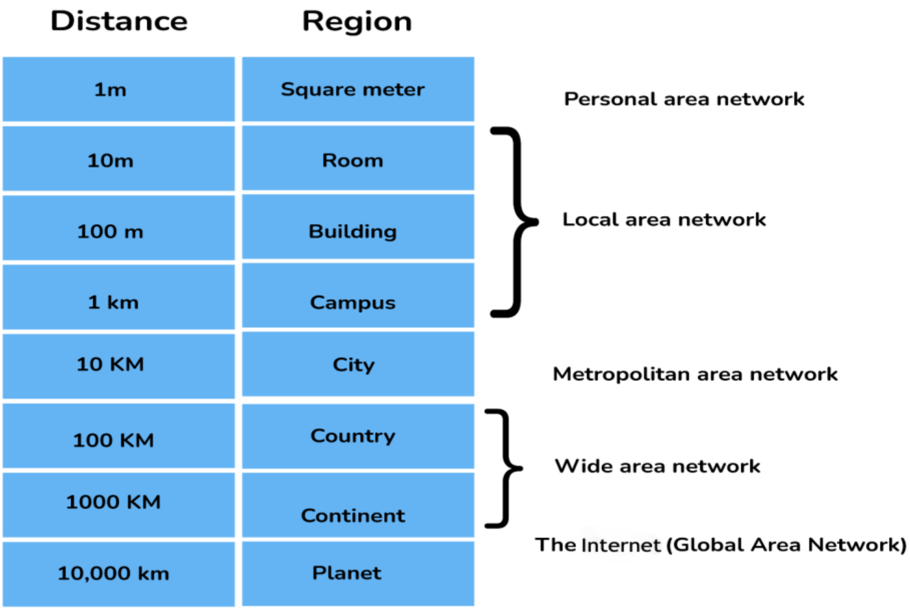
INTERVIEW QUESTIONS ON COMPUTER NETWORKS

1. 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:



Distance	Region	
1m	Square meter	Personal area network
10m	Room	Local area network
100 m	Building	
1 km	Campus	
10 KM	City	Metropolitan area network
100 KM	Country	Wide area network
1000 KM	Continent	
10,000 km	Planet	The Internet (Global Area Network)

2. Explain different types of networks.

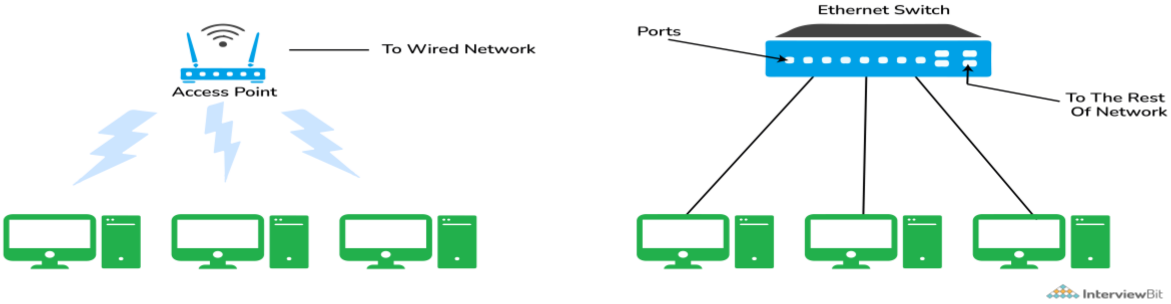
Below are few types of networks:

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

Type	Description
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.

3. Explain LAN (Local Area Network)

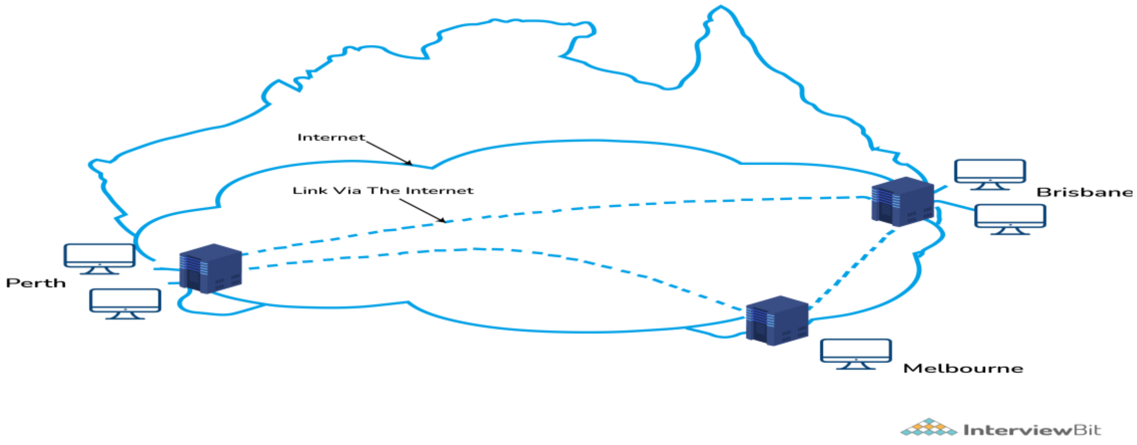
LANs are widely used to connect computers/laptops and consumer electronics which enables them to share resources (e.g., printers, fax machines) and exchange information. When LANs are used by companies or organizations, they are called **enterprise networks**. There are two different types of LAN networks 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)

4. 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)

5. 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.

6. What are the different types of VPN?

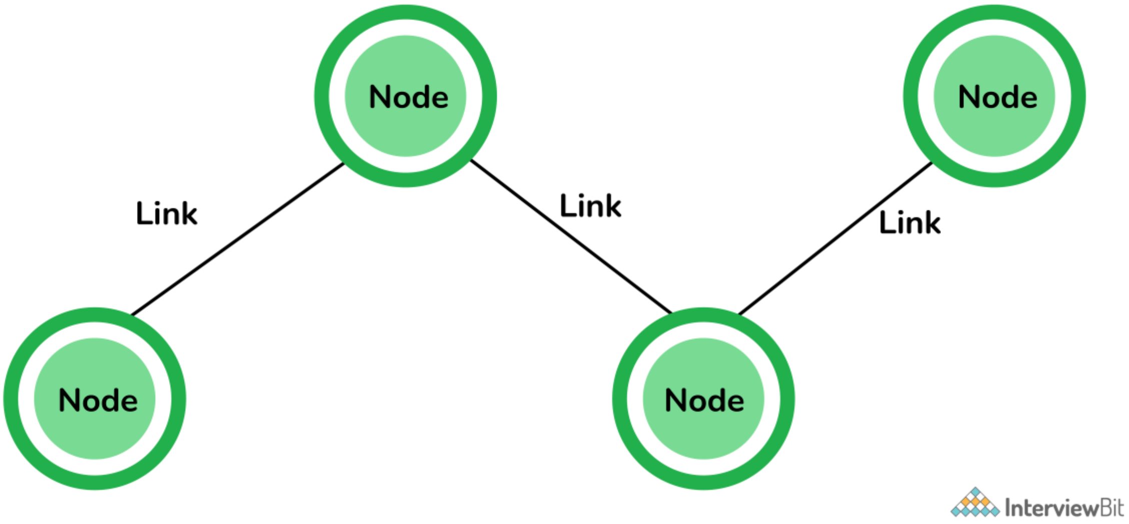
Few types of VPN are:

- **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.

7. 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.



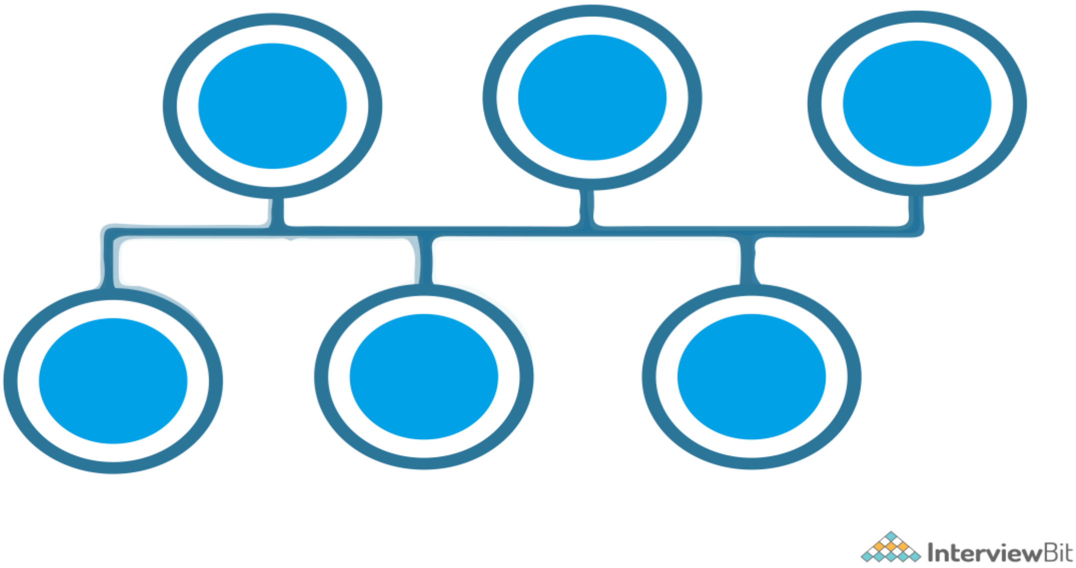
8. What is the network topology?

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.

9. Define different types of network topology

The different types of network topology are given below:

Bus Topology:

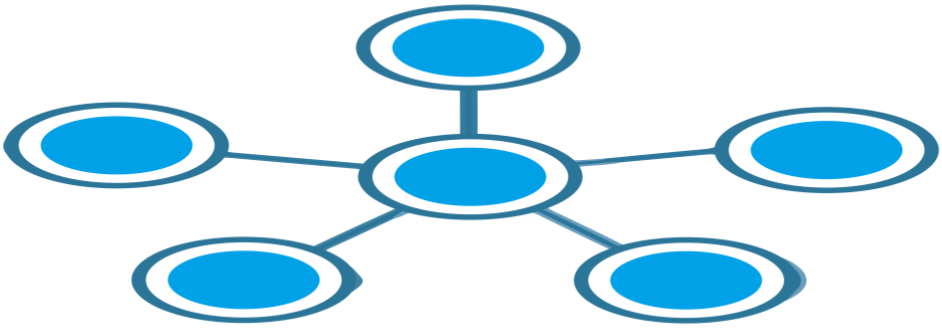


Bus Topology

- 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.

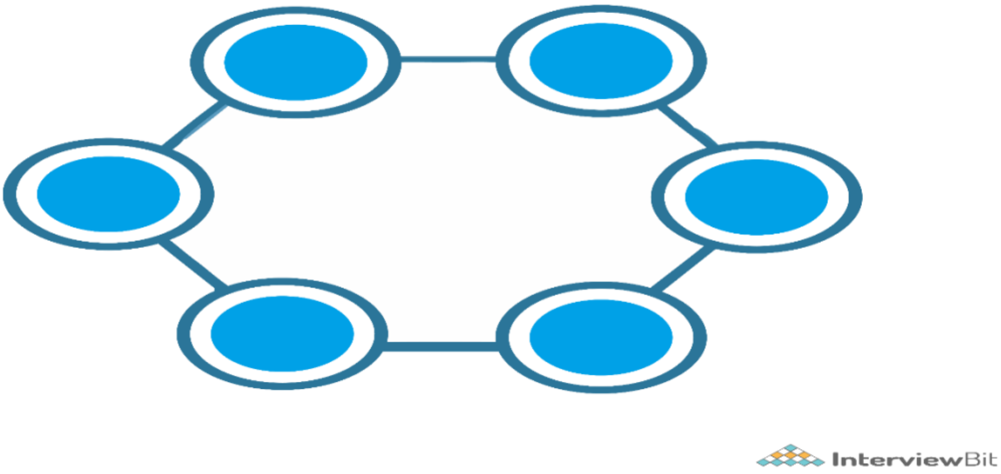
Star Topology:



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.

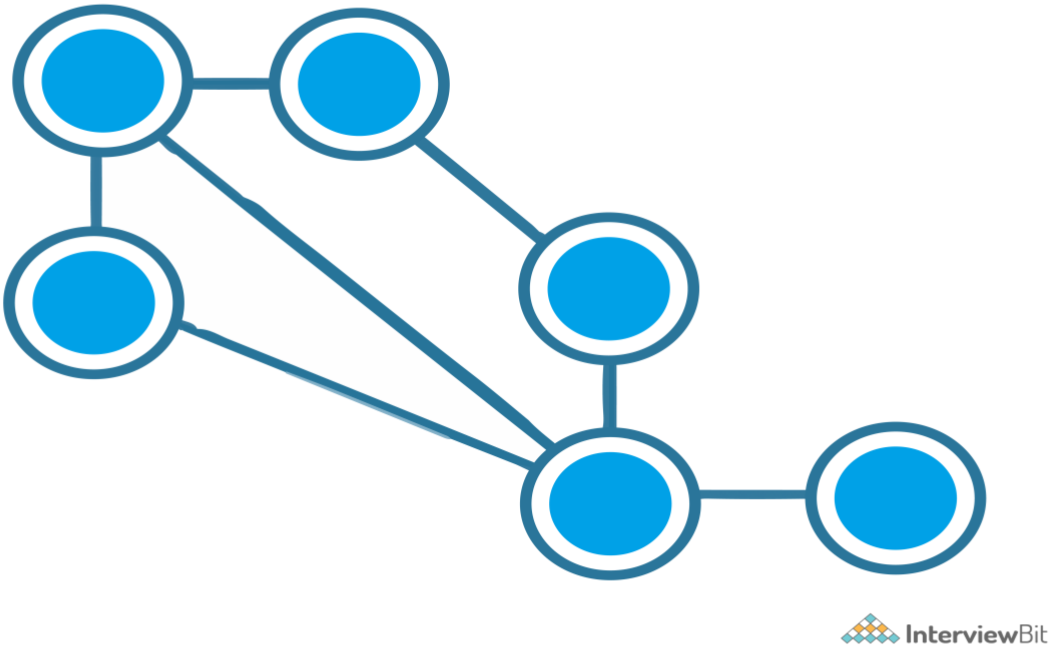
Ring Topology:



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

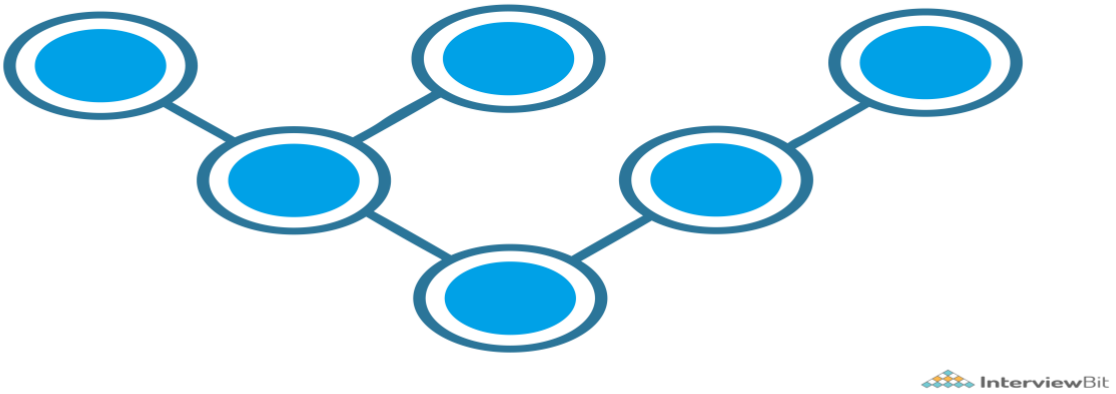
Mesh Topology:



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.

10. What is an IPv4 address? What are the different classes of IPv4?

An IP address is a 32-bit dynamic address of a node in the network. An IPv4 address has 4 octets of 8-bit each with each number with a value up to 255.

IPv4 classes are differentiated based on the number of hosts it supports on the network. There are five types of IPv4 classes and are based on the first octet of IP addresses which are classified as Class A, B, C, D, or E.

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage
A	0.0.0.0	127.255.255.255	Used for Large Network
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D

11. 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
B	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.

12. Describe the OSI Reference Model

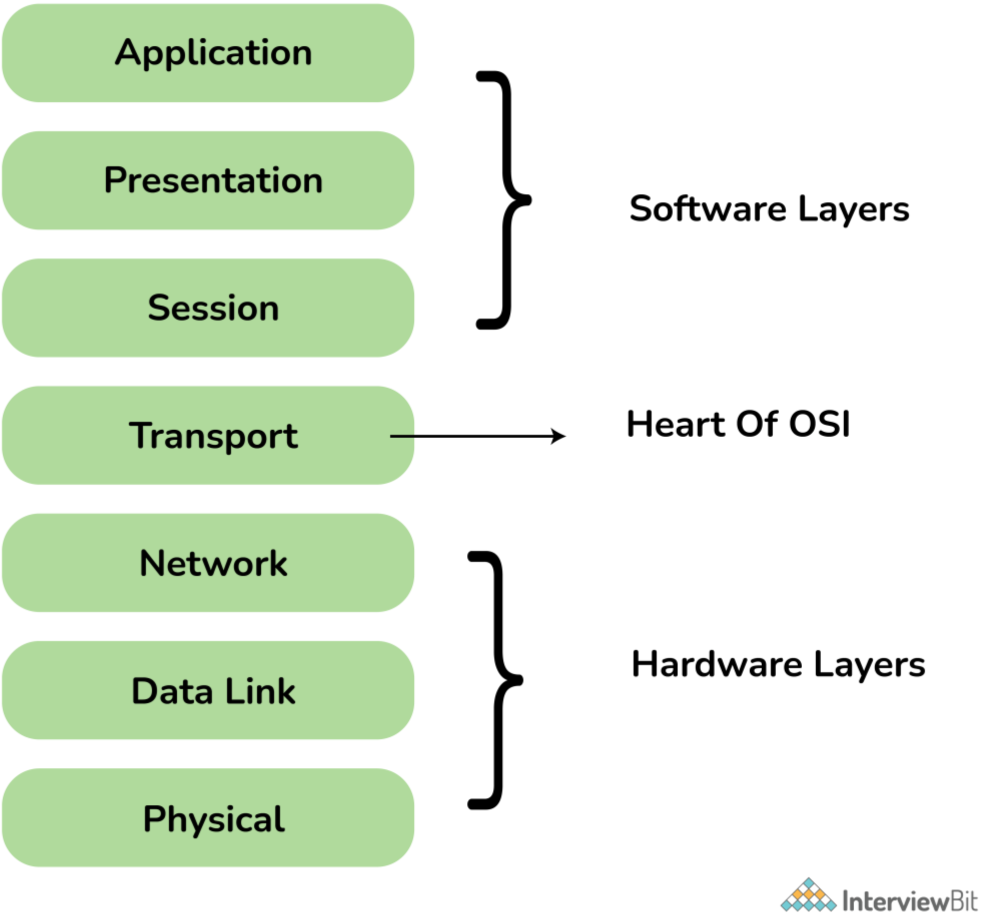
Open System Interconnections (OSI) is a network architecture model based on the ISO standards. It is called the OSI model as it deals with connecting the systems that are open for communication with other systems.

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.

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

Here the 7 layers of the OSI reference model:



Layers of OSI Model

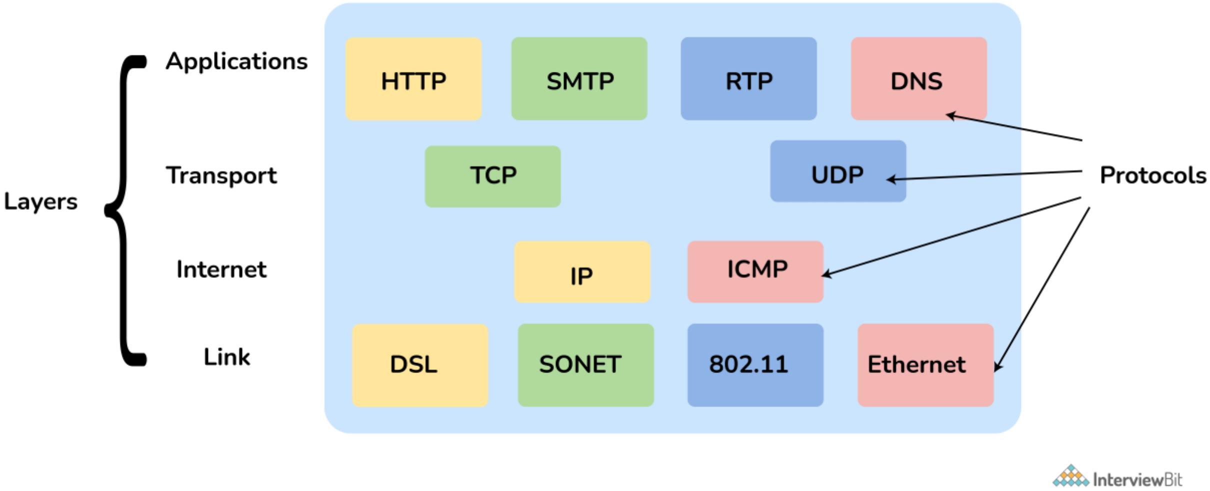
Layer	Unit Exchanged	Description
Physical	Bit	• It is concerned with transmitting raw bits over a communication channel. • Chooses which type of transmission mode is to be selected for the transmission. The available transmission modes are Simplex, Half Duplex and Full Duplex.,
Data Link	Frame	• The main task of this layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors. • It also allows detecting damaged packets using the CRC (Cyclic Redundancy Check) error-detecting, code. • When more than one node is connected to a shared link, Data Link Layer protocols are required to determine which device has control over the link at a given time. • It is implemented by protocols like CSMA/CD, CSMA/CA, ALOHA, and Token Passing.
Network	Packet	• It controls the operation of the subnet. • The network layer takes care of feedback messaging through ICMP messages.
Transport	TPDU - Transaction Protocol Data Unit	• The basic functionality of this layer is to accept data from the above layers, split it up into smaller units if needed, pass these to the network layer, and ensure that all the pieces arrive correctly at the other end. • The Transport Layer takes care of Segmentation and Reassembly.
Session	SPDU - Session Protocol Data Unit	• The session layer allows users on different machines to establish sessions between them.

Layer	Unit Exchanged	Description
		- Dialogue control is using the full-duplex link as half-duplex. It sends out dummy packets from the client to the server when the client is ideal.
Presentation	PPDU - Presentation Protocol Data Unit	- The presentation layer is concerned with the syntax and semantics of the information transmitted. - It translates a message from a common form to the encoded format which will be understood by the receiver.
Application	APDU - Application Protocol Data Unit	- It contains a variety of protocols that are commonly needed by users. - The application layer sends data of any size to the transport layer.

14. 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).

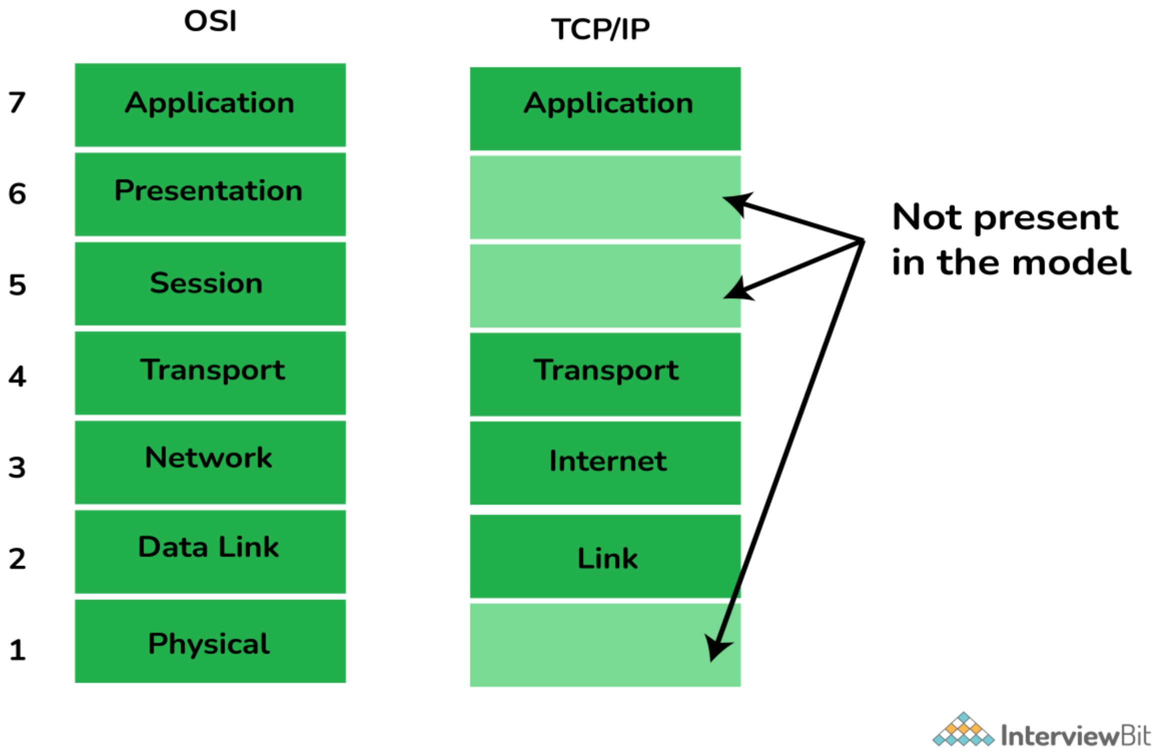
15. Define the 4 different layers of the TCP/IP Reference Model



Layers of TCP/IP

Layer	Description
Link	Decides which links such as serial lines or classic Ethernet must be used to meet the needs of the connectionless internet layer.
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.
Transport	Its functionality is almost the same as the OSI transport layer. It enables peer entities on the network to carry on a conversation.
Application	It contains all the higher-level protocols.

16. 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

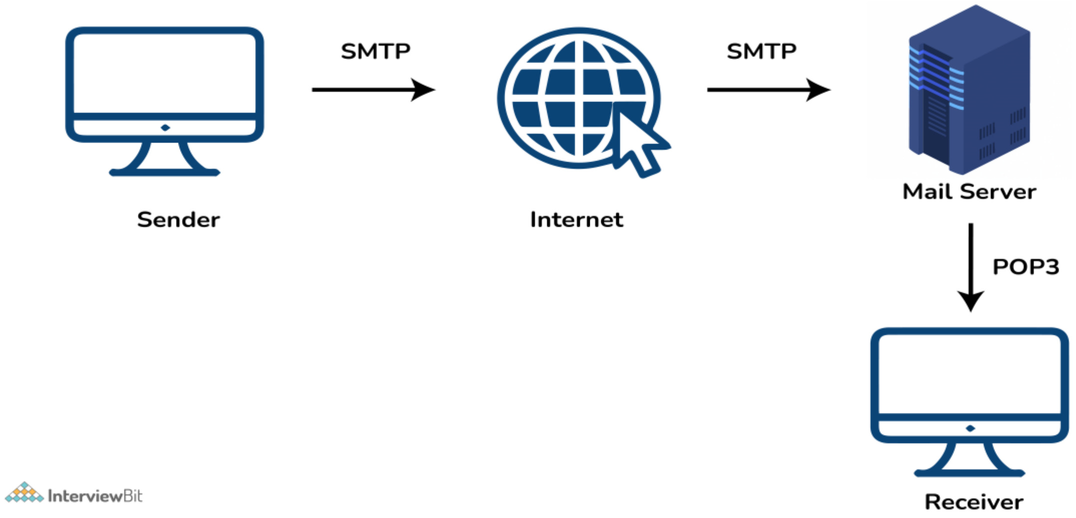
17. What are the HTTP and the HTTPS protocol?

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.

18. 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.



SMTP Protocol

19. 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.

20. 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.

21. 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.

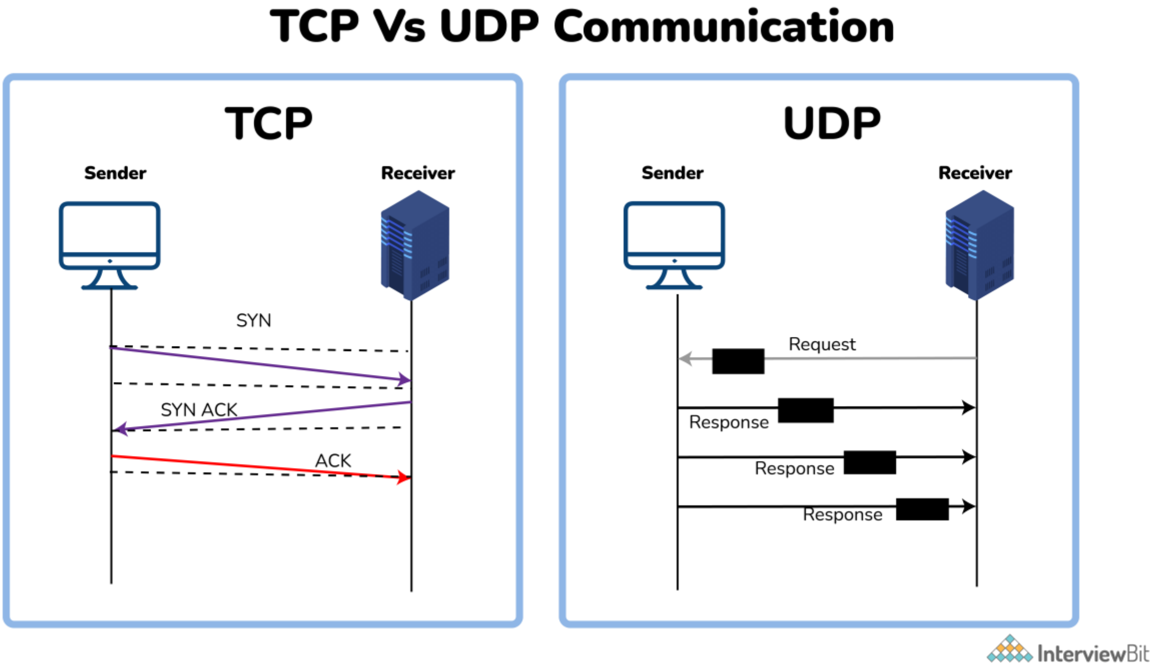
22. What is the UDP protocol?

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.

23. 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/IP	UDP
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



TCP VS UDP

24. 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.

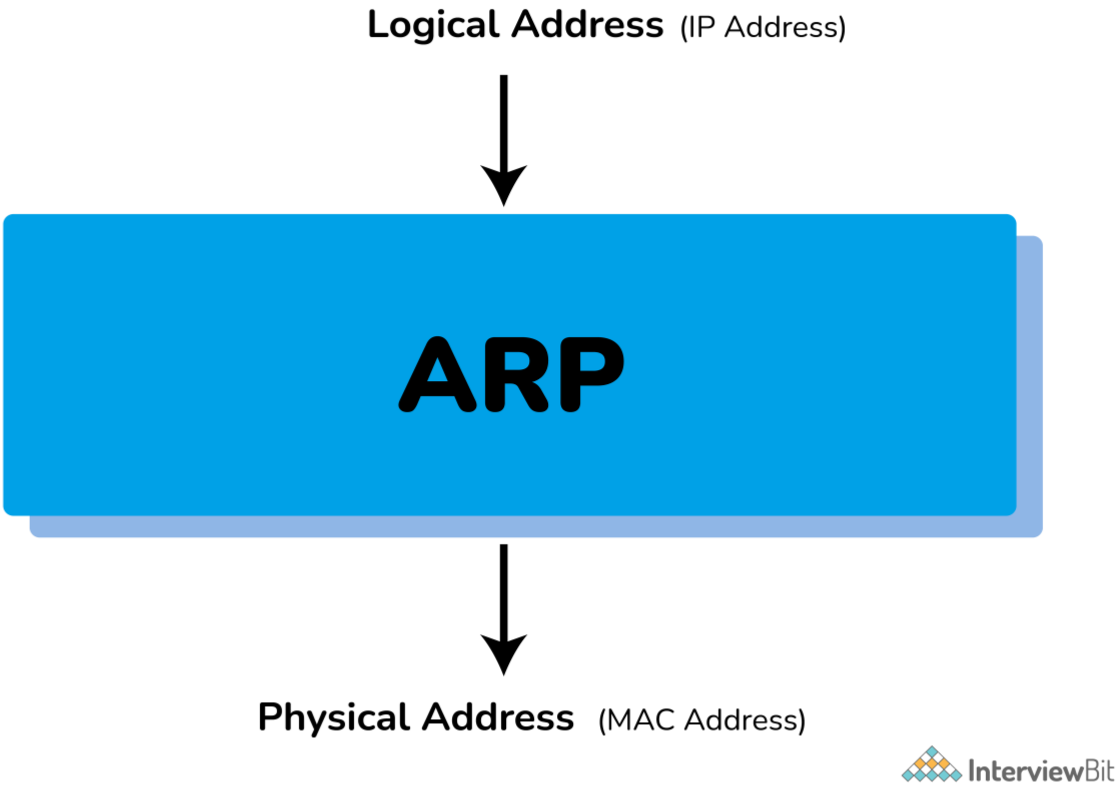
25. What do you mean by the DHCP Protocol?

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.

26. 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.



ARP Protocol

27. 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.

28. 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.

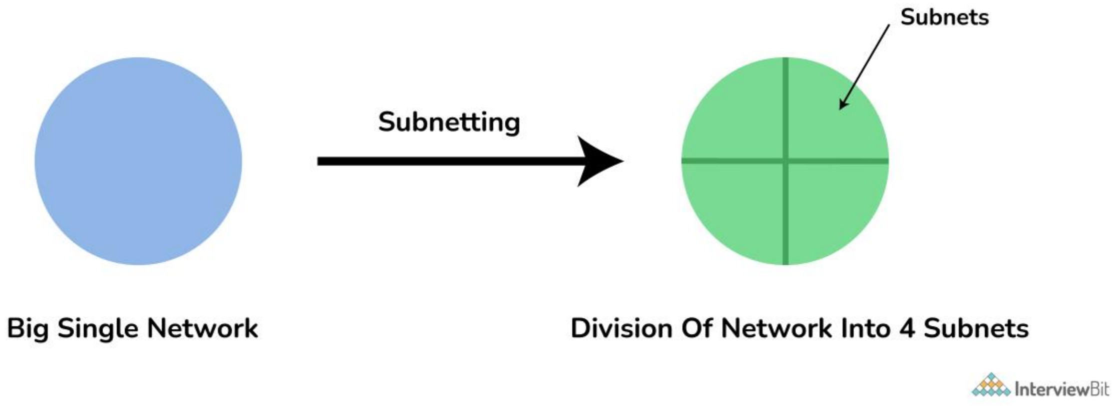
29. Differentiate the MAC address with the IP address

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.

30. 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

31. Compare the hub vs switch

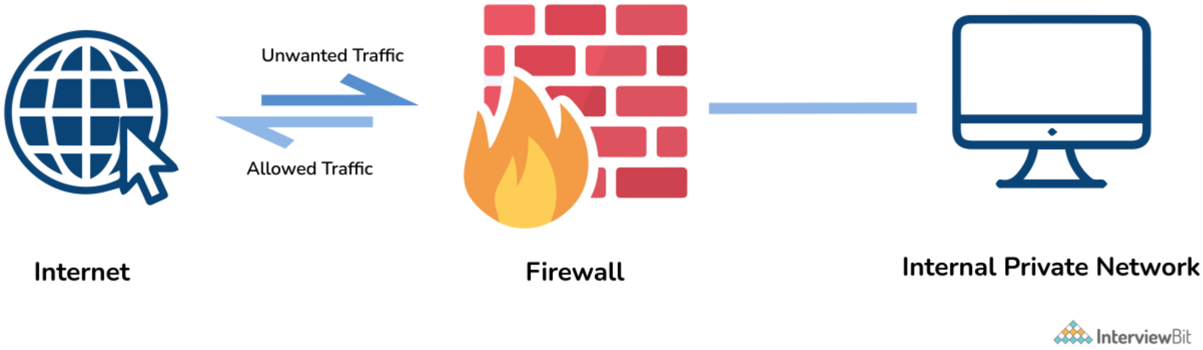
Hub	Switch
Operates at Physical Layer	Operates at Data Link Layer
Half-Duplex transmission mode	Full-Duplex transmission mode
Ethernet devices can be connectedsend	LAN devices can be connected
Less complex, less intelligent, and cheaper	Intelligent and effective
No software support for the administration	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

32. 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
Used to get the TCP/IP summary and allows to changes the DHCP and DNS settings	

33. 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

34. 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.

35. 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.

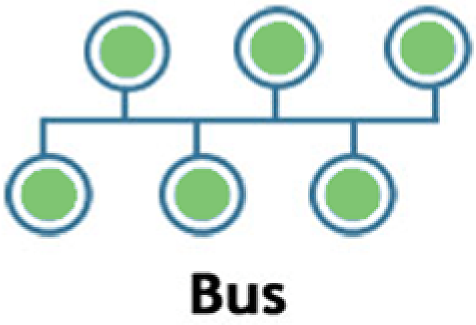
1) What is the network?

- 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?

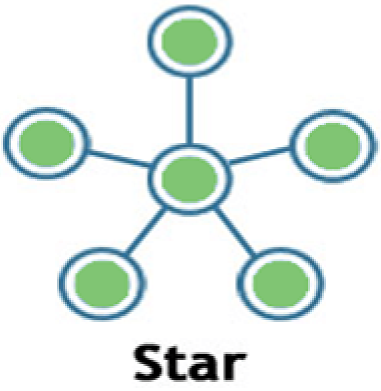
Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other. The types of topologies are:

Bus:



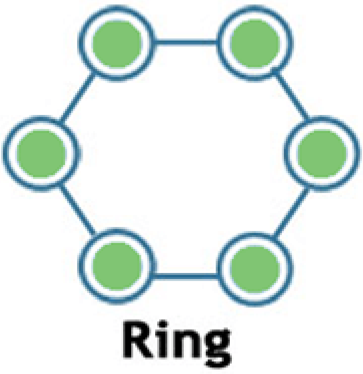
- Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
- It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to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

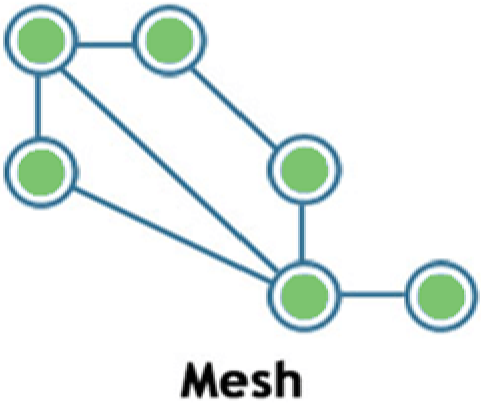
Ring



- 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.

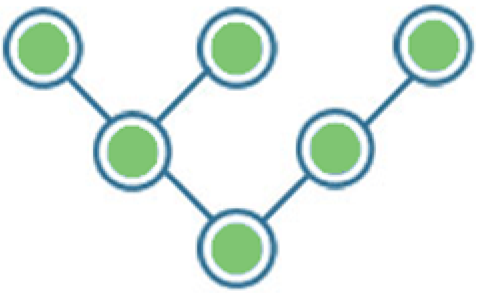
- Ring topology is very rarely used as it is expensive, difficult to install and manage.
- Examples of Ring topology are SONET network, SDH network, etc.

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

- 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) What are the advantages of Distributed Processing?

A list of advantages of distributed processing:

- Secure
- Support Encapsulation
- Distributed database
- Faster Problem solving
- Security through redundancy
- Collaborative Processing

4) What is the criteria to check the network reliability?

Network reliability: Network reliability means the ability of the network to carry out the desired operation through a network such as communication through a network.

Network reliability plays a significant role in the network functionality. The network monitoring systems and devices are the essential requirements for making the network reliable.The network monitoring system identifies the problems that are occurred in the network while the network devices ensure that data should reach the appropriate destination.

The reliability of a network can be measured by the following factors:

- **Downtime**: The downtime is defined as the required time to recover.
- **Failure Frequency**: It is the frequency when it fails to work the way it is intended.
- **Catastrophe**: It indicates that the network has been attacked by some unexpected event such as fire, earthquake.

5) Which are the different factors that affect the security of a network?

There are mainly two security affecting factors:

- Unauthorized Access
- Viruses

6) Which are the different factors that affect the reliability of a network?

The following factors affect the reliability of a network:

- Frequency of failure
- Recovery time of a network after a failure

7) Which are the different factors that affect the performance of a network?

The following factors affect the performance of a network:

- Large number of users
- Transmission medium types
- Hardware
- Software

8) What makes a network effective and efficient?

There are mainly two criteria which make a network effective and efficient:

- **Performance:** : performance can be measured in many ways like transmit time and response time.
- **Reliability:** reliability is measured by frequency of failure.
- **Robustness:** robustness specifies the quality or condition of being strong and in good condition.
- **Security:** It specifies how to protect data from unauthorized access and viruses.

9) What is bandwidth?

Every signal has a limit of upper range frequency and lower range frequency. The range of limit of network between its upper and lower frequency is called bandwidth.

10) What is a node and link?

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

11) What is a gateway? Is there any difference between a 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.

12) What is DNS?

DNS is an acronym stands for Domain Name System.

- DNS was introduced by Paul Mockapetris and Jon Postel in 1983.
- It is a naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate to resource easily over a network.
- DNS is an internet which maps the domain names to their associated IP addresses.
- Without DNS, users must know the IP address of the web page that you wanted to access.

Working of DNS:

If you want to visit the website of "javaTpoint", then the user will type "https://www.javatpoint.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.

13) What is DNS forwarder?

- A forwarder is used with 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.
- **Following are the ways that the DNS server behaves when it is configured as a forwarder**:
  - When the DNS server receives the query, then it resolves the query by using a cache.
  - If the DNS server is not able to resolve the query, then it forwards the query to another DNS server.
  - If the forwarder is not available, then it will try to resolve the query by using root hint.

14) What is NIC?

- 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.

15) What is the meaning of 10Base-T?

It is used to specify data transfer rate. In 10Base-T, 10 specify the data transfer rate, i.e., 10Mbps. The word Base specifies the baseband as opposed to broadband. T specifies the type of the cable which is a twisted pair.

16) What is NOS in computer networking?

- NOS stands for Network Operating System. It is specialized software which is used to provide network connectivity to a computer to make communication possible with other computers and connected devices.
- NOS is the software which allows the device to communicate, share files with other devices.
- The first network operating system was Novel NetWare released in 1983. Some other examples of NOS are Windows 2000, Windows XP, Linux, etc.

17) What are the different types of networks?

Networks can be divided on the basis of area of distribution. For example:

- **PAN (Personal Area Network)**: Its range limit is up to 10 meters. It is created for personal use. Generally, personal devices are connected to this network. For example computers, telephones, fax, printers, etc.
- **LAN (Local Area Network)**: It is used for a small geographical location like office, hospital, school, etc.
- **HAN (House Area Network)**: It is actually a LAN that is used within a house and used to connect homely devices like personal computers, phones, printers, etc.
- **CAN (Campus Area Network)**: It is a connection of devices within a campus area which links to other departments of the organization within the same campus.

- **MAN (Metropolitan Area Network)**: It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.
- **WAN (Wide Area Network)**: It is used over a wide geographical location that may range to connect cities and countries.
- **GAN (Global Area Network)**: It uses satellites to connect devices over global are.

18) What is POP3?

POP3 stands for Post Office Protocol version3. POP is responsible for accessing the mail service on a client machine. POP3 works on two models such as Delete mode and Keep mode.

19) What do you understand by MAC address?

MAC stands for Media Access Control. It is the address of the device at the Media Access Control Layer of Network Architecture. It is a unique address means no two devices can have same MAC addresses.

20) What is IP address?

IP address is a unique 32 bit software address of a computer in a network system.

21) What is 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 internet on these private IPs, you must have to use proxy server or NAT server.

22) What is public IP address?

A public IP address is an address taken by the Internet Service Provider which facilitates you to communication on the internet.

23) What is APIPA?

APIPA is an acronym stands for Automatic Private IP Addressing. This feature is generally found in Microsoft operating system.

24) What is the full form of ADS?

- ADS stands for Active Directory Structure.
- ADS is a microsoft technology used to manage the computers and other devices.
- ADS allows the network administrators to manage the domains, users and objects within the network.
- ADS consists of three main tiers:

- **Domain**: Users that use the same database will be grouped into a single domain.
- **Tree**: Multiple domains can be grouped into a single tree.
- **Forest**: Multiple trees can be grouped into a single forest.

25) What is RAID?

RAID is a method to provide Fault Tolerance by using multiple Hard Disc Drives.

26) What is anonymous FTP?

Anonymous FTP is used to grant users access to files in public servers. Users which are allowed access to data in these servers do not need to identify themselves, but instead log in as an anonymous guest.

27) What is protocol?

A protocol is a set of rules which is used to govern all the aspects of information communication.

28) What are the main elements of a protocol?

The main elements of a protocol are:

- **Syntax**: It specifies the structure or format of the data. It also specifies the order in which they are presented.
- **Semantics**: It specifies the meaning of each section of bits.
- **Timing**: Timing specifies two characteristics: When data should be sent and how fast it can be sent.

29 What is the Domain Name System?

There are two types of client/server programs. First is directly used by the users and the second supports application programs.

The Domain Name System is the second type supporting program that is used by other programs such as to find the IP address of an e-mail recipient.

30) What is link?

A link is connectivity between two devices which includes the cables and protocols used in order to make communication between devices.

31) 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.

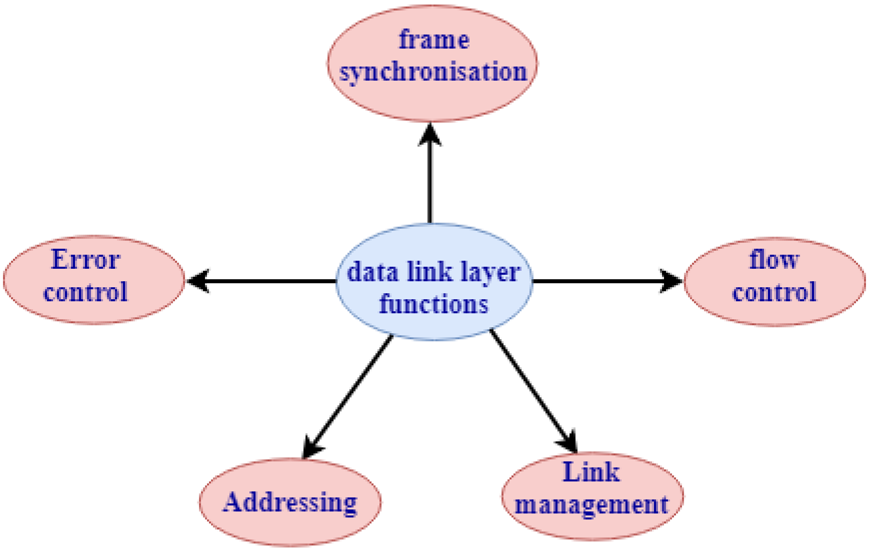
There are 7 layers in the OSI reference model.

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. DataLink Layer

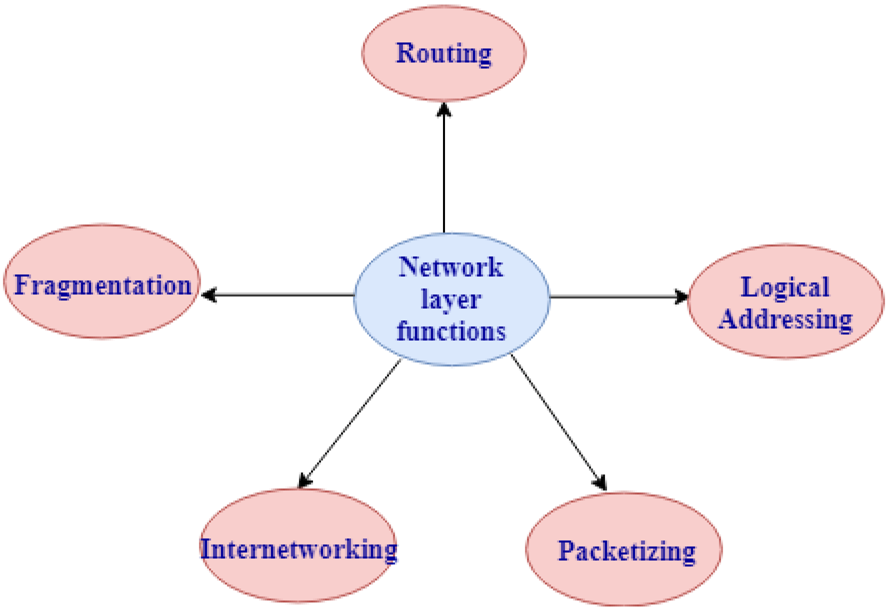
- It is used for transferring the data from one node to another node.
- It receives the data from the network layer and converts the data into data frames and then attach the physical address to these frames which are sent to the physical layer.
- It enables the error-free transfer of data from one node 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.

32) What is the usage of OSI physical layer?

The OSI physical layer is used to convert data bits into electrical signals and vice versa. On this layer, network devices and cable types are considered and setup.

33) Explain the functionality of OSI session layer?

OSI session layer provides the protocols and means for two devices on the network to communicate with each other by holding a session. This layer is responsible for setting up the session, managing information exchange during the session, and tear-down process upon termination of the session.

34) What is the maximum length allowed for a UTP cable?

The maximum length of UTP cable is 90 to 100 meters.

35) What is RIP?

- RIP stands for Routing Information Protocol. It is accessed by the routers to send data from one network to another.
- RIP is a dynamic protocol which is used to find the best route from source to the destination over a network by using the hop count algorithm.
- Routers use this protocol to exchange the network topology information.
- This protocol can be used by small or medium-sized networks.

36) 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.

37) What is netstat?

The "netstat" is a command line utility program. It gives useful information about the current TCP/IP setting of a connection.

38) What do you understand by ping command?

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.

39) What is Sneakernet?

Sneakernet is the earliest form of networking where the data is physically transported using removable media.

40) Explain the peer-peer process.

The processes on each machine that communicate at a given layer are called peer-peer process.

41) What is a congested switch?

A switch receives packets faster than the shared link. It can accommodate and stores in its memory, for an extended period of time, then the switch will eventually run out of buffer space, and some packets will have to be dropped. This state is called a congested state.

42) What is multiplexing in networking?

In Networking, multiplexing is the set of techniques that is used to allow the simultaneous transmission of multiple signals across a single data link.

43) What are the advantages of address sharing?

Address sharing provides security benefit instead of routing. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer that provides address translation and not the private IP addresses on the internal network.

44) What is RSA Algorithm?

RSA is short for Rivest-Shamir-Adleman algorithm. It is mostly used for public key encryption.

45) How many layers are in TCP/IP?

There are basic 4 layers in TCP/IP:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Layer

46) What is the difference between TCP/IP model and the OSI model?

Following are the differences between the TCP/IP model and OSI model:

TCP/IP model	OSI model
Full form of TCP is transmission control protocol.	Full form of OSI is Open System Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable than the OSI model.	OSI model is less reliable as compared to the TCP/IP model.
TCP/IP model uses horizontal approach.	OSI model uses vertical approach.
TCP/IP model uses both session and presentation layer in the application layer.	OSI Reference model uses separate session and presentation layers.
TCP/IP model developed the protocols first and then model.	OSI model developed the model first and then protocols.
In Network layer, TCP/IP model supports only connectionless communication.	In the Network layer, the OSI model supports both connection-oriented and connectionless communication.
TCP/IP model is a protocol dependent.	OSI model is a protocol independent.

47) What is the difference between domain and workgroup?

Workgroup	Domain
A workgroup is a peer-to-peer computer network.	A domain is a Client/Server network.
A Workgroup can consist of maximum 10 computers.	A domain can consist up to 2000 computers.
Every user can manage the resources individually on their PCs.	There is one administrator to administer the domain and its resources.
All the computers must be on the same local area network.	The computer can be on any network or anywhere in the world.
Each computer must be changed manually.	Any change made to the computer will reflect the changes to all the computers.

1. Name two technologies by which you would connect two offices in remote locations.

Two technologies by which would connect two offices in remote locations are VPN and Cloud computing.

2. What is internetworking?

Internetworking is a combination of two words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was interconnected. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

3. Name of the software layers or User support layer in OSI model.

- Application layer
- Presentation layer
- Session layer

4. Name of the hardware layers or network support layer in OSI model.

- Network layer
- Datalink layer
- Physical layer

5. Define HTTPS protocol?

The full form of HTTPS is Hypertext transfer protocol secure. It is an advanced version of the HTTP protocol. Its port number is 443 by default. It uses SSL/TLS protocol for providingsecurity.

6. Name some services provided by the application layer in the Internet model?

Some services provided by the application layer in the Internet model are as follows:

- Mail services
- Directory services
- File transfer
- Access management
- Network virtual terminal

7. In which OSI layer is the header and trailer added?

At Data link layer trailer is added and at OSI model layer 6,5,4,3 added header.

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

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

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

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

10. What is zone-based firewall?

A Zone-based firewall is an advanced method of the stateful firewall. In a stateful firewall, a stateful database is maintained in which source IP address, destination IP address, source port number, destination port number are recorded. Due to this, only the replies are allowed i.e if the traffic is Generated from inside the network then only the replies (of inside network traffic) coming from outside the network is allowed.

Cisco IOS router can be made firewall through two methods:

1. By using CBAC: create an access list and apply it to the interfaces keeping in mind what traffic should be allowed or denied and in what direction. This has an extra overhead for the administrator.
2. Using a Zone-based firewall.

For more details please refer Zone-based firewall article.

11. What is a server farm?

A server farm is a set of many servers interconnected together and housed within the same physical facility. A server farm provides the combined computing power of many servers by simultaneously executing one or more applications or services. A server farm is generally a part of an enterprise data center or a component of a supercomputer. A server farm is also known as a server cluster or computer ranch.

12. Name the three means of user authentication.

There is biometrics (e.g. a thumbprint, iris scan), a token, or a password. There is also two-level authentication, which employs two of those methods.

13. What is Confidentiality, Integrity & Availability?

Confidentiality – means information is not disclosed to unauthorized individuals, entities, and processes. For example, if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case, my password has been compromised and Confidentiality has been breached.

Integrity – means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example, if an employee leaves an organization then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition, this is only authorized person should be allowed to edit employee data.

Availability – means information must be available when needed. For example, if one needs to access information of a particular employee to check whether an employee has outstood the number of leaves, in that case, it requires collaboration from different organizational teams like network operations, development operations, incident response, and policy/change management.
Denial of service attack is one of the factors that can hamper the availability of information.

14. What is VPN?

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection. For more details please refer VPN article

15. What is Symmetric and Asymmetric Encryption?

Symmetric Key Encryption:
Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

Asymmetric Key Encryption:
Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different keys to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower. For more details please refer difference between symmetric and asymmetric encryption articles.

16. At what layer IPsec works?

An IPsec works on layer 3 of the OSI model.

17. What is a Tunnel mode?

This is a mode of data exchange wherein two communicating computers do not use IPSec themselves. Instead, the gateway that is connecting their LANs to the transit network creates a virtual tunnel that uses the IPSec protocol to secure all communication that passes through it. Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it. Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall

18. Define Digital Signatures?

As the name sounds are the new alternative to sign a document digitally. It ensures that the message is sent to the intended use without any tampering by any third party (attacker). In simple words, digital signatures are used to verify the authenticity of the message sent electronically.

or we can say that – A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

19. What is Authorization?

Authorization provides capabilities to enforce policies on network resources after the user has gained access to the network resources through authentication. After the authentication is successful, authorization can be used to determine what resources is the user allowed to access and the operations that can be performed.

20. What is the difference between IPS and a firewall?

The **intrusion Prevention System** is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it. Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity. IPS typically records information related to observed events, notifies security administrators of important observed events, and produces reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment, or changing the attack's content.

A **firewall** is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic, and based on a defined set of security rules it accepts, rejects, or drops that specific traffic.

21.What is IP Spoofing?

IP Spoofing is essentially a technique used by hackers to gain unauthorized access to Computers. Concepts of IP Spoofing were initially discussed in academic circles as early as 1980. IP Spoofing types of attacks had been known to Security experts on the theoretical level. It was primarily theoretical until Robert Morris discovered a security weakness in the TCP protocol known as sequence prediction. Occasionally IP spoofing is done to mask the origins of a Dos attack. In fact, Dos attacks often mask the actual IP addresses from where the attack has originated from.

22. What is the meaning of threat, vulnerability, and risk?

Threats are anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an **asset**. An asset can be anything people, property, or information. The asset is what we are trying to protect and a threat is what we are trying to protect against. **Vulnerability** means a gap or weakness in our protection efforts.

Risk is nothing but an intersection of assets, threats, and vulnerability.

A+T+V = R

23. What is the main purpose of a DNS server?

DNS stands for Domain Name Server. It translates Internet domain and hostnames to IP addresses and vice versa. DNS technology allows typing names into your Web browsers and our computer to automatically find that address on the Internet. A key element of the DNS is a worldwide collection of DNS servers. It has the responsibility of assigning domain names and mapping those names to Internet resources by designating an authoritative name server for each domain. The Internet maintains two main namespaces like Domain Name hierarchy and Internet protocol addresses space.

24. What is the protocol and port no of DNS?

Protocol – TCP/UDP

Port number- 53

25. What is the position of the transmission media in the OSI model?

In the OSI model, transmission media supports layer-1(Physical layer).

26. What is the importance of twisting in the twisted-pair cable?

The twisted-pair cable consists of two insulated copper wires twisted together. The twisting is important for minimizing electromagnetic radiation and external interference.

27. What kind of error is undetectable by the checksum?

In checksum, multiple bit errors can not be undetectable.

28. Which multiplexing technique is used in the Fiber-optic links?

The wavelength division multiplexing is commonly used in fiber optic links.

29. What are the Advantages of Fiber Optics?

- Bandwidth is above copper cables
- Less power loss and allows data transmission for extended distances
- The optical cable is resistant to electromagnetic interference
- Fiber cable is sized 4.5 times which is best than copper wires
- As the cable is lighter, thinner, in order that they use less area as compared to copper wires
- Installation is extremely easy thanks to less weight.
- Optical fiber cable is extremely hard to tap because they don't produce electromagnetic energy. These optical fiber cables are very secure for transmitting data.
- This cable opposes most acidic elements that hit copper wired also are flexible in nature.
- Optical fiber cables are often made cheaper than equivalent lengths of copper wire.
- Light has the fastest speed within the universe, such a lot faster signals
- Fiber optic cables allow much more cable than copper twisted-pair cables.
- Fiber optic cables have how more bandwidth than copper twisted-pair cables.

30.Which of the multiplexing techniques are used to combine analog signals?

To combine analog signals, commonly FDM(Frequency division multiplexing) and WDM(Wavelength-division multiplexing) are used.

31. Which of the multiplexing techniques is used to combine digital signals?

To combine digital signals, time division multiplexing techniques are used.

32. Can IP Multicast be load-balanced?

No, The ip multicast multipath command load splits the traffic and does not load balance the traffic. Traffic from a source will use only one path, even if the traffic far outweighs traffic from other sources.

33. What is CGMP(cisco group management protocol)?

CGMP is a simple protocol, the routers are the only devices that are producing CGMP messages. The switches only listen to these messages and act upon it. CGMP uses a well-known destination **MAC address (0100.0cdd.dddd)** for all its messages. When switches receive frames with this destination address, they flood it on all their interfaces which so all switches in the network will receive CGMP messages.

Within a CGMP message, the two most important items are:

- Group Destination Address (GDA)
- Unicast Source Address (USA)

The group destination address is the multicast group MAC address, the unicast source address is the MAC address of the host (receiver).

34. What is Multicast?

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network. For more details please read Multicasting in computer network article.

35. What is the difference between Bluetooth and wifi?

S.NO	Bluetooth	Wifi
1.	Bluetooth has no full form.	While wifi stands for Wireless Fidelity.
2.	It requires bluetooth adapter on all devices for connectivity.	Whereas it requires a wireless adapter Bluetooth for all devices and a wireless router for connectivity.
3.	Bluetooth consumes low power.	while it consumes high power.
4.	The security of BlueTooth is less in comparison to the number of wifi.	While it provides better security than BlueTooth.
5.	Bluetooth is less flexible means these limited users are supported.	Whereas wifi supports large amount of users.
6.	The radio signal range of BlueTooth is ten meters.	Whereas in wifi this range is a hundred meters.
7.	Bluetooth requires low bandwidth.	While it requires high bandwidth.

36. What is a reverse proxy?

Reverse Proxy Server: The job of a reverse proxy server to listen to the request made by the client and redirect to the particular web server which is present on different servers. This is also used to restrict the access of the clients to the confidential data residing on the particular servers. For more details please refer what is proxy server article.

37. What is the role of address in packet traveling through a datagram network?

The address field in a datagram network is end-to-end addressing.

38. Can a routing table in the datagram network have two entries with the same destination address?

No. routing tables in the datagram network have two entries with the same destination address, not possible because the destination address or receiver address is unique in the datagram network.

39. What kind of arithmetic is used to add data items in checksum calculation?

To add data items in checksum calculations, one’s complement arithmetic is used.

40. Define piggybacking?

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

41. What are the advantages and disadvantages of piggybacking?

The major advantage of piggybacking is better use of available channel bandwidth.

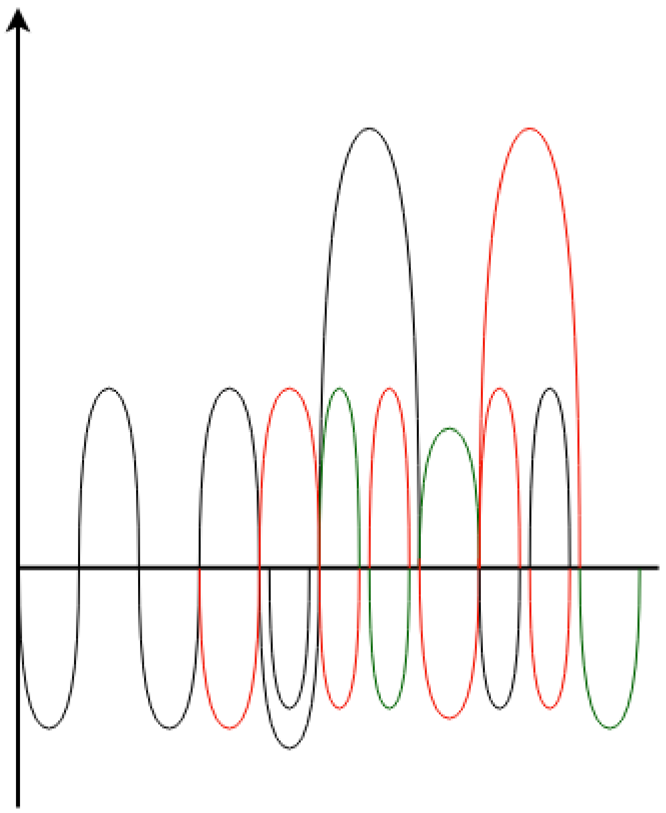
The major disadvantage of piggybacking is additional complexity and if the data link layer waits too long before transmitting the acknowledgment, then re-transmission of the frame would take place**.**

42. Which technique is used in byte-oriented protocols?

A byte stuffing is used in byte-oriented protocols. A special byte is added to the data section of the frame when there is a character with the same pattern as the flag.

43. Define the term OFDM?

Orthogonal Frequency Division Multiplexing (OFDM):
It is also the multiplexing technique that is used in an analog system. In OFDM, the Guard band is not required and the spectral efficiency of OFDM is high which oppose to the FDM. In OFDM, a Single data source attaches all the sub-channels.



OFDM

44. What is a transparent bridge?

Transparent Bridge:
A transparent bridge automatically maintains a routing table and updates tables in response to maintain changing topology. The transparent bridge mechanism consists of three mechanisms:

- Frame forwarding
- Address Learning
- Loop Resolution

The Transparent bridge is easy to use. Install the bridge and no software changes are needed in hosts. In all the cases, transparent bridges flooded the broadcast and multicast frames.

45. What is the minimum size of the icmpV4 packet what is the maximum size of the icmpv4 packet?

- Minimum size ICMPv4 packet = 28 bytes
- Maximum size ICMPv4 packet = 2068 bytes

46. Why do we OSPF a protocol that **is faster than our RIP?**

OSPF stands for Open Shortest Path First which uses a link-state routing algorithm. This protocol is faster than RIP because:

- Using the link-state information which is available in routers, it constructs the topology in which the topology determines the routing table for routing decisions.
- It supports both variable-length subnet masking and classless inter-domain routing addressing models.
- Since it uses Dijkstra's algorithm, it computes the shortest path tree for each route.
- OSPF (Open Shortest Path first) is handling the error detection by itself and it uses multicast addressing for routing in a broadcast domain

47. What are the two main categories of DNS messages?

The two categories of DNS messages are queries and replies.

48. Why do we need the **pop3 protocol for e-mail?**

Need of POP3:

The Post Office Protocol (POP3) is that the most widely used protocol and is being supported by most email clients. It provides a convenient and standard way for users to access mailboxes and download messages. An important advantage of this is that the mail messages get delivered to the client's PC and they can be read with or without accessing the web.

49. Define the term Jitter?

jitter is a "packet delay variance". It can simply mean that jitter is considered as a problem when different packets of data face different delays in a network and the data at the receiver application is time-sensitive, i.e. audio or video data. Jitter is measured in milliseconds(ms). It is defined as an interference in the normal order of sending data packets.

50. Why Bandwidth is an important to network performance parameter?

Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time. The term can be used in two different contexts with two distinctive estimating values. In the case of digital devices, the bandwidth is measured in bits per second(bps) or bytes per second. In the case of analog devices, the bandwidth is measured in cycles per second, or Hertz (Hz). Bandwidth is only one component of what an individual sees as the speed of a network. True internet speed is actually the amount of data you receive every second and that has a lot to do with latency too.

Q #1) What is a Network?

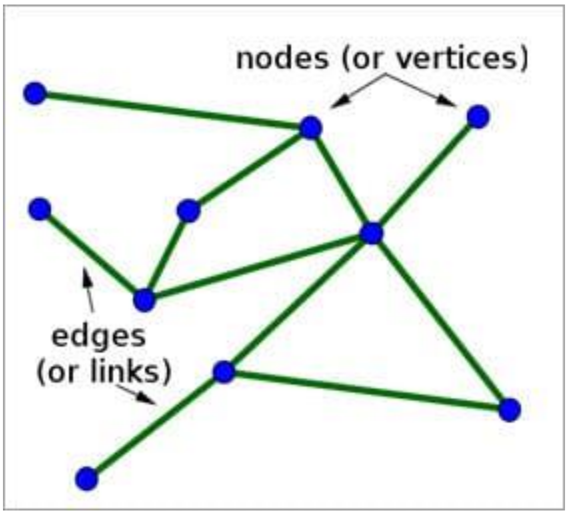
Answer: Network is defined as a set of devices connected to each other using a physical transmission medium.

For Example, A computer network is a group of computers connected with each other to communicate and share information and resources like hardware, data, and software. In a network, nodes are used to connect two or more networks.

Q #2) What is a Node?

Answer: Two or more computers are connected directly by an optical fiber or any other cable. A node is a point where a connection is established. It is a network component that is used to send, receive and forward the electronic information.

A device connected to a network is also termed as Node. Let's consider that in a network there are 2 computers, 2 printers, and a server are connected, then we can say that there are five nodes on the network.



[image source]

Q #3) What is Network Topology?

Answer: Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

Q #4) What are Routers?

Answer: The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.

Routers send the information in terms of data packets and when these data packets are forwarded from one router to another router then the router reads the network address in the packets and identifies the destination network.

Q #5) What is the OSI reference model?

Answer: Open **S**ystem **I**nterconnection, the name itself suggests that it is a reference model that defines how applications can communicate with each other over a networking system.

It also helps to understand the relationship between networks and defines the process of communication in a network.

Q #6) What are the layers in OSI Reference Models? Describe each layer briefly.

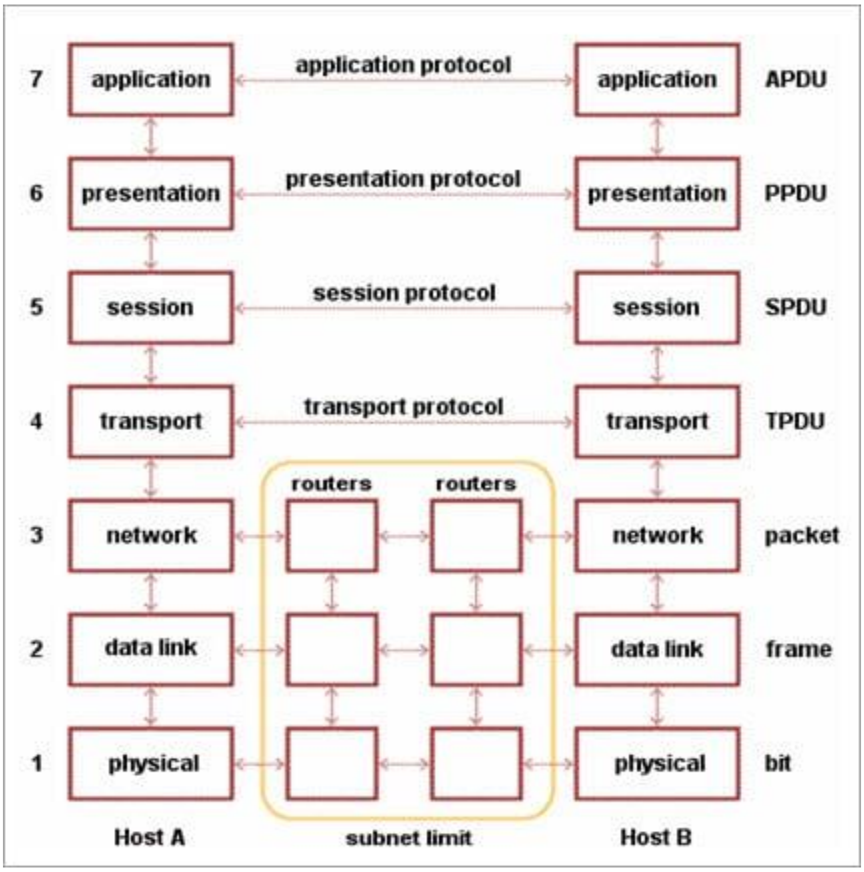
Answer: Given below are the seven layers of OSI Reference Models:

a) Physical Layer (Layer 1): It converts data bits into electrical impulses or radio signals. **Example:** Ethernet.

b) Data Link Layer (Layer 2): At the Data Link layer, data packets are encoded and decoded into bits and it provides a node to node data transfer. This layer also detects the errors that occurred at Layer 1.

c) Network Layer (Layer 3): This layer transfers variable length data sequence from one node to another node in the same network. This variable-length data sequence is also known as **"Datagrams"**.

d) Transport Layer (Layer 4): It transfers data between nodes and also provides acknowledgment of successful data transmission. It keeps track of transmission and sends the segments again if the transmission fails.



e) Session Layer (Layer 5): This layer manages and controls the connections between computers. It establishes, coordinates, exchange and terminates the connections between local and remote applications.

f) Presentation Layer (Layer 6): It is also called as "Syntax Layer". Layer 6 transforms the data into the form in which the application layer accepts.

g) Application Layer (Layer 7): This is the last layer of the OSI Reference Model and is the one that is close to the end-user. Both end-user and application layer interacts with the software application. This layer provides services for email, file transfer, etc.

Q #7) What is the difference between Hub, Switch, and Router?

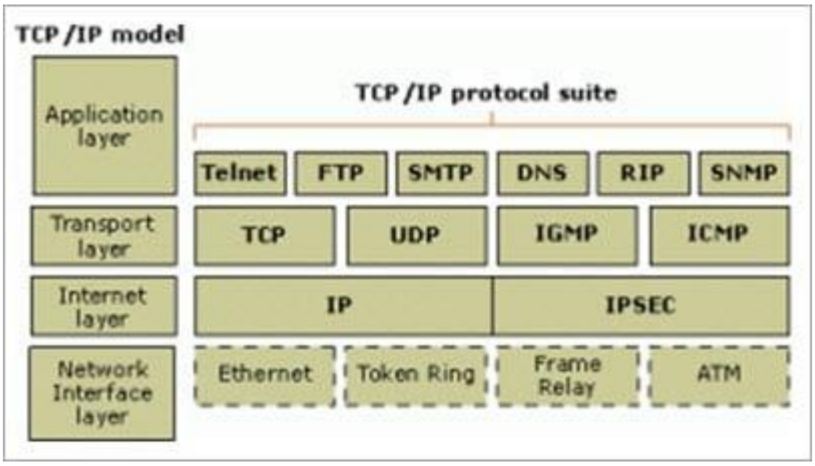
Answer:

Hub	**Switch**	**Router**
Hub is least expensive, least intelligent and least complicated of the three. It broadcast all data to every port which may cause serious security and reliability concern	Switches work similarly like Hubs but in a more efficient manner. It creates connections dynamically and provides information only to the requesting port	The router is smartest and most complicated out of these three. It comes in all shapes and sizes. Routers are similar like little computers dedicated for routing network traffic
In a Network, Hub is a common connection point for devices connected to the network. Hub contains multiple ports and is used to connect segments of LAN	Switch is a device in a network which forwards packets in a network	Routers are located at gateway and forwards data packets

Q #8) Explain TCP/IP Model

Answer: The most widely used and available protocol is TCP/IP i.e. Transmission Control Protocol and Internet Protocol. TCP/IP specifies how data should be packaged, transmitted and routed in their end to end data communication.

There are four layers as shown in the below diagram:



Given below is a brief explanation of each layer:

- **Application Layer**: This is the top layer in the TCP/IP model. It includes processes that use the Transport Layer Protocol to transmit the data to their destination. There are different Application Layer Protocols such as HTTP, FTP, SMTP, SNMP protocols, etc.
- **Transport Layer**: It receives the data from the Application Layer which is above the Transport Layer. It acts as a backbone between the host's system connected with each other and it mainly concerns about the transmission of data. TCP and UDP are mainly used as Transport Layer protocols.
- **Network or Internet Layer**: This layer sends the packets across the network. Packets mainly contain source & destination IP addresses and actual data to be transmitted.
- **Network Interface Layer**: It is the lowest layer of the TCP/IP model. It transfers the packets between different hosts. It includes encapsulation of IP packets into frames, mapping IP addresses to physical hardware devices, etc.

Q #9) What is HTTP and what port does it use?

Answer: HTTP is HyperText Transfer Protocol and it is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is the primary protocol and port used here is TCP port 80.

Q #10) What is HTTPs and what port does it use?

Answer: HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks.

In bi-directional communication, the HTTPs protocol encrypts the communication so that the tampering of the data gets avoided. With the help of an SSL certificate, it verifies if the requested server connection is a valid connection or not. HTTPs use TCP with port 443.

Q #11) What are TCP and UDP?

Answer: Common factors in TCP and UDP are:

- TCP and UDP are the most widely used protocols that are built on the top of the IP protocol.
- Both protocols TCP and UDP are used to send bits of data over the Internet, which is also known as 'packets'.
- When packets are transferred using either TCP or UDP, it is sent to an IP address. These packets are traversed through routers to the destination.

The difference between TCP and UDP are enlisted in the below table:

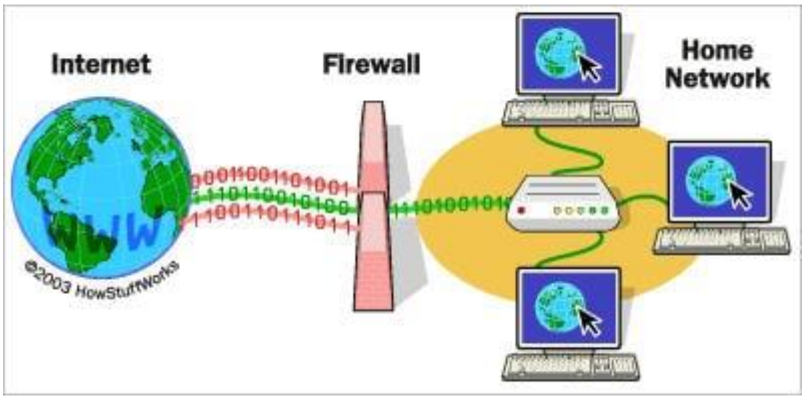
TCP	**UDP**
TCP stands for Transmission Control Protocol	UDP is stands for User Datagram Protocol or Universal Datagram Protocol
Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol	UDP is connectionless, simple protocol. Using UDP, messages are sent 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 transmission occurs in a sequential manner	UDP transmission also occurs in a sequential manner but it does not maintain the same sequence when it reaches the destination
It is heavy weight connection	It is lightweight transport layer
TCP tracks the data sent to ensure no data loss during data transmission	UDP does not ensure whether receiver receives

TCP	UDP
	packets are not. If packets are misses then they are just lost

Q #12) What is a Firewall?

Answer: Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked.



Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features. “

Windows Firewall” is an inbuilt Microsoft Windows application that comes along with the operating system. This “Windows Firewall” also helps to prevent viruses, worms, etc.

Q #13) What is DNS?

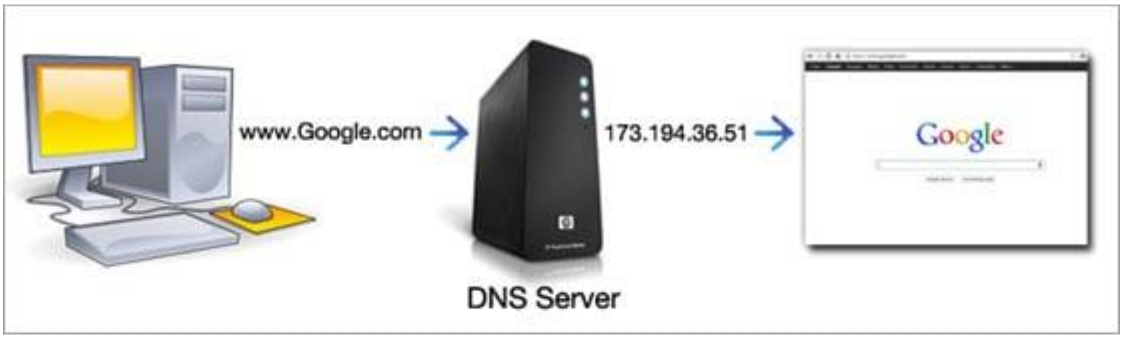
Answer: Domain Name Server (DNS), in a non-professional language and we can call it an Internet’s phone book. All the public IP addresses and their hostnames are stored in the DNS and later it translates into a corresponding IP address.

For a human being, it is easy to remember and recognize the domain name, however, the computer is a machine that does not understand the human language and they only understand the language of IP addresses for data transfer.

There is a “Central Registry” where all the domain names are stored and it gets updated on a periodic basis. All Internet service providers and different host companies usually interact with this central registry to get the updated DNS details.

For Example, When you type a website www.softwaretestinghelp.com, then your Internet service provider looks for the DNS associated with this domain name and translates this website command into a machine language – IP address – 151.144.210.59 (note that, this is the imaginary IP address and not the actual IP for the given website) so that you will get redirected to the appropriate destination.

This process is explained in the below diagram:



Q #14) What is the difference between a Domain and a Workgroup?

Answer: In a computer network, different computers are organized in different methods and these methods are – Domains and Workgroups. Usually, computers which run on the home network belong to a Workgroup.

However, computers that are running on an office network or any workplace network belong to the Domain.

Their differences are as follows:

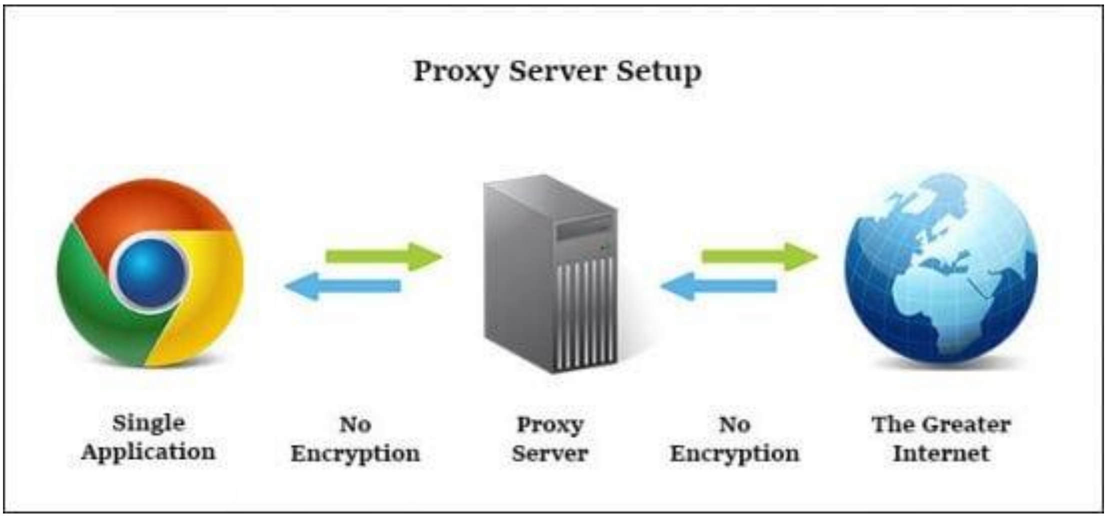
Workgroup	Domain
All computers are peers and no computer has control over another computer	Network admin uses one or more computer as a server and provide all accesses, security permission to all other computers in a network
In a Workgroup, each computer maintains their own database	The domain is a form of a computer network in which computers, printers, and user accounts are registered in a central database.
Each computer has their own authentication rule for every user account	It has centralized authentication servers which set authentication

Workgroup	Domain
Each computer has set of user account. If user has account on that computer then only user able to access the computer	If user has an account in a domain then user can login to any computer in a domain
Workgroup does not bind to any security permission or does not require any password	Domain user has to provide security credentials whenever they are accessing the domain network
Computer settings need to change manually for each computer in a Workgroup	In a domain, changes made in one computer automatically made same changes to all other com network
All computers must be on same local area network	In a domain, computers can be on a different local network
In a Workgroup, there can be only 20 computers connected	In a domain, thousands of computers can be connected

Q #15) What is a Proxy Server and how do they protect the computer network?

Answer: For data transmission, IP addresses are required and even DNS uses IP addresses to route to the correct website. It means without the knowledge of correct and actual IP addresses it is not possible to identify the physical location of the network.

Proxy servers prevent external users who are unauthorized to access such IP addresses of the internal network. It makes the computer network virtually invisible to external users.



Proxy Server also maintains the list of blacklisted websites so that the internal user is automatically prevented from getting easily infected by viruses, worms, etc.

Q #16) What are IP classes and how can you identify the IP class of given an IP address?

Answer: An IP address has 4 sets (octets) of numbers each with a value up to 255.

For Example, the range of the home or commercial connection started primarily between 190 x or 10 x. IP classes are differentiated based on the number of hosts it supports on a single network. If IP classes support more networks then very few IP addresses are available for each network.

There are three types of IP classes and are based on the first octet of IP addresses which are classified as Class A, B or C. If the first octet begins with 0 bit then it is of type Class A.

Class A type has a range up to 127.x.x.x (except 127.0.0.1). If it starts with bits 10 then it belongs to Class B. Class B having a range from 128.x to 191.x. IP class belongs to Class C if the octet starts with bits 110. Class C has a range from 192.x to 223.x.

Q #17) What is meant by 127.0.0.1 and localhost?

Answer: IP address 127.0.0.1, is reserved for loopback or localhost connections. These networks are usually reserved for the biggest customers or some of the original members of the Internet. To identify any connection issue, the initial step is to ping the server and check if it is responding.

If there is no response from the server then there are various causes like the network is down or the cable needs to be replaced or the network card is not in good condition. 127.0.0.1 is a loopback connection on the Network Interface Card (NIC) and if you are able to ping this server successfully, then it means that the hardware is in a good shape and condition.

127.0.0.1 and localhost are the same things in most of the computer network functioning.

Q #18) What is NIC?

Answer: NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.

Each NIC has a MAC address which helps in identifying the computer on a network.

Q #19) What is Data Encapsulation?

Answer: In a computer network, to enable data transmission from one computer to another, the network devices send messages in the form of packets. These packets are then added with the IP header by the OSI reference model layer.

The Data Link Layer encapsulates each packet in a frame that contains the hardware address of the source and the destination computer. If a destination computer is on the remote network then the frames are routed through a gateway or router to the destination computer.

Q #20) What is the difference between the Internet, Intranet, and Extranet?

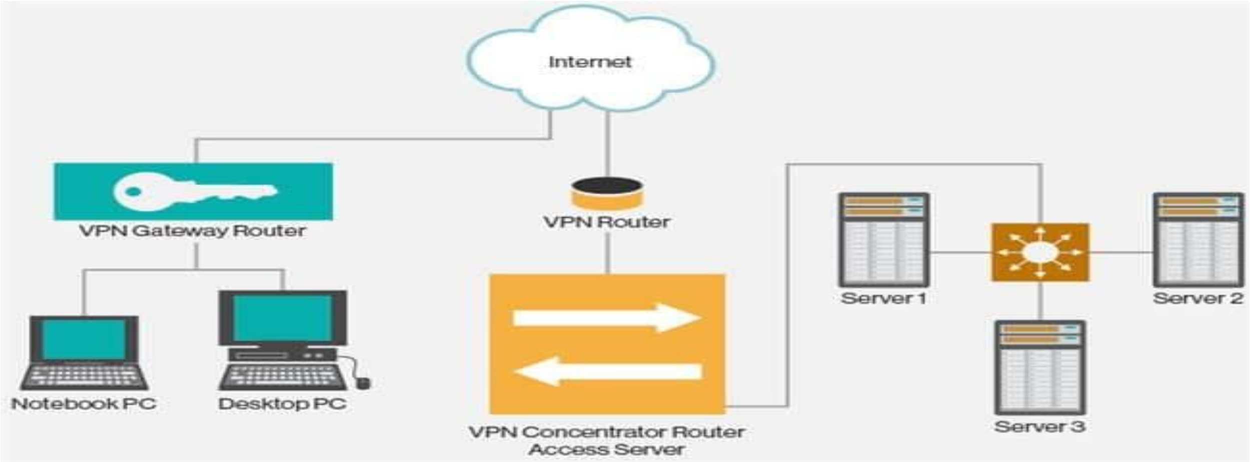
Answer: The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

- **Internet**: Applications are accessed by anyone from any location using the web.
- **Intranet**: It allows limited access to users in the same organization.
- **Extranet**: External users are allowed or provided with access to use the network application of the organization.

Q #21) What is a VPN?

Answer: VPN is the Virtual Private Network and is built on the Internet as a private wide area network. Internet-based VPNs are less expensive and can be connected from anywhere in the world.

VPNs are used to connect offices remotely and are less expensive when compared to WAN connections. VPNs are used for secure transactions and confidential data can be transferred between multiple offices. VPN keeps company information secure against any potential intrusion.



Given below are the 3 types of VPN's:

1. **Access VPN**: Access VPN's provide connectivity to mobile users and telecommuters. It is an alternative option for dial-up connections or ISDN connections. It provides low-cost solutions and a wide range of connectivity.
2. **Intranet VPN**: They are useful for connecting remote offices using shared infrastructure with the same policy as a private network.
3. **Extranet VPN**: Using shared infrastructure over an intranet, suppliers, customers, and partners are connected using dedicated connections.

Q #22) What are Ipconfig and Ifconfig?

Answer: Ipconfig stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.

The command Ipconfig is useful for displaying all TCP/IP network summary information currently available on a network. It also helps to modify the DHCP protocol and DNS setting.

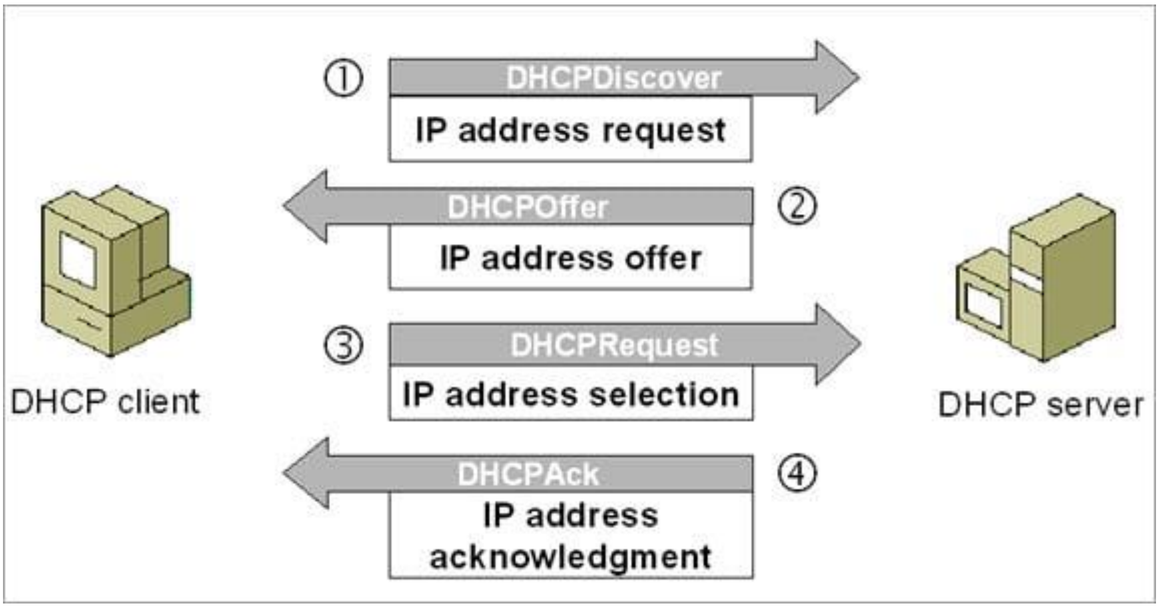
Ifconfig (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It is used to configure, control the TCP/IP network interface parameters from CLI i.e. Command Line Interface. It allows you to see the IP addresses of these network interfaces.

Q #23) Explain DHCP briefly?

Answer: DHCP stands for Dynamic Host Configuration Protocol and it automatically assigns IP addresses to the network devices. It completely removes the process of manual allocation of IP addresses and reduces the errors caused due to this.

This entire process is centralized so that the TCP/IP configuration can also be completed from a central location. DHCP has a "pool of IP addresses" from which it allocates the IP address to the network devices. DHCP cannot recognize if any device is configured manually and assigned with the same IP address from the DHCP pool.

In this situation, it throws the “IP address conflict” error.



DHCP environment requires DHCP servers to set-up the TCP/IP configuration. These servers then assign, release and renew the IP addresses as there might be a chance that network devices can leave the network and some of them can join back to the network.

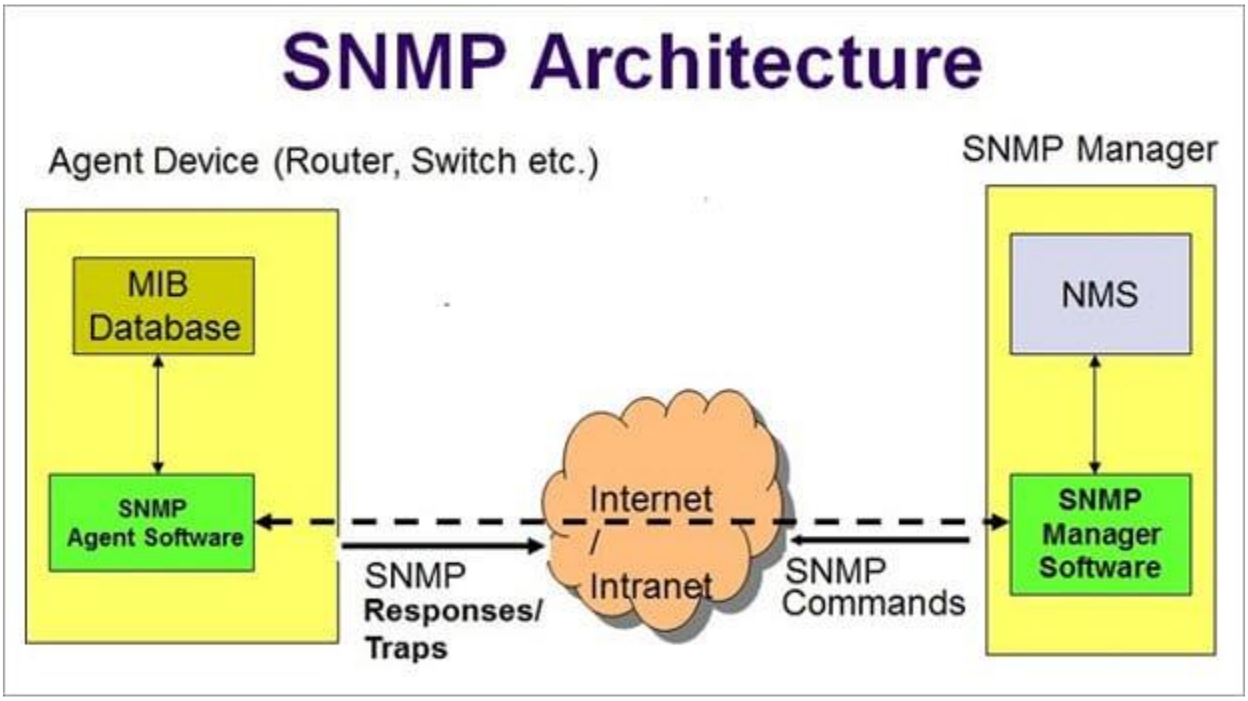
Q #24) What is SNMP?

Answer: SNMP stands for Simple Network Management Protocol. It is a network protocol used for collecting organizing and exchanging information between network devices. SNMP is widely used in network management for configuring network devices like switches, hubs, routers, printers, servers.

SNMP consists of the below components:

- SNMP Manager
- Managed device
- SNMP Agent
- Management Information Base (MIB)

The below diagram shows how these components are connected with each other in the SNMP architecture:



[image source]

SNMP is a part of the TCP/IP suite. There are 3 main versions of SNMP which include SNMPv1, SNMPv2, and SNMPv3.

Q #25) What are the different types of a network? Explain each briefly.

Answer: There are 4 major types of networks.

Let’s take a look at each of them in detail.

1. **Personal Area Network (PAN)**: It is the smallest and basic network type that is often used at home. It is a connection between the computer and another device such as phone, printer, modem tablets, etc
2. **Local Area Network (LAN)**: LAN is used in small offices and Internet cafes to connect a small group of computers to each other. Usually, they are used to transfer a file or for playing the game in a network.
3. **Metropolitan Area Network (MAN):** It is a powerful network type than LAN. The area covered by MAN is a small town, city, etc. A huge server is used to cover such a large span of area for connection.
4. **Wide Area Network (WAN)**: It is more complex than LAN and covers a large span of the area typically a large physical distance. The Internet is the largest WAN which is spread across the world. WAN is not owned by any single organization but it has distributed ownership.

There are some other types of the network as well:

- Storage Area Network (SAN)
- System Area Network (SAN)

- Enterprise Private Network (EPN)
- Passive Optical Local Area Network (POLAN)
-

Part 2: Networking Questions Series

Q #26) Differentiate Communication and Transmission?

Answer: Through Transmission the data gets transferred from source to destination (only one way). It is treated as the physical movement of data.

Communication means the process of sending and receiving data between two media (data is transferred between source and destination in both ways).

Q #27) Describe the layers of the OSI model?

Answer: OSI model stands for Open System Interconnection It is a framework that guides the applications on how they can communicate in a network.

OSI model has seven layers. They are listed below,

1. **Physical Layer**: Deals with transmission and reception of unstructured data through a physical medium.
2. **Data Link Layer:** Helps in transferring error-free data frames between nodes.
3. **Network Layer:** Decides the physical path that should be taken by the data as per the network conditions.
4. **Transport Layer:** Ensures that the messages are delivered in sequence and without any loss or duplication.
5. **Session Layer:** Helps in establishing a session between processes of different stations.
6. **Presentation Layer:** Formats the data as per the need and presents the same to the Application layer.
7. **Application Layer:** Serves as the mediator between Users and processes of applications.

Q #28) Explain various types of networks based on their sizes?

Answer: The size of the network is defined as the geographic area and the number of computers covered in it. **Based on the size of the network they are classified as below:**

1. **Local Area Network (LAN):** A network with a minimum of two computers to a maximum of thousands of computers within an office or a building is termed as LAN. Generally, it works for a single site where people can share resources like printers, data storage, etc.

2. **Metropolitan Area Network (MAN):** It is larger than LAN and used to connect various LANs across small regions, a city, campus of colleges or universities, etc which in turn forms a bigger network.
3. **Wide Area Network (WAN):** Multiple LANs and MAN's connected together form a WAN. It covers a wider area like a whole country or world.

Q #29) Define various types of Internet connections?

Answer: There are three types of Internet connections. They are listed below:

1. **Broadband Connection:** This type of connection gives continuous high-speed Internet. In this type, if we log off from the Internet for any reason then there is no need to log in again. **For Example,** Modems of cables, Fibres, wireless connection, satellite connection, etc.
2. **Wi-Fi:** It is a wireless Internet connection between the devices. It uses radio waves to connect to the devices or gadgets.
3. **WiMAX:** It is the most advanced type of Internet connection which is more featured than Wi-Fi. It is nothing but a high-speed and advanced type of broadband connection.

Q #30) A few important terminologies we come across networking concepts?

Answer: Below are a few important terms we need to know in networking:

- **Network:** A set of computers or devices connected together with a communication path to share data.
- **Networking:** The design and construction of a network are termed as networking.
- **Link:** The physical medium or the communication path through which the devices are connected in a network is called a Link.
- **Node:** The devices or the computers connected to the links are named as nodes.
- **Router/Gateway:** A device/computer/node that is connected to different networks is termed as a Gateway or Router. The basic difference between these two is that Gateway is used to control the traffic of two contradictory networks whereas the router controls the traffic of similar networks.
- **The router** is a switch that processes the signal/traffic using routing protocols.
- **Protocol:** A set of instructions or rules or guidelines that are used in establishing communications between computers of a network is called Protocol.

- **Unicasting:** When a piece of information or a packet is sent from a particular source to a specified destination then it is called Unicasting.
- **Anycasting:** Sending the datagrams from a source to the nearest device among the group of servers that provide the same service as the source is termed as Anycasting.
- **Multicasting:** Sending one copy of data from a single sender to multiple clients or receivers (selected clients) of the networks which are in need of such data.
- **Broadcasting:** Sending a packet to each device of the network is termed as broadcasting.

Q #31) Explain the characteristics of networking?

Answer: The main characteristics of networking are mentioned below:

- **Topology:** This deals with how the computers or nodes are arranged in the network. The computers are arranged physically or logically.
- **Protocols:** Deals with the process of how computers communicate with one another.
- **Medium:** This is nothing but the medium used by computers for communication.

Q #32) How many types of modes are used in data transferring through networks?

Answer: Data transferring modes in computer networks are of three types. They are listed below,

1. **Simplex:** Data transferring which takes place only in one direction is called Simplex. In Simplex mode, the data gets transferred either from sender to receiver or from receiver to sender. **For Example,** Radio signal, the print signal given from computer to printer, etc.
2. **Half Duplex:** Data transferring can happen in both directions but not at the same time. Alternatively, the data is sent and received. **For Example,** Browsing through the internet, a user sends the request to the server and later the server processes the request and sends back the web page.
3. **Full Duplex:** Data transferring happens in both directions that too simultaneously. **For Example,** Two-lane roads where traffic flows in both directions, communication through telephone, etc.

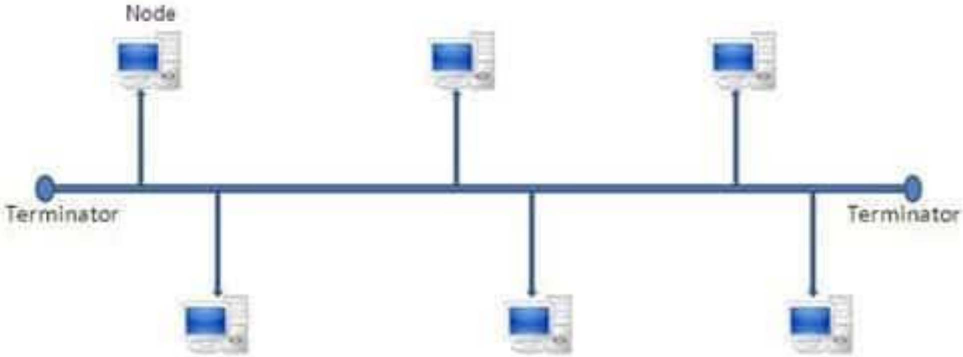
Q #33) Name the different types of network topologies and brief their advantages?

Answer: Network Topology is nothing but the physical or logical way in which the devices (like nodes, links, and computers) of a network are arranged. Physical Topology means the actual place where the elements of a network are located.

Logical Topology deals with the flow of data over the networks. A link is used to connect more than two devices of a network. And more than two links located nearby form a topology.

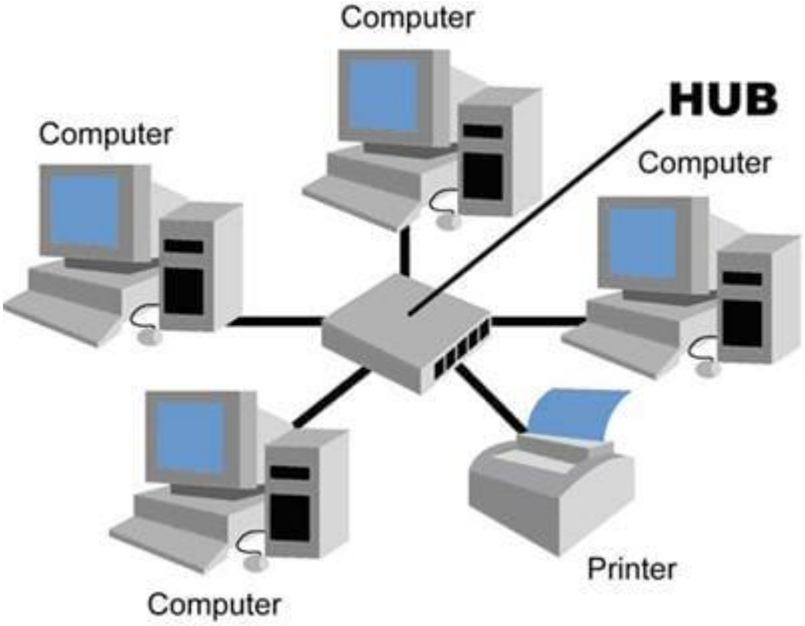
Network topologies are classified as below:

a) Bus Topology: In Bus Topology, all the devices of the network are connected to a common cable (also called as the backbone). As the devices are connected to a single cable, it is also termed as Linear Bus Topology.



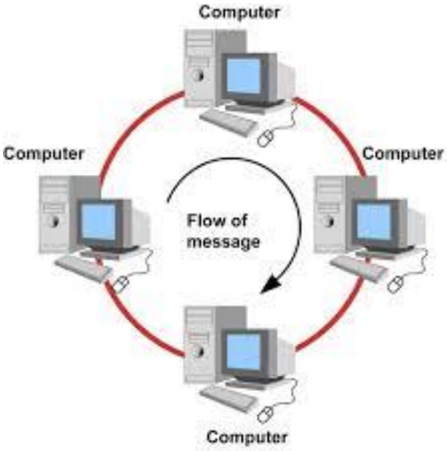
The advantage of bus topology is that it can be installed easily. And the disadvantage is that if the backbone cable breaks then the whole network will be down.

b) Star Topology: In Star Topology, there is a central controller or hub to which every node or device is connected through a cable. In this topology, the devices are not linked to each other. If a device needs to communicate with the other, then it has to send the signal or data to the central hub. And then the hub sends the same data to the destination device.



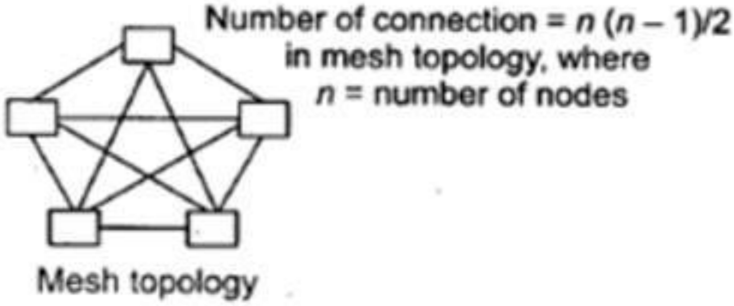
The advantage of the star topology is that if a link breaks then only that particular link is affected. The whole network remains undisturbed. The main disadvantage of the star topology is that all the devices of the network are dependent on a single point (hub). If the central hub gets failed, then the whole network gets down.

c) Ring Topology: In Ring Topology, each device of the network is connected to two other devices on either side which in turn forms a loop. Data or Signal in ring topology flow only in a single direction from one device to another and reaches the destination node.



The advantage of ring topology is that it can be installed easily. Adding or deleting devices to the network is also easy. The main disadvantage of ring topology is the data flows only in one direction. And a break at a node in the network can affect the whole network.

d) Mesh Topology: In a Mesh Topology, each device of the network is connected to all other devices of the network. Mesh Topology uses Routing and Flooding techniques for data transmission.


Number of connection = n (n – 1)/2 in mesh topology, where n = number of nodes
Mesh topology

The advantage of mesh topology is if one link breaks then it does not affect the whole network. And the disadvantage is, huge cabling is required and it is expensive.

Q #34) What is the full form of IDEA?

Answer: IDEA stands for International Data Encryption Algorithm.

Q #35) Define Piggybacking?

Answer: In data transmission, if the sender sends any data frame to the receiver then the receiver should send the acknowledgment to the sender. The receiver will temporarily delay (waits for the network layer to send the next data packet) the acknowledgment and hooks it to the next outgoing data frame, this process is called Piggybacking.

Q #36) In how many ways the data is represented and what are they?

Answer: Data transmitted through the networks' comes in different ways like text, audio, video, images, numbers, etc.

- **Audio:** It is nothing but the continuous sound which is different from text and numbers.
- **Video:** Continuous visual images or a combination of images.
- **Images:** Every image is divided into pixels. And the pixels are represented using bits. Pixels may vary in size based on image resolution.
- **Numbers:** These are converted into binary numbers and are represented using bits.
- **Text:** Text is also represented as bits.

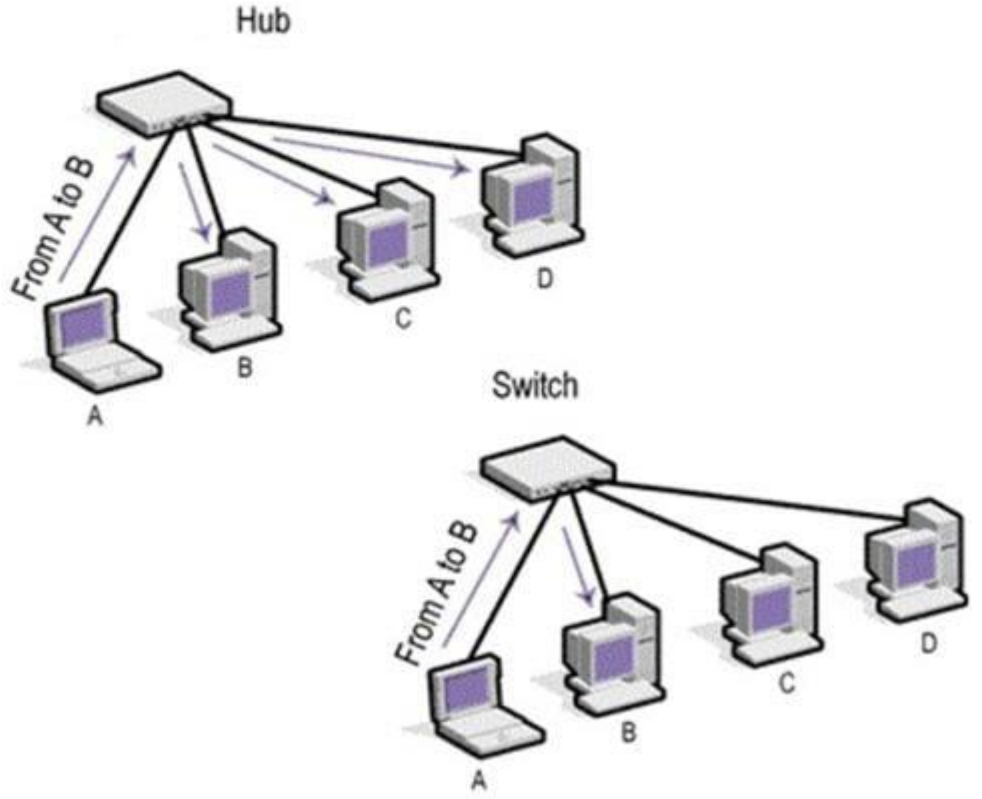
Q #37) What is the full form of ASCII?

Answer: ASCII stands for American Standard Code for Information Interchange.

Q #38) How a Switch is different from a Hub?

Answer: Below are the differences between a Switch and a Hub,

Below given snapshot clearly explains the difference:



Q #39) Define Round Trip Time?

Answer: The time taken for a signal to reach the destination and travel back to the sender with the acknowledgment is termed as Round Trip Time (RTT). It is also called Round Trip Delay (RTD).

Q #40) Define Brouter?

Answer: Brouter or Bridge Router is a device that acts as both a bridge and a router. As a bridge, it forwards data between the networks. And as a router, it routes the data to specified systems within a network.

Q #41) Define Static IP and Dynamic IP?

Answer: When a device or computer is assigned a specified IP address then it is named as Static IP. It is assigned by the Internet Service Provider as a permanent address.

Dynamic IP is the temporary IP address assigned by the network to a computing device. Dynamic IP is automatically assigned by the server to the network device.

Q #42) How VPN is used in the corporate world?

Answer: VPN stands for Virtual Private Network. With the help of a VPN, remote users can securely connect to the organization’s network. Corporate companies, educational institutions, government offices, etc use this VPN.

Q #43) What is the difference between Firewall and Antivirus?

Answer: Firewall and Antivirus are two different security applications used in networking. A firewall acts as a gatekeeper which prevents unauthorized users to access the private networks as intranets. A firewall examines each message and blocks the same which are unsecured.

Antivirus is a software program that protects a computer from any malicious software, any virus, spyware, adware, etc.

Note: A Firewall cannot protect the system from viruses, spyware, adware, etc.

Q #44) Explain Beaconing?

Answer: If a network self-repair its problem then it is termed as Beaconing. Mainly, it is used in the token ring and FDDI (Fiber Distributed Data Interface) networks. If a device in the network is facing any problem, then it notifies the other devices that they are not receiving any signal. Likewise, the problem gets repaired within the network.

Q #45) Why the standard of an OSI model is termed as 802.xx?

Answer: The OSI model was started in the month of February in 1980. So it is standardized as 802.XX. This ‘80’ stands for the year 1980 and ‘2’ represents the month of February.

Q #46) Expand DHCP and describe how it works?

Answer: DHCP stands for Dynamic Host Configuration Protocol.

DHCP is used to assign IP addresses automatically to the devices over the network. When a new device is added to the network, it broadcasts a message stating that it is new to the network. Then the message is transmitted to all the devices of the network.

Only the DHCP server will react to the message and assigns a new IP address to the newly added device of the network. With the help of DHCP, IP management became very easy.

Q #47) How can a network be certified as an effective network? What are the factors affecting them?

Answer: A network can be certified as an effective network based on below-mentioned factors:

- **Performance:** A network’s performance is based on its transmitted time and response time. The factors affecting the performance of a network are hardware, software, transmission medium types and the number of users using the network.
- **Reliability:** Reliability is nothing but measuring the probability of failures occurred in a network and the time taken by it to recover from it. The factors affecting the same are the frequency of failure and recovery time from failure.

- **Security:** Protecting the data from viruses and unauthorized users. The factors affecting the security are viruses and users who do not have permission to access the network.

Q #48) Explain DNS?

Answer: DNS stands for Domain Naming Server. DNS acts as a translator between domain names and IP addresses. As humans remember names, the computer understands only numbers. Generally, we assign names to websites and computers like Gmail.com, Hotmail, etc. When we type such names the DNS translates it into numbers and executes our requests.

Translating the names into numbers or IP address is named as a Forward lookup.

Translating the IP address to names is named as a Reverse lookup.

Q #49) Define IEEE in the networking world?

Answer: IEEE stands for the Institute of Electrical and Electronic Engineer. This is used to design or develop standards that are used for networking.

Q #50) What is the use of encryption and decryption?

Answer: Encryption is the process of converting the transmission data into another form that is not read by any other device other than the intended receiver.

Decryption is the process of converting back the encrypted data to its normal form. An algorithm called cipher is used in this conversion process.

Q #51) Brief Ethernet?

Answer: Ethernet is a technology that is used to connect computers all over the network to transmit the data between each other.

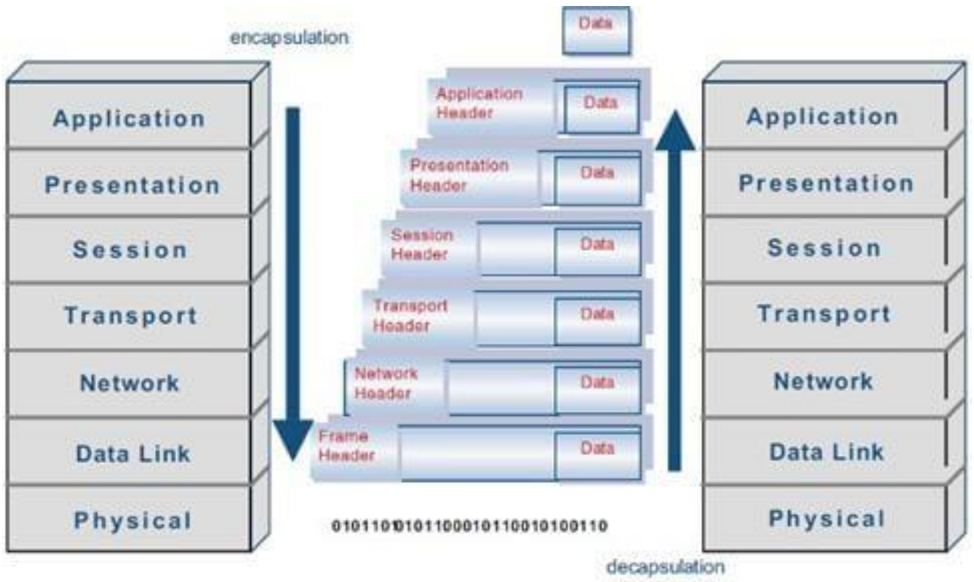
For Example, if we connect a computer and laptop to a printer, then we can call it as an Ethernet network. Ethernet acts as the carrier for the Internet within short distance networks like a network in a building.

The main difference between the Internet and Ethernet is security. Ethernet is safer than the Internet as Ethernet is a closed-loop and has only limited access.

Q #52) Explain Data Encapsulation?

Answer: Encapsulation means adding one thing on top of the other thing. When a message or a packet is passed through the communication network (OSI layers), every layer adds its header information to the actual packet. This process is termed as Data Encapsulation.

Note: Decapsulation is exactly the opposite of encapsulation. The process of removing the headers added by the OSI layers from the actual packet is termed as Decapsulation.



Q #53) How are networks classified based on their connections?

Answer: Networks are classified into two categories based on their connection types. **They are mentioned below:**

- **Peer-to-peer networks (P2P):** When two or more computers are connected together to share resources without the use of a central server is termed as a peer-to-peer network. Computers in this type of network act as both server and client. It is generally used in small companies as they are not expensive.
- **Server-based networks:** In this type of network, a central server is located to store the data, applications, etc of the clients. The server computer provides the security and network administration to the network.

Q #54) Define Pipelining?

Answer: In Networking, when a task is in progress another task gets started before the previous task is finished. This is termed as Pipelining.

Q #55) What is an Encoder?

Answer: Encoder is a circuit that uses an algorithm to convert any data or compress audio data or video data for transmission purposes. An encoder converts the analog signal into the digital signal.

Q #56) What is a Decoder?

Answer: Decoder is a circuit that converts the encoded data to its actual format. It converts the digital signal into an analog signal.

Q #57) How can you recover the data from a system which is infected with a Virus?

Answer: In another system (not infected with a virus) install an OS and antivirus with the latest updates. Then connect the HDD of the infected system as a secondary drive. Now scan the secondary HDD and clean it. Then copy the data into the system.

Q #58) Describe the key elements of the protocol?

Answer: Below are the 3 key elements of the protocol:

- **Syntax:** It is the format of the data. That means in which order the data is displayed.
- **Semantics:** Describes the meaning of the bits in each section.
- **Timing:** At what time the data is to be sent and how fast it is to be sent.

Q #59) Explain the difference between baseband and broadband transmission?

Answer:

- **Baseband Transmission:** A single signal consumes the whole bandwidth of the cable.
- **Broadband Transmission:** Multiple signals of multiple frequencies are sent simultaneously.

Q #60) Expand SLIP?

Answer: SLIP stands for Serial Line Interface Protocol. SLIP is a protocol used for transmitting IP datagrams over a serial line.

Q1. Differentiate between a router, a hub, and a switch.

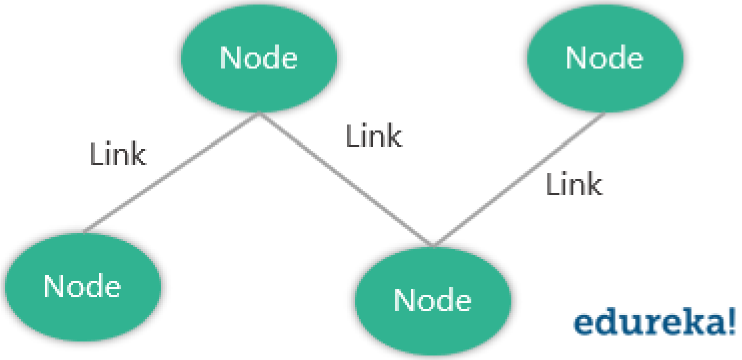
HUB	SWITCH	ROUTER
Connects two or more Ethernet devices	Connects two or more LAN devices	Can connect devices or a LAN and WAN
Does not perform filtering	Filters packets before forwarding them	Highly configured to filter and send packets
Least intelligent, least expensive and least complex	Similar to a hub, but more effective	Extremely smart and complex

Q2. What is a link?

A link basically is the connection between two or more computers or devices. It can be anything depending on whether it is a physical connection or a wireless one. Physical links include cables, hubs, switches, etc and wireless links wireless access points, routers, etc.

Q3. What do you mean by a Node?

The point of intersection in a network is called a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in case there are computers, there will be three nodes and so on. It is not necessary for a node to be a computer, it can be any communicating device such as a printer, servers, modems, etc.



Q4. What does a backbone network mean?

In any system, backbone is the most principle component that supports all other components. Similarly, in networking, a Backbone Network is a Network that interconnects various parts of the network to which it belongs and has a high capacity connectivity infrastructure.

Q5. What is Network Topology?

The physical layout of the computer network is called as Network Topology. It gives the design of how all the devices are connected in a network.

Type	Description
Bus Topology	All the devices share a common communication line

Star Topology	All nodes are connected to a central hub device
Ring Topology	Each node connects to exactly two other nodes
Mesh Topology	Each node is connected to one or more nodes
Tree Topology (Hierarchical Topology)	Similar to star topology and inherits the bus topology
Daisy Chain Topology	All nodes are connected linearly
Hybrid Topology	Nodes are connected in more than one topology styles
Point-to-Point Topology	Connects two hosts such as computers, servers, etc

Q6. Explain what is LAN?

A LAN or Local Area Network the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:

- Topology: The arrangement of nodes within the network
- Protocol: Refer to the rules for the transfer of data
- Media: These devices can be connected using optic fibers, twisted-pair wires, etc

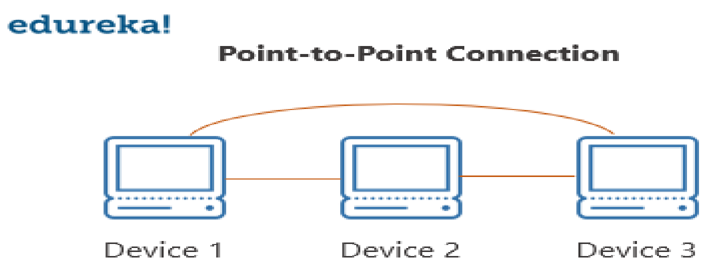
Q7. What are Routers?

A router is some device that transfers the data packets within a network. It basically performs the traffic directing functions within a network. A data packet can be anything such as an email, a web page, etc. Routers are located at the place where two or more networks meet or the gateways.

Routers can either be stand-alone devices or virtual. Stand-alone routers are traditional devices where as virtual routers are actually softwares that act like physical ones.

Q8. What is a Point-to-Point Network?

A Point-to-Point network refers to a physical connection between two nodes. It can be between any device of a network such as a computer, printer, etc.

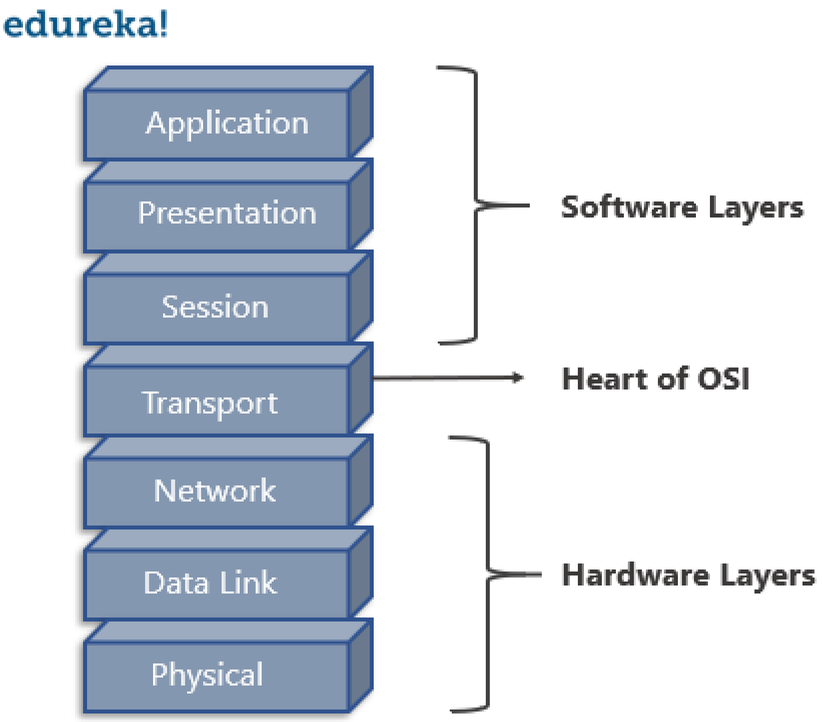


For example, as you can see in the above diagram, all the nodes are connected to each other i.e Device 1 is connected to Device 2 and Device 3 , Device 2 is connected to Device 3 and Device 1 and Device 3 is connected to Device 2 and Device 1 using physical links.

Q9. What is OSI Model?

OSI stands for Open Systems Interconnection. It is a conceptual model that standardizes communication functions of telecommunication. It has 7 layers which are:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Q10. Give a brief about each layer in the OSI Model.

Layer Name	Protocol	Description
Physical Layer	Symbol	Transfers raw bits of data over a physical link
Data Link Layer	Frame	Reliable transmission of data frames between nodes connected by the physical layer
Network Layer	Packet	Structures and manages a network with multiple nodes including addressing, routing and traffic control
Transport Layer	Segment, Datagram	Reliable Transmission of data packets between the different points of a network
Session Layer	Data	Manages the communication sessions

Presentation Layer	Data	Transmission of data between the service device and the application
Application Layer	Data	Specifies the shared communication protocols and the interface methods

To learn about Network Programming in Java and Python in detail refer to the following blogs:

- Socket Programming in Java
- Socket Programming in Python

Q11. What do you mean by anonymous FTP?

An anonymous FTP is a way of allowing a user to access data that is public. The user does not need to identify himself to the server and has to log in as anonymous.

So in case you are asked to use anonymous ftp, make sure you add “anonymous” in place of your user id. Anonymous FTPs are very effective while distributing large files to a lot of people, without having to give huge numbers of usernames and password combinations.

Q12. What is the meaning of Network?

A network is a connection between different devices. These devices communicate with each other using physical or wireless connections. Physical connections include twisted pair cables, optic fibers, and coaxial cables..wireless networks can be established with the help of waves such as radio waves infrared waves and microwaves Networks basically serve many purposes such as:

- Sharing hardware devices such as printers, input devices, etc
- Help in communications in many ways such as audios videos emails messages etc
- Help in sharing data and information using virtual devices
- They also help sharing softwares that are installed on other devices

Q13. What do you mean by a Subnet Mask?

A Subnet Mask is the number describing the range of IP addresses that can be used within a network. They are used to assign subnetworks or subnets. These subnetworks are various LAN’s connected to the internet.

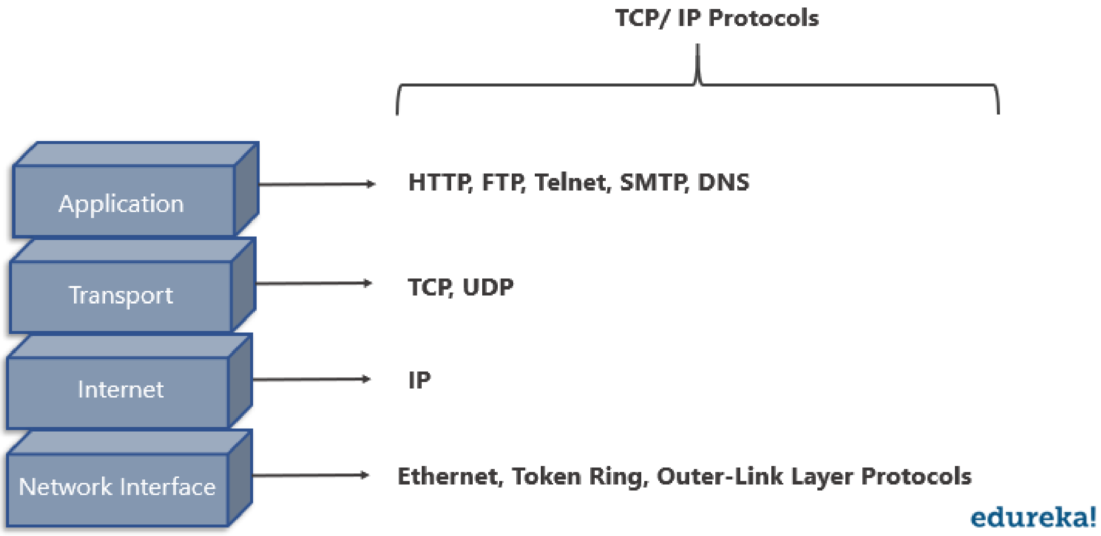
This Subnet mask is basically a 32-bit number and it masks the IP address and then divides the IP address into two parts i.e the network address and the host address. Subnet Masks are created by setting all the network bits to “1” and all the host bits to “0”s. There are two network addresses that cannot be assigned to any host on the network i.e

The “0” and “255” which are assigned to network and to the broadcast address, and this is why they cannot be assigned to any host.

Q14. Give a brief description of the TCP/ IP Model.

The TCP/ IP Model is a compressed version of the OSI Model. This Model contains 4 layers unlike the OSI Model which are:

1. Process(Application Layer)
2. Host-to-Host(Transport Layer)
3. Internet Layer (Network Layer)
4. Network Access(Combination of Physical and Data Link Layer)



Q15. What is the difference between the OSI Model and TCP/ IP Model?

TCP/ IP Model	OSI Model
Has four layers	Has seven layers
More reliable	Less reliable
No strict boundaries	Has strict boundaries
Horizontal Approach	Vertical Approach

Q16. What is a UTP cable?

A UTP cable is a 100 ohms cable made up of copper. It consists of 2-1800 unshielded twisted pairs that are surrounded by a non-metallic case. These twists provide immunity to electrical noise and EMI.

Q17. What is the maximum length allowed for a UTP cable?

The maximum length allowed for a UTP cable is 100m. This includes 90 m of solid cabling and 10m of standard patch cable.

Q18. Explain what is HTTP and which port does it use?

HTTP or HyperText Transfer Protocol allows communication over the Internet. This protocol basically defines how messages are to be transmitted and formatted over the world wide web. HTTP is a TCP/ IP protocol and it uses the port number 80.

Features of HTTP Protocol:

- It is connection-less
- Does not depend on the type of connecting media
- Stateless

Q19. What is NAT?

NAT stands for Network Address Translation. It deals with remapping one IP Address space with another by changing the IP headers of the packets that are being transmitted across a traffic routing device.

Q20. What is TCP?

TCP or Transmission Control Protocol is a connection-oriented protocol that establishes and maintains a connection between communicating devices until both of them are done exchanging messages. This protocol determines how application data can be broken down into packets that can be delivered over a network. It also sends and receives packets to and from the network layer and is in charge of flow control, etc.

Q21. Give a brief explanation about UDP?

UDP or the User Datagram Protocol is used to create a low-latency and loss-tolerating communications between applications connected over the internet. UDP enables process-to-process communication and communicates via datagrams or messages.

Q22. Differentiate between TCP and UDP.

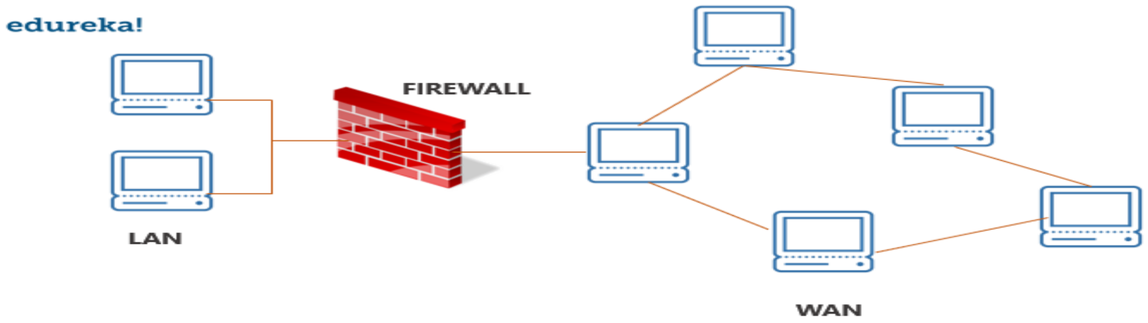
Factor of comparison	TCP	UDP
Connection	Connection made before application messages are exchanged	Connection not made before application messages are exchanged
Use	For applications needing more reliability and less speed	For applications needing more speedy and less reliability
Use by Protocols of the Application Layer	File transfer, e-mail, etc	Multimedia, DNS
Reliability	Messages will be delivered in order and without errors	No guarantee that the messages will be delivered in order and without errors
Data Segments	Data segments rearranged in required order	All segments are independent, therefore has no inherent order specification
Acknowledgment	ACK is received	ACK is not received
Flow Control	Has the congestion control mechanism	No flow control option
Check for Errors	Resends erroneous segments	Discards Erroneous segments

Q23. What is RIP?

RIP (Routing Information Protocol) is a dynamic routing protocol. It makes use of hop count as its primary metric to find the best path between the source and the destination. It works in the application layer and has an AD (Administrative Distance) value of 120.

Q24. Explain what is a firewall?

A firewall is a network security system which is used to monitor and control the network traffic based on some predefined rules. Firewalls are the first line of defense and establish barriers between the internal and external networks in order to avoid attack from untrusted external networks. Firewalls can be either hardware, software or sometimes both.



Q25. Explain what is NOS?

A Network Operating System (NOS) is an Operating System that is designed to support workstations, databases, personal computers, etc over a network. Some examples of NOS are MAC OS X, Linux, Windows Server 2008, etc. These Operating Systems provide various functionalities such as processor support, multiprocessing support, authentication, Web services, etc.

Q26. Explain what is Denial of Service (DoS)?

Denial of Service (DoS) is a kind of attack that prevents a legitimate user from accessing data over a network by a hacker or an attacker. The attacker floods the server with unnecessary requests in order to overload the server thereby preventing the legitimate users from accessing its services.

Q27. What is the full form of ASCII?

ASCII stands for American Standard Code for Information Interchange. It is a character encoding standard used in the electronic communication field. The ASCII codes basically represent text.

Q28. What is IEEE?

IEEE stands for **I**nstitute of **E**lectrical and **E**lectronics **E**ngineer. It is the world's largest technical professional society and is devoted to advancing innovation and technological excellence.

Q29. What is a MAC address and why is it required?

MAC or Media Access Control address is a computer's unique number assigned to a Network Interface Controller (NIC). It is a 48-bit number that identifies each device on a network and is also referred to as the physical address. MAC addresses are used as a network address for communications within a network such as an Ethernet, Wi-Fi, etc.

Q30. What is piggybacking?

During transmission of data packets in two-way communication, the receiver sends an acknowledgment (control frame or ACK) to the receiver after receiving the data packets. However, the receiver does not send the acknowledgment immediately, but, waits until its network layer passes in the next data packet. Then, the ACK is attached to the outgoing data frame. This process of delaying the ACK and attaching it to the next outgoing data frame is known as piggybacking.

Q31. Explain what is DNS?

DNS or Domain Name System is a naming system for devices connected over the internet. It is a hierarchical and decentralized system that translates domain names to the numerical IP Addresses which is required to identify and locate devices based on the underlying protocols.

All devices connected to the internet have unique IP addresses which are used to locate them on the network. The process involves conversion on hostnames into IP addresses. For example, in case the user wants to load some web page (xyz.com), this hostname is converted into an IP address that can be understood by the computer in order to load that web page.

Q32. Differentiate between Domain and a Workgroup.

Domain	Workgroup
Has one or more computer acting as a server	All computers are peers
Has a centralized database	Each computer has its own database
Computers can be on different LANs	All computers are on the same LAN

Q33. What is OSPF?

OSPF stands for Open Shortest Path First. It is basically a routing protocol that is used to find the best path for packets that are being transmitted over interconnected networks.

Q34. What is Round Trip Time?

Round Trip Time or Round Trip Delay Time refers to the time taken for a signal to be sent and the ACK of that signal to be received.

Q35. What is DHCP?

DHCP or Dynamic Host Configuration Protocol is a network management protocol. It is used on the UDP/IP networks and it automatically assigns IP addresses to the devices on the network. This, in turn, reduces the need of a network admin to manually assign IP addresses thereby reducing errors.

Q36. Briefly explain what is ICMP?

ICMP stands for Internet Control Message Protocol and is a part of the Internet Protocol Suite. It is basically a supporting protocol to the Internet protocol and is used to send error messages and information regarding the success or failure of communication with another IP address. For example, if a service is not available an error is reported.

Q37. What is a Ping?

A ping is a computer program that is used to test the reachability of a host and check if can accept requests on an IP network. It works by sending an ICMP (Internet Control Message Protocol) Echo to some computer on the network and waits for a reply from it. It can also be used for troubleshooting.

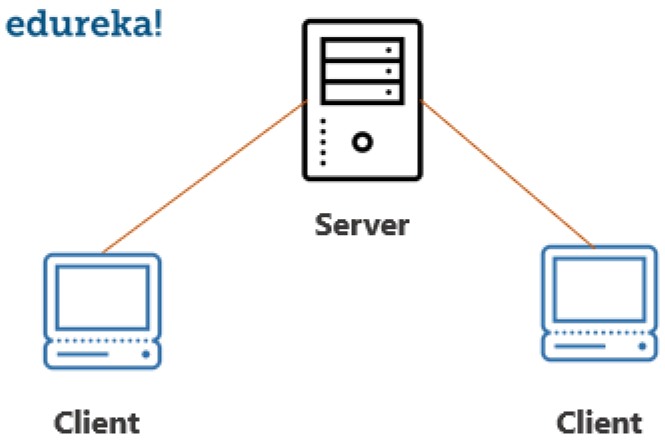
Q38. What are the advantages of optic fibers?

Optic fibers have a number of advantages such as:

- Greater bandwidth than other metal cables
- Low power loss allows longer transmission distances
- Optic cables are immune to electromagnetic interference
- Lesser production rates
- Thin and light
- The optical fiber cable is difficult to tap

Q39. What is a client/ server network?

A client/ server network is a network where one computer behaves as a server to the other computers. The server is usually more powerful than the clients and serves the clients.



Q40. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?

The best solution is to install anti-virus on all the computers in the network. This will protect each device from the other in case some malicious user tries to insert a virus into the servers or legitimate users.

Q41. What do you mean by Ethernet?

Ethernet is a network technology used in LAN, MAN and WAN that connects devices using cables for the transmission of data. It provides services on the Physical and Data Link layers of the OSI Model.

Q42.What is SLIP?

SLIP stands for Serial Line Internet Protocol which allows a user to access the internet using the modem.

Q43. What is the difference between CSMA/CD and CSMA/CA?

CSMA/ CD	CSMA/ CA
The effect is after a collision	The effect is before a collision
Minimizes the recovery time	Reduces the possibility of a collision
Usually used in wired networks	Usually used in wireless networks

Q44. Briefly explain what is tunnel mode?

Tunnel mode is used to encrypt the whole IP packet including the headers and the payload. It is basically used in a Site-to-Site VPN to secure communications between security gateways, firewalls, etc.

Q45. What do you mean by IPv6?

IPv6 stands for Internet Protocol version 6 and is the latest version of the Intenet Protocol. The IP address length is 128 bits which resolves the issue of approaching shortage of network addresses.

Q46. Explain the RSA algorithm briefly.

RSA is a cryptosystem used to secure data transmission named after Ron Rivest, Adi Shamir and Len Adleman. This algorithm has a public key for encryption while the decryption key is kept secure or private. The encryption key is created using two large prime numbers and is published along with an auxiliary value. Anybody can make use of this public key for encryption but only someone with the knowledge of the prime numbers can decrypt it. However, this algorithm is considered to be slow and for the same reason, it is not used very often to encrypt data.

Q47. What is an encoder?

An encoder is a program, circuit or a device that converts data from one format to another. Encoders convert analog signals into digital ones.

Q48. What is a decoder?

A decoder is a program, circuit or a device that converts the encoded data into its actual format. Decoders convert digital signals to analog ones.

Q49. What is sneakernet?

Sneakernet is the unofficial term for the transfer of electronic information by physically moving media which can be anything such as a Floppy disk, USB flash, optical disks, etc.

Q50. What are the components of a Protocol?

Protocols are a set of rules that govern communication. The key elements of a Protocol are as follows:

Name	Description
Syntax	Refers to the structure and format of data
Semantics	Refers to the meaning of each portion of bits
Timing	Refers to when data should be sent and received

1) What is a Link?

A link refers to the connectivity between two devices. It includes the type of cables and protocols used for one device to be able to communicate with the other.

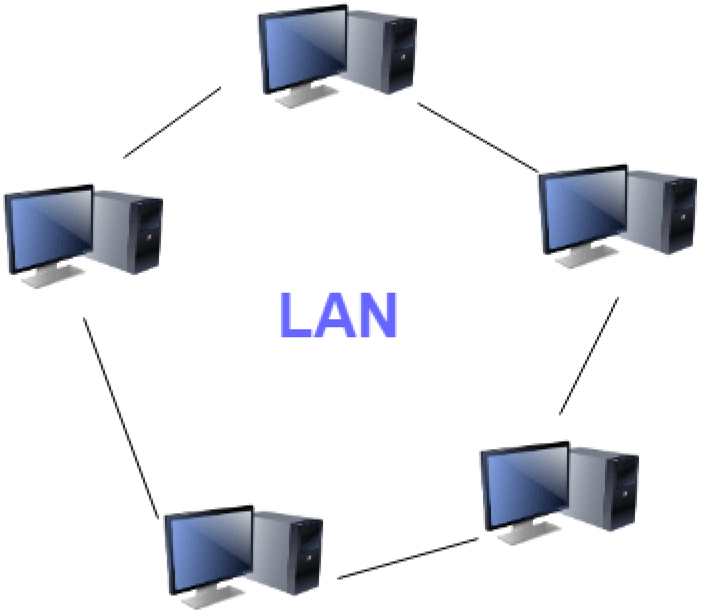
2) What are the layers of the OSI reference model?

There are 7 OSI layers: 1) Physical Layer, 2) Data Link Layer, 3) Network Layer, 4) Transport Layer, 5) Session Layer, 6) Presentation Layer, and 7) Application Layer.

3) What is the backbone network?

A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles the management of bandwidth and multiple channels.

4) What is a LAN?



LAN network

LAN stands for Local Area Network. It refers to the connection between computers and other network devices that are located within a small physical location.

5) What is a node?

A node refers to a point or joint where a connection takes place. It can be a computer or device that is part of a network. Two or more nodes are needed to form a network connection.

6) What are routers?

Router

Routers can connect two or more network segments. These are intelligent network devices that store information in its routing tables, such as paths, hops, and bottlenecks.

With this info, they can determine the best path for data transfer. Routers operate at the OSI Network Layer.

7) What is a point to point link?

It refers to a direct connection between two computers on a network. A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers.

8) What is anonymous FTP?

Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed access to data in these servers do not need to identify themselves, but instead, log in as an anonymous guest.

9) What is a subnet mask?

A subnet mask is combined with an IP address to identify two parts: the extended network address and the host address. Like an IP address, a subnet mask is made up of 32 bits.

10) What is the maximum length allowed for a UTP cable?

A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.

11) What is data encapsulation?

Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.

12) Describe Network Topology

Network Topology refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect.

13) What is a VPN?

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

14) Briefly describe NAT

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share a single connection to the Internet.

15) What is the job of the Network Layer under the OSI reference model?

The Network layer is responsible for data routing, packet switching, and control of network congestion. Routers operate under this layer.

16) How does a network topology affect your decision to set a network?

Network topology dictates what media you must use to interconnect devices. It also serves as a basis on what materials, connectors, and terminations that is applicable for the setup.

17) What is RIP?

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

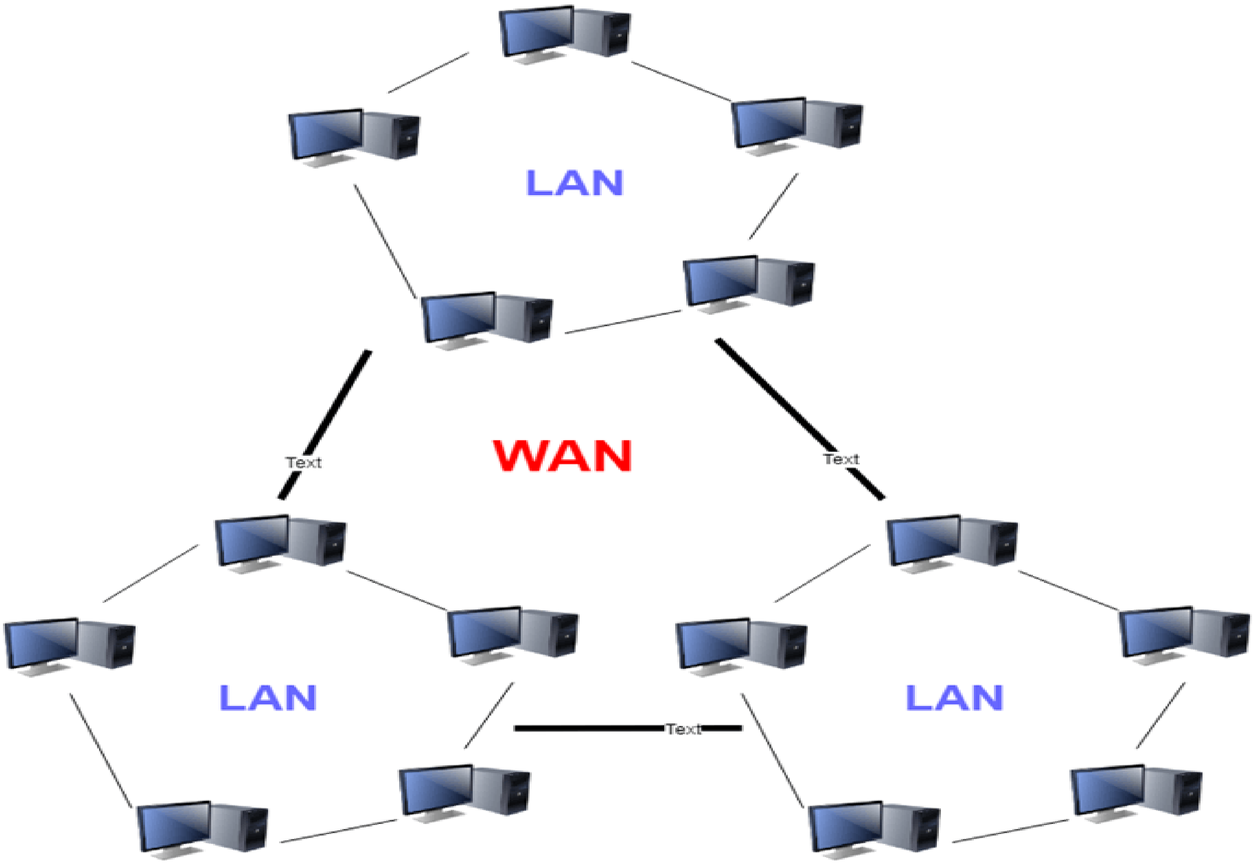
18) What are the different ways of securing a computer network?

There are several ways to do this. Install a reliable and updated anti-virus program on all computers. Make sure firewalls are setup and configured correctly. User authentication will also help a lot. All these combined would make a highly secured network.

19) What is NIC?

NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

20) What is WAN?



WAN network

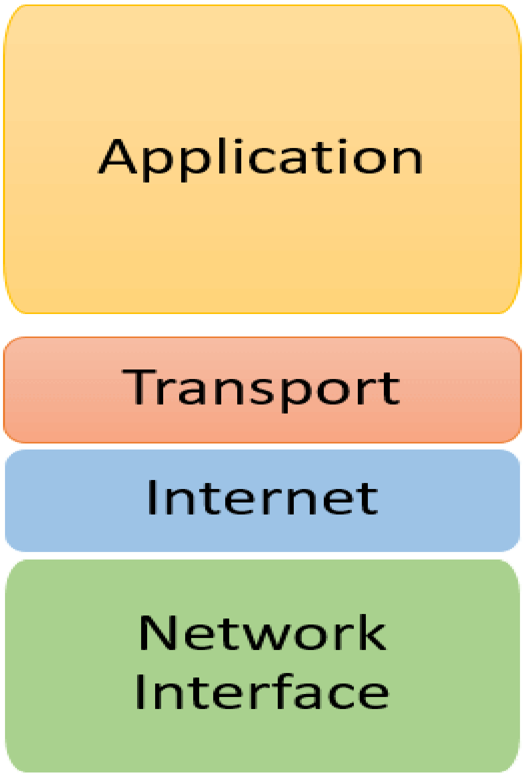
WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.

21) What is the importance of the OSI Physical Layer?

The physical layer does the conversion from data bits to the electrical signal, and vice versa. This is where network devices and cable types are considered and setup.

22) How many layers are there under TCP/IP?

There are four layers: 1) The Network Layer, 2) Internet Layer, 3) Transport Layer, and 4) Application Layer.



TCP/IP Layers

23) What are proxy servers, and how do they protect computer networks?

Proxy servers primarily prevent external users who are identifying the IP addresses of an internal network. Without knowledge of the correct IP address, even the physical location of the network cannot be identified. Proxy servers can make a network virtually invisible to external users.

24) What is the function of the OSI Session Layer?

This layer provides the protocols and means for two devices on the network to communicate with each other by holding a session. This includes setting up the session, managing information exchange during the session, and tear-down process upon termination of the session.

25) What is the importance of implementing a Fault Tolerance System?

A fault tolerance system ensures continuous data availability. This is done by eliminating a single point of failure.

26) What does 10Base-T mean?

The 10 refers to the data transfer rate. In this case, it is 10Mbps. The word Base refers to baseband, as opposed to broadband.

27) What is a private IP address?

Private IP addresses are assigned for use on intranets. These addresses are used for internal networks and are not routable on external public networks. These ensure that no conflicts are present among internal networks. At the same time, the same range of private IP addresses is reusable for multiple intranets since they do not "see" each other.

28) What is NOS?

NOS, or Network Operating System, is specialized software. The main task of this software is to provide network connectivity to a computer in order to communicate with other computers and connected devices.

29) What is DoS?

DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the Internet or any other network services. Such attacks may come in different forms and are done by a group of perpetrators. One common method of doing this is to overload the system server so it cannot anymore process legitimate traffic and will be forced to reset.

30) What is OSI, and what role does it play in computer networks?

OSI (Open Systems Interconnect) serves as a reference model for data communication. It is made up of 7 layers, with each layer defining a particular aspect of how network devices connect and communicate with one another. One layer may deal with the physical media used, while another layer dictates how data is transmitted across the network.

31) What is the purpose of cables being shielded and having twisted pairs?

The primary purpose of this is to prevent crosstalk. Crosstalk's are electromagnetic interferences or noise that can affect data being transmitted across cables.

32) What is the advantage of address sharing?

By using address translation instead of routing, address sharing provides an inherent security benefit. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer. Instead, it provides address translation and not the private IP addresses on the internal network.

33) What are MAC addresses?

MAC, or Media Access Control, uniquely identifies a device on the network. It is also known as a physical address or an Ethernet address. A MAC address is made up of 6-byte parts.

34) What is the equivalent layer or layers of the TCP/IP Application layer in terms of the OSI reference model?

The TCP/IP Application layer has three counterparts on the OSI model: 1) Session Layer, 2) Presentation Layer, and 3) Application Layer.

35) How can you identify the IP class of a given IP address?

By looking at the first octet of any given IP address, you can identify whether it’s Class A, B, or C. If the first octet begins with a 0 bit, that address is Class A. If it begins with bits 10 then that address is a Class B address. If it begins with 110, then it’s a Class C network.

36) What is the main purpose of OSPF?

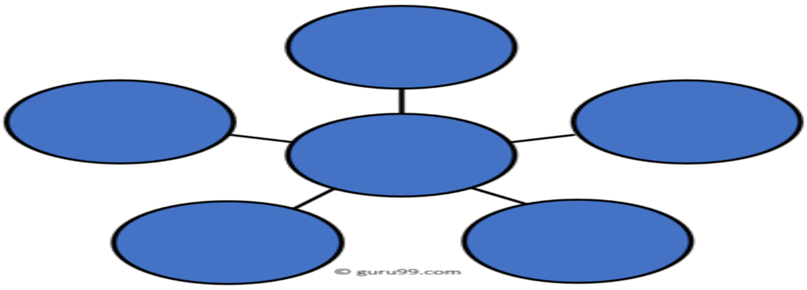
OSPF, or Open Shortest Path First, is a link-state routing protocol that uses routing tables to determine the best possible path for data exchange.

37) What are firewalls?

Firewalls serve to protect an internal network from external attacks. These external threats can be hackers who want to steal data or computer viruses that can wipe out data in an instant. It also prevents other users from external networks from gaining access to the private network.

38) Describe star topology

Star topology consists of a central hub that connects to nodes. This is one of the easiest to set up and maintain.



Star Topology

Advantages:

Here are pros/benefits of start topology:

- Easy to troubleshoot, set up, and modify.
- Only those nodes are affected, that has failed. Other nodes still work.
- Fast performance with few nodes and very low network traffic.

- In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages:

Here are cons/drawbacks of using Star:

- If the Hub or concentrator fails, attached nodes are disabled.
- The cost of installation of star topology is costly.
- Heavy network traffic can sometimes slow the bus considerably.
- Performance depends on the Hub’s capacity
- A damaged cable or lack of proper termination may bring the network down.

39) What are gateways?

Gateways provide connectivity between two or more network segments. It is usually a computer that runs the gateway software and provides translation services. This translation is key in allowing different systems to communicate on the network.

40) What is the disadvantage of a star topology?

One major disadvantage of star topology is that once the central Hub or switch gets damaged, the entire network becomes unusable.

41) What is SLIP?

SLIP, or Serial Line Interface Protocol, is an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.

42) Give some examples of private network addresses.

10.0.0.0 with a subnet mask of 255.0.0.0172.16.0.0 with subnet mask of 255.240.0.0192.168.0.0 with subnet mask of 255.255.0.0

43) What is tracert?

Tracert is a Windows utility program that can use to trace the route taken by data from the router to the destination network. It also shows the number of hops taken during the entire transmission route.

44) What are the functions of a network administrator?

A network administrator has many responsibilities that can be summarized into 3 key functions: installation of a network, a configuration of network settings, and maintenance/troubleshooting of networks.

45) What is the main disadvantage of a peer to peer network?

Accessing the resources that are shared by one of the workstations on the network takes a performance hit.

46) What is a Hybrid Network?

A hybrid network is a network setup that makes use of both client-server and peer-to-peer architecture.

47) What is DHCP?

DHCP is short for Dynamic Host Configuration Protocol. Its main task is to assign an IP address to devices across the network automatically. It first checks for the next available address not yet taken by any device, then assigns this to a network device.

48) What is the main job of the ARP?

The main task of the ARP or Address Resolution Protocol is to map a known IP address to a MAC layer address.

49) What is TCP/IP?

TCP/IP is short for Transmission Control Protocol / Internet Protocol. This is a set of protocol layers that is designed to make data exchange possible on different types of computer networks, also known as a heterogeneous network.

50) How can you manage a network using a router?

Routers have a built-in console that lets you configure different settings, like security and data logging. You can assign restrictions to computers, such as what resources it is allowed access or what particular time of the day, they can browse the Internet. You can even put restrictions on what websites are not viewable across the entire network.

51) What protocol can be applied when you want to transfer files between different platforms, such as UNIX systems and Windows servers?

Use FTP (File Transfer Protocol) for file transfers between such different servers. This is possible because FTP is platform-independent.

52) What is the use of a default gateway?

Default gateways provide means for the local networks to connect to the external network. The default gateway for connecting to the external network is usually the address of the external router port.

53) What can be considered as good passwords?

Good passwords are made up of not just letters, but by combining letters and numbers. A password that combines uppercase and lowercase letters is favorable than one that uses all upper case or all lower-case letters. Passwords must be not words that can easily be guessed by hackers, such as dates, names, favorites, etc. Longer passwords are also better than short ones.

54) What is the proper termination rate for UTP cables?

The proper termination for unshielded twisted pair network cable is 100 ohms.

55) What is netstat?

Netstat is a command-line utility program. It provides useful information about the current TCP/IP settings of a connection.

56) What is the number of network IDs in a Class C network?

For a Class C network, the number of usable Network ID bits is 21. The number of possible network IDs is 2 raised to 21 or 2,097,152. The number of host IDs per network ID is 2 raised to 8 minus 2, or 254.

57) What happens when you use cables longer than the prescribed length?

Cables that are too long would result in signal loss. It means that data transmission and reception would be affected because the signal degrades over length.

58) What common software problems can lead to network defects?

Software related problems can be any or a combination of the following:

- Client-server problems
- Application conflicts
- Error in configuration
- Protocol mismatch
- Security issues
- User policy and rights issues

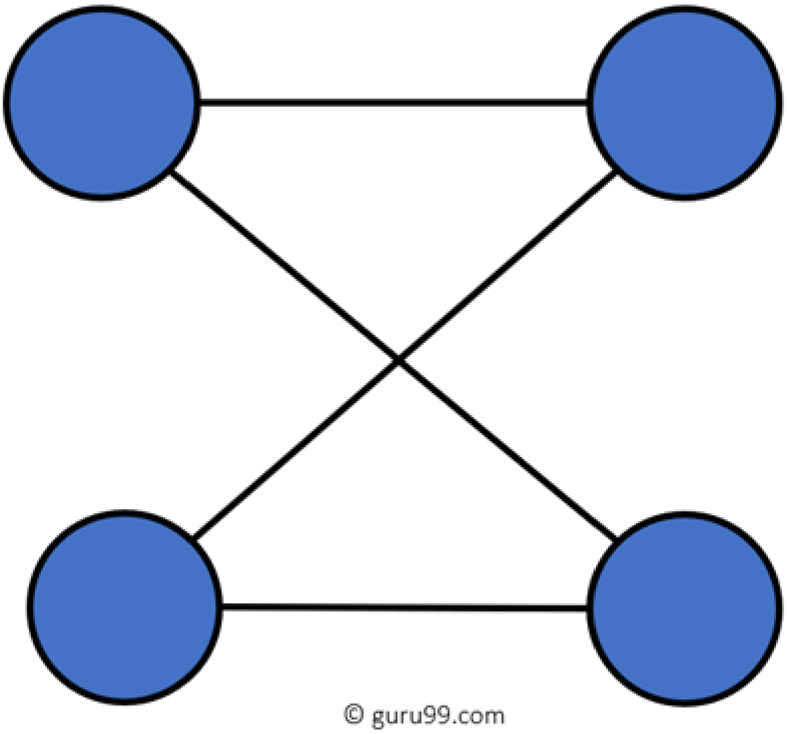
59) What is ICMP?

ICMP is an Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP/IP stack. This is also the protocol that manages error messages that are used by network tools such as PING.

60) What is Ping?

Ping is a utility program that allows you to check connectivity between network devices on the network. You can ping a device by using its IP address or device name, such as a computer name.

61) What is peer to peer?



P2P Network

Peer to peer (P2P) are networks that do not rely on a server. All PCs on this network act as individual workstations.

62) What is DNS?

DNS is the Domain Name System. The main function of this network service is to provide host names to TCP/IP address resolution.

63) What advantages does fiber optics have over other media?

One major advantage of fiber optics is that it is less susceptible to electrical interference. It also supports higher bandwidth, meaning more data can be transmitted and received. Signal degrading is also very minimal over long distances.

64) What is the difference between a hub and a switch?

Here is the major difference between Hub and switch:

Hub	**Switch**
A hub operates on the physical layer.	A switch operates on the data link layer.
Hubs perform frame flooding that can be unicast, multicast, or broadcast.	It performs broadcast, then the unicast and multicast as needed.

Just a singular domain of collision is present in a hub.	Varied ports have separate collision domains
The transmission mode is Half-duplex	The transmission mode is Full duplex
Hubs operate as a Layer 1 device per the OSI model.	Network switches help you to operate at Layer 2 o
To connect a network of personal computers should be joined through a central hub.	Allow connecting multiple devices and ports
Uses electrical signal orbits	Uses frame & packet
Does not offer Spanning-Tree	Multiple Spanning-Tree is possible
Collisions occur mostly in setups using hubs.	No collisions occur in a full-duplex switch.
Hub is a passive device	A switch is an active device
A network hub can’t store MAC addresses.	Switches use CAM (Content Accessible Memory) by ASIC (Application Specific Integrated Chips).
Not an intelligent device	Intelligent device
Its speed is up to 10 Mbps	10/100 Mbps, 1 Gbps, 10 Gbps
Does not use software	Has software for administration

65) What are the different network protocols that are supported by Windows RRAS services?

There are three main network protocols supported: NetBEUI, TCP/IP, and IPX.

66) What are the maximum networks and hosts in class A, B, and C network?

For Class A, there are 126 possible networks and 16,777,214 hosts. For Class B, there are 16,384 possible networks and 65,534 hosts. For Class C, there are 2,097,152 possible networks and 254 hosts

67) What is the standard color sequence of a straight-through cable?

Orange/white, orange, green/white, blue, blue/white, green, brown/white, brown.

68) What protocols fall under the Application layer of the TCP/IP stack?

The following are the protocols under the TCP/IP Application layer: FTP, TFTP, Telnet, and SMTP.

69) You need to connect two computers for file sharing. Is it possible to do this without using a hub or a router?

Yes, you can connect two computers, using only one cable. A crossover type cable can be used in this scenario. In this setup, the data transmit pin of one cable is connected to the data receive pin of the other cable, and vice versa.

70) What is ipconfig?

Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

71) What is the difference between a straight-through and crossover cable?

A straight-through cable is used to connect computers to a switch, hub, or router. A crossover cable is used to connect two similar devices, such as a PC to PC or Hub, to the Hub.

72) What is the client/server?

Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refer to a workstation that accesses the server.

73) Describe networking.

Networking refers to the interconnection between computers and peripherals for data communication. Networking can be done using wired cabling or through a wireless link.

74) When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?

Yes, that’s because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when another one replaced the NIC card.

75) Explain clustering support

Clustering support refers to the ability of a network operating system to connect multiple servers in a fault-tolerant group. The main purpose of this is the if one server fails, all processing will continue with the next server in the cluster.

76) Where is the best place to install an Anti-virus program?

An anti-virus program must be installed on all servers and workstations to ensure protection. That’s because individual users can access any workstation and introduce a computer virus. You can plug in their removable hard drives or flash drives.

77) Describe Ethernet.

Ethernet is one of the popular networking technologies used these days. It was developed during the early 1970s and is based on specifications, as stated in the IEEE. Ethernet is used in local area networks.

78) What are some drawbacks of implementing a ring topology?

In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular network, the entire network must be temporarily brought down.

79) What is the difference between CSMA/CD and CSMA/CA?

CSMA/CD, or Collision Detect, retransmits data frames whenever a collision occurred. CSMA/CA, or Collision Avoidance, will first broadcast intent to send prior to data transmission.

80) What is SMTP?

SMTP is short for Simple Mail Transfer Protocol. This protocol deals with all internal mail and provides the necessary mail delivery services on the TCP/IP protocol stack.

81) What is multicast routing?

Multicast routing is a targeted form of broadcasting that sends a message to a selected group of the user instead of sending it to all users on a subnet.

82) What is the importance of Encryption on a network?

Encryption is the process of translating information into a code that is unreadable by the user. It is then translated back or decrypted back to its normal readable format using a secret key or password. Encryption ensures that information that is intercepted halfway would remain unreadable because the user must have the correct password or key for it.

83) How are IP addresses arranged and displayed?

IP addresses are displayed as a series of four decimal numbers that are separated by period or dots. Another term for this arrangement is the dotted-decimal format. An example is 192.168.101.2

84) Explain the importance of authentication.

Authentication is the process of verifying a user’s credentials before he can log into the network. It is normally performed using a username and password. This provides a secure means of limiting access from unwanted intruders on the network.

85) What is meaning by tunnel mode?

This is a mode of data exchange wherein two communicating computers do not use IPsec themselves. Instead, the gateway that is connecting their LANs to the transit network creates a virtual tunnel. So, it uses the IPsec protocol to secure all communication that passes through it.

86) What are the different technologies involved in establishing WAN links?

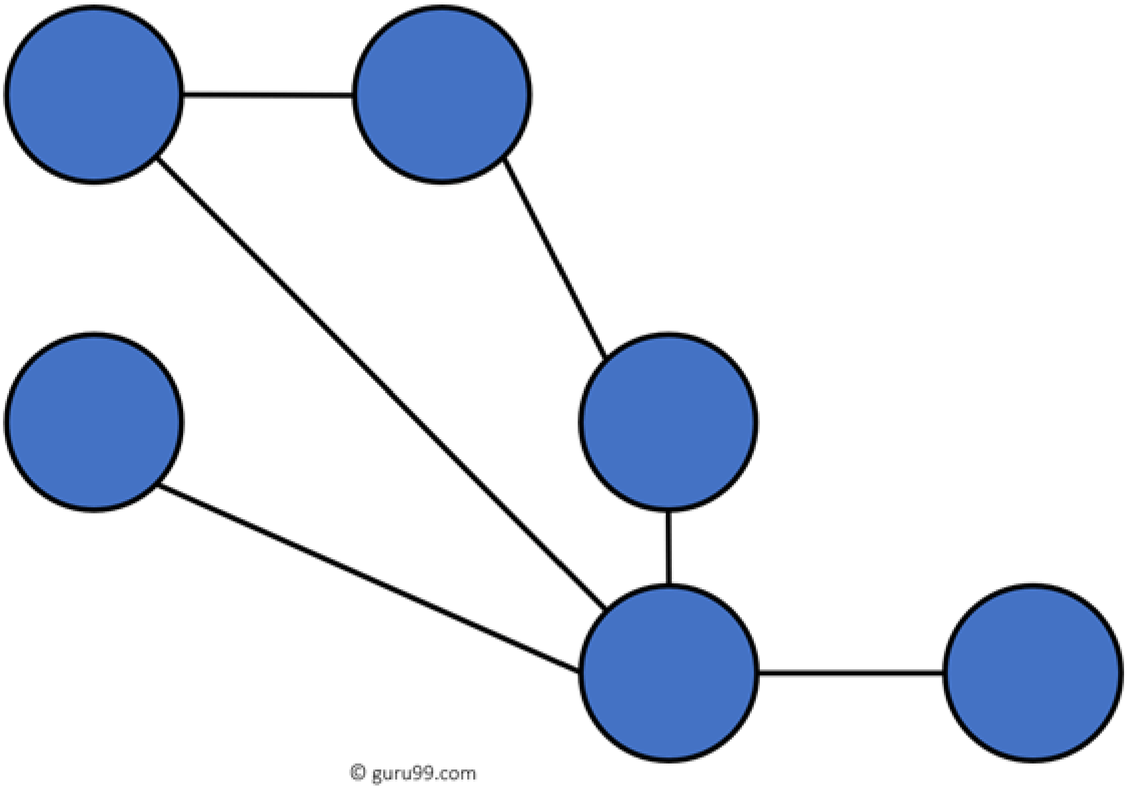
- Analog connections – using conventional telephone lines
- Digital connections – using digital-grade telephone lines
- Switched connections – using multiple sets of links between the sender and receiver to move data.

87) Explain Mesh Topology

The mesh topology has a unique network design in which each computer on the network connects to every other. It is developing a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, data still has an alternative path to reach its destination.

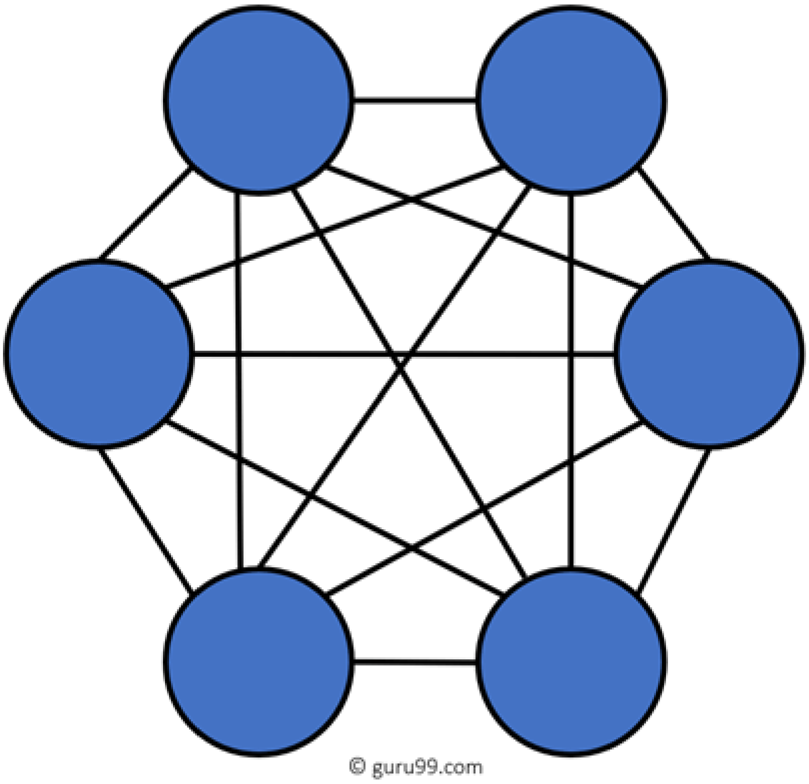
Types of Mesh Topology:

Partial Mesh Topology: In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices.



Partially Connected Mesh Topology

Full Mesh Topology: In this topology, every node or device are directly connected with each other.



Fully Connected Mesh Topology

88) When troubleshooting computer network problems, what common hardware-related problems can occur?

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs, and even hardware startups. Incorrect hardware configuration is also one of those culprits to look into.

89) How can you fix signal attenuation problems?

A common way of dealing with such a problem is to use repeaters and hubs because it will help regenerate the signal and therefore prevent signal loss. Checking if cables are properly terminated is also a must.

90) How does dynamic host configuration protocol aid in network administration?

Instead of having to visit each client computer to configure a static IP address, the network administrator can apply dynamic host configuration protocol to create a pool of IP addresses known as scopes that can be dynamically assigned to clients.

91) Explain profile in terms of networking concepts

Profiles are the configuration settings made for each user. A profile may be created that puts a user in a group, for example.

92) What is sneakernet?

Sneakernet is believed to be the earliest form of networking wherein data is physically transported using removable media, such as disk, tapes.

93) What is the role of the IEEE in computer networking?

IEEE, or the Institute of Electrical and Electronics Engineers, is an organization composed of engineers that issues and manages standards for electrical and electronic devices. This includes networking devices, network interfaces, cablings, and connectors.

94) What protocols fall under the TCP/IP Internet Layer?

There are 4 protocols that are being managed by this layer. These are ICMP, IGMP, IP, and ARP.

95) When it comes to networking, what are rights?

Rights refer to the authorized permission to perform specific actions on the network. Each user on the network can be assigned individual rights, depending on what must be allowed for that user.

96) What is one basic requirement for establishing VLANs?

A VLAN is required because at the switch level. There is only one broadcast domain. It means whenever a new user is connected to switch. This information is spread throughout the network. VLAN on switch helps to create a separate broadcast domain at the switch level. It is used for security purposes.

97) What is IPv6?

IPv6, or Internet Protocol version 6, was developed to replace IPv4. At present, IPv4 is being used to control internet traffic but is expected to get saturated in the near future. IPv6 was designed to overcome this limitation.

98) What is the RSA algorithm?

RSA is short for the Rivest-Shamir-Adleman algorithm. It is the most commonly used public-key encryption algorithm in use today.

99) What is mesh topology?

Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device has at least two network connections.

100) what is the maximum segment length of a 100Base-FX network?

The maximum allowable length for a network segment using 100Base-FX is 412 meters. The maximum length for the entire network is 5 kilometers.

101) What is the 5-4-3 rule, and in which architecture is it used?

The 5-4-3 rule is used in 10Base2 and 10Base5 Ethernet architectures. In this rule, there can be a maximum of five segments in a network connected with four repeaters. Out of these five segments, only three segments can be populated with nodes.

102) What is the difference between TCP and UDP?

Here are some major differences between TCP and UDP protocols:

TCP	**UDP**
It is a connection-oriented protocol.	It is a connectionless protocol.
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the Internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed for TCP is slower.	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	The header size is 8 bytes.
TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.
TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.
Acknowledgment segments	No Acknowledgment segments
Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.
TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data.	UDP has just a single error checking mechanism that is used for checksums.

103) What are the important elements of the protocol?

Here, are three most important elements of the protocol:

- **Syntax:** It is the format of the data. It is an order the data is displayed.
- **Semantics:** It describes the meaning of the bits in each section.
- **Timing:** What time the data is to be sent and how fast it is to be sent.

104) What is the maximum segment length of a 100Base-FX network?

The maximum length for a network segment using 100Base-FX is 412 meters.

105) What is a Decoder?

The decoder is a type of circuit that converts the encoded data to its original format. It also converts the digital signal into an analog signal.

106) What is Brouter?

Brouter is also known as Bridge Router. It is a device that acts as both a bridge and a router. As a bridge can forwards data between the networks. It also routes the data to specified systems within a network.

107) How to use VPN?

By using a Virtual Private Network (VPN), users can connect to the organization’s network. Corporate companies, educational institutions, government offices.

108) Why the standard OSI model is known as 802.xx?

The OSI model was started in February 1980. In 802.XX, ’80’ stands for the year 1980, and ‘2’ represents the month of February.

109) What is NVT (Network Virtual Terminal)?

NVT is a set of pre-defined rules to very simple virtual terminal interaction. This terminal helps you to start a Telnet session.

110) What is the source route?

The source route is a sequence of IP addresses that helps you to identify the route a datagram. You can include the source route in the IP datagram header.

111) Explain the term Pipelining

Pipelining describes the sequencing of processes. When any new task begins before an ongoing task is finished, it is called sequencing.

112) Which measurement unit is used to measure the transmission speed of Ethernet?

The transmission speed of Ethernet is mostly measured in Mbps.

113) What is the maximum length of Thinnet cable?

The length of the Thinnet cable is 185 meters.

114) Which cable is also called as the RG8 cable?

Thicknet cable is also called as the RG8 cable.

115) Is coaxial cable still used in the computer network?

No, Nowadays, coaxial cable no longer used in a computer network.

116) Which cable uses the RJ11 connector?

Most of the telephone cable uses the RJ11 connector.

117) Explain Multi-homed Host

It is a host that has multiple network interfaces that multiple IP addresses is called a Multi-homed Host.

118) Explain EGP

The full form of EGP is Exterior Gateway Protocol. It is the protocol of the routers. It is the neighboring autonomous systems that help you to identify the set of networks that you will able to reach within or via each independent system.

119) Explain the term Passive Topology

When a computer in the network listen and receive the signal, they are called passive topology.

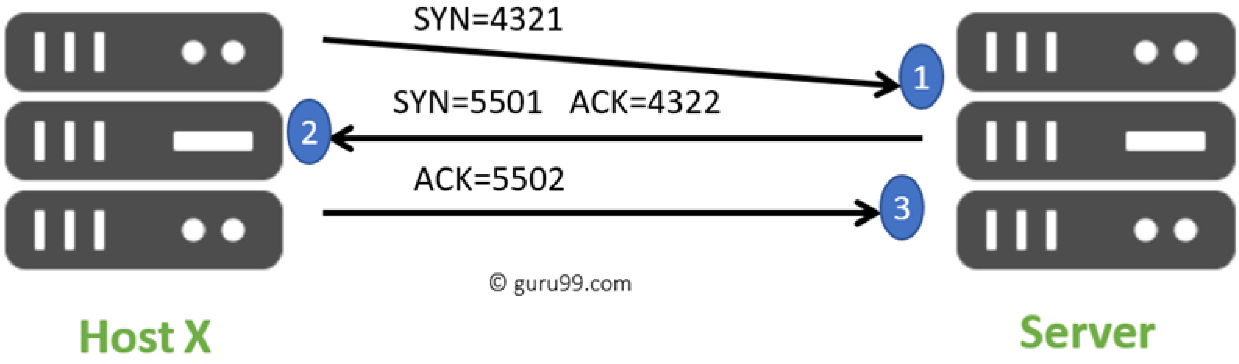
120) What is the use of a Pseudo TTY?

It is a false terminal which allows you external machines to connect through Telnet or log in. Without this, no connection can take place.

121) Explain Redirector

Redirector is a kind of software which intercepts file or prints I/O requests and translates them into network requests. This component comes under the presentation layer.

122) What Is TCP Three-Way Handshake?



TCP Three-Way Handshake

THREE-WAY handshake or a TCP 3-way handshake is a process that 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 synchronization and acknowledgment packets before the real data communication process starts.

123) What is a Hamming code?

Hamming code is a liner code that is useful for error detection up to two immediate bit errors. It is capable of single-bit errors.

In Hamming code, the source encodes the message by adding redundant bits in the message. These redundant bits are mostly inserted and generated at certain positions in the message to accomplish the error detection and correction process.

124) What is the Application of Hamming code?

Here are some common applications of using Hemming code:

- Satellites
- Computer Memory
- Modems
- PlasmaCAM
- Open connectors
- Shielding wire
- Embedded Processor

125) What are the benefits of the Hamming code?

Here, are important benefits of Hamming code

- The Hamming code method is effective on networks where the data streams are given for the single-bit errors.
- Hamming code not only provides the detection of a bit error but also helps you to indent bit containing error so that it can be corrected.
- The ease of use of hamming codes makes it suitable for use in computer memory and single-error correction.

126) What is a MAC Address?

MAC address is a unique identifier that is assigned to a NIC (Network Interface Controller/ Card). It consists of a 48 bit or 64-bit address, which is associated with the network adapter. MAC address can be in hexadecimal format. The full form of MAC address is Media Access Control address.

127) Why Use MAC Address?

Here are the important reasons for using MAC address:

- It provides a secure way to find senders or receivers in the network.
- MAC address helps you to prevent unwanted network access.
- MAC address is a unique number. Hence it can be used to track the device.
- Wi-Fi networks at the airport use the MAC address of a specific device in order to identify it.

128) What are the types of MAC Addresses?

Here are the important types of MAC addresses:

- Universally Administered AddressUAA(Universally Administered Address) is the most used type of MAC address. It is given to the network adapter at the time of manufacturing.
- Locally Administered AddressLAA (Locally Administered Address) is an address that changes the MAC address of the adapter. You may assign this address to a device used by network administrator.

129) What are the important differences between MAC address and IP address

Here, are some difference between MAC and IP address:

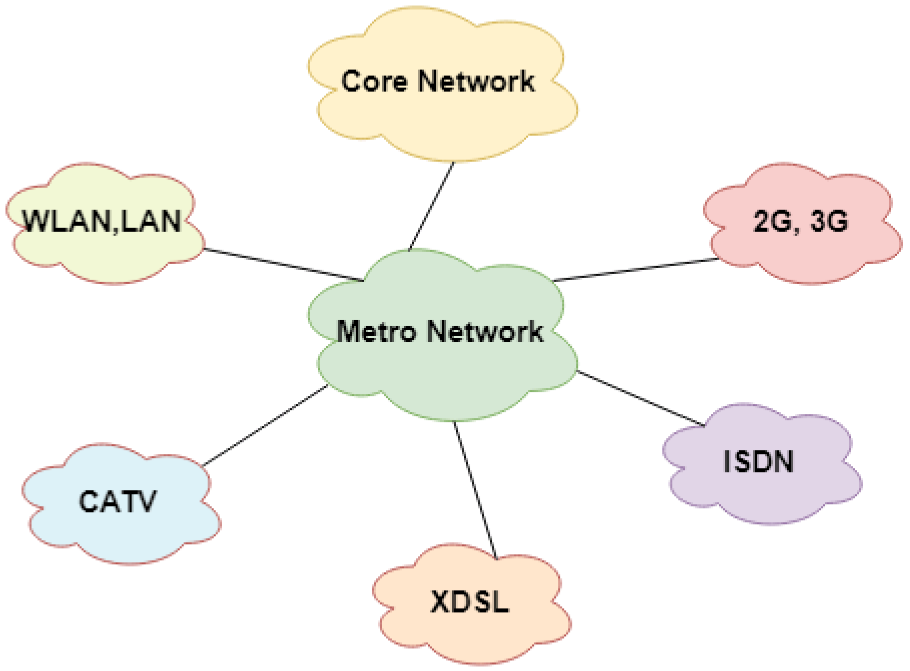
MAC	**IP address**
The MAC address stands for Media Access Control Address.	IP address stands for Internet Protocol Address.
It consists of a 48-bit address.	It consists of a 32-bit address.
MAC address works at the link layer of the OSI model.	IP address works at the network layer of OSI model.
It is referred to as a physical address.	It is referred to as a logical address.
You can retrieve the MAC address of any device using ARP protocol.	You can retrieve the MAC address of any device RARP protocol.
Classes are not used in MAC address.	In IP, IPv4 uses A, B, C, D, and E classes.

132) What are the differences between analog and digital signal?

Here are the main differences between Analog and Digital Signal:

Analog	Digital
An analog signal is a continuous signal that represents physical measurements.	Digital signals are time separated signals which are generated using digital modulation.
It is denoted by sine waves	It is denoted by square waves.
It uses a continuous range of values that help you to represent information.	The Digital signal uses discrete 0 and 1 to represent information.
The analog signal bandwidth is low	The digital signal bandwidth is high.
Analog hardware never offers flexible implementation.	Digital hardware offers flexibility in implementation.
It is suited for audio and video transmission.	It is suited for Computing and digital electronics.
The Analog signal doesn't offer any fixed range.	Digital signal has a finite number, i.e., 0 and 1.

133) What is MAN?



MAN network

A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

134) What is Modem?

A modem (modulator-demodulator) is a device that modulates an analog signal to digital information. It also decodes carrier signals to demodulates the transmitted information.

The main aim of the Modem is to produce a signal that can be transmitted easily and decoded to reproduce the digital data in its original form. Modems are also used for transmitting analog signals, from Light Emitting Diodes (LED) to radio.

Q1. What do you mean by Network?
Set of devices connected to each other over the physical medium is known as a computer network. For example the Internet.

Q2. What do you mean by Node?
In the computer network, the node is known as a device.

Q3. What do you mean by Network Topology?
A network topology is a physical structure of the network which defines how the computers or node will be connected to each other.

Q4. What is Routers?

A router is a device which is responsible for sending data from source to destination

over the computer network.

Q5. What is the OSI model?

OSI model stands for Open System Interconnection. It’s a reference model which describes that how different applications will communicate to each other over the computer network.

Q6. Explain the Different layers of the OSI model.

The different layers of the OSI model are given below:

Physical Layer	Converts data bit into an electrical impulse.
Datalink Layer	Data packet will be encoded and decoded into bits.
Network Layer	Transfer of datagrams from one to another.
Transport Layer	Responsible for Data transfer from one to another.
Session Layer	Manage and control signals between computers.
Presentation Layer	Transform data into application layer format.
Application Layer	An end user will interact with the Application layer

Q7. Describe Hub, Switch and Router?

- **Hub:** Hub will broadcast all data to every port. It has a common connection point for all devices.
- **Switch:** Switch will create the dynamic connection and provide information to the requesting port.

- **Router**: Router is the devices which will be responsible for forwarding data packets.

Q8. What do you mean by the TCP/IP Model?
TCP/IP stands for Transmission control protocol and Internet protocol. It describes how the data will get transmitted and routed from end to end communication.

Q9. Explain the different Layers of TCP/IP Model.
Application Layer, Transport Layer, Network or Internet Layer, Network interface layer.

Q10. What do you mean by HTTP?
HTTP stands for Hyper Text Transfer Protocol and the port for this is 80. This protocol is responsible for web content.

Q11. What do you mean by TCP and UDP?
TCP stands for Transfer control protocol and UDP stands for User Datagrams protocol and TCP is a connection-oriented protocol and UDP is a Connectionless protocol.

Q12. What do you mean by a Firewall?
Firewall is a concept of a security system that will helps computers to protect it with unauthorized access or any cyber-attack.

Q13. What do you mean by DNS?
DNS Stands for Domain Name System. It’s an internet address mapping process with the local name. We can also call it as an internet phonebook.

Q14. What do you mean by Proxy server?
Proxy server prevents the external users which are unauthorized to access the network.

Q15. What do you mean by Classes of Network?
The Classes of IPV4 are of 5 types:

Class A	0.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255

Class D	224.0.0.0 to 239.255.255.255
Class E	240.0.0.0 to 247.255.255.255

Q16. What do you mean by NIC?
NIC stands for Network interface card. It is an adapter that will be installed on the computer and because of that NIC, only that computer will interact with the network.

Q17. What do you mean by ASCII?
ASCII is the American Standard Code for Information Interchange.

Q18. What are the types of mode available in Network?
Data transferring mode in a computer network will be of three types:
Simplex, Half-Duplex and Full Duplex.

Q19. What do you mean by SLIP protocol?
SLIP stands for Serial Line Interface Protocol. It is used for sending IP datagram over a network in a single line.

Q20. What are the key elements of the protocol?
There are three key elements of the protocol:

- Syntax: Describe the format of the data.
- Semantics: Describes the meaning of each section.
- Timings: Explain the timing that how fast the data can be sent.

Q21. What do you mean by Decoder?
A decoder is a program which converts the encrypted data into its actual format.

Q22. What is the role of IEEE in the world of computer network?
IEEE full form is the Institute of Electrical and electronic Engineer which is used to define and develop the standards which will be used over the network.

Q23. What is the maximum segment length of a 100Base-FX network?
The maximum segment length will be 412 meters.

1. What is meant by a link and node?

A network includes two or more computers connected directly by a physical medium like coaxial cable or optical fiber. Link is the physical medium of connection in this setup, and nodes are the computers connected.

2. Define IP address.

In a network system, an IP address is a unique software address of a computer. It is 32 bit.

3. What do you understand by DNS?

There are two types of server/client programs. One is directly used by the user and the other support application programs. Domain Name system belongs to the second type as it is used by other programs, for example, to find the IP address of an e-mail

4. What is a peer-to-peer process?

A peer-to-peer process refers to all processes on a machine that communicates at a given layer.

5. Define network topology.

Network topology refers to the network's physical structure that defines how nodes or computers will be connected.

6. What is a firewall?

A firewall is a security system concept that helps in protecting computers from any cyber-attack or unauthorized access.

7. Tell us the maximum segment length of the 100Base-FX network.

The maximum length of a 100Base-FX network is 412 meters.

8. What is the role of the network layer in the OSI reference model?

The network layer is responsible for packet switching, control of network congestion, and data routing. This layer has routers operating under it.

9. Explain OSI and its role in computer networks.

OSI or Open Systems Interconnect is a reference model for data communication. It has seven layers, each defining a particular aspect of how network devices communicate and connect. One layer dictates how data is transmitted, while the other deals with physical media used.

10. Give the disadvantage of the peer-peer network.

As the resources to be accessed are shared by one of the workstations on the network, there is a performance hit.

11. Define ping.

Ping is a utility program that allows us to check connectivity on the network between network devices. A device can be pinged by using its device name(like computer name) or IP address.

12. What is meant by clustering support?

Clustering support is the ability of a network operating system in a fault-tolerant group to connect multiple servers. The primary purpose of clustering is that if one server fails, the processing can continue with the next server in the cluster.

13. How does dynamic host configuration protocol help in network administration?

The network administrator applies the dynamic host configuration protocol to create a pool of IP addresses instead of visiting each client computer to configure a static IP address. This pool is known as the scope that can be assigned to clients dynamically.

14. What do you understand by decoder?

The decoder is a type of circuit that converts the digital signal into an analog signal and encoded data into its original format.

15. Can you tell us about the use of Pseudo TTY?

It is a false terminal allowing external machines to log in or to connect through Telnet. No connection can take place without it.

16. Tell us about the advantages of a Modem.

Some advantages of modem are:

- Its speed depends on the cost
- It is more helpful in connecting LAN with the Internet
- It is the most widely used data communication roadway.

17. Explain Proxy Server and its function.

IP addresses are required for data transmission and are even used by DNS to route to the correct website. Without knowledge of the actual and correct IP address, it is not possible to identify the network's physical location. Proxy servers prevent unauthorized access of IP addresses and make the computer network virtually invisible to external users.

18. What are the characteristics of networking?

The characteristics of networking are:

- Medium- the channel used by computers for communication
- Topology- the way computers are arranged in the network physically or logically
- Protocols- deals with how computers communicate with one another.

19. What do you understand by beaconing?

When a network self-repair its issues, then it is known as beaconing. It is mainly used in Fiber Distributed Data Interface (FDDI) and token ring networks. If a device in the network faces any problem, then the devices that are not receiving any signal are notified. This way, the problem gets repaired within the network.

20. What is SLIP?

SLIP refers to Serial Line Interface Protocol. It is used for transmitting IP datagrams over a serial line.

1. Can you explain what LAN is?

LAN refers to Local Area Network. It is the network between devices located in a remote physical location. It can be either wired or wireless. LANs differ from each other based on given factors:

- Protocol - rules for data transfer
- Media - medium for connecting like twisted pair wires and optic fibers
- Topology - arrangement of nodes in the network

2. What is an anonymous FTP?

Anonymous FTP allows users to access public data. The user need not identify himself to the server, and the login is anonymous. So, while using anonymous FTP, you are required to add 'anonymous' in place of the user id. Anonymous FTPs effectively distribute large files to many people without giving vast numbers of password and username combinations.

3. Tell us about UTP cable.

A UTP cable is made up of copper and has a resistance of 100 ohms. It includes 2-1800 unshielded twisted pairs surrounded by a non-metallic case. These twists provide immunity to EMI and electrical noise.

4. What do you understand by TCP?

Transmission Control Protocol or TCP is a connection-oriented protocol that maintains an established connection between communicating devices until both are done exchanging messages. This protocol is used to determine how application data can be delivered over a network using packets. It also receives and sends packets from and to the network layer and is in charge of flow control.

5. What is meant by NOS?

NOS or Network Operating System is an operating system designed to support databases, workstations, personal computers, and networks. For example, Linux, MAC OS X, Windows Server 2008. These OS provide functionalities such as multiprocessing support, processor support, web services, authentication, etc.

6. Explain piggybacking.

In two-way communication, the receiver sends an acknowledgment to the sender on receiving the data packets. Suppose the receiver does not send the acknowledgment immediately and waits till the network layer passes in the following data packet. In that case, an acknowledgment is attached to the outgoing data frame. This process is known as piggybacking.

7. What do you understand by DHCP?

Dynamic Host Configuration Protocol or DHCP is a network management protocol. DHCP automatically assigns IP addresses to the devices on the network and is used on the UDP/IP networks. In turn, it reduces the need for a network admin to assign IP addresses manually; this further reduces errors.

8. What is the best place to install an antivirus program in a network containing twenty workstations and two servers?

The best option is to install antivirus on all the computers of the network. This will protect all devices from others in case there is a virus inserted into the server.

9. Tell us about IPv6.

IPv6 refers to the Internet Protocol version 6. This is the latest version of the Internet Protocol. Its IP address length is 128 bits which resolve the issue of approaching network addresses shortage.

10. What do you understand by sneakernet?

Sneakernet refers to the unofficial term for transferring electronic information by physically moving media like the USB flash, Floppy disk, optical disks, etc.