Most Asked Computer Network Interview Questions

Network:

An inter-connection of multiple devices known as host, that are connected using multiple paths for the purpose of sending/receiving data.

Network Topology:

Layout arrangement of different devices in a network.

Types of Topology:

1. Star -- Star topology is a network topology in which all the nodes are connected to a single device known as a central device
2. 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.
3. 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.
4. Mesh -- Mesh topology is a network topology in which all the nodes are individually connected to other nodes.

Bandwidth:

Bandwidth is defined as the potential of the data that is to be transferred in a specific period of time. It is the data carrying capacity of the network or transmission medium.

LAN:

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. A LAN typically

relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN.

VPN:

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

Advantages of VPN:

1. VPN is used to connect offices in different geographical locations remotely
2. VPN encrypts the internet traffic and disguises the online identity
3. VPN can be also used to bypass geographical locations.

IPv4 Address:

An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. IP addresses are displayed as a set of four digits. The total IP address range ranges from 0.0.0.0 to 255.255.255.255. Example - 192.158.02.252

Differences between IPv4 and IPv6:

IPv4	IPv6
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided

HTTP and HTTPS:

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.

DHCP:

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.

ARP:

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.

Media Access Control (MAC) Address:

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC is a type og physical address which is used to communicate or transfer the data from one computer to another computer

---

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.

Layers in OSI model:

It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

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.

1. **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 attaches 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.

1. **Network Layer** :

- Network layer converts the logical address into the physical address.
- 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.

1. **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.

1. **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

1. **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

1. **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.

TCP/IP Model:

It is a compressed version of the OSI model with only 4 layers. It stands for Transmission Control Protocol/Internet Protocol. The layers are:

- Process/Application Layer
- Host-to-Host/Transport Layer
- Internet Layer
- Network Access/Link Layer

TCP 3-Way Handshake Process:

- Step 1 (SYN) : In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that client is likely to start communication and with what sequence number it starts segments with
- Step 2 (SYN + ACK): Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of segment it received and SYN signifies with what sequence number it is likely to start the segments with
- Step 3 (ACK) : In the final part client acknowledges the response of server and they both establish a reliable connection with which they will start eh actual data transfer.

What happens when you hit an URL: (THIS IS THE MOST IMP QUESTION OF ALL)

- A URL may contain a request to HTML, image file or any other type.
- If the content of the typed URL is in the cache and fresh, then display the content.
- Else find the IP address for the domain so that a TCP connection can be set up. Browser does a DNS lookup.

- Browser needs to know the IP address for a URL so that it can set up a TCP connection. This is why browser needs DNS service. The browser first looks for URL-IP mapping browser cache, then in OS cache. If all caches are empty, then it makes a recursive query to the local DNS server. The local DNS server provides the IP address.
- Browser sets up a TCP connection using three-way handshake.
- Browser sends a HTTP request.
- Server has a web server like Apache, IIS running that handles incoming HTTP request and sends an HTTP response.
- Browser receives the HTTP response and renders the content.