Short Definitions Top 50 Questions

Basic Networking Concepts

1. **What is a computer network?**
   A computer network is a group of interconnected devices that share resources and information.
2. **What are the types of networks?**
   - LAN (Local Area Network)
   - WAN (Wide Area Network)
   - MAN (Metropolitan Area Network)
   - PAN (Personal Area Network)
3. **What is a protocol?**
   A set of rules that govern data communication between devices.
4. **What is IP?**
   The Internet Protocol is used to address and route packets in a network.
5. **Differentiate between IPv4 and IPv6.**
   - IPv4: 32-bit address, 4.3 billion addresses.
   - IPv6: 128-bit address, virtually unlimited addresses.
6. **What is a MAC address?**
   A unique identifier assigned to a device's network interface card (NIC).
7. **What is DNS?**
   The Domain Name System translates domain names into IP addresses.
8. **What is DHCP?**
   The Dynamic Host Configuration Protocol assigns IP addresses dynamically.
9. **What is NAT?**
   Network Address Translation maps private IP addresses to public IPs to access the internet.
10. **What is a subnet mask?**
    It determines the network and host portions of an IP address.

OSI and TCP/IP Models

11. **What are the layers of the OSI model?**

- Physical, Data Link, Network, Transport, Session, Presentation, Application.

12. **How does the TCP/IP model differ from OSI?**
    TCP/IP has 4 layers: Network Interface, Internet, Transport, and Application.
13. **What is the role of the Transport Layer?**
    Ensures reliable data transfer with protocols like TCP and UDP.

14. **What is encapsulation?**
    The process of adding headers and footers to data as it moves down the OSI layers.

15. **What is the difference between TCP and UDP?**

- TCP: Connection-oriented, reliable.
- UDP: Connectionless, faster, less reliable.

Devices in Networking

16. **What is a router?**
    A device that routes data between networks.

17. **What is a switch?**
    A device that connects devices in a LAN and forwards data based on MAC addresses.

18. **What is a hub?**
    A basic networking device that broadcasts data to all devices.

19. **What is a modem?**
    A device that modulates and demodulates data for internet access over telephone lines.

20. **What is a firewall?**
    A security device that monitors and controls incoming and outgoing traffic.

Networking Concepts

21. **What is bandwidth?**
    The maximum data transfer rate of a network.

22. **What is latency?**
    The delay in data transmission over a network.

23. **What is jitter?**
    Variation in latency during data transmission.

24. **What is a VPN?**
    A Virtual Private Network extends a private network across a public network.

25. **What is ARP?**
    The Address Resolution Protocol maps IP addresses to MAC addresses.

26. **What is a socket?**
    An endpoint for communication between devices in a network.

27. **What is port forwarding?**
    Redirecting communication requests from one address/port to another.

28. **What is an IP conflict?**
    When two devices are assigned the same IP address on a network.

29. **What is the default gateway?**
    The device that connects a local network to other networks.

30. **What is a VLAN?**
    A Virtual LAN segments a physical LAN into logical groups for better management and security.

Network Security

31. **What is encryption?**
    Securing data by converting it into a coded format.

32. **What is SSL/TLS?**
    Protocols for encrypting data over the internet (e.g., HTTPS).

33. **What is phishing?**
    A cyberattack where attackers deceive users to steal sensitive information.

34. **What is a Denial of Service (DoS) attack?**
    Overloading a network/service to make it unavailable.

35. **What is a proxy server?**
    A server that acts as an intermediary between users and the internet.

Wireless Networking

36. **What is Wi-Fi?**
    Wireless networking technology based on IEEE 802.11 standards.

37. **What is SSID?**
    The name of a Wi-Fi network.

38. **What is WPA/WPA2?**
    Wireless security protocols for encrypting Wi-Fi networks.

39. **What is Bluetooth?**
    A short-range wireless technology for data transfer between devices.

40. **What is 5G?**
    The fifth generation of mobile network technology offering higher speeds and lower latency.

Advanced Concepts

41. **What is MPLS?**
    Multiprotocol Label Switching directs data based on labels instead of IP addresses.

42. **What is QoS?**
    Quality of Service prioritizes specific types of traffic to improve network performance.

43. **What is BGP?**
    The Border Gateway Protocol routes data between autonomous systems on the internet.

44. **What is multicast?**
    Sending data to multiple devices in a group using a single transmission.
45. **What is a CDN?**
    A Content Delivery Network distributes content geographically for faster delivery.

Troubleshooting

46. **What is ping?**
    A command to test connectivity and measure response time between devices.
47. **What is traceroute?**
    A command to trace the path data takes to a destination.
48. **What is packet sniffing?**
    Monitoring network traffic to capture and analyze data packets.
49. **What is a loopback address?**
    127.0.0.1, used to test the network stack on a local machine.
50. **What is a network topology?**
    The arrangement of devices in a network (e.g., star, bus, ring).

Important Questions with detailed answer

1) What is the network?

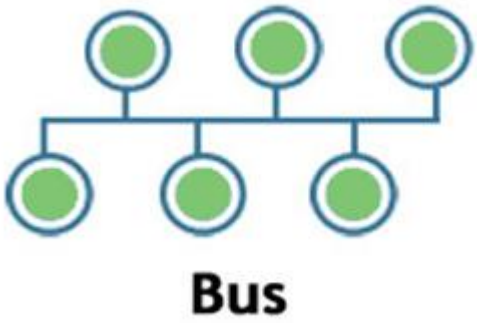
- A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes.
- A network is a collection of devices connected to each other to allow the sharing of data.
- Example of a network is an internet. An internet connects the millions of people across the world.

---

2) What do you mean by network topology?

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

Bus:

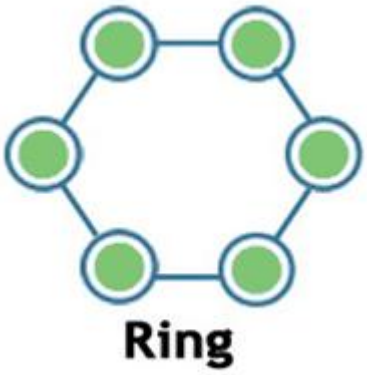


- Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
- It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.
- Bus topology is useful for a small number of devices. As if the bus is damaged then the whole network fails.

Star:

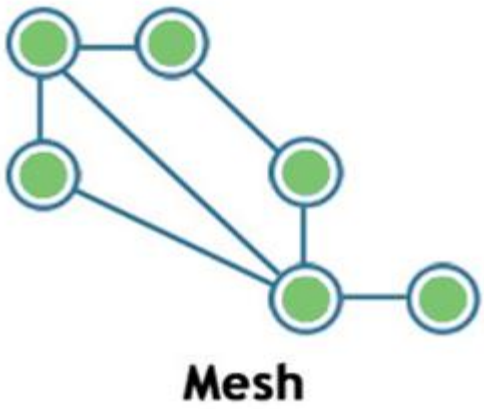
- Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
- Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only disconnect a specific computer connected to this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

Ring



- 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.
- It does not need any central server to control the connectivity among the nodes.
- If the single node is damaged, then the whole network fails.
- Ring topology is very rarely used as it is expensive, difficult to install and manage.
- Examples of Ring topology are SONET network, SDH network, etc.

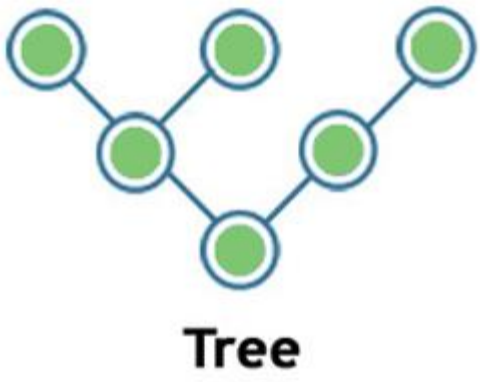
Mesh



- Mesh topology is a network topology in which all the nodes are individually connected to other nodes.
- It does not need any central switch or hub to control the connectivity among the nodes.
- Mesh topology is categorized 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.

- It is a robust as a failure in one cable will only disconnect the specified computer connected to this cable.
- Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
- Cabling cost is high as it requires bulk wiring.

Tree



- Tree topology is a combination of star and bus topology. It is also known as the expanded star topology.
- In tree topology, all the star networks are connected to a single bus.
- Ethernet protocol is used in this topology.
- In this, the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged, but there is no effect on other segments.
- Tree topology depends on the "main bus," and if it breaks, then the whole network gets damaged.

Hybrid

- A hybrid topology is a combination of different topologies to form a resulting topology.
- If star topology is connected with another star topology, then it remains star topology. If star topology is connected with different topology, then it becomes a Hybrid topology.
- It provides flexibility as it can be implemented in a different network environment.
- The weakness of a topology is ignored, and only strength will be taken into consideration.

3) How many layers are in OSI reference model?

OSI reference model: OSI reference model is an ISO standard which defines a networking framework for implementing the protocols in seven layers. These seven layers can be grouped into three categories:

- Network layer: Layer 1, Layer 2 and layer 3 are the network layers.

- Transport layer: Layer 4 is a transport layer.
- Application layer. Layer 5, Layer 6 and Layer 7 are the application layers.

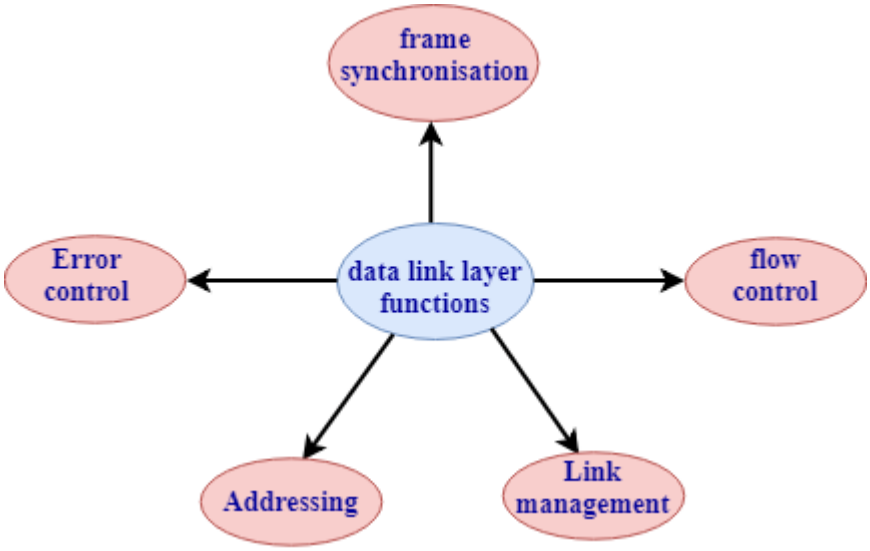
There are 7 layers in the OSI reference model.

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. Data Link 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 attach 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:

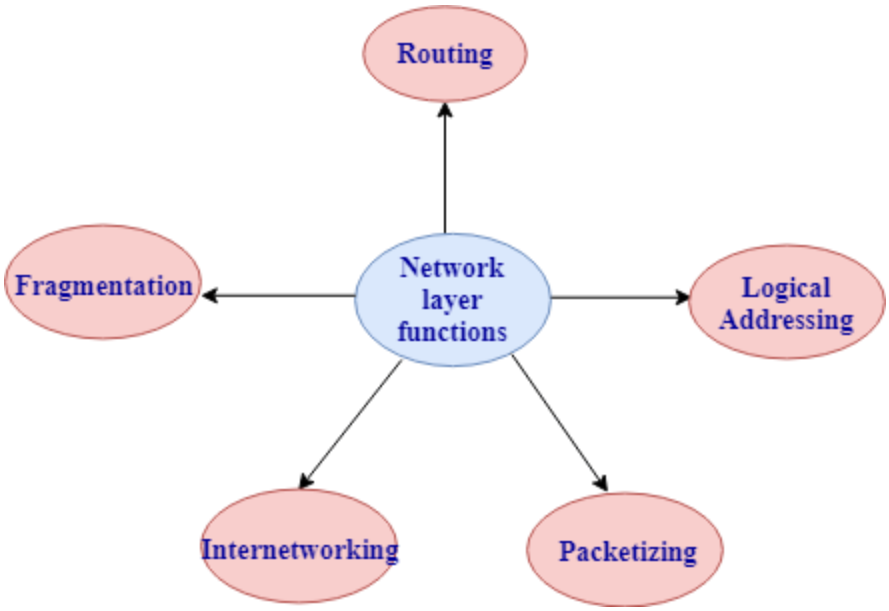


- Frame synchronization: Data-link layer converts the data into frames, and it ensures that the destination must recognize the starting and ending of each frame.
- Flow control: Data-link layer controls the data flow within the network.
- Error control: It detects and corrects the error occurred during the transmission from source to destination.
- Addressing: Data-link layer 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.
- It provides 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 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 the 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.

4. What happens in the OSI model, as a data packet moves from the lower to upper layers?

In the OSI model, as a data packet moves from the lower to upper layers, headers get removed.

5. What happens in the OSI model, as a data packet moves from the upper to lower layers?

In the OSI model, as a data packet moves from the upper to lower layers, headers are added. This header contains useful information.

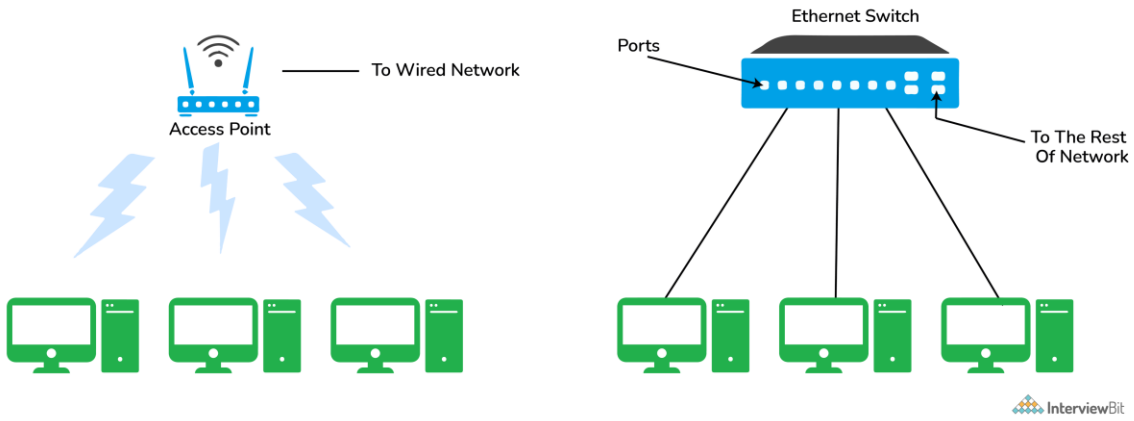
6. Explain different types of networks.

Below are few types of networks:

Type	Description
PAN (Personal Area Network)	Let devices connect and communicate over the range of a person. E.g. connecting Bluetooth devices.
LAN (Local Area Network)	It is a privately owned network that operates within and nearby a single building like a home, office, or factory
MAN (Metropolitan Area Network)	It connects and covers the whole city. E.g. TV Cable connection over the city
WAN (Wide Area Network)	It spans a large geographical area, often a country or continent. The Internet is the largest WAN
GAN (Global Area Network)	It is also known as the Internet which connects the globe using satellites. The Internet is also called the Network of WANs.

7. Explain LAN (Local Area Network)

LANs are widely used to connect computers/laptops and consumer electronics which enables them to share resources (e.g., printers, fax machines) and exchange information. When LANs are used by companies or organizations, they are called **enterprise networks**. There are two different types of LAN networks i.e. wireless LAN (no wires involved achieved using Wi-Fi) and wired LAN (achieved using LAN cable). Wireless LANs are very popular these days for places where installing wire is difficult. The below diagrams explain both wireless and wired LAN.



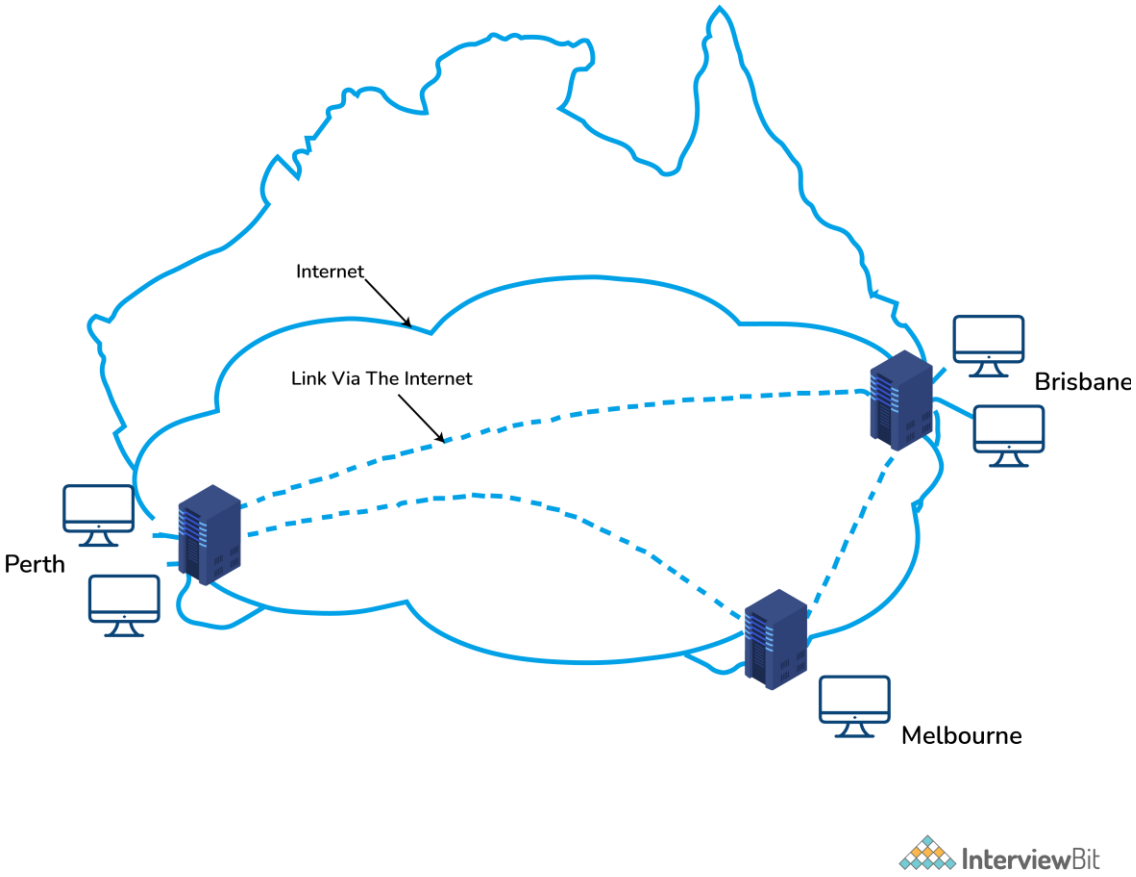
LAN (Local Area Network)

---

8. What is 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 organization's network

remotely. The below diagram shows an organizational WAN network over Australia created using VPN:



VPN (Virtual Private Network)

9. What are the advantages of using a VPN?

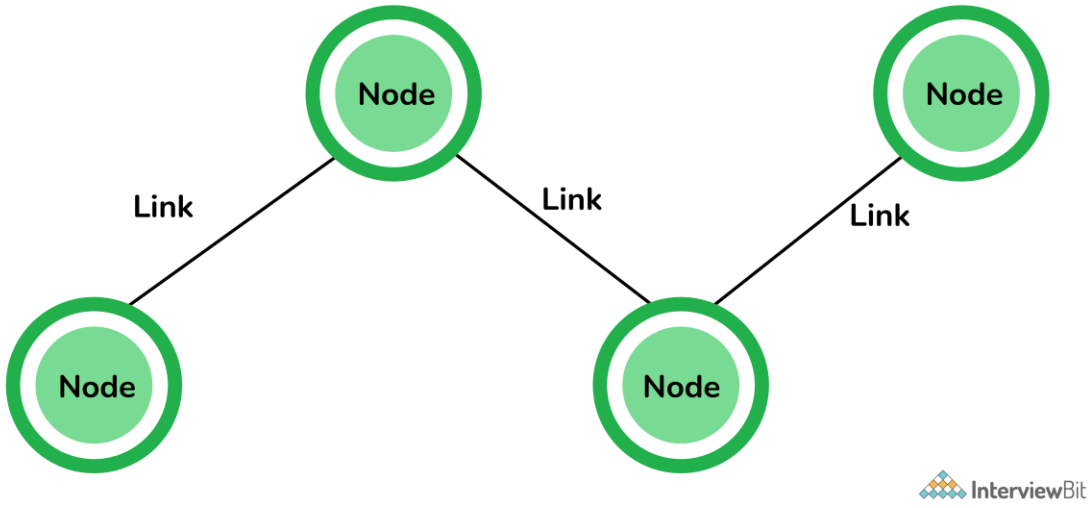
Below are few advantages of using VPN:

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

10. What are nodes and links?

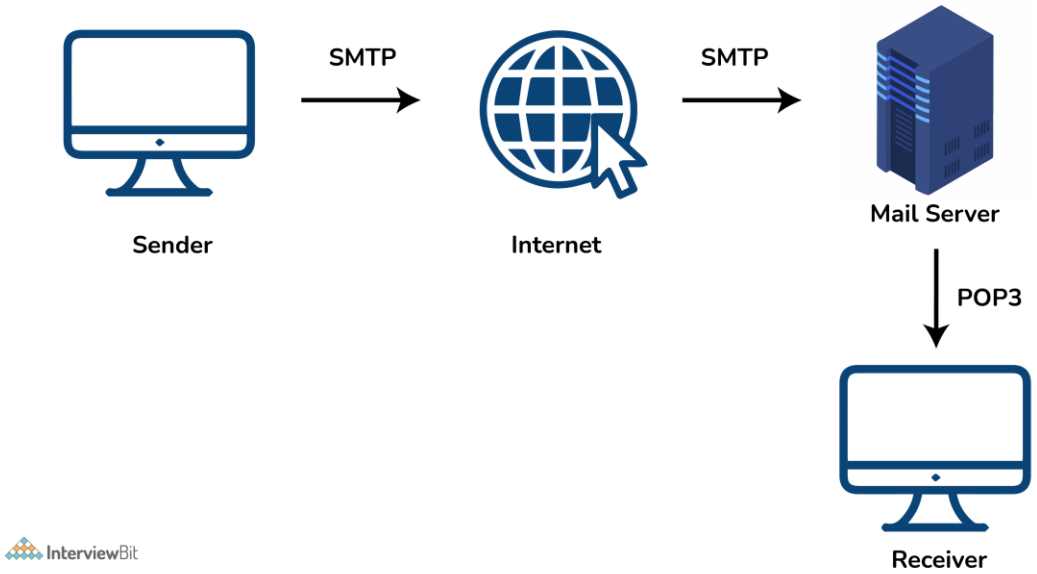
Node: Any communicating device in a network is called a Node. Node is the point of intersection in a network. It can send/receive data and information within a network. Examples of the node can be computers, laptops, printers, servers, modems, etc.

Link: A link or edge refers to the connectivity between two nodes in the network. It includes the type of connectivity (wired or wireless) between the nodes and protocols used for one node to be able to communicate with the other.



11.What is the 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.



12. What do you understand by TCP/IP?

TCP/IP is short for Transmission Control Protocol /Internet protocol. It is a set of protocol layers that is designed for exchanging data on different types of networks.

13. HTTP VS HTTPS?

HTTP is the Hyper Text 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 Hyper Text Transfer Protocol Secure or Secure HTTP. It is an advanced and 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.

14. Compare between TCP and UDP

TCP/IP	UDP
Connection-Oriented Protocol	Connectionless Protocol
More Reliable	Less Reliable
Slower Transmission	Faster Transmission
Packets order can be preserved or can be rearranged	Packets order is not fixed and packets are independent of each other
Uses three ways handshake model for connection	No handshake for establishing the connection
TCP packets are heavy-weight	UDP packets are light-weight
Offers error checking mechanism	No error checking mechanism
Protocols like HTTP, FTP, Telnet, SMTP, HTTPS, etc use TCP at the transport layer	Protocols like DNS, RIP, SNMP, RTP, BOOTP, TFTP, NIP, etc use UDP at the transport layer

15. MAC VS IP Address

Aspect	MAC Address	IP Address
Definition	A hardware address assigned to the network interface card (NIC) of a device.	A logical address assigned to a device in a network for identification and communication.
Format	48-bit address (e.g., 00:1A:2B:3C:4D:5E).	IPv4: 32-bit (e.g., 192.168.1.1). IPv6: 128-bit (e.g., 2001:0db8::1).

Aspect	MAC Address	IP Address
Permanence	Permanent and unique to the device (burned into hardware).	Can be dynamic (assigned by DHCP) or static (manually configured).
Scope	Operates within a local network (Data Link Layer).	Operates across networks (Network Layer).
Purpose	Identifies a device at the hardware level for local communication.	Identifies a device on a network for routing and global communication.

16. Hub vs Switch?

Aspect	Hub	Switch
Definition	A basic networking device that broadcasts data to all connected devices.	A network device that forwards data to specific devices based on their MAC addresses.
Data Transmission	Broadcasts data to all devices in the network, causing collisions.	Sends data only to the intended recipient, reducing collisions.
Efficiency	Less efficient, as it cannot differentiate between devices.	More efficient, as it uses MAC addresses to direct traffic.
Collision Domain	All devices share a single collision domain.	Each port has its own collision domain.
Layer of Operation	Operates at the Physical Layer (Layer 1) of the OSI model.	Operates at the Data Link Layer (Layer 2) of the OSI model.
Speed	Typically slower due to broadcasting.	Faster due to intelligent data routing.

17. What happens when you enter google.com in the web browser?

Below are the steps that are being followed:

- Check the browser cache first if the content is fresh and present in 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 request 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 process 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.

18. **What is DNS?**

The **Domain Name System (DNS)** is a protocol that translates human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.168.1.1 for IPv4 or 2001:0db8::1 for IPv6). It acts like the phonebook of the internet, allowing users to access websites using easy-to-remember names instead of numeric IP addresses.

How DNS Works (Example)

1. **You type www.google.com into your browser.**
    - Your browser needs the IP address of Google's server to connect.
2. **The query is sent to a DNS resolver (ISP or public DNS server like Google DNS).**
    - The DNS resolver checks its cache. If the IP address is not found, it queries other DNS servers.
3. **DNS hierarchy is queried:**
    - **Root DNS server**: Directs to the appropriate Top-Level Domain (TLD) server (e.g., .com).
    - **TLD DNS server**: Directs to the authoritative DNS server for google.com.
    - **Authoritative DNS server**: Returns the IP address of www.google.com.
4. **The IP address is returned to your browser.**
    - For example, 172.217.164.110.
5. **Your browser connects to the server.**
    - The browser uses the IP address to load Google's website.
    -

19. Example of data packet movement?

Example: Sending an Email

1. You type and send an email using an app.
2. The app sends the data to the SMTP server over TCP.

3. The data packet moves through switches and routers to the recipient's email server.
4. The recipient’s server receives the packet, reassembles it, and stores it in their mailbox.
5. The recipient’s email app retrieves and displays the message.

Visual Representation

1. Sender:
   App → TCP/UDP → IP → MAC → Signal.
2. Network:
   Signal → Switch (MAC layer) → Router (IP layer) → Internet.
3. Receiver:
   Signal → MAC → IP → TCP/UDP → App.

20. What is handshaking?

Handshaking is the process used in networking to establish a connection between two devices before data transfer. It ensures that both devices agree on communication parameters, such as protocols, data size, and speed.

The most common example of handshaking is the **TCP three-way handshake**, used to establish a reliable connection in the **Transport Layer**.