Experiment 1

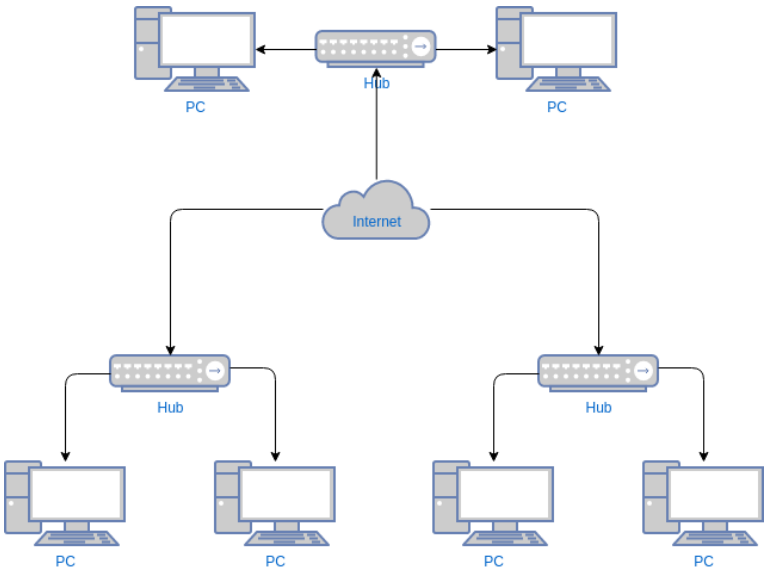
Introduction to Computer Networks

Aim : - To study OSI model and different types of Network Devices

Q1] Explain Computer Network with a neat Diagram

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.

Nodes and Links are the basic building block of a Computer Network. Data is transmitted and generated through the nodes such as computers, switches, and modems. After that, a transmission media which is the link is used to bond among the nodes. The nodes will transfer and receive data via connections by following the protocols. The Computer Network Architecture defines the design associated with these physical and logical components. It provides the definitions for the network's physical components, functional organization, protocols, and procedures.



Types of Computer Networks

Division Based on the Communication Medium

• Wired Network: Communication done in a wired medium. Copper wire, twisted pair, or fiber optic cables are all options. A wired network employs wires to link devices to the Internet or another network, such as laptops or desktop PCs.

• Wireless Network: "Wireless" means without wire, media that is made up of electromagnetic waves (EM Waves) or infrared waves. Antennas or sensors will be present on all wireless devices. For data or voice communication, a wireless network uses radio frequency waves rather than wires.

Division Based on Area Covered

• Local Area Network (LAN): A LAN is a network that covers an area of around 10 kilometers. For example, a college network or an office network. Depending upon the needs of the organization, a LAN can be a single office, building, or Campus. We can have two PCs and one printer in-home office or it can extend throughout the company and include audio and video devices. Each host in LAN has an identifier, an address that defines hosts in LAN. A packet sent by the host to another host carries both the source host's and the destination host's address.

• Metropolitan Area Network (MAN): MAN refers to a network that covers an entire city. For example: consider the cable television network.

• Wide Area Network (WAN): WAN refers to a network that connects countries or continents. For example, the Internet allows users to access a distributed system called www from anywhere around the globe.WAN interconnects connecting devices such as switches, routers, or modems. A LAN is normally privately owned by an organization that uses it. We see two distinct examples of WANs today: point-to-point WANs and Switched WANs

• Point To Point: Connects two connecting devices through transmission media.

• Switched: A switched WAN is a network with more than two ends.

Based on Types of Communication

• Point To Point networks: Point-to-Point networking is a type of data networking that establishes a direct link between two networking nodes. A direct link between two devices, such as a computer and a printer, is known as a point-to-point connection.

• Multipoint: is the one in which more than two specific devices share links. In the multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection.

• Broadcast networks: In broadcast networks, a signal method in which numerous parties can hear a single sender. Radio stations are an excellent illustration of the "Broadcast Network" in everyday life. The radio station is a sender of data/signal in this scenario, and data is only intended to travel in one direction. Away from the radio transmission tower, to be precise.

Based on the Type of Architecture

• P2P Networks: Computers with similar capabilities and configurations are referred to as peers. The "peers" in a peer-to-peer network are computer systems that are connected to each other over the Internet. Without the use of a central server, files can be shared directly between systems on the network.

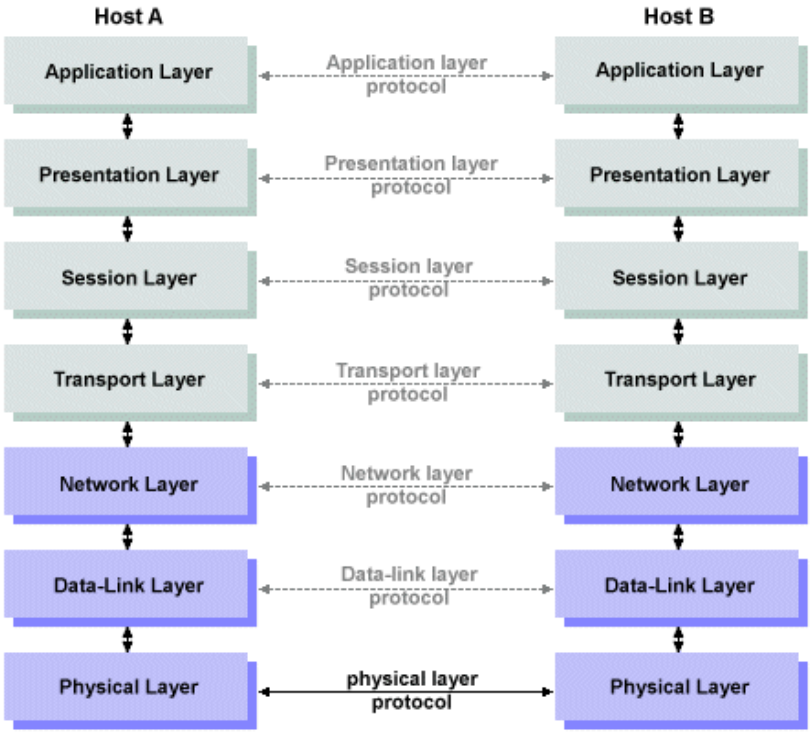
• Client-Server Networks: Each computer or process on the network is either a client or a server in a clientserver architecture (client/server). The client asks for services from the server, which the server provides. Servers are high-performance computers or processes that manage disc drives (file servers), printers (print servers), or network traffic (network servers)

• Hybrid Networks: The hybrid model uses a combination of client-server and peer-to-peer architecture. Eg: Torrent.

Q2] Describe OSI Reference Model

OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network. This model focuses on providing a visual design of how each communications layer is built on top of the other, starting with the physical cabling, all the way to the application that's trying to communicate with other devices on a network.

A reference model is a conceptual framework for understanding relationships. The purpose of the OSI reference model is to guide technology vendors and developers so the digital communications products and software programs they create can interoperate and to promote a clear framework that describes the functions of a networking or telecommunications system that's in use.



7 layers of the OSI model

Layer 7. The application layer

The application layer enables the user -- human or software -- to interact with the application or network whenever the user elects to read messages, transfer files or perform other network-related tasks. Web browsers and other internet-connected apps, such as Outlook and Skype, use Layer 7 application protocols.

Layer 6. The presentation layer

The presentation layer translates or formats data for the application layer based on the semantics or syntax the application accepts. This layer also handles the encryption and decryption that the application layer requires.

Layer 5. The session layer

The session layer sets up, coordinates and terminates conversations between applications. Its services include authentication and reconnection after an interruption. This layer determines how long a system will wait for another application to respond. Examples of session layer protocols include X.225 and Zone Information Protocol (ZIP).

Layer 4. The transport layer

The transport layer is responsible for transferring data across a network and provides error-checking mechanisms and data flow controls. It determines how much data to send, where it gets sent and at what rate. TCP within the TCP/IP suite is the best-known example of the transport layer. This is where the communications select TCP port numbers to categorize and organize data transmissions across a network.

Layer 3. The network layer

The primary function of the network layer is to move data into and through other networks. Network layer protocols accomplish this by packaging data with correct network address information, selecting the appropriate network routes and forwarding the packaged data up the stack to the transport layer. From a TCP/IP perspective, this is where IP addresses are applied for routing purposes.

Layer 2. The data-link layer

The data-link, or protocol layer, in a program handles moving data into and out of a physical link in a network. This layer handles problems that occur as a result of bit transmission errors. It ensures that the pace of the data flow doesn't overwhelm the sending and receiving devices. This layer also permits the transmission of data to Layer 3, the network layer, where it's addressed and routed.

The data-link layer can be further divided into two sublayers. The higher layer, which is called logical link control (LLC), is responsible for multiplexing, flow control, acknowledgement and notifying upper layers if transmit/receive (TX/RX) errors occur.

The media access control sublayer is responsible for tracking data frames using MAC addresses of the sending and receiving hardware. It's also responsible for organizing each frame, marking the starting and ending bits and organizing timing regarding when each frame can be sent along the physical layer medium.

Layer 1. The physical layer

The physical layer transports data using electrical, mechanical or procedural interfaces. This layer is responsible for sending computer bits from one device to another along the network. It determines how physical connections to the network are set up and how bits are represented into predictable signals as they're transmitted either electrically, optically or via radio waves.

Pros and cons of the OSI model

The OSI model has a number of advantages, including the following:

1. It's considered a standard model in computer networking.
2. The model supports connectionless, as well as connection-oriented, services. Users can take advantage of connectionless services when they need faster data transmissions over the internet and the connection-oriented model when they're looking for reliability.
3. It has the flexibility to adapt to many protocols.
4. The model is more adaptable and secure than having all services bundled in one layer.

The disadvantages of the OSI model include the following:

1. It doesn't define any particular protocol.
2. The session layer, which is used for session management, and the presentation layer, which deals with user interaction, aren't as useful as other layers in the OSI model.
3. Some services are duplicated at various layers, such as the transport and data-link layers.
4. Layers can't work in parallel; each layer must wait to receive data from the previous layer.

Q3] Study Various Networking Devices

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

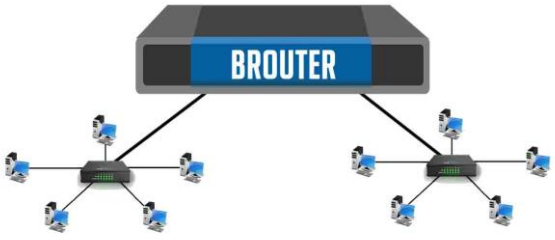
3. Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

4. Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

5. Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

6. Gateway – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

7. Brouter – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.



Conclusion: OSI Model and different types of network devices was successfully studied.