TOP 50

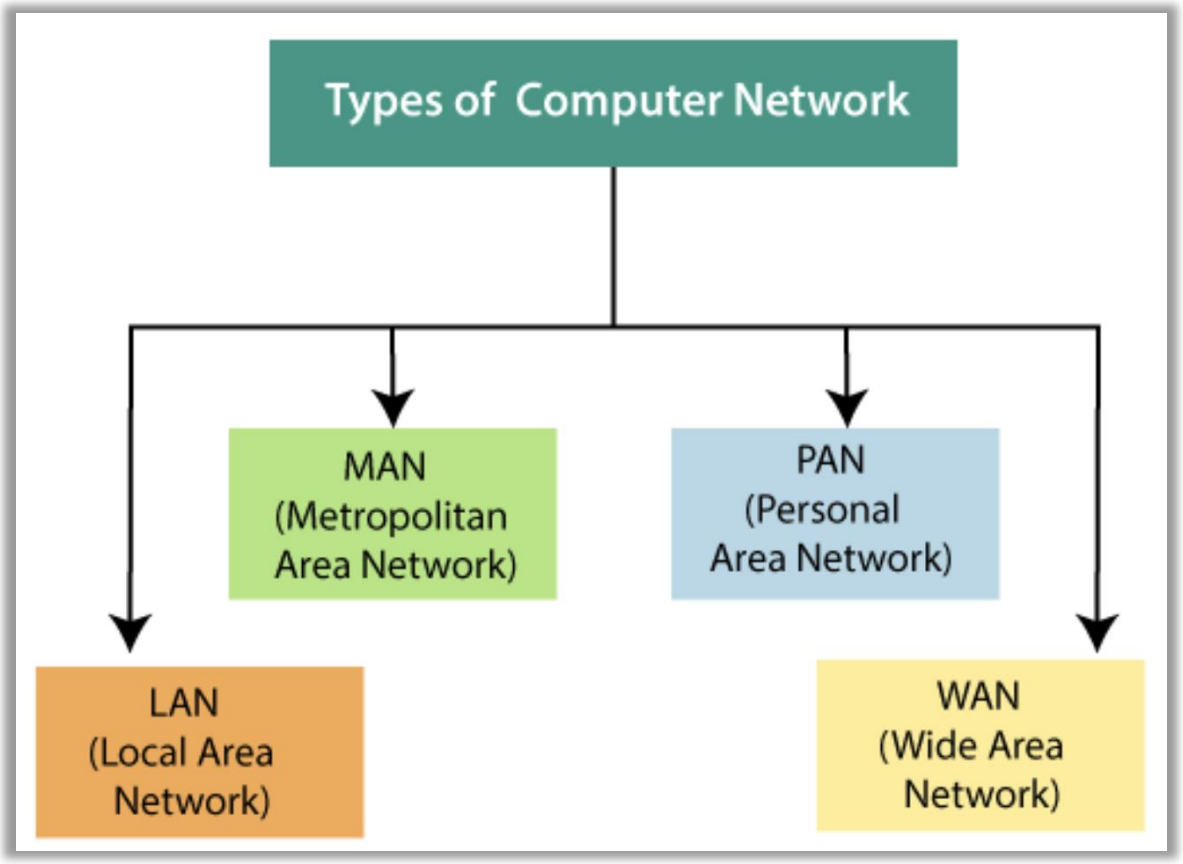
Computer Network

INTERVIEW QUESTION

Created by- TOPPERWORLD

Q 1. Explain different types of networks.

Ans: Below are few types of Network:

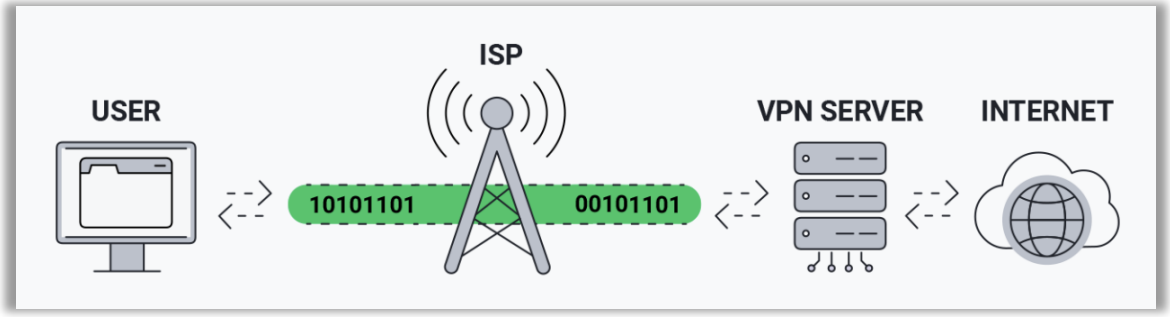


Q 2. What is internetworking ?

Ans: 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 gateways. 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.

Q 3. Tell me something about VPN (Virtual Private Network)

Ans: 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:



Q 4. What are the different types of VPN ?

Ans: 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.

Q 5. Name some services provided by the application layer in the Internet model ?

Ans: 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

Q 6. What is a server farm ?

Ans: 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.

Q 7. Name the three means of user authentication.

Ans: 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.

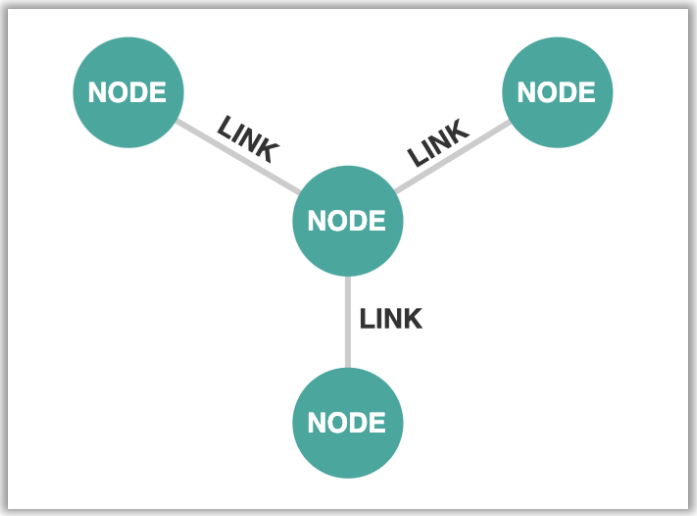
Q 8. What is a zone-based firewall ?

Ans: The A Zone-based firewall is an advanced method of stateful firewall. In a stateful firewall, a stateful database is maintained in which the source IP address, destination IP address, source port number, and 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 are allowed.
Cisco IOS router can be made firewall through two methods:

- 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.
- Using a Zone-based firewall.

Q 9. What are nodes and links ?

Ans: **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.

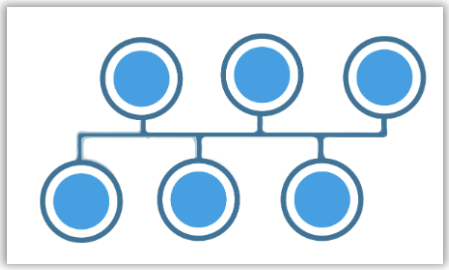


Q 10. What is the network topology and define different types of network topology ?

Ans: 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.
The different types of network topology are given below:

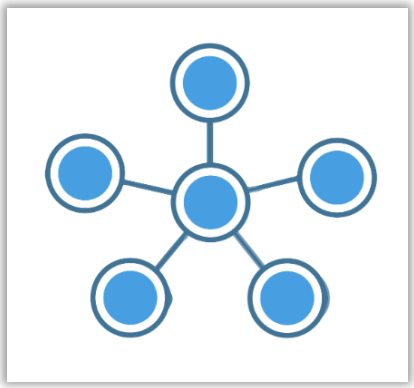
- **Bus Topology:**

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



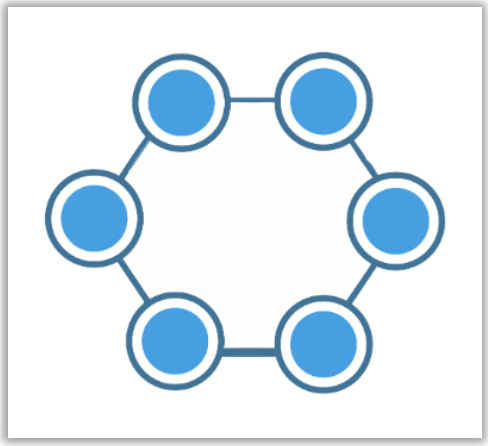
- **Star Topology:**

1. All the nodes are connected to one single node known as the central node.
2. It is more robust.
3. If the central node fails the complete network is damaged.
4. Easy to troubleshoot.
5. Mainly used in home and office networks.



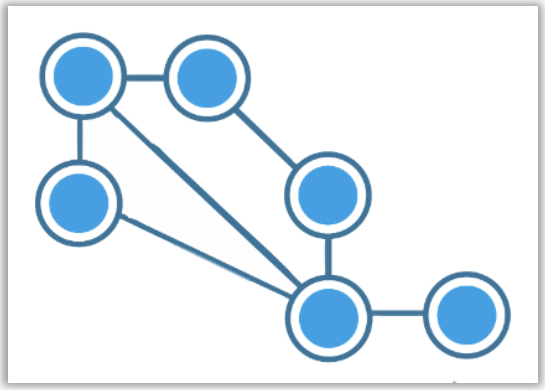
- **Ring Topology:**

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



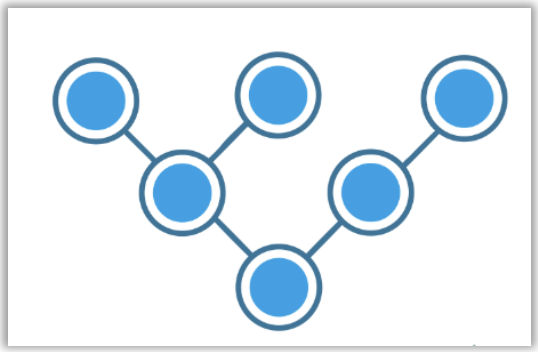
- **Mesh Topology:**

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



- **Tree Topology:**

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



- **Hybrid:**

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

Q 11. What are Private and Special IP addresses ?

Ans: **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.

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.

Q 12. What is Confidentiality, Integrity & Availability ?

Ans: **Confidentiality –** means information is not disclosed to unauthorized individuals, entities, or processes. For example, if we say I have a password for my Gmail account but someone saw it while I was doing login into my Gmail account. In that case, my password has been compromised and Confidentiality has been breached.
Integrity – means maintaining the 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 the status to JOB LEFT so that data is complete and accurate in addition, this is only authorized persons should be allowed to edit employee data.
Availability – means information must be available when needed. For example, if one needs to access information about a particular employee to check whether an employee has outstood the number of leaves, 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.

Q 13. What is Confidentiality, Integrity & Availability ?

Ans: **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.

Q 14. What is a Tunnel mode ?

Ans: 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.

Q 15. What are the HTTP and the HTTPS protocol ?

Ans: **HTTP** is the HyperText Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on the World Wide Web (WWW). It helps the web browsers and web servers for communication. It is a 'stateless protocol' where each command is independent with respect to the previous command. HTTP is an application layer protocol built upon the TCP. It uses port 80 by default.
HTTPS is the HyperText Transfer Protocol Secure or Secure HTTP. It is an advanced and 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.

Q 16. Define Digital Signatures ?

Ans: As the name sounds are the new alternative to signing 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

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

Q 17. What is Authorization ?

Ans: 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.

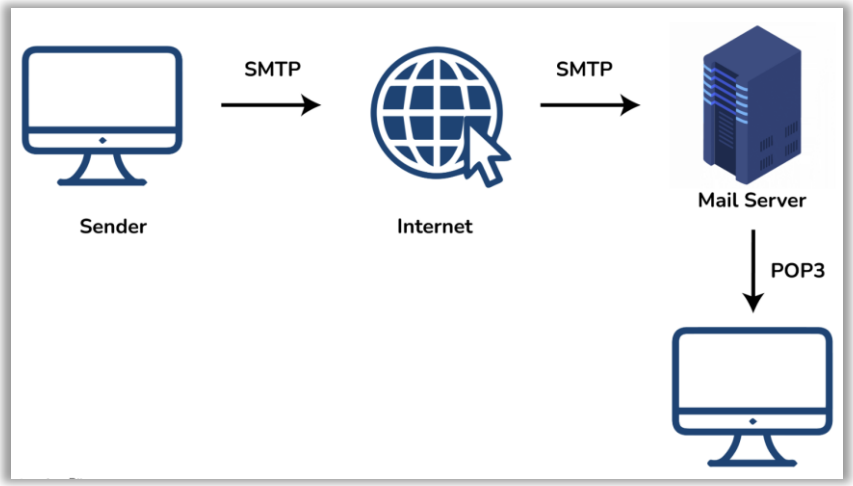
Q 18. What is the difference between IPS and a firewall?

Ans: 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.

Q 19. What is the SMTP protocol ?

Ans: SMTP is the Simple Mail Transfer Protocol. SMTP sets the rule for communication between servers. This set of rules helps the software to transmit emails over the internet. It supports both End-to-End and Store-and-Forward methods. It is in always-listening mode on port 25.



Q 20. What is IP Spoofing ?

Ans: **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.

Q 21. What is the DNS ?

Ans: IP 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.

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

Ans: **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.

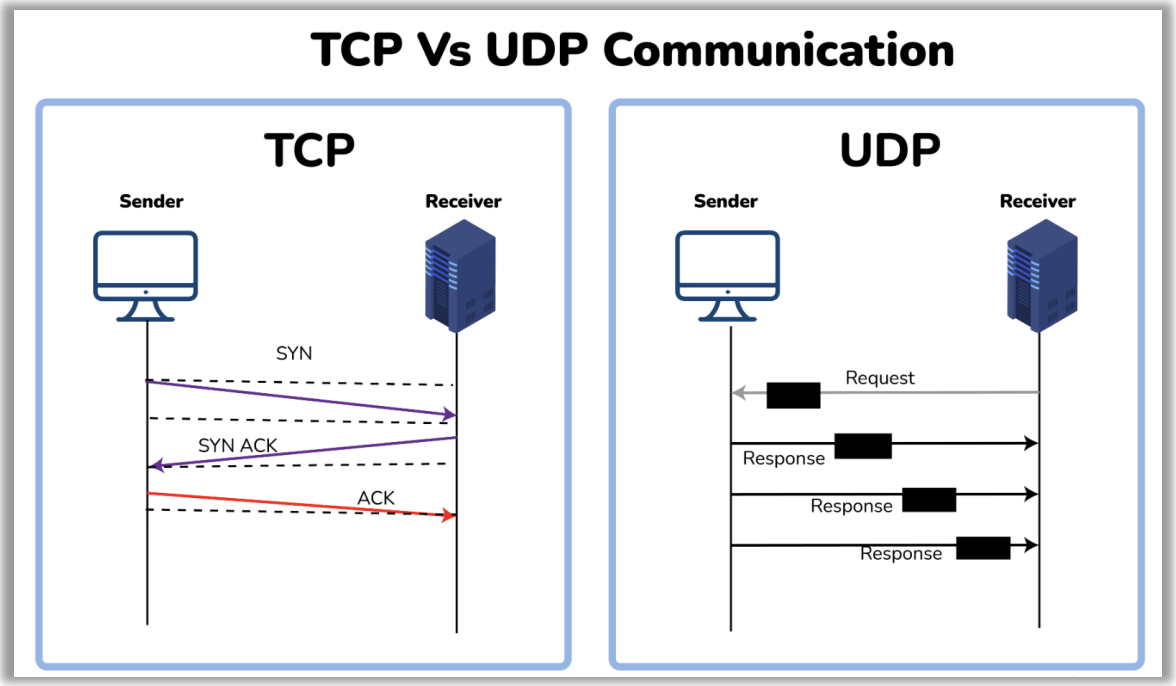
Q 23. What is the use of a router and how is it different from a gateway ?

Ans: 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.

Q 24. What is the TCP and UDP protocol and difference between them ?

Ans: **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.
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.

TCP	UDP
Sequenced	Unsequenced
Reliable	Unreliable
Connection-oriented	Connectionless
Virtual circuit	Low overhead
Acknowledgements	No acknowledgements
Windowing flow control	No windowing or flow control



Q 25. What are the Advantages of Fiber Optics ?

Ans: The advantages of Fiber Optics are mentioned below:

- 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, and 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 wires 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.

Q 26. What is the ICMP protocol ?

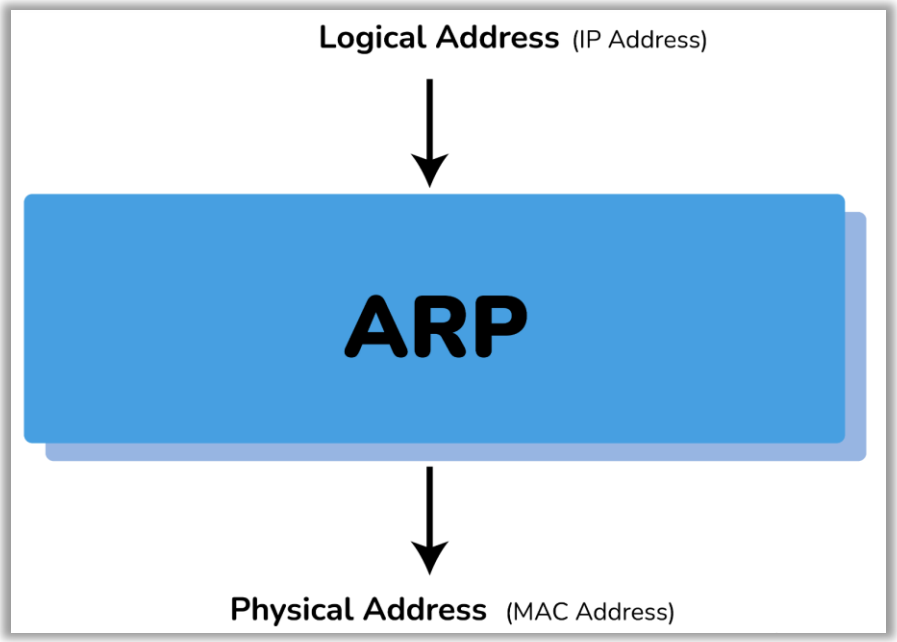
Ans: ICMP is the Internet Control Message Protocol. It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting and testing if the data is reaching the preferred destination in time.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

Q 27. What do you mean by the DHCP and ARP Protocol?

Ans: **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.

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.



Q 28. What is Multicast ?

Ans: 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.

Q 29. What is CGMP (Cisco Group Management Protocol) ?

Ans: 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 them. 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 Bluetoothso 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)

Q 30. What is the difference between Bluetooth and WIFI ?

Ans:

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

Q 31. What is the MAC address and how is it related to NIC ?

Ans: 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.

Q 32. Differentiate the MAC address with the IP address.

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

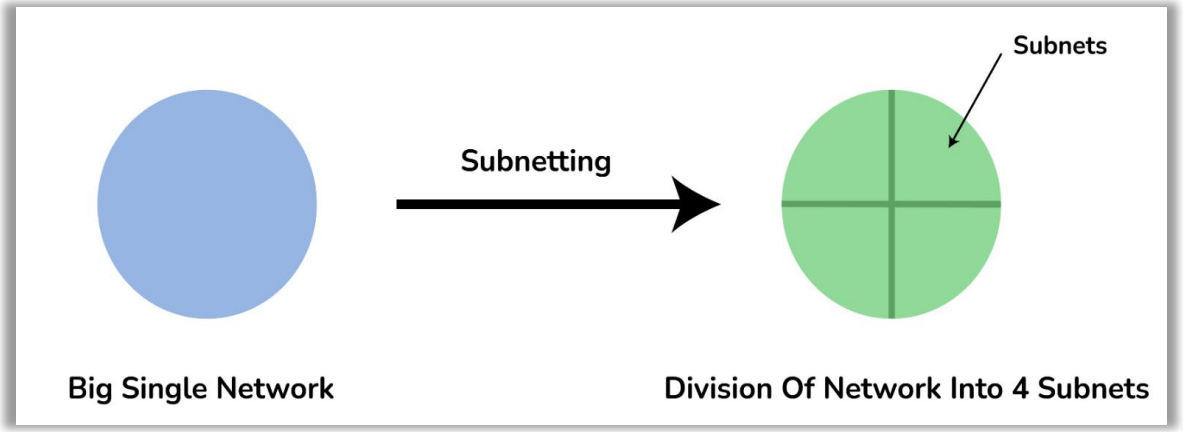
MAC Address	IP Address
Media Access Control Address	Internet Protocol Address
6 or 8-byte hexadecimal number	4 (IPv4) or 16 (IPv6) Byte address
It is embedded with NIC	It is obtained from the network
Physical Address	Logical Address
Operates at Data Link Layer	Operates at Network Layer.
Helps to identify the device	Helps to identify the device connectivity on the network.

Q 33. What is a reverse proxy ?

Ans: **Reverse Proxy Server:** The job of a reverse proxy server is 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 particular servers.

Q 34. What is a subnet ?

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



Q 35. Define piggybacking ?

Ans: 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.

Q 36. What are the advantages and disadvantages of piggybacking ?

Ans: **Advantages of Piggybacking**

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

Disadvantages of Piggybacking

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.

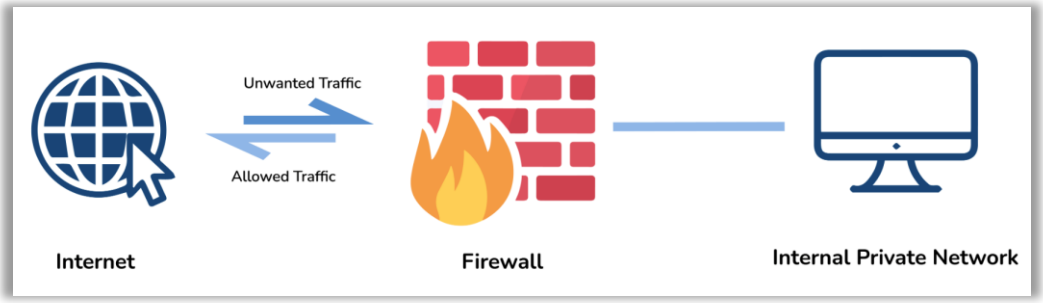
Q 37. Compare the hub vs switch.

Ans:

HUB	SWITCH
1). HUB is a broadcasting device.	1). SWITCH is a point to point communication device.
2).HUB operates at physical layer of OSI Model.	2).SWITCH operates at Data link layer of OSI model.
3).It is not an intelligent device, so it is cheap.	3).SWITCH is an intelligent device ,so it is an expensive.
4).HUB cannot act as REPEATER(that is generates the original bit pattern).	4).SWITCH can be used as REPEATER to regenerate the original bit pattern.
5).HUB simply broadcast the incoming packet.	5).SWITCH uses switching table to find out the current destination.

Q 38. What is the firewall ?

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



Q 39. What are Unicasting, Anycasting, Multicasting and Broadcasting ?

Ans: **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.

Q 40. What happens when you enter google.com in the web browser ?

Ans:

- 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.

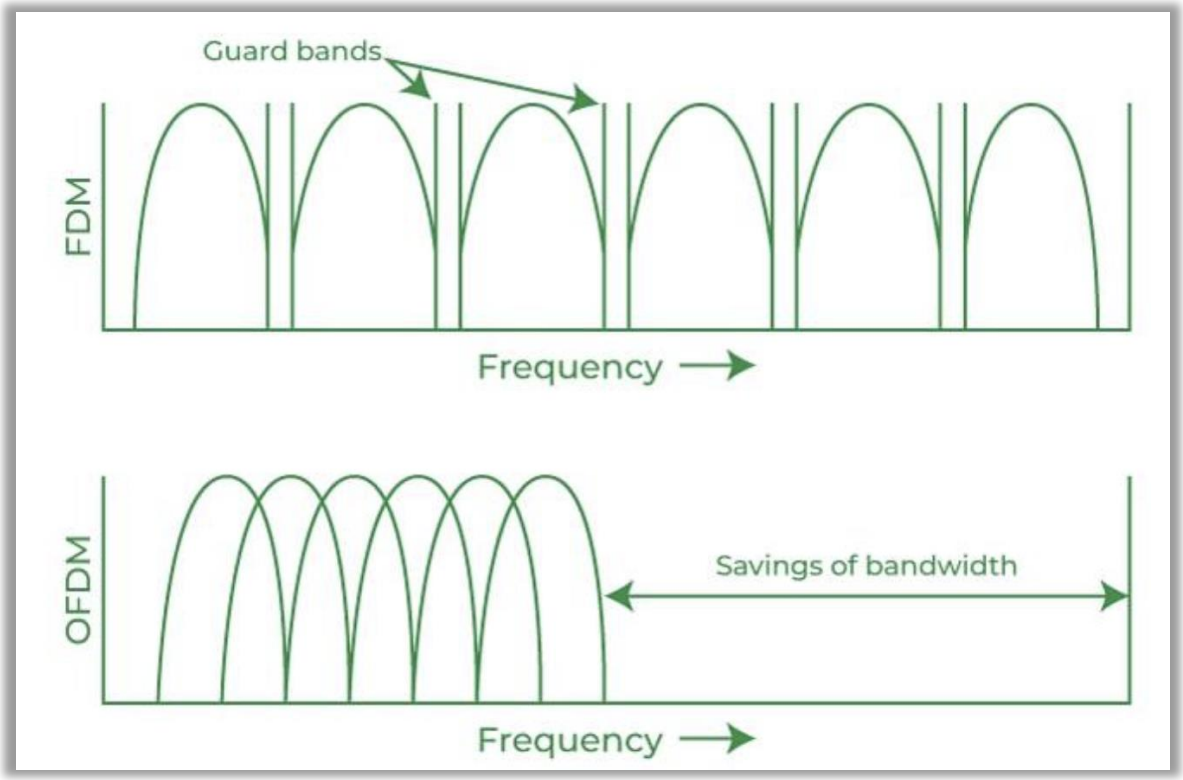
Q 41. What is the difference between the ipconfig and the ifconfig ?

Ans:

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	

Q 42. Define the term OFDM ?

Ans: OFDM stands for Orthogonal Frequency Division Multiplexing. 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.



Q 43. What is a transparent bridge ?

Ans: **Transparent Bridge:** A transparent bridge automatically maintains a routing table and updates tables in response to maintaining 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 the hosts. In all the cases, transparent bridges flooded the broadcast and multicast frames.

Q 44. What is the FTP protocol ?

Ans: 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.

Q 45. Describe the OSI Reference Model

Ans: 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.

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

Ans: 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 of Bluetooth which Bluetooth 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

Q 47. Why do we need the pop3 protocol for e-mail ?

Ans: **Need of POP3:** The Post Office Protocol (POP3) is the most widely used protocol and is 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.

Q 48. Define the term Jitter ?

Ans: Jitter is a "packet delay variance". It can simply mean that jitter is considered 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.

Q 49. Why Bandwidth is important to network performance parameters ?

Ans: 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 50. What is the minimum size of the icmpV4 packet what is the maximum size of the icmpv4 packet ?

Ans:

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

"UNLOCK YOUR POTENTIAL"

With- TOPPERWORLD

Explore More

topperworld.in

DSA TUTORIAL

C TUTORIAL

C++ TUTORIAL

JAVA TUTORIAL

PYTHON TUTORIAL

Follow Us On

E-mail

topperworld.in@gmail.com