, and then route the request to one of these backend instances using client-side load balancing libraries like Netflix Ribbon.

Advantages of client-side load balancing:

No more single point of failure as in the case of the traditional load balancer approach.
Reduced cost as the need for server-side load balancer goes away.
Less network latency as the client can directly invoke the backend servers removing an extra hop for the load balancer.

18. RSA Algorithm
    RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes, the Public Key is given to everyone and the Private key is kept private.

    An example of asymmetric cryptography :
    A client (for example browser) sends its public key to the server and requests for some data.
    The server encrypts the data using the client's public key and sends the encrypted data.
    Client receives this data and decrypts it.
    Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.

19. What is HTTP and HTTPS protocol ?
    HTTP is the HyperText Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on the World Wide Web (WWW). It helps the web browsers and web servers for communication. It is a ‘stateless protocol’ where each command is independent with respect to the previous command. HTTP is an application layer protocol built upon the TCP. It uses port 80 by default.
    HTTPS is the HyperText Transfer Protocol Secure or Secure HTTP. It is an advanced and a secured version of HTTP. On top of HTTP, SSL/TLS protocol is used to provide security. It enables secure transactions by encrypting the communication and also helps identify network servers securely. It uses port 443 by default.

20. What is SMTP protocol ?
    SMTP is the Simple Mail Transfer Protocol. SMTP sets the rule for communication between servers. This set of rules helps the software to transmit emails

over the internet. It supports both End-to-End and Store-and-Forward methods. It is in
always-listening mode on port 25.

21. TCP and UDP protocol, prepare differences
    TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP. Overall, UDP is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with TCP

    TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data. UDP has only the basic error checking mechanism using checksums.

22. What happens when you enter “google.com” (very very famous question)
    Steps :
    ● Check the browser cache first if the content is fresh and present in the cache display the same.
    ● If not, the browser checks if the IP of the URL is present in the cache (browser and OS) if not then requests the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.
    ● A new TCP connection is set between the browser and the server using three-way handshaking.
    ● An HTTP request is sent to the server using the TCP connection.
    ● The web servers running on the Servers handle the incoming HTTP request and send the HTTP response.
    ● The browser processes the HTTP response sent by the server and may close the TCP
    connection or reuse the same for future requests.
    ● If the response data is cacheable then browsers cache the same.
    ● Browser decodes the response and renders the content.
23. Hub vs Switch
    Hub: Hub is a networking device which is used to transmit the signal to each port (except one port) to respond from which the signal was received. Hub is operated on a Physical layer. In this packet filtering is not available. It is of two types: Active Hub, Passive Hub.
    Switch: Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. Switch is operated on the Data link layer. In this packet filtering is available. It is a type of full duplex transmission mode and it is also called an efficient bridge

24. VPN, advantages and disadvantages of it
    VPN (Virtual Private Network) : VPN or the Virtual Private Network is a private WAN

(Wide Area Network) built on the internet. It allows the creation of a secured tunnel (protected network) between different networks using the internet (public network). By using the VPN, a client can connect to the organisation’s network remotely.

Advantages of VPN :
1. VPN is used to connect offices in different geographical locations remotely and is cheaper when compared to WAN connections.
2. VPN is used for secure transactions and confidential data transfer between multiple offices located in different geographical locations.
3. VPN keeps an organisation’s information secured against any potential threats or intrusions by using virtualization.
4. VPN encrypts the internet traffic and disguises the online identity

Disadvantages of VPN :
1. Not designed for continuous use
2. Complexity prevents scalability
3. Lack of granular security
4. Unpredictable performance
5. Unreliable availability

25. LAN

A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.