**Important Keypoints for Networking**

**What is a network?**

A computer network is a group of interconnected devices that are designed to communicate and share information with each other.

**Uses of computer networks**

1. **Resource Sharing**: Computer networks allow for the sharing of hardware resources such as printers, scanners, and storage devices. This enables multiple users to access and utilize these resources efficiently, reducing costs and improving productivity.
2. **Communication**: Networks facilitate communication between individuals, organizations, and devices. They enable the exchange of data, messages, and information through various communication channels such as email, instant messaging, video conferencing, and voice calls.
3. **Information Access**: Computer networks provide access to vast amounts of information stored on servers, databases, and other networked resources. Users can retrieve, share, and collaborate on data and information resources regardless of their physical location.
4. **Centralized Management**: Networks allow for centralized management of resources, security policies, and configurations. Centralized management simplifies administration tasks, enhances security, and ensures consistency across the network infrastructure.
5. **Remote Access**: Networks enable remote access to resources and services from anywhere with an internet connection. Users can remotely connect to their organization's network, access files, applications, and other resources securely, enhancing flexibility and productivity.

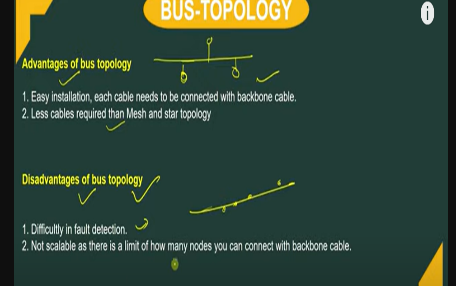
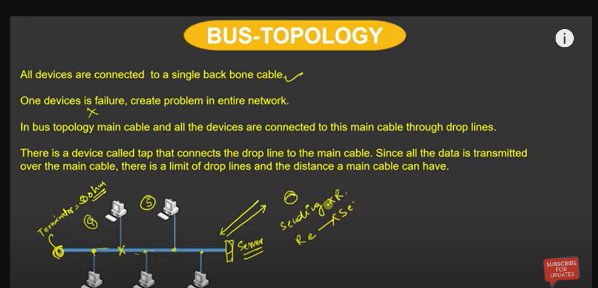
**Types of networks**

1. **Local Area Network (LAN)**:
   * LANs connect devices over a limited geographical area, typically within a single building or campus.
   * They are commonly used in homes, offices, schools, and small businesses.
   * LANs facilitate resource sharing, communication, and centralized management within the local area.
2. **Metropolitan Area Network (MAN)**:
   * MANs cover a larger geographical area than LANs but are smaller than WANs, typically spanning across a city or metropolitan area.
   * They connect multiple LANs and other network devices over a broader geographic region.
   * MANs are often used by large organizations or service providers to interconnect their facilities or provide high-speed connectivity within a city.
3. **Wide Area Network (WAN)**:
   * WANs span large geographical distances, connecting devices across cities, countries, or even continents.
   * They utilize various communication technologies such as leased lines, satellites, and optical fibers to establish connections between distant locations.
   * WANs enable organizations to connect remote offices, branches, and data centers, facilitating data exchange and access to centralized resources over long distances.
4. **Personal Area Network (PAN)**:
   * PANs are used for connecting personal devices over a very short range, typically within a person's workspace or immediate vicinity.
   * Common PAN technologies include Bluetooth and Wi-Fi Direct, allowing devices like smartphones, tablets, laptops, and wearable gadgets to communicate and share data wirelessly.
   * PANs enable personal device connectivity, file sharing, and peripheral device interaction within a small area.

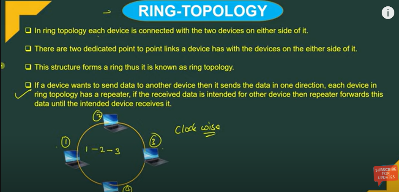
**Network Topologies**

A network topology refers to how devices are connected in a network.

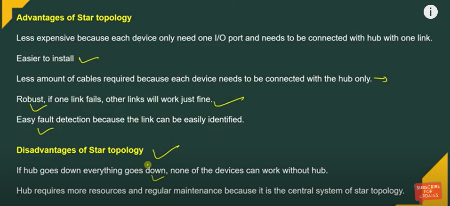
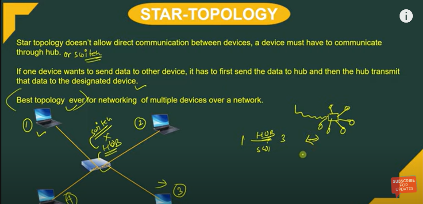
1. Bus:-



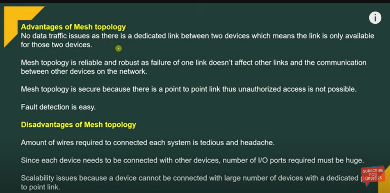
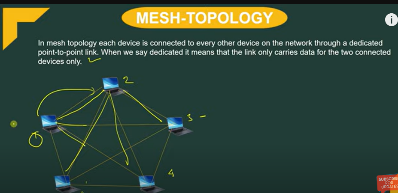
1. Ring:-



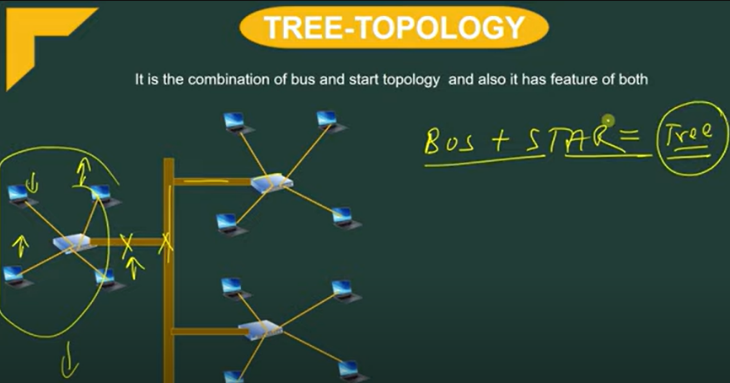
1. Star:-



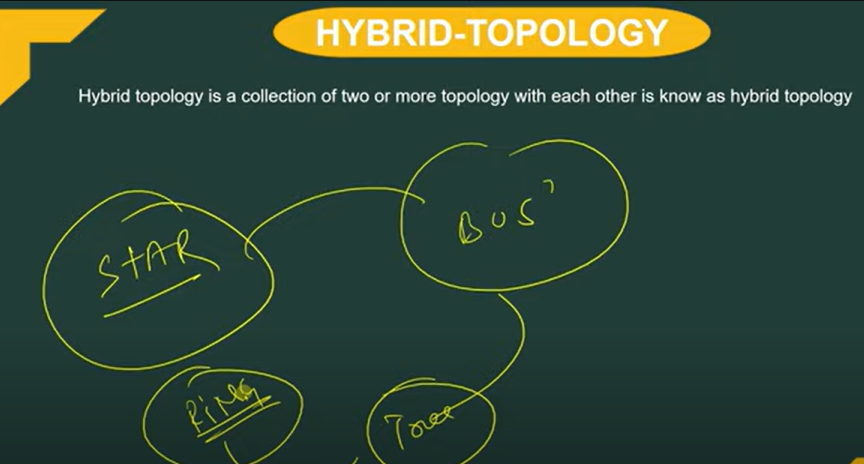
1. Mesh:-



1. Tree:-



1. Hybrid:-



**OSI Model**

The OSI (Open Systems Interconnection) model is a conceptual framework for understanding how computer networks work. It is composed of seven layers, each of which serves a specific purpose in the communication process. OSI model was developed by **ISO – ‘International Organization for Standardization**‘, in the year 1984.

The layers are: Layer 1—Physical;

Layer 2—Data Link;

Layer 3—Network;

Layer 4—Transport;

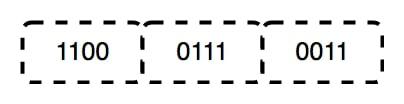
Layer 5—Session;

Layer 6—Presentation;

Layer 7—Application.

**Physical Layer – Layer 1**

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of**bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



**Functions of the Physical Layer**

* **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
* **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
* **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
* **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

***Note:***

1. *Hub, Repeater, Modem, and Cables are Physical Layer devices.*
2. *Network Layer, Data Link Layer, and Physical Layer are also known as****Lower Layers****or****Hardware Layers****.*

**Data Link Layer (DLL) – Layer 2**

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.   
The Data Link Layer is divided into two sublayers:

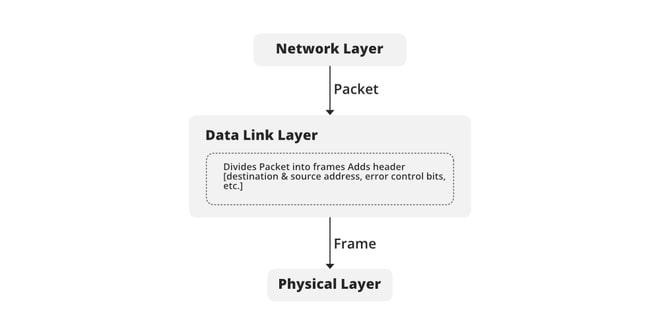
1. [Logical Link Control (LLC)](https://www.geeksforgeeks.org/logical-link-control-llc-protocol-data-unit/)
2. [Media Access Control (MAC)](https://www.geeksforgeeks.org/introduction-of-mac-address-in-computer-network/)

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an [ARP(Address Resolution Protocol)](https://www.geeksforgeeks.org/how-address-resolution-protocol-arp-works/)request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

**Functions of the Data Link Layer**

* **Framing:**Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
* **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
* **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
* **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
* **Access control:**When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.



***Note:***

1. *Packet in the Data Link layer is referred to as****Frame.***
2. *Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
3. *Switch & Bridge are Data Link Layer devices.*

**Network Layer – Layer 3**

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer.

**Functions of the Network Layer**

* **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
* **Logical Addressing:**To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

***Note:***

1. *Segment in the Network layer is referred to as****Packet****.*
2. *Network layer is implemented by networking devices such as routers and switches.*

**Transport Layer – Layer 4**

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

**At the sender’s side:**The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

***Note:****The sender needs to know the port number associated with the receiver’s application.*

*Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.*

***At the receiver’s side:****Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.*

**Functions of the Transport Layer**

* **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
* **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

**Services Provided by Transport Layer**

1. [Connection-Oriented Service](https://www.geeksforgeeks.org/connection-oriented-service/)
2. [Connectionless Service](https://www.geeksforgeeks.org/connection-less-service/)

**1. Connection-Oriented Service:** It is a three-phase process that includes

* Connection Establishment
* Data Transfer
* Termination/disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

**2. Connectionless service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

***Note:***

1. *Data in the Transport Layer is called****Segments****.*
2. *Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*
3. *The transport layer is called as****Heart of the OSI****model.*
4. ***Device or Protocol Use :****TCP, UDP  NetBIOS, PPTP*

**Session Layer – Layer 5**

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

**Functions of the Session Layer**

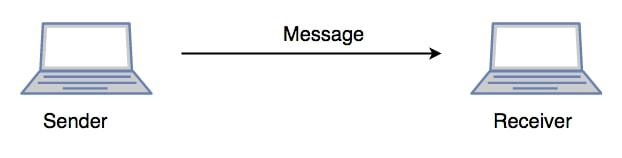
* **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use, and terminate a connection.
* **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
* **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

***Note:***

1. *All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as the ????pplication Layer”.*
2. *Implementation of these 3 layers is done by the network application itself. These are also known as****Upper Layers or******Software Layers.***
3. ***Device or Protocol Use :****NetBIOS, PPTP.*

**For example:-**

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0’s and 1’s) so that it can be transmitted.



*Communication in Session Layer*

***Presentation Layer – Layer 6***

*The presentation layer is also called the****Translation layer****. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.*

***Functions of the Presentation Layer***

* ***Translation:****For example, ASCII to EBCDIC.*
* ***Encryption/ Decryption:****Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.*
* ***Compression:****Reduces the number of bits that need to be transmitted on the network.*

*Note:****Device or Protocol Use:****JPEG, MPEG, GIF*

***Application Layer – Layer 7***

*At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.*

***Example****: Application – Browsers, Skype Messenger, etc.*

***Note:****1. The application Layer is also called Desktop Layer.*

*2.****Device or Protocol Use :****SMTP*

***Functions of the Application Layer***

*The main functions of the application layer are given below.*

* *Network Virtual Terminal: It allows a user to log on to a remote host.*
* *FTAM- File transfer access and management: This application allows a user to  
  access files in a remote host, retrieve files in a remote host, and manage or  
  control files from a remote computer.*
* *Mail Services: Provide email service.*
* *Directory Services: This application provides distributed database sources  
  and access for global information about various objects and services.*

***Note:****OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.*

***What is the Flow of Data in OSI Model?***

*When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender’s end and then climbs back 7 layers on the receiver’s end.*

*Let’s look at it with an Example:*

*Luffy sends an e-mail to his friend Zoro.*

***Step 1:****Luffy interacts with e-mail application like Gmail, outlook, etc. Writes his email to send. (This happens in****Layer 7: Application layer****)*

***Step 2:****Mail application prepares for data transmission like encrypting data and formatting it for transmission. (This happens in****Layer 6: Presentation Layer****)*

***Step 3:****There is a connection established between the sender and receiver on the internet. (This happens in****Layer 5: Session Layer****)*

***Step 4:****Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information. (This happens in****Layer 4: Transport Layer****)*

***Step 5:****Addressing of packets is done in order to find the best route for transfer. (This happens in****Layer 3: Network Layer****)*

***Step 6:****Data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection. (This happens in****Layer 2: Data Link Layer****)*

***Step 7:****Lastly Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.*

*After the email reaches the receiver i.e. Zoro, the process will reverse and decrypt the e-mail content. At last, the email will be shown on Zoro’s email client.*

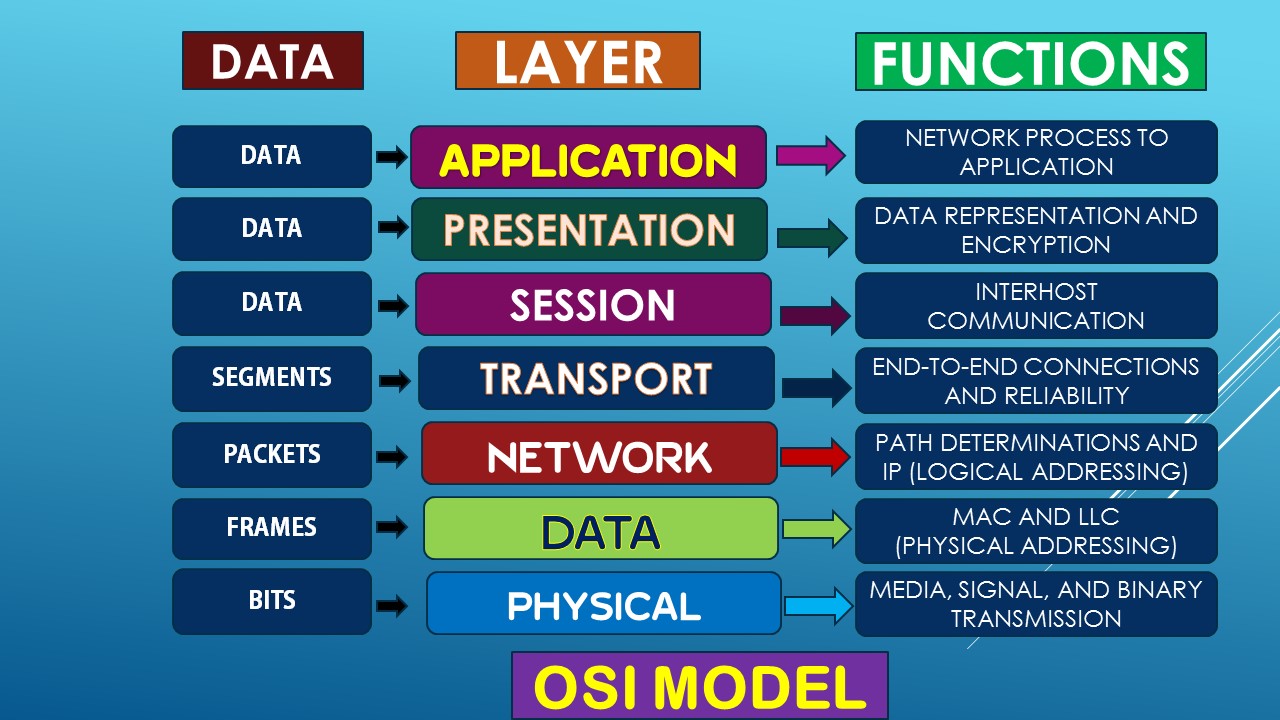
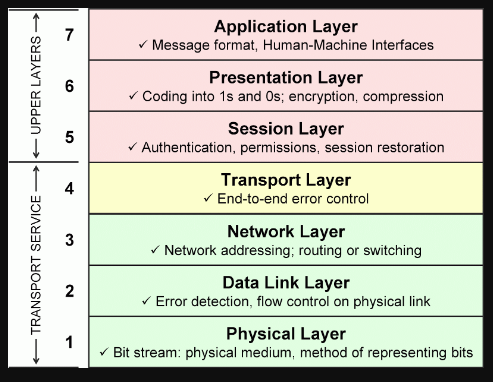
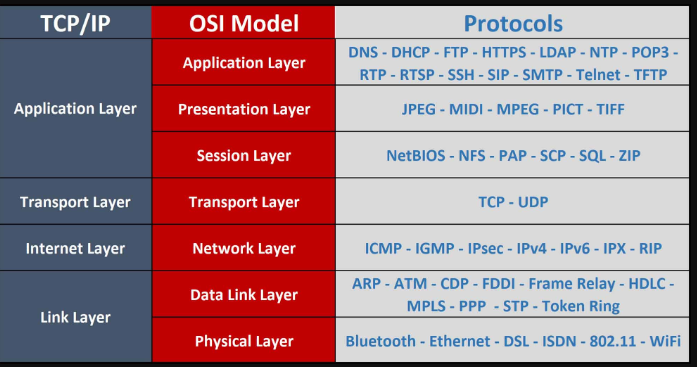
***Advantages of OSI Model***

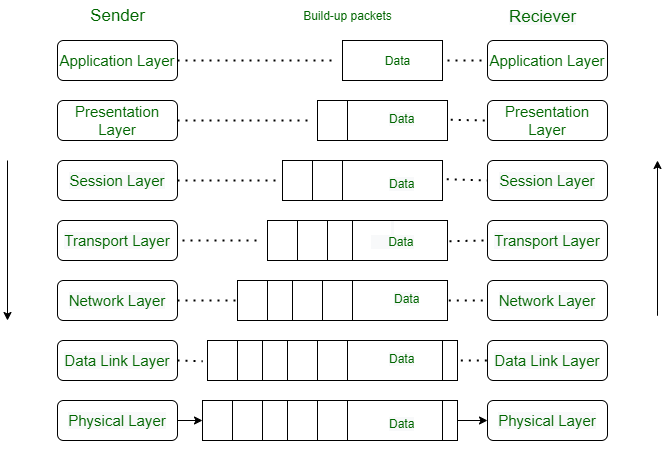
*OSI Model defines the communication of a computing system into 7 different layers. Advantages of OSI Model include:*

* *It divides network communication into 7 layers which makes it easier to understand and troubleshoot.*
* *It standardizes network communications, as each layer has fixed functions and protocols.*
* *Diagnosing network problems is easier with the OSI model.*
* *It is easier to improve with advancements as each layer can get updates separately*

**OSI Model in a Nutshell**

| **Layer No** | **Layer Name** | **Responsibility** | **Information Form(Data Unit)** | **Device or Protocol** |
| --- | --- | --- | --- | --- |
| **7** | Application Layer | Helps in identifying the client and synchronizing communication. | Message | SMTP |
| **6** | Presentation Layer | Data from the application layer is extracted and manipulated in the required format for transmission. | Message | JPEG, MPEG, GIF |
| **5** | Session Layer | Establishes Connection, Maintenance, Ensures Authentication and Ensures security. | Message | Gateway |
| **4** | Transport Layer | Take Service from Network Layer and provide it to the Application Layer. | Segment | Firewall |
| **3** | Network Layer | Transmission of data from one host to another, located in different networks. | Packet | Router |
| **2** | Data Link Layer | Node to Node Delivery of Message. | Frame | Switch, Bridge |
| **1** | Physical Layer | Establishing Physical Connections between Devices. | Bits | Hub, Repeater, Modem, Cables |

[](https://4.bp.blogspot.com/-C8I5dB1DeaE/WCB26ug5dVI/AAAAAAAAAH0/17IN_NjJyz0LNZSW46mQ73HnEljIfKu5QCLcB/s1600/ldb-osi.jpg)**

**

***TCP/IP Model***

*The TCP/IP (Transmission Control Protocol/Internet Protocol) model is a widely used networking model that provides a framework for communication over the internet. It is composed of four layers, each with its own set of protocols and functions.*

***What Does TCP/IP Do?***

*The main work of TCP/IP is to transfer the data of a computer from one device to another. The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender. To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.*

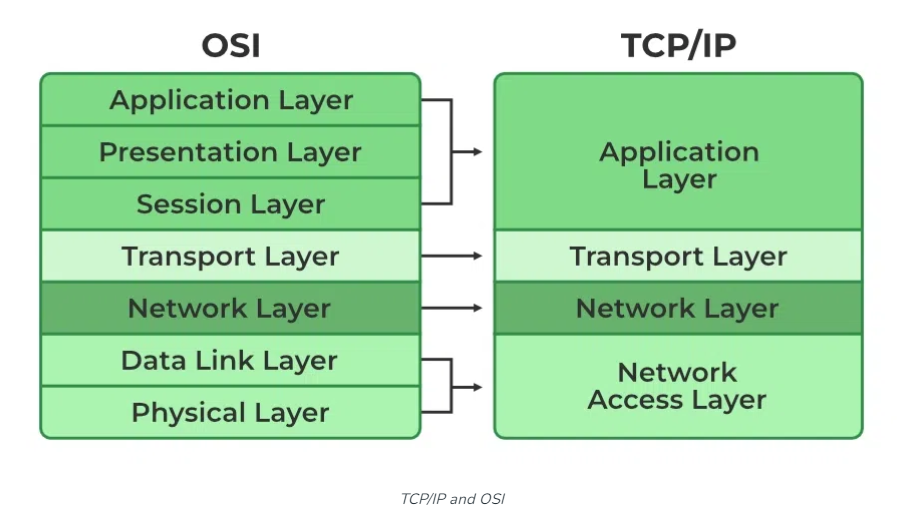
***What is the Difference between TCP and IP?***

[*TCP*](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp/)*and*[*IP*](https://www.geeksforgeeks.org/what-is-an-ip-address/)*are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.*

***Layers of TCP/IP Model***

1. *Application Layer*
2. [*Transport Layer(TCP/UDP)*](https://www.geeksforgeeks.org/tcp-and-udp-in-transport-layer/)
3. *Network Layer*
4. *Network Access Layer*

*The diagrammatic comparison of the****TCP/IP and OSI****model is as follows:*

**

| ***TCP/IP*** | ***OSI*** |
| --- | --- |
| *TCP refers to Transmission Control Protocol.* | *OSI refers to Open Systems Interconnection.* |
| *TCP/IP uses both the session and presentation layer in the application layer itself.* | *OSI uses different session and presentation layers.* |
| *TCP/IP follows connectionless a horizontal approach.* | *OSI follows a vertical approach.* |
| *The Transport layer in TCP/IP does not provide assurance delivery of packets.* | *In the OSI model, the transport layer provides assurance delivery of packets.* |
| *Protocols cannot be replaced easily in TCP/IP model.* | *While in the OSI model, Protocols are better covered and are easy to replace with the technology change.* |
| *TCP/IP model network layer only provides connectionless (IP) services. The transport layer (TCP) provides connections.* | *Connectionless and connection-oriented services are provided by the network layer in the OSI model.* |

***Network Devices***

*These are physical devices that allow hardware on a computer network to communicate and interact with one another. Example: Hub, Switch, Router, etc.*

1. ***Hub****: A hub is the simplest networking device among the three. It operates at the physical layer (Layer 1) of the OSI model. Hubs are essentially multiport repeaters. When a signal arrives at one port, it is broadcasted to all other ports, regardless of whether the destination device is connected to that port or not. This means that all devices connected to a hub share the same bandwidth, leading to potential network congestion and collisions, especially in larger networks. Hubs are rarely used in modern networks due to their limitations.*
2. ***Switch****: A switch operates at the data link layer (Layer 2) of the OSI model. It is more intelligent than a hub because it can selectively forward data only to the port where the destination device is located. This makes network communication more efficient and reduces collisions compared to hubs. Switches build and maintain MAC (Media Access Control) address tables, allowing them to make forwarding decisions based on MAC addresses. Switches are widely used in Ethernet networks to create local area networks (LANs) and segment network traffic.*
3. ***Router****: A router operates at the network layer (Layer 3) of the OSI model. Unlike switches, which operate based on MAC addresses, routers make forwarding decisions based on IP addresses. Routers connect different networks (such as LANs or the Internet) and are responsible for routing data packets between them. Routers use routing tables to determine the best path for forwarding packets to their destination. They provide functionalities like network address translation (NAT), firewalling, and traffic shaping. Routers are essential for connecting multiple networks and enabling communication between devices across different networks.*

*In summary, while hubs, switches, and routers are all networking devices, they serve different functions and operate at different layers of the OSI model, with routers being the most complex and versatile among them.*

***Network Protocols***

*Network protocols define how data is transmitted, received, and processed between devices. They are essential for ensuring that devices can communicate with each other.*

***IP Address:-***

* + *Each device that uses a network receives an IP address, which is a special identifier number.*
  + *IP addresses are necessary for routing packets of data between devices and for enabling Internet communication between devices.*

***TCP(Transmission Control Protocol):-***

* + *TCP is a reliable, connection-oriented protocol.*
  + *provides error-checking, flow control, and congestion avoidance mechanisms.*
  + *When using TCP, a connection is established between the sender and receiver before data transmission begins.*

***UDP(User Datagram Protocol):-***

* + *UDP is a connectionless, unreliable protocol.*
  + *It does not provide error-checking, flow control, or congestion avoidance mechanisms.*
  + *Data is transmitted without establishing a connection, and packets are transmitted without any guarantees of delivery.*

***Note:-*** *Both* ***TCP*** *and* ***UDP*** *are* ***Transport Layer*** *Protocols*

***Dynamic Host Configuration Protocol(DHCP):-***

* + *It is a network protocol used to automatically assign IP addresses and other network configuration settings to devices on a network.*
  + *Without DHCP, devices on a network would need to be manually configured with IP addresses.*

***Wireless Networks***

*A wireless network is a type of computer network that uses radio waves instead of physical cables to connect devices. Wireless networks are commonly used for internet access, as well as for sharing files, printers, and other resources between devices.*