What is the OSI model?

OSI stands for Open System Interconnection is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

Explain the different layers of the OSI model
There are the seven OSI layers. Each layer has different functions to perform. All these seven layers work collaboratively to transmit the data from one layer to another. A list of seven layers are given below:

- Physical Layer
- Data-Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Layer 7 – The Application Layer
Layer 7 is the layer most people are familiar with because it communicates directly with the user. An application that runs on a device might communicate with other OSI layers, but the interface runs on layer 7. For instance, an email client that transfers messages between client and server runs on layer 7. When a message is received on the client software, the application layer is what presents it to the user. Application protocols include SMTP (Simple Mail Transfer Protocol) and HTTP, which is the protocol for communication between browsers and web servers.

Layer 6 – The Presentation Layer
We mentioned that the application layer displays information to users, but the presentation layer of the OSI model is what prepares data so that it can be displayed to the user. It’s common for two different applications to use encoding. For instance, communicating with a web server over HTTPS uses encrypted information. The presentation layer is responsible for encoding and decoding information so that it can be displayed in plaintext. The presentation layer is also

responsible for compressing and decompressing data as it travels from one device to another.

Layer 5 – The Session Layer

To communicate between two devices, an application must first create a session. A session is unique to the user and identifies them on the remote server. The session must be open long enough for data to be transferred but still closed after the transfer is complete. When large volumes of data are transferred, the session is responsible for ensuring that the file is completely transferred, and retransmission is established, should the data be incomplete. For instance, if 10MB of data is transferred and only 5MB completes, the session layer ensures that only 5MB is retransferred. This transfer makes communication over a network more efficient instead of wasting resources and transferring the entire file again.

Layer 4 – The Transport Layer

The transport layer is responsible for taking data and breaking it up into smaller chunks. When data is transferred across a network, it is not transferred as one packet. To make transfers more efficient and faster, the transport layer breaks data into smaller segments. These smaller segments contain header information that can be reassembled at the target device. Segmented data also has error control to tell the session layer to reestablish a connection should packets fail to fully transfer to the target recipient.

Layer 3 – The Network Layer

The network layer is responsible for breaking up the data on the sender's device and reassembling it on the recipient's device when the transmission is across two different networks. When communicating within the same network, the network layer is unnecessary, but most users connect to other networks, such as cloud networks. When data travels across different networks, the network layer is responsible for creating small data packets routed to their destination and then rebuilt on the recipient's device.

Layer 2 – The Data Link Layer

The network layer facilitates communication across different networks, but the data link layer is responsible for transferring information on the same network. The data link layer turns packets received from the network layer into frames.

Just like the network layer, the data link layer is responsible for error control and flow to ensure successful transmission.

Layer 1 – The Physical Layer
Just as the name suggests, the physical layer is responsible for the equipment that facilitates data transfer, such as cables and routers installed on the network. This layer is one aspect of network transmission, where standards are essential. Without standards, transmission across different manufacturer devices is impossible.

What do you mean by the TCP/IP Model?

TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together. The purpose of the TCP/IP model is to allow communication over large distances.

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP Stack is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

Advantages of the TCP/IP model

- It operates independently of the operating system.
- It supports many routing-protocols.
- It enables the internetworking between the organizations.
- It can be used to establish a connection between two computers.

Disadvantages of the TCP/IP model

- TCP/IP is a complicated model to set up and manage.
- In this model the transport layer does not guarantee delivery of packets.
- Replacing protocol in TCP/IP is not easy.
- It has no clear separation from its services, interfaces, and protocols.

What do you mean by HTTP, TCP and UDP

HTTP (HyperText Transfer Protocol)
The communications protocol used to connect to Web servers on the Internet or on a local network (intranet). The primary function of HTTP is to establish a connection with the server and send HTML pages back to the user's browser. It is also used to download data from the server either to the browser or to any requesting application that uses HTTP.

TCP (Transmission Control Protocol)
It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

UDP (The User Datagram Protocol)
Is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves a minimum amount of communication mechanisms. UDP is said to be an unreliable transport protocol but it uses IP services which provide the best effort delivery mechanism.
In UDP, the receiver does not generate an acknowledgement of the packet received and in turn, the sender does not wait for any acknowledgement of the packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

What is a Firewall?

A firewall can be defined as a special type of network security device or a software program that monitors and filters incoming and outgoing network traffic based on a defined set of security rules. It acts as a barrier between internal private networks and external sources (such as the public Internet).

The primary purpose of a firewall is to allow non-threatening traffic and prevent malicious or unwanted data traffic for protecting the computer from viruses and attacks. A firewall is a cybersecurity tool that filters network traffic and helps users block malicious software from accessing the Internet in infected computers.

Explain DNS

The domain name system (i.e., “DNS”) is responsible for translating domain names into a specific IP address so that the initiating client can load the requested Internet resources. The domain name system works much like a phone book where users can search for a requested person and retrieve their phone number. DNS servers translate requests for specific domains into IP addresses, controlling which server users with access when they enter the domain name into their browser.

To put it simply, DNS helps direct traffic on the Internet by connecting domain names with actual web servers. Essentially, it takes a human-friendly request for a domain name like damola.com – and translates it into a computer-friendly server IP address like “216.3.128.12”.

How Does DNS Work?

When a user enters a URL in their web browser, DNS gets to work to connect that URL to the IP address of the actual server. This is called DNS name resolution and involves a DNS recursor querying various nameservers to figure out the actual IP address of a server.

DNS is primarily concerned with four components:

- Domain Registrar(GoDaddy or Namecheap): The domain must be registered with a domain registrar.
- Nameservers: Nameservers must be specified by the domain registrar.
- DNS Records(A,CNAME,MX,TXT): DNS records must be added to the nameservers specified by the domain registrar
- Web-based services (such as website hosting and email): The DNS records must be fully propagated to associate the domain with each relevant web service.