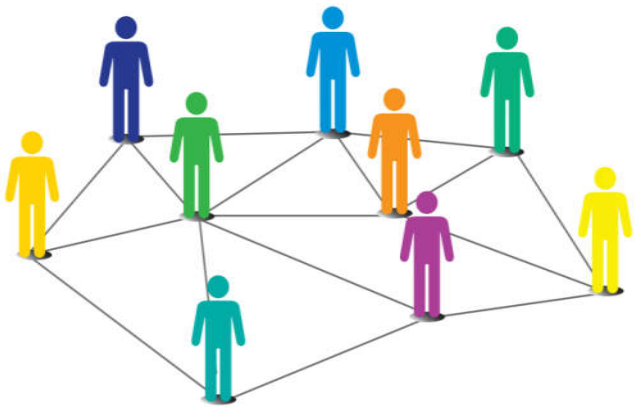
1. Introduction

A network is a collection of two or more computer systems linked physically and through software components to enable communication and information sharing. This connection is established through a shared communication link, with data being the shared component.

A transmission medium serves as the physical pathway connecting the systems, while a set of rules, known as protocols, governs how they communicate. Network protocols are software installed on machines that determine the agreed-upon rules for communication between two or more machines.

Comparing protocols to human languages, it's like a group of people in a room who need to decide on a language to speak, how to identify each other, whether to make general announcements or have private conversations, etc. Machines using different protocols cannot communicate with each other.

Networks are extensively used by companies and individuals alike. For companies, networks should provide high reliability, cost efficiency, and resource sharing capabilities.



2. Definitions

- ✓ A computer network is a collection of interconnected computers and other devices which are able to communicate with each other and share hardware and software resources.
- ✓ LAN definition:A *local area network* (LAN) is a number of computers and computerperipherals (disc storage devices, printers) connected by high speed datalines within a building or adjacent buildings.

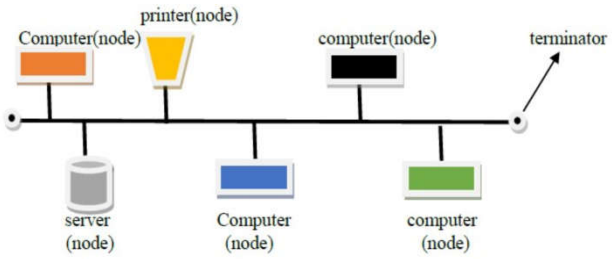
3. Network Topologies

The arrangement of connecting different computers in a network is referred to as network topology. In other words, network topology defines how the nodes (computers or other devices that need to communicate) in a network are interconnected.

Several factors should be considered when selecting a network topology, including:

- The cost of establishing the network topology.
- The required length of cables.
- The type of cables to be used in the topology (options include Coaxial, Twisted Pair, or Optical Fiber Cable).

✓ **Bus Topology:** In bus topology, all the nodes are connected to a main cable calledBackbone.



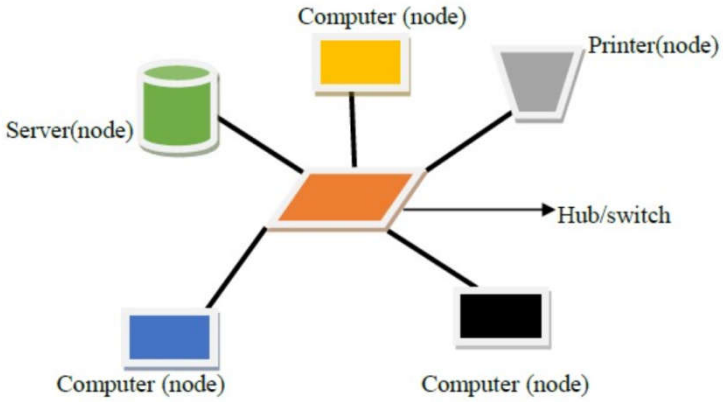
Advantages

- It is easy to install.
- It requires less cable length and hence it is cost effective.

Disadvantages

- In case of cable (backbone) or terminator fault, the entire network breaks down.
- Fault diagnosis is difficult.
- At a time only one node can transmit data.

✓ **Star Topology:** In star topology, each node is directly connected to a hub/switch.



Advantages

- It is easy to install.
- It is easy to diagnose the fault in Star topology.
- It is easy to expand depending on the specifications of central hub/switch.

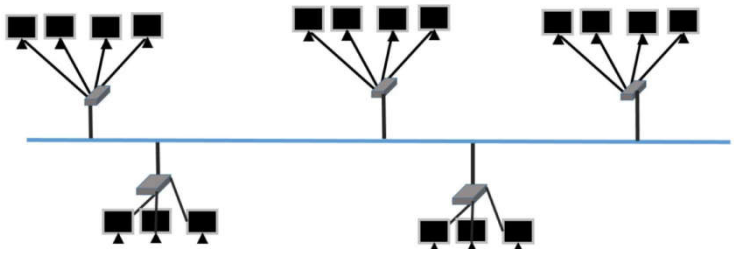
Disadvantages

- Failure of hub/switch leads to failure of entire network.
- It requires more cable length as compared to bus topology.

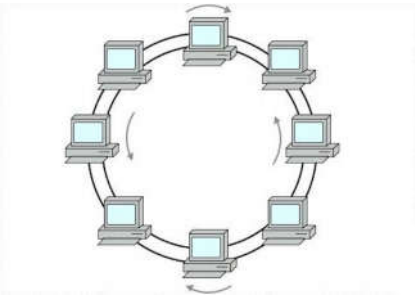
✓ **Tree Topology:** Tree topology is a combination of bus and star topologies. It is used tocombine multiple star topology networks.

Advantages

- It offers easy way of network expansion.
- Even if one network (star) fails, the other networks remain connected and working.



✓ **Ring Topology:**In Ring Topology, all the nodes are connected to each-other in such a way that they make a closed loop. Each workstation is connected to two other components on either side, and it communicates with these two adjacent neighbors. Data travels around the network, in one direction. Sending and receiving of data takes place by the help of TOKEN.



Advantages

- This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of

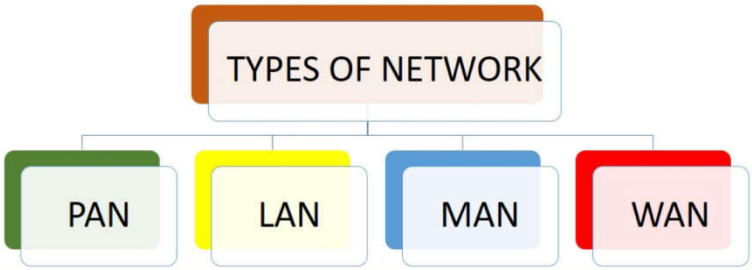
collision. Also in ring topology all the traffic flows in only one direction at very high speed.

- Even when the load on the network increases, its performance is better than that of Bus topology.
- There is no need for network server to control the connectivity between workstations.
- Additional components do not affect the performance of network.
- Each computer has equal access to resources.

Disadvantages

- Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.
- If one workstation or port goes down, the entire network gets affected.
- Network is highly dependent on the wire which connects different components.
- MAU's and network cards are expensive as compared to Ethernet cards and hubs.

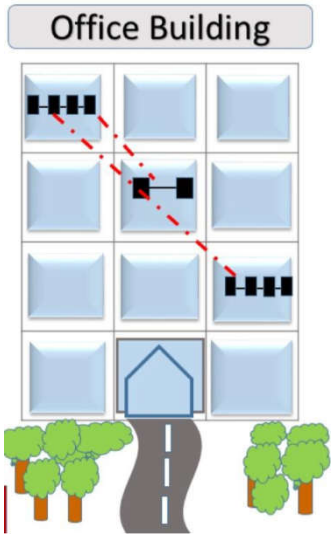
4. **Types of Networks**:

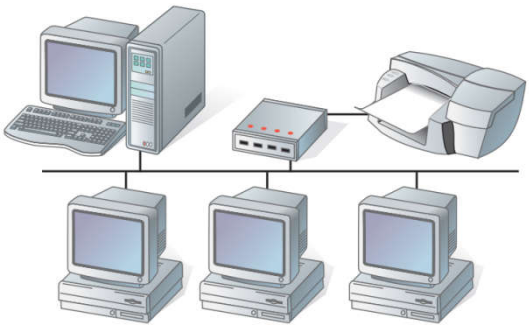


Based on the area covered, computer networks are classified as follows:

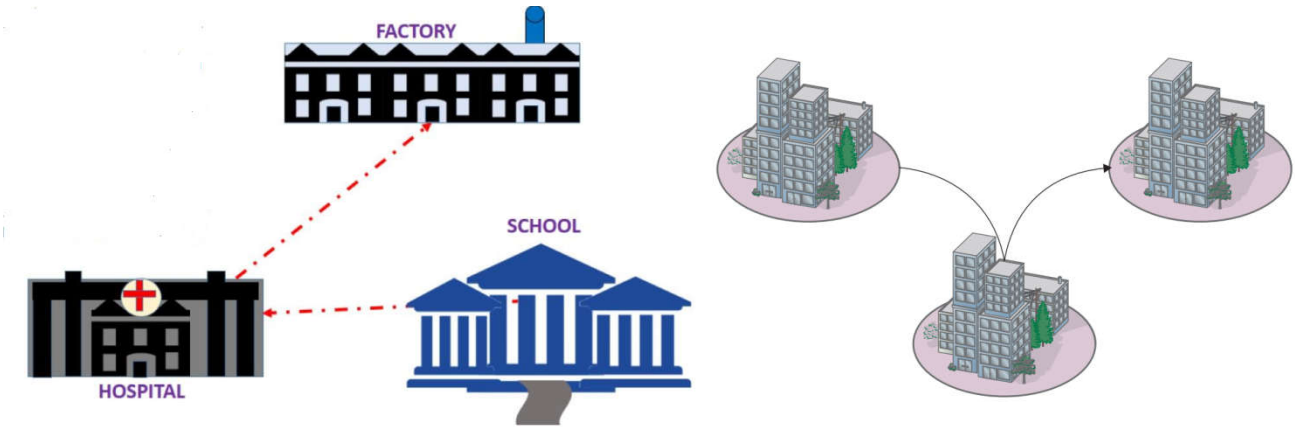
PAN - Personal Area Network: A PAN is a network of communication devices such as computers, phones, MP3/MP4 players, cameras, etc., located in the proximity of an individual. It typically spans an area of approximately a 10-meter radius. PANs can be established using either guided media, such as USB cables, or unguided media like Bluetooth and Infrared technology.

LAN - Local Area Network: A LAN is a network of computing and communicating devices within a confined space, such as a room, building, or campus. It can cover an area ranging from a few meters to several kilometers in radius, and in some cases, it may extend to encompass a group of nearby buildings.

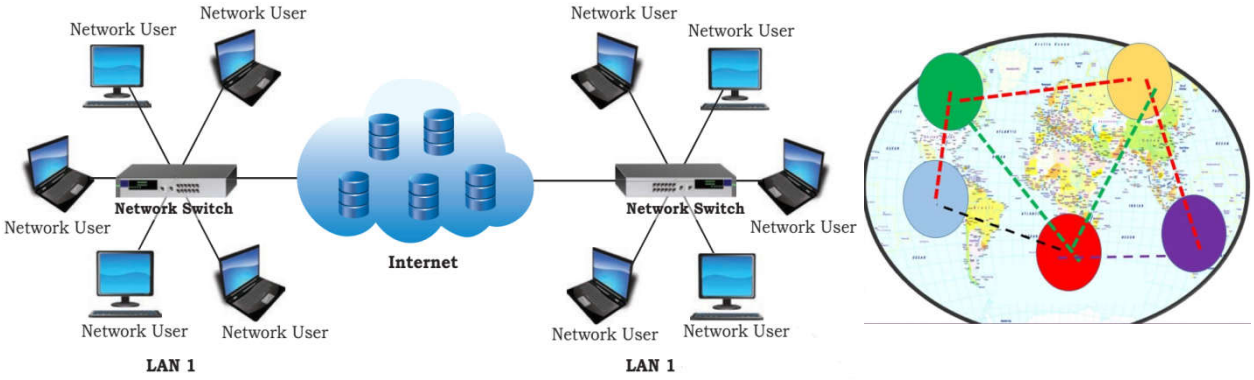




MAN - Metropolitan Area Network: A MAN is a network of computing and communicating devices that encompasses a city or metropolitan area. It can cover an area ranging from a few kilometers to a few hundred kilometers in radius. Examples of MANs include networks connecting schools, banks, government offices, and other institutions within a city. For instance, interconnected state government offices form a MAN.



WAN - Wide Area Network: A WAN is a network that spans beyond the limits of a city, country, or even a continent. It covers an extensive area, often hundreds of kilometers in radius. WANs connect computing and communicating devices, such as ATMs, banks, national government offices, and international organizations' offices, spread over a country or even multiple continents. The internet is a well-known example of a WAN.



Network devices

Network communication and configuration require various devices such as Modem, Ethernet Card (NIC), RJ45 connector, Repeater, Hub, Switch, Router, and Gateway.

Modem: A Modem (MOdulatorDEModulator) converts digital data into analog signals for transmission and vice versa. At the sender's end, it modulates digital data into analog signals, while at the receiver's end, it demodulates analog signals back to digital data.

Ethernet Card (NIC): An Ethernet Card or Network Interface Card (NIC) connects computers to wired networks. It facilitates data transfer between 10 Mbps and 1 Gbps and is identified by a unique MAC address.

RJ45 Connector: The RJ45 connector is an eight-pin interface exclusively used with Ethernet cables. It plugs into the RJ-45 jacks of Ethernet cards in computing devices, enabling networking.

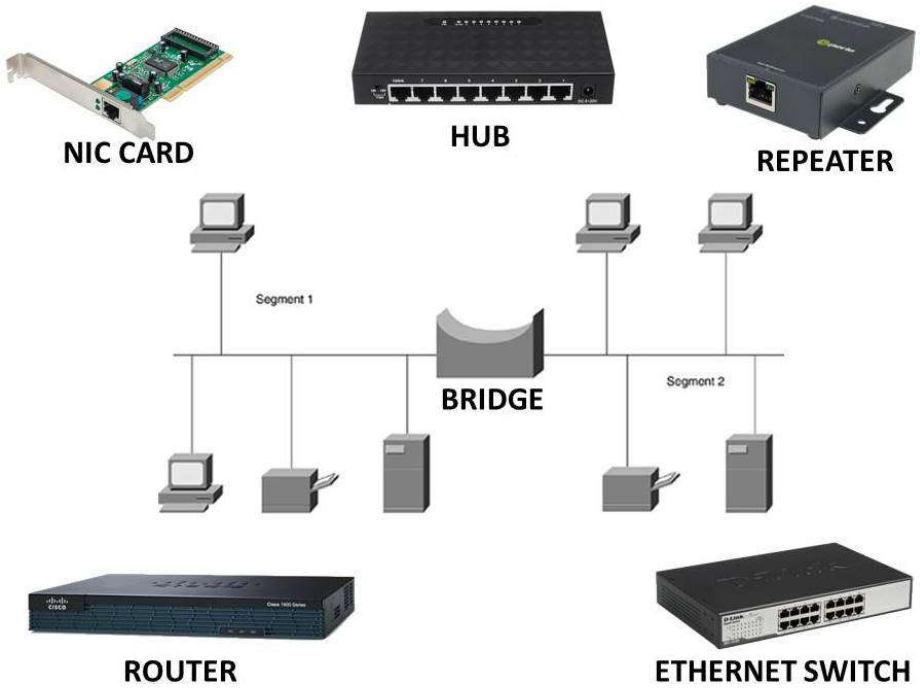
Repeater: A repeater boosts weakened signals on cables, regenerating them to extend transmission distances beyond limitations.

Hub: An Ethernet hub connects devices through wired connections, but data collisions may occur when data from multiple devices arrive simultaneously.

Switch: A network switch in a Local Area Network (LAN) selectively forwards data to specific devices based on destination addresses, improving efficiency compared to hubs.

Router: Routers analyze and transmit data between networks, making decisions on packaging and routing. They can repackage data for different networks and connect local networks to the internet.

Gateway: A gateway acts as an access point between an internal network and the external internet. It routes data in and out of networks, maintaining connection paths. It can be implemented in hardware, software, or both, often integrated with firewalls.



5. Identification of computers and users over a network:

Each node in a network should be uniquely identified so that a network device can identify the sender and receiver and decide a routing path to transmit data. Let us explore further and know how each node is distinguished in a network.

- ✓ **MAC** (Media Access Control) address: A machine with a Network Interface Card (NIC) can be uniquely identified through its NIC's MAC address. The MAC address of an NIC is permanent and never changes. For instance, in the following MAC address: 00:A0:C9:14:C8:35, the prefix "00:A0:C9" indicates the ID number of the adapter manufacturer, while the second half "14:C8:35" represents the serial number assigned to the adapter (NIC) by its manufacturer.
- ✓ **IP Address**: Every machine in a network also has a unique identifying number, known as its IP Address. An IP address is a group of four bytes (or 32 bits), each of which can be a number from 0 to 255. A typical IP address appears as follows: 59.177.134.72. On a network, an IP address is used to identify a machine. However, the MAC address is utilized only when a specific machine is to be targeted. For example, if there is a need to block a particular PC from accessing certain network

resources, using the PC's IP address may not be effective as its IP address might change when it reconnects to the network. In such cases, the PC's MAC address is used for this purpose, as it remains constant.

Comparison of IP Address and MAC Address:

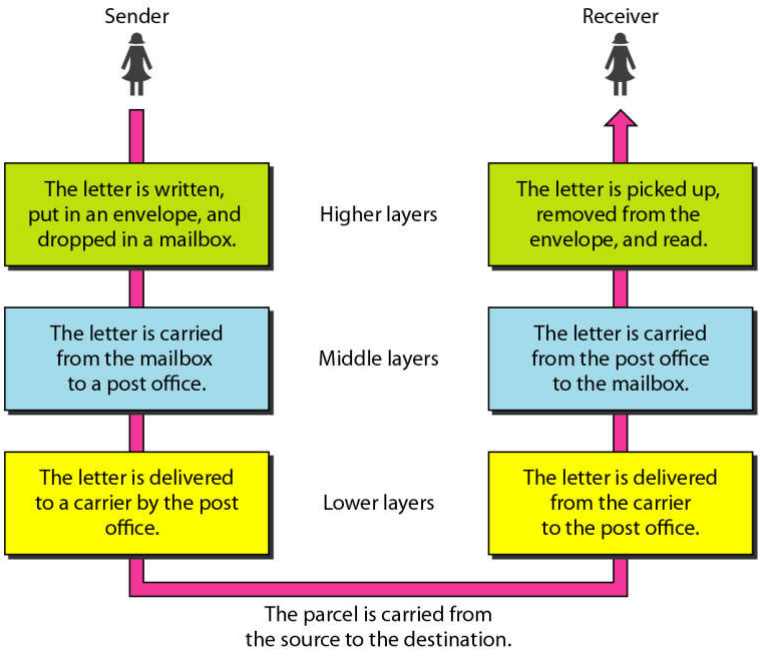
(i) The IP address is assigned by the network administrator or the internet service provider, whereas the MAC address is assigned by the manufacturer.

(ii) If a computer is transferred from one network to another, its IP address gets changed, while the MAC address remains the same.

6. OSI Model and TCP/IP models

Layered tasks

We often apply the concept of layers in our daily lives. For instance, consider two friends communicating via postal mail. Sending a letter would become intricate without the services provided by the post office.



Tasks involved in sending a letter

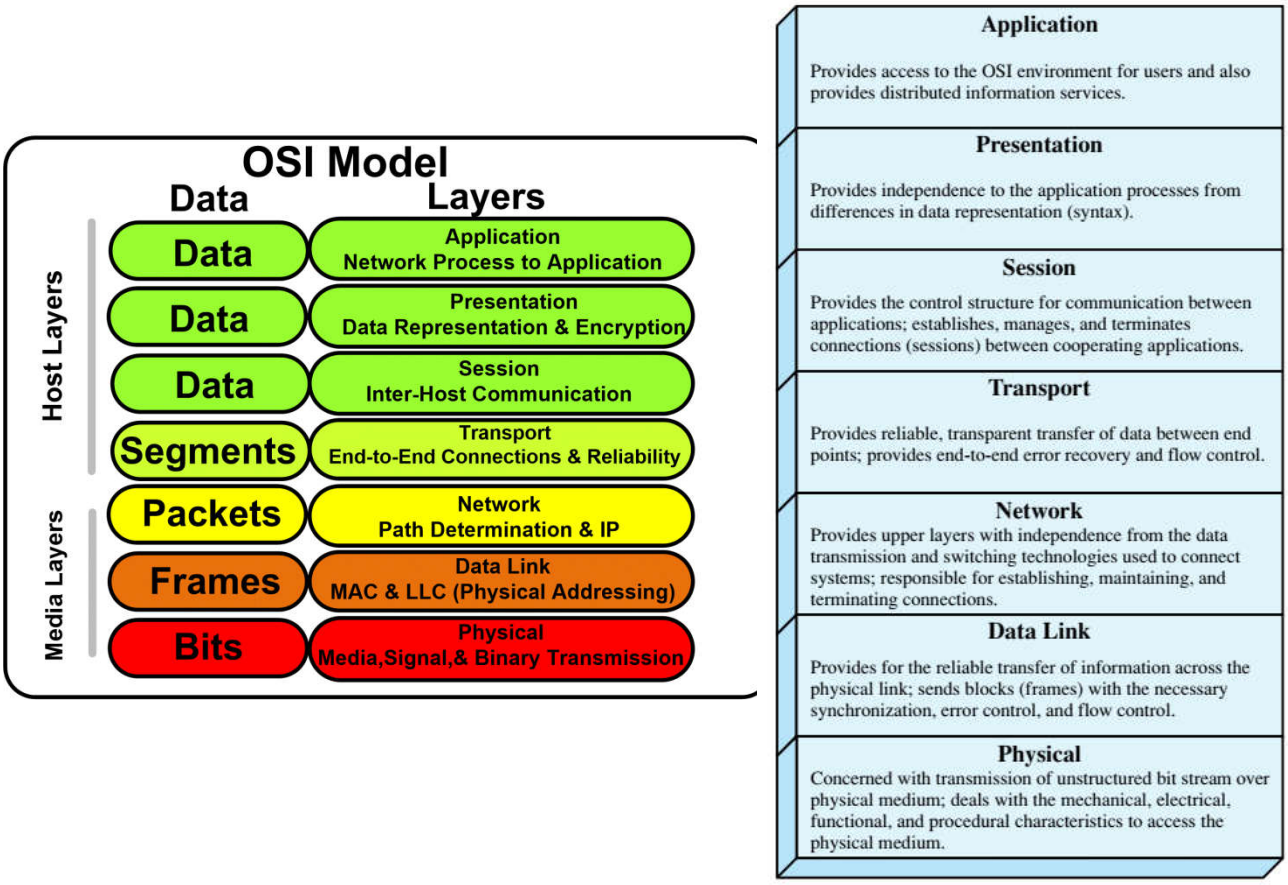
The OSI model

The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) reference model as a blueprint for computer protocol architecture and protocol standards development.

OSI stands for Open System Interconnection, a reference model that describes how information or data flow from one computer to another through a network.

The OSI model enables heterogeneous systems to interconnect and exchange information. It is therefore independent of the structure and technology of the hardware used. This model provides a framework to ensure maximum compatibility between communicating entities while minimizing the constraints required to achieve them.

Figure X illustrates the OSI model, offering concise definitions of functions at each layer. The OSI model aims to guide protocol development to fulfill the tasks of each layer.



OSI layers

The TCP/IP Layers

In communication, three key components come into play: applications, computers, and networks. Applications include tasks like file transfer and email. Here, we're focused on distributed applications that exchange data between computers. These applications, along with

others, run on computers capable of supporting multiple tasks simultaneously. Computers are linked through networks, which facilitate data transfer between them.

To streamline the communication process, we break it down into five distinct layers:

Physical Layer: Deals with the interface between data transmission devices and networks. It specifies aspects like transmission medium characteristics, signal nature, and data rates.

Network Access Layer: Manages data exchange between end systems and their attached networks. It involves providing the network with destination addresses, invoking specific services, and using network-specific software standards.

Internet Layer: Focuses on routing data across networks. The Internet Protocol (IP) ensures data traversal over interconnected networks, implemented both in end systems and routers.

Host-to-host Layer: Ensures reliable data exchange and order preservation regardless of application type. The Transmission Control Protocol (TCP) is commonly used for this purpose.

Application Layer: Houses the logic required to support various user applications, each requiring distinct modules tailored to their functionality.

Key differences between TCP/IP and OSI model

Layer Structure:

- OSI: Comprises 7 layers.
- TCP/IP: Consists of 4 layers.

Conceptual vs Practical:

- OSI: Conceptual model defining network communication for interconnection.
- TCP/IP: Practical guidelines for internet connectivity and data transmission.

Header Size:

- OSI: Header size is 5 bytes.
- TCP/IP: Header size is 20 bytes.

Naming:

- OSI: Stands for Open Systems Interconnection.
- TCP/IP: Stands for Transmission Control Protocol/Internet Protocol.

Approach:

- OSI: Follows a vertical approach.
- TCP/IP: Follows a horizontal approach.

Connection Type:

- OSI: Transport layer is only connection-oriented.
- TCP/IP: Offers both connection-oriented and connectionless options.

Origin:

- OSI: Developed by ISO (International Organization for Standardization).
- TCP/IP: Developed by ARPANET (Advanced Research Projects Agency Network).

Hardware vs Connectivity:

- OSI: Aids in standardizing hardware like routers, switches, and motherboards.
- TCP/IP: Focuses on establishing connections between diverse computer types.

7. **Access Control to the Medium**

Issue: In scenarios where N computers seek access to the transmission channel, collisions can arise when two computers attempt to transmit data simultaneously. This poses a significant challenge in network communication.

***Static Allocation*:** When faced with N computers and a network with a capacity of C bits/sec, a static allocation approach is employed. The concept involves reserving a portion of C/N bits/sec for each computer. This is regulated through time multiplexing. However, this method has its limitations. While it ensures that each user receives C/N bits of the overall throughput, it is more suitable for steady data streams, like telephone networks, but proves unsatisfactory for sporadic usage patterns.

Additionally, this approach doesn't effectively manage the channel and hence necessitates the exploration of more efficient methods.

***Control Techniques*:** In order to address these challenges, control techniques are introduced.

- **Principle:** These techniques are rooted in the principles of defining access control rules and instilling a sense of politeness among the participating computers.
- **Politeness Rules:** A set of politeness rules guides the behavior of computers attempting to access the channel:
- **Listen Before Transmitting:** Computers are required to listen to the channel before initiating any transmission attempts.
- **No Concurrent Transmission:** If a computer detects ongoing transmission, it refrains from transmitting to prevent collisions.

Local Network Application: These rules are particularly relevant in a local network environment.

Solution: Two prominent solutions emerge:

***Competition-based Access*:** This method, known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD), employs a competitive approach to access the channel.

***Election-based Access*:** Another method involves the use of token-based techniques, where stations acquire access through an election process.

***CSMA (Carrier Sense Multiple Access) Listening*:** Characterized by its bus topology, CSMA allows multiple computers simultaneous access to the medium. It functions by listening to and detecting signals on the network before initiating transmission. The key principle is to transmit only when no signals are detected.

***CSMA with Collision Detection (CSMA/CD)*:** To overcome the issue of simultaneous transmissions leading to collisions, the CSMA/CD technique is employed. This approach minimizes losses through collision detection. It involves listening not only before transmission but also during message transmission, enhancing collision detection capabilities. Additionally, listening for a period equal to twice the propagation time to the furthest point on the bus further aids collision detection. If a collision occurs, the transmission is halted, and retransmission takes place after a randomly determined time interval. The IEEE 802.3 Ethernet network is an example of a system implementing this technique.

Token Technique (Token Ring): Characterized by its ring topology, the token technique is structured around the circulation of a single frame among stations. Only one station transmits at any given time, and the token serves as the control mechanism for accessing the medium.

***Process for Transmitting Station*:** A station that wishes to transmit follows these steps:

***Capture the Token*:** When the token becomes accessible, the station captures it.

***Transmit a Frame*:** The station sends its data frame.

Recipient Verification: The transmitting station verifies that the intended recipient received the message.

***Release and Pass*:** After verification, the station releases the token and passes it to the next station in line.

In cases where the token is lost or destroyed, algorithms are in place to regenerate it, ensuring the continuous functioning of the token-based access control mechanism.