1. Define network

   ANS: 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

ANS:

Network topology is the arrangement of nodes and links of a network.

Topologies are categorized as either physical network topology or logical network topology.

The topology of a network is key to determining its performance.

Network topology can be categorized into – Bus Topology, Ring Topology, Star Topology, Mesh Topology, Tree Topology.

3. Define bandwidth, node and link ?

ANS: 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 ..

ANS: 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

ANS: There are majorly 2 main layers in the OSI model:

- Physical Layer
- Data Link Layer

6. Significance of Data Link Layer

ANS:

- 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.

7. Define gateway, difference between gateway and router ..

ANS: 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 ?

ANS: 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, ?

ANS:

DNS:
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.

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 MAC address ?

    ANS: 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.

11. What is IP address, private IP address, public IP address, APIPA ?

ANS: 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

13. What is subnet ?
    ANS: 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

    ANS: 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

ANS: 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:

- Transmission Delay
- Propagation delay
- Queueing delay
- Processing delay

16. 3 way handshaking

ANS: 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.

17. Server-side load balancer

ANS: 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.

18. RSA Algorithm

ANS: 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 ?

    ANS: 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 ?

    ANS: 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.

ANS: 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)

- ANS: 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

ANS: **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 .

ANS: 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

ANS: 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.