Computer NetworksUnit – I
Introduction to computer networks and Internet

- **Understanding of network and Internet**
- **The network edge**
- **The network core**
- **Understanding of Delay**
- **Loss and Throughput in the packet-switching network**
- **Protocols layers and their service model**
- **History of the computer network**

NETWORKS

→ A network is a set of devices (often referred to as *nodes)* connected by communication links.
→ A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
→ A network is a combination of hardware and software that sends data from one location to another.
→ The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of instruction sets that make possible the services that we expect from a network.

Computer Network

→ **A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.**
→ A computer network is a system in which multiple computers are connected to each other to share information and resources.
→ The physical connection between networked computing devices is established using either cable media or wireless media.
→ The best-known computer network is the Internet.

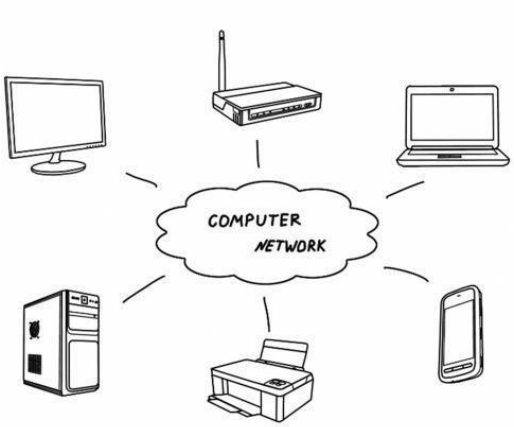
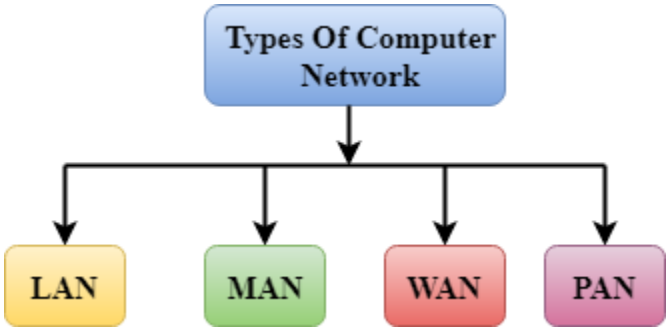


Figure 1: Computer Network

TYPES OF COMPUTER NETWORKS

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



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

Prof. Tejal Tandel
Assistant Professor,
IT Dept.,
MBIT, New V.V.Nagar

LAN (Local Area Network)

→ A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus

→ Local Area Network is a group of computers connected to each other in a small area such as building, office.

→ Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals.

→ Currently, LAN size is limited to a few kilometers.

→ 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.

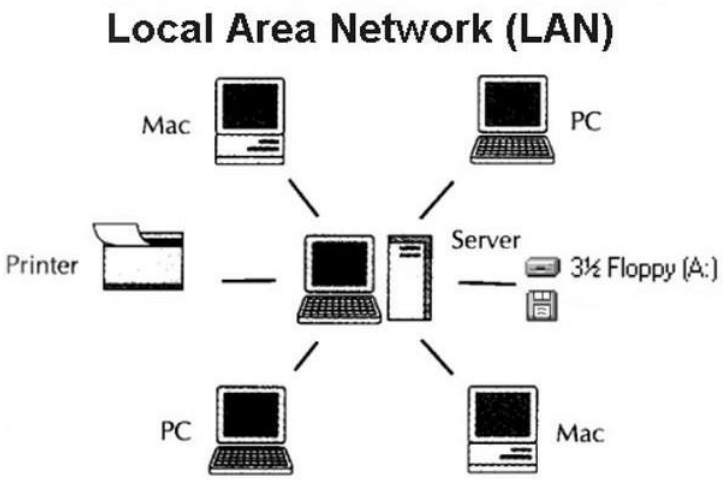
→ The data is transferred at an extremely faster rate in Local Area Network. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

→ Local Area Network provides higher security.

→ They exist in a limited geographical area.

→ In LAN, all the machines are connected to a single cable.

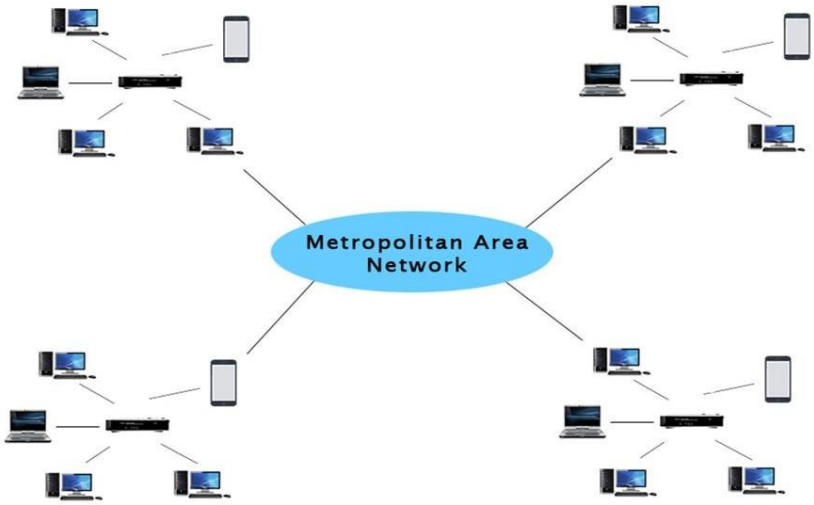
→ LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star.



Prof. Tejal Tandel
Assistant Professor,
IT Dept.,
MBIT, New V.V.Nagar

MAN (Metropolitan Area Network)

→ A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
→ It normally covers the area inside a town or a city.
→ It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.
→ A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.
→ Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.



WAN (Wide Area Network)

→ A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.

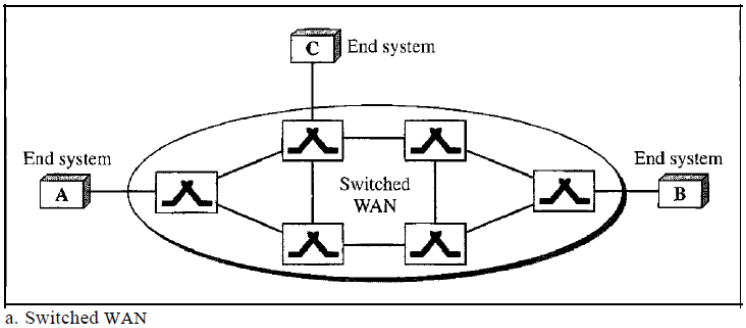
→ A Wide Area Network is a network that extends over a large geographical area such as states or countries.

→ A Wide Area Network is quite bigger network than the LAN.

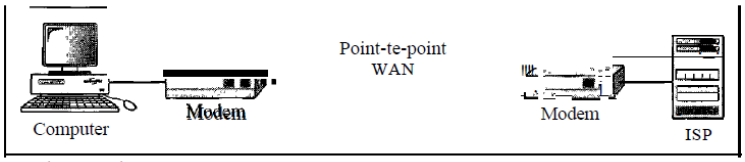
→ The internet is one of the biggest WAN in the world.

→ A Wide Area Network is widely used in the field of Business, government, and education, etc.

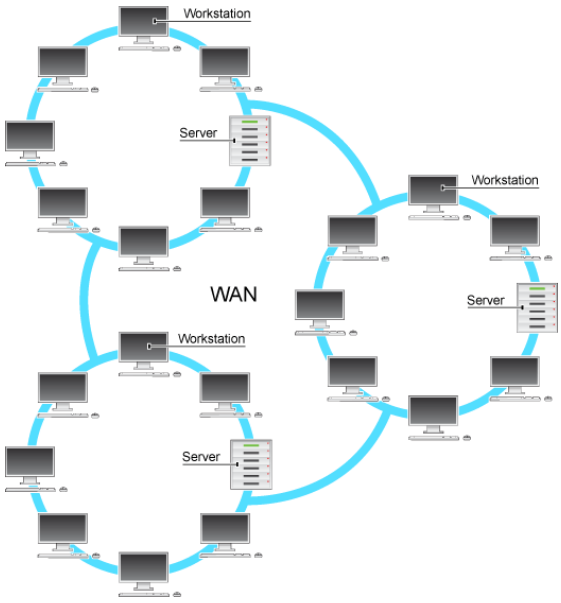
→ WAN links different metropolitan's countries and national boundaries there by enabling easy communication.

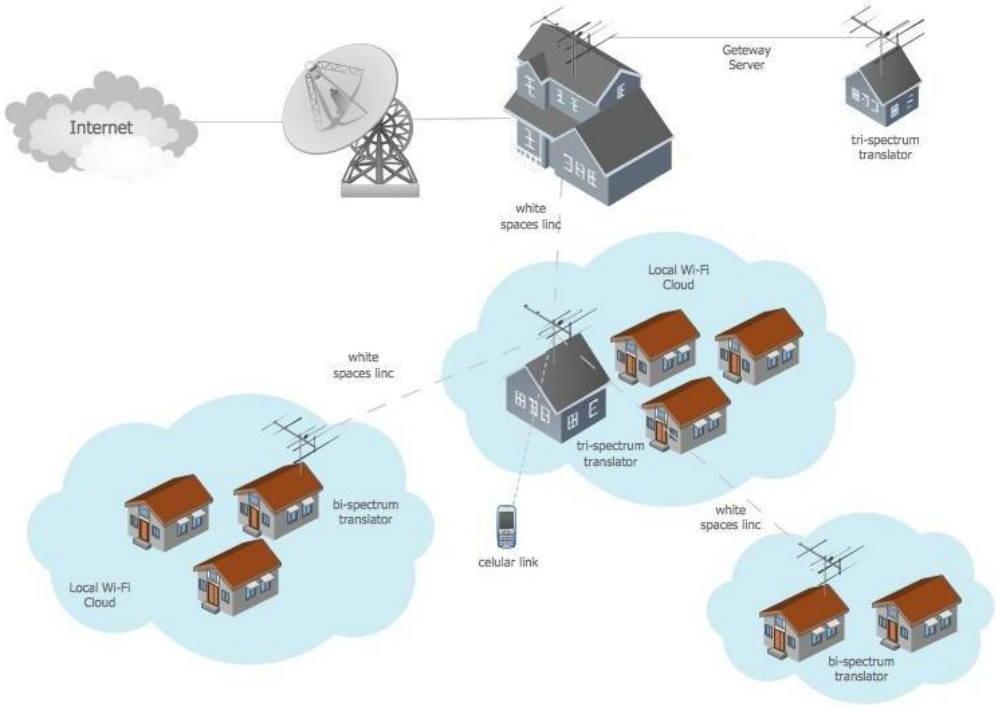


a. Switched WAN



b. Point-to-point WAN





→ A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells.

Difference between LAN, MAN and WAN.

Parameter	LAN	MAN	WAN
Area covered	Covers small area. i.e. within building	Covers larger than LAN & smaller than WAN	Covers large area
Error rates	Lowest	Moderate	Highest
Transmission speed	High speed	Moderate speed	Low speed
Equipment cost	Inexpensive	Moderate expensive	Most expensive
Design & maintenance	Easy	Moderate	Difficult
Speed	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
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.
Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.
Ownership	private	Private or public	Might not be owned by one organization.

Prof. Tejal Tandel
Professor,
IT Dept.,
MBIT, New V.V.Nagar

Internet

→ The internet is a type of world-wide computer network.

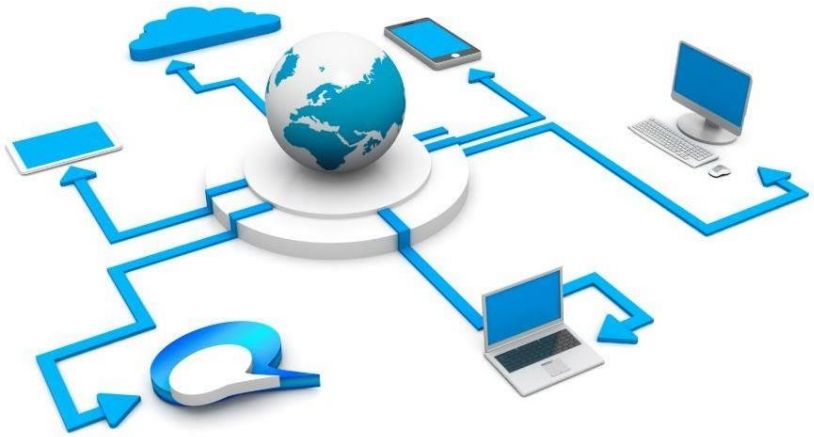
→ The internet is the collection of infinite numbers of connected computers that are spread across the world.

→ We can also say that, the Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world.

→ It is established as the largest network and sometimes called network of network that consists of numerous academic, business and government networks, which together carry various information.

→ Internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communicationprotocols.

→ When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.



Protocols

→ In computer networks, communication occurs between entities in different systems.
→ An entity is anything capable of sending or receiving information.
→ However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol.
→ **A protocol is a set of rules that govern data communications.**
→ A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax.**

→ The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented.
→ For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

- **Semantics.**

→ The word *semantics* refers to the meaning of each section of bits.
→ How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation?
→ For example, does an address identify the route to be taken or the final destination of the message?

- **Timing.**

→ The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent.
→ For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Network Edge

→ The computers and other devices connected to the Internet are often referred to as **end systems.**

→ They are referred to as end systems because they sit at the ***edge of the Internet***, as shown in Figure 1.3.

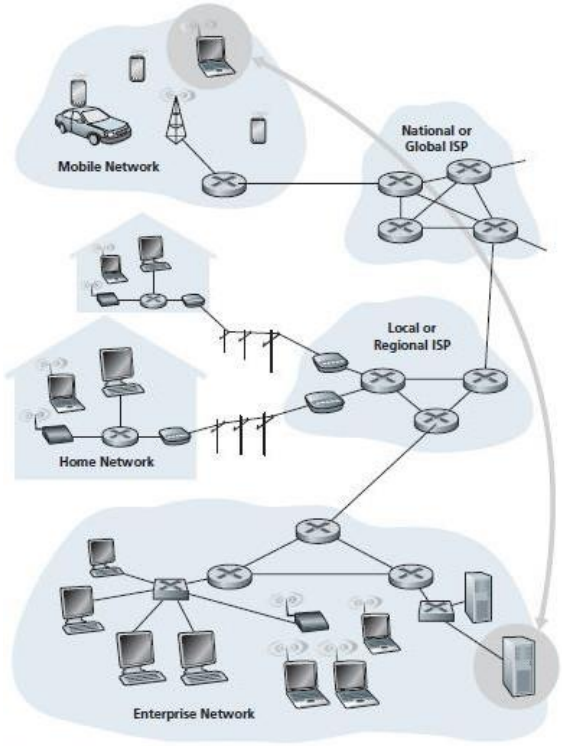


Figure 1.3 ♦ End-system interaction

→ The Internet's end systems include desktop computers (e.g., desktop PCs, Macs, and Linux boxes), servers (e.g., Web and e-mail servers), and mobile computers (e.g., laptops, smartphones, and tablets).

- Furthermore, an increasing number of non-traditional devices are being attached to the Internet as end systems.

→ End systems are also referred to as ***hosts*** because they host (that is, run) application programs such as

- a Web browser program,
- a Web server program,
- an e-mail client program, or
- an e-mail server program.

→ Throughout we will use the terms ***hosts and end systems interchangeably***;

→ That is, ***host = end system***.

→ Hosts are sometimes further divided into two categories: **clients** and **servers**.

→ Informally,

- clients tend to be
  - desktop and mobile PCs, smartphones, and so on,
- Whereas servers tend to be
  - more powerful machines that store and distribute
    - Web pages,
    - stream video,
    - Relay e-mail, and so on.

→ Today, most of the servers from which we receive search results, e-mail, Web pages, and videos reside in large **data centers**. For example, Google has 30–50 data centers, with many having more than one hundred thousand servers.

Delay, Loss, and Throughput in Packet-Switched Networks

→ A packet starts in a host (the source), passes through a series of routers, and ends its journey in another host (the destination).

→ As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at *each* node along the path.

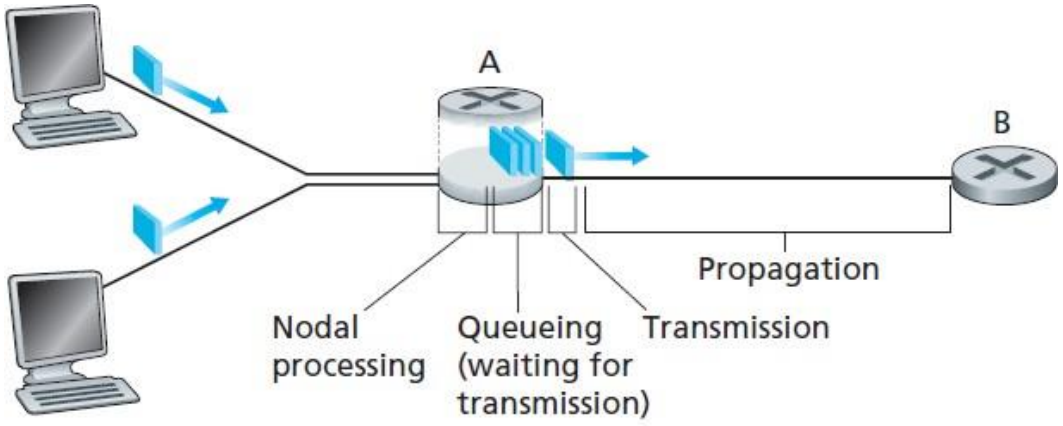
→ The most important of these delays are the

- **Nodal processing delay,**
- **Queuing delay,**
- **Transmission delay,** and
- **Propagation delay**; together, these delays accumulate to give a **total nodal delay**.

→ The performance of many Internet applications—such as search, Web browsing, email, maps, instant messaging, and voice-over-IP—are greatly affected by network delays.

→ In order to acquire a deep understanding of packet switching and computer networks, we must understand the nature and importance of these delays.

Nodal Processing Delay



♦ The nodal delay at router A

→ Its end-to-end route between source and destination, a packet is sent from the upstream node through router A to router B.
→ Our goal is to characterize the nodal delay at router A.
→ Note that router A has an outbound link leading to router B.
→ This link is preceded by a queue (also known as a buffer).
→ When the packet arrives at router A from the upstream node, router A examines the packet's header to determine the appropriate outbound link for the packet and then directs the packet to this link.
→ In this example, the outbound link for the packet is the one that leads to router B.
→ A packet can be transmitted on a link only if there is no other packet currently being transmitted on the link and if there are no other packets preceding it in the queue; if the link is currently busy or if there are other packets already queued for the link, the newly arriving packet will then join the queue.

Processing Delay

→ The time required to examine the packet's header and determine where to direct the packet is part of the **processing delay**.
→ The processing delay can also include other factors, such as
  - The time needed to check for bit-level errors in the packet that occurred in transmitting the packet's bits from the upstream node to router A.

→ Processing delays in high-speed routers are typically on the order of microseconds or less.
→ After this nodal processing, the router directs the packet to the queue that precedes the link to router B.

Queue Delay

→ At the queue, the packet experiences a **queuing delay** as it waits to be transmitted onto the link.
→ The length of the queuing delay of a specific packet will depend on the number of earlier-arriving packets that are queued and waiting for transmission onto the link.
→ If the queue is empty and no other packet is currently being transmitted, then our packet's queuing delay will be zero.
→ On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long.
→ We will see shortly that the number of packets that an arriving packet might expect to find is a function of the intensity and nature of the traffic arriving at the queue.
→ Queuing delays can be on the order of microseconds to milliseconds in practice.

Transmission Delay

→ Assuming that packets are transmitted in a first-come-first-served manner, as is common in packet-switched networks, our packet can be transmitted only after all the packets that have arrived before it have been transmitted.
→ Denote the length of the packet by L bits, and denote the transmission rate of the link from router A to router B by R bits/sec.
→ For example,
for a 10 Mbps Ethernet link, the rate is R = 10 Mbps; for a 100 Mbps Ethernet link, the rate is R = 100 Mbps.
→ The **transmission delay** is L/R.
→ This is the amount of time required to push (that is, transmit) all of the packet's bits into the link.
→ Transmission delays are typically on the order of microseconds to milliseconds in practice.

Propagation Delay

→ Once a bit is pushed into the link, it needs to propagate to router B.
→ The time required to propagate from the beginning of the link to router B is the **propagation delay**.
→ The bit propagates at the propagation speed of the link.
→ The propagation speed depends on the physical medium of the link (that is, fiber optics, twisted-pair copper wire, and so on) and is in the range of $2 \cdot 10^8$ meters/sec to $3 \cdot 10^8$ meters/sec
→ Which is equal to, or a little less than, the speed of light.
→ The propagation delay is the distance between two routers divided by the propagation speed.
→ That is, the propagation delay is d/s, where d is the distance between router A and router B and s is the propagation speed of the link.
→ Once the last bit of the packet propagates to node B, it and all the preceding bits of the packet are stored in router B.
→ The whole process then continues with router B now performing the forwarding.
→ In wide-area networks, propagation delays are on the order of milliseconds.

1) Transmission Delay(T_t): If there is a host and if it is having a data packet,the time taken by the host to put the data packet on to the outgoing link is called transmission delay.

$$T_t = L/B \text{ sec}$$

→ Time taken to put the data packet on the transmission link is called as **transmission delay**.

- Transmission delay a Length / Size of data packet
- Transmission delay a 1 / Bandwidth

$$\text{Transmission delay} = \frac{\text{Length / Size of data packet}}{\text{Bandwidth of Network}}$$

example:

L=1000bits Bandwidth=1Kbps what is T_t?
Sol:
$T_t = L/B$
1000/1000=1sec

2) Propogation delay (T_p): Time taken by the single or one bit to reach from one end of the link to other link is called propogation delay.

→ Time taken for one bit to travel from sender to receiver end of the link is called as **propagation delay**.

- Propagation delay a Distance between sender and receiver
- Propagation delay a 1 / transmission speed

$$\text{Propagation delay} = \frac{\text{Distance between sender and receiver}}{\text{Transmission speed}}$$

Factor on which propogation delay depends:

a) Distance (d)

b) Velocity (v)

$$T_p = d/v \text{ sec}$$

Example:

Distance=2.1 km
Velocity=2.1*10^8 m/s
T_p ?
Sol:
$T_p = 2.1*10^3/2.1*10^8$
$= 10^{-5}$ sec
= 10µsec

3) Queuing delay(T_q): Time taken to stay in queue before processing the last packet on receiver.

→ Time spent by the data packet waiting in the queue before it is taken for execution is called as **queuing delay**.
→ It depends on the congestion in the network.

4) Processing delay(T_{proc}): Time taken to process next packet from queue to the processor on receiver end.

→ Time taken by the processor to process the data packet is called as **processing delay**.
→ It depends on the speed of the processor.
→ Processing of the data packet helps in detecting bit level errors that occurs during transmission.

Total delay in sending one data packet or End to End time
= Transmission delay + Propagation delay + Queuing delay + Processing delay

LAYERS IN THE OSI MODEL

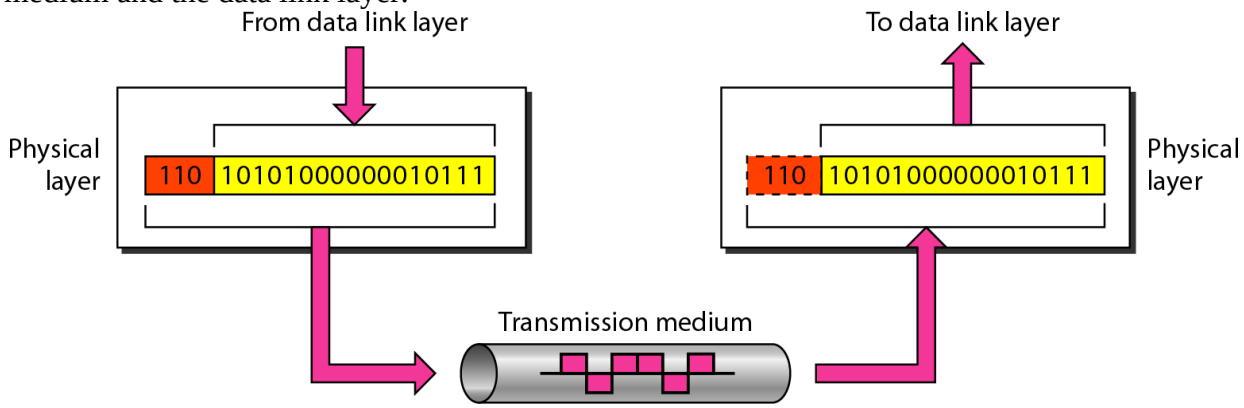
▪ Physical Layer

→ The physical layer coordinates the functions required to carry a bit stream over a physical medium.

→ It deals with the mechanical and electrical specifications of the interface and transmission medium.

→ It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur.

→ Below figure shows the position of the physical layer with respect to the transmission medium and the data link layer.



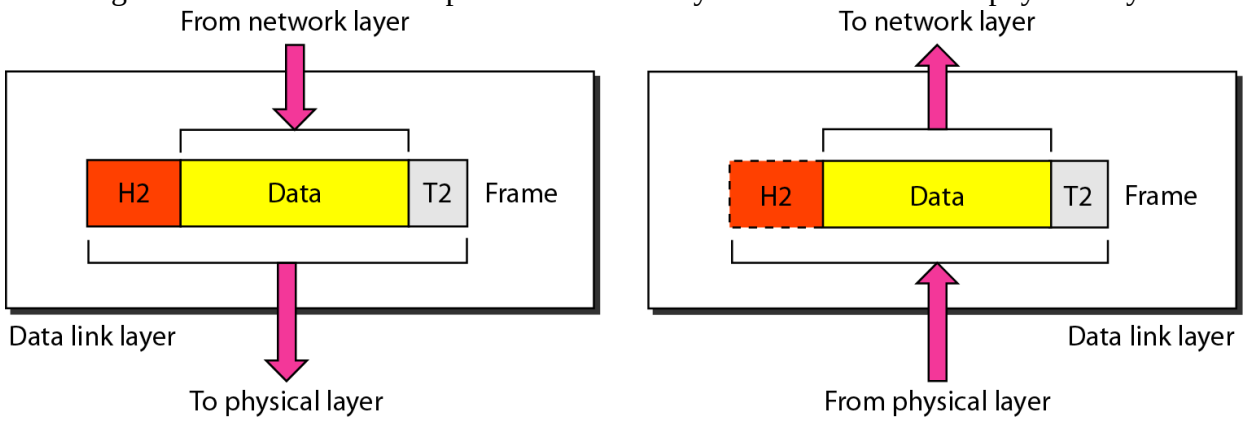
→ **The physical layer is also concerned with the following:**

- Physical characteristics of interfaces and medium.
  - The physical layer defines the characteristics of the interface between the devices and the transmission medium.
  - It also defines the type of transmission medium.
- Representation of bits.
  - The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation.
  - To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and I s 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 not only must use the same bit rate but also must 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 through a dedicated link.
  - In a multipoint configuration, a link is shared among several devices.
- Physical topology.
  - The physical topology defines how devices are connected to make a network.
  - Devices can be connected by using a
    - mesh topology (every device is 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),
    - a bus topology (every device is on a common link), or
    - a hybrid topology (this is a combination of two or more topologies).
- Transmission mode.
  - The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.
  - In simplex mode, only one device can send; the other can only receive.
  - The simplex mode is a one-way communication.
  - In the half-duplex mode, two devices can send and receive, but not at the same time.
  - In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

Data Link Layer

→ The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

→ Below Figure shows the relationship of the data link layer to the network and physical layers.

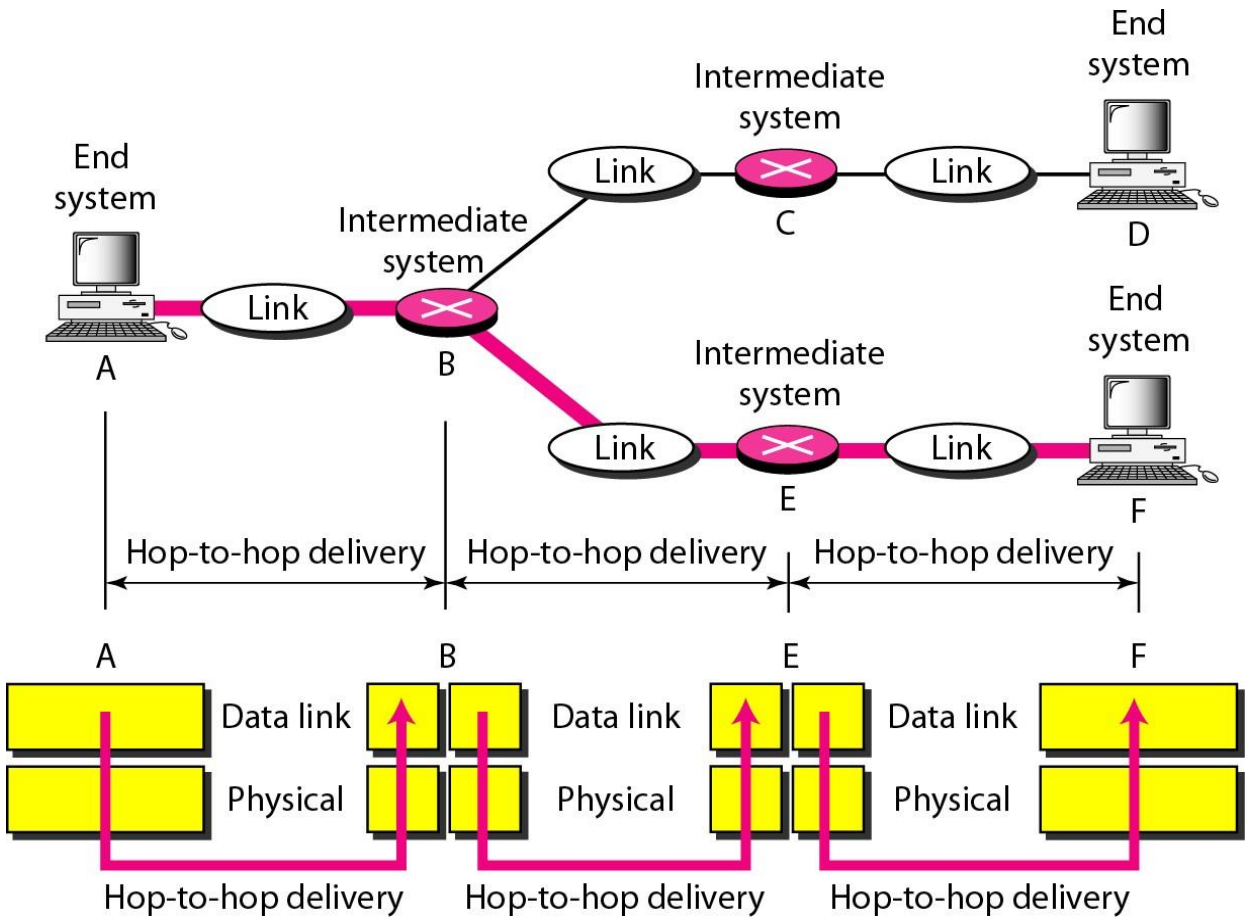


→ The data link layer is responsible for moving frames from one hop (node) to the next.

→ **Other responsibilities of the data link layer include the following:**

- 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 device that connects the network to the next one.
- Flow control.
  - If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid 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.

→ **Hop-to-hop (node-to-node) delivery by the data link layer.**



→ As the figure shows,

- Communication at the data link layer occurs between two adjacent nodes.
- To send data from A to F, three partial deliveries are made.
- First, the data link layer at A sends a frame to the data link layer at B (a router).
- Second, the data link layer at B sends a new frame to the data link layer at E.
- Finally, the data link layer at E sends a new frame to the data link layer at F.
- Note that the frames that are exchanged between the three nodes have different values in the headers.
- The frame from A to B has B as the destination address and A as the source address.
- The frame from B to E has E as the destination address and B as the source address.
- The frame from E to F has F as the destination address and E as the source address.
- The values of the trailers can also be different if error checking includes the header of the frame.

Network Layer

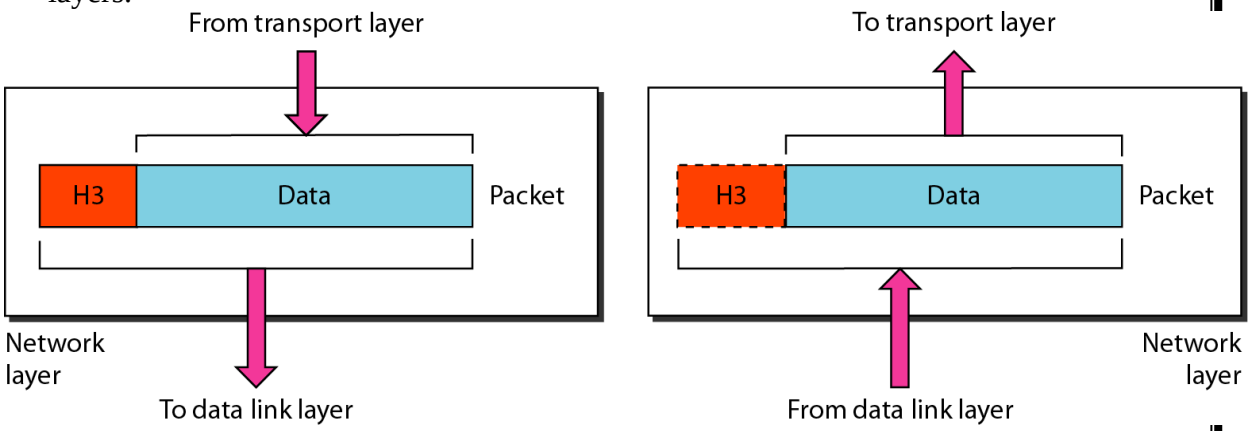
→ The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

→ Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

→ If two systems are connected to the same link, there is usually no need for a network layer.

→ However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

→ Below Figure shows the relationship of the network layer to the data link and transport layers.

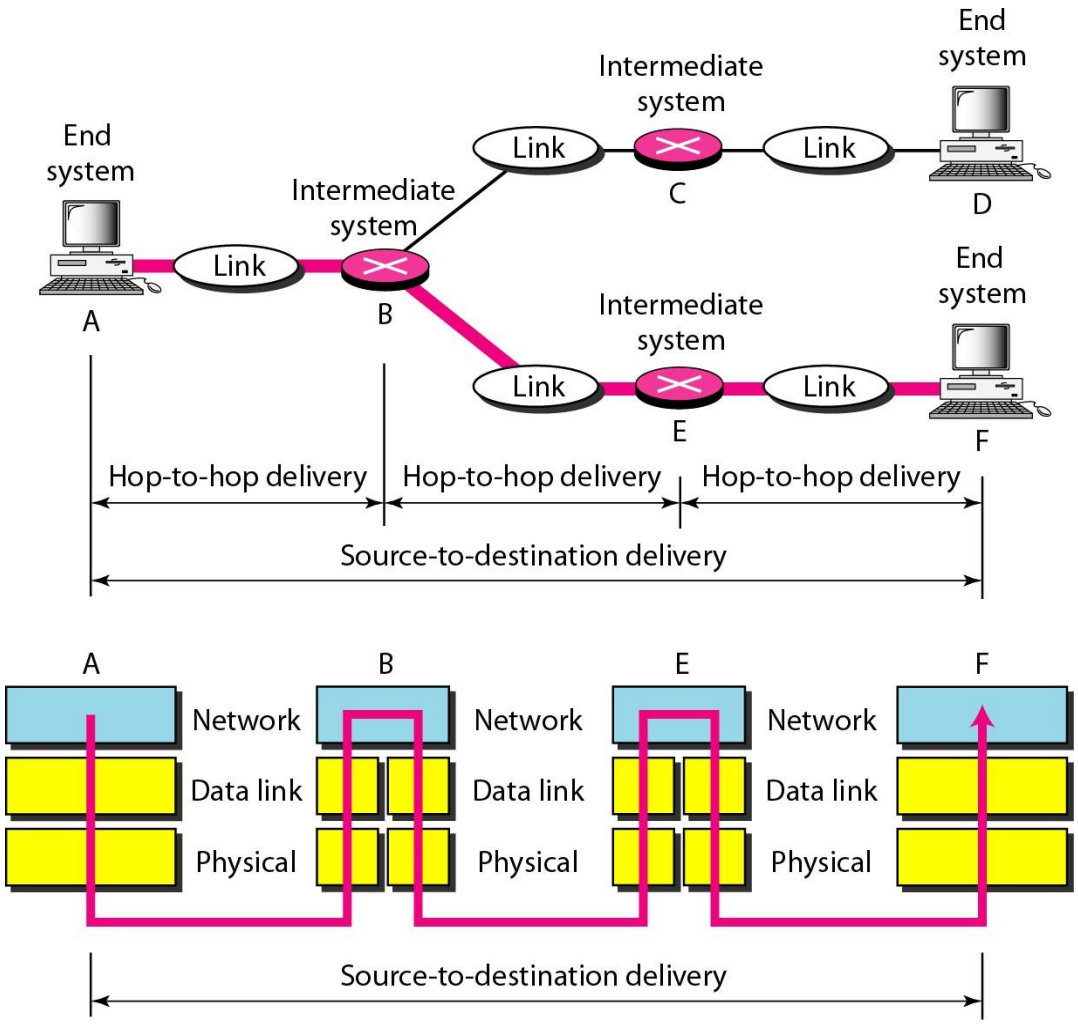


→ **The network layer is responsible for the delivery of individual packets from the source host to the destination host.**

→ **<u>Other responsibilities of the network layer include the following:</u>**

- 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 to create *inter-networks* (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.

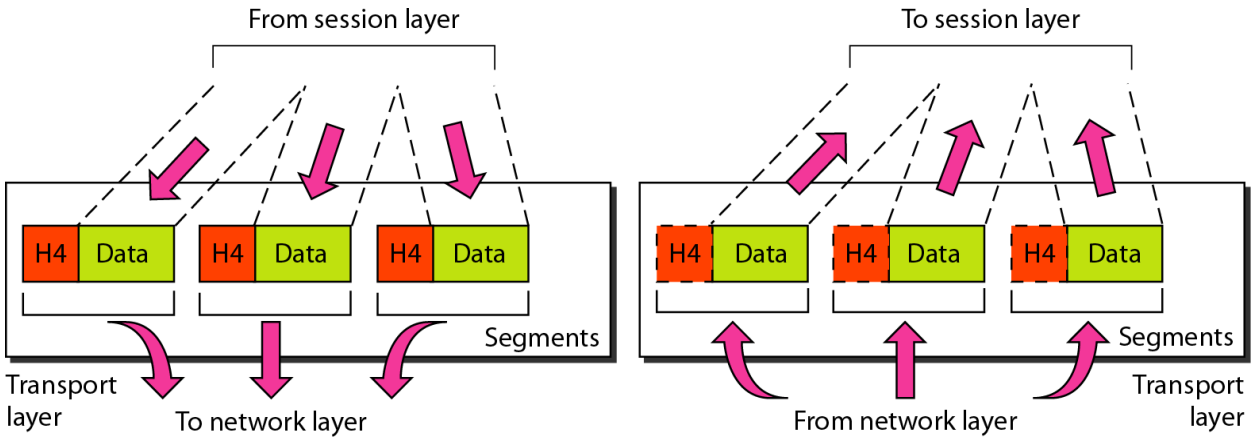
- Illustrates end-to-end delivery by the network layer. (***Source-to-destination delivery***)



- As the figure shows, now we need a source-to-destination delivery.
- The network layer at A sends the packet to the network layer at B.
- When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet.
- As we will see in later chapters, router B uses its routing table to find that the next hop is router E.
- The network layer at B, therefore, sends the packet to the network layer at E.
- The network layer at E, in tum, sends the packet to the network layer at F.

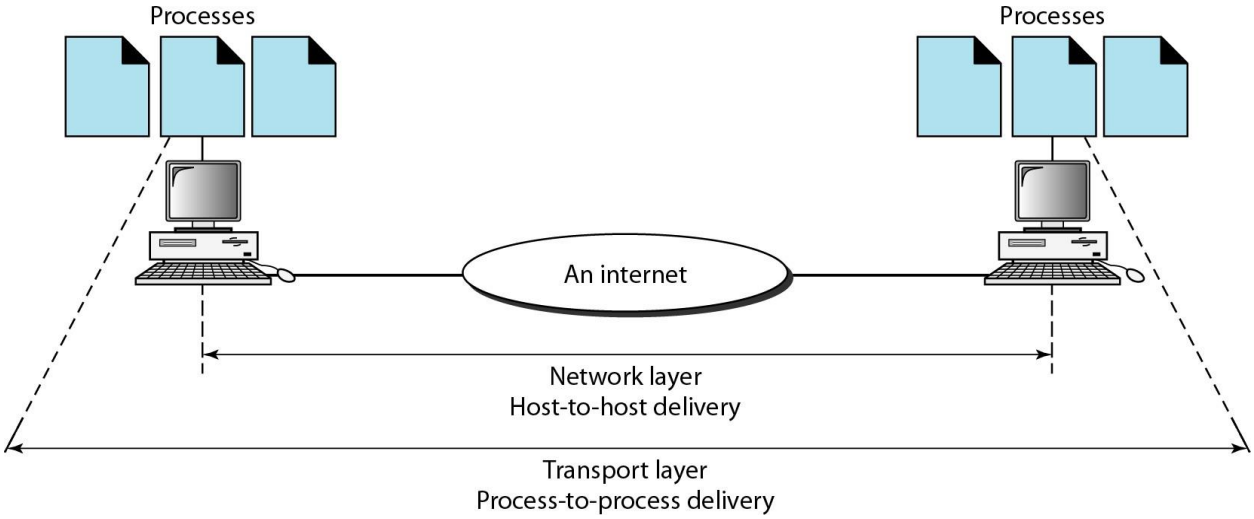
Transport Layer

→ The transport layer is responsible for process-to-process delivery of the entire message.
→ A process is an application program running on a host.
→ Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
→ It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
→ The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.
→ Below figure shows the relationship of the transport layer to the network and session layers.



→ **The transport layer is responsible for the delivery of a message from one process to another.**

→ **Reliable process-to-process delivery of a message**



Prof. Tejal Tandel
Assistant Professor,
IT Dept.,
MBIT, New V.V.Nagar

→ **Other responsibilities of the transport layer include the following:**

- 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 makes 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

→ The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network *dialog controller*.

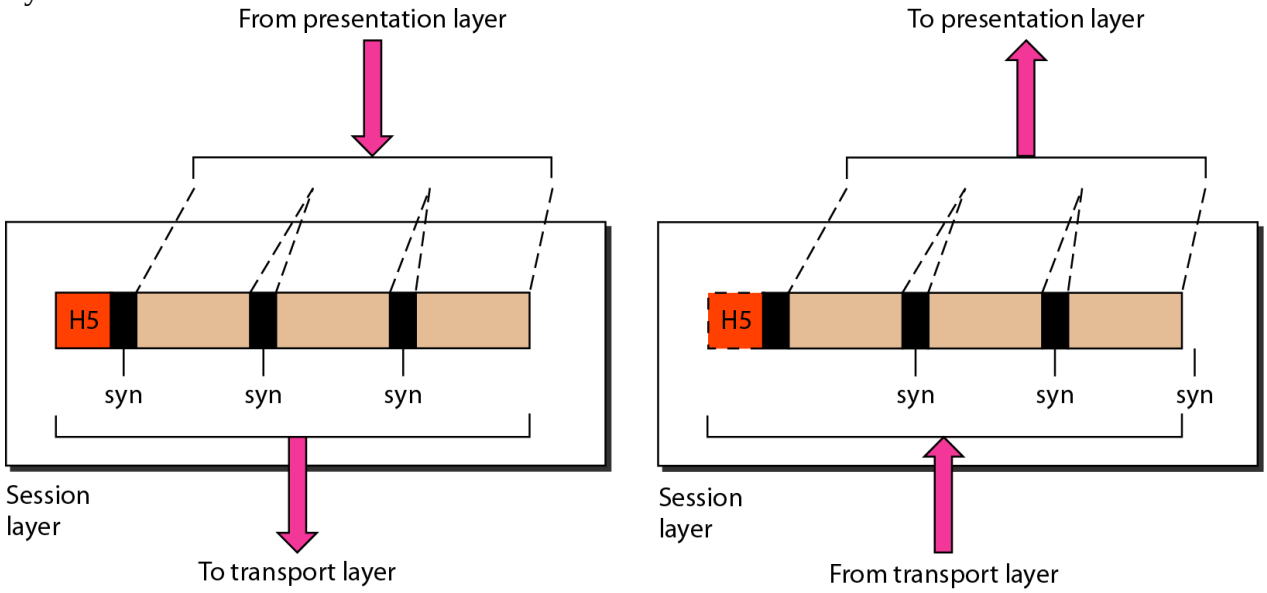
→ It establishes, maintains, and synchronizes the interaction among communicating systems.

→ **The session layer is responsible for dialog control and synchronization.**

→ **Specific responsibilities of the session layer include the following:**

- 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, or synchronization points, to a stream of data.
  - For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.
  - In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523.
  - Pages previous to 501 need not be resent.

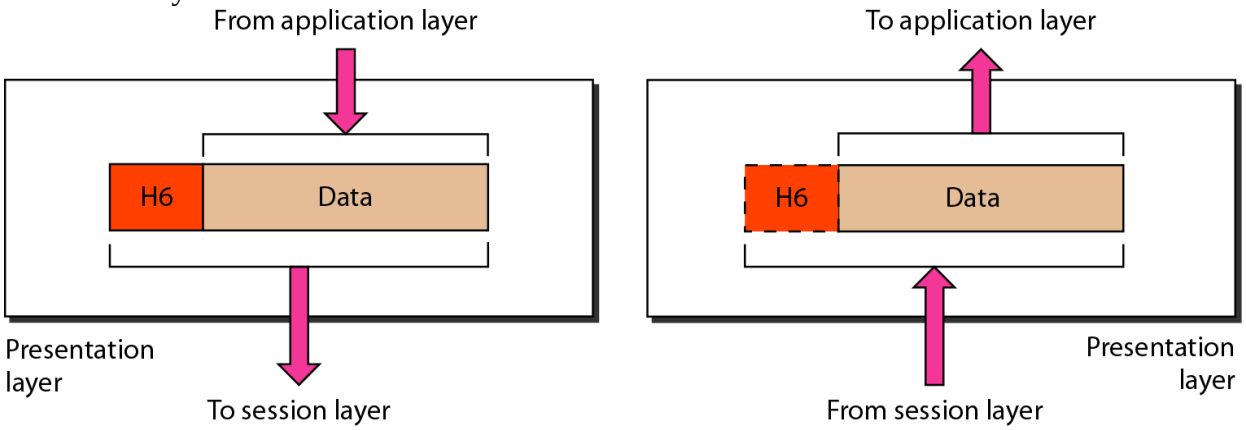
→ Below Figure illustrates the relationship of the session layer to the transport and presentation layers.



Presentation Layer

→ The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

→ Below Figure shows the relationship between the presentation layer and the application and session layers.



→ **The presentation layer is responsible for translation, compression, and encryption.**

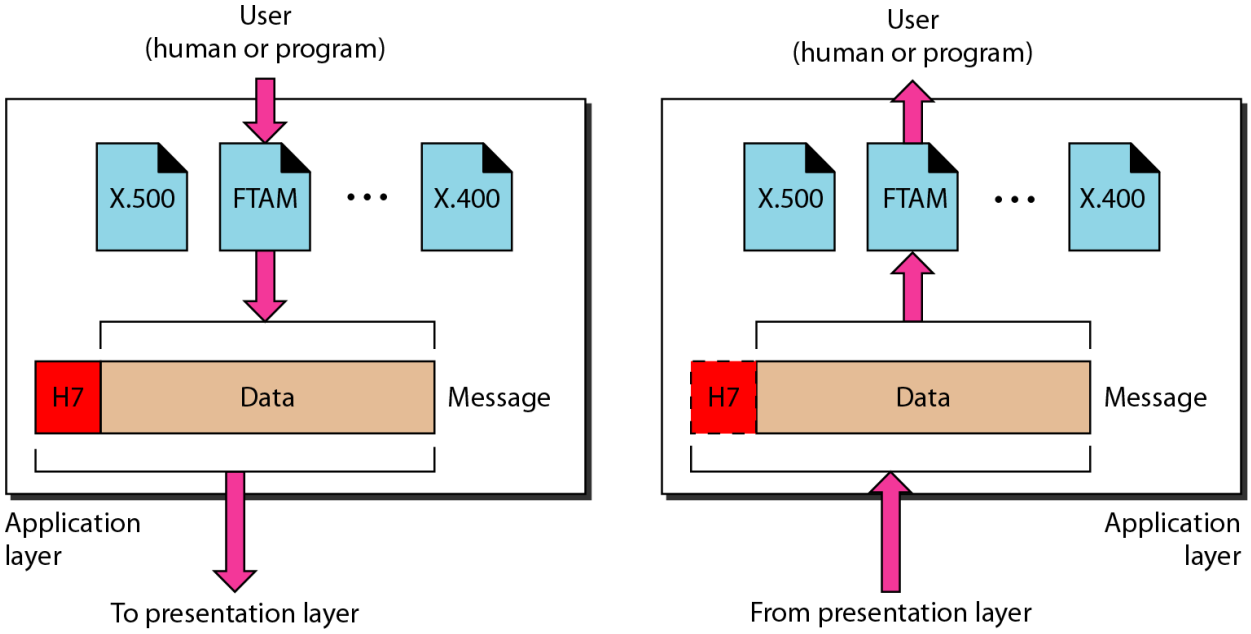
→ **Specific responsibilities of the presentation layer include the following:**

- Translation.
  - The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on.
  - The information must be changed to bit streams before being transmitted.
  - Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
  - 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 ensure 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

→ The application layer enables the user, whether human or software, to access the network.

→ It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.



→ Above Figure shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three: *XAOO* (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM).

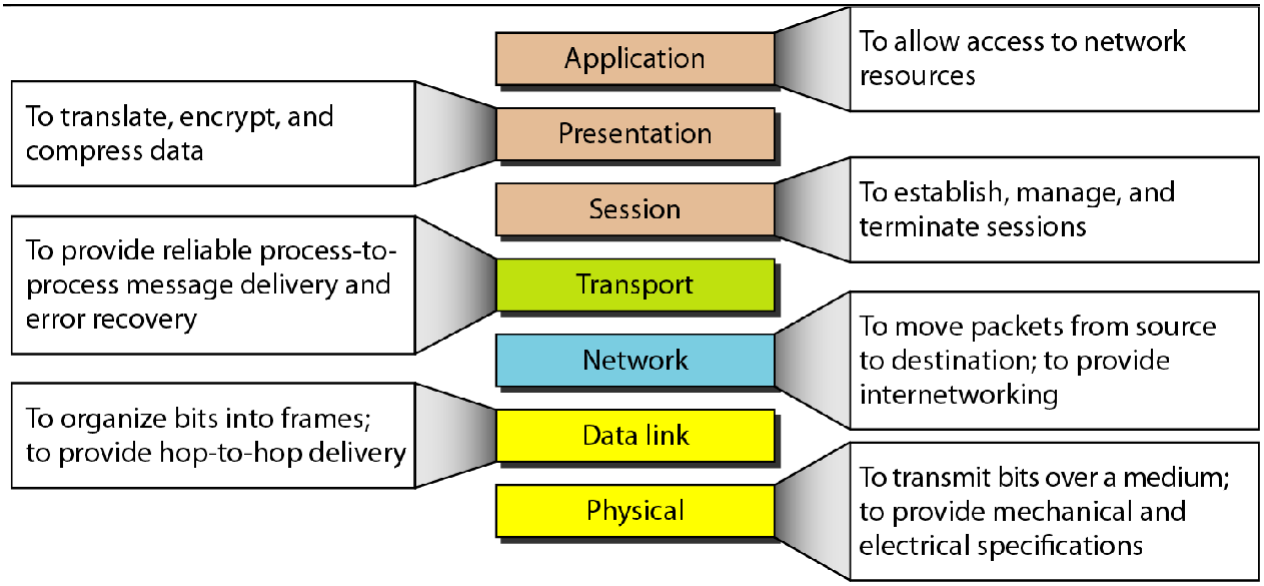
→ The user in this example employs *XAOO* to send an e-mail message.

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

→ **Specific services provided by the application layer include the following:**

- Network virtual terminal.
  - A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
  - To do so, the application creates a software emulation of a terminal at the remote host.
  - The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa.
  - The remote host believes it is communicating with one of its own terminals and allows the user to log on.
  - File transfer, access, and management.
  - This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- Mail services.
  - This application provides the basis for e-mail forwarding and storage.
- Directory services.
  - This application provides distributed database sources and access for global information about various objects and services.
  - File transfer, access, and management.
  - This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- Mail services.
  - This application provides the basis for e-mail forwarding and storage.
- Directory services.
  - This application provides distributed database sources and access for global information about various objects and services.

- ***Summary of layers***



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP		Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Computer NetworksUnit – I
Introduction to computer networks and Internet

Assistant Professor,
IT Dept.,
MBIT, New V.V.Nagar