ADITYA ENGINEERING COLLEGE (A)

Computer Networks

By

Dr. M. Vamsi Krishna
Professor

Dept of Computer Science and Engineering
Aditya Engineering College(A)
Surampalem.

Course Outcomes

- ***CO 1:*** *Explain the computer network fundamentals and reference models.*
- ***CO 2:*** *Identify data link layer services and functions.*
- ***CO 3:*** *Classify MAC layer protocols and LAN technologies.*
- ***CO 4:*** *Apply various routing algorithms and Congestion control techniques for effective data transmission.*
- ***CO 5:*** *Utilize the services provided by the transport layer and application layer.*

Syllabus

- Unit – I
- **Introduction**:
- Network Types, LAN, MAN, WAN, Network Topologies Reference models- The OSI Reference Model, the TCP/IP Reference Model , A Comparison of the OSI and TCP/IP Reference Models, OSI Vs TCP/IP, Lack of OSI models success, Internet History.

- **Physical Layer**: Introduction to Guided Media- Twisted-pair cable, Coaxial cable and Fiber optic cable and unguided media: Wireless-Radio waves, microwaves, infrared.

Unit - II

- **Data link layer**: Design issues, **Framing**: fixed size framing, variable size framing, flow control, error control, error detection and correction codes, CRC, Checksum: idea, one's complement internet checksum, services provided to Network Layer.

- **Elementary Data Link Layer protocols**: Simplex protocol, Simplex stop and wait, Simplex protocol for Noisy Channel.

- **Sliding window protocol**: One bit, Go back N, Selective repeat-Stop and wait protocol, Data link layer in HDLC: configuration and transfer modes, frames, control field, point to point protocol (PPP): framing transition phase, multiplexing, multi link PPP.

Unit – III

- **Media Access Control**:
- Random Access: ALOHA, Carrier sense multiple access (CSMA), CSMA with Collision Detection, CSMA with Collision Avoidance, Controlled Access: Reservation, Polling, Token Passing, Channelization: frequency division multiple Access(FDMA), time division multiple access(TDMA), code division multiple access(CDMA).Wired LANs: Ethernet, Ethernet Protocol, Standard Ethernet, Fast Ethernet(100 Mbps), Gigabit Ethernet, 10 Gigabit Ethernet.

Unit - IV

- **The Network Layer Design Issues**:
- Store and Forward Packet Switching, Services Provided to the Transport layer, Implementation of Connectionless Service, Implementation of Connection Oriented Service, Comparison of Virtual Circuit and Datagram Networks, Routing Algorithms: The Optimality principle, Shortest path, Flooding, Distance vector, Link state, Hierarchical, Congestion Control algorithms: General principles of congestion control, Congestion prevention polices, Approaches to Congestion Control, Traffic Aware Routing, Admission Control, Traffic Throttling, Load Shedding, Traffic Control Algorithm:Leaky bucket & Token bucket.Internet Working: Network layer in the internet, IP protocols: IP Version 4,IP Version 6,Transition from IPV4 to IPV6, Comparison of IPV4 & IPV6,Internet control protocols: ICMP, ARP, DHCP

Unit - V

- **The Transport Layer**:
- Transport layer protocols: Introduction, services, port number, User data gram protocol: UDP services, UDP applications, Transmission control protocol: TCP services, TCP features, Segment, A TCP connection, windows in TCP, flow control, Error control, Congestion control in TCP.

- **Application Layer**:
- World Wide Web: HTTP, Electronic mail, Architecture, web based mail, email security, TELENET, local versus remote Logging, Domain Name System: Name Space, DNS, SNMP.

Text Books

1. Computer Networks — Andrew S Tanenbaum and David J Wetherall, 5th Edition, Pearson Education, 2013.
2. Data Communications and Networking – Behrouz A.Forouzan, 5th Edition, McGraw Hill Education, 2012.

Reference Books

1. Data Communications and Networks- Achut S Godbole, AtulKahate
2. Computer Networks, Mayank Dave, CENGAGE
3. An Engineering Approach to Computer Networks-S. Keshav, 2nd Edition, Pearson Education.

Web Links

- https://nptel.ac.in/courses/106105081
- https://www.coursera.org/learn/fundamentals-network-communications
- https://nptel.ac.in/courses/106/106/106106091/
- https://www.udemy.com/course/mta-networking-fundamentals/

Introduction

Unit - I

Contents

- Introduction:
- Network Types:
  - LAN, MAN, WAN.
- Network Topologies and Reference models.
  - The OSI Reference Model.
  - TCP/IP Reference .
  - A Comparison of the OSI and TCP/IP Reference Models.
  - OSI Vs TCP/IP.
  - Lack of OSI models success.
  - Internet History.
- Physical Layer:
  - Introduction to Guided Media
    - Twisted-pair cable.
    - Coaxial cable.

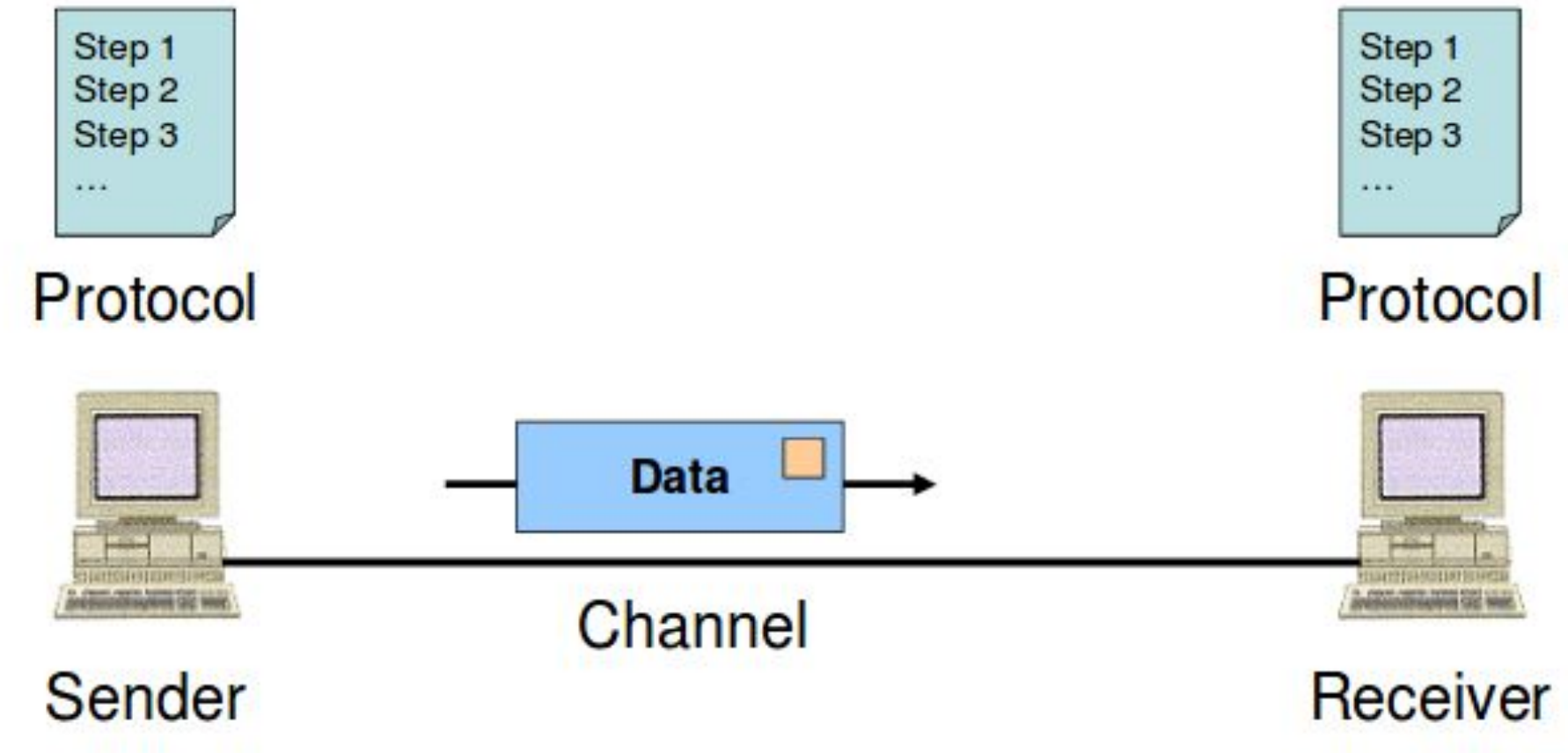
Introduction to Networks

- **Data Communication**: When we communicate, we are sharing information. This sharing can be local or remote.
- **Computer Network**: A computer network is a set of computers connected together for the purpose of sharing resources.

Components

- A data communications system has five components.

1. **Message**. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. **Sender**. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver**. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium**. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves
5. **Protocol**. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.


Step 1
Step 2
Step 3
...
Protocol
Step 1
Step 2
Step 3
...
Protocol
Data
Channel
Sender
Receiver

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.
- **Distributed Processing**
- Most networks use distributed processing, in which a task is divided among multiple computers.
- Instead of one single large machine being responsible for all aspects of a process, separate computers (usually a personal computer or workstation) handle a subset.

Network Criteria

- A network must be able to meet a certain number of criteria. The most important of these are **performance, reliability, and security**.
- **Performance**:
- Performance can be measured in many ways, including transit time and response time. **Transit time** is the amount of time required for a message to travel from one device to another.
- **Response time** is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
- Performance is often evaluated by two networking metrics: **throughput** and **delay**. We often need more throughput and less delay.
- However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

- **Reliability:**
- In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

- **Security**:
- Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Physical Structures:

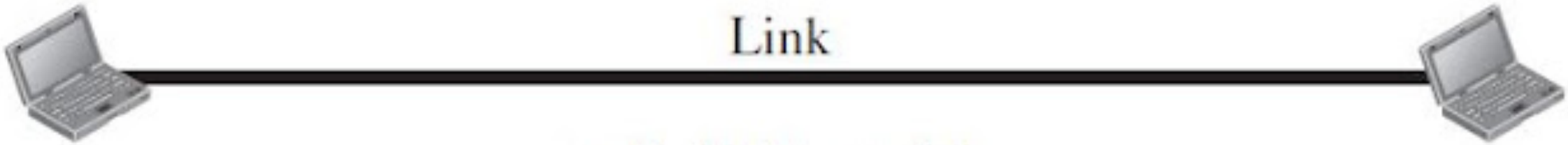
- **Type of Connection**
- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.
- For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time.
- There are two possible types of connections: **point-to-point** and **multipoint**.

Point-to-Point

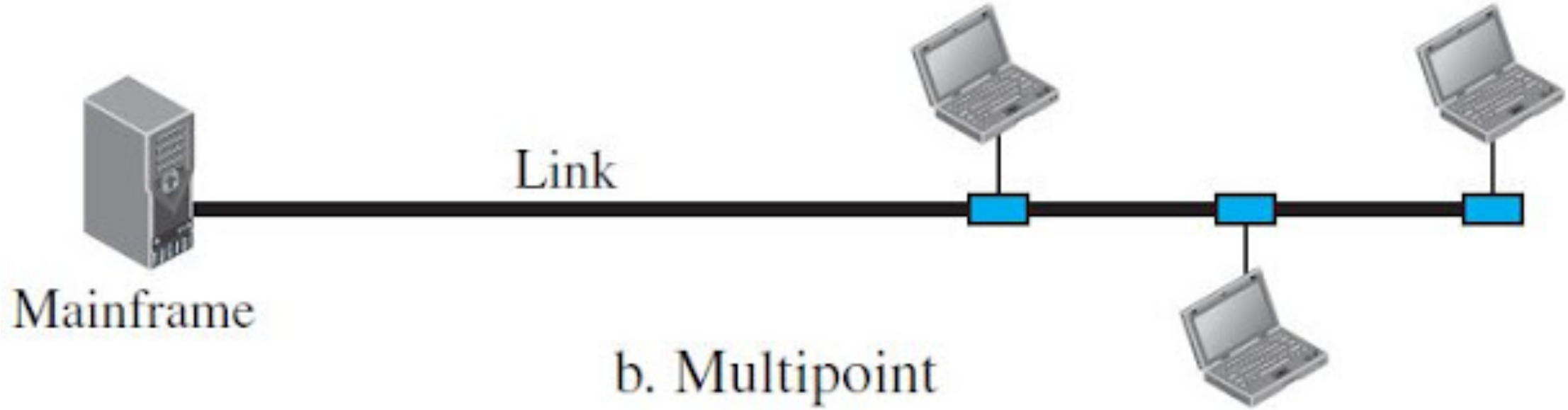
- A point-to-point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.
- Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.
- When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

Multipoint

- A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.
- In a multipoint environment, the capacity of the channel is shared, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection.
- If users must take turns, it is a timeshared connection.



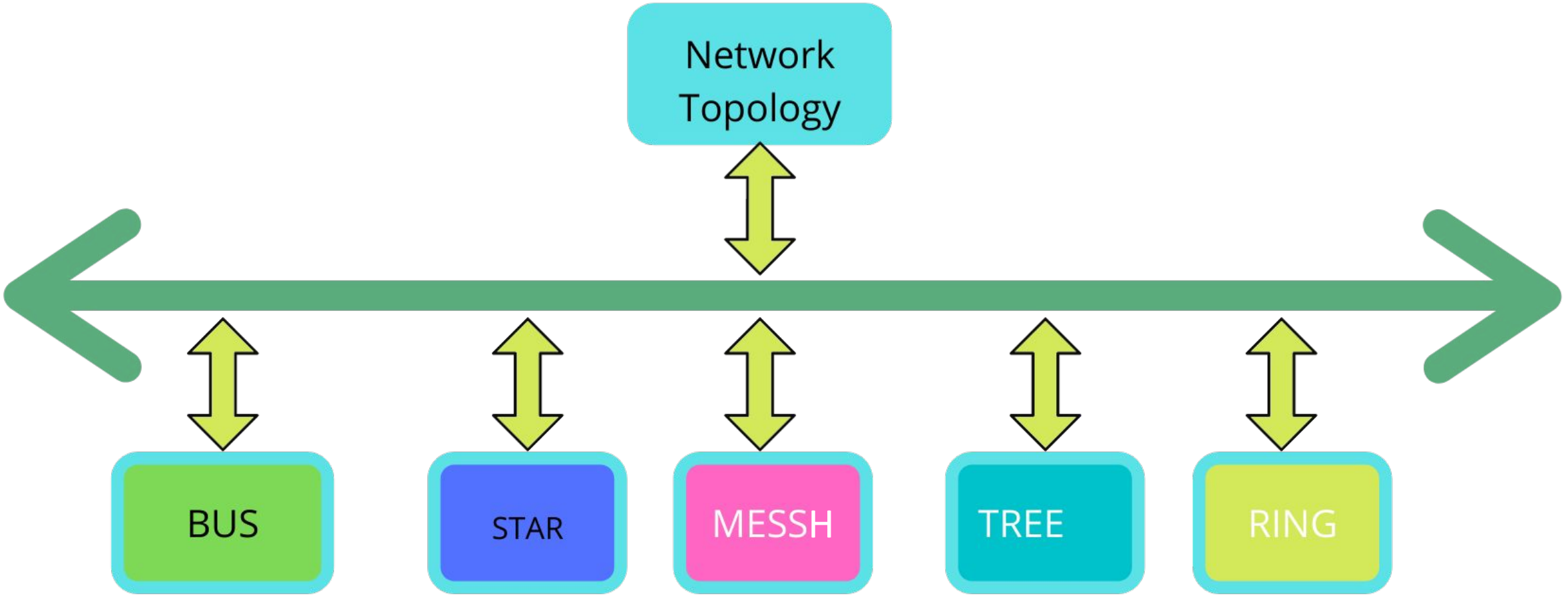
a. Point-to-point



b. Multipoint

Physical Topology

- The term physical topology refers to the way in which a network is laid out physically.
- One or more devices connect to a link; two or more links form a topology.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are five basic topologies possible: mesh, star, bus, tree, and ring


Network Topology
BUS
STAR
MESSH
TREE
RING

Mesh

- In a mesh topology, every device has a dedicated point-to-point link to every other device.
- The term dedicated means that the link carries traffic only between the two devices it connects.
- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node.
- Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes.
- We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2.
- In other words, we can say that in a mesh topology, we need n(n -1) /2 duplex-mode links.
- To accommodate that many links, every device on the network must have n – 1 input/output (VO) ports to be connected to the other n - 1 stations.

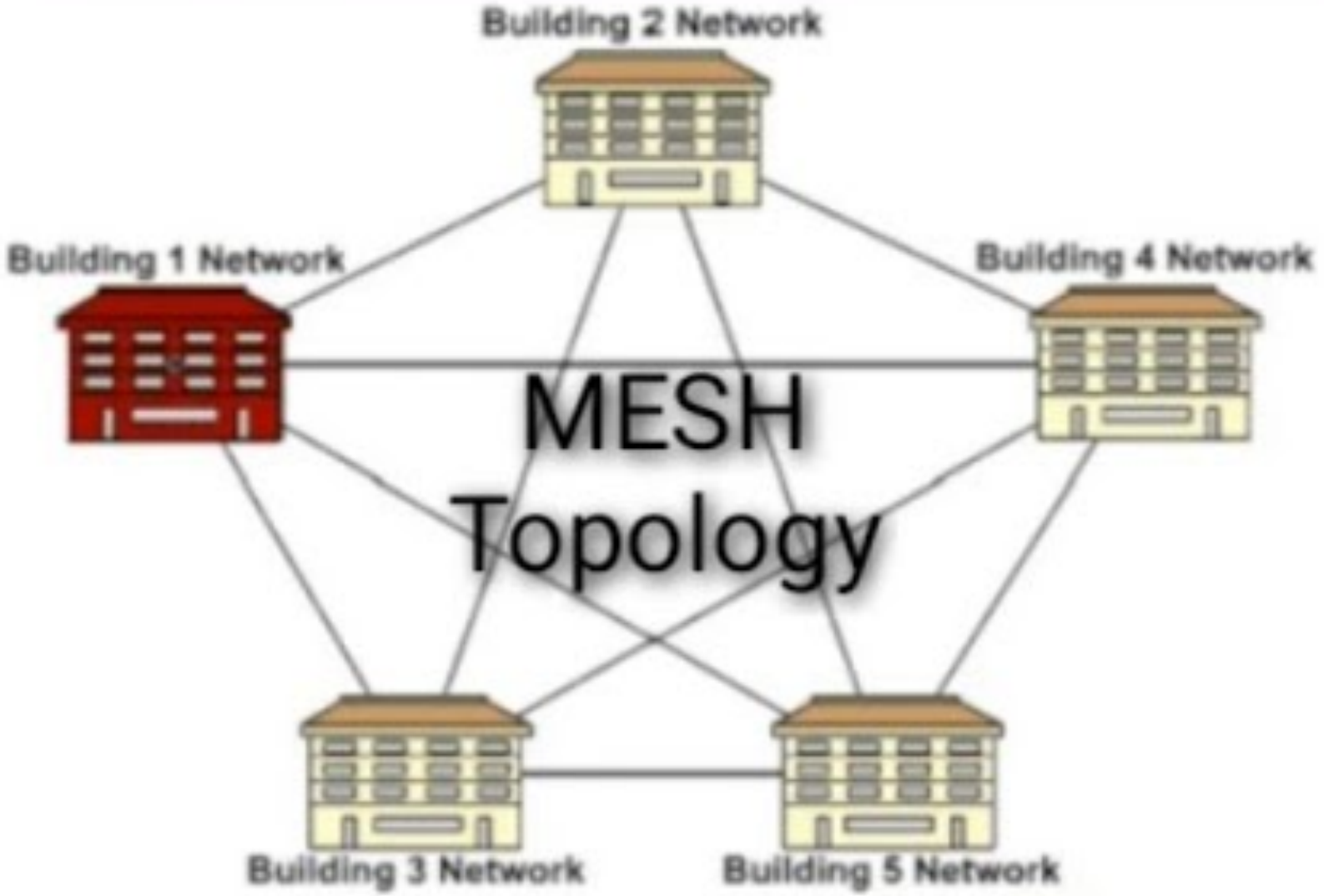
Advantages

1. The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
3. there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantage

1. Mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.
2. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

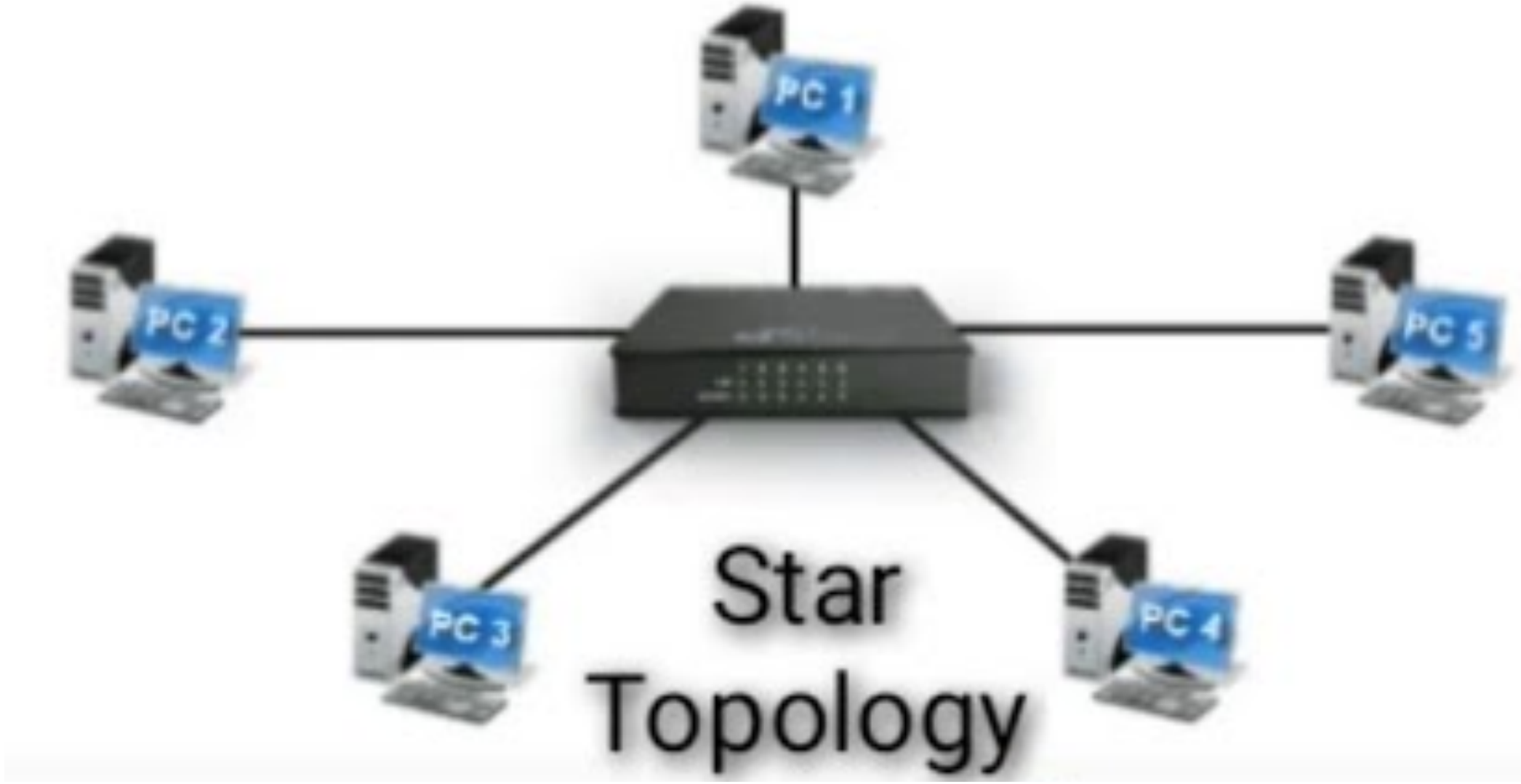
For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.


Building 2 Network
Building 1 Network
Building 4 Network
MESH
Topology
Building 3 Network
Building 5 Network

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .
- A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
- Other advantages include robustness. If one link fails, only that link is affected. All other links remain active.
- This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub.
- If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub.
- For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).


PC 1
PC 2
PC 5
PC 3
PC 4
Star
Topology

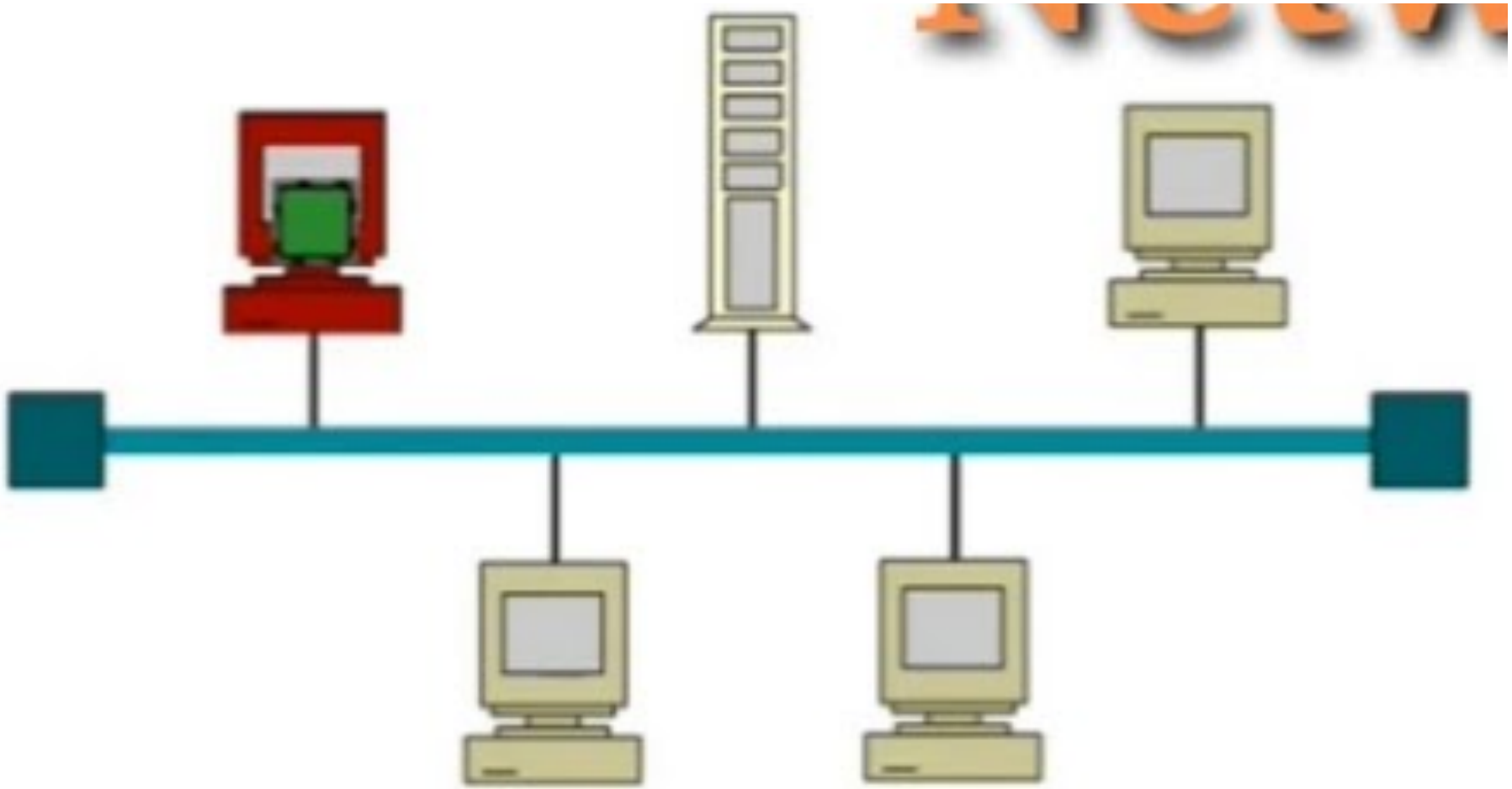
Bus Topology

- The preceding examples all describe point-to-point connections.
- A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed into heat.
- Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

- Advantages of a bus topology include ease of installation.
- Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
- In this way, a bus uses less cabling than mesh or star topologies.
- In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub.
- In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility.
- Each drop line has to reach only as far as the nearest point on the backbone.

- Disadvantages include difficult reconnection and fault isolation.
- A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
- Signal reflection at the taps can cause degradation in quality.
- This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
- Adding new devices may therefore require modification or replacement of the backbone.

- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.
- The damaged area reflects signals back in the direction of origin, creating noise in both directions.
- Bus topology was the one of the first topologies used in the design of early local area networks.
- Ethernet LANs can use a bus topology, but they are less popular.
- Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



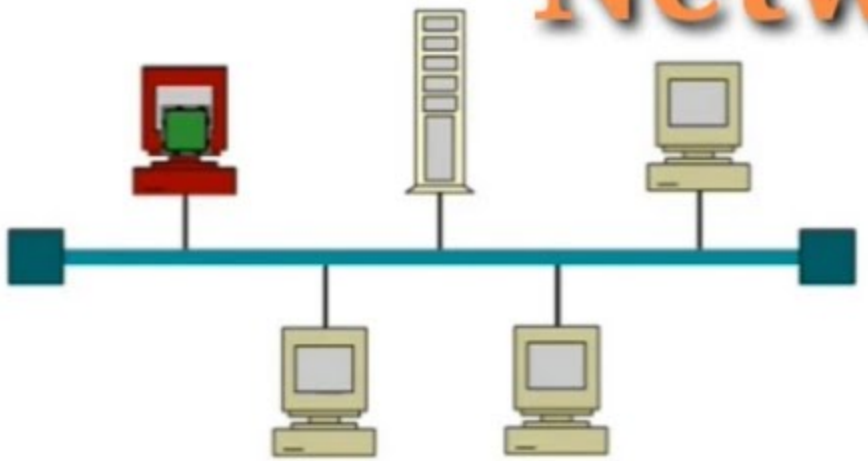
BUS Topology

Ring Topology

- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).
- To add or delete a device requires changing only two connections.
- The only constraints are media and traffic considerations (maximum ring length and number of devices).
- In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm.
- The alarm alerts the network operator to the problem and its location.

- However, unidirectional traffic can be a disadvantage.
- In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.
- This weakness can be solved by using a dual ring or a switch capable of closing off the break.
- Ring topology was prevalent when IBM introduced its local-area network Token Ring.
- Today, the need for higher-speed LANs has made this topology less popular. Hybrid Topology A network can be hybrid.

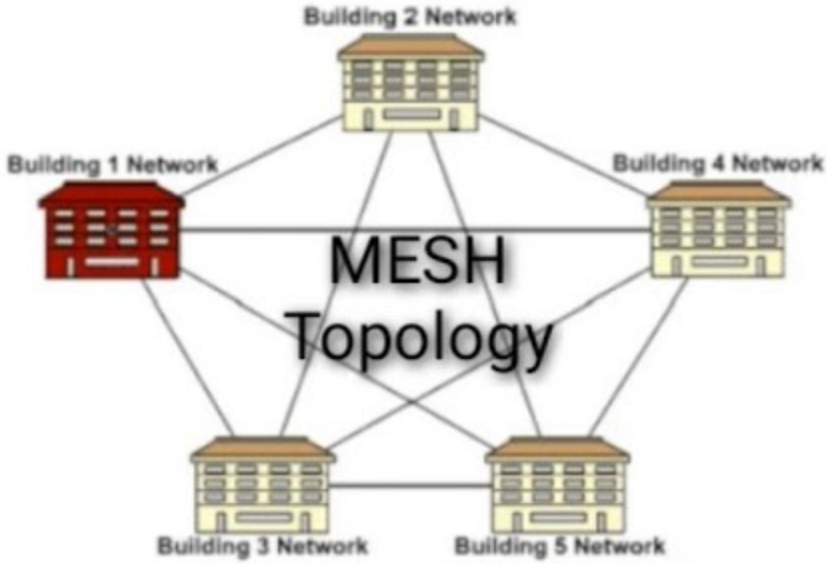
Network Topology

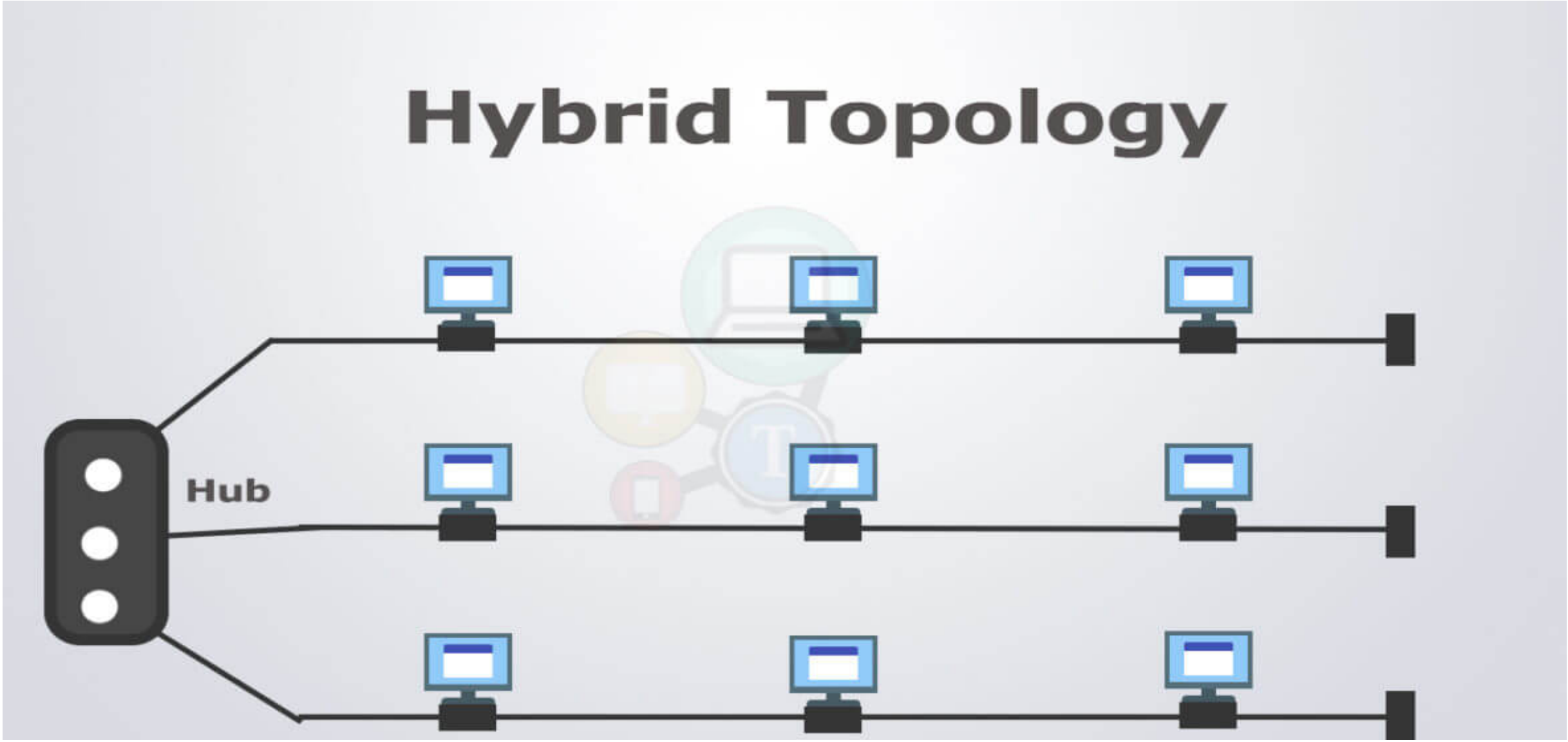


BUS Topology

Star Topology

Tree Topology




Hybrid Topology
Hub

Network Categories

- PAN
- LAN
- MAN
- WAN
- Internet

PAN

- Stands for **P**ersonal **A**rea **N**etworks.
- *It let devices communicate over the range of a person.*
- *A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer.*
- *Without using wireless, this connection must be done with cables.*
- *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.*
- *The idea is that if your devices have Bluetooth, then you need no cables. You just put them down, turn them on, and they work together.*

LAN

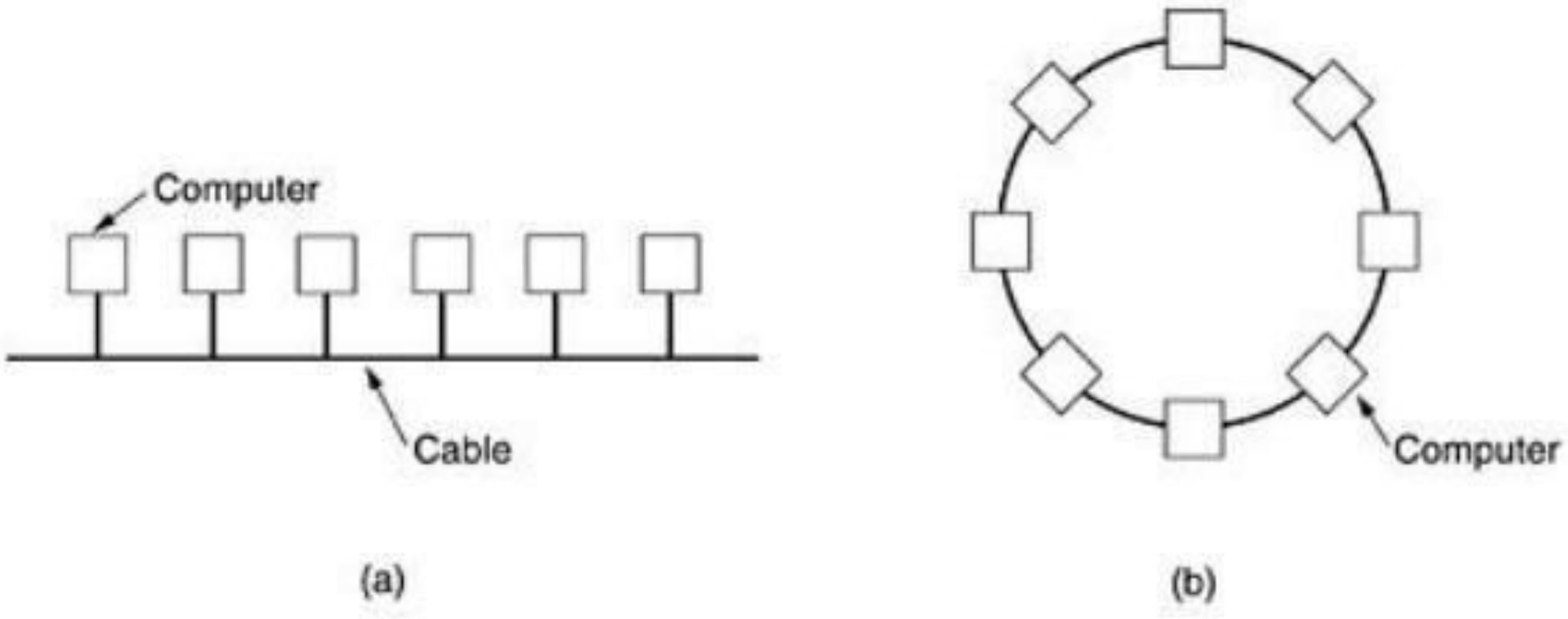
- Stands for **L**ocal **A**rea **N**etwork.
- *A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.*
- *LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.*
- *When LANs are used by companies, they are called **Enterprise Networks**.*
- *There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread.*

- *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.*
- *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.*
- *However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.*

- *LANs are distinguished from other kinds of networks by three characteristics:*
  - *Their size,*
  - *Their transmission technology, and*
  - *Their topology.*
- *LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.*
- *Knowing this bound makes it possible to use certain kinds of designs that would not otherwise be possible.*

- *It also simplifies network management.*
- *LANs may use a transmission technology consisting of a cable to which all the machines are attached, like the telephone company party lines once used in rural areas.*
- *Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay (microseconds or nanoseconds), and make very few errors.*
- *Newer LANs operate at up to 10 Gbps Various topologies are possible for broadcast LANs.*
- *Figure shows two of them. In a bus (i.e., a linear cable) network, at any instant at most one machine is the master and is allowed to transmit. All other machines are required to refrain from sending.*
- *An arbitration mechanism is needed to resolve conflicts when two or more machines want to transmit simultaneously. The arbitration mechanism may be centralized or distributed.*
- ***IEEE 802.3**, popularly called **Ethernet**, for example, is a bus-based broadcast network with decentralized control, usually operating at 10 Mbps to 10 Gbps.*
- *Computers on an Ethernet can transmit whenever they want to; if two or more packets collide, each computer just waits a random time and tries again later.*

Fig.1: Two broadcast networks . (a) Bus. (b) Ring.



- *A second type of broadcast system is the ring.*
- *In a ring, each bit propagates around on its own, not waiting for the rest of the packet to which it belongs.*
- *Typically, each bit circumnavigates the entire ring in the time it takes to transmit a few bits, often before the complete packet has even been transmitted.*
- *As with all other broadcast systems, some rule is needed for arbitrating simultaneous accesses to the ring.*
- *Various methods, such as having the machines take turns, are in use.*
- ***IEEE 802.5** (the IBM **Token Ring**), is a ring-based LAN operating at 4 and 16 Mbps. FDDI (Fiber Distributed Data Interface)is another example of a ring network.*

MAN

- *Stands for **M**etropolitan **A**rea **N**etwork.*
- *The best-known example of a MAN is the cable television network available in many cities.*
- *This system grew from earlier community antenna systems used in areas with poor over-the-air television reception.*
- *In these early systems, a large antenna was placed on top of a nearby hill and signal was then piped to the subscribers' houses.*
- *At first, these were locally-designed, ad hoc systems. Then companies began jumping into the business, getting contracts from city governments to wire up an entire city.*
- *The next step was television programming and even entire channels designed for cable only.*
- *Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on.*
- *But from their inception until the late 1990s, they were intended for television reception only.*

- *Cable television is not the only MAN. Recent developments in high-speed wireless Internet access resulted in another MAN, which has been standardized as **IEEE 802.16** popularly known as **WiMAX**.*
- *MAN is implemented by a standard called **DQDB** (Distributed Queue Dual Bus) or IEEE 802.16. DQDB has two unidirectional buses (or cables) to which all the computers are attached.*

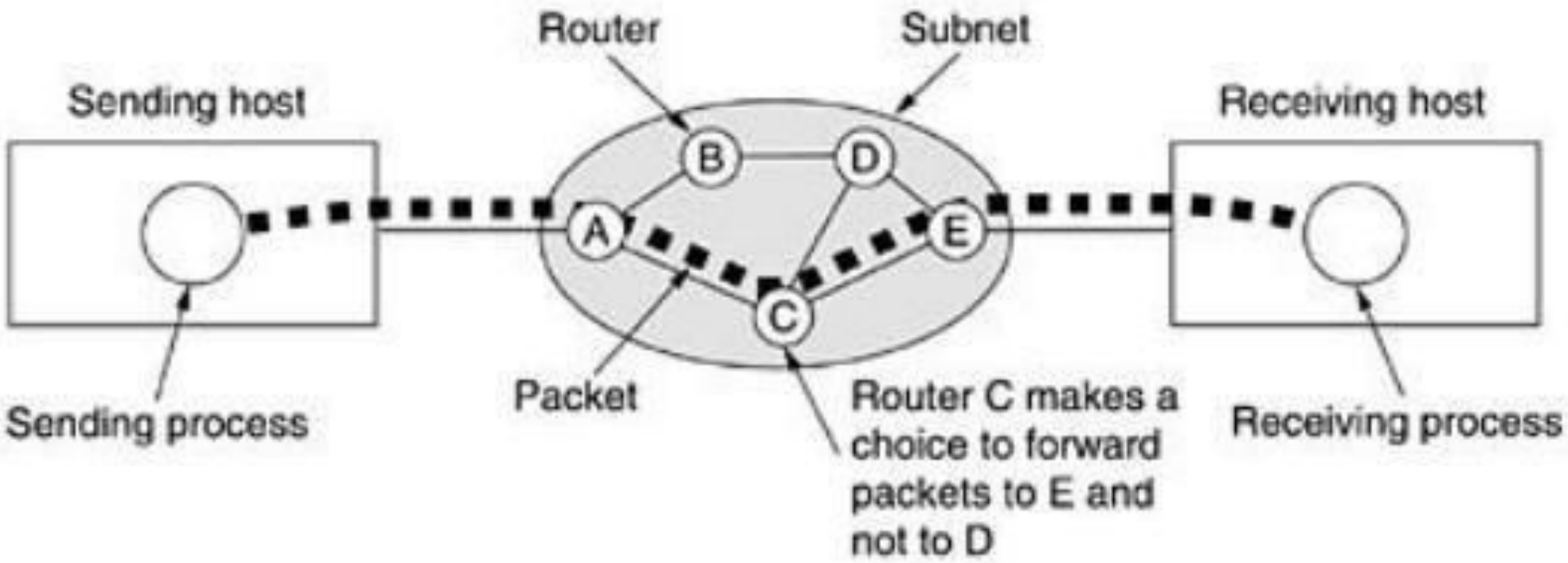
WAN

- *Stands for **W**ide **A**rea **N**etwork.*
- *It spans a large geographical area, often a country or continent.*
- *It contains a collection of machines intended for running user (i.e., application) programs.*
- *These machines are called as hosts.*
- *The hosts are connected by a communication subnet, or just subnet for short.*
- *The hosts are owned by the customers (e.g., people's personal computers), whereas the communication subnet is typically owned and operated by a telephone company or Internet service provider.*
- *The job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener.*

- *Separation of the pure communication aspects of the network (the subnet) from the application aspects (the hosts), greatly simplifies the complete network design.*
- *In most wide area networks, the subnet consists of two 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.*
- *In most WANs, the network contains numerous transmission lines, each one connecting a pair of routers.*
- *If two routers that do not share a transmission line wish to communicate, they must do this indirectly, via other routers.*
- *When a packet is sent from one router to another via one or more intermediate routers, the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded.*
- *A subnet organized according to this principle is called a* ***store-and-forward*** *or* ***packet-switched*** *subnet.*
- *Nearly all wide area networks (except those using satellites) have store-and-forward subnets.*
- *When the packets are small and all the same size, they are often called* ***cells****.*

- *The principle of a packet-switched WAN is so important.*
- *Generally, when a process on some host has a message to be sent to a process on some other host, the sending host first cuts the message into packets, each one bearing its number in the sequence.*
- *These packets are then injected into the network one at a time in quick succession.*
- *The packets are transported individually over the network and deposited at the receiving host, where they are reassembled into the original message and delivered to the receiving process.*
- *A stream of packets resulting from some initial message is illustrated in Fig.*
- *In this figure, all the packets follow the route ACE, rather than ABDE or ACDE.*
- *In some networks all packets from a given message must follow the same route; in others each packet is routed separately.*
- *Of course, if ACE is the best route, all packets may be sent along it, even if each packet is individually routed.*

Fig: A stream of packets from sender to receiver.



- *Not all WANs are packet switched.*
- *A second possibility for a WAN is a satellite system.*
- *Each router has an antenna through which it can send and receive.*
- *All routers can hear the output from the satellite, and in some cases they can also hear the upward transmissions of their fellow routers to the satellite as well.*
- *Sometimes the routers are connected to a substantial point-to-point subnet, with only some of them having a satellite antenna.*
- *Satellite networks are inherently broadcast and are most useful when the broadcast property is important.*

Internetworks

- *The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time.*
- *The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.*

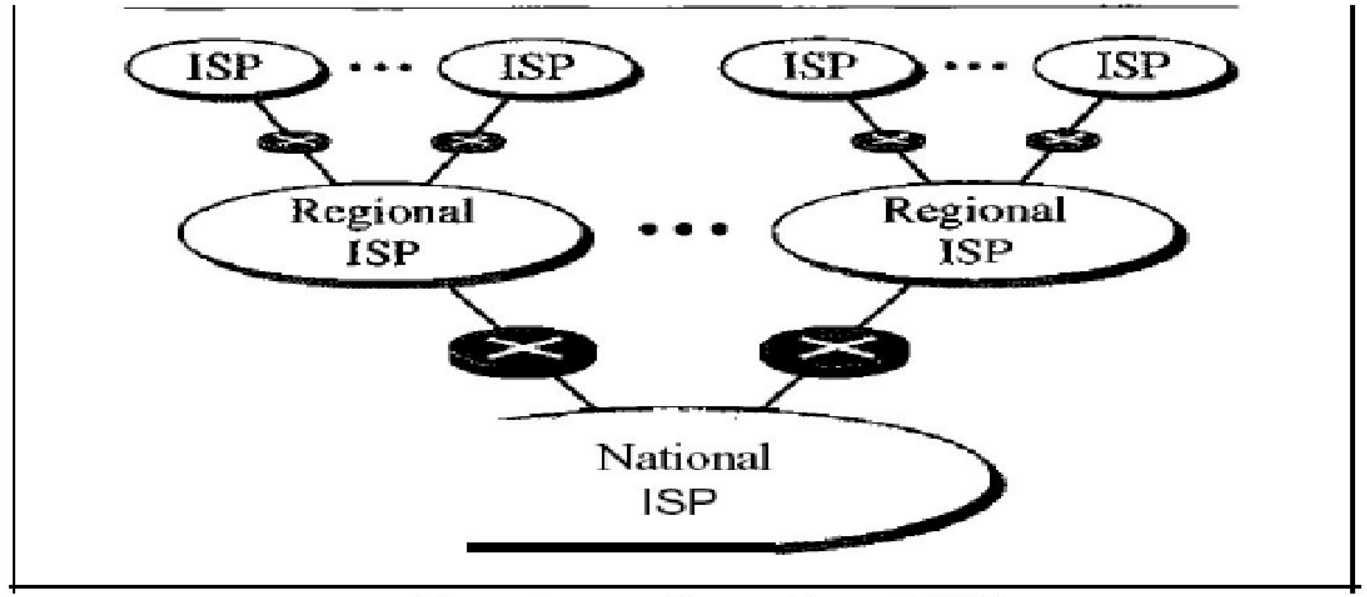
- *A network is a group of connected communicating devices such as computers and printers.*
- *An internet (note the lowercase letter i) is two or more networks that can communicate with each other.*
- *The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.*
- *Private individuals as well as various organizations such as government agencies, schools, research facilities, corporations, and libraries in more than 100 countries use the Internet.*
- *Millions of people are users. Yet this extraordinary communication system only came into being in 1969.*

- *In the mid-1960s, mainframe computers in research organizations were standalone devices.*
- *Computers from different manufacturers were unable to communicate with one another.*
- *The **A**dvanced **R**esearch **P**rojects **A**gency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.*
- *In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP).*
- *The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.*
- *By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network.*
- *Software called the **N**etwork **C**ontrol **P**rotocol (NCP) provided communication between the hosts.*

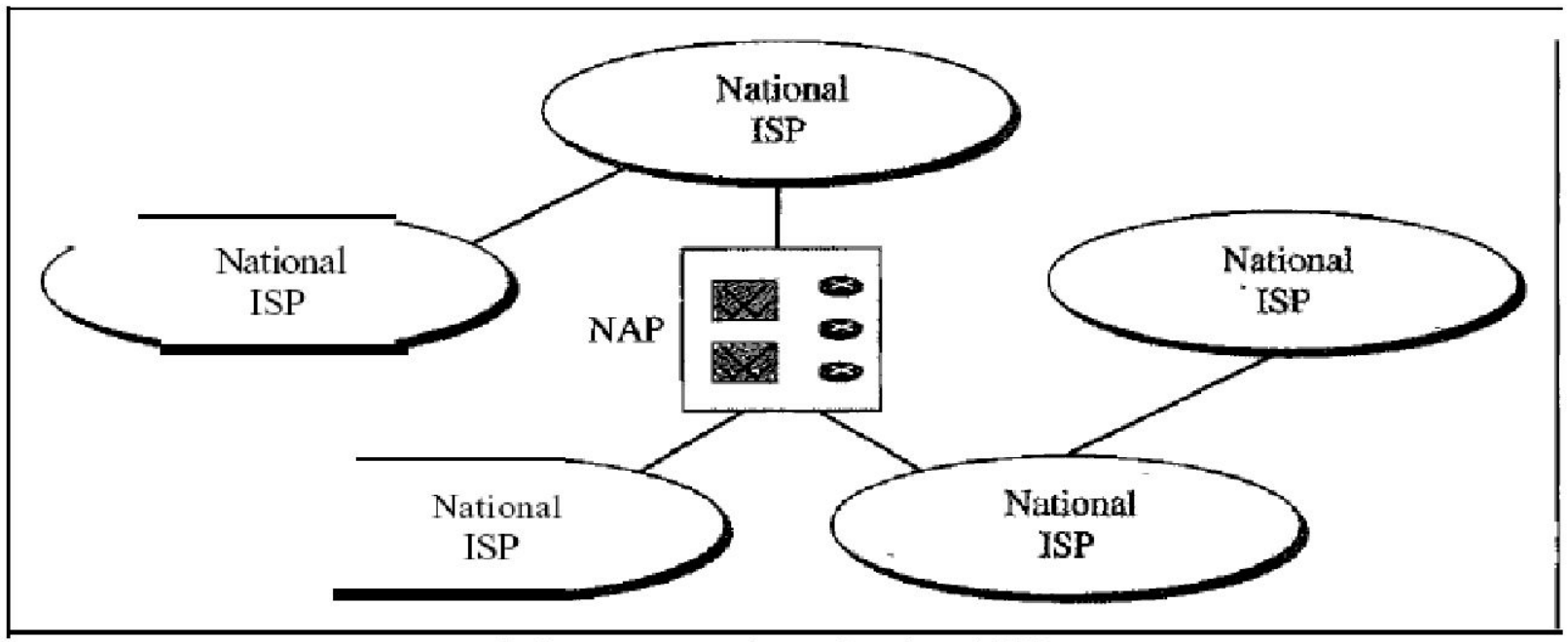
- *In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Project.*
- *Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.*
- *Shortly thereafter, authorities made a decision to split TCP into two protocols: **T**ransmission **C**ontrol **P**rotocol (TCP) and **I**nternetworking **P**rotocol (IP).*
- *IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection.*
- *The internetworking protocol became known as **TCP/IP**.*

Internet Today

- *The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure.*
- *It is made up of many wide- and local-area networks joined by connecting devices and switching stations.*
- *It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed.*
- *Today most end users who want Internet connection use the services of Internet service providers (lSPs).*
- *There are international service providers, national service providers, regional service providers, and local service providers.*
- *The Internet today is run by private companies, not the government.*



a. Structure of a national ISP



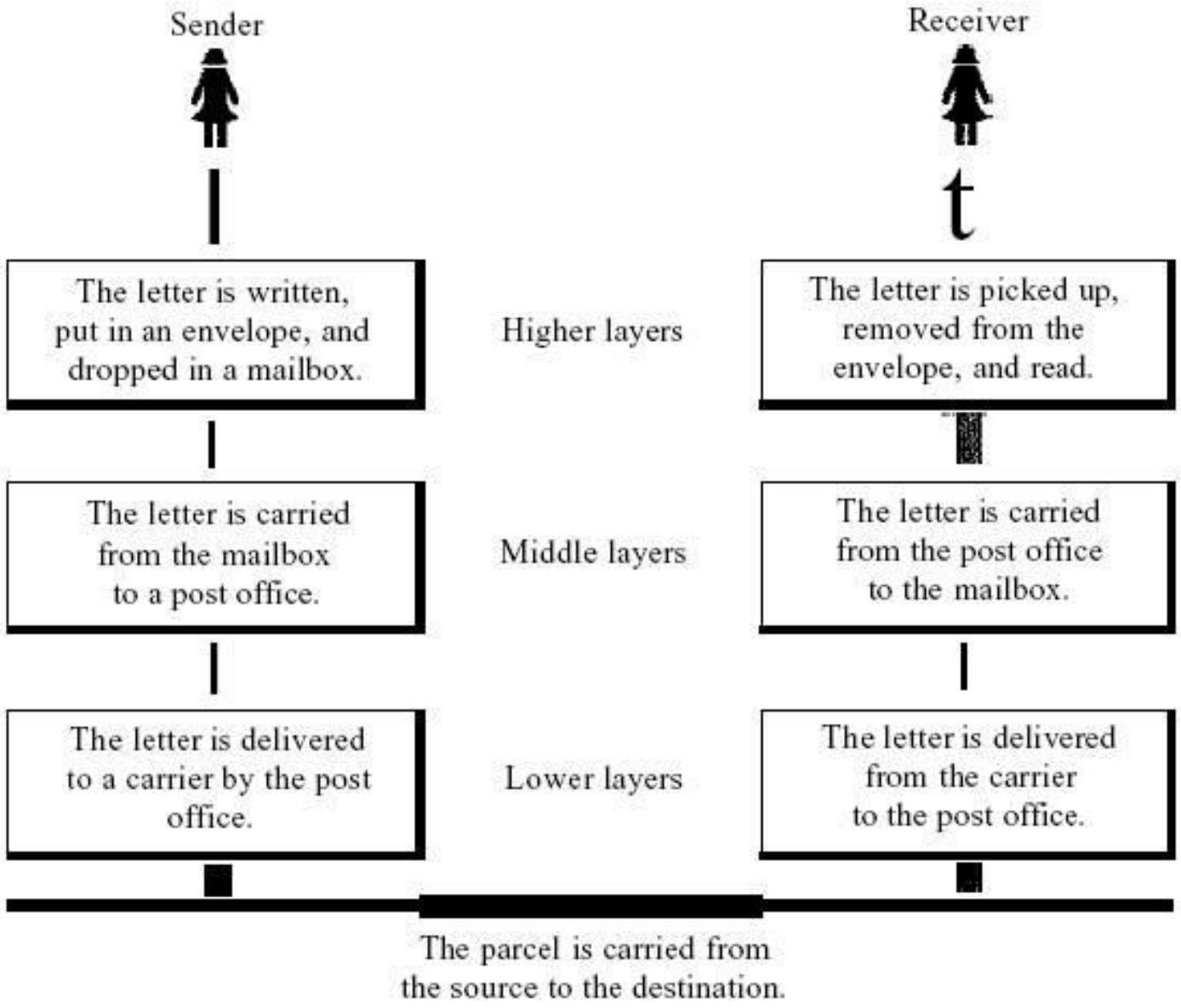
b. Interconnection of national ISPs

- ***International Internet Service Providers***:
- *At the top of the hierarchy are the international service providers that connect nations together.*
- ***National Internet Service Providers***:
- *The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel.*
- *To provide connectivity between the end users, these backbone networks are connected by complex switching stations (normally run by a third party) called **N**etwork **A**ccess **P**oints (NAPs).*
- *Some national ISP networks are also connected to one another by private switching stations called peering points.*
- *These normally operate at a high data rate (up to 600 Mbps).*

- ***Regional Internet Service Providers***:
- *Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs.*
- *They are at the third level of the hierarchy with a smaller data rate.*
- ***Local Internet Service Providers***:
- *Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs.*
- *Most end users are connected to the local ISPs.*
- *Note that in this sense, a local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network.*
- *Each of these local ISPs can be connected to a regional or national service provider.*

Layered Tasks

- *We use the concept of layers in our daily life.*
- *As an example, let us consider two friends who communicate through postal mail.*
- *The process of sending a letter to a friend would be complex if there were no services available from the post office.*
- *Below Figure shows the steps in this task.*


Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

- *In Figure we have a sender, a receiver, and a carrier that transports the letter.*
- *There is a hierarchy of tasks.*
- ***At the Sender Site***
- *Let us first describe, in order, the activities that take place at the sender site.*
  - ***Higher layer**. The sender writes the letter, inserts the letter in an envelope, writes the sender and receiver addresses, and drops the letter in a mailbox.*
  - ***Middle layer**. The letter is picked up by a letter carrier and delivered to the post office.*
  - ***Lower layer**. The letter is sorted at the post office; a carrier transports the letter.*

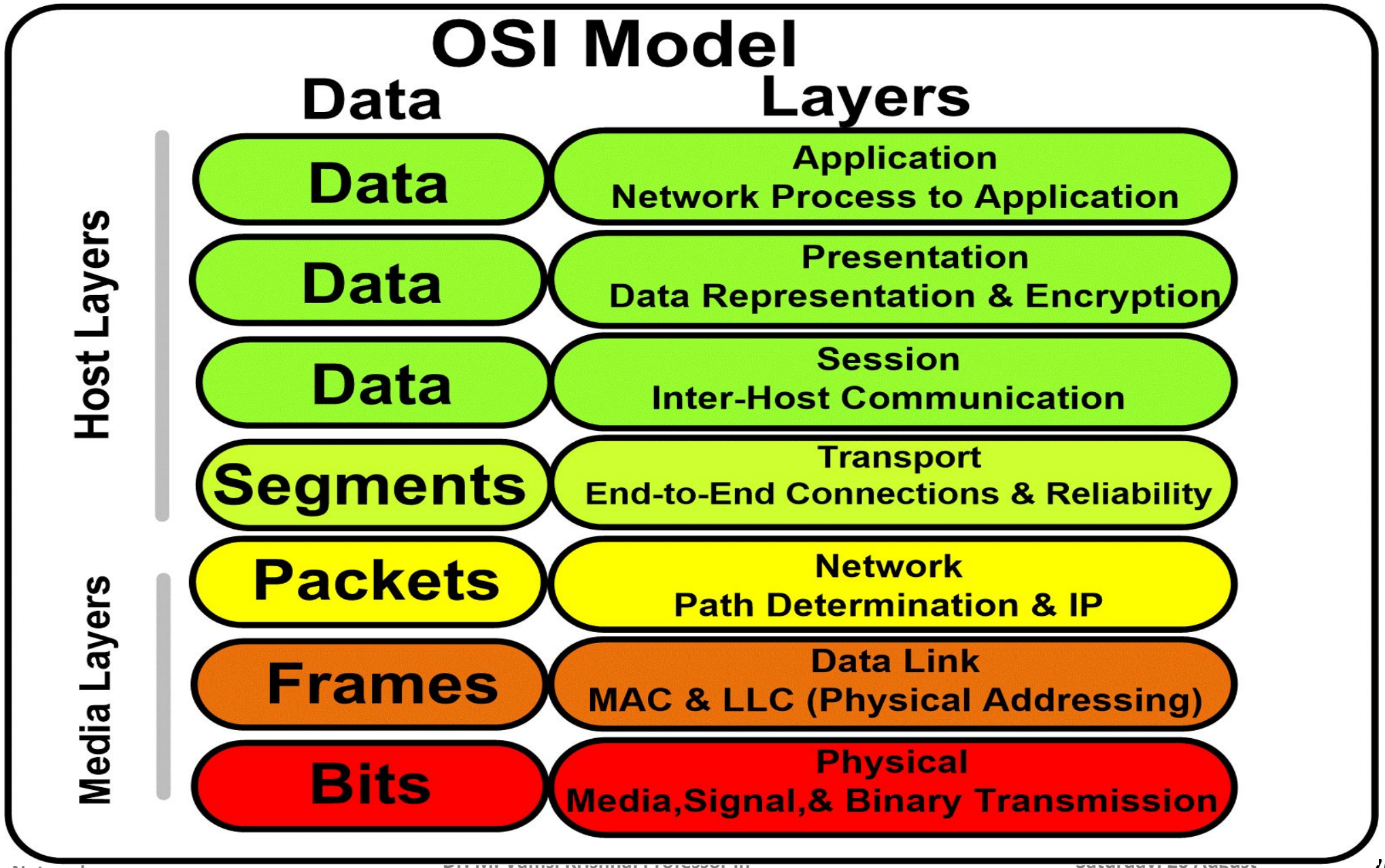
- ***0n the Way***:
- *The letter is then on its way to the recipient. On the way to the recipient's local post office, the letter may actually go through a central office. In addition, it may be transported by truck, train, airplane, boat, or a combination of these.*
- ***At the Receiver Site***
- ***Lower layer***. *The carrier transports the letter to the post office.*
- ***Middle layer***. *The letter is sorted and delivered to the recipient's mailbox.*
- ***Higher layer***. *The receiver picks up the letter, opens the envelope, and reads it.*

OSI Reference Model

- *The OSI model (minus the physical medium) is shown in Figure.*
- *This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983).*
- *It was revised in 1995 (Day, 1995).*
- *The model is called the ISO OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.*

- *The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:*

1. *A layer should be created where a different abstraction is needed.*
2. *Each layer should perform a well-defined function.*
3. *The function of each layer should be chosen with an eye toward defining internationally standardized protocols.*
4. *The layer boundaries should be chosen to minimize the information flow across the interfaces.*
5. *The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.*


OSI Model
Data
Layers
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation & Encryption
Data
Session
Inter-Host Communication
Segments
Transport
End-to-End Connections & Reliability
Packets
Network
Path Determination & IP
Frames
Data Link
MAC & LLC (Physical Addressing)
Bits
Physical
Media,Signal,& Binary Transmission

The Physical Layer

- *The physical layer is concerned with transmitting raw bits 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 bit, not as a 0 bit.*
- *Typical questions here are*
  - *what electrical signals should be used to represent a 1 and a 0*
  - *how many nanoseconds a bit lasts*
  - *whether transmission may proceed simultaneously in both directions*
  - *how the initial connection is established*
  - *how it is torn down when both sides are finished*
  - *how many pins the network connector has and what each pin is used for.*
- *These design issues largely deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium, which lies below the physical layer.*

The Data Link Layer

- *The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors.*
- *It does so by masking the real errors so the network layer does not see them.*
- *It accomplishes this task by having the sender break up the input data into data frames and transmit the frames sequentially.*
- *If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.*
- *Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data.*
- *Some traffic regulation mechanism may be needed to let the transmitter know when the receiver can accept more data.*
- *Broadcast networks have an additional issue in the data link layer: how to control access to the shared channel.*
- *A special sublayer of the data link layer, the medium access control sublayer, deals with this problem.*

The Network Layer

- *The network layer controls the operation of the subnet.*
- *A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are ‘‘wired into’’ the network and rarely changed, or more often they can be updated automatically to avoid failed components.*
- *If too many packets are present in the subnet at the same time, they will get in one another’s way, forming bottlenecks.*
- *Handling congestion is also a responsibility of the network layer, in conjunction with higher layers that adapt the load they place on the network. More generally, the quality of service provided (delay, transit time, jitter, etc.) is also a network layer issue.*
- *When a packet has to travel from one network to another to get to its destination, many problems can arise.*
  - *The addressing used by the second network may be different from that used by the first one.*
  - *The second one may not accept the packet at all because it is too large.*
  - *The protocols may differ, and so on.*
- *It is up to the network layer to overcome all these problems to allow heterogeneous networks to be interconnected.*
- *In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.*

The Transport Layer

- *The basic function of the transport layer is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.*
- *Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology over the course of time.*
- *The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network.*
- *The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.*
- *However, other possible kinds of transport service exist, such as the transporting of isolated messages with no guarantee about the order of delivery, and the broadcasting of messages to multiple destinations.*

Transport Layer contd…

- *The type of service is determined when the connection is established. (As an aside, an error-free channel is completely impossible to achieve; what people really mean by this term is that the error rate is low enough to ignore in practice.)*
- *The transport layer is a true end-to-end layer; it carries data all the way from the source to the destination. In other words, a program on the source machine carries on a conversation with a similar program on the destination machine, using the message headers and control messages.*
- *In the lower layers, each protocols is between a machine and its immediate neighbours, and not between the ultimate source and destination machines, which may be separated by many routers.*

The Session Layer

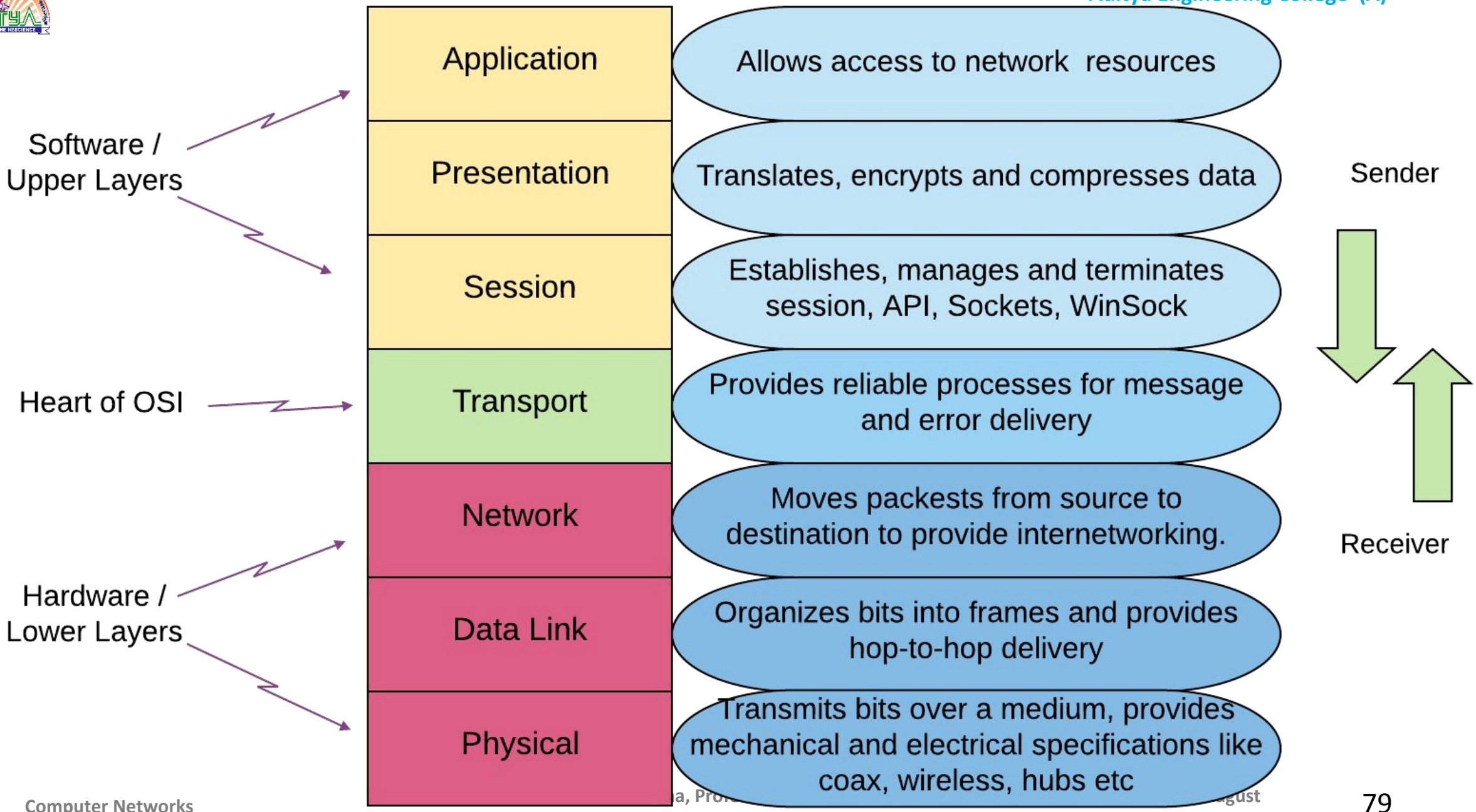
- *The session layer allows users on different machines to establish sessions between them.*
- *Sessions offer various services:*
  - *including dialog control (keeping track of whose turn it is to transmit).*
  - *token management (preventing two parties from attempting the same critical operation simultaneously).*
  - *synchronization (checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).*

The Presentation Layer

- *Unlike the lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted.*
- *In order to make it possible for computers with different internal data 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 presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records) to be defined and exchanged.*

The Application Layer

- *The application layer contains a variety of protocols that are commonly needed by users.*
- *One widely used application protocol is HTTP (HyperText Transfer Protocol), which is the basis for the World Wide Web.*
- *When a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back.*
- *Other application protocols are used for file transfer, electronic mail, and network news.*


Application
Presentation
Session
Transport
Network
Data Link
Physical
Allows access to network resources
Translates, encrypts and compresses data
Establishes, manages and terminates session, API, Sockets, WinSock
Provides reliable processes for message and error delivery
Moves packests from source to destination to provide internetworking.
Organizes bits into frames and provides hop-to-hop delivery
Transmits bits over a medium, provides mechanical and electrical specifications like coax, wireless, hubs etc
Software / Upper Layers
Heart of OSI
Hardware / Lower Layers
Sender
Receiver

The TCP/IP Reference Model

- *The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,*

1. *To connect multiple networks together so that they appear as a single network.*
2. *To survive after partial subnet hardware failures.*
3. *To provide a flexible architecture.*

- *Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,*

1. *Link Layer*
2. *Internet Layer*
3. *Transport Layer*
4. *Application Layer*

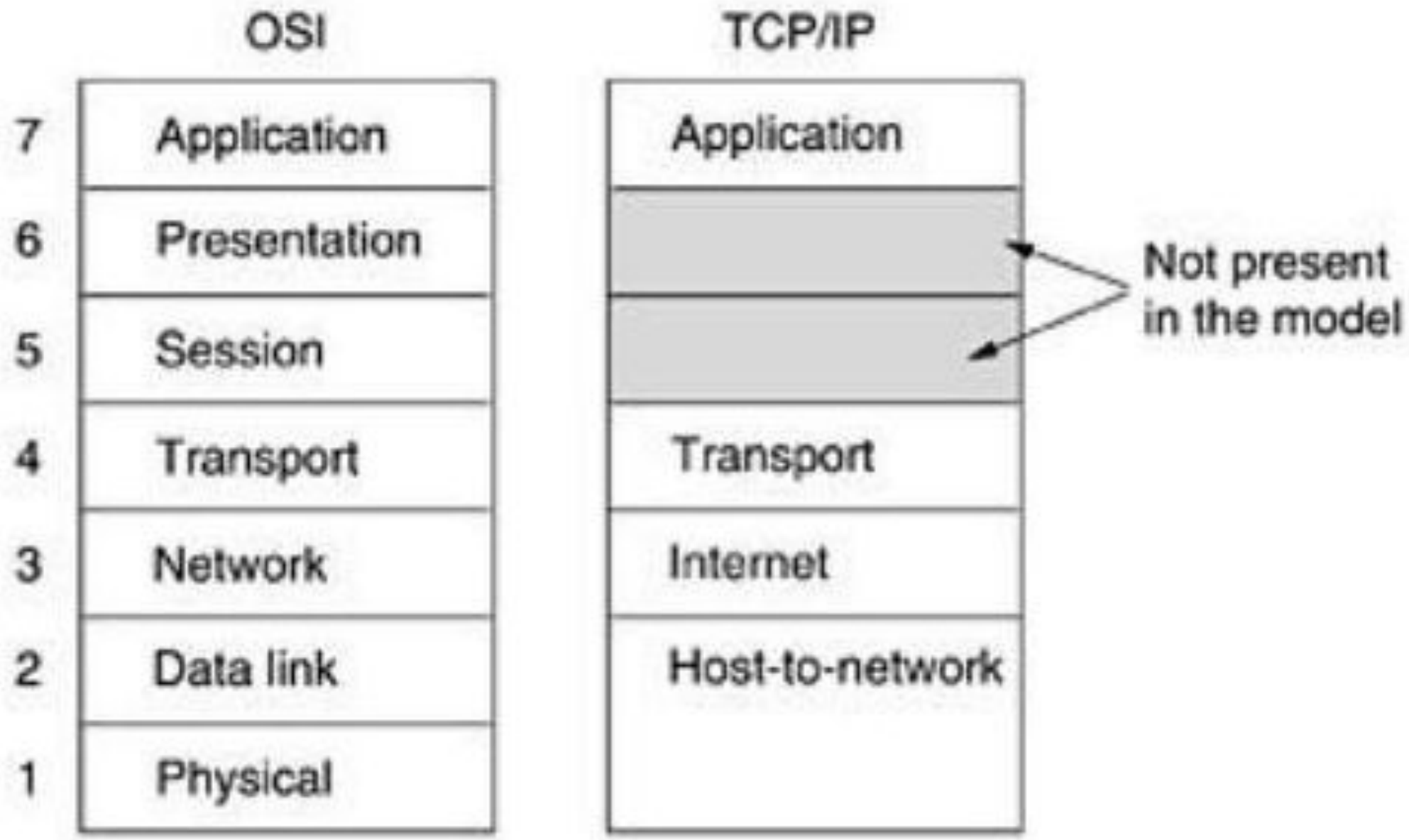
The Link Layer

- *The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer.*
- *It is not really a layer at all, in the normal sense of the term, but rather an interface between hosts and transmission links.*
- *The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it.*
- *This protocol is not defined and varies from host to host and network to network.*
- *Earlier, it is called as **Host – to – Network Layer**.*

The Internet Layer

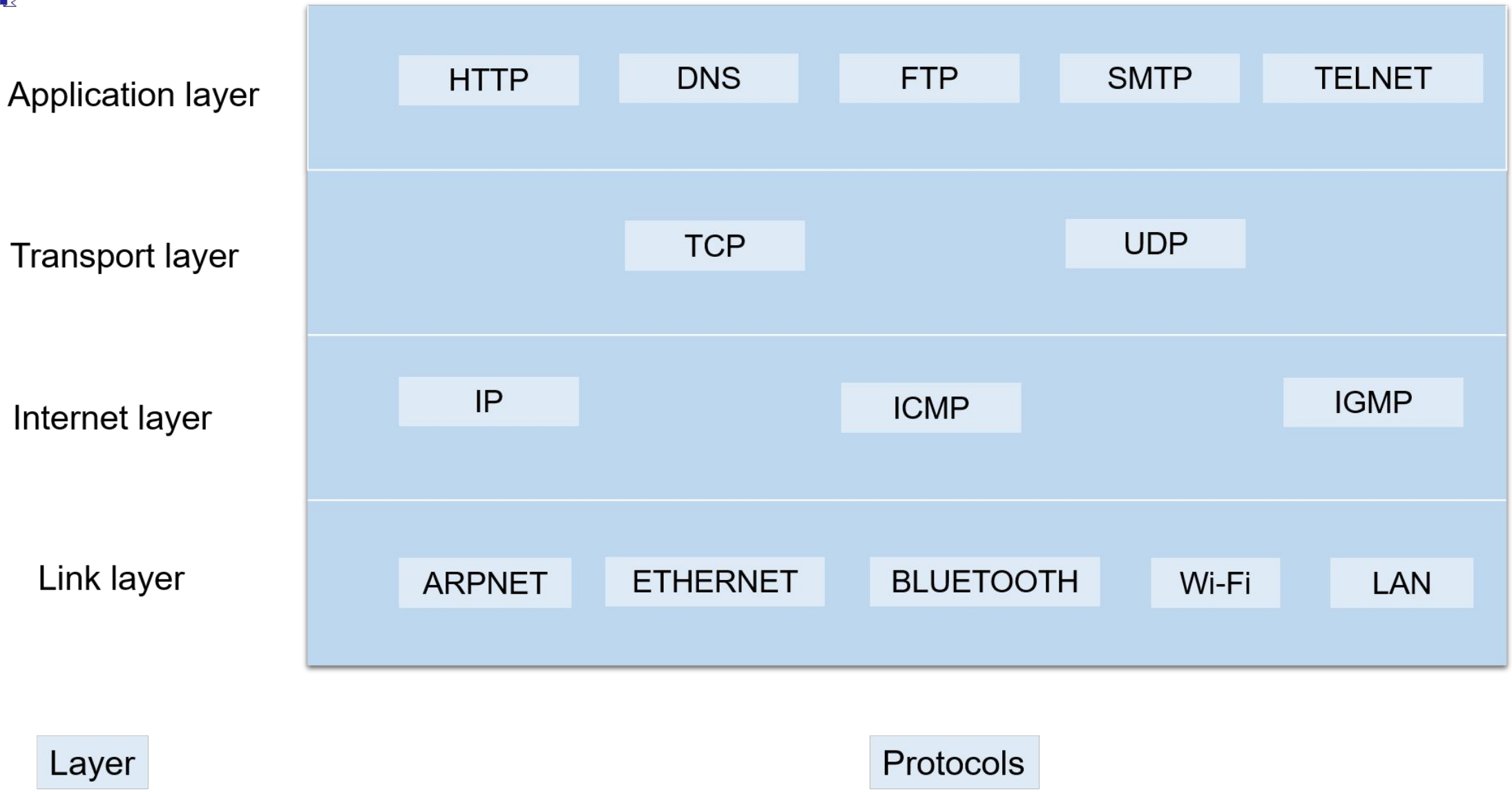
- *The internet layer is the linchpin that holds the whole architecture together.*
- *It is shown in Figure as corresponding roughly to the OSI network layer.*
- *Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network).*
- *They may even arrive in a completely different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.*
- *Note that ‘‘internet’’ is used here in a generic sense, even though this layer is present in the Internet.*

- *The analogy here is with the (snail) mail system.*
- *A person can drop a sequence of international letters into a mailbox in one country, and with a little luck, most of them will be delivered to the correct address in the destination country.*
- *The letters will probably travel through one or more international mail gateways along the way, but this is transparent to the users.*
- *Furthermore, that each country (i.e., each network) has its own stamps, preferred envelope sizes, and delivery rules is hidden from the users.*
- *The internet layer defines an official packet format and protocol called IP (Internet Protocol), plus a companion protocol called ICMP (Internet Control Message Protocol) that helps it function.*
- *The job of the internet layer is to deliver IP packets where they are supposed to go.*
- *Packet routing is clearly a major issue here, as is congestion (though IP has not proven effective at avoiding congestion).*


OSI
TCP/IP
7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical
Application
Transport
Internet
Host-to-network
Not present in the model

The Transport Layer

- *The layer above the internet layer in the TCP/IP model is called the transport layer.*
- *It is designed to allow peer entities on the source and destination hosts to carry on a conversation, just as in the OSI transport layer.*
- *Two end-to-end transport protocols have been defined here.*
  - *The first one, TCP (Transmission Control Protocol), is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. It segments the incoming byte stream into discrete messages and passes each one on to the internet layer.*
  - *At the destination, the receiving TCP process reassembles the received messages into the output stream.*
  - *TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.*
  - *The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.*
  - *It is also widely used for one-shot, client-server-type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video.*
- *The relation of IP, TCP, and UDP is shown in Figure. Since the model was developed, IP has been implemented on many other networks.*


Application layer
HTTP
DNS
FTP
SMTP
TELNET
Transport layer
TCP
UDP
Internet layer
IP
ICMP
IGMP
Link layer
ARPNET
ETHERNET
BLUETOOTH
Wi-Fi
LAN
Layer
Protocols

The Application Layer

- *The TCP/IP model does not have session or presentation layers.*
- *No need for them was perceived.*
- *Instead, applications simply include any session and presentation functions that they require.*
- *Experience with the OSI model has proven this view correct: these layers are of little use to most applications.*
- *On top of the transport layer is the application layer.*
- *It contains all the higher- level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).*
- *Many other protocols have been added to these over the years. Some important ones that we will study, include*
  - *The Domain Name System (DNS), for mapping host names onto their network addresses,*
  - *HTTP, the protocol for fetching pages on the World Wide Web,*
  - *RTP, the protocol for delivering real-time media such as voice or movies.*

Comparison of the OSI and TCP/IP Reference Models:

- *The OSI and TCP/IP reference models have much in common.*
- *Both are based on the concept of a stack of independent protocols.*
- *Also, the functionality of the layers is roughly similar.*
- *In both models, the layers above transport are application-oriented users of the transport service.*
- *Despite these fundamental similarities, the two models also have many differences Three concepts are central to the OSI model:*

1. *Services.*
2. *Interfaces.*
3. *Protocols.*

- *Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicit.*
- *Each layer performs some services for the layer above it.*
- *It defines the layer's semantics.*
- *A layer's interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, says nothing about how the layer works inside.*
- *Finally, the peer protocols used in a layer are the layer's own business.*
- *It can use any protocols it wants to, as long as it gets the job done (i.e., provides the offered services).*
- *It can also change them at will without affecting software in higher layers.*

- *The TCP/IP model did not originally clearly distinguish between service, interface, and protocol, although people have tried to retrofit it after the fact to make it more OSI-like.*
- *The protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.*
- *Being able to make such changes is one of the main purposes of having layered protocols in the first place.*
- *The OSI reference model was devised before the corresponding protocols were invented. This ordering means that the model was not biased toward one particular set of protocols, a fact that made it quite general.*
- *The downside of this ordering is that the designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.*

- *Another difference is in the area of connectionless versus connection-oriented communication.*
- *The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer, where it counts (because the transport service is visible to the users).*
- *The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer, giving the users a choice.*
- *This choice is especially important for simple request-response protocols.*

OSI vs TCP/IP Model

OSI(Open System Interconnection)	*TCP/IP(Transmission Control Protocol / Internet Protocol)*
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	*1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.*
2. In OSI model the transport layer guarantees the delivery of packets.	*2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.*
3. Follows vertical approach.	*3. Follows horizontal approach.*
4. OSI model has a separate Presentation layer and Session layer.	*4. TCP/IP does not have a separate Presentation layer or Session layer.*
5. Transport Layer is Connection Oriented.	*5. Transport Layer is both Connection Oriented and Connection less.*
6. Network Layer is both Connection Oriented and Connection less.	*6. Network Layer is Connection less.*
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	*7. TCP/IP model is, in a way implementation of the OSI model.*

OSI(Open System Interconnection)	*TCP/IP(Transmission Control Protocol / Internet Protocol)*
8. Network layer of OSI model provides both connection oriented	*8. The Network layer in TCP/IP model provides connectionless service.*
9. OSI model has a problem of fitting the protocols into the model.	*9. TCP/IP model does not fit any protocol*
10. Protocols are hidden in OSI model changes.	*10. In TCP/IP replacing protocol is not easy.*
11. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	*11. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.*
12. It has 7 layers	*12. It has 4 layers*

Network Models

TCP/IP MODEL	OSI MODEL	PROTOCOLS
Application Layer	Application Layer	FTP,HTTP,Telnet
	Presentation Layer	JPEG,MPEG
	Session Layer	NFS,SQL,PAP
Transport Layer	Transport Layer	TCP,UDP
Network Layer	Network Layer	IPv4,IPv6
Network Access Layer	Data Link Layer	ARP,CDP,STP
	Physical Layer	Ethernet,Wi-Fi

Lack of OSI Models Success

- *This can be summarized into four categories:*

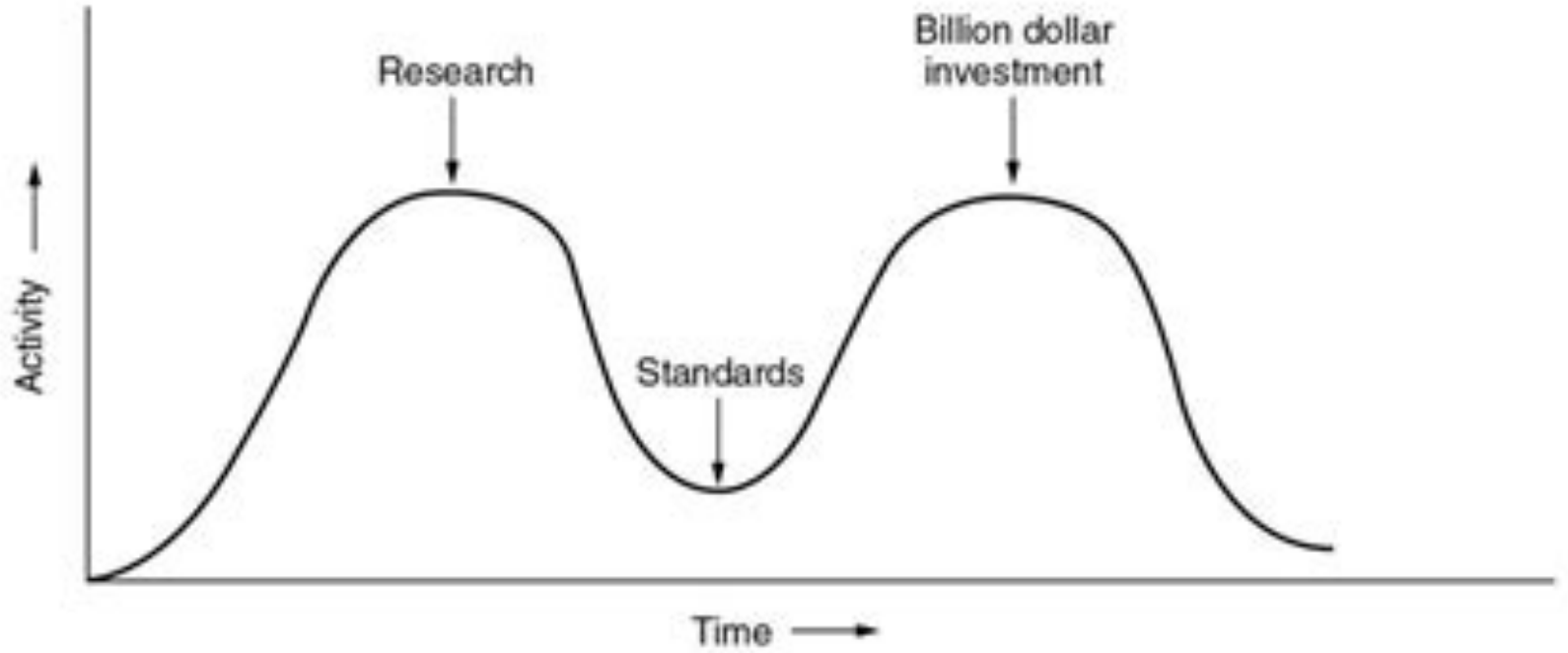
1. *Bad timing.*
2. *Bad technology.*
3. *Bad implementations.*
4. *Bad politics.*

Bad Timing

- *The time at which a standard is established is absolutely critical to its success.*
- *David Clark of M.I.T. has a theory of standards that he calls the apocalypse of the two elephants, which is illustrated in fig.*
- *This figure shows the amount of activity surrounding a new subject.*
- *When the subject is first discovered, there is a burst of research activity in the form of discussions, papers, and meetings.*
- *After a while this activity subsides, corporations discover the subject, and the billion-dollar wave of investment hits.*

- *It is essential that the standards be written in the trough in between the two ‘‘elephants.’’ If they are written too early (before the research results are well established), the subject may still be poorly understood; the result is a bad standard.*
- *If they are written too late, so many companies may have already made major investments in different ways of doing things that the standards are effectively ignored.*
- *If the interval between the two elephants is very short (because everyone is in a hurry to get started), the people developing the standards may get crushed.*
- *It now appears that the standard OSI protocols got crushed. The competing TCP/IP protocols were already in widespread use by research universities by the time the OSI protocols appeared.*
- *While the billion-dollar wave of investment had not yet hit, the academic market was large enough that many vendors had begun cautiously offering TCP/IP products.*
- *When OSI came around, they did not want to support a second protocol stack until they were forced to, so there were no initial offerings.*
- *With every company waiting for every other company to go first, no company went first and OSI never happened.*

Bad Timing



The apocalypse of the two elephants.

Bad Technology

- *The second reason that OSI never caught on is that both the model and the protocols are flawed.*
- *The choice of seven layers was more political than technical, and two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull.*
- *The OSI model, along with its associated service definitions and protocols, is extraordinarily complex. When piled up, the printed standards occupy a significant fraction of a meter of paper.*
- *They are also difficult to implement and inefficient in operation.*

- *In this context, a riddle posed by Paul Mockapetris and cited by Rose (1993):*
- *Q: What do you get when you cross a mobster with an international standard?*
- *A: Someone who makes you an offer you can't understand.*

- *In addition to being incomprehensible, another problem with OSI is that some functions, such as addressing, flow control, and error control, reappear again and again in each layer.*
- *Saltzer et al. (1984), for example, have pointed out that to be effective, error control must be done in the highest layer, so that repeating it over and over in each of the lower layers is often unnecessary and inefficient.*

Bad Implementation

- *Given the enormous complexity of the model and the protocols, it will come as no surprise that the initial implementations were huge, unwieldy, and slow.*
- *Everyone who tried them got burned.*
- *It did not take long for people to associate ‘‘OSI’’ with ‘‘poor quality.’’ Although the products improved in the course of time, the image stuck.*
- *In contrast, one of the first implementations of TCP/IP was part of Berkeley UNIX and was quite good (not to mention, free).*
- *People began using it quickly, which led to a large user community, which led to improvements, which led to an even larger community. Here the spiral was upward instead of downward.*

Bad Politics

- *On account of the initial implementation, many people, especially in academia, thought of TCP/IP as part of UNIX, and UNIX in the 1980s in academia was not unlike parenthood (then incorrectly called motherhood) and apple pie.*
- *OSI, on the other hand, was widely thought to be the creature of the European telecommunication ministries, the European Community, and later the U.S. Government.*
- *This belief was only partly true, but the very idea of a bunch of government bureaucrats trying to shove a technically inferior standard down the throats of the poor researchers and programmers down in the trenches actually developing computer networks did not aid OSI's cause.*
- *Some people viewed this development in the same light as IBM announcing in the 1960s that PL/I was the language of the future, or the DoD correcting this later by announcing that it was actually Ada.*

Internet History

- *The Internet is not a network at all, but a vast collection of different networks that use certain common protocols and provide certain common services.*
- *It is an unusual system in that it was not planned by anyone and is not controlled by anyone.*
- *To better understand it, let us start from the beginning and see how it has developed and why.*

ARPANET

- *The story begins in the late 1950s. At the height of the Cold War, the DoD wanted a command-and-control network that could survive a nuclear war.*
- *At that time, all military communications used the public telephone network, which was considered vulnerable.*
- *Around 1960, the DoD awarded a contract to the RAND Corporation to find a solution.*
- *One of its employees, Paul Baran, came up with the highly distributed and fault-tolerant design.*

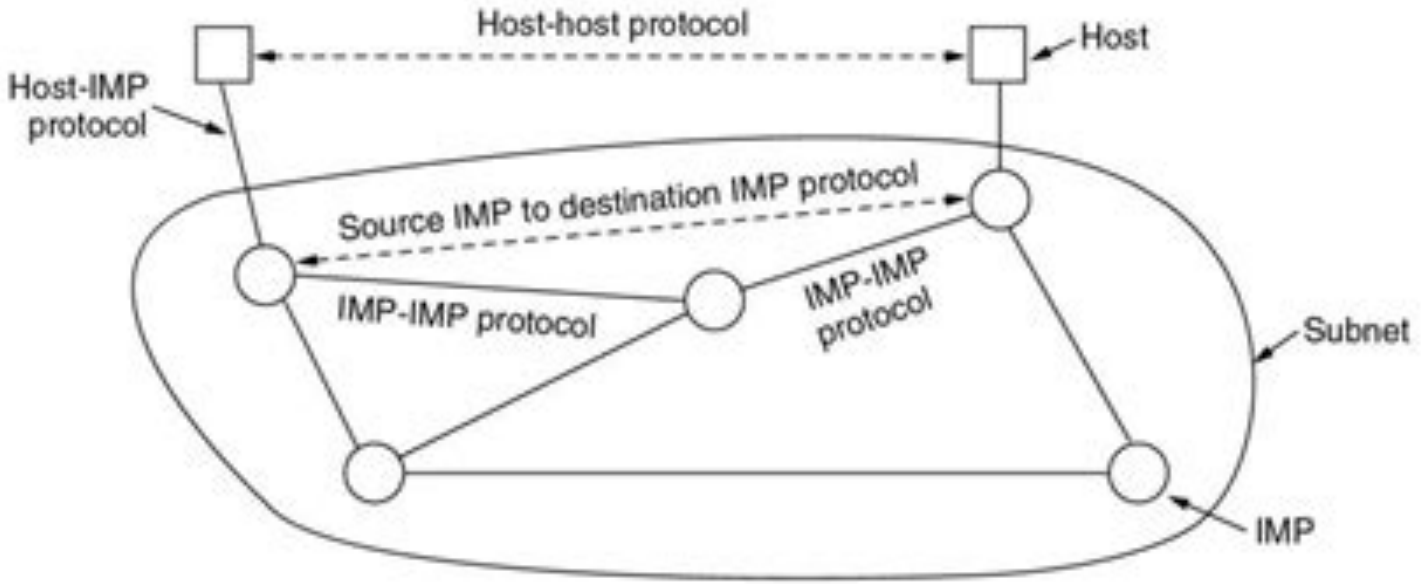
- *Baran wrote several reports for the DoD describing his ideas in detail.*
- *Officials at the Pentagon liked the concept and asked AT&T, then the U.S. national telephone monopoly, to build a prototype.*
- *AT&T dismissed Baran's ideas out of hand.*
- *The biggest and richest corporation in the world was not about to allow some young whippersnapper tell it how to build a telephone system. They said Baran's network could not be built and the idea was killed.*

- *For the first few years, ARPA tried to figure out what its mission should be, but in 1967, the attention of ARPA's then director, Larry Roberts, turned to networking.*
- *He contacted various experts to decide what to do. One of them, Wesley Clark, suggested building a packet-switched subnet, giving each host its own router.*
- *After some initial skepticism, Roberts bought the idea and presented a somewhat vague paper about it at the ACM SIGOPS Symposium on Operating System Principles held in Gatlinburg, Tennessee in late 1967 (Roberts, 1967).*
- *Much to Roberts' surprise, another paper at the conference described a similar system that had not only been designed but actually implemented under the direction of Donald Davies at the National Physical Laboratory in England.*

- *The NPL system was not a national system (it just connected several computers on the NPL campus), but it demonstrated that packet switching could be made to work.*
- *Furthermore, it cited Baran's now discarded earlier work.*
- *Roberts came away from Gatlinburg determined to build what later became known as the ARPANET.*
- *The subnet would consist of minicomputers called IMPs (Interface Message Processors) connected by 56-kbps transmission lines.*
- *For high reliability, each IMP would be connected to at least two other IMPs.*
- *The subnet was to be a datagram subnet, so if some lines and IMPs were destroyed, messages could be automatically rerouted along alternative paths.*

- *Each node of the network was to consist of an IMP and a host, in the same room, connected by a short wire.*
- *A host could send messages of up to 8063 bits to its IMP, which would then break these up into packets of at most 1008 bits and forward them independently toward the destination.*
- *Each packet was received in its entirety before being forwarded, so the subnet was the first electronic store and forward packet-switching network.*

The ARPANET (2)



The original ARPANET design.

- *The software was split into two parts: subnet and host.*
- *The subnet software consisted of the IMP end of the host-IMP connection, the IMP-IMP protocol, and a source IMP to destination IMP protocol designed to improve reliability.*
- *Outside the subnet, software was also needed, namely, the host end of the host-IMP connection, the host-host protocol, and the application software.*
- *It soon became clear that BBN was of the opinion that when it had accepted a message on a host-IMP wire and placed it on the host-IMP wire at the destination, its job was done.*

Physical Layer

- Introduction to Guided Media
  - Twisted-pair cable
  - Coaxial cable
  - Fiber optic cable
- unguided media
  - Wireless-Radio waves
  - Microwaves
  - infrared.

Physical Layer - Introduction

- *It defines the electrical, timing and other interfaces by which bits are sent as signals over channels.*
- *The physical layer is the foundation on which the network is built.*
- *The properties of different kinds of physical channels determine the performance (e.g., throughput, latency, and error rate)*

- *The purpose of the physical layer is to transport bits from one machine to another.*
- *Various physical media can be used for the actual transmission.*
- *Each one has its own niche in terms of bandwidth, delay, cost, and ease of installation and maintenance.*
- *Media are roughly grouped into guided media, such as copper wire and fiber optics, and unguided media, such as terrestrial wireless, satellite, and lasers through the air.*

Guided Media

- Magnetic Media
- Twisted Pair
- Coaxial Cable
- Power Lines
- Fiber Optics

Unguided Media

- Wireless Transmission
  - Electromagnetic Spectrum
  - Radio Transmission
  - Microwave Transmission
  - Infrared Transmission
  - Light Transmission

Magnetic Media

- *One of the most common ways to transport data from one computer to another is to write them onto magnetic tape or removable media (e.g., recordable DVDs), physically transport the tape or disks to the destination machine, and read them back in again.*
- *it is often more cost effective, especially for applications in which high bandwidth or cost per bit transported is the key factor.*

Twisted Pair

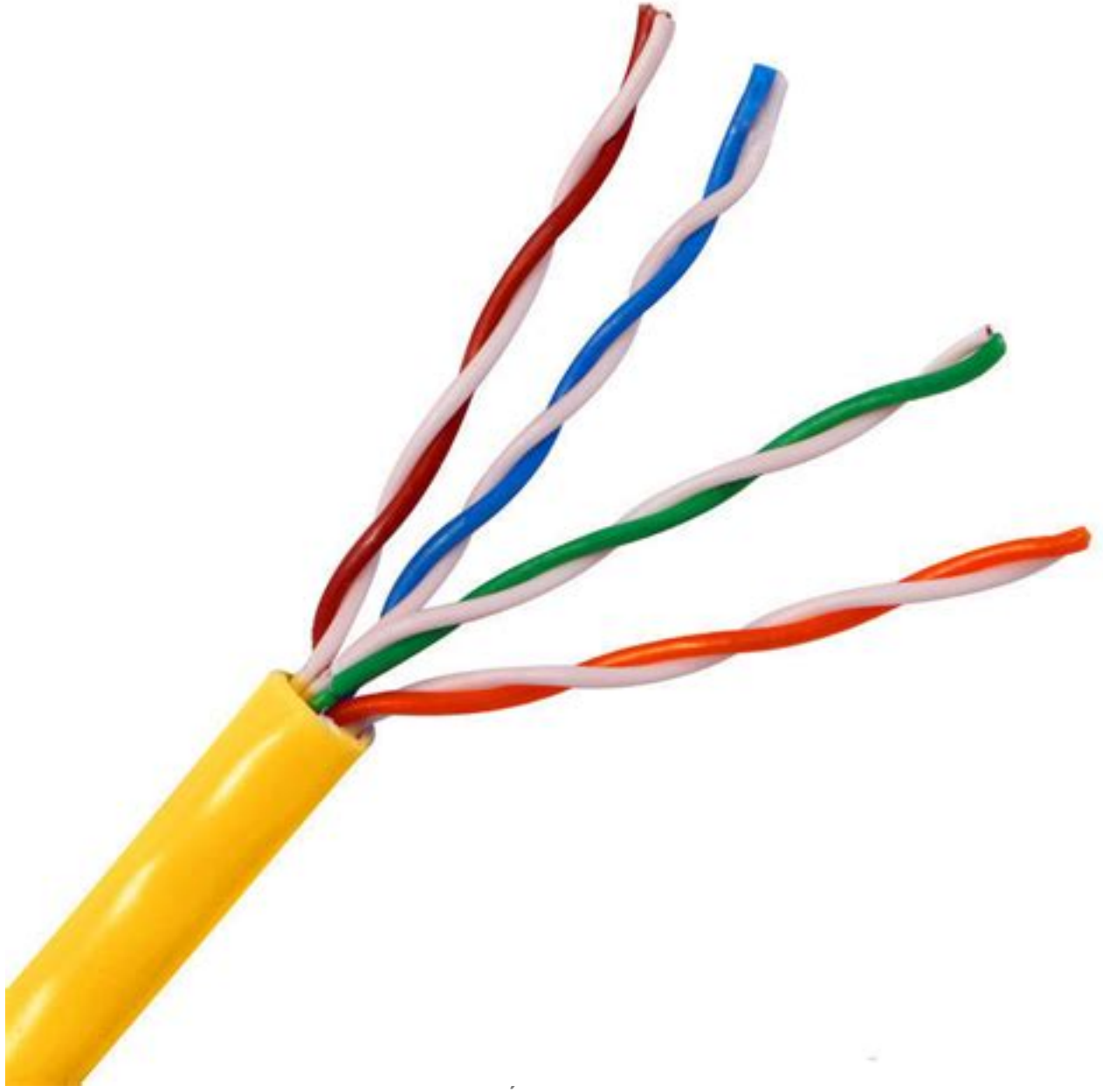
- *Although the bandwidth characteristics of magnetic tape are excellent, the delay characteristics are poor.*
- *Transmission time is measured in minutes or hours, not milliseconds.*
- *One of the oldest and still most common transmission media is twisted pair.*
- *A twisted pair consists of two insulated copper wires, typically about 1 mm thick.*
- *The wires are twisted together in a helical form, just like a DNA molecule. Twisting is done because two parallel wires constitute a fine antenna.*
- *When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively.*

- *A signal is usually carried as the difference in voltage between the two wires in the pair.*
- *This provides better immunity to external noise because the noise tends to affect both wires the same, leaving the differential unchanged.*
- *The most common application of the twisted pair is the telephone system.*

- *Twisted pairs can run several kilometers without amplification, but for longer distances the signal becomes too attenuated and repeaters are needed.*
- *When many twisted pairs run in parallel for a substantial distance, such as all the wires coming from an apartment building to the telephone company office, they are bundled together and encased in a protective sheath.*
- *The pairs in these bundles would interfere with one another if it were not for the twisting.*
- *In parts of the world where telephone lines run on poles above ground, it is common to see bundles several centimeters in diameter.*

- *Twisted pairs can be used for transmitting either analog or digital information.*
- *The bandwidth depends on the thickness of the wire and the distance traveled, but several megabits/sec can be achieved for a few kilometers in many cases.*
- *Due to their adequate performance and low cost, twisted pairs are widely used and are likely to remain so for years to come.*

- *Twisted-pair cabling comes in several varieties.*
- *The garden variety deployed in many office buildings is called Category 5 cabling, or ‘‘Cat 5.’’*
- *A category 5 twisted pair consists of two insulated wires gently twisted together.*
- *Four such pairs are typically grouped in a plastic sheath to protect the wires and keep them together.*



- *Different LAN standards may use the twisted pairs differently.*
- *For example, 100-Mbps Ethernet uses two (out of the four) pairs, one pair for each direction.*
- *To reach higher speeds, 1-Gbps Ethernet uses all four pairs in both directions simultaneously;*
- *this requires the receiver to factor out the signal that is transmitted locally*

- *Links that can be used in both directions at the same time, like a two-lane road, are called **full-duplex** links.*
- *In contrast, links that can be used in either direction, but only one way at a time, like a single-track railroad line are called **half-duplex** links.*
- *A third category consists of links that allow traffic in only one direction, like a one-way street. They are called **simplex** links.*

- *Cat 5 replaced earlier Category 3 cables with a similar cable that uses the same connector, but has more twists per meter.*
- *More twists result in less crosstalk and a better-quality signal over longer distances, making the cables more suitable for high-speed computer communication, especially 100-Mbps and 1-Gbps Ethernet LANs.*
- *New wiring is more likely to be Category 6 or even Category 7.*
- *These categories has more stringent specifications to handle signals with greater bandwidths.*
- *Some cables in Category 6 and above are rated for signals of 500 MHz and can support the 10-Gbps links that will soon be deployed.*

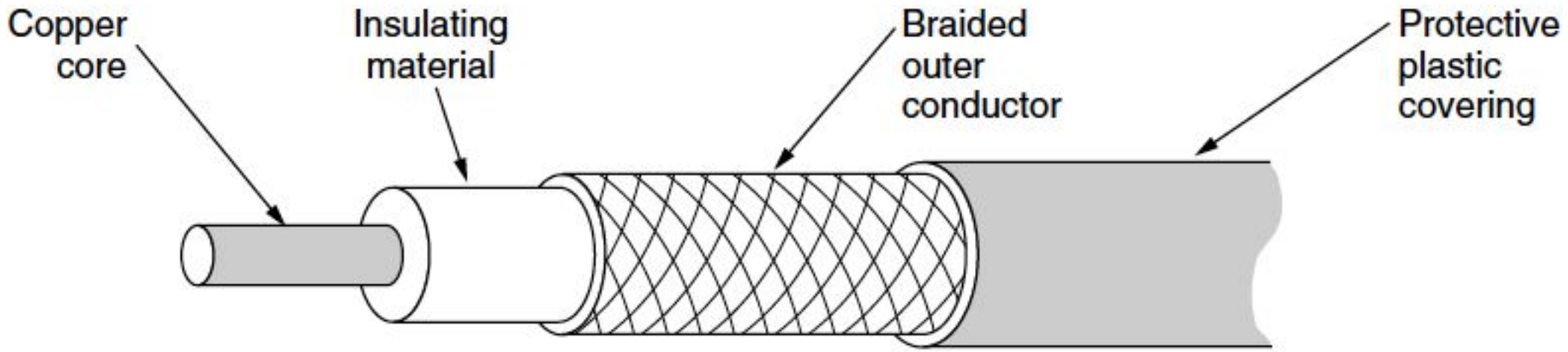
- *Through Category 6, these wiring types are referred to as UTP (Unshielded Twisted Pair) as they consist simply of wires and insulators.*
- *In contrast to these, Category 7 cables have shielding on the individual twisted pairs, as well as around the entire cable (but inside the plastic protective sheath).*
- *Shielding reduces the susceptibility to external interference and crosstalk with other nearby cables to meet demanding performance specifications.*
- *The cables are reminiscent of the high-quality.*

Coaxial Cable

- *Another common transmission medium is the coaxial cable (also known as just ‘‘coax’’ and pronounced ‘‘co-ax’’).*
- *It has better shielding and greater bandwidth than unshielded twisted pairs, so it can span longer distances at higher speeds.*

- *Two kinds of coaxial cable are widely used.*
- *One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start.*
- *The other kind, 75-ohm cable, is commonly used for analog transmission and cable television.*
- *This distinction is based on historical, rather than technical, factors (e.g., early dipole antennas had an impedance of 300 ohms, and it was easy to use existing 4:1 impedance-matching transformers).*
- *Starting in the mid-1990s, cable TV operators began to provide Internet access over cable which has made 75-ohm cable more important for data communication.*

- *A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material.*
- *The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh.*
- *The outer conductor is covered in a protective plastic sheath.*
- *A cutaway view of a coaxial cable is shown in Fig.*


Copper core
Insulating material
Braided outer conductor
Protective plastic covering

- *The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.*
- *The bandwidth possible depends on the cable quality and length.*
- *Modern cables have a bandwidth of up to a few GHz.*
- *Coaxial cables used to be widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics on longhaul routes.*
- *Coax is still widely used for cable television and metropolitan area networks.*

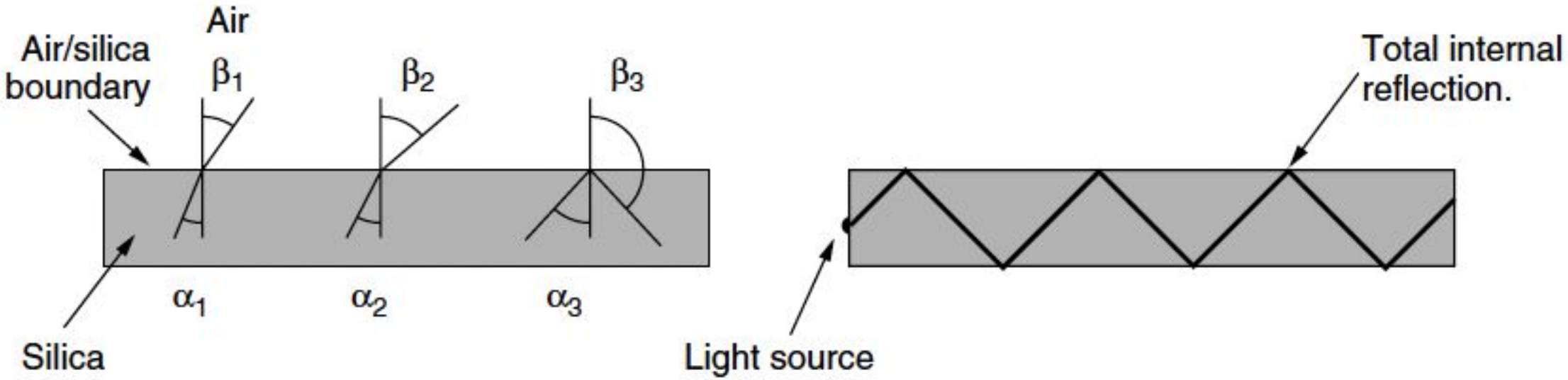
Fiber Optics

- *Many people in the computer industry take enormous pride in how fast computer technology is improving as it follows Moore's law, which predicts a doubling of the number of transistors per chip roughly every two years (Schaller, 1997).*
- *The original (1981) IBM PC ran at a clock speed of 4.77 MHz.*
- *Twenty Eight years later, PCs could run a four-core CPU at 3 GHz.*
- *This increase is a gain of a factor of around 2500, or 16 per decade.*

- *In the same period, wide area communication links went from 45 Mbps to 100 Gbps.*
- *This gain is similarly impressive, more than a factor of 2000 and close to 16 per decade, while at the same time the error rate went from 10^{-5} per bit to almost zero.*
- *Fiber optics are used for long-haul transmission in network backbones, highspeed LANs*
- *An optical transmission system has three key components: the light source, the transmission medium, and the detector.*

- *Conventionally, a pulse of light indicates a 1 bit and the absence of light indicates a 0 bit.*
- *The transmission medium is an ultra-thin fiber of glass.*
- *The detector generates an electrical pulse when light falls on it. By attaching a light source to one end of an optical fiber and a detector to the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.*

- *This transmission system would leak light and be useless in practice were it not for an interesting principle of physics.*
- *When a light ray passes from one medium to another—for example, from fused silica to air—the ray is refracted (bent) at the silica/air boundary, as shown in Fig*


Air
Air/silica boundary
β1
β2
β3
Total internal reflection.
α1
α2
α3
Silica
Light source

Transmission of Light Through Fiber

- *Optical fibers are made of glass, which, in turn, is made from sand, an inexpensive raw material available in unlimited amounts.*
- *Glassmaking was known to the ancient Egyptians, but their glass had to be no more than 1 mm thick or the light could not shine through.*
- *Glass transparent enough to be useful for windows was developed during the Renaissance.*
- *The glass used for modern optical fibers is so transparent that if the oceans were full of it instead of water, the seabed would be as visible from the surface as the ground is from an airplane on a clear day.*

- *The attenuation of light through glass depends on the wavelength of the light*
- *It is defined as the ratio of input to output signal power.*

Fiber Cables

- *Fiber optic cables are similar to coax, except without the braid.*
- *Figure shows a single fiber viewed from the side.*
- *At the center is the glass core through which the light propagates. In multimode fibers, the core is typically 50 microns in diameter, about the thickness of a human hair.*
- *In single-mode fibers, the core is 8 to 10 microns.*

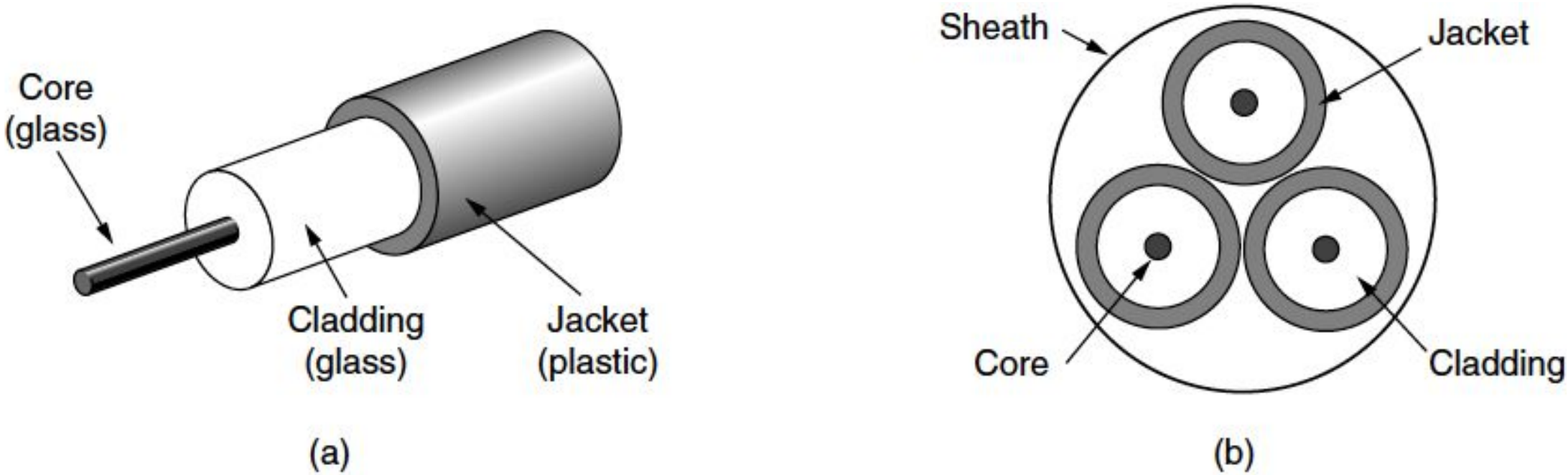


Figure 2-8. (a) Side view of a single fiber. (b) End view of a sheath with three fibers.

- *The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.*
- *Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath.*
- *Figure 2-8(b) shows a sheath with three fibers.*

- *Terrestrial fiber sheaths are normally laid in the ground within a meter of the surface, where they are occasionally subject to attacks by backhoes or gophers.*
- *Near the shore, transoceanic fiber sheaths are buried in trenches by a kind of seaplow.*
- *In deep water, they just lie on the bottom, where they can be snagged by fishing trawlers or attacked by giant squid.*

- *Fibers can be connected in three different ways.*
- *First, they can terminate in connectors and be plugged into fiber sockets. Connectors lose about 10 to 20% of the light, but they make it easy to reconfigure systems.*
- *Second, they can be spliced mechanically. Mechanical splices just lay the two carefully cut ends next to each other in a special sleeve and clamp them in place. Alignment can be improved by passing light through the junction and then making small adjustments to maximize the signal.*
- *Mechanical splices take trained personnel about 5 minutes and result in a 10% light loss.*

- *Third, two pieces of fiber can be fused (melted) to form a solid connection.*
- *A fusion splice is almost as good as a single drawn fiber, but even here, a small amount of attenuation occurs*
- *For all three kinds of splices, reflections can occur at the point of the splice, and the reflected energy can interfere with the signal.*
- *Two kinds of light sources are typically used to do the signaling.*
- *These are LEDs (Light Emitting Diodes) and semiconductor lasers.*

Item	LED	Semiconductor laser
Data rate	Low	High
Mode	Multimode	Multimode or single mode
Distance	Short	Long
Lifetime	Long life	Short life
Temperature sensitivity	Minor	Substantial
Cost	Low cost	Expensive

Wireless Transmission

- *Our age has given rise to information junkies: people who need to be online all the time.*
- *For these mobile users, twisted pair, coax, and fiber optics are of no use.*
- *They need to get their ‘‘hits’’ of data for their laptop, notebook, shirt pocket, palmtop, or wristwatch computers without being tethered to the terrestrial communication infrastructure.*
- *For these users, wireless communication is the answer.*
- *Wireless has advantages for even fixed devices in some circumstances.*
- *For example, if running a fiber to a building is difficult due to the terrain (mountains, jungles, swamps, etc.), wireless may be better.*
- *It is noteworthy that modern wireless digital communication began in the Hawaiian Islands, where large chunks of Pacific Ocean separated the users from their computer center and the telephone system was inadequate.*

Radio Transmission

- *Radio frequency (RF) waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.*
- *Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.*
- *Sometimes omnidirectional radio is good, but sometimes it is bad.*

- *The properties of radio waves are frequency dependent.*
- *At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source—at least as fast as $1/r^2$ in air—as the signal energy is spread more thinly over a larger surface.*
- *This attenuation is called **path loss**.*
- *At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles.*
- *Path loss still reduces power, though the received signal can depend strongly on reflections as well.*
- *High-frequency radio waves are also absorbed by rain and other obstacles to a larger extent than are low-frequency ones.*
- *At all frequencies, radio waves are subject to interference from motors and other electrical equipment.*

- *It is interesting to compare the attenuation of radio waves to that of signals in guided media.*
- *With fiber, coax and twisted pair, the signal drops by the same fraction per unit distance, for example 20 dB per 100m for twisted pair.*
- *With radio, the signal drops by the same fraction as the distance doubles, for example 6 dB per doubling in free space.*
- *This behavior means that radio waves can travel long distances, and interference between users is a problem.*

- *In the VLF, LF, and MF bands, radio waves follow the ground, as illustrated in Fig. 2-12(a).*
- *These waves can be detected for perhaps 1000 km at the lower frequencies, less at the higher ones.*
- *AM radio broadcasting uses the MF band.*
- *Radio waves in these bands pass through buildings easily, which is why portable radios work indoors.*
- *The main problem with using these bands for data communication is their low bandwidth*

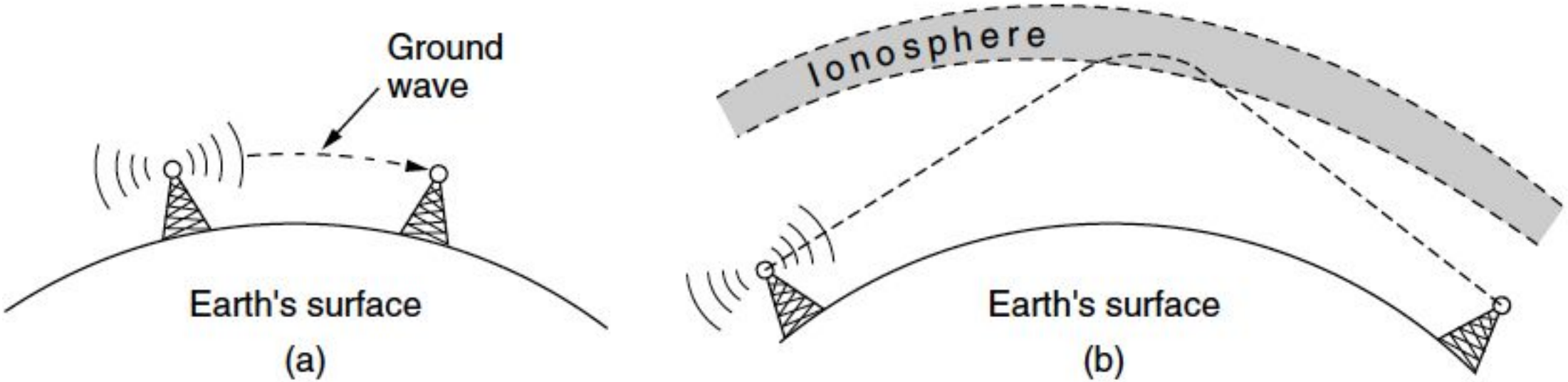


Figure 2-12. (a) In the VLF, LF, and MF bands, radio waves follow the curvature of the earth. (b) In the HF band, they bounce off the ionosphere.

- *In the HF and VHF bands, the ground waves tend to be absorbed by the earth.*
- *However, the waves that reach the ionosphere, a layer of charged particles circling the earth at a height of 100 to 500 km, are refracted by it and sent back to earth, as shown in Fig. 2-12(b).*
- *Under certain atmospheric conditions, the signals can bounce several times.*
- *Amateur radio operators (hams) use these bands to talk long distance.*
- *The military also communicate in the HF and VHF bands.*

Microwave Transmission

- *Above 100 MHz, the waves travel in nearly straight lines and can therefore be narrowly focused.*
- *Concentrating all the energy into a small beam by means of a parabolic antenna (like the familiar satellite TV dish) gives a much higher signal to-noise ratio, but the transmitting and receiving antennas must be accurately aligned with each other.*
- *In addition, this directionality allows multiple transmitters lined up in a row to communicate with multiple receivers in a row without interference, provided some minimum spacing rules are observed.*
- *Before fiber optics, for decades these microwaves formed the heart of the long-distance telephone transmission system.*

- *Microwaves travel in a straight line, so if the towers are too far apart, the earth will get in the way.*
- *Thus, repeaters are needed periodically.*
- *The higher the towers are, the farther apart they can be.*
- *The distance between repeaters goes up very roughly with the square root of the tower height.*
- *For 100-meter-high towers, repeaters can be 80 km apart.*

- *Unlike radio waves at lower frequencies, microwaves do not pass through buildings well.*
- *In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space.*
- *Some waves may be refracted off low-lying atmospheric layers and may take slightly longer to arrive than the direct waves.*
- *The delayed waves may arrive out of phase with the direct wave and thus cancel the signal.*
- *This effect is called **multipath fading** and is often a serious problem. It is weather and frequency dependent.*
- *Some operators keep 10% of their channels idle as spares to switch on when multipath fading temporarily wipes out some frequency band.*

- *microwave communication is so widely used for long-distance telephone communication, mobile phones, television distribution, and other purposes that a severe shortage of spectrum has developed.*
- *It has several key advantages over fiber.*
- *The main one is that no right of way is needed to lay down cables.*
- *By buying a small plot of ground every 50 km and putting a microwave tower on it, one can bypass the telephone system entirely.*
- *Microwave is also relatively inexpensive. So, putting up two simple towers (which can be just big poles with four guy wires) and putting antennas on each one may be cheaper*

Infrared Transmission

- *Unguided infrared waves are widely used for short-range communication.*
- *The remote controls used for televisions, VCRs, and stereos all use infrared communication.*
- *They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects.*
- *In general, as we go from long-wave radio toward visible light, the waves behave more and more like light and less and less like radio.*

- *On the other hand, the fact that infrared waves do not pass through solid walls well is also a plus.*
- *It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings: you cannot control your neighbor's television with your remote control.*
- *Furthermore, security of infrared systems against eavesdropping is better than that of radio systems precisely for this reason.*
- *Therefore, no government license is needed to operate an infrared system, in contrast to radio systems, which must be licensed outside the ISM bands.*
- *Infrared communication has a limited use on the desktop, for example, to connect notebook computers and printers with the IrDA (Infrared Data Association) standard, but it is not a major player in the communication game.*