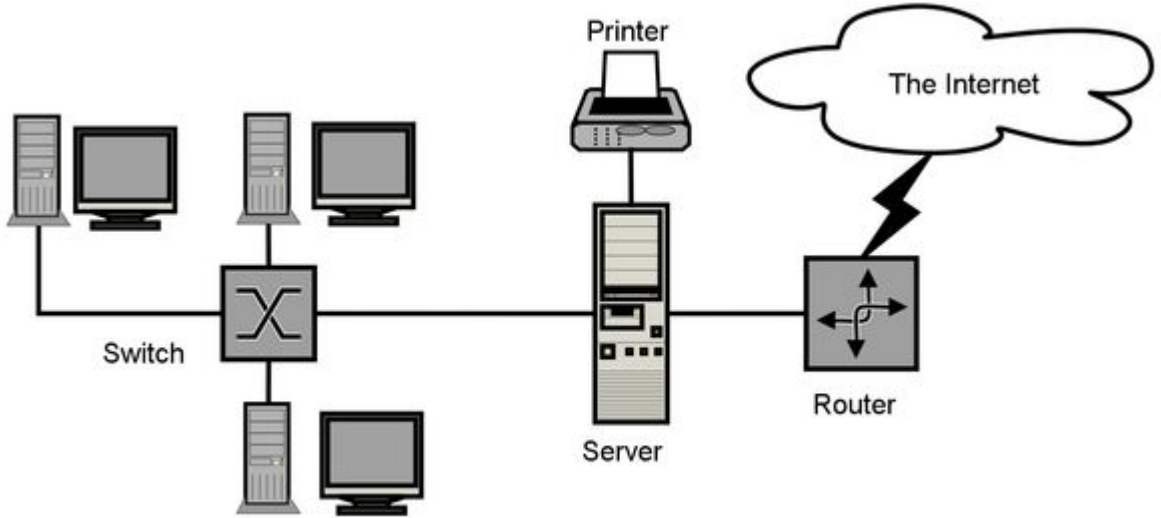
COMPUTER NETWORKS

I MODULE

Networks

- It is the interconnection of a set of devices capable of communication.
- A device can be a host like desktop, laptop, phone etc. or a connecting device like router or switch.
- These devices in a network are connected using wired or wireless transmission media.



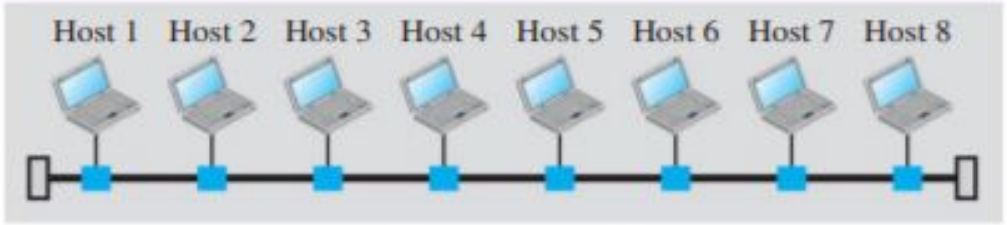
Uses of networks

- Information and resource sharing
- Retrieve remote information
- Speedy interpersonal communication
- E-commerce etc.

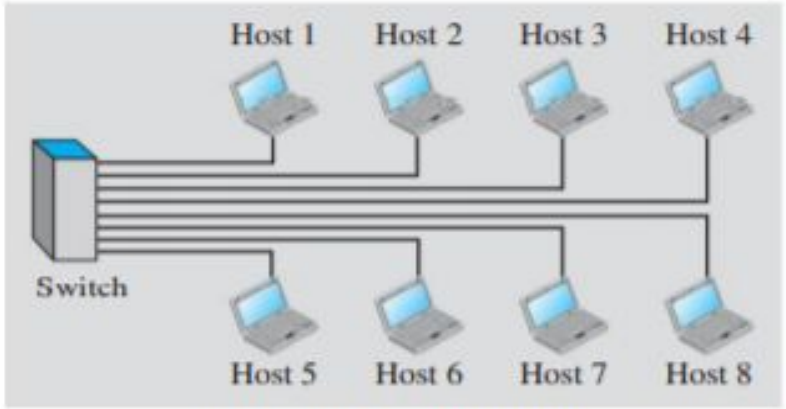
Types of networks

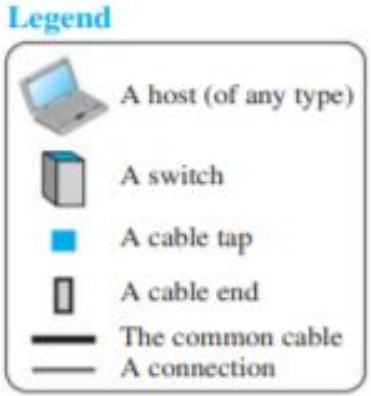
Local Area Networks(LAN):

- It is usually privately owned and connects some hosts in a single office, building, or campus.
- The group of computers and devices are connected together through a common cable or by a switch.
- LANs cover smaller geographical area may be from 1 km to 10 kms.
- The data transmission speed of LANs is much higher than in other types of networks(speed: 1 to 10Mbps).
- The error and noise are minimized because of their shorter distance.



a. LAN with a common cable (past)





b. LAN with a switch (today)

Metropolitan Area Networks(MAN):

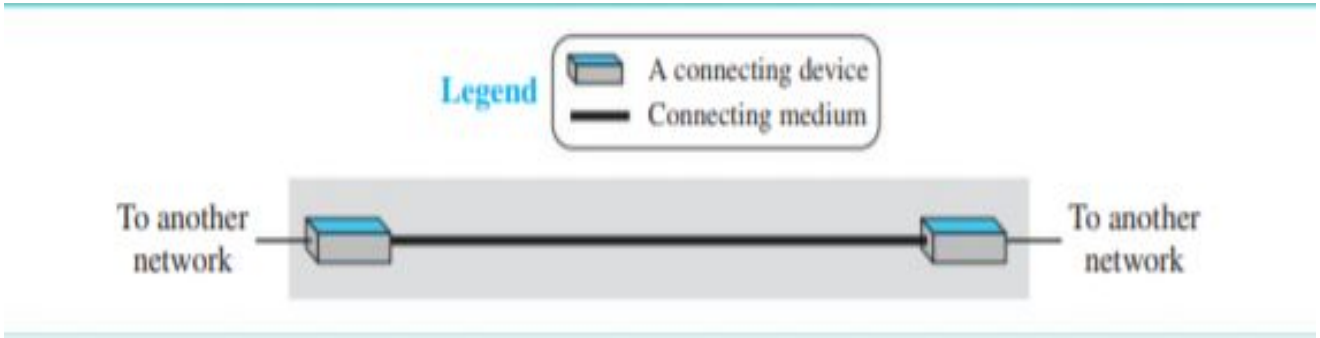
- It covers the larger area than LAN such as small towns, cities, etc.
- The fault tolerance is less and also there is more congestion in the network.
- The data transfer rate and the propagation delay of MAN is moderate.
- Eg: cable TV network in a city.

Wide Area Networks(WAN):

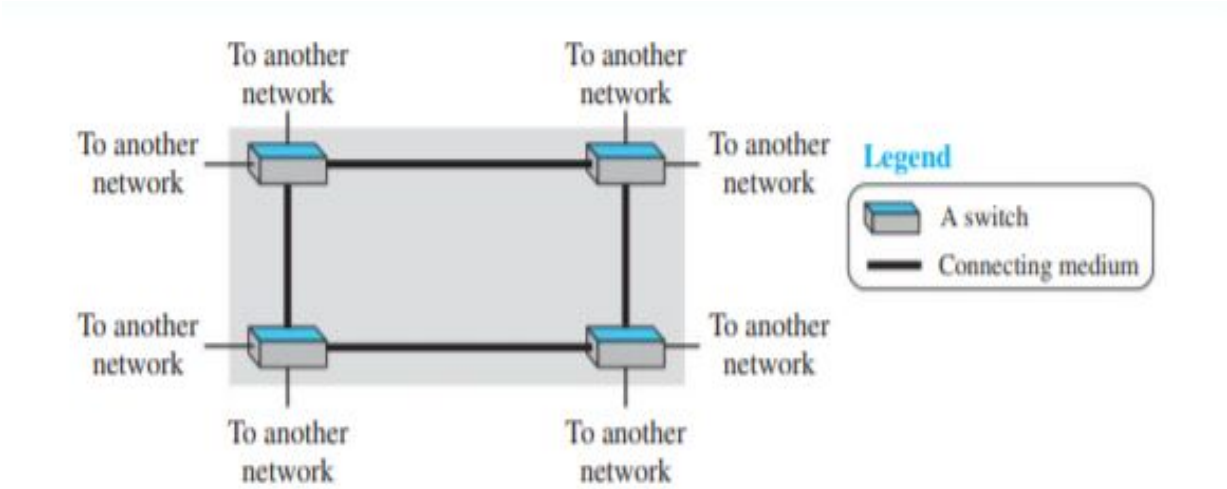
- Are computer networks that extends over a large geographical area, spanning a town, a state, a country, or even the world.
- a WAN interconnects connecting devices such as switches, routers, or modems.
- the fault tolerance of a WAN is less and there is more congestion in the network.
- Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites.

Types of WAN:

- **Point to point WAN**: is a network that connects two communicating devices through a transmission media (cable or air).
- Eg: a dial-up line that connects a home computer to the Internet.



- **Switched WAN:**
  - It is a combination of several point-to-point WANs that are connected by switches.



Internetwork:

- When two or more networks are connected, they make an internetwork.

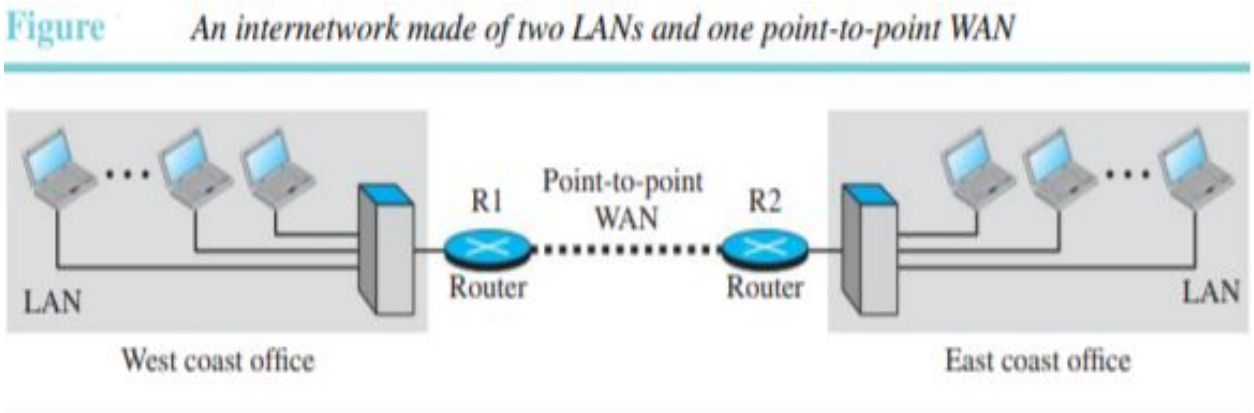
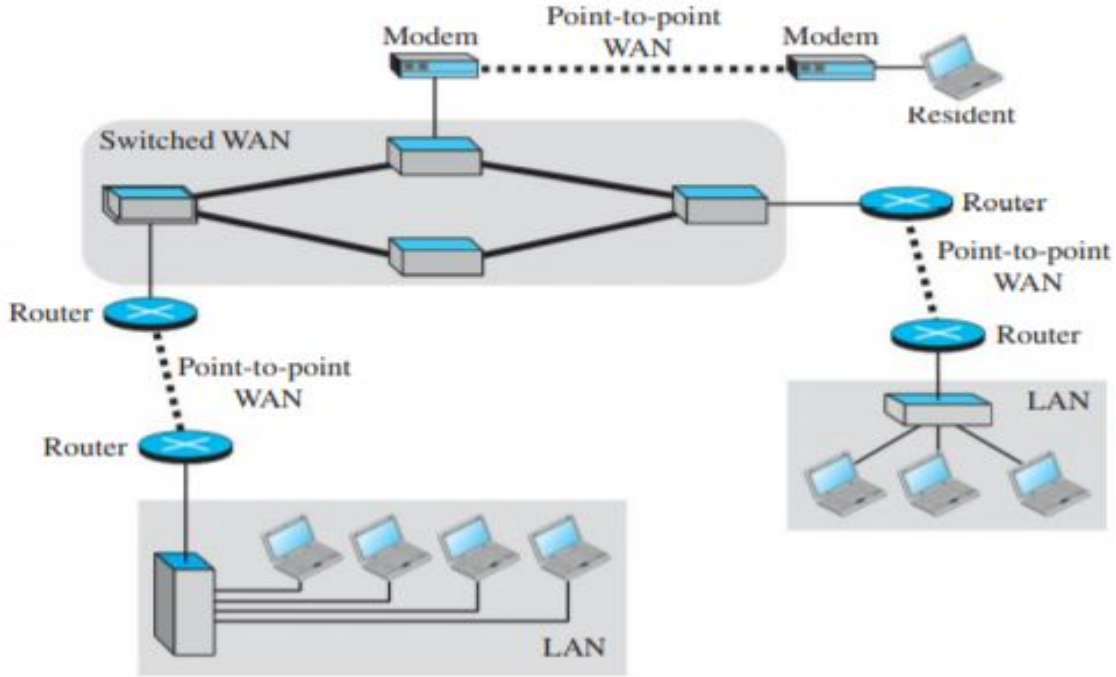
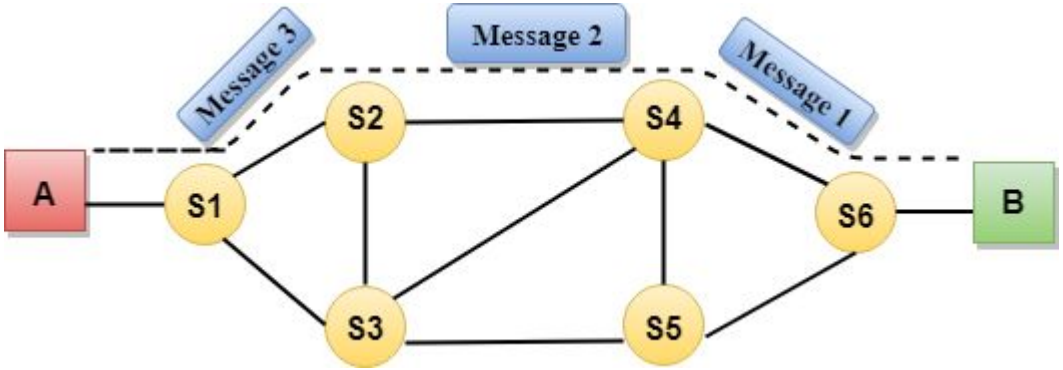


Figure *A heterogeneous network made of four WANs and three LANs*



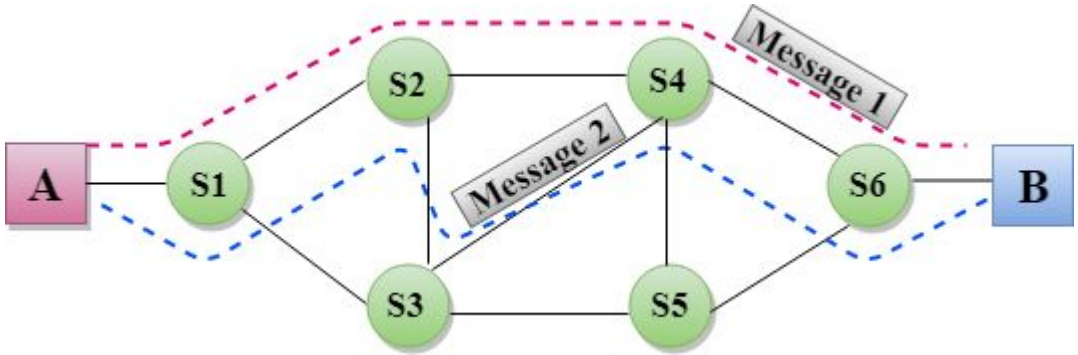
Switching

- It is the process of forwarding packets from an incoming port to the port that leads to the destination.
- i) Circuit Switching:
  - two nodes communicate with each other over a dedicated communication path.
  - 3 phases: establish a circuit, data transfer and disconnect the circuit.
  - Eg: telephonic conversation



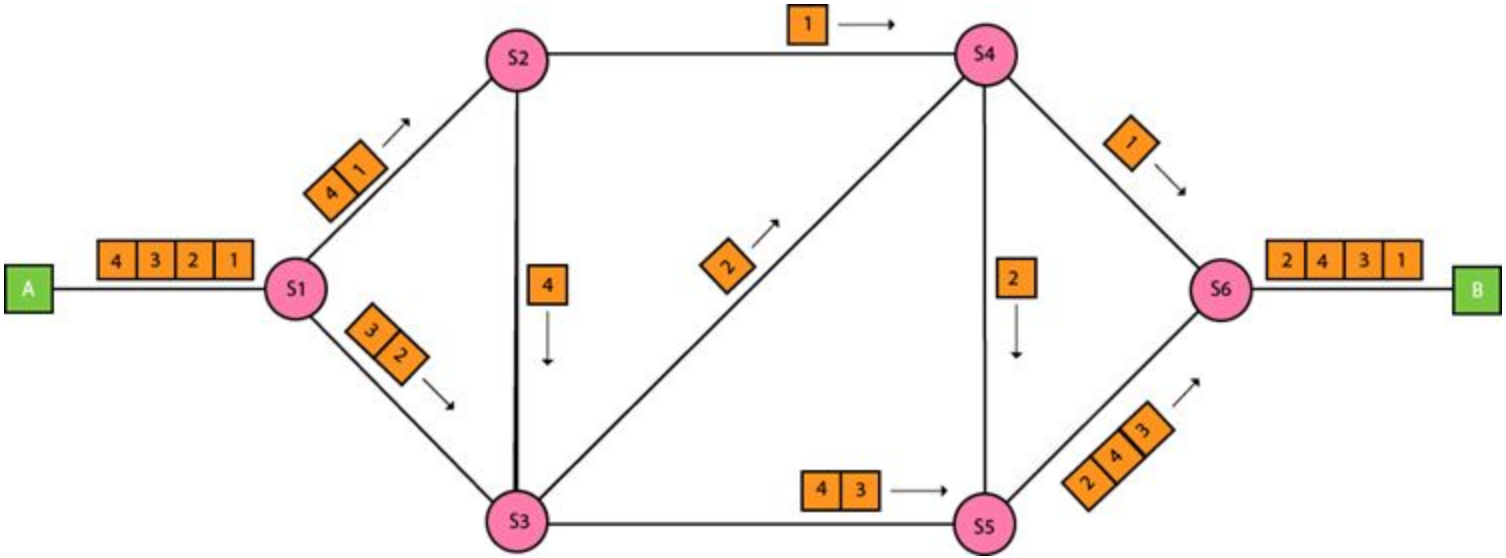
ii) Message switching:

- a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded
- No dedicated path is established between the sender and receiver
- the message is routed through the intermediate nodes based on the information available in the message.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**



iii) Packet switching:

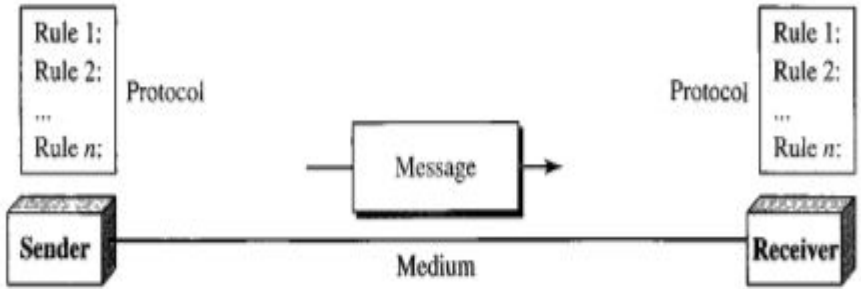
- Message is divided into blocks called packets each with a unique number.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible
- All the packets are reassembled at the receiving end in correct order
- If any packet is missing or corrupted, then the message will be sent to resend the message.


A
4 3 2 1
S1
S2
S3
S4
S5
S6
B
2 4 3 1
1
4 1
3 2
4
2
2
1
4 3
2 4 3

Basic Communications Model

- Data communication is the exchange of data between two devices via a transmission medium which can be either wired or wireless.
-

Figure 1.1 *Five components of data communication*



i) Message: data to be communicated

ii) Sender: the device that sends the message.

iii) Receiver: the device that receives the message.

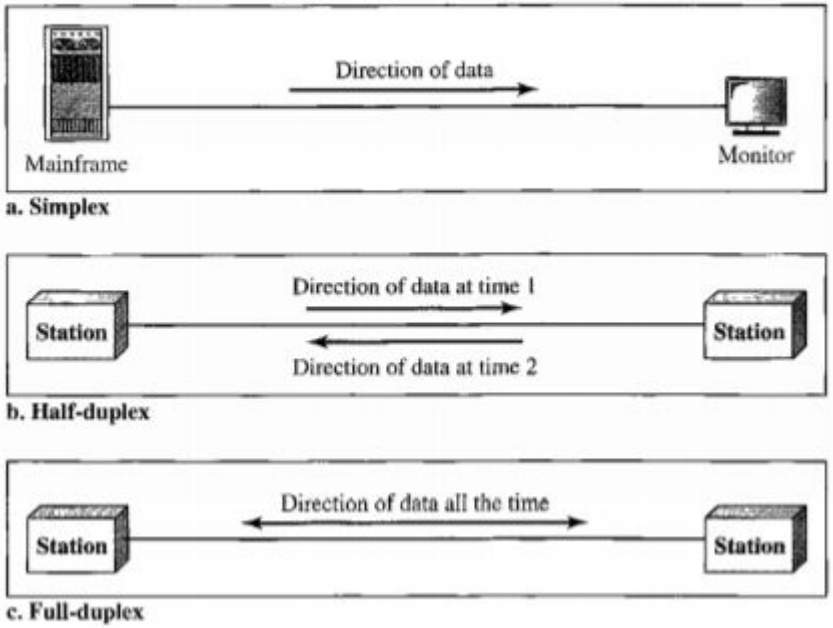
iv) Transmission medium: physical path by which the message travels from sender to receiver.

v) Protocol: set of rules that govern the communication.

Data Flow

Communication can be simplex, half-duplex or full-duplex.

Figure *Data flow (simplex, half-duplex, and full-duplex)*



Simplex Mode

- the communication is unidirectional.
- Only one of the two devices on a link can transmit, the other can only receive.
- The simplex mode can use the entire capacity of the channel to send data in one direction.
- Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.

Half-Duplex Mode

- In half-duplex mode, each station can both transmit and receive, but not at the same time.
- When one device is sending, the other can only receive, and vice versa.
- The entire capacity of the channel can be utilized for each direction.
- Example: Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

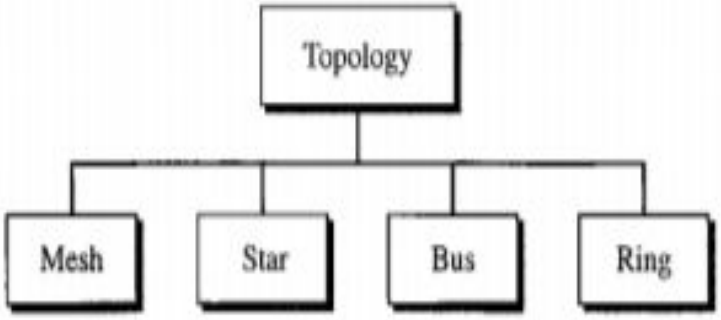
Full-Duplex Mode

- In full-duplex mode, both stations can transmit and receive simultaneously.
- In full_duplex mode, signals going in one direction share the capacity of the link with signals going in other direction, this sharing can occur in two ways:
    - •Either the link must contain two physically separate transmission paths, one for sending and other for receiving.
    - •Or the capacity is divided between signals travelling in both directions.
- The capacity of the channel, however must be divided between the two directions.
- Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

Network Topologies

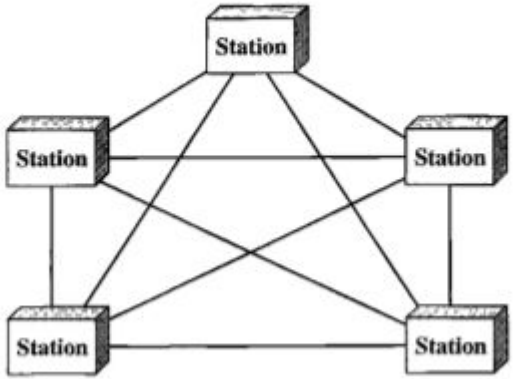
- The way in which the network is laid out physically.
-

Figure *Categories of topology*



i) Mesh Topology: every device has a dedicated point to point link to every other device.

Figure *A fully connected mesh topology (five devices)*



- If N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1 and the total number of dedicated links required to connect them is N(N-1)/2.

Advantages:

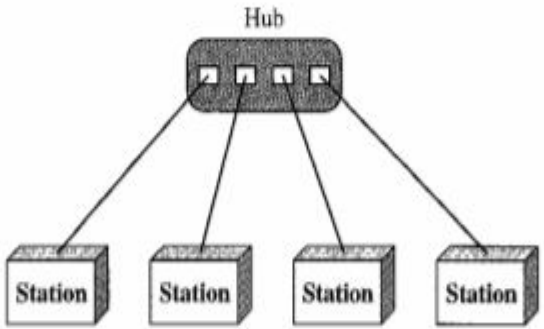
- It is robust.
- The fault is diagnosed easily.
- Provides security and privacy.

Disadvantages:

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

ii) Star topology: each device has a dedicated point to point link only to a central controller, usually called hub.

Figure A star topology connecting four stations



- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.

Advantages:

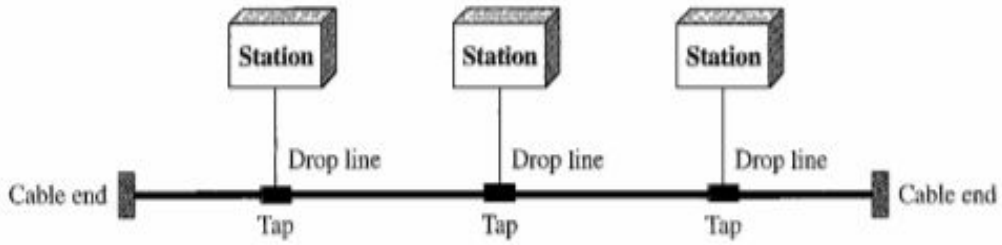
- Easy to set up
- Fault identification easy.

Disadvantages:

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.

iii) Bus topology: a multi-point connection; all the devices in the network are connected to a single cable.

Figure *A bus topology connecting three stations*



- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is known as backbone cable, and N drop lines are required.

Advantages:

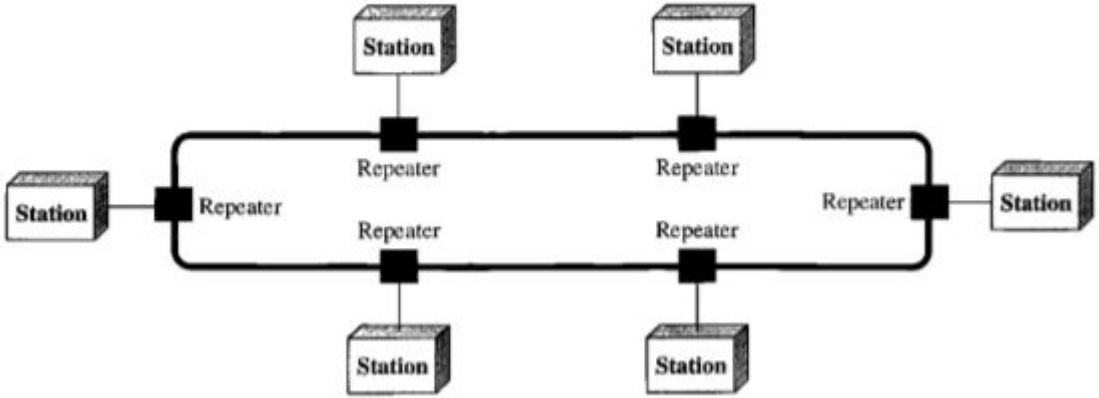
- The cost of the cable is less as compared to other topologies, but it is used to build small networks.
- Easy to connect a device to the bus.

Disadvantages:

- If the common cable fails, then the whole system will crash down.
- Terminators are required at both ends of the backbone cable.
- If the network traffic is heavy, it increases collisions in the network.
- Security is very low.
- Fault identification is difficult

iv) Ring topology: Each device has a dedicated point to point link with only the two devices on either side of it.

Figure *A ring topology connecting six stations*



- to prevent data loss repeaters are used in the network.

Advantages:

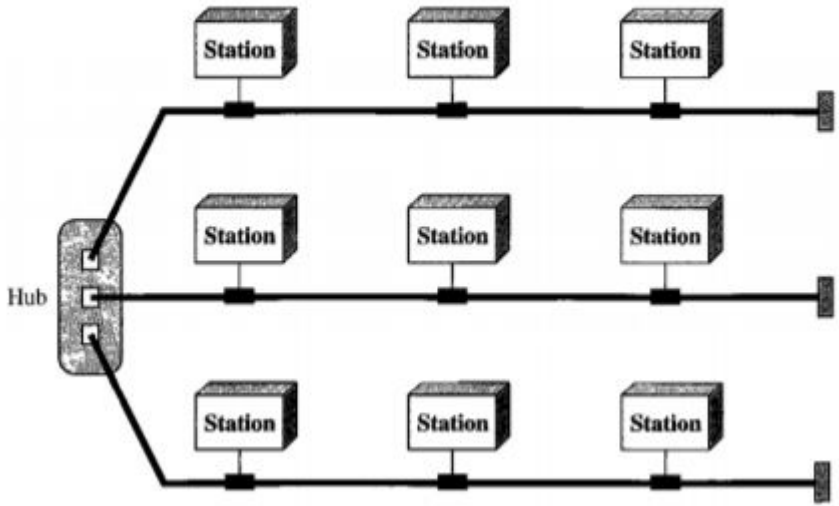
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Disadvantages:

- Troubleshooting is difficult in this topology.
- The addition of stations in between or removal of stations can disturb the whole topology.
- Less secure.
- Slow transmission across the ring network
- If any of the nodes fail, then the ring breaks and stops the transmission of data.

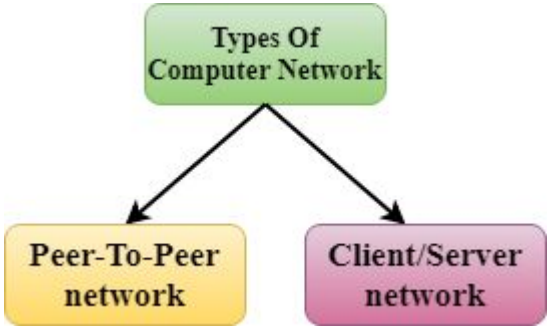
v) Hybrid topology:

Figure *A hybrid topology: a star backbone with three bus networks*



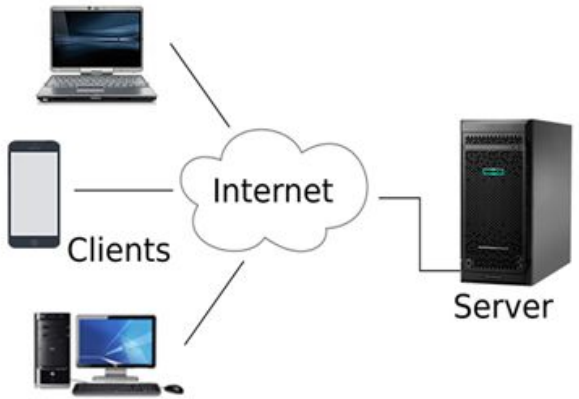
Network Architecture

- It is the overall design of the computer network that describes how a network is configured and what strategies are being used.
- It aims at the functions of the network.
- Two network architectures are:



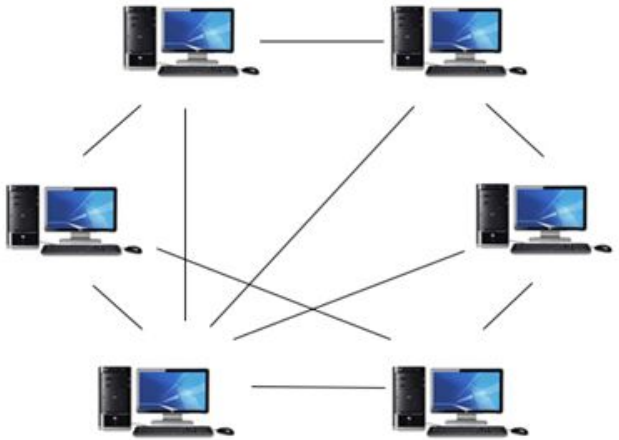
1) Client/Server Architecture:

- Client/Server network is a network model designed for the end users called clients, to access the resources 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, manages all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server.



2) 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.
- 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.



PROTOCOL LAYERING

- A protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.
- For simple communication, we need only a simple protocol.
- For complex communication, we may have to divide the task into different layers each having its own protocol(protocol layering).

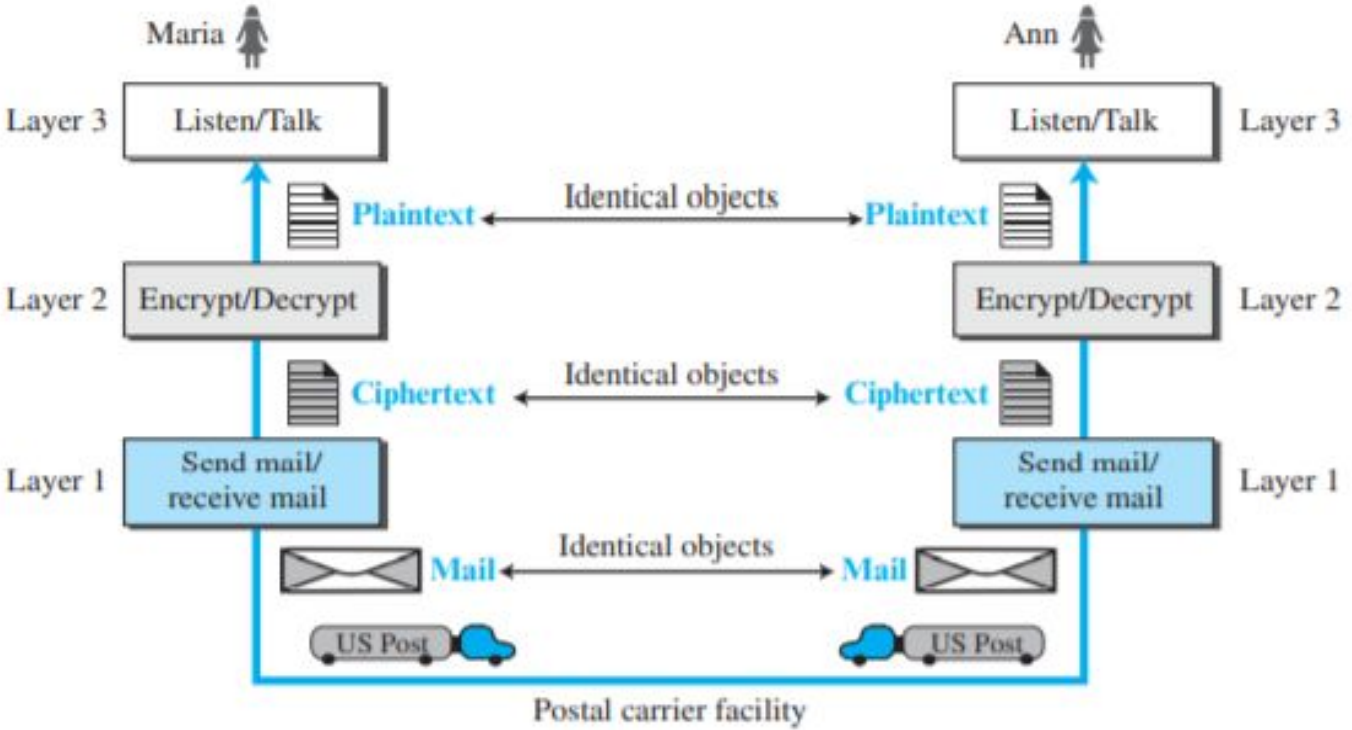
Why layering ?

Dealing with complex systems:

- explicit structure allows identification, relationship of complex system’s pieces
- modularization eases maintenance, updating of system
    - change of implementation of layer’s service transparent to rest of system

Figure *A single-layer protocol*

Figure 1.10 *A three-layer protocol*

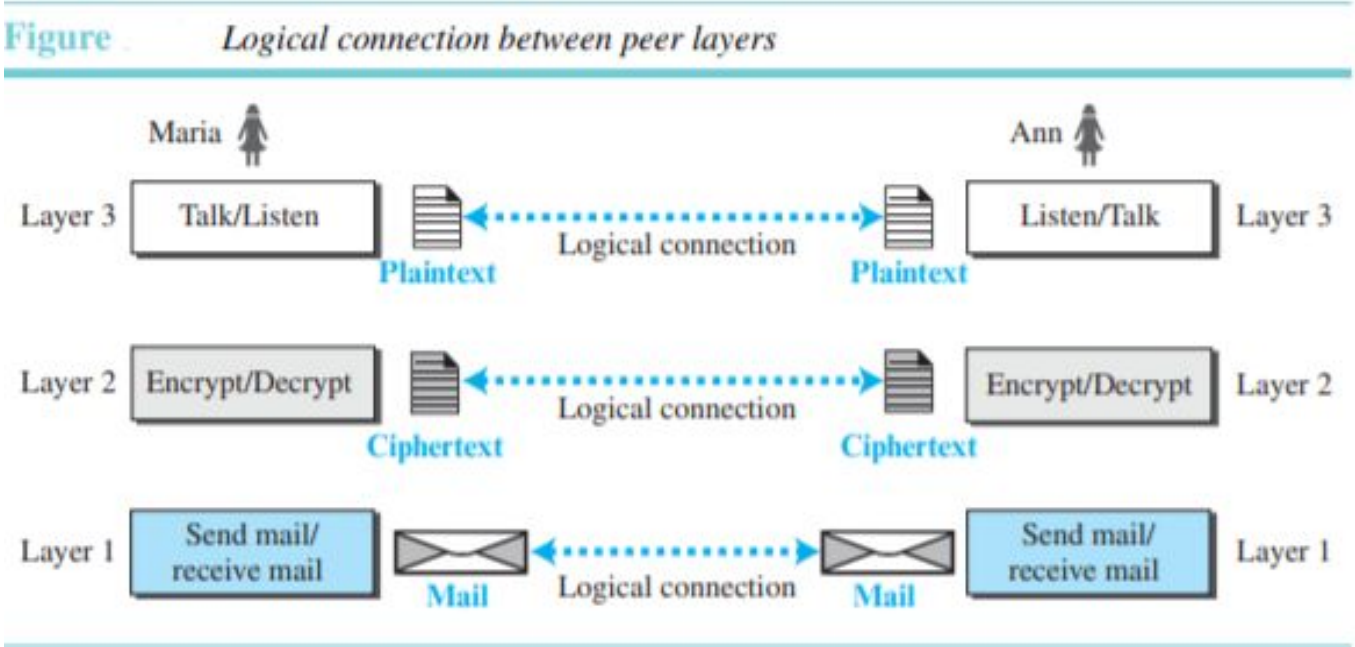


Principles of Protocol Layering

i) For bidirectional communication, each layer must perform two opposite tasks, one in each direction.

ii) the two objects under each layer at both sites should be identical.

Logical Connections



OSI Model(Open System Interconnection)

- It is an ISO standard that covers all aspects of network communications.
- An **open system** is a set of protocols that allows any two systems to communicate regardless of their underlying architecture.
- OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems.

Figure *Seven layers of the OSI model*

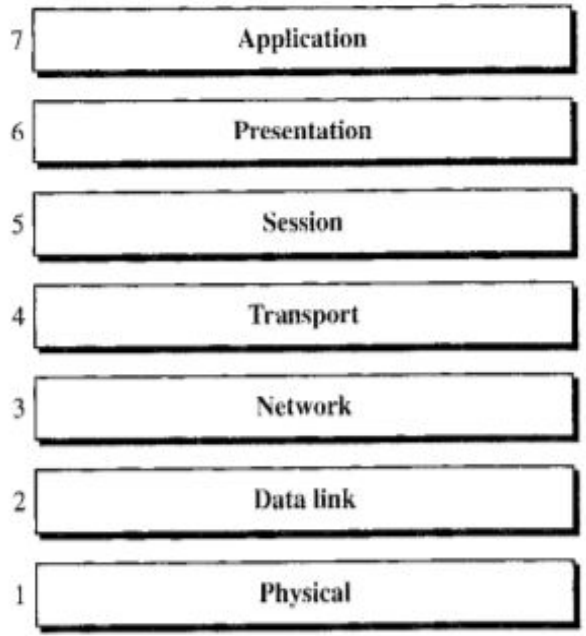
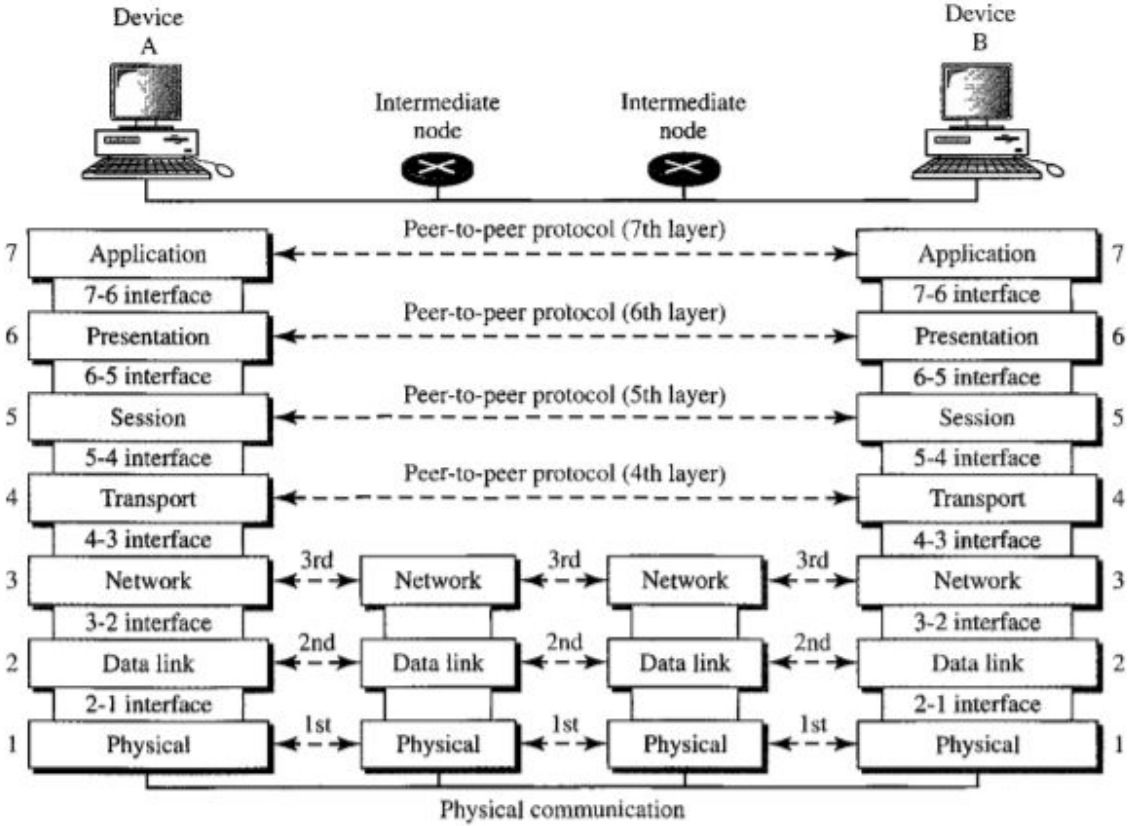


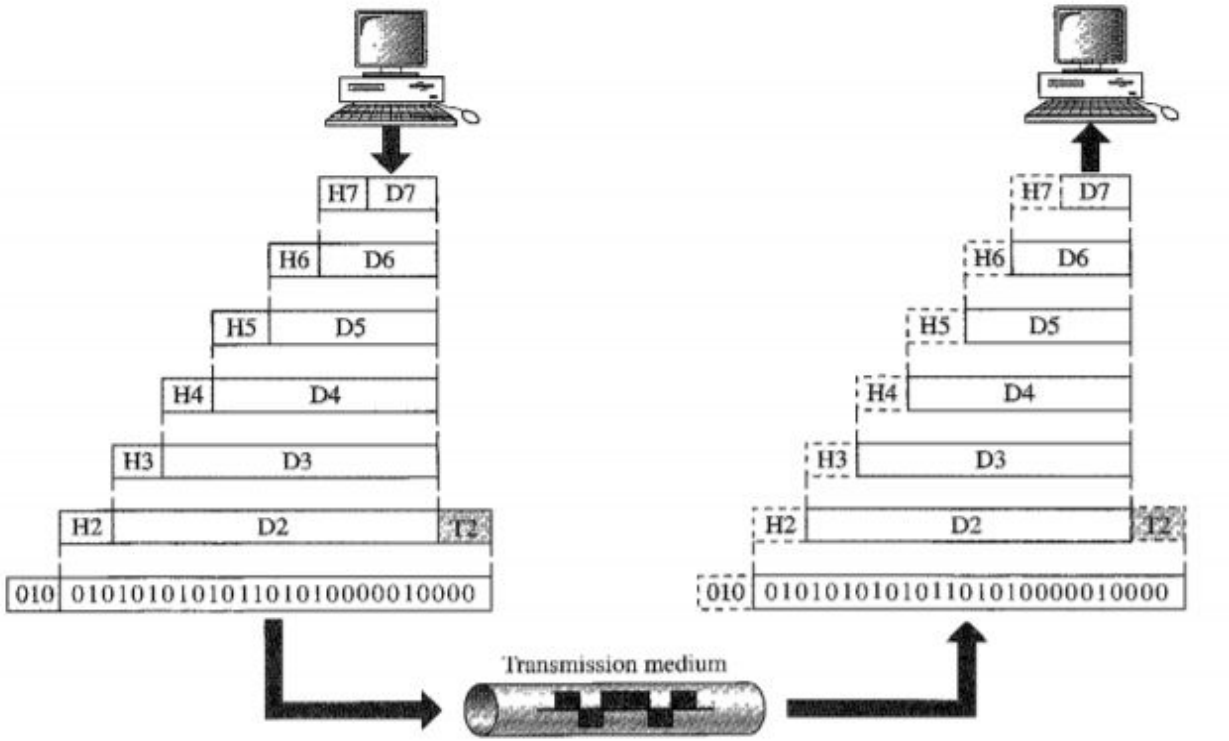
Figure *The interaction between layers in the OSI model*



- Each layer has a set of unique functions.
- Each layer uses the services provided by the lower layer and provides services to the upper layer.
- Between machines, layer x on one machine communicates with layer x on the other machine.
- The processes on each machine that communicate at a given layer are called peer to peer processes.
- Each layer in the sending device adds its own information to the message it received from the upper layer and passes the whole package to the lower layer.
- At the receiving side, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.
- The passing of data and network information between the layers is made possible by an **interface** between each pair of adjacent layers.

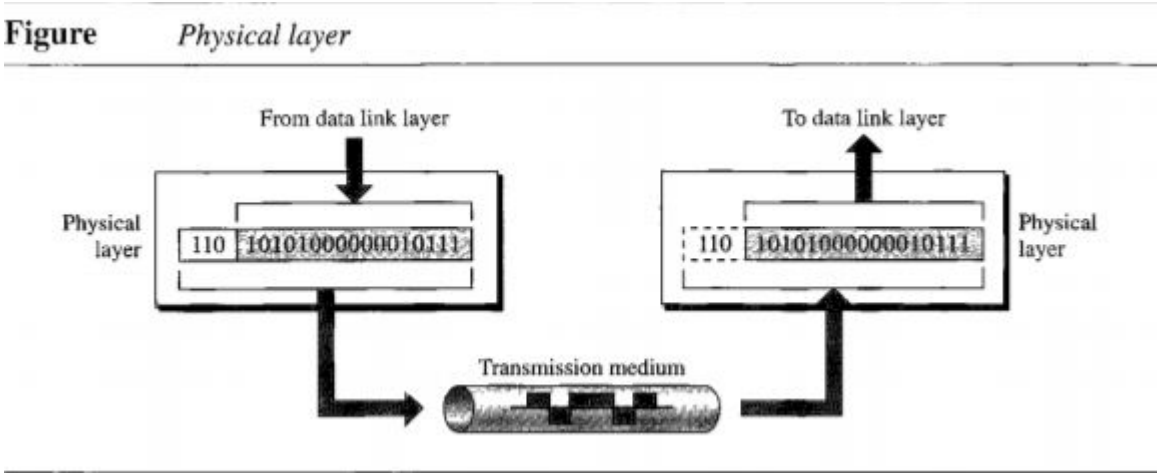
- Layers can be grouped as:
    - Network support layers:
        - Physical, data link and network.
        - They deal with the physical aspects of sending data from one device to another.
    - User support layers:
        - Session, presentation and application
        - They allow interoperability among unrelated software systems.
    - The network layer links the two subgroups.
- The upper OSI layers are usually software whereas lower layers are a combination of hardware and software. (Physical layer is but mostly hardware).

Figure *An exchange using the OSI model*



Layers in the OSI Model

1) Physical Layer:
   - It deals with the transmission of bit streams over the transmission medium.
   - It handles the mechanical and electrical specifications of the medium.



Physical layer also handles the following:

- Physical characteristics of interfaces and medium
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode

The physical layer is also concerned with the following:

•**Physical characteristics of interfaces and media**. The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media.

•**Representation of bits**. The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals . The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

•**Data rate**. The transmission rate - the number of bits sent each second—is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

•**Synchronization of bits**. The sender and receiver must not only use the same bit rate but must also be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

- Line configuration. The Physical layer is concerned with the connection of devices to the media. In a **point-to-point configuration**, two devices are connected together through a dedicated link. In a **multipoint configuration**, a link is shared between several devices.

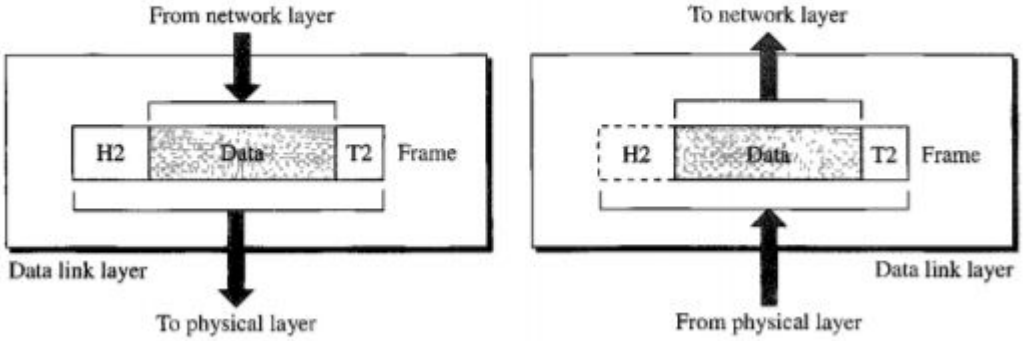
•**Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh topology (every device connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), or a bus topology (every device on a common link).

•**Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data Link Layer

- It is responsible for the node to node delivery of the message.
- It makes sure that data transfer is error-free from one node to another, over the physical layer.

Figure : *Data link layer*



- Framing
- Physical Addressing
- Flow Control
- Error Control
- Access Control

•**Flow control.** If the rate at which the data is absorbed by the receiver is less than the rate produced at the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

•**Error control**. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames.

It also uses a mechanism to recognize duplicate frames.

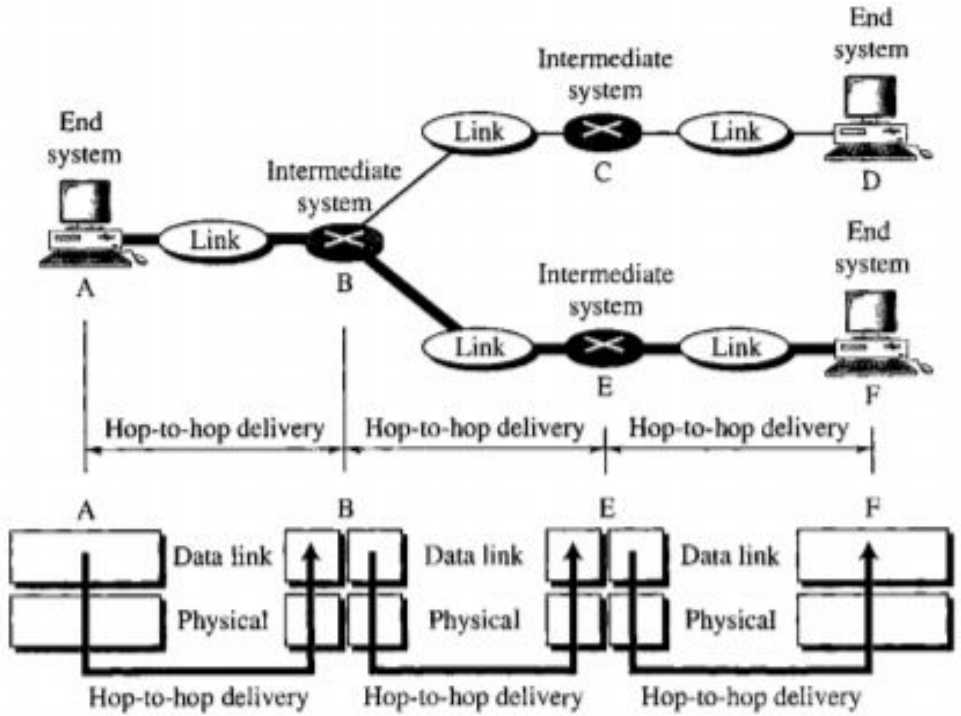
Error control is normally achieved through a trailer added to the end of the frame.

•**Access control**: when two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

•**Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

•**Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the connecting device that connects the network to the next one.

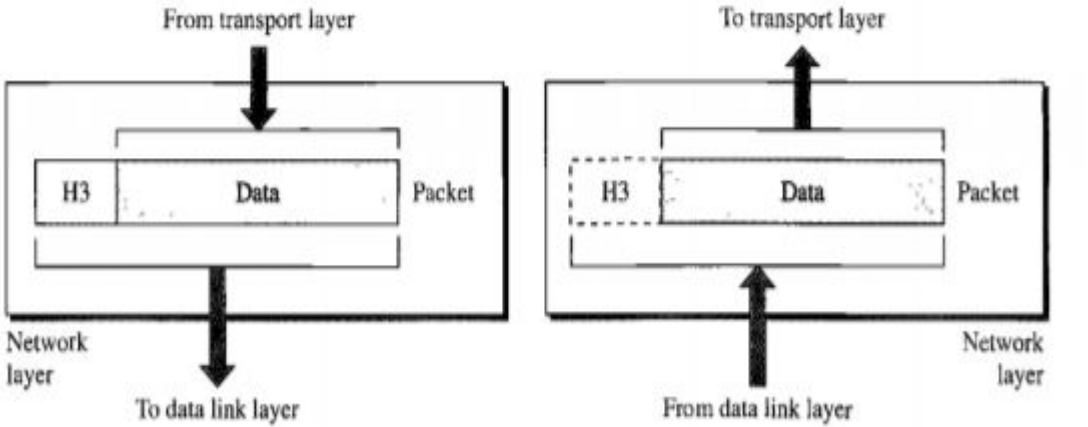
Figure *Hop-to-hop delivery*



Network Layer

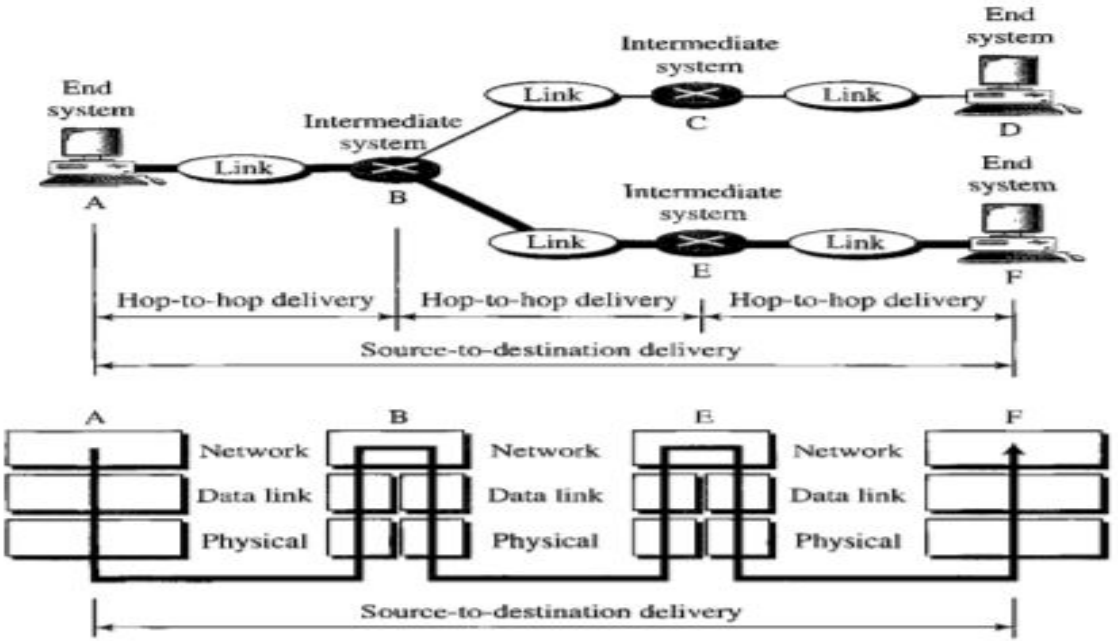
- It is responsible for source to destination delivery of a packet.
-

Figure *Network layer*



- Logical Addressing
- Routing

Figure *Source-to-destination delivery*



- **Logical addressing**.

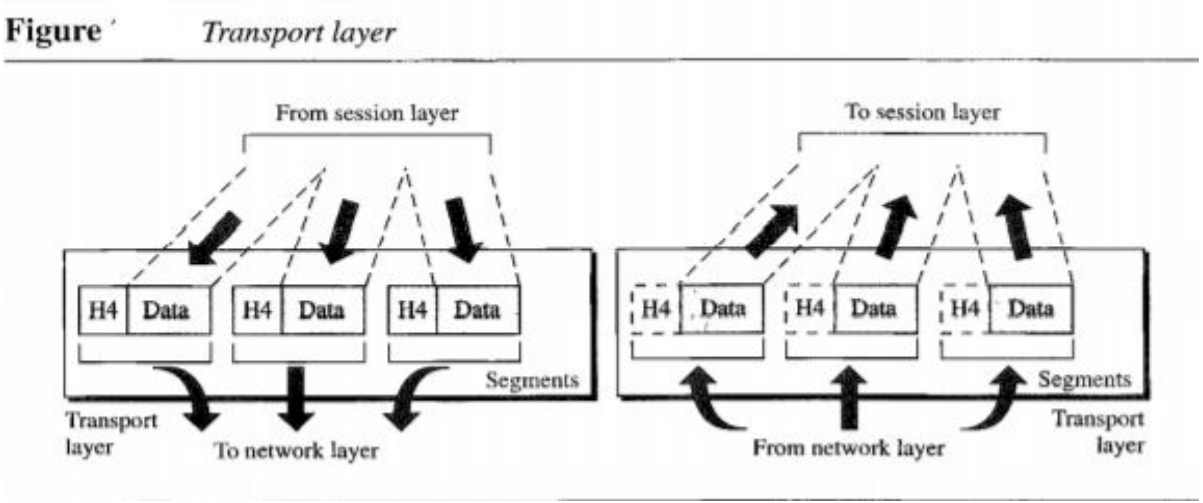
- The physical addressing implemented by the data link layer handles the addressing problem locally.
- If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems.
- The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

- **Routing.**

- When independent networks or links are connected together to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.
- One of the functions of the network layer is to provide this mechanism.

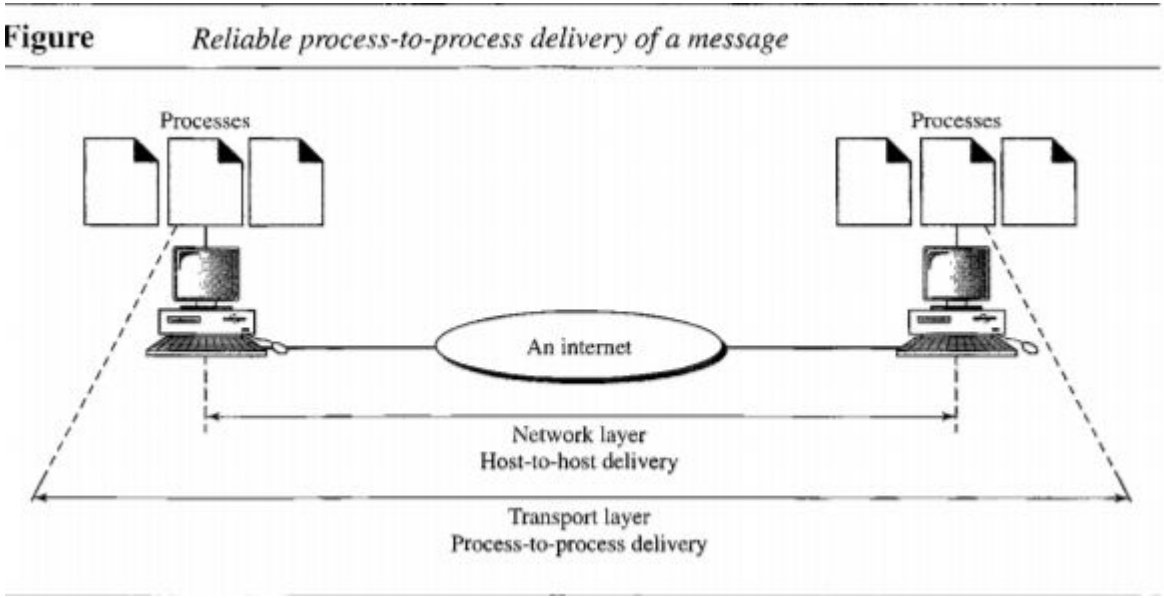
Transport Layer

- Responsible for process to process delivery of the entire message.
- Process means an application running on a host
- Ensures that the whole message arrives intact and in order



Functionalities:

- Service point addressing (port address)
- Segmentation and reassembly
- Connection control
- Flow control
- Error control



Service-point addressing

•Computers often run several programs at the same time.

• For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other.
The transport layer header must therefore include a type of address called **a service- point address (or port address).**

• The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

•Segmentation and reassembly

•A message is divided into transmittable segments, with each segment containing a sequence number.

•These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

•**Connection control**

•The transport layer can be either connectionless or connection- oriented.

• A **connectionless transport layer** treats each segment as an independent packet and delivers it to the transport layer at the destination machine.

•A **connection- oriented transport layer** make a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated

•**Flow control.**

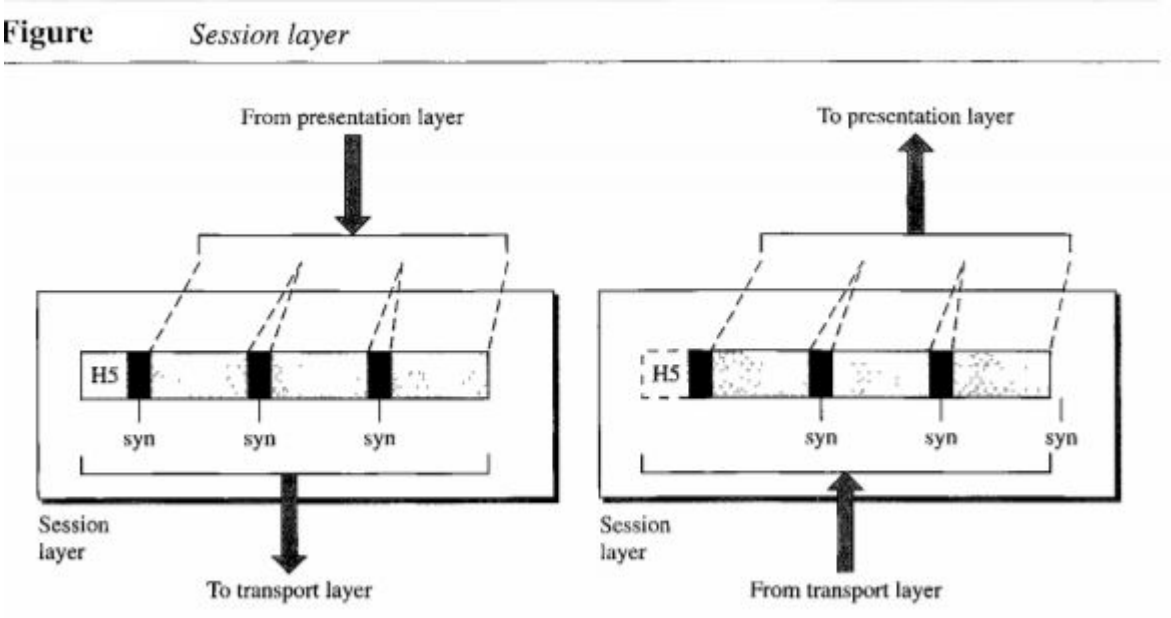
•Like the data link layer, the transport layer is responsible for flow control.
•However, flow control at this layer is performed end to end rather than across a single link.

Error control.

- Like the data link layer, the transport layer is responsible for error control.
- However, error control at this layer is performed process-to-process rather than across a single link.
- The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).
- Error correction is usually achieved through retransmission.

Session Layer

- It is the network dialog controller
- It establishes, maintains and synchronizes the interaction among communicating devices.
- Functionalities:
  - Dialog control
  - synchronization



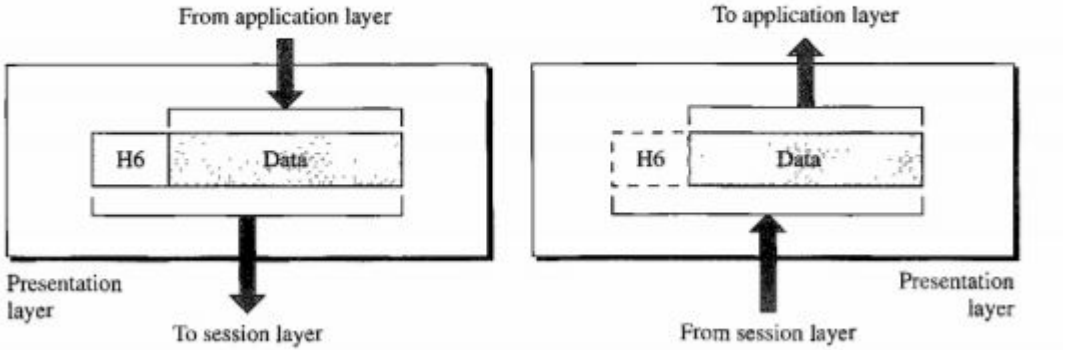
•**Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.

• **Synchronization.** The session layer allows a process to add checkpoints (synchronization points) into a stream of data.

Presentation Layer

- Deals with the syntax and semantics of the information exchanged between two systems.

Figure *Presentation layer*



Other functionalities:

- Translation
- Encryption
- Compression

Translation.

•The presentation layer at the sender changes the information from its sender-dependent format into a common format.

•The presentation layer at the receiving machine changes the common format into its receiver- dependent format.

Encryption

•To carry sensitive information a system must be able to assure privacy.

•Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.

•Decryption reverses the original process to transform the message back to its original form.

Compression.

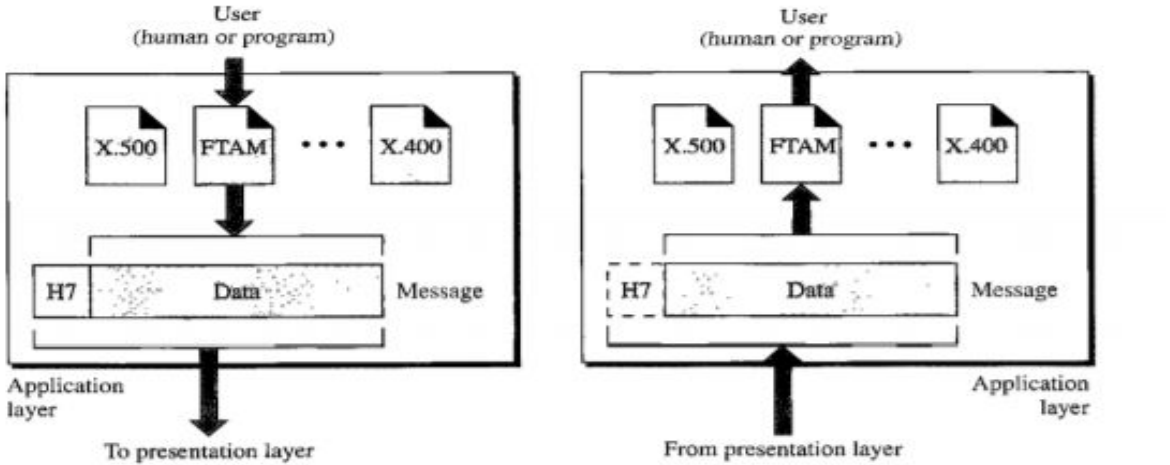
•Data compression reduces the number of bits contained in the information.

•Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer

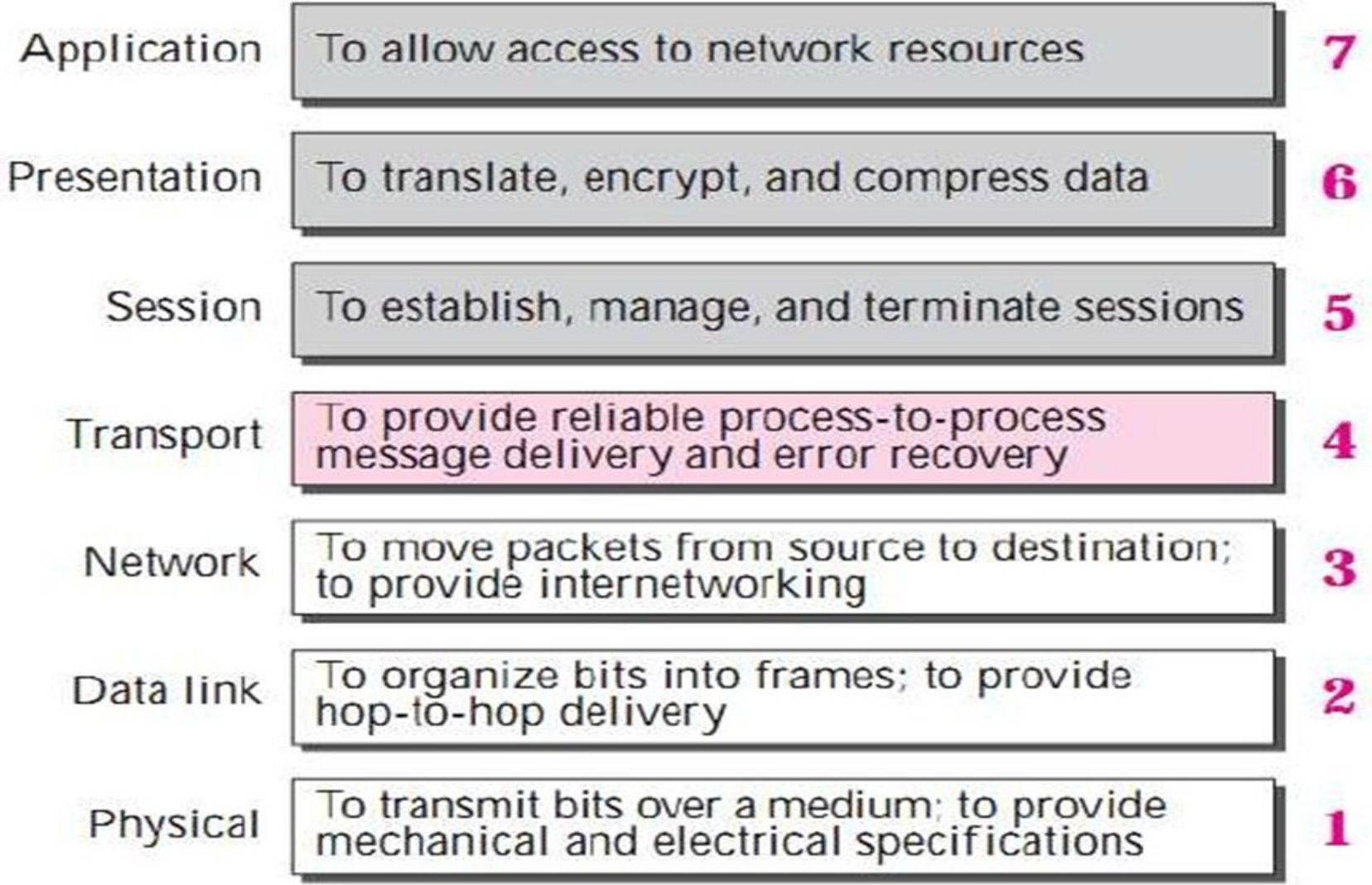
- It is the layer where user-computer interaction takes place directly
- Is responsible for providing services to the user
-

Figure *Application layer*



Some services are:

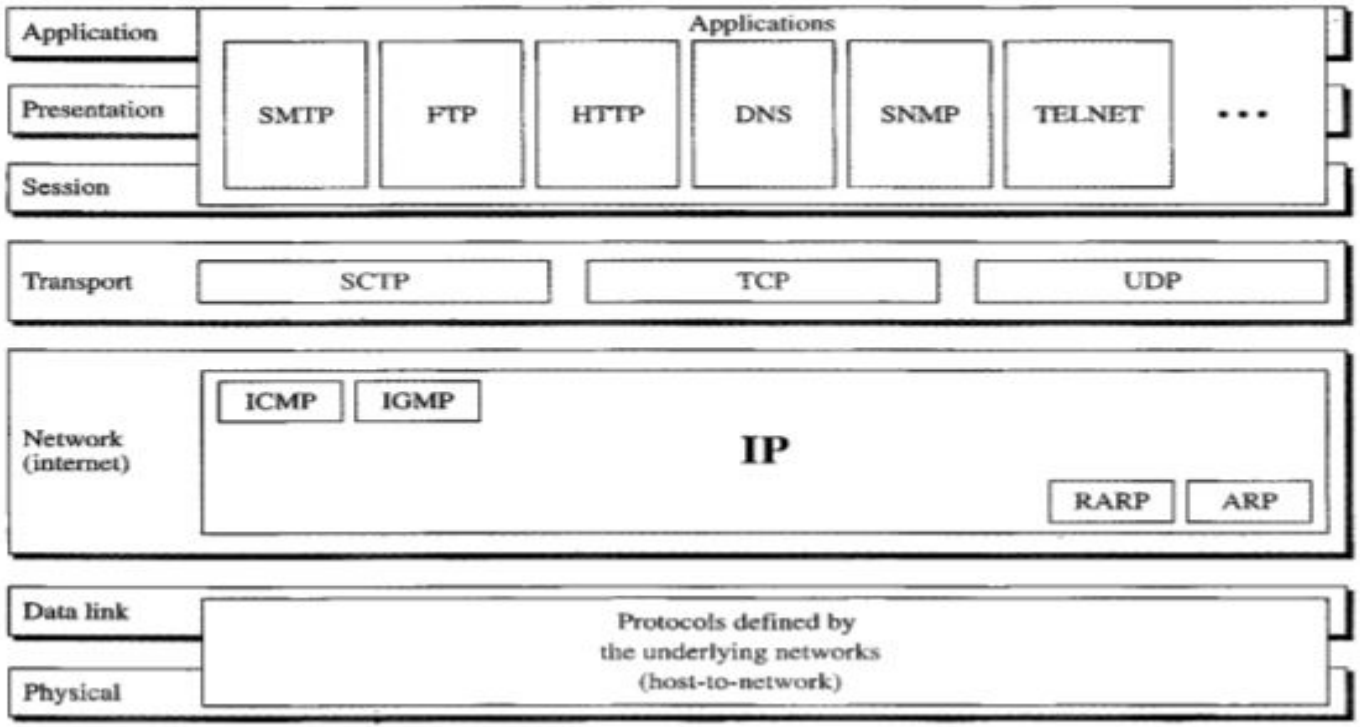
- Network virtual terminal
- File transfer, access and management
- Mail services
- Directory services


Application
To allow access to network resources
7
Presentation
To translate, encrypt, and compress data
6
Session
To establish, manage, and terminate sessions
5
Transport
To provide reliable process-to-process message delivery and error recovery
4
Network
To move packets from source to destination; to provide internetworking
3
Data link
To organize bits into frames; to provide hop-to-hop delivery
2
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications
1

TCP/IP PROTOCOL SUITE

- The original TCP/IP protocol suite was having 4 layers: host-to-network, internet, transport and application.
- Comparing to OSI:
  - Host-to-network: equivalent to physical and data link layers
  - Internet: equivalent to network layer
  - Transport: equivalent to transport layer
  - Application: equivalent to session, presentation and application layers

Figure 2.16 *TCP/IP and OSI model*



•**Application Layer**

•The application layer is where network applications and their application-layer protocols reside.

• The Internet's application layer includes many protocols, such as the HTTP protocol (which provides for Web document request and transfer), SMTP (which provides for the transfer of e-mail messages), and FTP (which provides for the transfer of files between two end systems).

Certain network functions, such as the translation of human-friendly names for Internet end systems like www.ietf.org to a 32- bit network address, are also done with the help of a specific application-layer protocol, namely, the domain name system (DNS)

Transport Layer:

The Internet's transport layer transports application-layer messages between application endpoints.

- In the Internet there are two transport protocols, TCP and UDP, either of which can transport application-layer messages.

- TCP provides a connection-oriented service to its applications.
  - This service includes guaranteed delivery of application-layer messages to the destination and flow control (that is, sender/receiver speed matching).
  - Transport-layer packet as a **segment.**
- TCP also breaks long messages into shorter segments and provides a congestion-control mechanism, so that a source throttles its transmission rate when the network is congested.
  - The UDP protocol provides a **connectionless service** to its applications.
  - This is a no-frills service that provides no reliability, no flow control, and no congestion control

Transport layer:

i) User Datagram Protocol (UDP):

- Unreliable and Connection-less protocol
- No guarantee of packet delivery and order, duplicate-protection

ii) Transmission Control Protocol (TCP):

- reliable , connection-oriented protocol

iii) Stream Control Transmission Protocol (SCTP):

- For newer applications like voice over internet

Network Layer

•The Internet's network layer is responsible for moving network-layer packets known as **datagrams from one host to another.**

•The Internet transport-layer protocol (TCP or UDP) in a source host passes a transport-layer segment and a destination address to the network layer.

●The network layer then provides the service of delivering the segment to the transport layer in the destination host.

•The Internet's network layer includes the IP Protocol, which defines the fields in the datagram as well as how the end systems and routers act on these fields.

-There is only one IP protocol, and all Internet components that have a network layer must run the IP protocol.

•The Internet's network layer also contains routing protocols that determine the routes that datagrams take between sources and destinations.

•The Internet has many routing protocols

Network layer:

- Main protocol is IP.
- Supporting protocols are: ARP, RARP, ICMP, IGMP

i) IP:

- Unreliable, connection-less protocol
- Data unit: datagrams

ii) Address Resolution Protocol(ARP):

- Finds the physical address of a node when its IP address is known.

iii) Reverse Address Resolution Protocol(RARP):

- Finds the IP address of a node when its physical address is known.

iv) Internet Control Message Protocol(ICMP):

- Error reporting protocol
- To diagnose network communication issues.

v) Internet Group Message Protocol (IGMP):

- Facilitates simultaneous transmission of messages to a group of receipients.

Link Layer

•Data transfer between neighboring network elements

Physical Layer

•While the job of the link layer is to move entire frames from one network element to an adjacent network element, the job of the physical layer is to move the *individual bits within the frame from one node to the next.*

•The protocols in this layer are again link dependent and further depend on the actual transmission medium of the link (for example, twisted-pair copper wire, single-mode fiber optics).

• For example, Ethernet has many physical-layer protocols:

•one for twisted-pair copper wire, another for coaxial cable, another for fiber, and so on.

• In each case, a bit is moved across the link in a different way.