1. Illustrate the architecture of ISO-OSI model with neat diagram by mentioning Protocols at each layer.

OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.

OSI consists of seven layers, and each layer performs a particular network function

OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.

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

The OSI model is divided into two categories:   
 upper layers   
 lower layers.

The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software.  
The lower layer of the OSI model deals with the data transport issues.

Physical layer

* It is the lowest layer of the OSI model.
* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It establishes, maintains and deactivates the physical connection.
* Network devices used in physical layer were Hub, NIC, Cable

### Data-Link Layer

This layer is responsible for the error-free transfer of data frames.  
It provides a reliable and efficient communication between two or more devices.  
It is mainly responsible for the unique identification of each device that resides on a local network.

The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

### Network Layer

It is a layer 3. that manages device addressing, tracks the location of devices on the network.  
 It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.  
 The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6  
 Network devices used in Network layer were Router

### Transport Layer

The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.  
 The main responsibility of the transport layer is to transfer the data completely.  
 It receives the data from the upper layer and converts them into smaller units known as segments.  
 This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

### Session Layer

The session layer is the fifth layer, which controls the connections between multiple computers.  
 The session layer tracks the dialogs between computers, which are also called sessions.  
 This layer establishes controls and ends the sessions between local and remote applications.

Presentation Layer

A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.  
 It acts as a data translator for a network.  
 This layer is a part of the operating system that converts the data from one presentation format to another format.  
 The Presentation layer is also known as the syntax layer.

Application Layer

An application layer serves as a window for users and application processes to access network service.  
 It handles issues such as network transparency, resource allocation, etc.  
 An application layer is not an application, but it performs the application layer functions.  
 This layer provides the network services to the end-users.

1. Discuss DHCP protocol in detail  
    Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to any device, or node on a network so they can communicate using IP (Internet Protocol)

DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices.

DHCP can be implemented on local networks as well as large enterprise networks.

DHCP maintains the unique IP address of the host using a DHCP server.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

**Components of DHCP**

* DHCP Server
* DHCP client
* IP address pool
* Subnet
* Lease
* DHCP relay

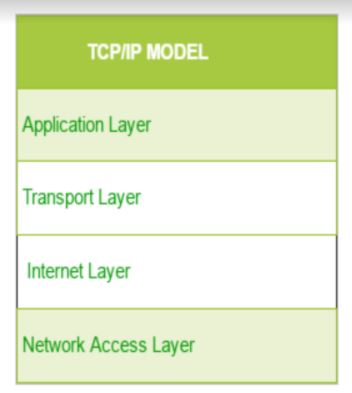
1. **Illustrate the various layers of TCP/IP along with protocols at each layer with a neat diagram.**

TCP stands for 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.

**The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:**



**Application Layer**

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer.  
 It is responsible for node-to-node communication and controls user-interface specifications  
 Some of the protocols present in this layer are: HTTP, HTTPS, FTP, SMTP.

**Network Access Layer**

It is responsible for end-to-end communication and error-free delivery of data.  
 It shields the upper-layer applications from the complexities of data.

The two main protocols present in this layer are

**Transmission Control Protocol (TCP)** – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism.

**User Datagram Protocol (UDP)** – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

**Internet Layer**

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network.

The main protocols residing at this layer are

**IP** – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:  
 IPv4   
 IPv6.

**ARP** – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

**The Network Interface Layer**

Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer.   
 It helps you to defines details of how data should be sent using the network.  
 This layer is responsible for the transmission of the data between two devices on the same network.

1. **Discuss IPV4 and IPV6 protocols in detail**

An IP stands for internet protocol. An IP address is assigned to each device connected to a network.  
 Each device uses an IP address for communication.  
 It also behaves as an identifier as this address is used to identify the device on a network. It defines the technical format of the packets.

**There are two types of IP addresses:**

* IPv4
* IPv6

**IPv4**

IPv4 is a version 4 of IP. It is a current version and the most commonly used IP address.  
 It is a 32-bit address written in four numbers separated by 'dot', i.e., periods. This address is unique for each device.  
 IP address in which each group of numbers separated by periods is called an Octet. Each number in an octet is in the range from 0-255.

**IPv6**

IPv4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong.  
 IPv6 is the next generation of IP addresses.  
 The main difference between IPv4 and IPv6 is the address size of IP addresses.  
 The IPv4 is a 32-bit address, whereas IPv6 is a 128-bit hexadecimal address. IPv6 provides a large address space, and it contains a simple header as compared to IPv4.

It provides transition strategies that convert IPv4 into IPv6, and these strategies are as follows:

**Dual stacking**: It allows us to have both the versions, i.e., IPv4 and IPv6, on the same device.

**Tunneling**: In this approach, all the users have IPv6 communicates with an IPv4 network to reach IPv6.

**Network Address Translation:** The translation allows the communication between the hosts having a different version of IP.

1. **Address Resolution Protocol (ARP) and its types**

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address.   
 This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet.

There are four types of Address Resolution Protocol, which is given below:

* Proxy ARP
* Gratuitous ARP
* Reverse ARP (RARP)
* Inverse ARP
* **Proxy Arp**

If Host A wants to transmit data to Host B, which is on the different network, then Host A sends an ARP request message to receive a MAC address for Host B. The router responds to Host A with its own MAC address pretend itself as a destination. When the data is transmitted to the destination by Host A, it will send to the gateway so that it sends to Host B. This is known as proxy ARP.

* **Gratuitous ARP**
  + The gratuitous ARP is used to update the ARP table of other devices.
  + It also checks whether the host is using the original IP address or a duplicate one.
* **Reverse ARP (RARP)**

It is a networking protocol used by the client system in a local area network (LAN) to request its IPv4 address from the ARP gateway router table.

A table is created by the network administrator in the gateway-router that is used to find out the MAC address to the corresponding IP address.

* **Inverse ARP**

Inverse ARP is inverse of the ARP, and it is used to find the IP addresses of the nodes from the data link layer addresses.

These are mainly used for the frame relays, and ATM networks.