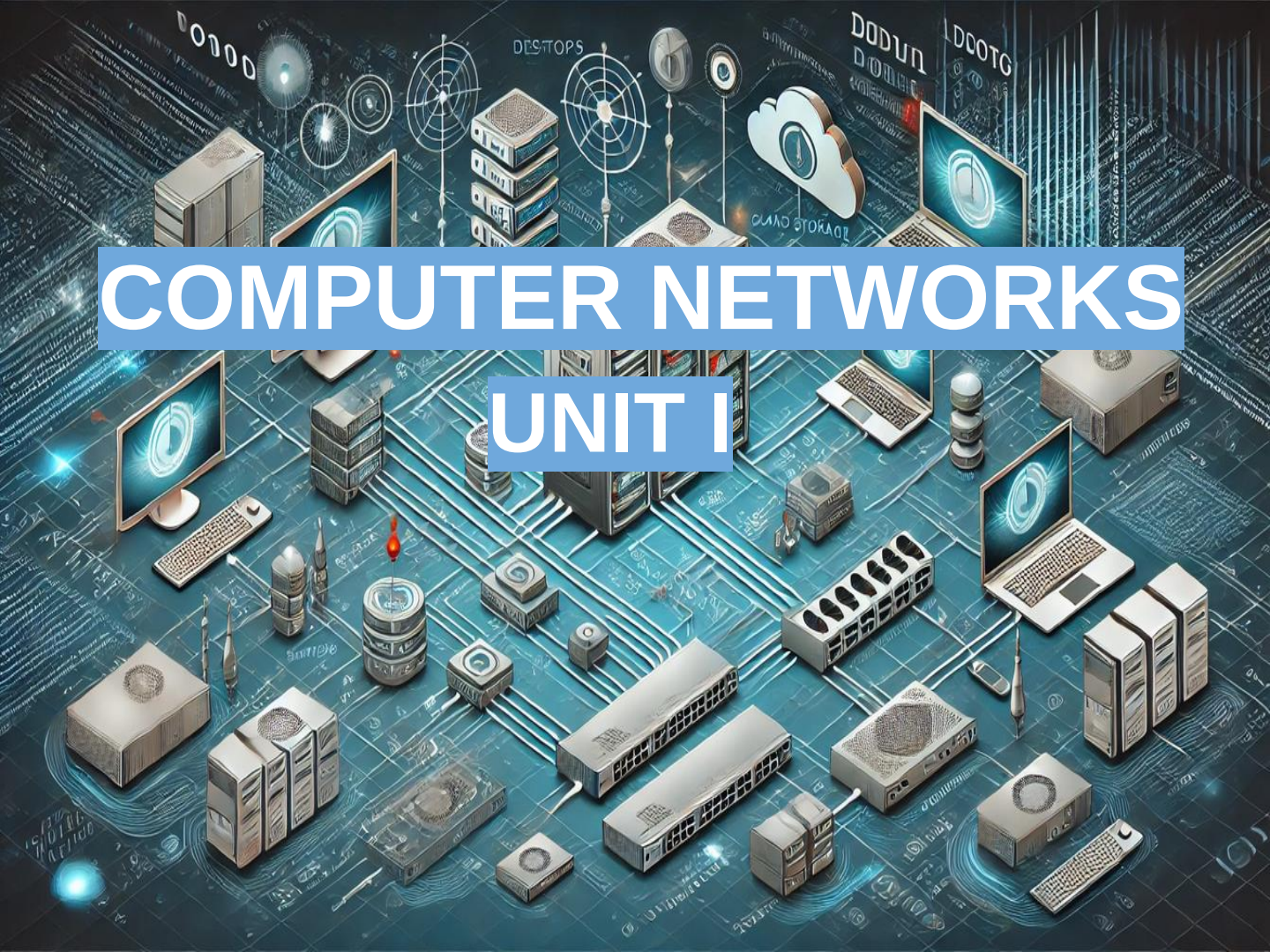

COMPUTER NETWORKS
UNIT I

UNIT-I

- Introduction to Networks
- Network Types: LAN, MAN, PAN, WAN
- Network Topology: BUS, STAR, RING, MESH, HYBRID
- Switching: Circuit Switching, Packet Switching
- OSI Layered Architecture
- TCP/IP Model - Physical Layer Overview
- Latency, Bandwidth, Delay
- Guided Media: Twisted pair, Coaxial cable, Fiber optic cable
- Unguided Media: Radio waves, Microwaves, Infrared.

Introduction to Networks

- A network is a group of computers, printers, and other devices that are connected together
- Data Communications is the transfer of data or information between a source and a receiver. The source transmits the data and the receiver receives it with cables.
- The major criteria that a data communication network must meet are:

1. Performance
2. Consistency
3. Reliability
4. Recovery
5. Security

DATA TRANSMISSION MODES

- In simplex mode the communication can take place in one direction. The receiver receives the signal from the transmitting device. In this mode the flow of information is unidirectional. Hence, it is rarely used for data Communication.
- In half duplex mode the communication channel is used in both directions, but only in one direction at a time. Thus, a half duplex line can alternately send and receive data.
- In full duplex the communication channel is used in both directions at the same time. Use of full duplex line improves the efficiency as the line turnaround time required in half duplex arrangement is eliminated. Example of this mode of transmission is the telephone line.

Network Types: LAN

- LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.
- When LANs are used by companies, they are called enterprise networks.
- Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables.
- In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers.
- In most cases, each computer talks to a device in the ceiling . This device, called an AP (Access Point), wireless router, or base station, relays packets between the wireless computers and also between them and the Internet.
- Being the AP is like being the popular kid as school because everyone wants to talk to you.
- However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.
- There is a standard for wireless LANs called IEEE 802.11, popularly known as WiFi, which has become very widespread.

Network Types: LAN

- Wired LANs use a range of different transmission technologies.
- It runs at speeds anywhere from 11 to hundreds of Mbps.
- Most of them use copper wires, but some use optical fiber.
- The topology of many wired LANs is built from point-to-point links.
- IEEE 802.3, popularly called Ethernet, is, by far, the most common type of wired LAN.
- Each computer speaks the Ethernet protocol and connects to a box called a switch with a point-to-point link.
- A switch has multiple ports, each of which can connect to one computer.
- The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.

Advantages of LANs:

- High security and speed
- Simplifies device connection
- Broad compatibility
- Secure data transfer
- Storage of data in a central location
- Internet connection sharing for multiple devices

Network Types: PAN

- Personal Area Networks devices communicate over the range of a person.
- A example is a wireless network that connects a computer with its peripherals.
- Almost every computer has an attached monitor, keyboard, mouse, and printer.
- So many new users have a hard time finding the right cables and plugging them into the right little holes (even though they are usually color coded) that most computer vendors offer the option of sending a technician to the user's home to do it.
- To help these users, some companies got together to design a short-range wireless network called Bluetooth to connect these components without wires.
- Bluetooth networks use the master-slave paradigm.
- PANs can also be built with other technologies that communicate over short ranges, such as RFID on smartcards and library books.

Advantages of PANs:

- Increased safety
- Simple connection setup
- Low complexity of network components
- Economical energy consumption

Network Types: WAN

- Wide Area Network spans a large geographical area, a country or continent.
- Each offices contains computers intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
- The network that connects these hosts is then called the communication subnet, or just subnet for short.
- The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.
- The subnet consists of 2 distinct components: transmission lines and switching elements.
- Transmission lines move bits between machines.They can be made of copper wire, optical fiber, or even radio links.
- Most companies do not have transmission lines lying about, so instead they lease the lines from a telecommunications company.
- Switching elements, / switches, are specialized computers that connect two or more transmission lines.
- When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.
- These switching computers have been called by various names in the past; the name router is now most commonly used.

Advantages of WANs:

• Improved communication and collaboration, Efficient data exchange,Flexibility and scaling, High security and data protection

Network Types: MAN

- Metropolitan Area Network covers a city.
- The best-known examples are the cable television networks .
- These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception.
- When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum.
- At that point, the cable TV system began to morph from simply a way to distribute television to a metropolitan area network.
- To a first approximation, a MAN might look something both television signals and Internet being fed into the centralized cable headend for subsequent distribution to people's homes.
- Recent developments in highspeed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.

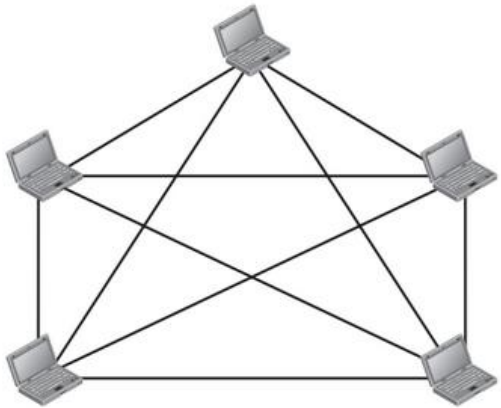
Advantages of MANs:

- Efficient communication
- Low latency
- Higher bandwidth
- Flexibility in network distribution
- Infrastructure for various services

Category	LAN (Local Area Network)	MAN (Metropolitan Area Network)	WAN (Wide Area Network)	PAN (Personal Area Network)
Scope	Computers connected in a small area (Building or office)	Network interconnecting LANs in a larger area(City/Town)	Network that extends over a large geographical area (States or countries.)	Network arranged in 10 m.
Uses	Connecting two or more PC through a twisted pair, coaxial cable, etc.	Government agencies connecting to citizens and private industries.	Used in business, government, and education.	Connecting devices like laptops, phones, media players, and play stations.
Error Rates	Low error rates.	Moderate error rates.	Higher error rates due to long distance & multiple connection	Very low error rates.
Media	Twisted-pair wire, coaxial cables, fiber optic cables, or radio waves.	Fiber optic cables and microwave communication.	Leased lines, satellite, and fiber optics.	Bluetooth, infrared, and other short-range wireless communication
Topology	Ring, bus, or star.	Ring or bus	Mesh and hierarchical	Point-to-point
Data Rates	High data rates 10-1000 Mbps	Moderate data rates, > WAN but < LAN.	Lower data rates compared to LAN and MAN, but suitable for long-distance communication.	Low data rates, up to a few Mbps.
Network Management	By the user or organization owning the network.	By service providers or organizations within city.	By service providers and telecommunications companies.	By individual user.
Resource Sharing	Facilitates sharing of files, printers, & resources.	Enables sharing of resources and services across multiple LANs.	Enables connectivity and resource sharing across large distances.	Enables sharing of personal resources like files and internet connection.
Packet Routing	Uses switches and routers to direct packets to their destination within the network.	Uses routers and switches to manage packet routing.	Uses routers to route packets over long distances.	Direct device-to-device communication without complex routing.
Path Establishment	Direct and fixed paths	Dynamic paths	Dynamic and complex paths	Direct connection
Cost	Low	Moderate	High, due to extensive infrastructure and long-distance charges.	Very low, limited to device costs and minimal setup.

Network Topology: MESH

- In this networking topology, each communicating device is connected with every other device in the network.
- Such a network can handle large amounts of traffic since multiple nodes can transmit data simultaneously.
- Also, such networks are more reliable in the sense that even if a node gets down, it does not cause any break in the transmission of data between other nodes.
- This topology is also more secure as compared to other topologies because each cable between two nodes carries different data.
- However, wiring is complex and cabling cost is high in creating such networks and there are many redundant or unutilised connections.



Network Topology: MESH

- Mesh topologies are used in critical connection of host computers (typically telephone exchanges).
- Alternate paths allow each computer to balance the load to other computer systems in the network by using more than one of the connection paths available.
- A fully connected mesh network therefore has n (n-1)/2 physical channels to link n devices.
- To accommodate these, every device on the network must have (n-l) input/output ports.

Advantages of Mesh Topology

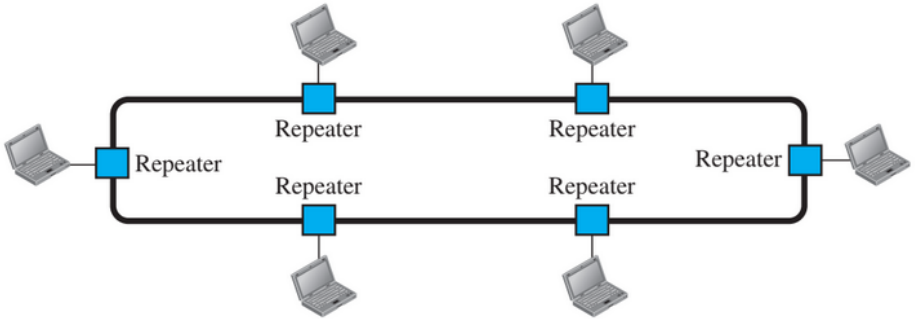
- Use of dedicated links eliminates traffic problems.
- Failure in one of the computers does not affect the entire network.
- Point-to-point link makes fault isolation easy.
- It is robust.
- Privacy between computers is maintained as messages travel along dedicated path.

Disadvantages of Mesh Topology

- The amount of cabling required is high.
- A large number of I/O (input/output) ports are required.

Network Topology: RING

- In ring topology, each node is connected to two other devices, one each on either side.
- The nodes connected with each other thus forms a ring.
- The link in a ring topology is unidirectional.
- Data is transmitted around the ring in one direction only; each station passing on the data to the next station till it reaches its destination.(clockwise or counterclockwise).
- Ring systems use 4 pair cables (separate send/receive).
- The common implementation of this topology is token ring.
- A break in the ring causes the entire network to fail. Individual workstations can be isolated from the ring.



Network Topology: RING

- Each packet of data sent on the ring is prefixed by the address of the station to which it is being sent.
- When a packet of data arrives, the workstation checks to see if the packet address is the same as its own, if it is, it grabs the data in the packet.
- If the packet does not belong to it, it sends to the next workstation in the ring.
- Faulty workstations can be isolated from the ring.
- When the workstation is powered on, it connects itself to the ring.
- When power is off, it disconnects itself from the ring and allows the information to bypass the workstation.

Advantages of Ring Topology

- Easy to install and modify the network.
- Fault isolation is simplified.
- Unlike Bus topology, there is no signal loss in Ring topology because the tokens are data packets that are re-generated at each node.

Disadvantages of Ring Topology

- Adding or removing computers disrupts the entire network.
- A break in the ring can stop the transmission in the entire network.
- Finding fault is difficult.
- Expensive when compared to other topologies.

Network Topology: BUS

- In bus topology , each communicating device connects to a transmission medium,central cable, called the bus or backbone..
- Data sent from a node are passed on to the bus and hence are transmitted to the length of the bus in both directions.
- That means, data can be received by any of the nodes connected to the bus.
- In this topology, a single backbone wire called bus is shared among the nodes, which makes it cheaper and easier to maintain.
- If one workstation goes faulty all workstations may be affected as all workstations share the same cable for the sending and receiving of information.
- Both ring and bus topologies are considered to be less secure and less reliable.
- The common implementation of this topology is Ethernet.

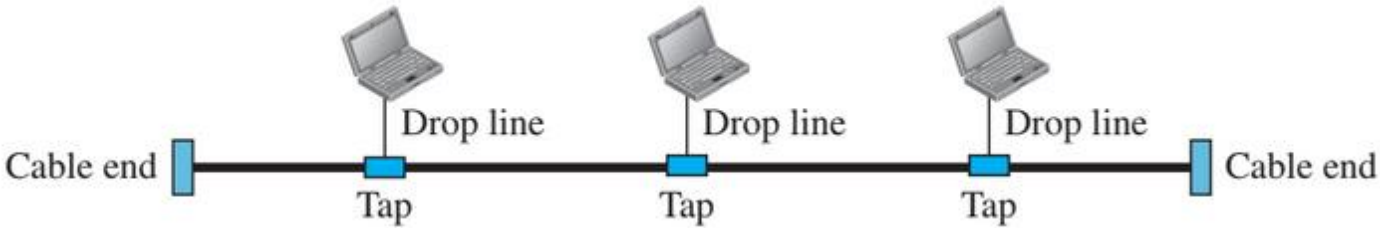
Network Topology: BUS

Advantages of Bus Topology

- Installation is easy and cheap when compared to other topologies
- Connections are simple and this topology is easy to use.
- Less cabling is required.

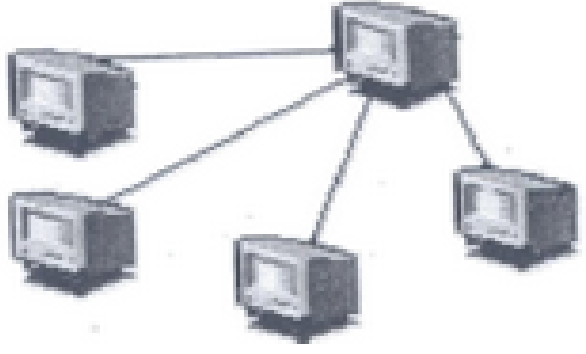
Disadvantages of Bus Topology

- Used only in comparatively small networks.
- As all computers share the same bus, the performance of the network deteriorates when we increase the number of computers beyond a certain limit.
- Fault identification is difficult.
- A single fault in the cable stops all transmission.



Network Topology: STAR

- In star topology, each communicating device is connected to a central node, which is a networking device like a hub or a switch.
- Star topology is considered very effective, efficient and fast as each device is directly connected with the central device.
- Although disturbance in one device will not affect the rest of the network, any failure in a central networking device may lead to the failure of complete network.
- The central node can be either a broadcasting device means data will be transmitted to all the nodes in the network, or a unicast device means the node can identify the destination and forward data to that node only.



Network Topology: STAR

Advantages of Star Topology

- Installation and configuration of network is easy.
- Less expensive when compared to mesh topology.
- Faults in the network can be easily traced.
- Expansion and modification of star network is easy.
- Single computer failure does not affect the network.
- Supports multiple cable types like shielded twisted pair cable, unshielded twisted pair cable, ordinary telephone cable etc.

Disadvantages of Star Topology

- Failure in the central hub brings the entire network to a halt.
- More cabling is required in comparison to tree or bus topology because each node is connected to the central hub.

Network Topology: HYBRID

- It is a hierarchical topology, in which there are multiple branches and each branch can have one or more basic topologies like star, ring and bus.
- Such topologies are usually realised in WANs where multiple LANs are Connected.
  Those LANs may be in the form of a ring, bus or star.
- In this type of network, data transmitted from source first reaches the centralised device and from there the data passes through every branch where each branch can have links for more nodes.
- A tree topology combines characteristics of linear bus and star topologies.
- It consists of groups of star configured workstations connected to a linear bus backbone cable.
- Tree topologies allow for the expansion of an existing network,and enable schools to configure a network to meet their needs.

Category	Star	Ring	Bus	Mesh
Structure	Central hub with all terminals connected to it	Workstations connected in a closed loop	Single cable connects all workstations in a point-to-point manner	Each computer connected to all other computers
Central Hub/Node	Central hub (host computer)	No central hub; workstations connected to two others	No central hub; single cable serves as the backbone	No central hub; fully connected network
Cabling Requirements	Significant; each terminal wired back to the hub	Moderate; 4-pair cables (separate send/receive)	Least; single cable used for all connections	Very high; requires multiple cables to connect
Routing	Central hub makes all routing decisions	Data transmitted in one direction; each station passes data along	No routing required; all workstations hear every message	No specific routing; multiple paths available
Failure Impact	Failure of one terminal doesn’t affect others; hub failure affects all	Failure of one workstation can be isolated; break in the ring causes full network failure	Failure of one workstation affects all others	Failure of one computer doesn't affect others due to redundant paths
Data Transmission	All data passes through the central hub	Data moves in one direction around the ring	Data sent by one workstation is heard by all others	Data can be sent through multiple paths
Common Use Case	Connecting terminals to a host computer	Token ring networks	Ethernet networks	Critical connections (e.g., telephone exchanges)
Cost	High, due to extensive cabling	Moderate	Low, due to minimal cabling	Very high, due to extensive cabling requirements
Scalability	Easy to add or remove terminals	Moderate; adding/removing requires adjusting connections	Difficult; adding/removing requires adjusting cable connections	Difficult; adding new computers requires extensive cabling

Switching: Circuit Switching

- Circuit Switched networks use a networking technology that provides a temporary, but dedicated connection between two stations no matter how many switching devices are used in the data transfer route.
- Circuit switching was originally developed for the analog based telephone system in order to guarantee steady and consistent service for two people engaged in a phone conversation.
- Analog circuit switching has given way to digital circuit switching, and the digital counterpart still maintains the connection until broken (one side hangs up).
- This means bandwidth is continuously reserved and “silence is transmitted” just the same as digital audio in voice conversation.

Switching: Circuit Switching

- **Resource Reservation:** Circuit switching reserves resources (buffers, link transmission rate) along a path for the duration of a communication session between end systems.
- **Resource Utilization:** Packet switching is considered more efficient as it does not reserve resources, unlike circuit switching which can leave resources idle during silent periods.
- **Complexity:** Circuit switching requires complex signaling software to establish end-to-end circuits and reserve transmission capacity.
- **Example:** Traditional telephone networks establish a circuit between sender and receiver, reserving a constant transmission rate for the connection.

Multiplexing in Circuit-Switched Networks

- **Frequency-Division Multiplexing (FDM):** Divides the frequency spectrum of a link into bands, each dedicated to a connection.
- **Time-Division Multiplexing (TDM):** Divides time into frames with fixed slots, each slot dedicated to a connection.

Switching: Circuit Switching

Example Calculation

- **File Transmission:** To send a 640,000-bit file over a circuit-switched network with 1.536 Mbps links using TDM (24 slots) and a 500 msec circuit establishment time:
  - Each circuit's transmission rate: 1.536 Mbps/24=64 kbps1.536 \text{ Mbps} / 24 = 64 \text{ kbps}1.536 Mbps/24=64 kbps
  - Transmission time for file: 640,000 bits/64 kbps=10 seconds640,000 \text{ bits} / 64 \text{ kbps} = 10 \text{ seconds}640,000 bits/64 kbps=10 seconds
  - Total time (including circuit establishment): 10 seconds+0.5 seconds=10.5 seconds10 \text{ seconds} + 0.5 \text{ seconds} = 10.5 \text{ seconds}10 seconds+0.5 seconds=10.5 seconds

This comparison highlights the key differences between packet switching and circuit switching, focusing on efficiency, resource utilization, and complexity.

Switching: Packet Switching

- Packet switched Networks use a networking technology that breaks up a message into smaller packets for transmission and switches them to their required destination.
- Unlike circuit switching, which requires a constant point-to-point circuit to be established, each packet in a packet-switched network contains a destination address.
- Thus, all packets in a single message do not have to travel the same path. They can be dynamically routed over the network as lines become available or unavailable.
- The destination computer reassembles the packets back into their proper sequence.
- Packet switching efficiently handles messages of different lengths and priorities.
- By accounting for packets sent, a public network can charge customers for only the data they transmit.
- Packet switching has been widely used for data, but not for real-time voice and video.
- However, this is beginning to change. IP and ATM technologies are expected to enable packet switching to be used for everything.
- The first international standard for wide area packet switching networks was X.25, which was defined when all circuits were digited and susceptible to noise.
- Subsequent technologies, such as frame relay and SMDS were designed for today's almost-error-free digital lines.
- ATM uses a cell-switching technology that provides the bandwidth sharing efficiency of packet switching with the guaranteed bandwidth of circuit switching.
- Higher-level protocols, such as TCPIIP, IPX/SPX and NetBIOS, are also packet based and are designed to ride over packet-switched topologies.
- Public packet switching networks may provide value added services, such as protocol conversion and electronic mail.

Switching: Packet Switching

- **End Systems and Messages:** In a network, end systems (like computers and smartphones) exchange messages. Messages can contain anything the application designer wants, such as control functions or data like emails and images.
- **Packets:** Long messages are broken into smaller chunks of data known as packets.
- **Transmission:** Packets travel through communication links and packet switches (routers and link-layer switches). Each packet is transmitted over communication links at the full transmission rate of the link.

Store-and-Forward Transmission

- **Definition:** In store-and-forward transmission, a packet switch receives the entire packet before transmitting any part of it onto the outbound link.
- **Example Network:** Consider a simple network with two end systems connected by a single router. If a source has three packets to send, it transmits them one by one. The router must store each entire packet before forwarding it to the destination.
- **Delay Calculation:**
    - Time to send one packet: L/RL/RL/R seconds (where LLL is packet length in bits and RRR is transmission rate in bits/second).
    - Total delay for one packet: 2L/R2L/R2L/R seconds (store-and-forward delay).
    - Total delay for three packets: 4L/R4L/R4L/R seconds.

Switching: Packet Switching

Queuing Delays and Packet Loss

- **Output Buffers:** Each packet switch has output buffers for storing packets before transmission.
- **Queuing Delay:** If a link is busy, arriving packets must wait in the output buffer, causing variable queuing delays.
- **Packet Loss:** If the buffer is full, arriving packets or already-queued packets will be dropped.

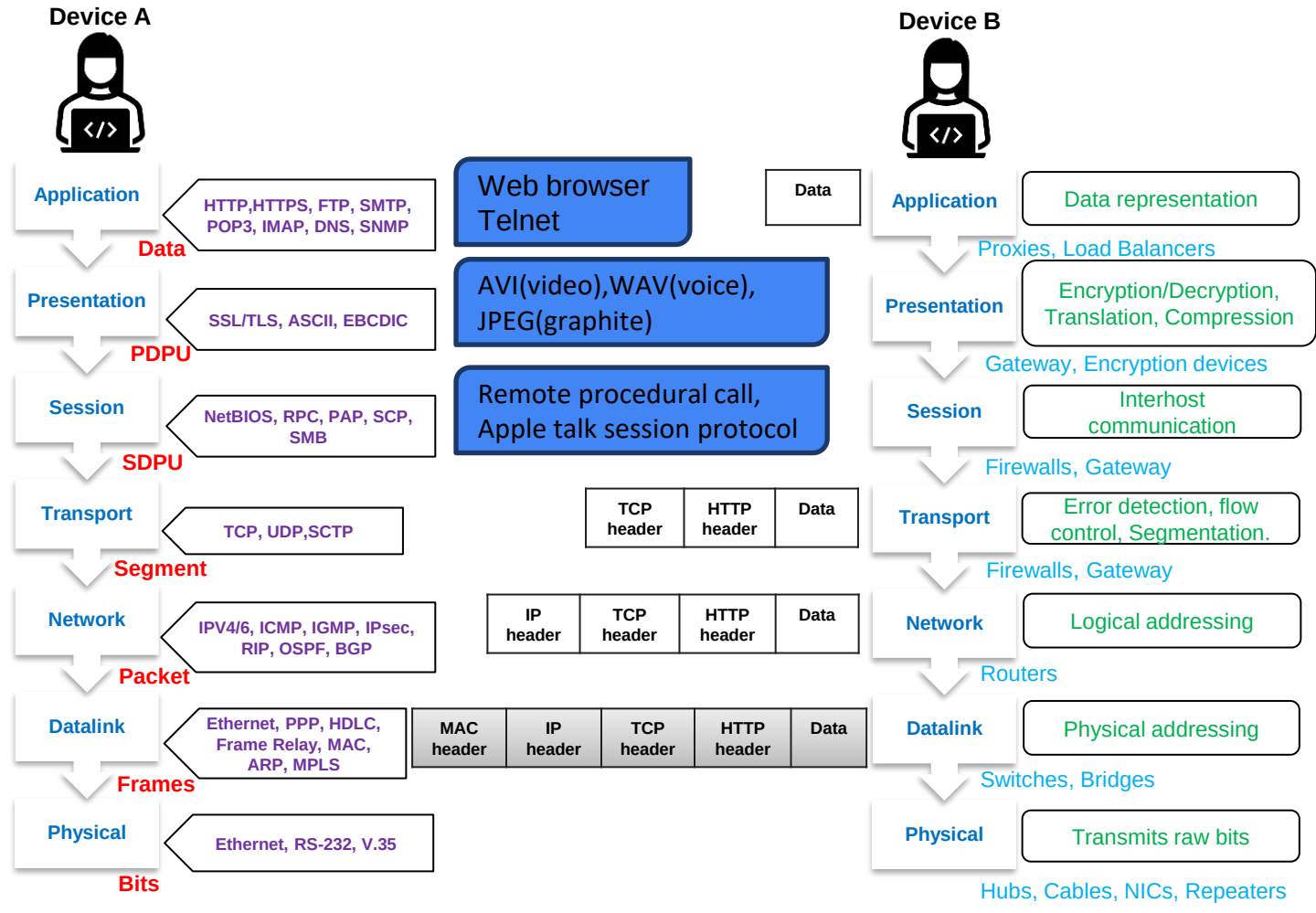
Forwarding Tables and Routing Protocols

- **Packet Forwarding:** Routers forward packets based on the destination IP address in the packet's header.
- **Forwarding Table:** Each router has a forwarding table mapping destination addresses to outbound links.
- **Routing Protocols:** Special protocols automatically set forwarding tables, determining paths and configuring routers accordingly.

	Packet switching	Circuit switching
Transmission Capacity	Better sharing of transmission capacity, as link usage is allocated on demand.	Pre-allocates transmission capacity regardless of demand, leading to potential unused link time.
Implementation Complexity	Simpler, more efficient, and less costly to implement.	More complex and costly to implement.
Real-Time Services	Variable and unpredictable end-to-end delays due to queuing, less suitable for real-time services like telephone calls and video conferencing.	Predictable and fixed delays, making it more suitable for real-time services.
Performance	Performance can degrade when the number of active users exceeds the capacity, but this is statistically rare.	Consistent performance, but only supports a limited number of simultaneous users based on fixed capacity allocation.
Efficiency	High efficiency, especially when users have intermittent periods of activity and inactivity.	Less efficient, as capacity must be reserved for each user at all times.
Scalability	Highly scalable, supports a large number of users by sharing the transmission link dynamically based on demand.	Limited scalability, as it can only support a fixed number of users based on the pre-allocated capacity.
Resource Utilization	Utilizes resources more effectively by dynamically allocating bandwidth to active users.	Less effective resource utilization due to static allocation, leading to potential underuse.
Delay	Variable delays depending on network congestion and queuing.	Fixed and predictable delays.
Data Transmission	Transmits data in packets, each potentially taking a different route to the destination.	Establishes a dedicated circuit for the duration of the communication session.
Adaptability	More adaptable to varying network conditions and user demands.	Less adaptable, as it relies on fixed allocations.

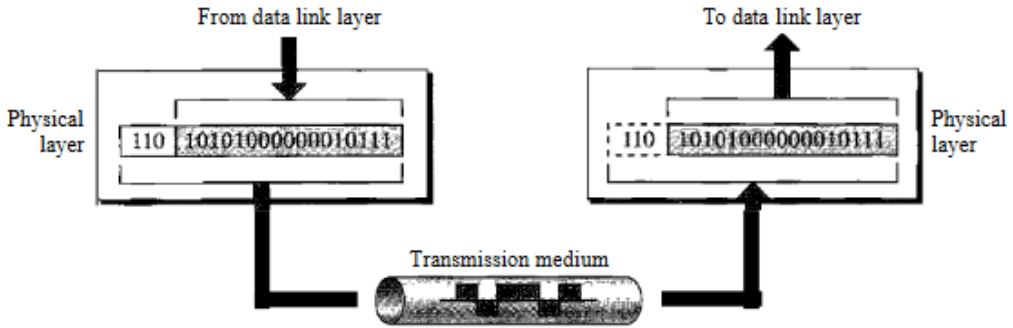
Open System Interconnection (OSI)

- The Open System Interconnection (OSI) model is a set of protocols that attempt to define and standardise the data communications process; we can say that it is a concept that describes how data communications should take place.
- The OSI model was set by the International Standards Organisation (ISO) in 1984, and it is now considered the primary architectural model for inter-computer communications.
- The OSI model has the support of most major computer and network vendors, many large customers, and most governments in different countries.
- The Open Systems Interconnection (OS1) reference model describes how information from a software application in one computer moves through a network medium to a software application in another computer.
- The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups.
- A task or group of tasks is then assigned to each of the seven OSI layers.
- Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently.
- This enables the solutions offered by one layer to be updated without affecting the other layers.


Device A
Device B
Application
HTTP,HTTPS, FTP, SMTP, POP3, IMAP, DNS, SNMP
Data
Web browser
Telnet
Data
Application
Data representation
Proxies, Load Balancers
Presentation
SSL/TLS, ASCII, EBCDIC
PDPU
AVI(video),WAV(voice), JPEG(graphite)
Presentation
Encryption/Decryption, Translation, Compression
Gateway, Encryption devices
Session
NetBIOS, RPC, PAP, SCP, SMB
SDPU
Remote procedural call, Apple talk session protocol
Session
Interhost communication
Firewalls, Gateway
Transport
TCP, UDP,SCTP
Segment
TCP header
HTTP header
Data
Transport
Error detection, flow control, Segmentation.
Firewalls, Gateway
Network
IPV4/6, ICMP, IGMP, IPsec, RIP, OSPF, BGP
Packet
IP header
TCP header
HTTP header
Data
Network
Logical addressing
Routers
Datalink
Ethernet, PPP, HDLC, Frame Relay, MAC, ARP, MPLS
Frames
MAC header
IP header
TCP header
HTTP header
Data
Datalink
Physical addressing
Switches, Bridges
Physical
Ethernet, RS-232, V.35
Bits
Physical
Transmits raw bits
Hubs, Cables, NICs, Repeaters

Physical layer

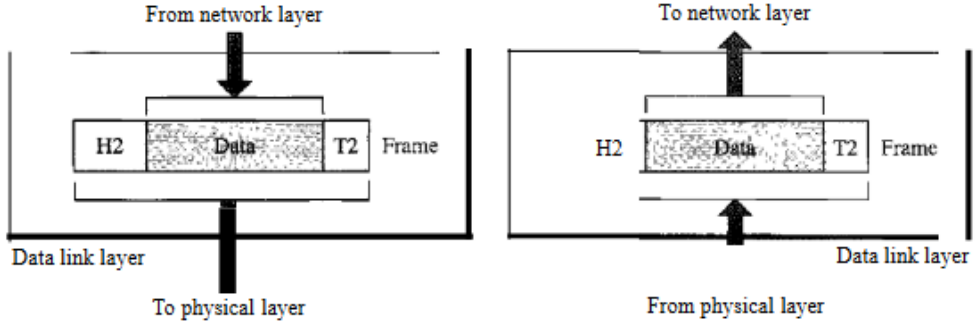
- The physical layer is the first /lowest layer in the OSI model.
- This layer is concerned with transmitting raw bits of data over a communication channel.
- The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1, not a 0 bit.
- Layer 1, the physical layer, defines the electrical, mechanical and functional interface between a DCE and the transmission medium to enable bits to be transmitted successfully.
- The layer is always implemented in hardware.
- A common example used extensively in modems is the ITU-T's V.24 serial interface.



Data link layer

- The data link layer provides the node to node packet delivery service.
- Its function includes transmission/reception of structured streams of bits over the network media.
- It provides the facility to subdivide the raw bit stream into structured blocks of information commonly called frames/packets.
- Data link protocols usually include some means of error detection, typically based upon a simple checksum included at the end of the frame.
- A noise burst on the line can destroy a frame completely.
- In this case the data link layer's software on the source machine must retransmit the frame.
- Multiple transmissions of the same frame introduces the possibility of duplicate frames.
- A duplicate frame could be sent, for example, if the acknowledgement frame from the receiver back to the sender was destroyed.
- It is up to this layer to solve the problems caused by damaged, lost, and duplicate frames so that layer 3 can assume it is working with an error free line.
- Another problem that arises at the data link layer and at most of the higher layers is how to keep a fast transmitter from drowning a slow receiver in data.
- Some mechanisms must be employed to let the transmitter know how much buffer space the receiver has at the moment.
- Typically, this mechanism and error handling are integrated together.

Data link layer

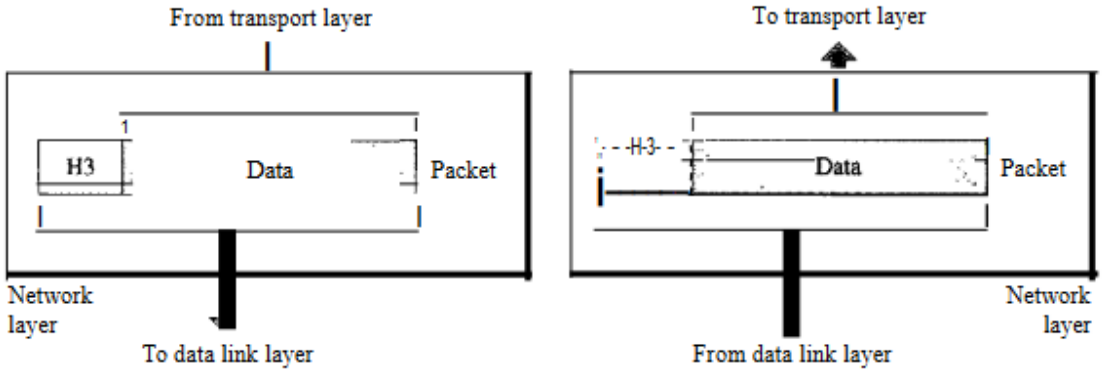


Responsibilities of the data link layer include the following:

- 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 devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any time.

Network layer

- This unit determines how packets, the units of information exchange in layer 3, are routed within the network.
- It should also insure that all packets are correctly received at their destinations and in the proper order.
- This layer basically receives messages from the source host, converts them into packets, and sees to it that the packets get directed towards the destination.
- A key design issue is how the route is determined. This layer also looks after congestion control.



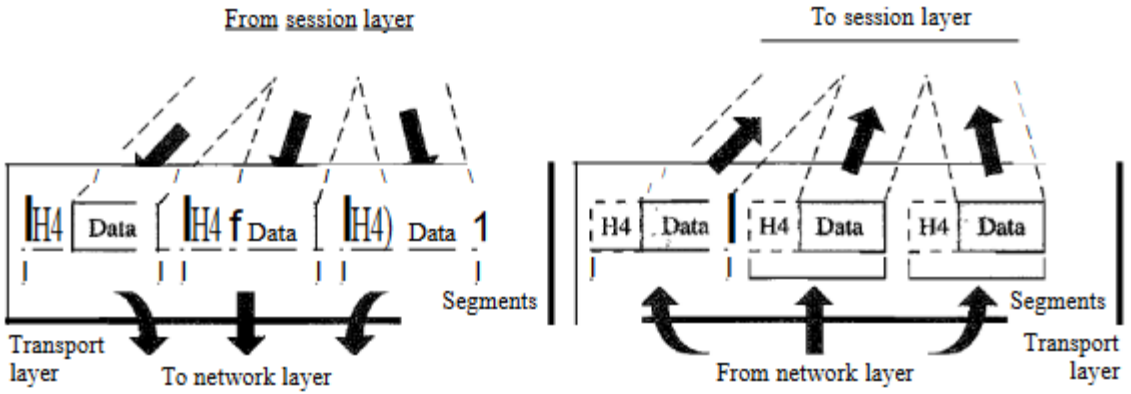
Network layer

Responsibilities of the network layer include the following:

- 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. We discuss logical addresses later in this chapter.
- Routing. When independent networks or links are connected to create intemetworks (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

- This layer provides for the transparent transfer of data, e.g., files between systems which might organize their data somewhat differently.
- It relieves the transport user from any concern about how in detail data transfers may be affected and optimises the available communications resources.
- This layer can be viewed as a bridge between the communication oriented lower three layers and the application oriented upper three layers.



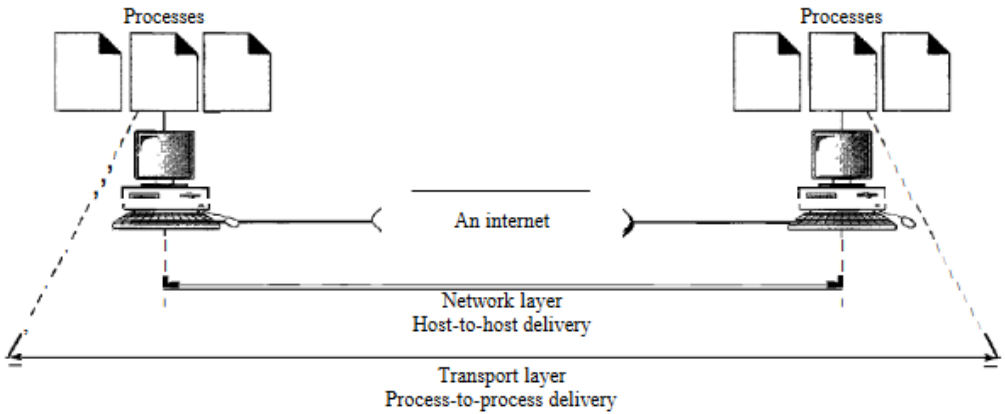
Transport layer

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 tne 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.

Transport layer

- 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.

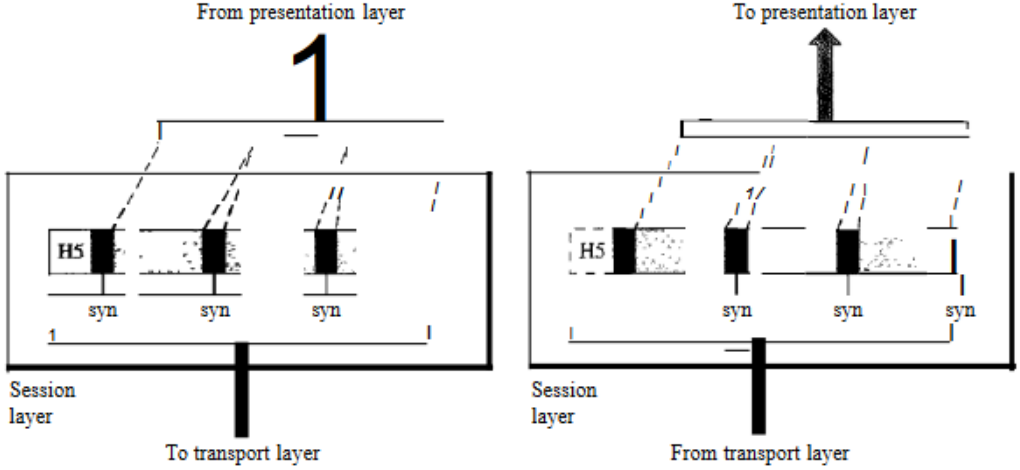


Session layer

- This layer supports the establishment, control and termination of dialogues between application processes.
- It facilitates full duplex operation and maintains continuity of session connections.
- It also supports synchronization between user's equipment and generally manages the data exchanges for the applications task.

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.



Presentation layer

- The presentation layer is concerned with the syntax and semantics of the information transmitted.
- A typical example of a presentation service is encoding data in a standard agreed upon way.
- Most user programs do not exchange random binary bit strings.
- They exchange things such as people's names, dates, amount of money, and invoices.
- These items are represented as character strings, integers, floating point numbers, and data structures composed of several simpler items.
- Different computers have different codes for representing character strings (e.g., ASCII and ABCDIC), integers (e.g.,one's complement and two's complement)..
- In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used ‘on the wire’.
- The job of managing these abstract data structures and converting from the representation used inside the computer to the network standard representation is handled by the presentation layer.
- The presentation layer is also concerned with other aspects of information representation.
- For example, data compression can be used here to reduce the number of bits that have to be transmitted and cryptography is frequently required for privacy and authentication.

Presentation layer

a. Data Representation

- Different computers have different internal representations for data.
- All the large IBM mainframes use EBCDIC as the character code, whereas practically all other computers use ASCII.
- Some computers also represent integers in one's complement and other in two's complement.
- To solve this problem, a conversion will have to be made and this is carried out by the presentation layer.

b. Data Compression

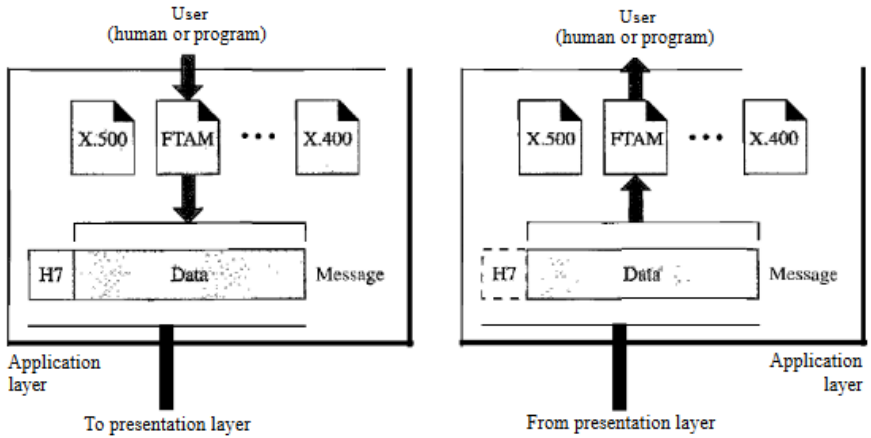
- The organizations that operate computer networks frequently expect to be paid for their efforts.
- In nearly all cases, the cost of using a network depends on the amount of data sent.
- It is clear that the more bytes sent, the more it costs, so the final bill can be reduced by compressing the data before sending them.
- Data compression has been studied in many context for years.
- It is widely used to save space in memory, on disk, and on magnetic tape.

c. Network Security and Privacy

- All the organization had to do was station a guard at the door to the computer room.
- The guard made sure that no one removed any tapes, disks, or card from the room unless explicitly authorized to do so.

Application layer

- The Application layer is probably the most easily misunderstood layer of the model.
- This top layer defines the language and syntax that programs use to communicate with other programs.
- The application layer represents the purpose of communicating in the first place.
- For example, a program in a client workstation uses commands to request data from a program in the server.
- Common functions at this layer are opening, closing, reading and writing files, transferring files and e-mail messages, executing remote jobs and obtaining directory information about network resources etc.



TCP/IP PROTOCOL SUITE

- The TCP/IP protocol architecture is a result of protocol research and development conducted on the experimental packet-switched network, ARPANET, funded by the Defense Advanced Research Projects Agency (DARPA), and is generally referred to as the TCP/IP protocol suite.
- The TCP/IP protocol suite was developed prior to the OSI model.
- Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers:
  - host-to-network,
  - Internet
  - transport, and
  - application.
- However, when TCP/IP is compared to OSI, we can say that the host-to-network layer is equivalent to the combination of the physical and data link layers.
- The internet layer is equivalent to the network layer, and the application layer is roughly doing the job of the session, presentation, and application layers with the transport layer in TCP/IP taking care of part of the duties of the session layer.

TCP/IP PROTOCOL SUITE

- TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- Whereas the OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system.
- The term hierarchical means that each upper-level protocol is supported by one or more lower-level protocols.
- At the transport layer, TCP/IP defines three protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).
- At the network layer, the main protocol defined by TCP/IP is the Internetworking Protocol (IP); there are also some other protocols that support data movement in this layer

Bandwidth

- **Bandwidth** measures network performance
- Bandwidth in hertz and bandwidth in bits per second.

Bandwidth in Hertz

- Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.
- For example, bandwidth of a subscriber telephone line is 4 kHz.

Bandwidth in Bits per Seconds

- The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit.
- For example, bandwidth of a Fast Ethernet network is a maximum of 100 Mbps.

Latency

- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.
- Latency is made of four components:
  - Propagation time,
  - Transmission time,
  - Queuing time and
  - Processing delay.

Latency = propagation time + transmission time + queuing time + processing delay

- Propagation time measures the time required for a bit to travel from the source to the destination.
- The propagation time is calculated by dividing the distance by the propagation speed.
- The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal.
- For example, in a vacuum, light is propagated with a speed of 3 × 10 ^8 m/s.
- It is lower in air; it is much lower in cable

Latency

- In data communications we don't send just 1 bit, we send a message.
- The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time.
- However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver.
- The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later.
- The transmission time of a message depends on the size of the message and the bandwidth of the channel

Transmission time = (Message size) / Bandwidth

- The queuing time, the time needed for each intermediate or end device to hold the message before it can be processed.
- The queuing time is not a fixed factor; it changes with the load imposed on the network.
- When there is heavy traffic on the network, the queuing time increases.
- An intermediate device, such as a router, queues the arrived messages and processes them one by one.
- If there are many messages, each message will have to wait.

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable

Twisted Pair

- The least-expensive and most widely-used guided transmission medium is twisted Pair
- Twisted-pair cable is used for baseband communication over relatively short distances, typically in modern LAN installations.
- A twisted pair possesses low inductance but high capacitance which causes substantial attenuation of signals at higher frequencies.
- Some environments where twisted-pair cables are deployed contain excessive electrical interference which may easily ingress into cable pairs and lead to excessive signal degradation.
- This typically occurs in the vicinity of high-voltage equipment.
- In such situations shielded twisted-pair cable may be used.
- Shielding consists of a tube of metallic braid, or winding a strip of foil, around each pair within the cable to minimize the amount of interference.
- Twisted-pair cables are therefore described as unshielded twisted pair (UTP) or shielded twisted pair (STP)

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable

–Separately insulated
–Twisted together
–Often "bundled" into cables
–Usually installed in buliding when built

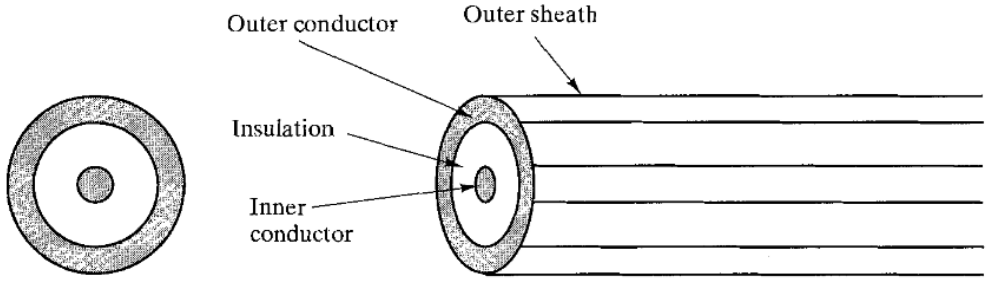
Twisted Pair

- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- A wire pair acts as a single communication link.
- Typically, a number of these pairs are bundled together into a cable by wrapping them in a tough protective sheath.
- Over longer distances, cables may contain hundreds of pairs. The twisting tends to decrease the crosstalk interference between adjacent pairs in a cable.
- Neighboring pairs in a bundle typically have somewhat different twist lengths to reduce the crosstalk interference.
- On long-distance links, the twist length typically varies from two to six inches. The wires in a pair have thicknesses of from 0.016 to 0.036 inches.

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable

- Unshielded twisted pair (UTP) is ordinary telephone wire.
- Office buildings, by universal practice, are pre-wired with a great deal of excess unshielded twisted pair, more than is needed for simple telephone support.
- This is the least expensive of all the transmission media commonly used for local area networks, and is easy to work with and simple to install.
- Unshielded twisted pair is subject to external electromagnetic interference, including interference from nearby twisted pair and from noise generated in the environment.
- A way to improve the characteristics of this medium is to shield the twisted pair with a metallic braid or sheathing that reduces interference.
- This shielded twisted pair (STP) provides better performance at lower data rates.
- However, it is more expensive and more difficult to work with than unshielded twisted pair

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable



–Outer conductor is braided shield
–Inner conductor is solid metal
–Separated by insulating material
–Covered by padding

Coaxial cable

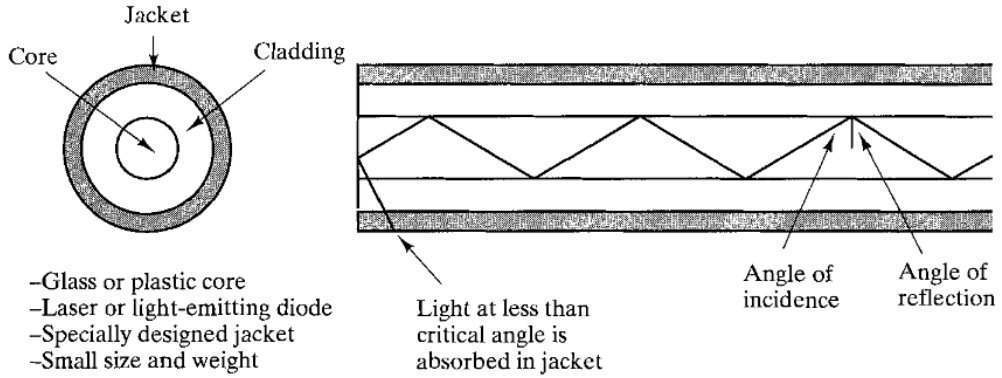
- Coaxial cable consists of two conductors, but is constructed differently to permit it to operate over a wider range of frequencies.
- It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor .
- The inner conductor is held in place by either regularly spaced insulating rings or a solid dielectric material.
- The outer conductor is covered with a jacket or shield.

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable

Coaxial cable

- The outer conductor is covered with a jacket or shield.
- A single coaxial cable has a diameter of from 0.4 to about 1 in.
- Because of its shielded, concentric construction, coaxial cable is much less susceptible to interference and crosstalk than is twisted pair.
- Coaxial cable can be used over longer distances and supports more stations on a shared line than twisted pair.
- Coaxial cable is used to transmit both analog and digital signals.
- Because of its shielded, concentric construction, coaxial cable is much less susceptible to interference and crosstalk than twisted pair.
- The principal constraints on performance are attenuation, thermal noise, and intermodulation noise.
- The latter is present only when several channels (FDM) or frequency bands are in use on the cable.
- For long-distance transmission of analog signals, amplifiers are needed every few kilometers, with closer spacing required if higher frequencies are used.
- The usable spectrum for analog signaling extends to about 400 MHz.
- For digital signaling, repeaters are needed every kilometer or so, with closer spacing needed for higher data rates.

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable



Optical fibre

- An optical fiber is a thin (2 to 125 pm), flexible medium capable of conducting an optical ray.
- Various glasses and plastics can be used to make optical fibers.
- The lowest losses have been obtained using fibers of ultrapure fused silica.
- Ultrapure fiber is difficult to manufacture; higher-loss multicomponent glass fibers are more economical and still provide good performance.

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable

Optical fibre

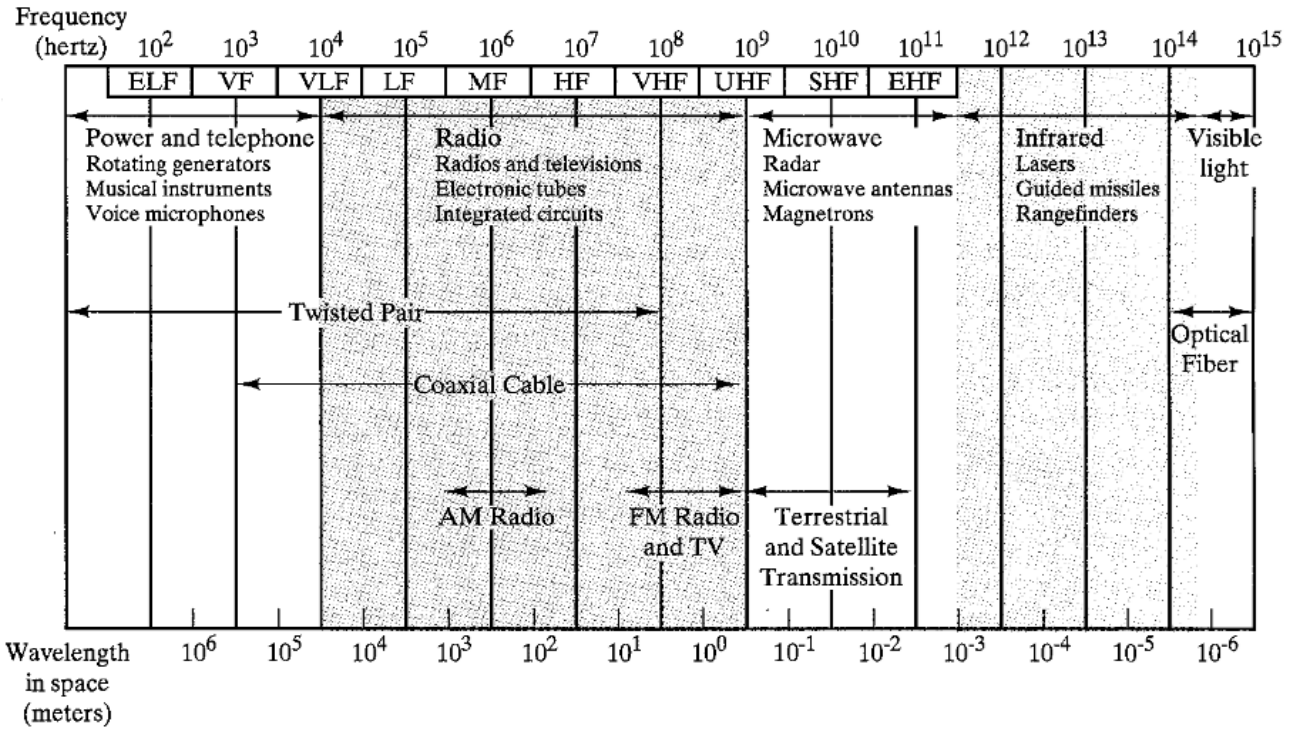
- Plastic fiber is even less costly and can be used for short-haul links, for which moderately high losses are acceptable.
- An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket.
- The core is the inner most section and consists of one or more very thin strands, or fibers, made of glass or plastic.
- Each fiber is surrounded by its own cladding, a glass or plastic coating has optical properties different from those of the core.
- The outermost layer, surrounding one or a bundle of cladded fibers, is the jacket.
- The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.
- Optical fiber systems operate in the range of about 10^14 to 10^15 Hz; this covers portions of the infrared and visible spectrums.

Guided Media: Twisted pair, Coaxial cable, Fiber optic cable

Optical fibre

- The principle of optical fiber transmission is as follows.
- Light from a source enters the cylindrical glass or plastic core.
- Rays at shallow angles are reflected and propagated along the fiber; other rays are absorbed by the surrounding material.
- This form of propagation is called multimode, referring to the variety of angles that will reflect.
- When the fiber core radius is reduced, fewer angles will reflect.
- By reducing the radius of the core to the order of a wavelength, only a single angle or mode can pass: the axial ray.
- This single mode propagation provides superior performance for the following reason:
- With multimode transmission, multiple propagation paths exist, each with a different path length and, hence, time to traverse the fiber; this causes signal elements to spread out in time, which limits the rate at which data can be accurately received.
- Because there is a single transmission path with single-mode transmission, such distortion cannot occur.

Unguided Media: Radio waves, Microwaves, Infrared



Unguided Media: Radio waves, Microwaves, Infrared.

Infrared

- Infrared communications is achieved using transmitters/receivers (transceivers) that modulate noncoherent infrared light.
- Transceivers must be in line of sight of each other, either directly or via reflection from a light-colored surface such as the ceiling of a room.
- One important difference between infrared and microwave transmission is that the former does not penetrate walls.
- Thus, the security and interference problems encountered in microwave systems are not present.
- Furthermore, there is no frequency allocation issue with infrared, because no licensing is required.
- Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.
- Infrared waves, having high frequencies, cannot penetrate walls.

Characteristics of Infrared Signals

- Infrared signal supports high bandwidth, so the data rate will be very high.
- It can not penetrate the wall. So communication in one room can not be interrupted by the nearby rooms.
- Its provides better security and minimum interference.
- Infrared communication doesn’t work well outside because sunlight interferes with the infrared signals.

- **Radio waves** are electromagnetic signals used for various wireless communication technologies, such as Wi-Fi, Bluetooth and radio broadcasting.
- Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves.
- Radio waves are omnidirectional.
- When an antenna transmits radio waves, they are propagated in all directions.
- This means that the sending and receiving antennas do not have to be aligned.
- A sending antenna sends waves that can be received by any receiving antenna.
- The omnidirectional property has a disadvantage, too.
- The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band.
- Radio waves use omnidirectional antennas that send out signals in all directions.
- Based on the wavelength, strength, and the purpose of transmission, we can have several types of antennas.

Advantages of Radio Waves

- It is used in WAN (Wide Area Network).
- Used in mobile Cellular phones.
- Radio wave spread in large area so they can penetrate the wall.
- It’s provide a higher transmission rate.

Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional.
- The sending and receiving antennas need to be aligned.
- The unidirectional property has an obvious advantage.
- A pair of antennas can be aligned without interfering with another pair of aligned antennas.
- Microwaves need unidirectional antennas that send out signals in one direction.
- Two types of antennas are used for microwave communications: the **parabolic dish** and the **horn**.

Terrestrial Microwave are microwaves that transmits the beam of a radio signal from one ground based antenna to another ground based antenna.

Characteristics of Terrestrial Microwave

- **Frequency range:** The frequency range of terrestrial microwave is from 4 GHz to 23 GHz.
- **Bandwidth:** Terrestrial Microwave supports the bandwidth range from 1 to 10 Mbps.
- **Short distance:** Terrestrial Microwave inexpensive for short distance.
- **Long distance:** Terrestrial Microwave expensive because it requires a higher tower length for a longer distance.
- **Attenuation:** Attenuation refer loss of signal. It is because of environmental conditions and antenna size.

- A satellite is a object that revolve around the earth. A satellite microwave is a type of communication technology that uses microwave radio waves to transmit data between a ground-based station and an orbiting satellite.
- A satellite get signal from ground based station, enhance that signal and transfer bak to another ground based station that is situated at different location on the earth. They orbit high above the planet, allowing them to cover large areas. This process enables long-distance communication, GPS navigation, and weather monitoring.