Computer Networks

@bzlearnin

Basic Inteview Questions

1.What is a Computer Network?

- **Answer:** A computer network is a group of interconnected computers that can communicate and share resources with each other.

2.What is the OSI Model?

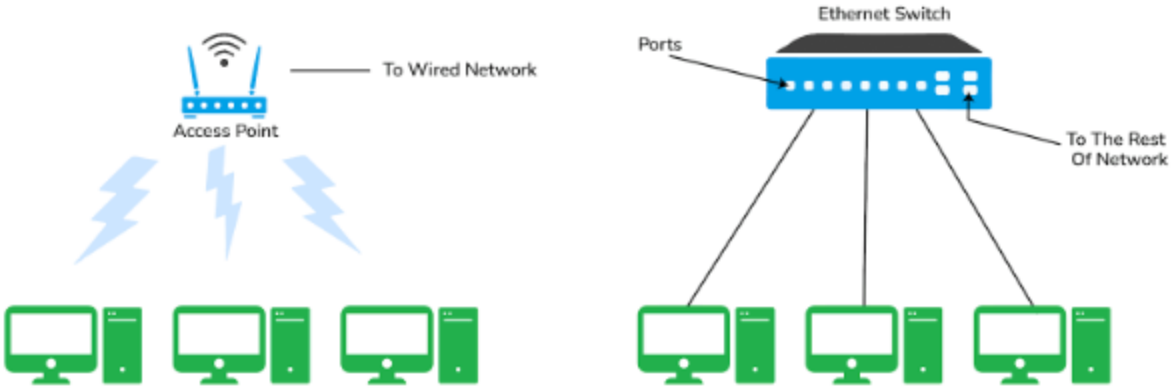
- **Answer:** The OSI model is a conceptual framework used to understand network interactions in seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

3.What is TCP/IP?

- **Answer:** TCP/IP is a set of communication protocols used to connect network devices on the internet, consisting of four layers: Network Interface, Internet, Transport, and Application.

4. 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.

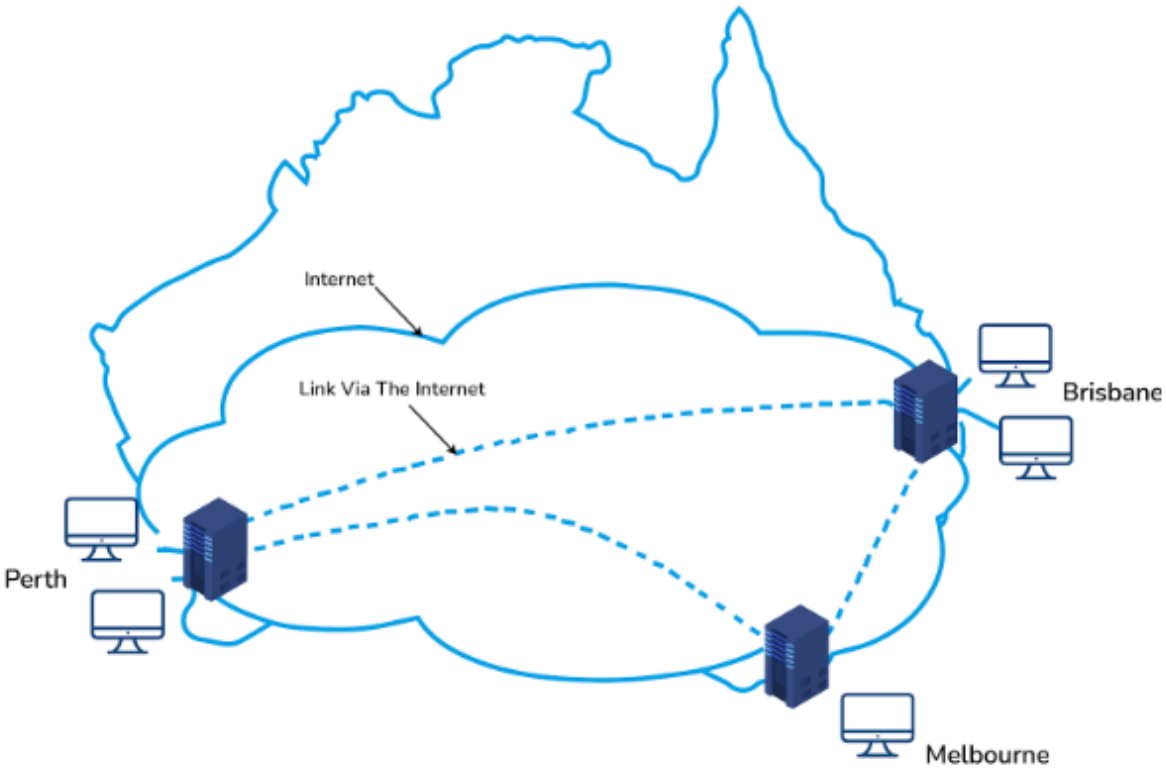


LAN (Local Area Network)

---

5. Tell me something about 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)

6. 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.

7. What are the different types of VPN?

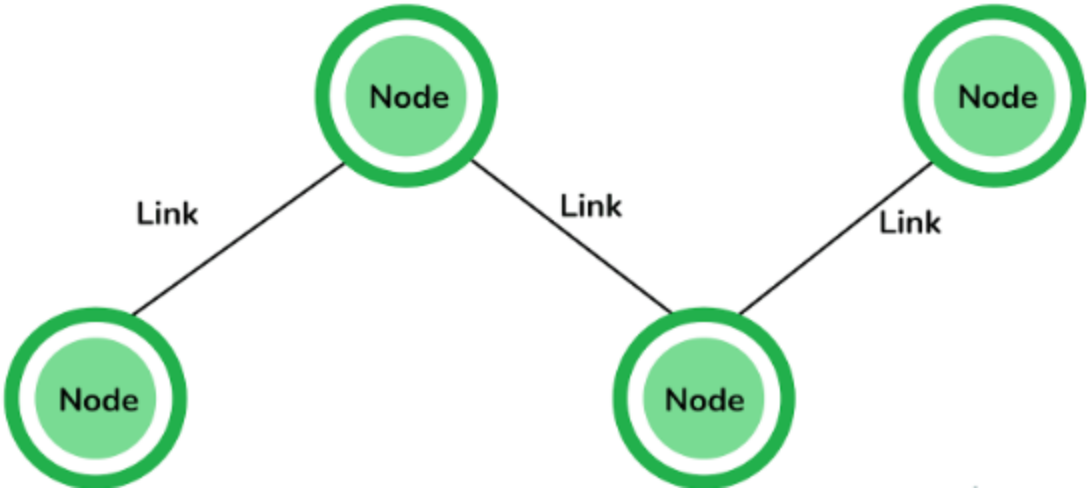
Few types of VPN are:

- Access VPN: Access VPN is used to provide connectivity to remote mobile users and telecommuters. It serves as an alternative to dial-up connections or ISDN (Integrated Services Digital Network) connections. It is a low-cost solution and provides a wide range of connectivity.
- Site-to-Site VPN: A Site-to-Site or Router-to-Router VPN is commonly used in large companies having branches in different locations to connect the network of one office to another in different locations. There are 2 sub-categories as mentioned below:
- Intranet VPN: Intranet VPN is useful for connecting remote offices in different geographical locations using shared infrastructure (internet connectivity and servers) with the same accessibility policies as a private WAN (wide area network).
- Extranet VPN: Extranet VPN uses shared infrastructure over an intranet, suppliers, customers, partners, and other entities and connects them using dedicated connections.

8. 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.



Nodes and Links

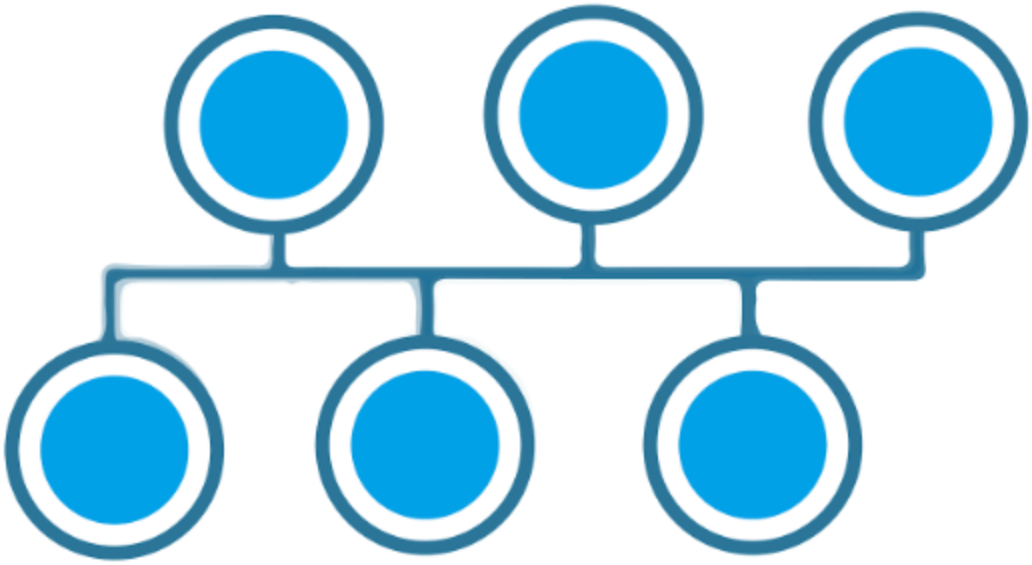
9. What is the network topology?

Network topology is a physical layout of the network, connecting the different nodes using the links. It depicts the connectivity between the computers, devices, cables, etc.

10. Define different types of network topology

The different types of network topology are given below:

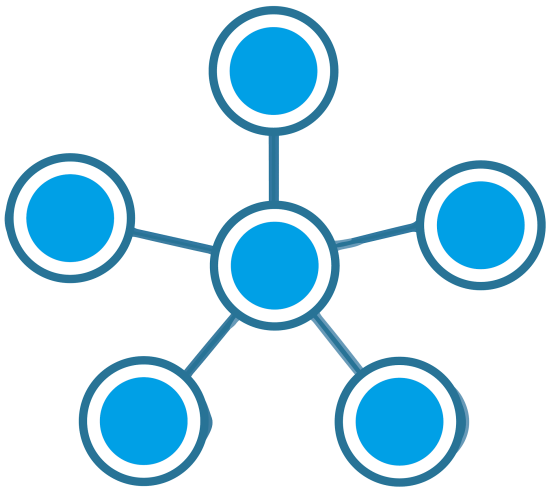
Bus Topology:



Bus Topology

- All the nodes are connected using the central link known as the bus.
- It is useful to connect a smaller number of devices.
- If the main cable gets damaged, it will damage the whole network.

Star Topology:

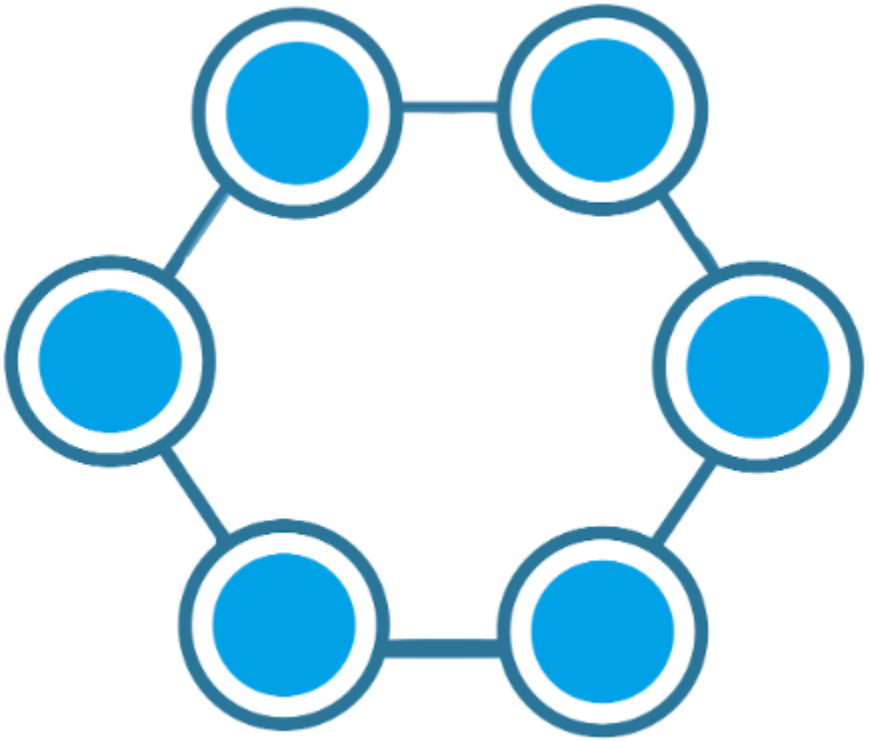


Star Topology

- All the nodes are connected to one single node known as the central node.
- It is more robust.

- If the central node fails the complete network is damaged.
- Easy to troubleshoot.
- Mainly used in home and office networks.

Ring Topology:



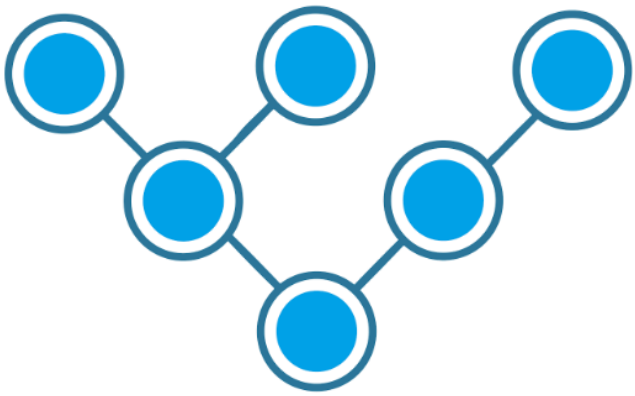
Ring Topology

- Each node is connected to exactly two nodes forming a ring structure
- If one of the nodes are damaged, it will damage the whole network
- It is used very rarely as it is expensive and hard to install and manage

Mesh Topology:

- Each node is connected to one or many nodes.
- It is robust as failure in one link only disconnects that node.
- It is rarely used and installation and management are difficult.

Tree Topology:



Tree Topology

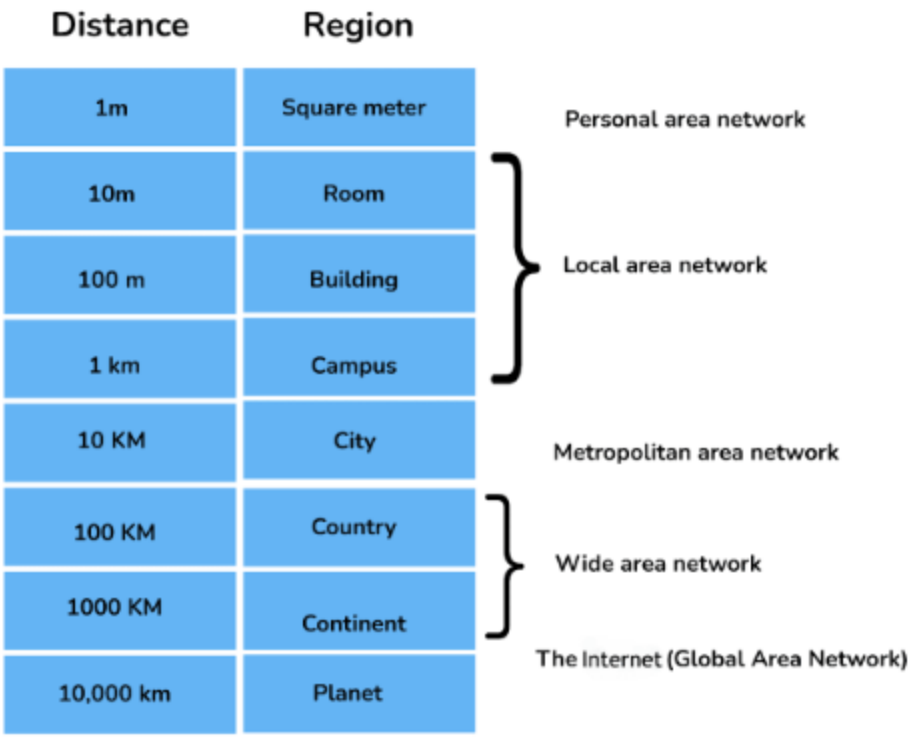
- A combination of star and bus topology also know as an extended bus topology.
- All the smaller star networks are connected to a single bus.
- If the main bus fails, the whole network is damaged.

Hybrid:

- It is a combination of different topologies to form a new topology.
- It helps to ignore the drawback of a particular topology and helps to pick the strengths from other.

11. How are Network types classified?

Network types can be classified and divided based on the area of distribution of the network. The below diagram would help to understand the same:



Network Types

12. What are Private and Special IP addresses?

Private Address: For each class, there are specific IPs that are reserved specifically for private use only. This IP address cannot be used for devices on the Internet as they are non-routable.

IPv4 Class	Private IPv4 Start Address	Private IPv4 End Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255

C	192.168.0.0	192.168.255.255

Special Address: IP Range from 127.0.0.1 to 127.255.255.255 are network testing addresses also known as loopback addresses are the special IP address.

Intermediate Interview Questions

1. What is the DNS?

DNS is the Domain Name System. It is considered as the devices/services directory of the Internet. It is a decentralized and hierarchical naming system for devices/services connected to the Internet. It translates the domain names to their corresponding IPs. For e.g. interviewbit.com to 172.217.166.36. It uses port 53 by default.

2. What is the use of a router and how is it different from a gateway?

The router is a networking device used for connecting two or more network segments. It directs the traffic in the network. It transfers information and data like web pages, emails, images, videos, etc. from source to destination in the form of packets. It operates at the network layer. The gateways are also used to route and regulate the network traffic but, they can also send data between two dissimilar networks while a router can only send data to similar networks.

3. 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.

4. Describe the OSI Reference Model

Open System Interconnections (OSI) 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 summarized briefly as below:

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

5. Define the 7 different layers of the OSI Reference Model

https://www.forcepoint.com/cyber-edu/osi-model

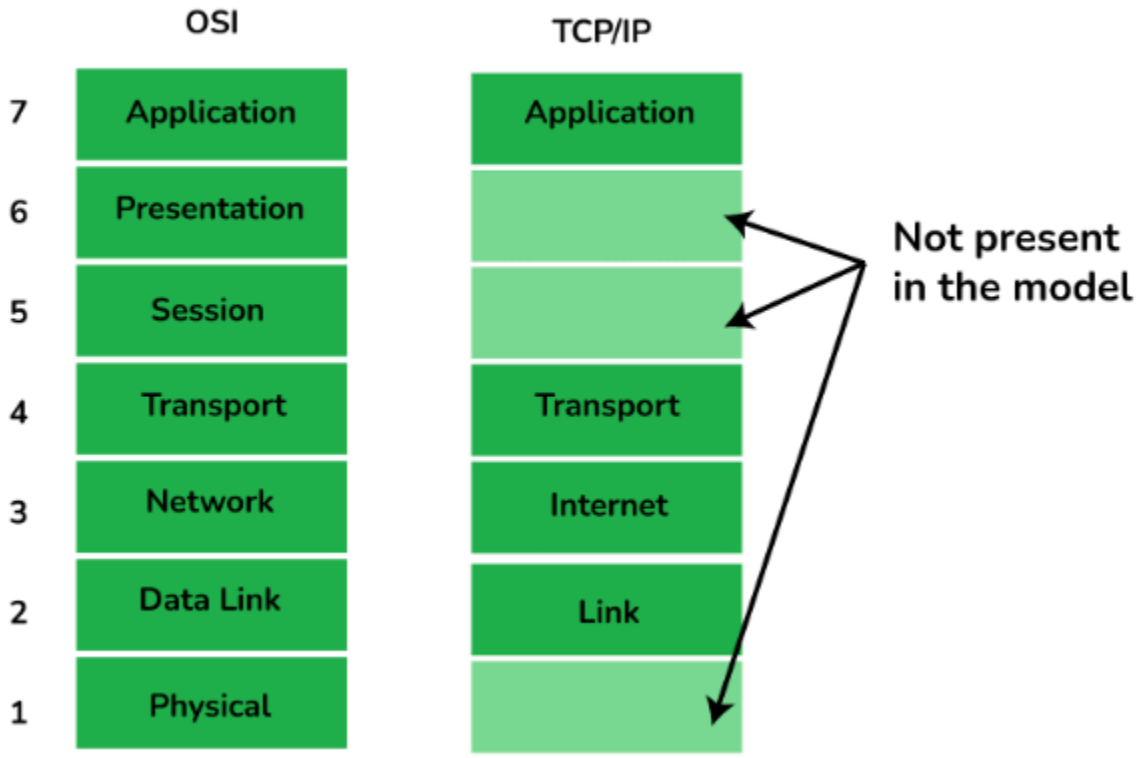
6. Describe the TCP/IP Reference Model

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 1980s. The name of this model is based on 2 standard protocols used i.e. TCP (Transmission Control Protocol) and IP (Internet Protocol).

7. Define the 4 different layers of the TCP/IP Reference Model

https://www.geeksforgeeks.org/tcp-ip-model/

8. Differentiate OSI Reference Model with TCP/IP Reference Model



OSI Vs TCP/IP

OSI Reference Model	TCP/IP Reference Model
7 layered architecture	4 layered architecture
Fixed boundaries and functionality for each layer	Flexible architecture with no strict boundaries between layers
Low Reliability	High Reliability
Vertical Layer Approach	Horizontal Layer Approach

9. What are the HTTP and the 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 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.

Advanced Interview Questions

1. What is the FTP protocol?

FTP is a File Transfer Protocol. It is an application layer protocol used to transfer files and data reliably and efficiently between hosts. It can also be used to download files from remote servers to your computer. It uses port 27 by default.

2. What is the TCP protocol?

TCP or TCP/IP is the Transmission Control Protocol/Internet Protocol. It is a set of rules that decides how a computer connects to the Internet and how to transmit the data over the network. It creates a virtual network when more than one computer is connected to the network and uses the three ways handshake model to establish the connection which makes it more reliable.

3. What is the UDP protocol?

UDP is the User Datagram Protocol and is based on Datagrams. Mainly, it is used for multicasting and broadcasting. Its functionality is almost the same as TCP/IP Protocol

except for the three ways of handshaking and error checking. It uses a simple transmission without any hand-shaking which makes it less reliable.

4. 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

5. What is the ICMP protocol?

ICMP is the Internet Control Message Protocol. It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing if the data is reaching the preferred destination in time. It uses port 7 by default.

6. What do you mean by the DHCP Protocol?

DHCP is the Dynamic Host Configuration Protocol.

It is an application layer protocol used to auto-configure devices on IP networks enabling them to use the TCP and UDP-based protocols. The DHCP servers auto-assign the IPs and other network configurations to the devices individually which enables them to communicate over the IP network. It helps to get the subnet mask, IP address and helps to resolve the DNS. It uses port 67 by default.

7. What is the ARP protocol?

ARP is Address Resolution Protocol. It is a network-level protocol used to convert the logical address i.e. IP address to the device's physical address i.e. MAC address. It can also be used to get the MAC address of devices when they are trying to communicate over the local network.

8. What is the MAC address and how is it related to NIC?

MAC address is the Media Access Control address. It is a 48-bit or 64-bit unique identifier of devices in the network. It is also called the physical address embedded with Network Interface Card (NIC) used at the Data Link Layer. NIC is a hardware component in the networking device using which a device can connect to the network.

9. Differentiate the MAC address with the IP address

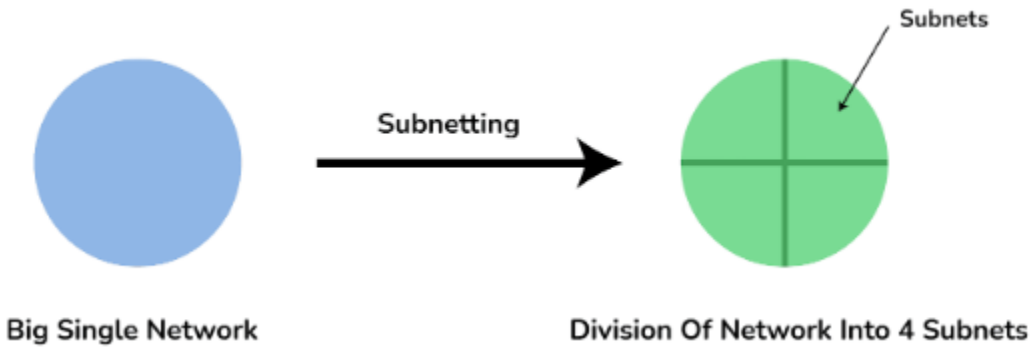
The difference between MAC address and IP address are as follows:

MAC Address	IP Address
Media Access Control Address	Internet Protocol Address
6 or 8-byte hexadecimal number	4 (IPv4) or 16 (IPv6) Byte address
It is embedded with NIC	It is obtained from the network

Physical Address	Logical Address
Operates at Data Link Layer	Operates at Network Layer.
Helps to identify the device	Helps to identify the device connectivity on the network.

10. What is a 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.



Subnet

11. Compare the hub vs switch

Hub	Switch
Operates at Physical Layer	Operates at Data Link Layer
Half-Duplex transmission mode	Full-Duplex transmission mode

Ethernet devices can be connectedsend	LAN devices can be connected
Less complex, less intelligent, and cheaper	Intelligent and effective
No software support for the administration	Administration software support is present
Less speed up to 100 MBPS	Supports high speed in GBPS
Less efficient as there is no way to avoid collisions when more than one nodes sends the packets at the same time	More efficient as the collisions can be avoided or reduced as compared to Hub

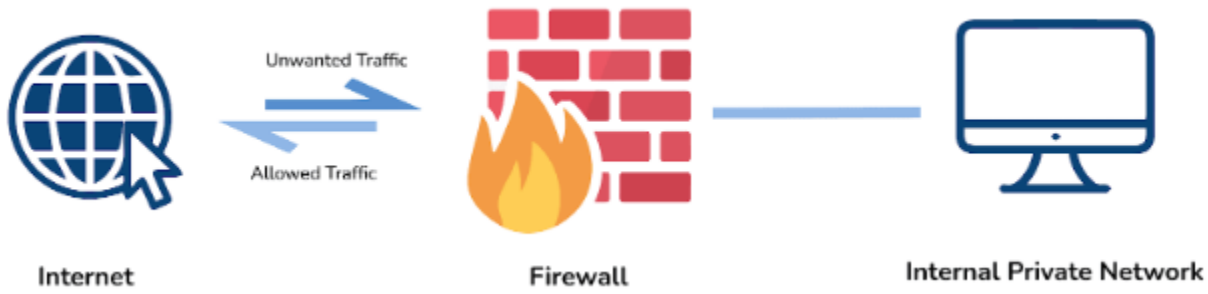
12. What is the difference between the ipconfig and the ifconfig?

ipconfig	ifconfig
Internet Protocol Configuration	Interface Configuration
Command used in Microsoft operating systems to view and configure network interfaces	Command used in MAC, Linux, UNIX operating systems to view and configure network interfaces

13. What is the firewall?

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.



Firewall

14. What are Unicasting, Anycasting, Multicasting and Broadcasting?

- Unicasting: If the message is sent to a single node from the source then it is known as unicasting. This is commonly used in networks to establish a new connection.
- Anycasting: If the message is sent to any of the nodes from the source then it is known as anycasting. It is mainly used to get the content from any of the servers in the Content Delivery System.
- Multicasting: If the message is sent to a subset of nodes from the source then it is known as multicasting. Used to send the same data to multiple receivers.
- Broadcasting: If the message is sent to all the nodes in a network from a source then it is known as broadcasting. DHCP and ARP in the local network use broadcasting.

15. 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.