COMPUTER COMMUNICATION AND NETWORKS

BCA III SEM(NEP)

NOTES

Prepared By

Mr. Prabhu Kichadi, BE, MTECH

9880437187

UNIT – I

Introduction: Computer Networks and its applications, Network structure, network architecture, Topologies, LAN, WAN, MAN, The OSI reference model, The TCP/IP reference model.

Introduction, Computer Networks, and its applications:

A network can be defined as two or more computers connected in such a way that they can share resources.

A network is simply a collection of computers or other hardware devices that are connected, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate.

A resource may be:

- A file
- A folder
- A printer
- A disk drives
- Or just about anything else that exists on a computer.

Need for computer network because of following features.

we will see why we need computer networks in more detail below –

To share computer files

Networks enable users to share files with others. For example, in a company, one file is to be shared by multiple branches. When we locate this file on the network system, all the branches can use this file.

To share computer equipment

Laser printers and large hard-disk drives can be expensive. Networks enable users to share such equipment by networking microcomputers or workstations together.

To enable unlike computer equipment to communicate

A company with computers of multiple uses using several operating systems, including MS-DOS, UNIX, WINDOWS 95, and Apple DOS, cannot share files from one computer to another unless arranged using a Networking operating system including Network 4.1 or Windows NT 4.0.

To improve communication speed and accuracy

Sending messages through networks is virtually instantaneous, and there is also less chance of a message being lost.

To reduce the cost of data transfer

The cost of transfers of files using computers associated with networks is less expensive than other traditional means like telegrams.

Verify Data Transfer

Fluctuations of costs in foreign exchange and shares can be broadcasted promptly using the channel of computer communications. The transmission can be increased and checked at any occurrence of time.

High Reliability

All files can be recreated on a few machines, and therefore if one of them is unavailable (because of hardware failure), the different copies can be used.

Advantages/Applications of networking:

- Connectivity and Communication
- Data Sharing
- Hardware Sharing
- Internet Access
- Internet Access Sharing
- Data Security and Management
- Performance Enhancement and Balancing
- Entertainment

- **Electronic Messaging:** – Electronic mail (e-mail) is the most widely used network application.
- **Cable Television:** - Future Services provided by cable television network can include video on request.
- **Resource Sharing: -** Resource sharing is an application of a computer network. Resource sharing means you can share one Hardware and Software among multiple users. Hardware includes printers, Disks, Fax Machines, etc.
- **Social media: -** social media is also a great example of a computer network application. It helps people to share and receive any information related to political, ethical, and social issues.
- **Information Sharing: -** Using a computer network, we can share Information over the network, and it provides Search capabilities such as WWW.
- **Communication: -** Communication includes email, calls, message broadcast, electronic funds transfer system etc.
- **Access to Remote Databases: -** Computer networks allow us to access the Remote Database of the various applications by the end-users. Some applications are Reservation for Hotels, Airplane Booking, Home Banking, Automated Newspaper, Automated Library etc.

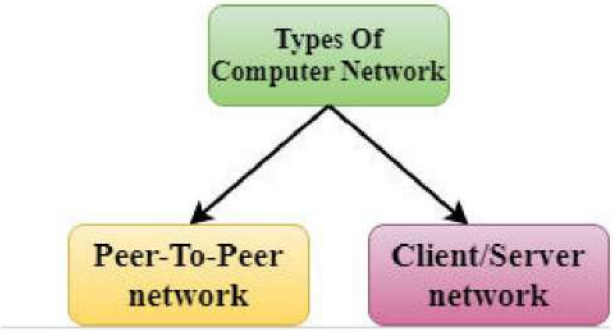
Network structure: Computer Network Architecture is defined as the physical and logical design of the software, hardware, protocols, and media of the transmission of data. Simply we can say that how computers are organized and how tasks are allocated to the computer.

Network architecture:

Architecture refers to a network's structural (Physical) and logical (Flow of data) layout. It describes how the network devices are connected and the rules that govern data transfer between them.

It mainly focuses on Performance of the network.
There are many ways to approach network architecture design, which depend on the purpose and size of the network.

These are the two types of architectures:



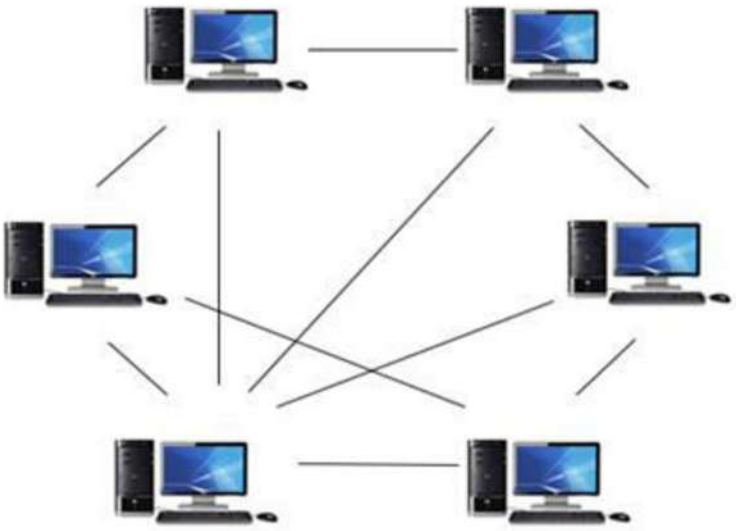
1. peer-to-peer

2. client-server OR Network architectures.

1. Peer-to-Peer Architecture:

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Every node can act as both client and server.

- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.



Advantages Of Peer-To-Peer Network:

- It is less costly as it does not contain any dedicated server.
- If one computer stops working but, other computers will not stop working.
- It is easy to set up and maintain as each computer manages itself.

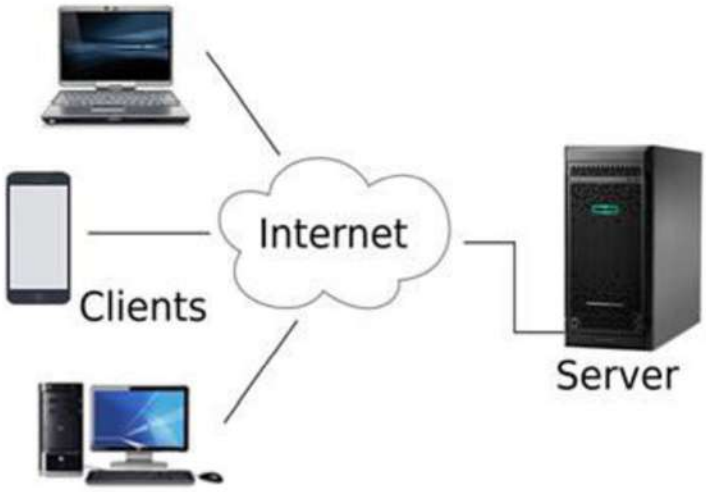
Disadvantages Of Peer-To-Peer Network:

- In the case of Peer-To-Peer network, it does not contain the centralized system. Therefore, it cannot back up the data as the data is different in different locations.
- It has a security issue as the device is managed itself.

2. Client-Server Network Architecture:

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.

- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.



Advantages Of Client-Server network:

- A Client/Server network contains the centralized system. Therefore, we can back up the data easily.
- A Client/Server network has a dedicated server that improves the overall performance of the whole system.
- Security is better in Client/Server network as a single server administers the shared resources.
- It also increases the speed of the sharing resources.

Disadvantages Of Client-Server network:

- Client/Server network is expensive as it requires the server with large memory.

- A server has a Network Operating System (NOS) to provide the resources to the clients, but the cost of NOS is very high.
- It requires a dedicated network administrator to manage all the resources.

Topology: Topology defines the structure of the network of how all the components are interconnected to each other.

The diagrammatic or pictorial representation of computer network is called as network topology.

Topology is used to explain how a network is physically connected and the logical flow of information in the network.

In computer networks, there are mainly two types of topologies, they are:

Physical Topology: A physical topology describes the way in which the computers or nodes are connected with each other in a computer network. It is the arrangement of various elements (link, nodes, etc.), including the device location and code installation of a computer network. In other words, we can say that it is the physical layout of nodes, workstations, and cables in the network.

Logical Topology: A logical topology describes the way, data flow from one computer to another. It is bound to a network protocol and defines how data is moved throughout the network and which path it takes. In other words, it is the way in which the devices communicate internally.

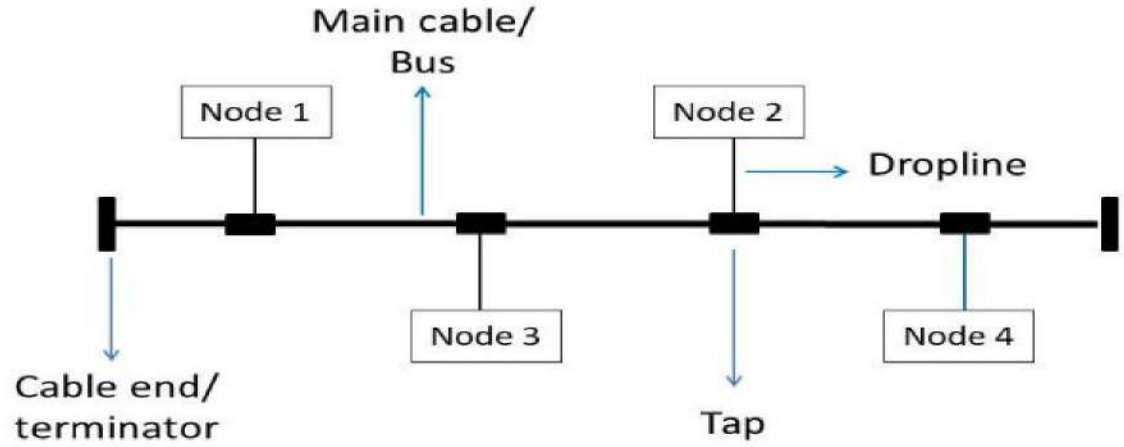
In a computer network, there are mainly six types of physical topology, they are:

1. Bus Topology
2. Ring Topology
3. Star Topology
4. Mesh Topology
5. Tree Topology
6. Hybrid Topology

1. Bus Topology:

Bus topology is the simplest kind of topology in which a common bus or channel is used for communication in the network.

The bus is connected to various taps and droplines. Taps are the connectors, while droplines are the cables connecting the bus with the computer. In other words, there is only a single transmission line for all nodes.



- ✓ In this topology, the bus acts as the backbone of the network, which joins every computer and peripherals in the network. Both ends of the shared channel have line terminators.
- ✓ The data is sent only in one direction and as soon as it reaches the end, the terminator removes the data from the communication line.

Advantages of Bus topology:

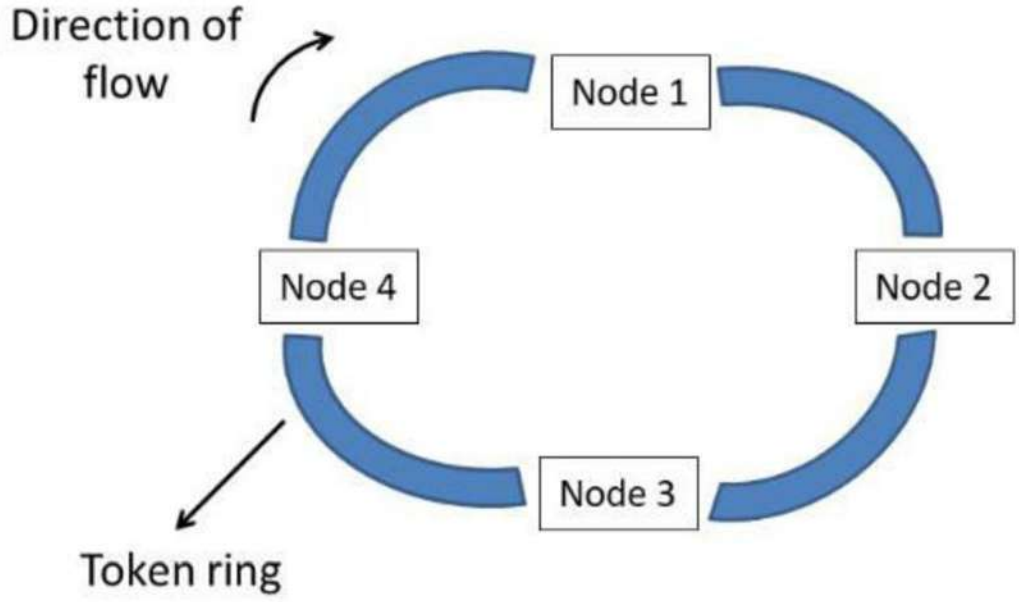
1. Simple to use and install.
2. If a node fails, it will not affect other nodes.
3. Less cabling is required.
4. Cost-efficient to implement.

Disadvantages of Bus topology:

1. Efficiency is less when nodes are more (strength of signal decreases).
2. If the bus fails, the network will fail.
3. A limited number of nodes can connect to the bus due to limited bus length.

2. Ring Topology:

Ring topology is a topology in which each computer is connected to exactly two other computers to form the ring. The message passing is unidirectional and circular in nature.



In a ring topology, if a token is free then the node can capture the token and attach the data and destination address to the token, and then leaves the token for communication. When this token reaches the destination node, the data is removed by the receiver and the token is made free to carry the next data.

Advantages of Ring topology:

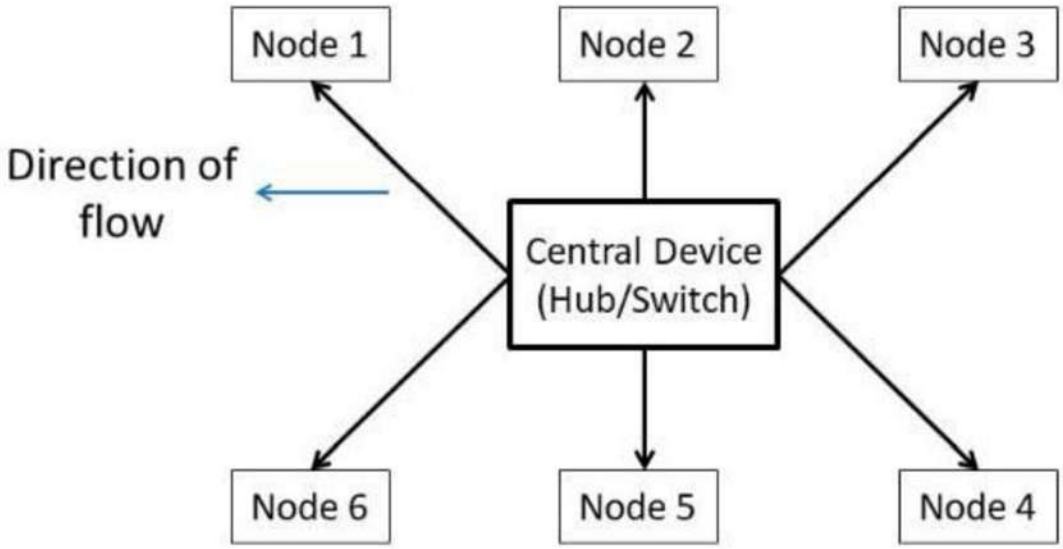
1. Easy Installation.
2. Less Cabling Required.
3. Reduces chances of data collision(unidirectional).
4. Easy to troubleshoot(the faulty node does not pass the token).
5. Each node gets the same access time.

Disadvantages of Ring topology:

1. If a node fails, the whole network will fail.
2. Slow data transmission speed (each message has to go through the ring path).
3. Difficult to reconfigure (we have to break the ring).

3. Star Topology:

Star topology is a computer network topology in which all the nodes are connected to a centralized hub. The hub or switch acts as a middleware between the nodes. Any node requesting for service or providing service, first contact the hub for communication.



The central device (hub or switch) has point to point communication link(the dedicated link between the devices which cannot be accessed by some other computer) with the devices.

In a star topology, hub and switch act as a server, and the other connected devices act as clients.

Advantages of Star topology:

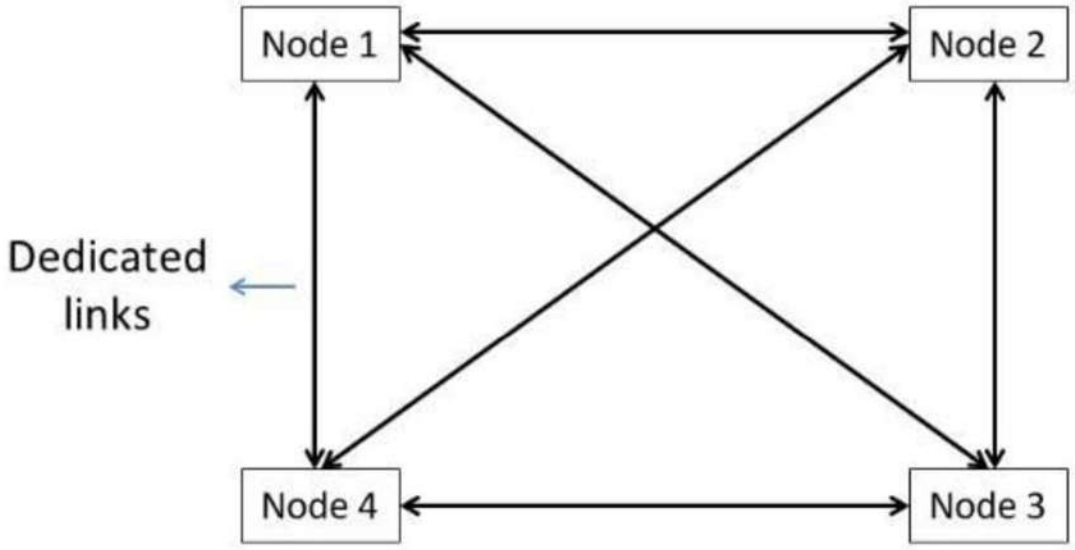
1. Centralized control.
2. Less Expensive.
3. Easy to troubleshoot (the faulty node does not give response).
4. Good fault tolerance due to centralized control on nodes.
5. Easy to scale (nodes can be added or removed to the network easily).
6. If a node fails, it will not affect other nodes.
7. Easy to reconfigure and upgrade (configured using a central device).

Disadvantages of Star topology:

1. If the central device fails, the network will fail.
2. The number of devices in the network is limited (due to limited input-output port in a central device).

4. Mesh Topology:

Mesh topology is a computer network topology in which nodes are interconnected with each other. In other words, direct communication takes place between the nodes in the network.



There are mainly two types of Mesh:

1. **Full Mesh:** In which each node is connected to every other node in the network.
2. **Partial Mesh:** In which, some nodes are not connected to every node in the network.

In a fully connected mesh topology, each device has a point-to-point link with every other device in the network.

If there are **'n'** devices in the network, then each device has exactly **'(n-1)'** input-output ports and communication links.

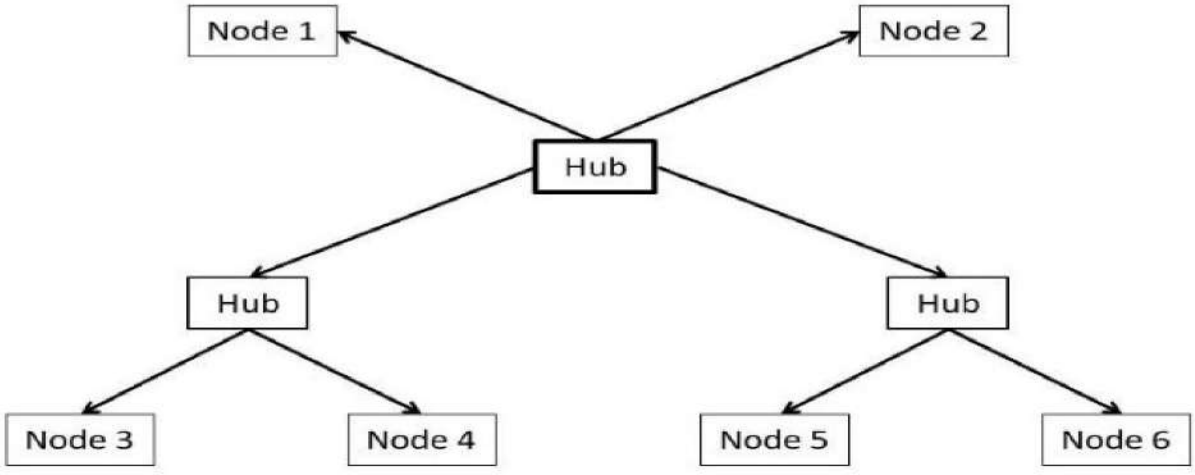
Advantages of Mesh topology:

1. Dedicated links facilitate direct communication.
2. No congestion or traffic problems on the channels.
3. Good Fault tolerance due to the dedicated path for each node.
4. Very fast communication.
5. Maintains privacy and security due to a separate channel for communication.
6. If a node fails, other alternatives are present in the network.

Disadvantages of Mesh topology:

1. Very high cabling required.
2. Cost inefficient to implement.
3. Complex to implement and takes large space to install the network.
4. Installation and maintenance are very difficult.

5. Tree Topology: Tree topology is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable. Tree topology is a combination of Bus and Star topology.



In a tree topology, the whole network is divided into segments, which can be easily managed and maintained. There is a main hub and all the other sub-hubs are connected to each other in this topology.

Following are the advantages of Tree topology:

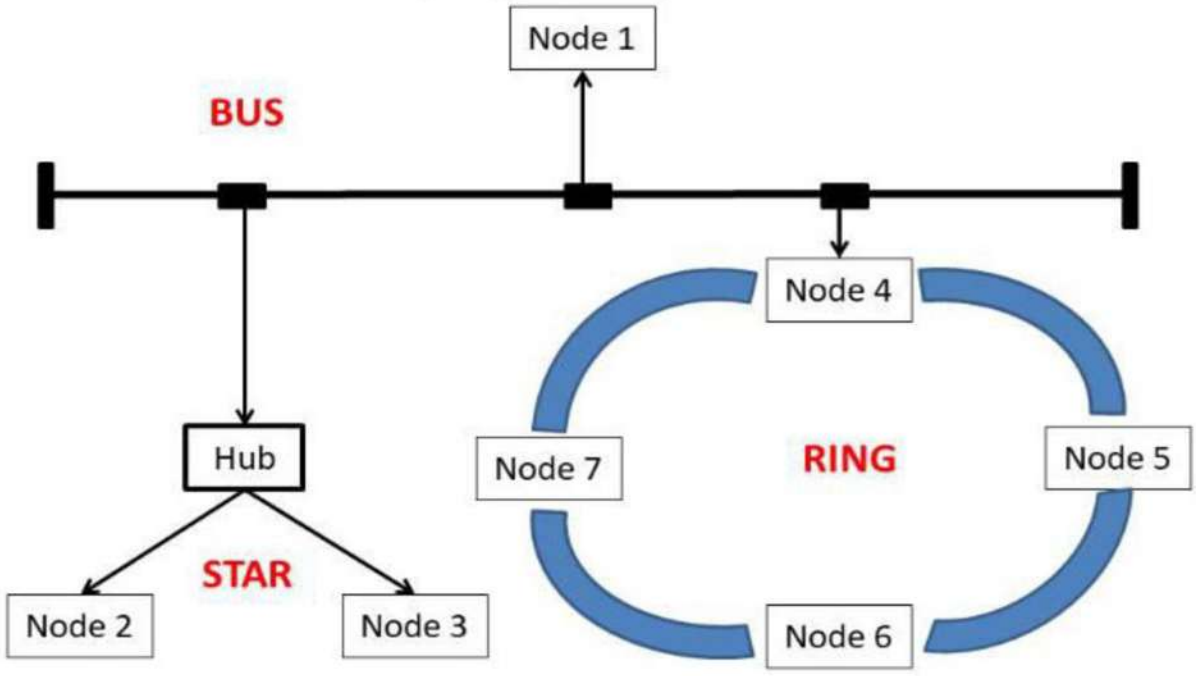
1. Large distance network coverage.
2. Fault finding is easy by checking each hierarchy.
3. Least or no data loss.
4. A Large number of nodes can be connected directly or indirectly.
5. Other hierarchical networks are not affected if one of them fails.

Following are the disadvantages of Tree topology:

1. Cabling and hardware cost is high.
2. Complex to implement.
3. Hub cabling is also required.
4. A large network using tree topology is hard to manage.
5. It requires very high maintenance.
6. If the main bus fails, the network will fail.

6. Hybrid Topology:

A Hybrid topology is a computer topology which is a combination of two or more topologies. In practical use, they are the most widely used.



Advantages of Hybrid topology:

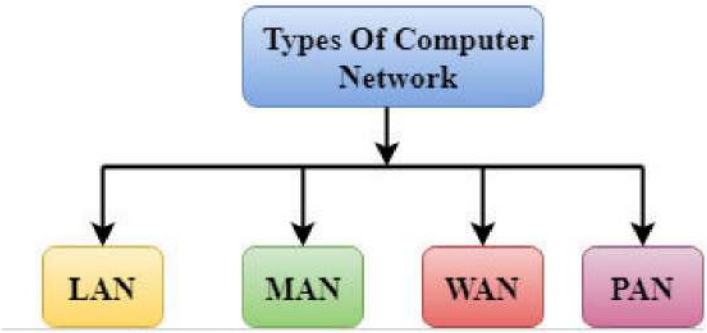
1. It can handle a large volume of nodes.
2. It provides flexibility to modify the network according to our needs.
3. Very Reliable (if one node fails it will not affect the whole network).

Disadvantages of Hybrid topology:

1. Complex design.
2. Expensive to implement.

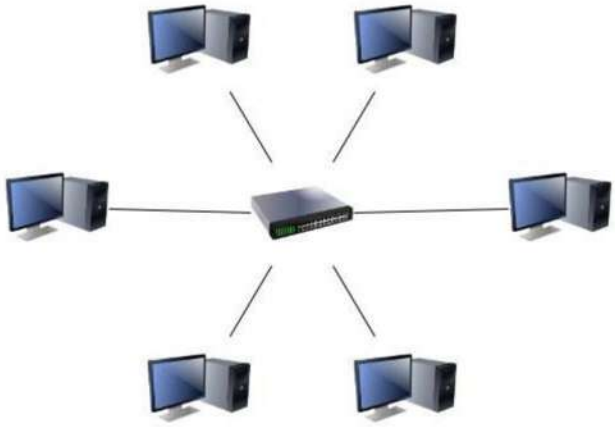
Types of Networks: A computer network can be categorized by their size. A computer network is mainly of four types:

1. **LAN (Local Area Network)**
2. **PAN (Personal Area Network)**
3. **MAN (Metropolitan Area Network)**
4. **WAN (Wide Area Network)**



1. LAN (Local Area Network):

- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network. They range from 100 Mbps to 1000 Mbps.

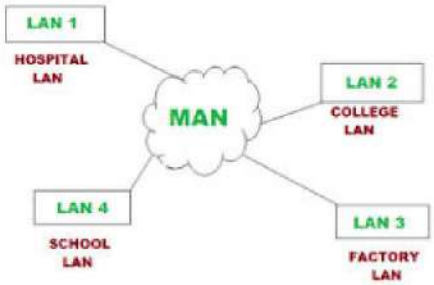


2. MAN (Metropolitan Area Network):

- A metropolitan area network (MAN) is a network with a size greater than LAN but smaller than a WAN.
- It normally comprises networked interconnections within a city that also offers a connection to the Internet.
- Network size generally ranges from 5 to 50 km. It may be as small as a group of buildings in a campus to as large as covering the whole city.
- Data rates are moderate to high.
- In general, a MAN is either owned by a user group or by a network provider who sells service to users, rather than a single organization as in LAN.
- It facilitates sharing of regional resources.
- They provide uplinks for connecting LANs to WANs and Internet.

Examples:

- Cable TV network
- Telephone networks providing high-speed DSL lines



3. WAN (Wide Area Network):

- A wide area network (WAN) is a computer network that covers a large geographical area comprising a region, a country, a continent or even the whole world.
- WAN includes the technologies to transmit data, image, audio and video information over long distances and among different LANs and MANs.
- WANs have a large capacity, connecting a large number of computers over a large area, and are inherently scalable.
- They provide uplinks for connecting LANs and MANs to the Internet.
- Communication links are provided by public carriers like telephone networks, network providers, cable systems, satellites etc.
- Typically, they have low data transfer rate and high propagation delay, i.e. they have low communication speed.
- They generally have a higher bit error rate.

Example of WAN

- The Internet
- 4G Mobile Broadband Systems

Sr.No.	Key	LAN	MAN	WAN
1	**Definition**	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
2	**Ownership**	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.
3	**Speed**	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
4	**Delay**	Network Propagation Delay is short in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
5	**Congestion**	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
6	**Fault Tolerance**	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.
7	**Maintenance**	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.

The OSI reference model:

OSI: Established in 1947, the **International Standards Organization** (ISO) is a multinational body dedicated to worldwide agreement on international standards.

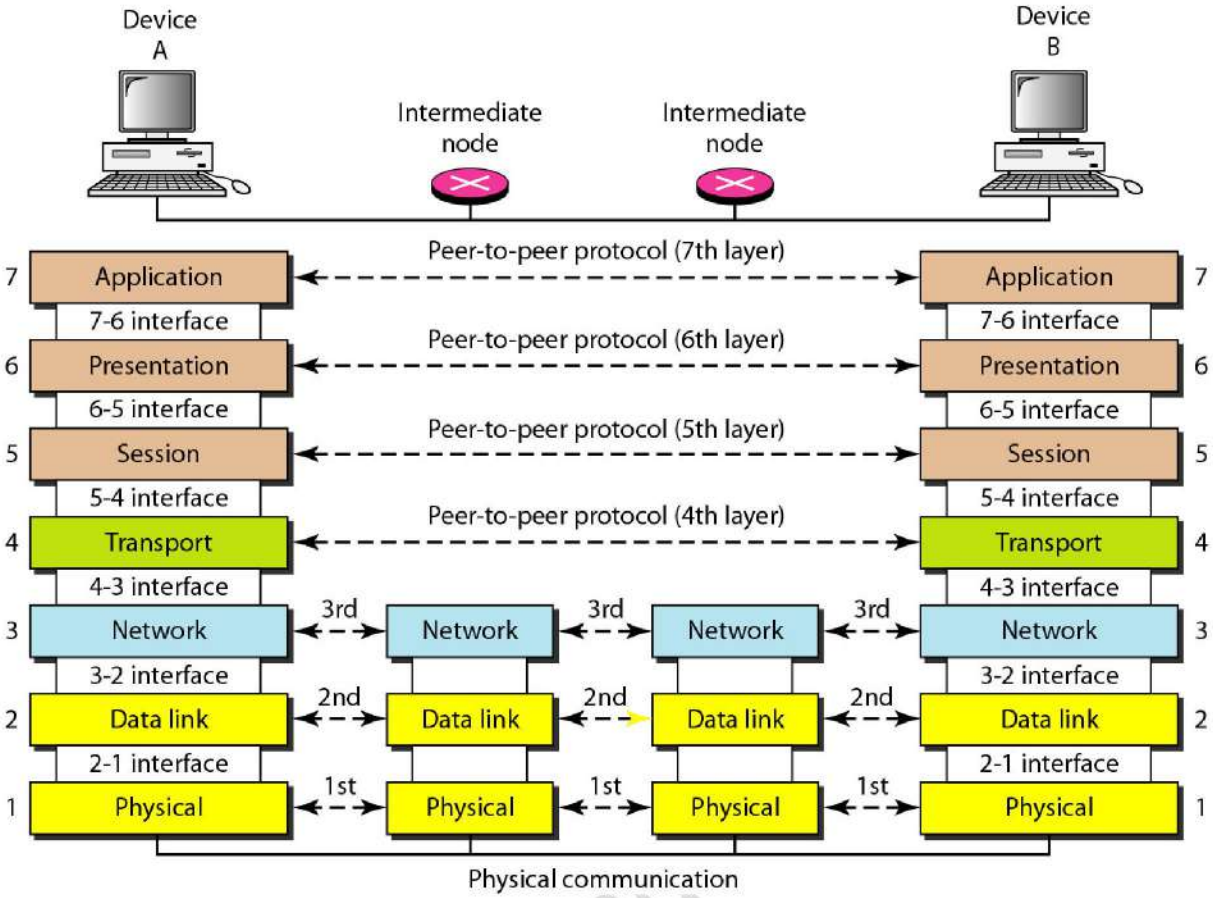
An ISO is the **Open Systems Interconnection** (OSI) model is the standard that covers all aspects of network communications from ISO. It was first introduced in the late 1970s.

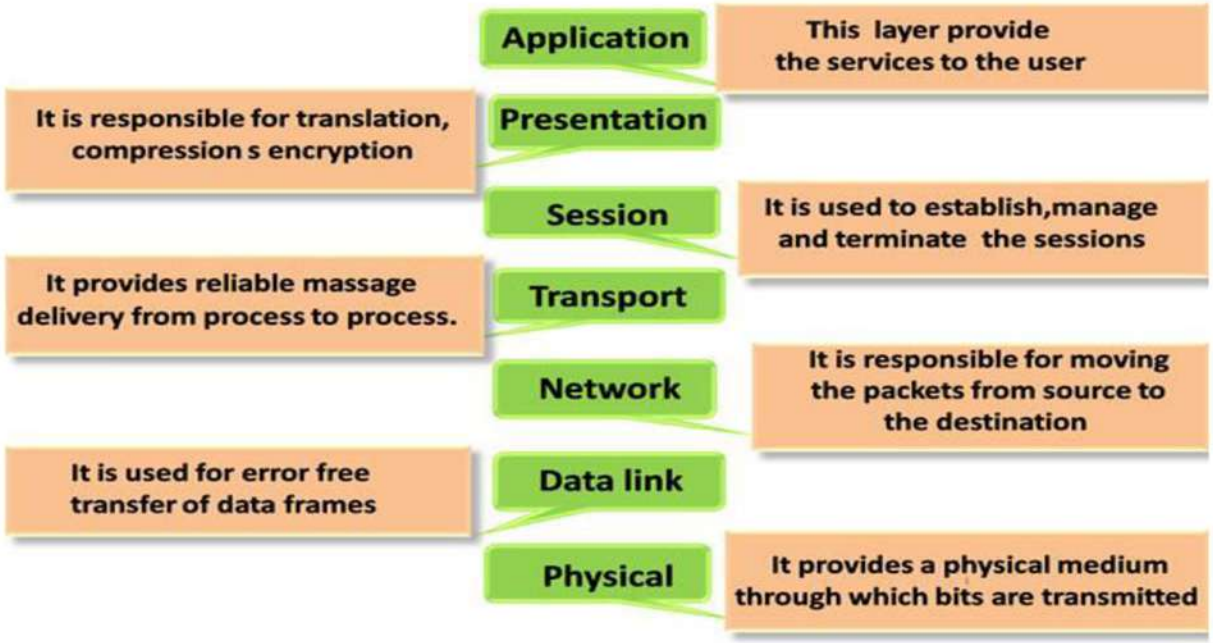
Layered Architecture:

- A layered model
- Each layer performs a subset of the required communication functions
- Each layer relies on the next lower layer to perform more primitive functions
- Each layer provides services to the next higher layer
- Changes in one layer should not require changes in other layers
- The processes on each machine at a given layer are called peer-to-peer process

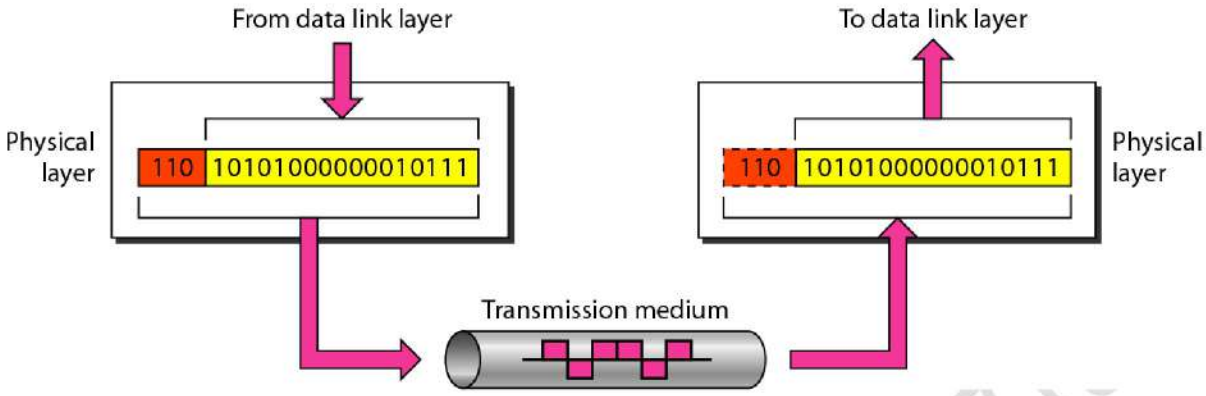
Peer-to-peer process:

- Communication must move downward through the layers on the sending device, over the communication channel, and upward to the receiving device
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it
- At the receiving device, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it
- The passing of the data and network information down through the layers of the sending device and backup through the layers of the receiving device is made possible by interface between each pair of adjacent layers
- Interface defines what information and services a layer must provide for the layer above it.


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication


Application
This layer provide the services to the user
It is responsible for translation, compression s encryption
Presentation
Session
It is used to establish,manage and terminate the sessions
It provides reliable massage delivery from process to process.
Transport
Network
It is responsible for moving the packets from source to the destination
It is used for error free transfer of data frames
Data link
Physical
It provides a physical medium through which bits are transmitted

1. Physical Layer (Layer 1):

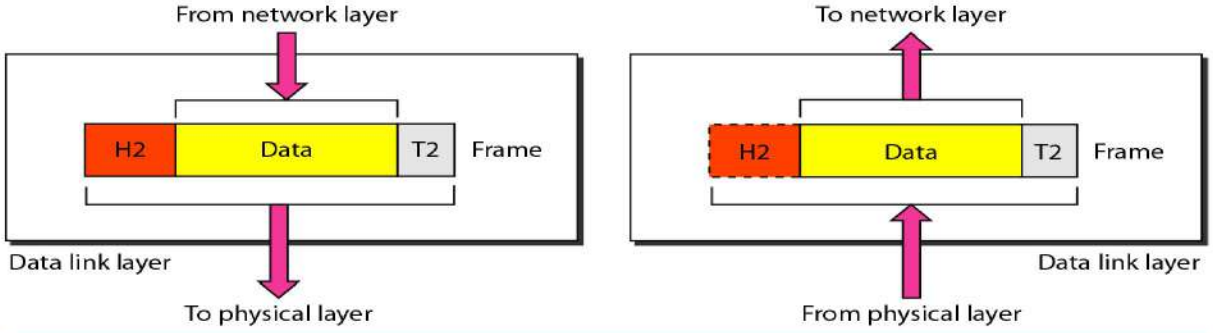


The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.**

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.
The functions of the physical layer are as follows:

1. **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 bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e., the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

2. Data Link Layer (DLL) (Layer 2):



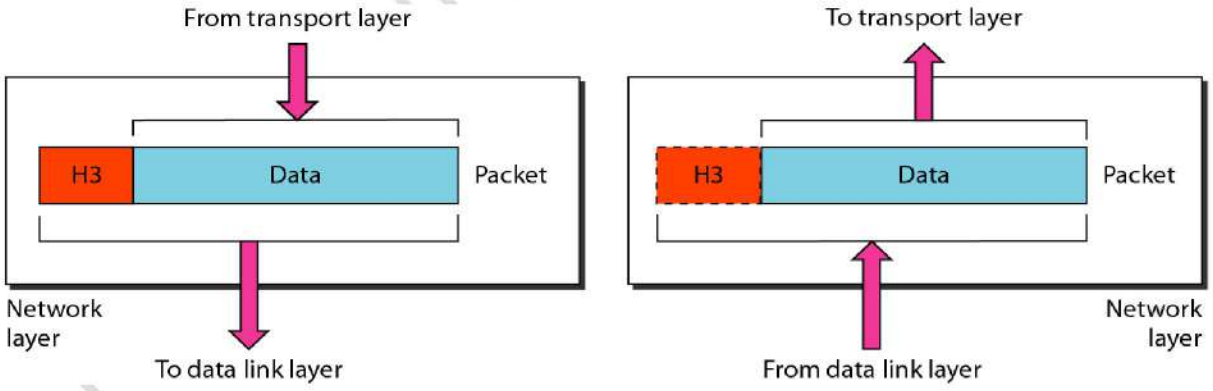
The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

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

The functions of the Data Link layer are:

1. **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.
2. **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC address) of the sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **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 acknowledgement.
5. **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.

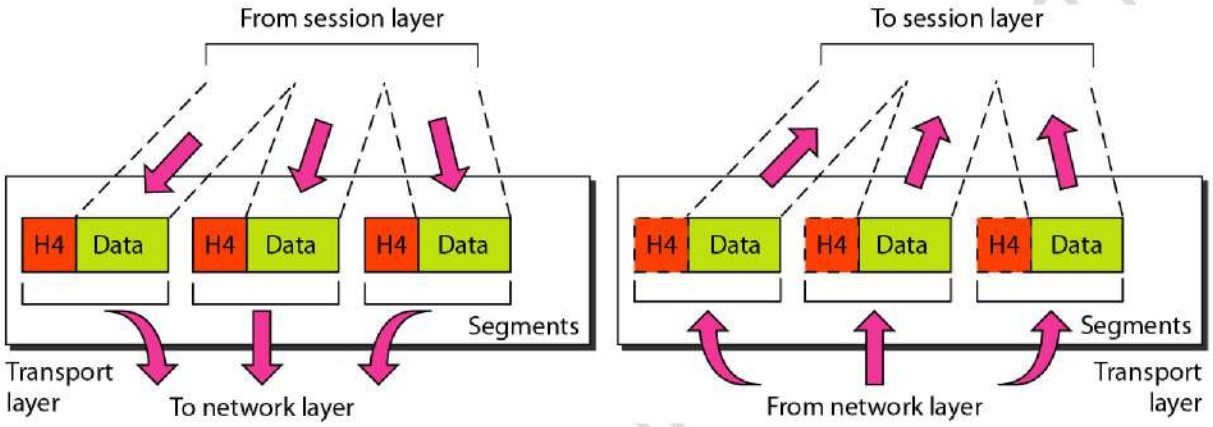
3. Network Layer (Layer 3):



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 functions of the Network layer are:

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order 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.

4. Transport 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 acknowledgement of the successful data transmission and re-transmits the data if an error is found.

- Process-to- process delivery
- Functions
  - **Port addressing:** In order to deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address.
  - **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.
  - **Connection control (Connection-oriented or connection-less):**
    - **Connection-less:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet.
    - **Connection-oriented:** It is a three-phase process that includes

Connection Establishment, Data Transfer, Termination / disconnection

In this type of transmission, the receiving device sends an acknowledgement

- Flow control:
- Error control

5. Session Layer:

The session layer is responsible for dialog control and synchronization.

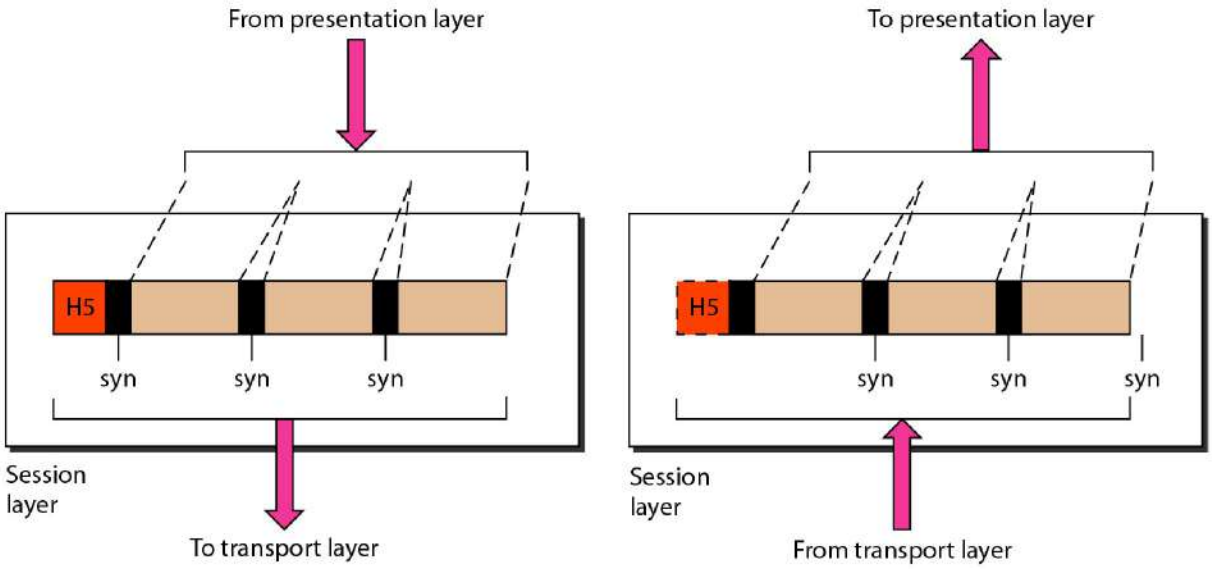
It establishes, maintains, and synchronize the interaction between communicating system

Functions

Dialog control

Synchronization (checkpoints)

1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into 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.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.



6. Presentation Layer:

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.
The functions of the presentation layer are :

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.

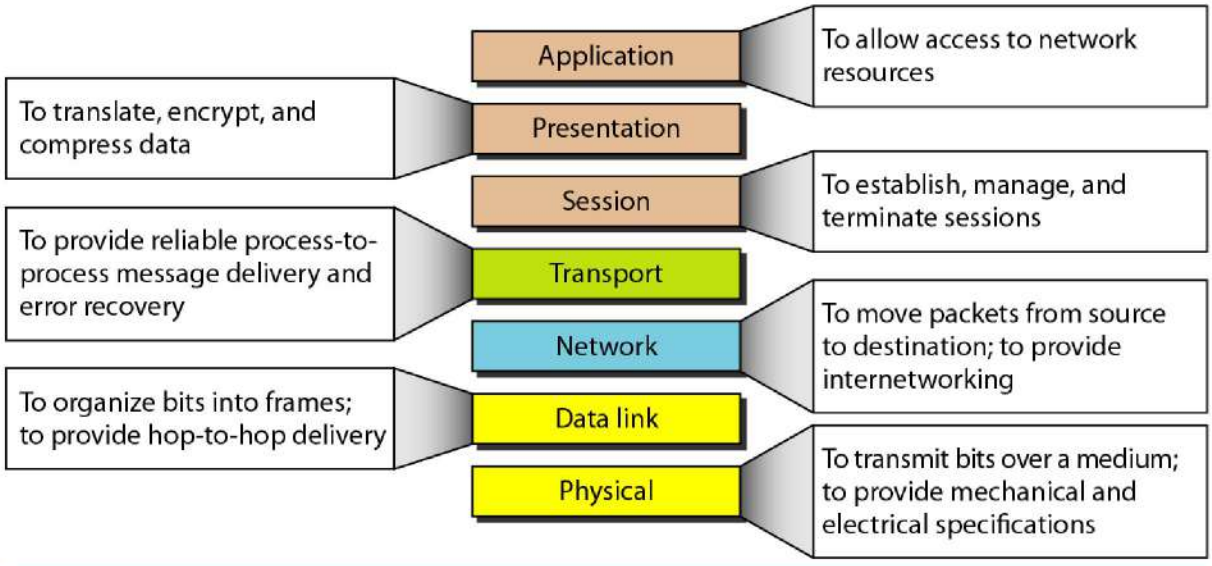
7. Application Layer:

The application layer is responsible for providing services to the user.

Functions

- Network virtual terminal (Remote log-in)
- File transfer and access
- Mail services
- Directory services (Distributed Database)
- Accessing the World Wide Web

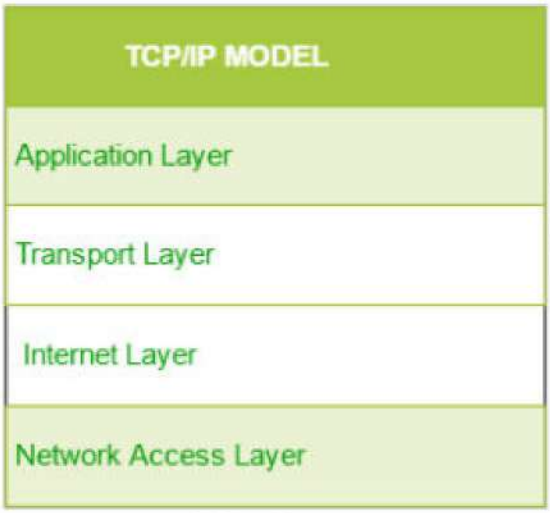
Summary of OSI Layered Architecture:



The TCP/IP reference model.

it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. 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:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer



1. Process/Application Layer:

The application layer is provided by the program that uses TCP/IP for communication.

An application is a user process cooperating with another process usually on a different host (there is also a benefit to application communication within a single host).

Examples of applications include Telnet and the File Transfer Protocol (FTP).

• The interface between the application and transport layers is defined by port numbers and sockets, Protocols at the application layer

- **HTTP:** – Browser and web server communication.
- **FTP:** – File transfer protocol, transmission of files between computers.
- **TELNET:** – Primary function is to allow user to log into remote host system in UNIX environment. DNS (Domain Name Service).

2. Host-to-Host/Transport Layer:

This layer is analogous to the transport layer of the OSI model. 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:

1. 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. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

2. 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.

3. 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 :

1. **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 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **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.

4. Network Access/Link Layer

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model.

It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.