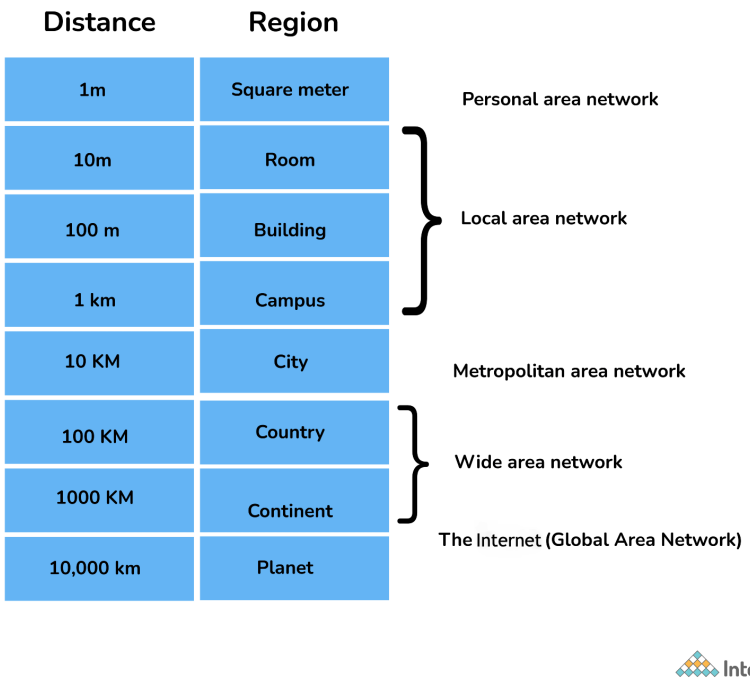
(41 questions)

Basic Networking Interview Questions

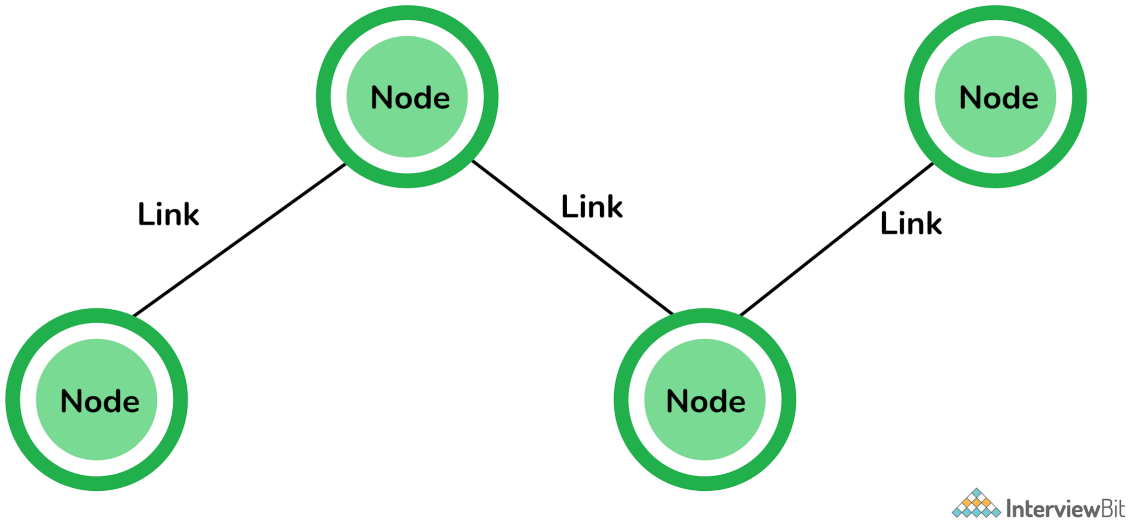
1. How are Network types classified?



2. What are nodes and links?

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

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



Nodes and Links

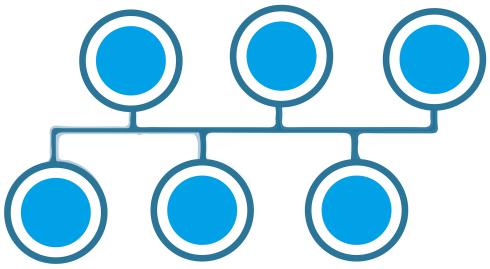
3. What is the network topology?

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.

4. Define different types of network topology

The different types of network topology are given below:

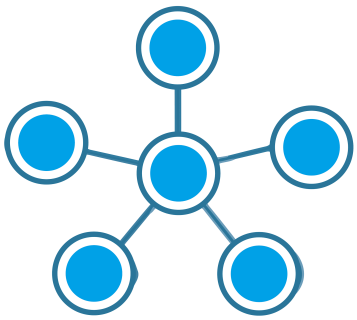
Bus Topology:



Bus Topology

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

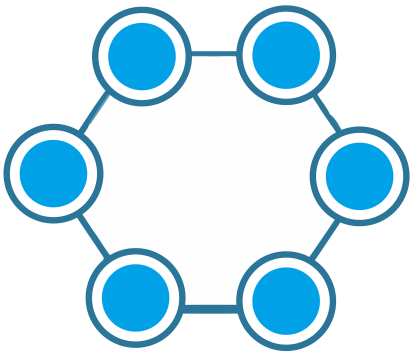
Star Topology:



Star Topology

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

Ring Topology:



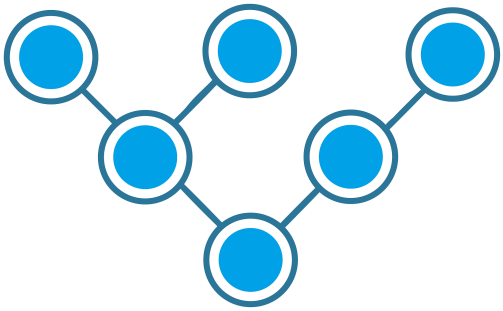
Ring Topology

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

Mesh Topology

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

Tree Topology:



Tree Topology

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

Hybrid:

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

5. 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

6. 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.

Intermediate Interview Questions

7. 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.

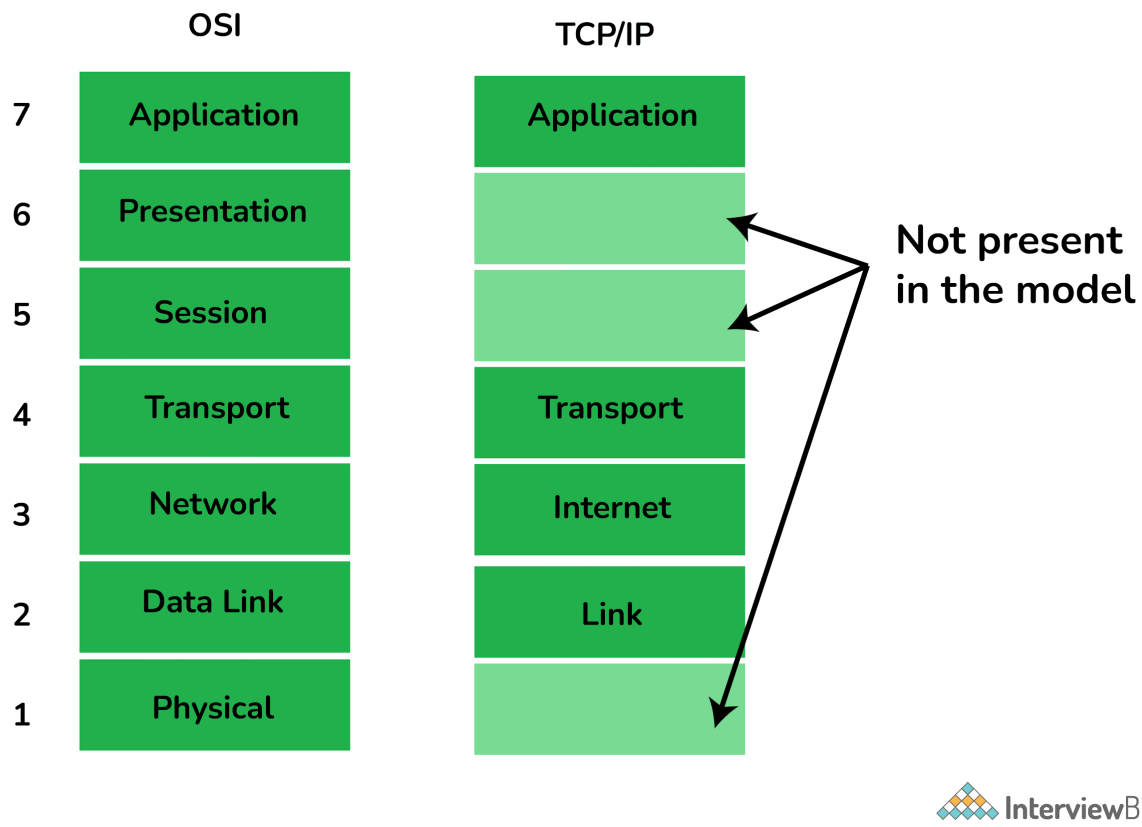
The OSI model has seven layers. The principles used to arrive at the seven layers can be summarized briefly as below:

- 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.

8. 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).

9. 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

10. 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.

11. What is the SMTP protocol?

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

12. What 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.

13. 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.

Advanced Interview Questions

14. 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.

15. 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.

16. Compare between TCP and UDP

TCP/IP	UDP
Connection-Oriented Protocol	Connectionless Protocol
More Reliable	Less Reliable
Slower Transmission	Faster Transmission
Packets order can be preserved or can be rearranged	Packets order is not fixed and packets are independent of each other

Uses three ways handshake model for connection	No handshake for establishing the connection
TCP packets are heavy-weight	UDP packets are light-weight
Offers error checking mechanism	No error checking mechanism
Protocols like HTTP, FTP, Telnet, SMTP, HTTPS, etc use TCP at the transport layer	Protocols like DNS, RIP, SNMP, RTP, BOOTP, TFTP, NIP, etc use UDP at the transport layer

17. 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.

18. 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.

19. 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.

20. 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.

21. Differentiate the MAC address with the IP address

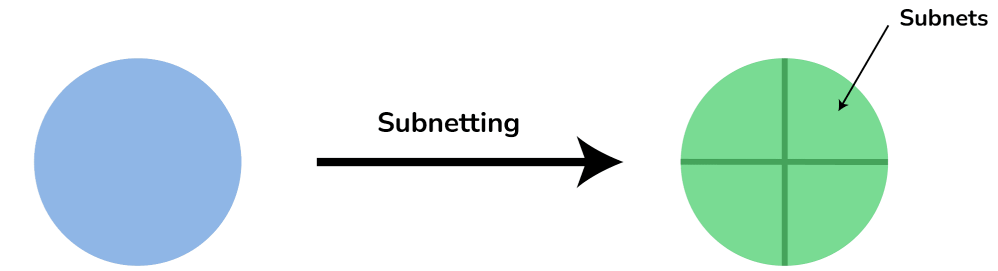
The difference between MAC address and IP address are as follows:

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.

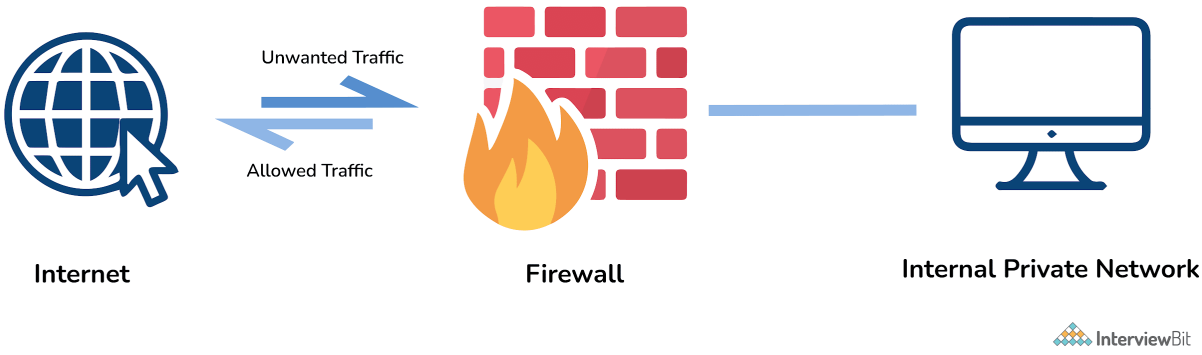
22. What is a subnet?

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.



23. 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

24. 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.

25. 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.

26) 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.

---

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

There are mainly two security affecting factors:

- Unauthorized Access
- Viruses

---

28) 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

---

29) 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

---

30) 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.

---

31) 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.

---

32) 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.

---

33) 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.

---

34) 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.

---

35) What is RAID?

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

---

36) 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.

---

37) What is protocol?

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

---

38) What is netstat?

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

---

39) 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.

---

40) 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.

---

41. 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.