Unit-1

Introduction to Data Communication and Network Models

Lecture Slides by Behrouz A Forouzon,

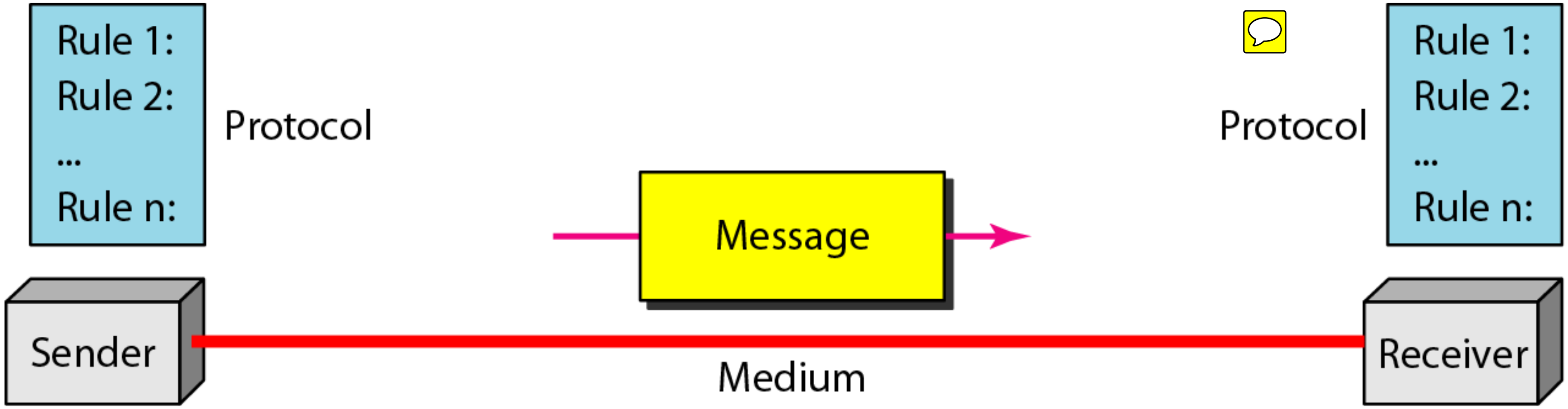
Tata McGraw Hill Publishing

Recompiled by : Aniruddhsinh Parmar

1-1 DATA COMMUNICATIONS

- The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.
- Means of sending or receiving information, such as telephone lines or computers.

Five components of data communication



Fundamental Characteristics of Data Communication

- Effectiveness of a data communication depends on four fundamental characteristics
  - **Delivery**: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
  - **Accuracy**: The system must deliver data accurately.
  - **Timeliness**: The system must deliver data in a timely manner.
    - Real time transmission: Transmitting data as they are produced, in the same order that they are produced and without significant delay.
  - **Jitter**: Jitter refers to the variation in the packet arrival time.

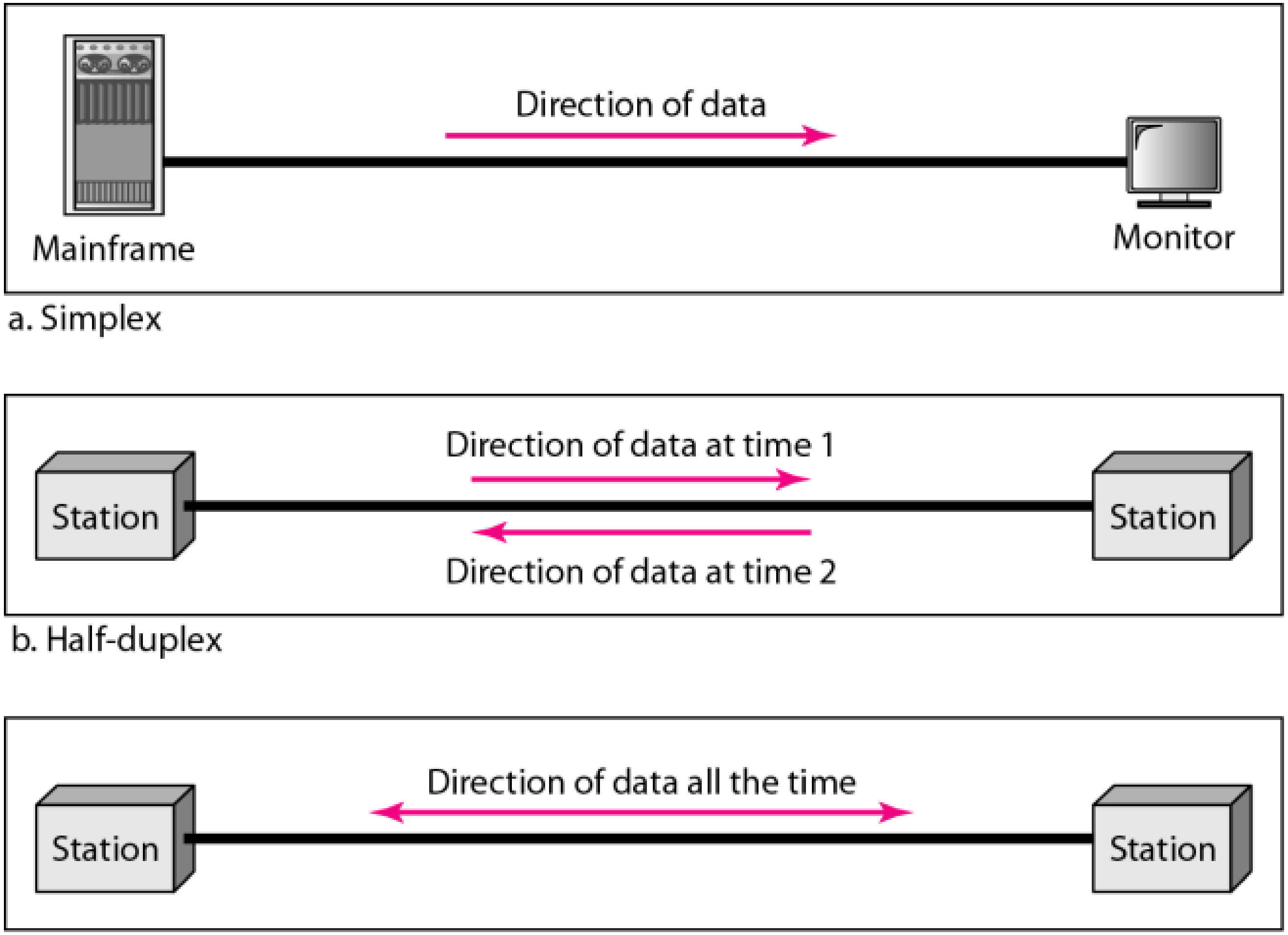
Data Representation in Communication

- Text: It is represented as a bit pattern, a sequence of bits. Different sets of bit pattern have been designed to represent symbols. Ex. ASCII, Unicode
- Numbers: The number is directly converted to a binary number to simplify mathematical operations.
- Images: Each pixel is assigned a bit pattern. The size and the value of the pattern depends on the image.
  - Black white Image : 1 bit pattern
  - To include gray scale: 2 bit pattern
  - Color Images: RGB or YCM
- Audio: Audio refers to the recording or broadcasting of sound or music. It is represented as continuous signal.
- Video: Video refers to the recording of a picture or movie. It can either be produced as continuous entity or it can be combination of images arranged to convey the idea of motion.

Data Flow in Communication

- Simplex : In this mode transmission is possible only in one direction.
- Half-Duplex: In this mode transmission is possible in both direction but not at the same time. Ex. Walkie Talkie
- Full Duplex: In this mode transmission is possible in both direction at the same time. Ex. Telephone, Mobile

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


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

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.

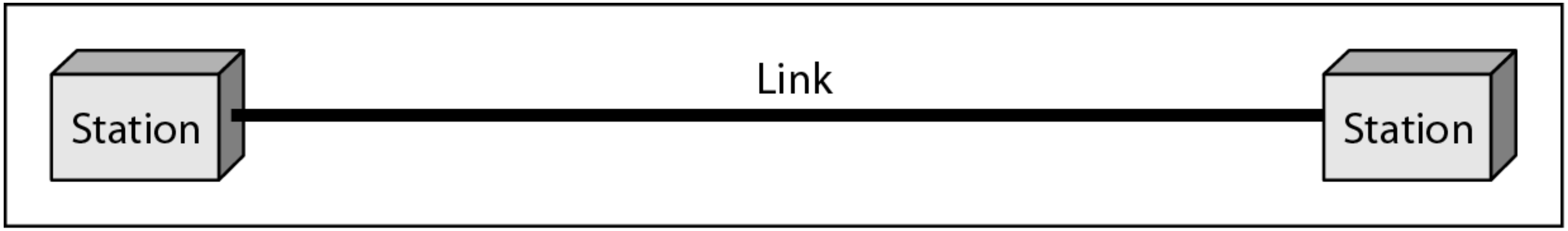
- Which are the different measures to check the efficiency of the network?

Network Measure

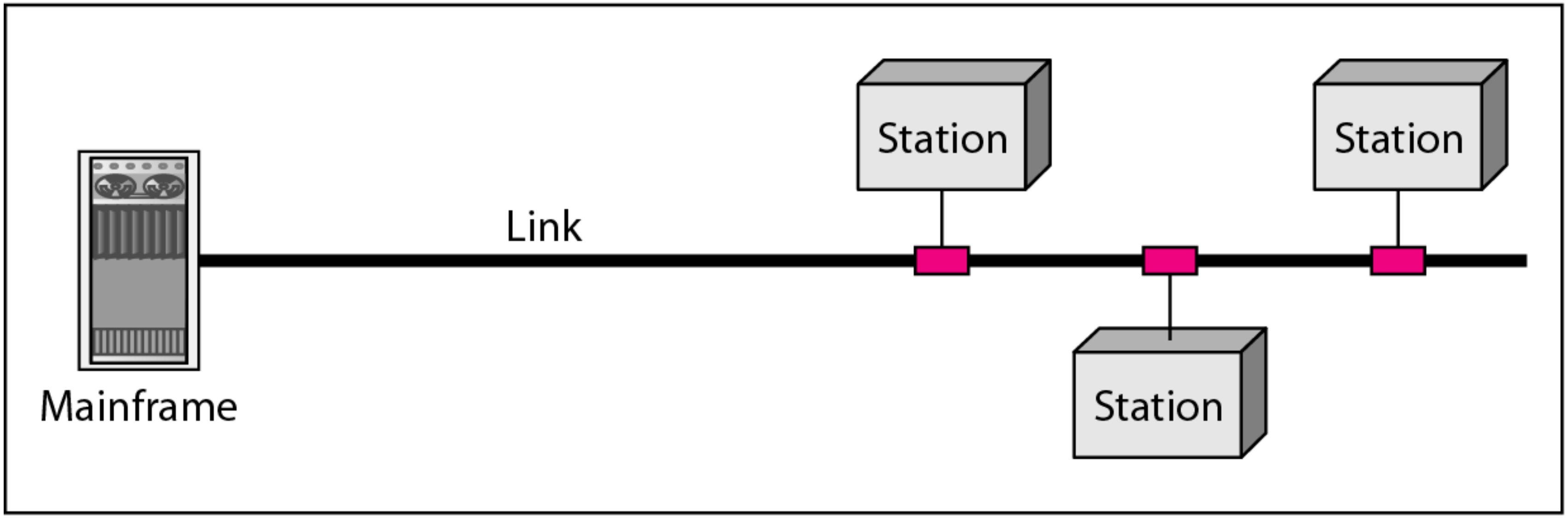
- Network criteria: a network must be able to meet a certain number of criteria
  - **Performance** can be measured in many ways, including transit time and response time
    - **Transit Time**: It is the amount of time required for a message to travel from one device to another.
    - **Response Time**: It is the elapsed time between an inquiry and a response.
  - **Performance of a network depends on number of factors**
    - Number of users
    - Type of transmission medium
    - Capabilities of the connected hardware
    - Efficiency of the software
  - **Performance is often evaluated by two networking metrics**
    - Throughput is an actual measurement of how fast we can send data.
    - Latency (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

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

Types of Connections

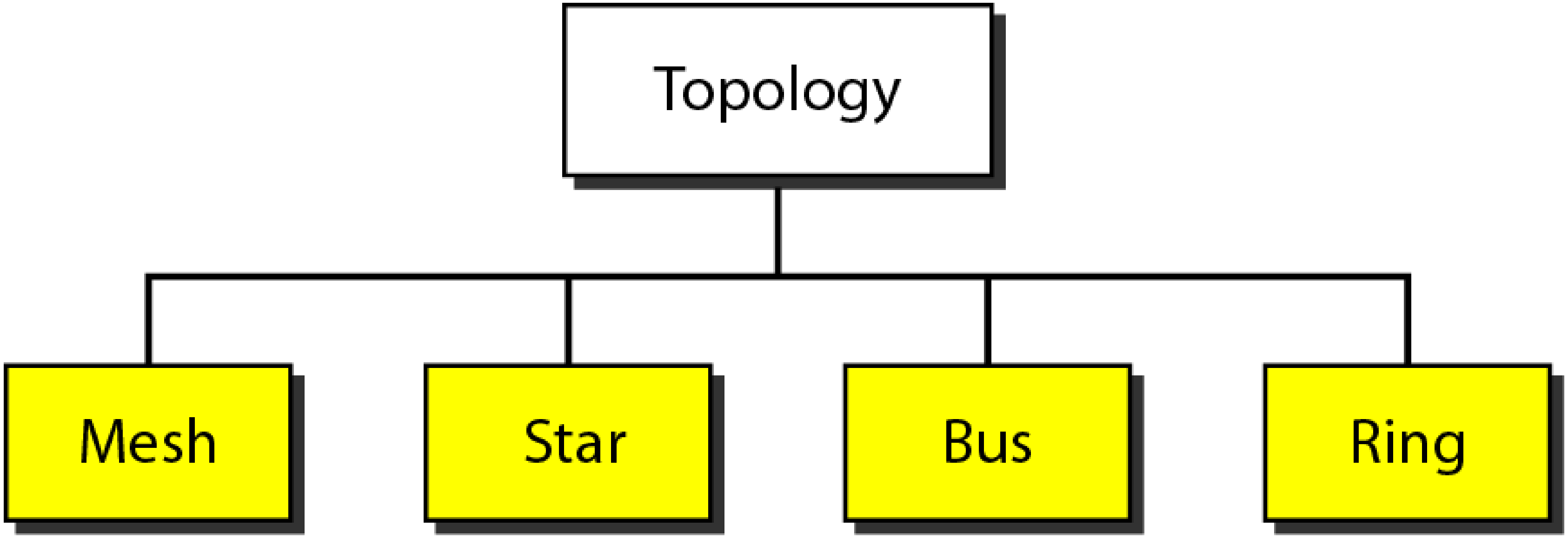


a. Point-to-point



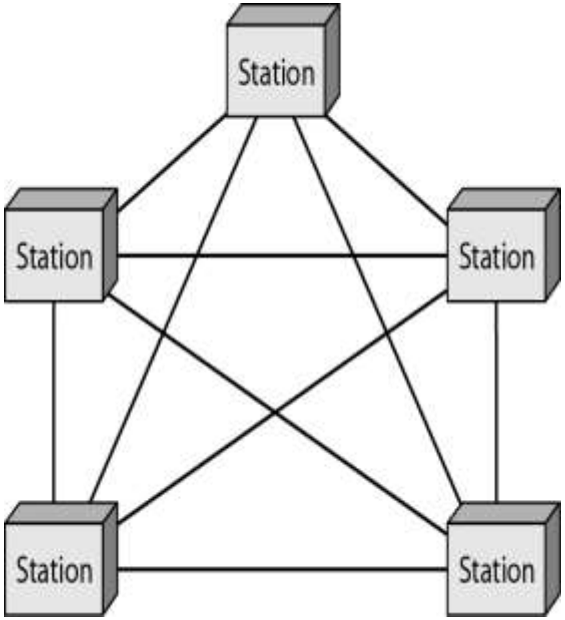
b. Multipoint

Categories of Topology



Topology : Physical Representation of all the available devices in any network

Mesh Topology



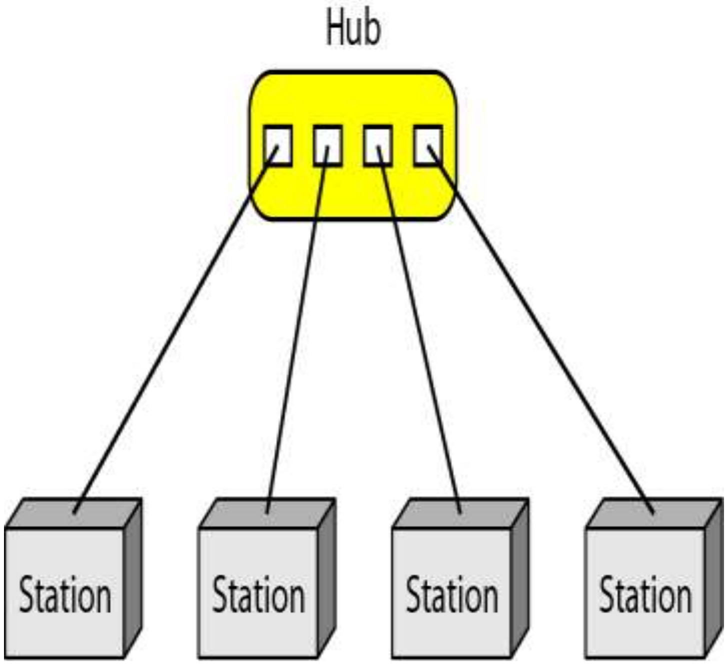
Advantages:

- Very Fast
- Very Secure
- Easy Fault Identification and Isolation

Disadvantages:

- Very Costly
- Installation and modification is time consuming

Star Topology



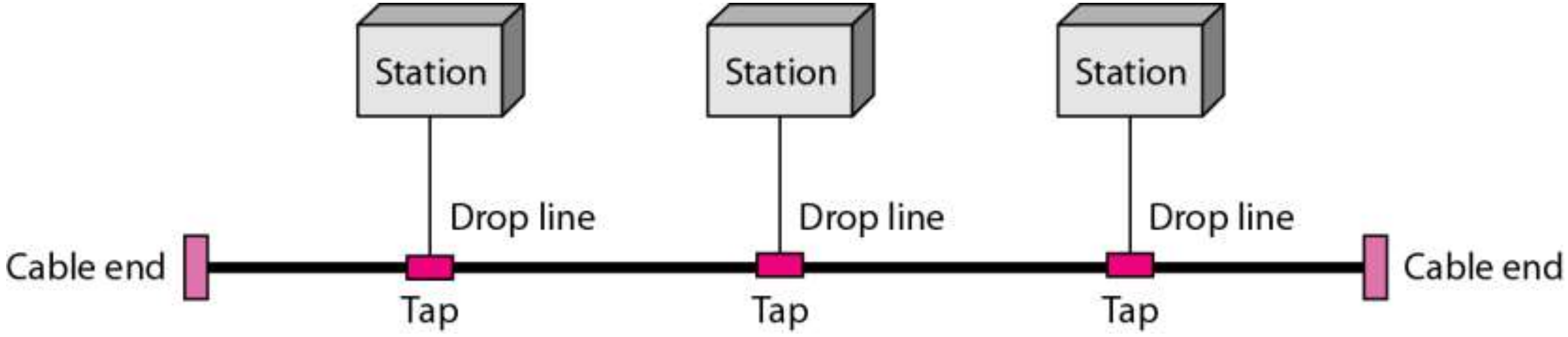
Advantages:

- Cheaper compare to Mesh Topology
- Easy Fault Identification and Isolation

Disadvantages:

- Single point of Failure
- Data communication is time consuming
- Installation and modification is difficult
- Less secure compare to Mesh Topology

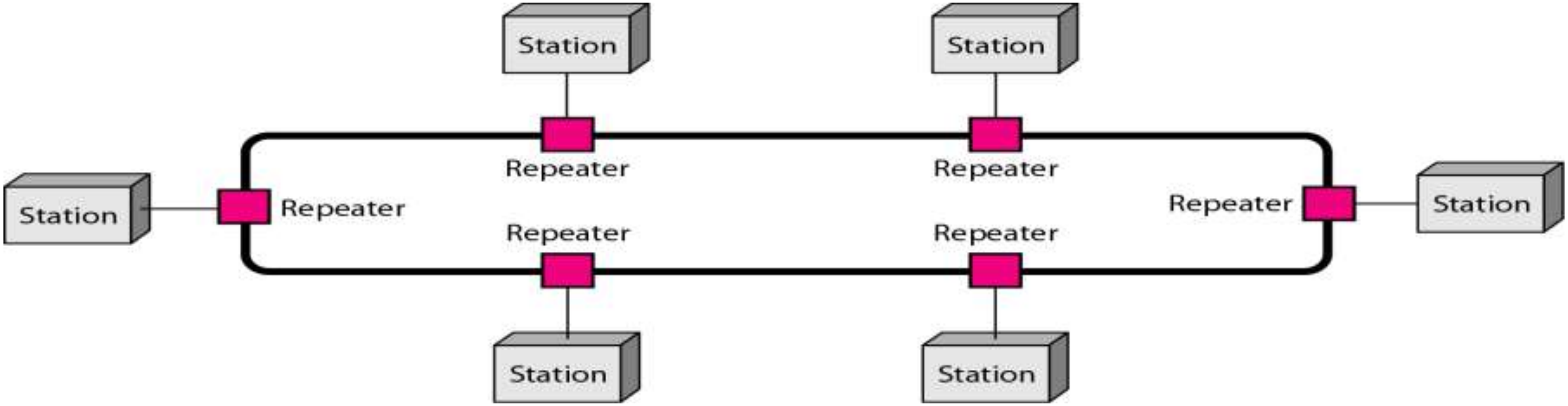
Bus Topology



Advantages:
- Cheaper compare to Mesh and Star Topology
- Installation and modification is easy in small network

Disadvantages:
- Fault Identification is difficult
- There is a limit on central cable length and number of nodes that can be connected
- If main cable is not working than communication is not possible
- Data communication is time consuming
- Less secure compare to Mesh Topology

Ring Topology

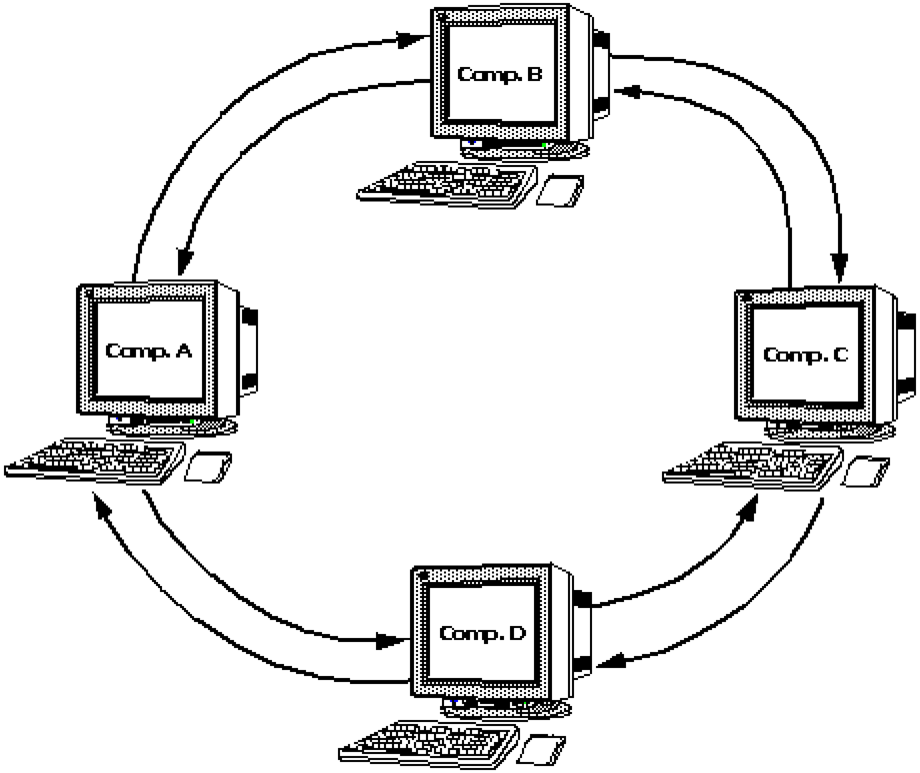


Advantages:

- Cheaper compare to Mesh and Star Topology
- Most used topology

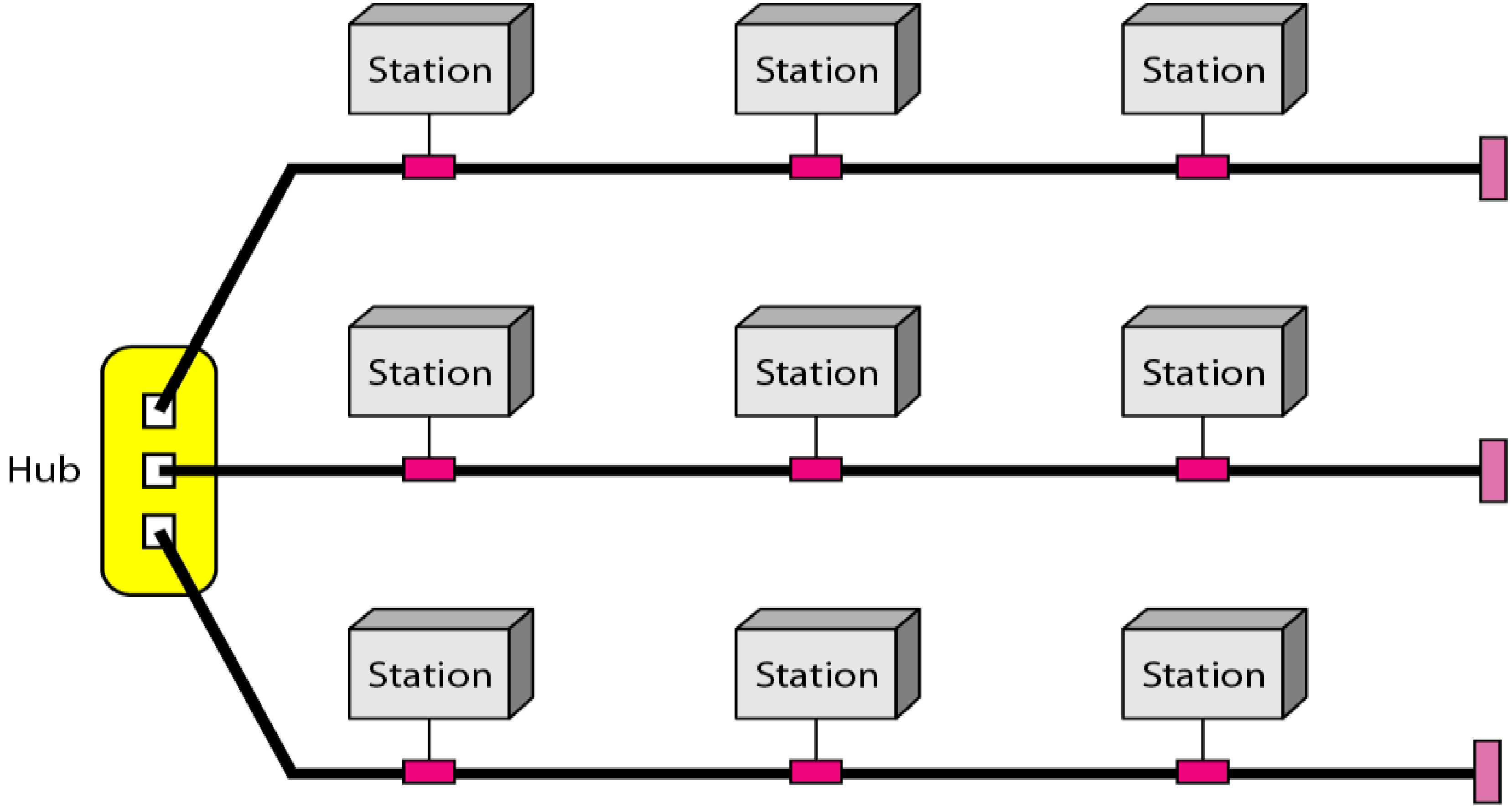
Disadvantages:

- Unidirectional communication
- Requirement of additional hardware device to enhance the signal quality
- Data communication is time consuming
- Less secure compare to Mesh Topology



To overcome the problem of unidirectional communication, double ring was introduce.

Hybrid Topology



Types of Networks

- LAN : Local Area Network
- MAN : Metropolitan Area Network
- WAN : Wide Area Network
- VPN : Virtual Private Network
- Intranet
- Extranet
- Internet

Local area network

- A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node.
- The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines.

Metropolitan area network

- A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

Wide area network

- A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

VPN (Virtual Private Network)

- It provides both secure and cost-effective networking
- Decrease telecommunication budgets and increase the number of services available to the user community.
- It uses technology known as private tunneling
- Privacy is created through the symmetrical encryption of the network traffic
- Two modes
  - Transport mode: transport mode uses encryption on the data part of the packet only. In transport mode the original packet headers are left encrypted.
  - Tunnel mode: in tunnel mode everything gets encrypted (headers and information sections of the packet). Because the original headers are encrypted, the entire packet needs to be encapsulated in a new packet.

Protocols and Standards

Protocol is synonymous with rule.
Standards, which are agreed-upon rules.

- **Protocols**
  - A protocol is a set of rules that govern data communication. A protocol defines what is communicated, how it is communicated and when it is communicated.
  - **Key elements of a protocol are syntax, semantics and timing**
    - **Syntax:** The term syntax refers to the structure or format of the data, meaning the order in which they are presented. Ex. First eight bits for sender's address and last eight bits for receiver's address.
    - **Semantics**: The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on the interpretation.
    - **Timing**: The timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 10 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

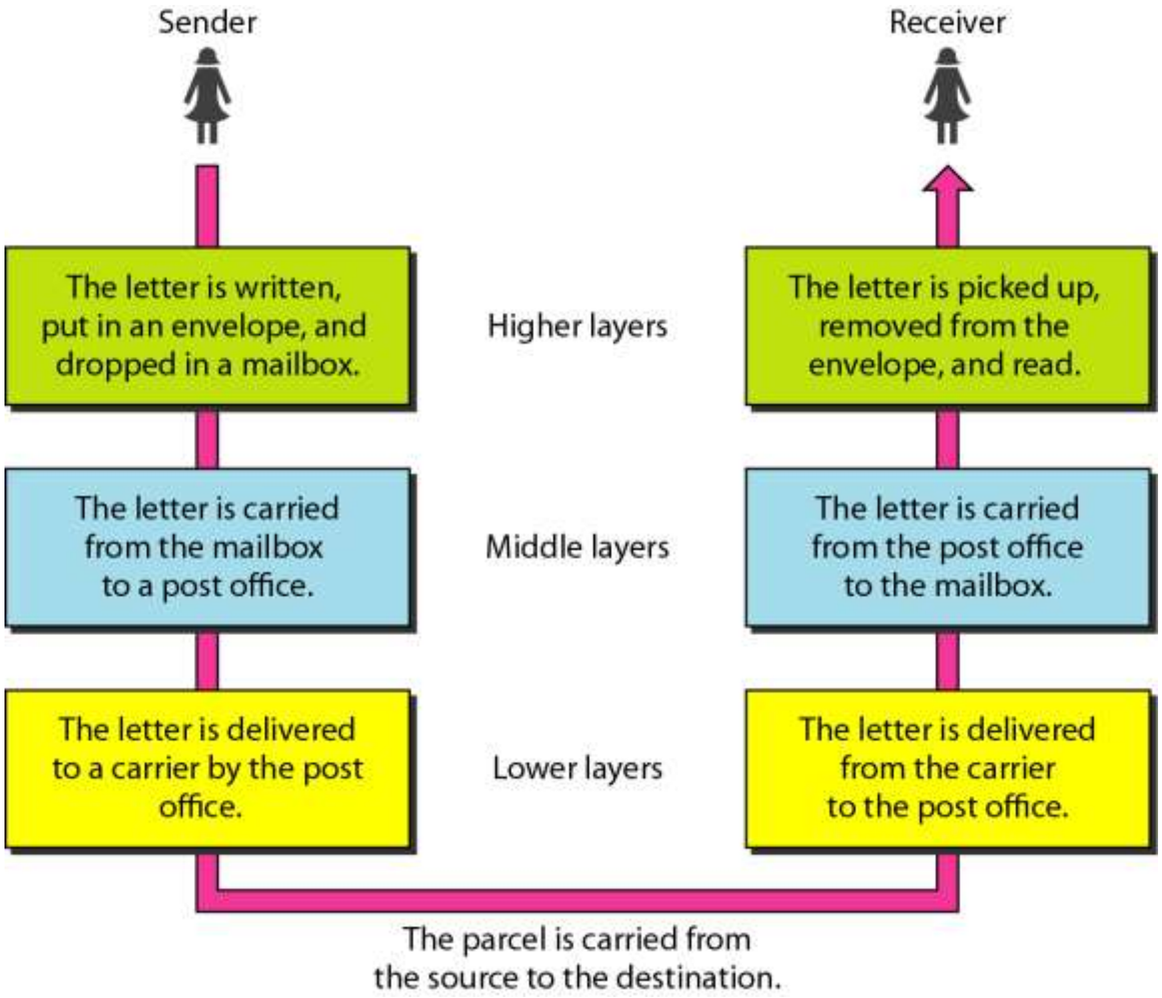
- **Standards**
  - Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes. Data communication standards fall into two categories: de facto (by fact or by convention) and de jure (by law or by regulation).
  - De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
  - De jure standards that have been legislated by an officially recognized body ex. Federal Communications Commission (FCC)
  - **Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.**
  - **Ex. EIA(Electronic Industries Alliance)-232F and USB**

- **Internet Standards (IETF) (Process of making Internet Standards)**
  - IETF: Internet Engineering Task Force
  - An internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the internet.
  - There is a strict procedure by which a specification attains Internet Standard status.
    - A specification begins as an internet draft. An internet draft is a working document with no official status and a 6-month lifetime.
    - Upon recommendation from the internet authorities, a draft may be published as a request for comment.
    - Each RFC is edited, assigned a number, and made available to all interested parties.
    - RFCs go through maturity levels and are categorized according to their requirement level.
- RFC: Request for Comment
- In computer network engineering, a Request for Comments (RFC) is a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems

Layered Architecture

OSI and TCP/IP Model

Layered 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.

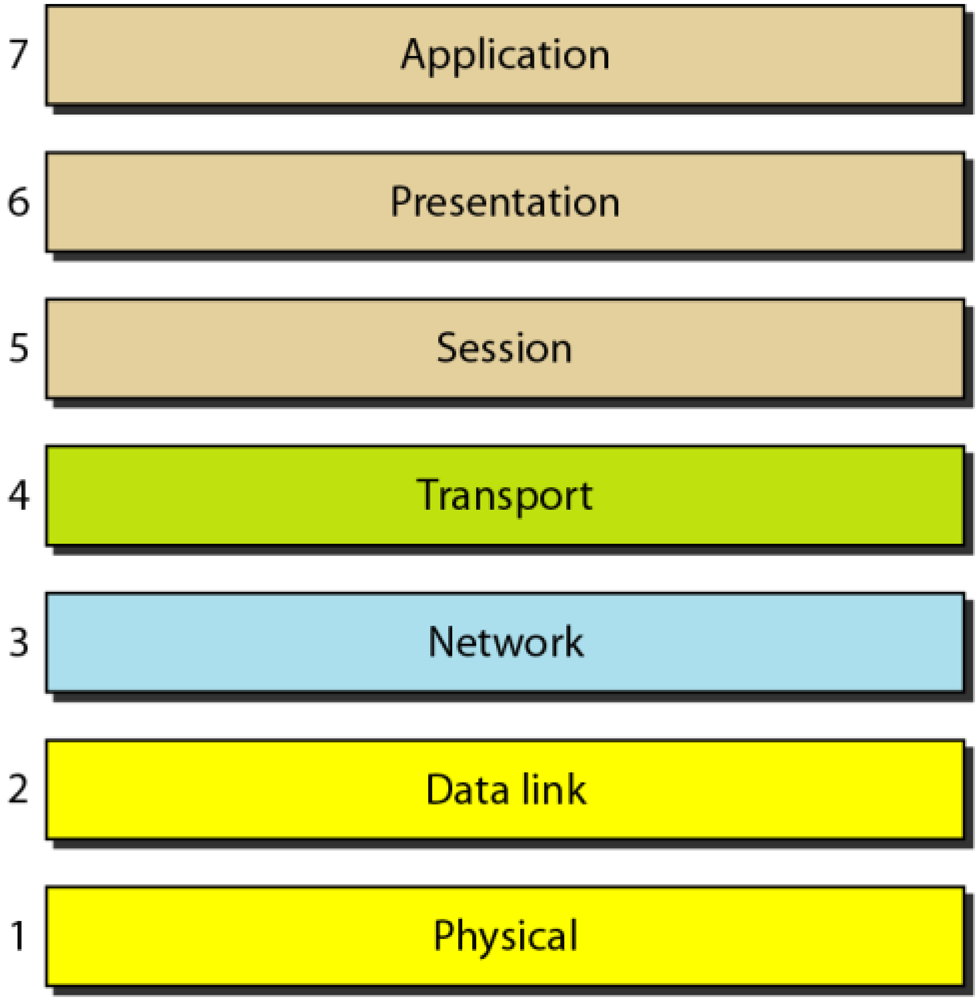
The letter is delivered to a carrier by the post office.

Lower layers

The letter is delivered from the carrier to the post office.

The parcel is carried from the source to the destination.

- Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.
- ISO is the organization.
  OSI is the model.



7 Application

6 Presentation

5 Session

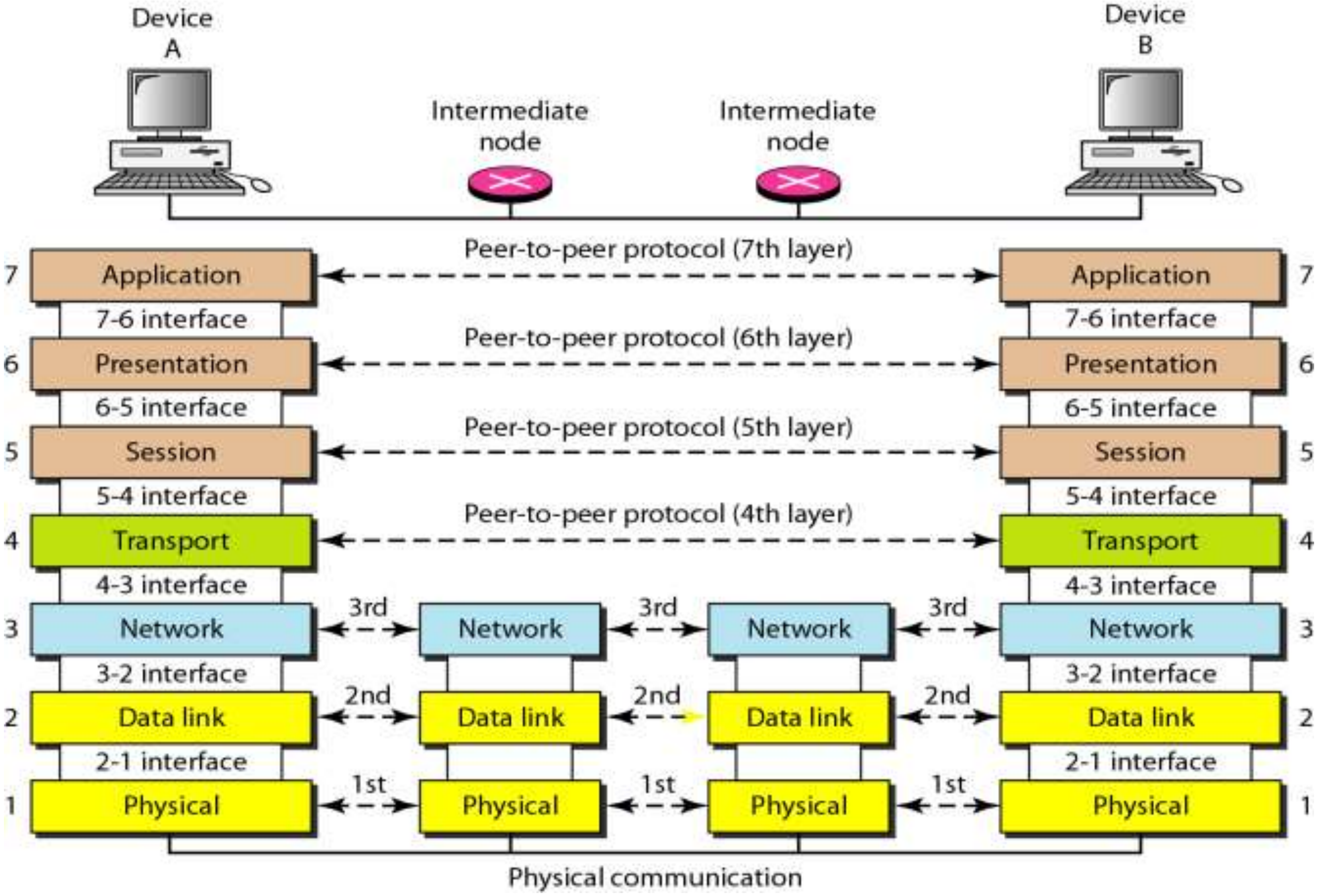
4 Transport

3 Network

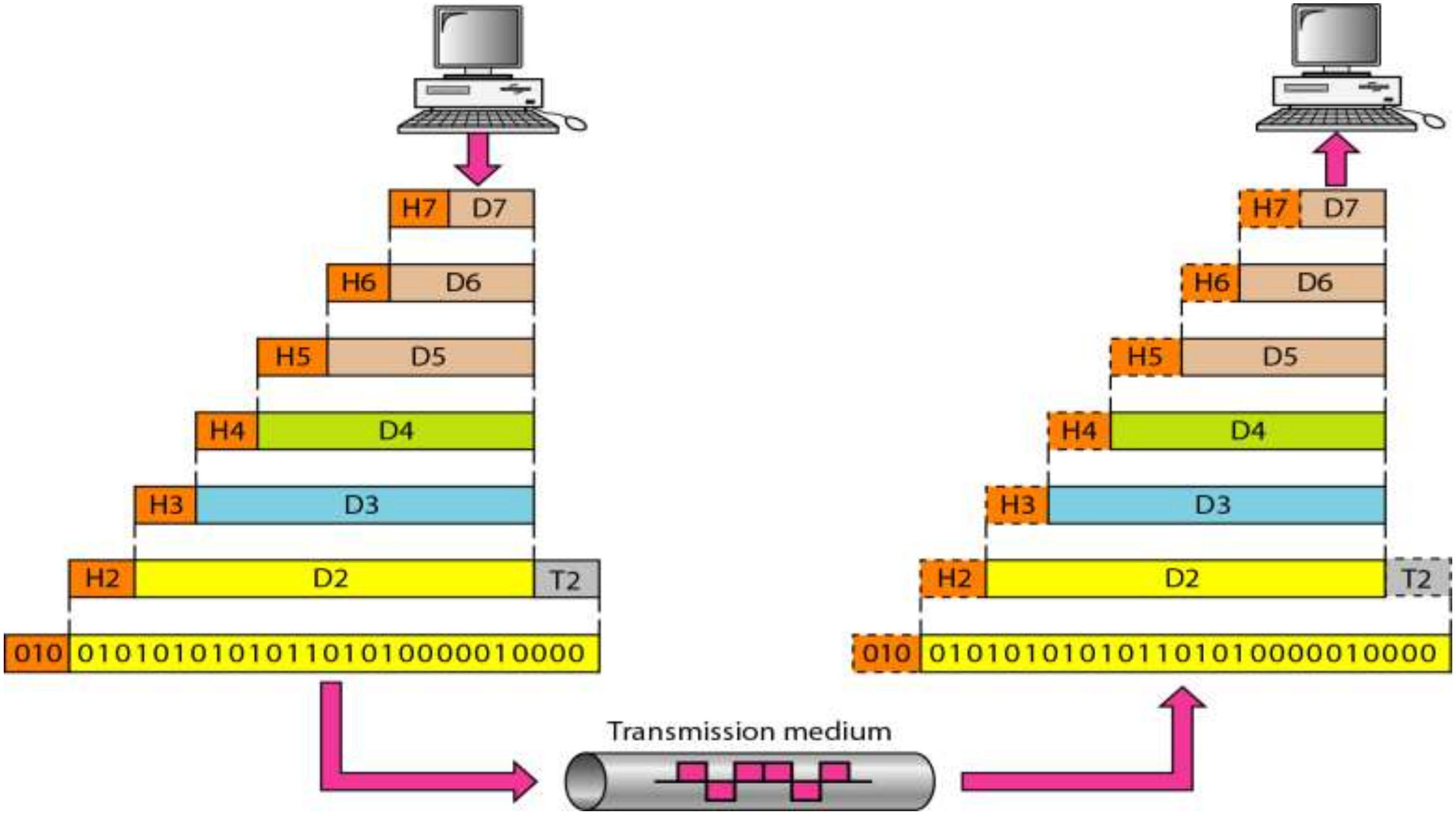
2 Data link

1 Physical

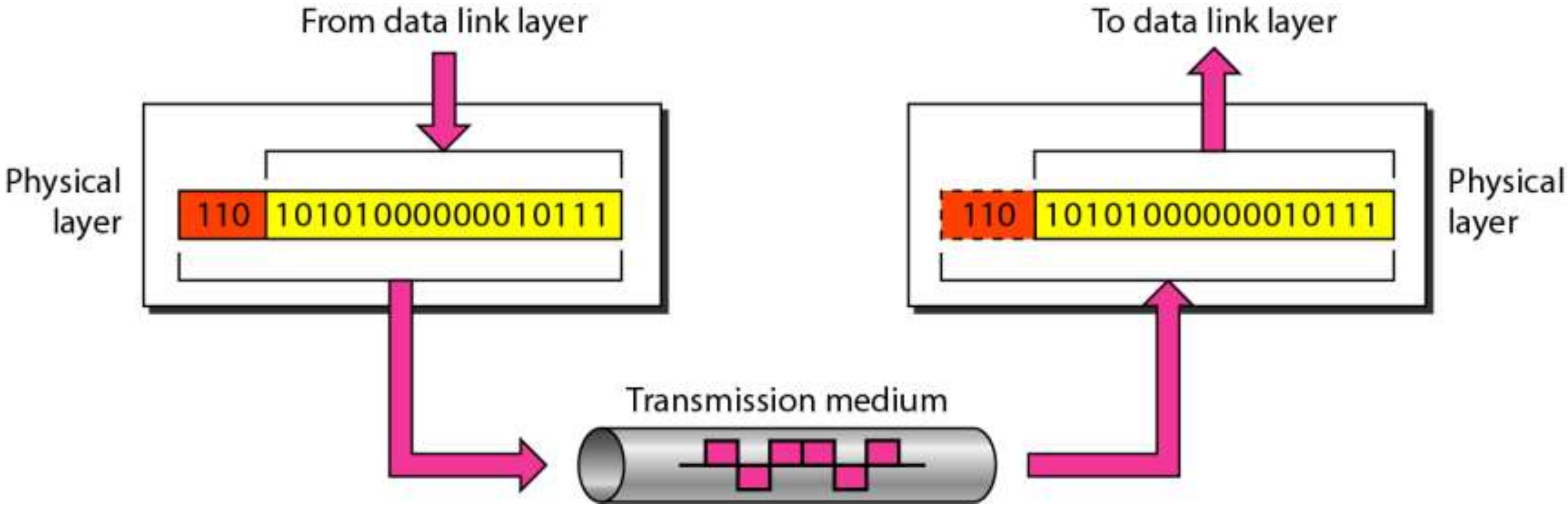
Interaction between layers



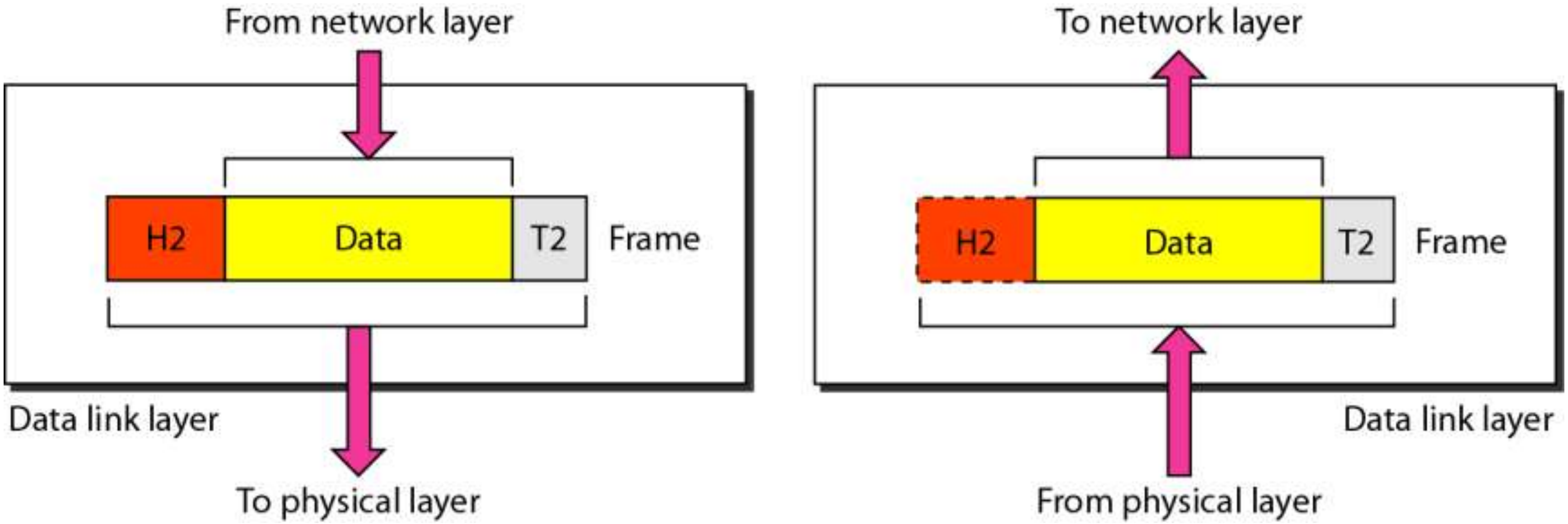
Exchange using OSI Model



Physical Layer

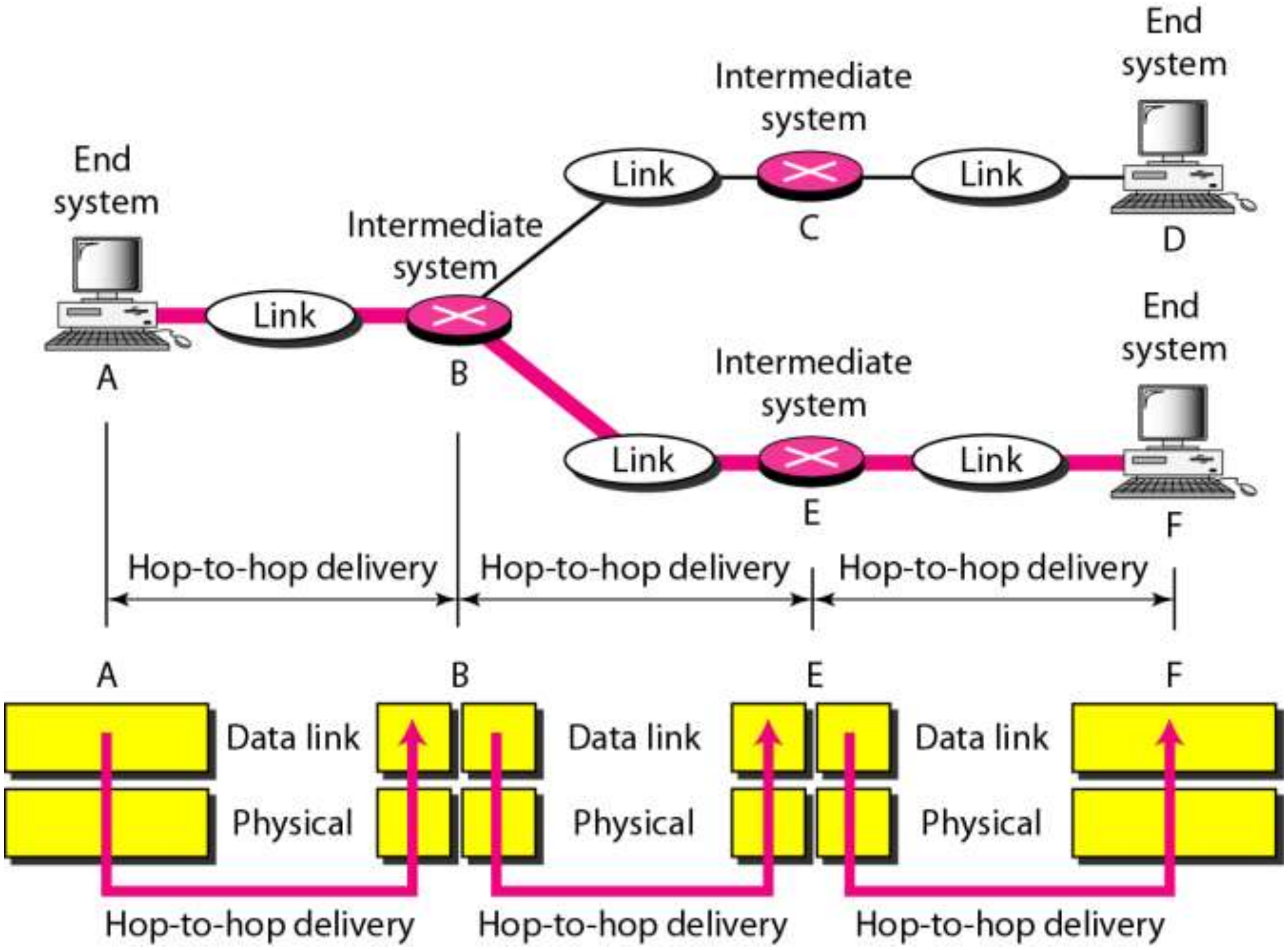


The physical layer is responsible for movements of individual bits from one hop (node) to the next.

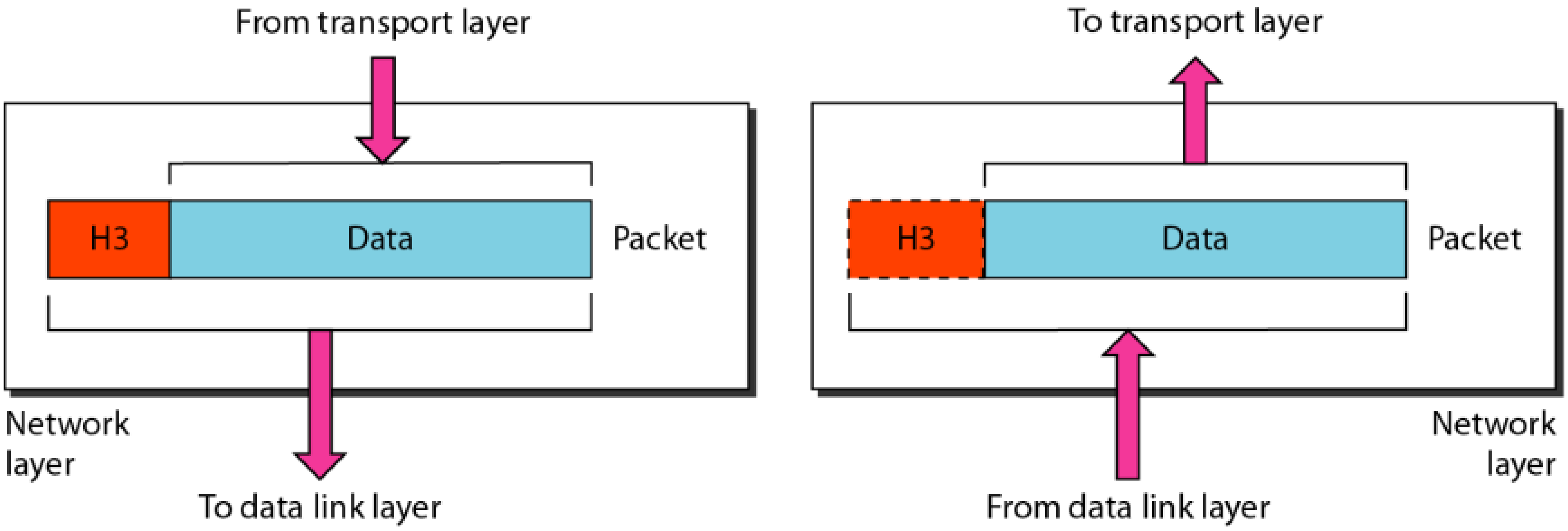


The data link layer is responsible for moving frames from one hop (node) to the next.

Hop to hop delivery

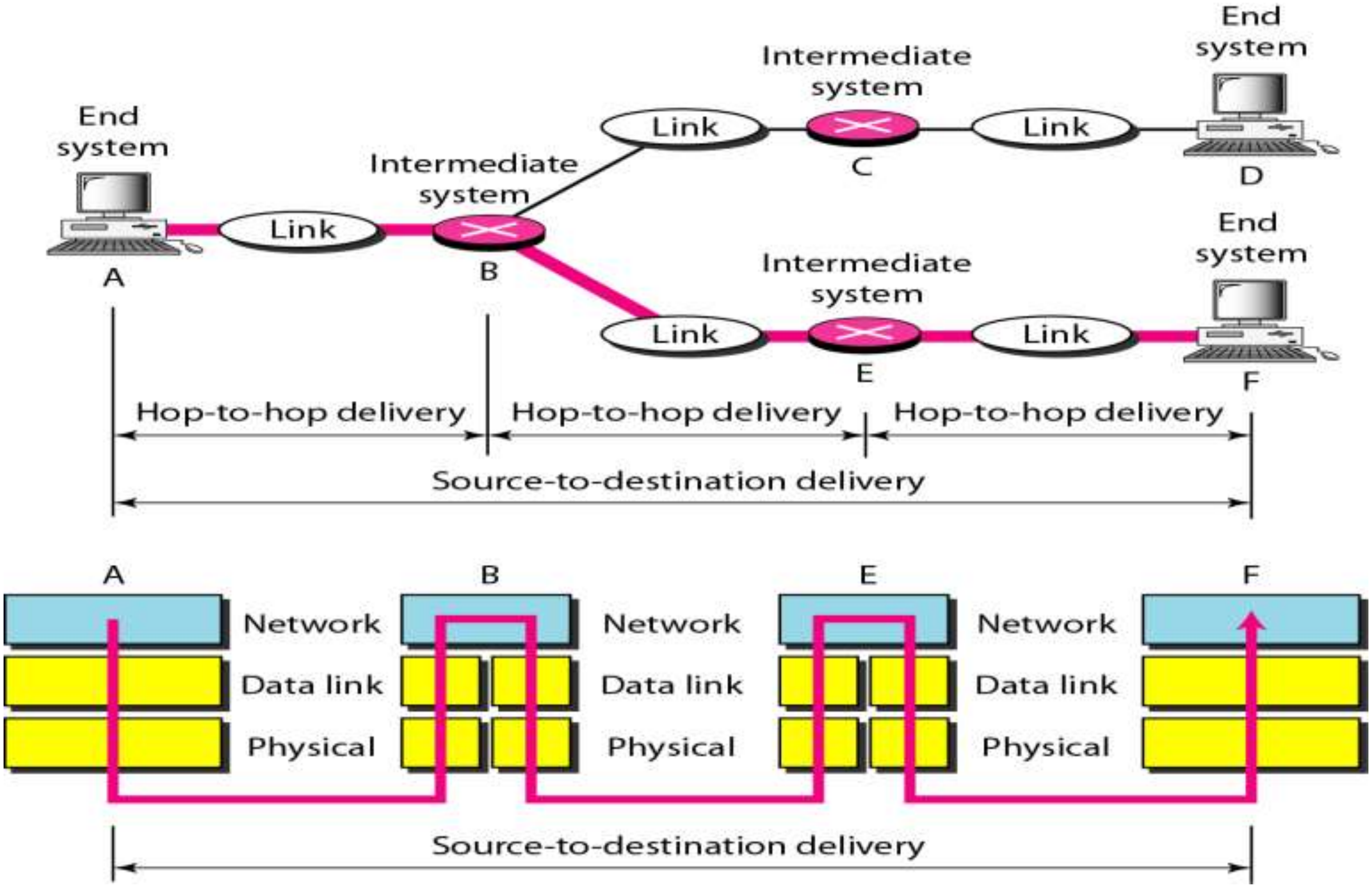


Network Layer

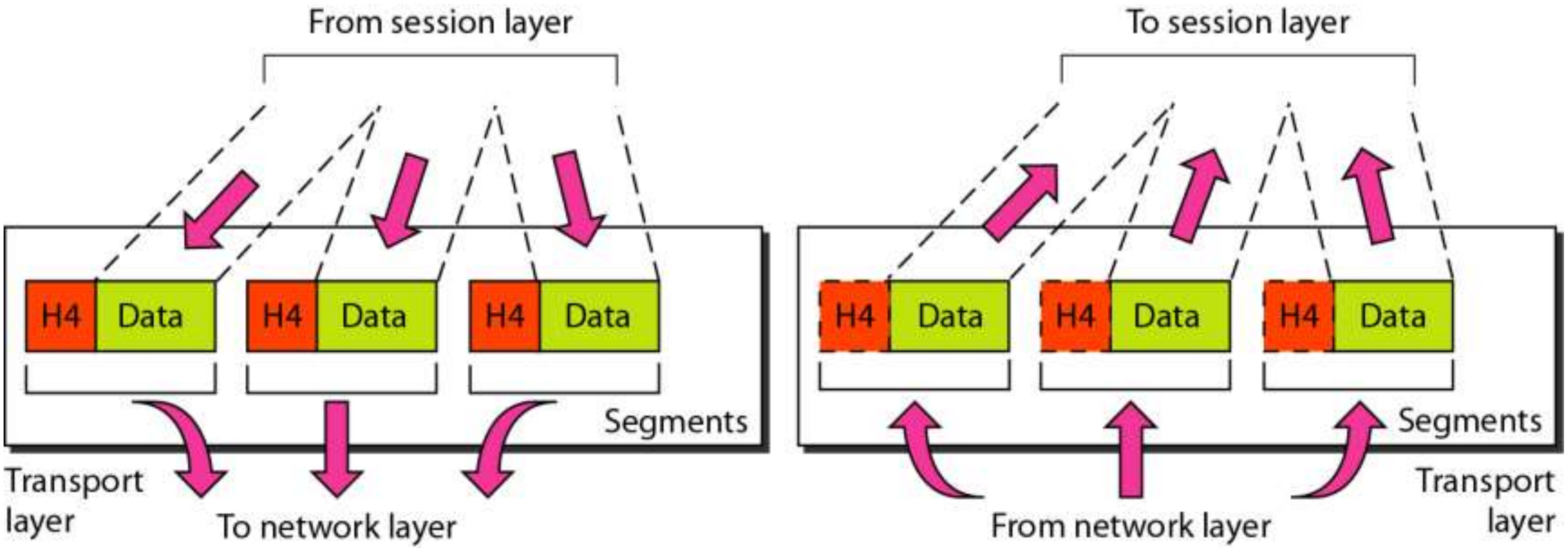


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Source-to-destination delivery

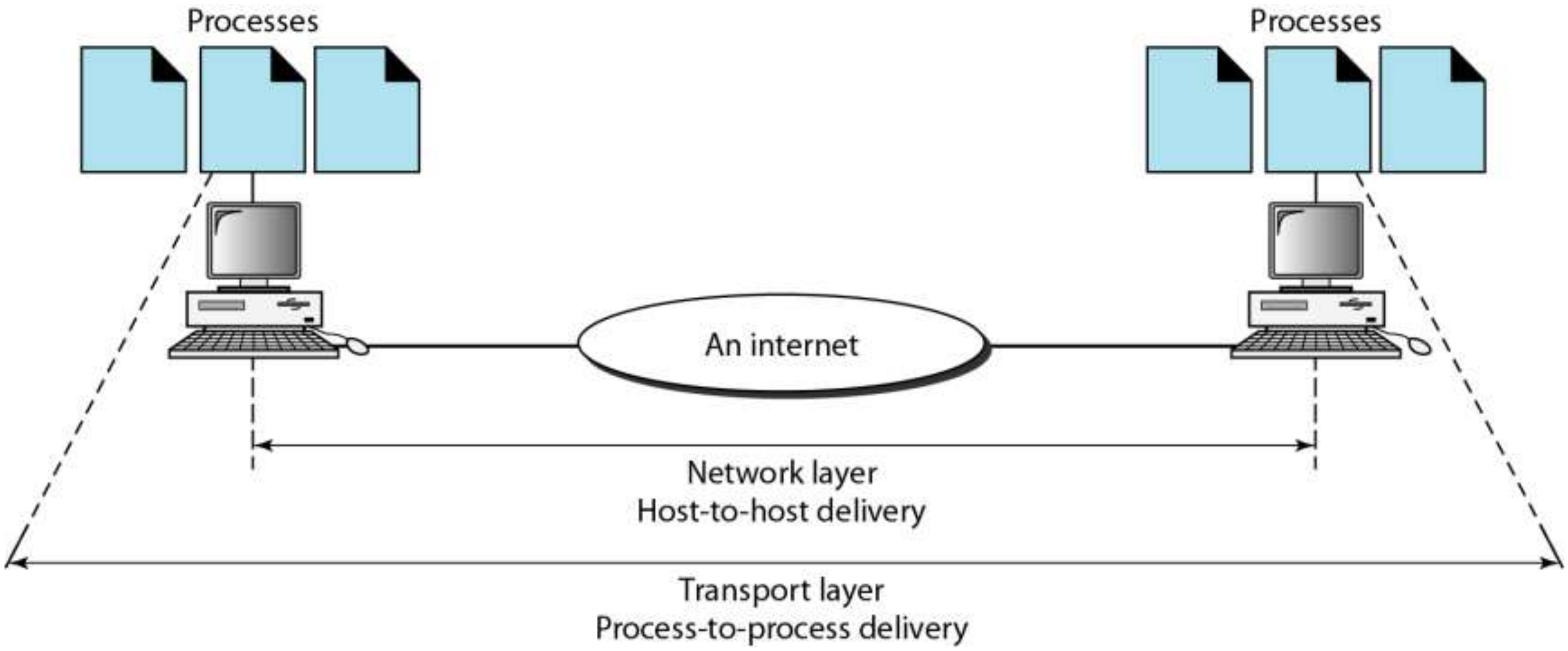


Transport Layer

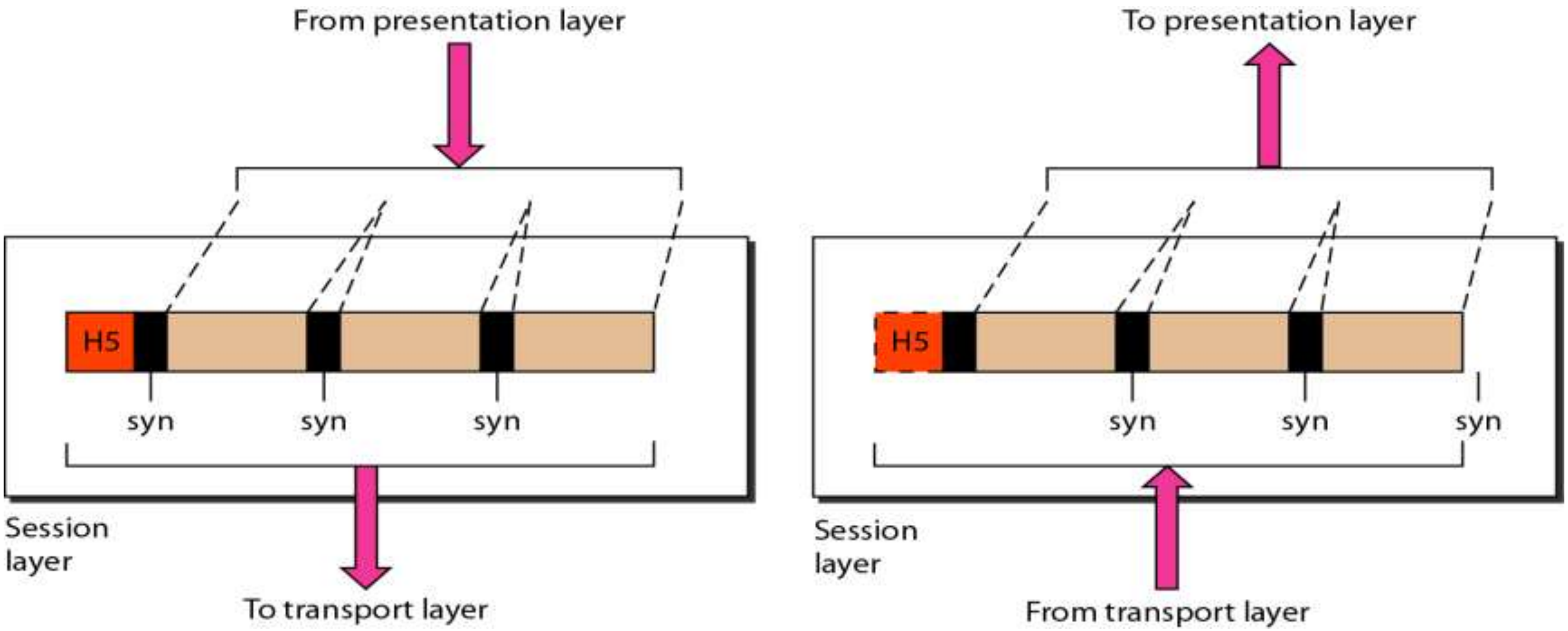


The transport layer is responsible for the delivery of a message from one process to another

Reliable Process to Process Delivery

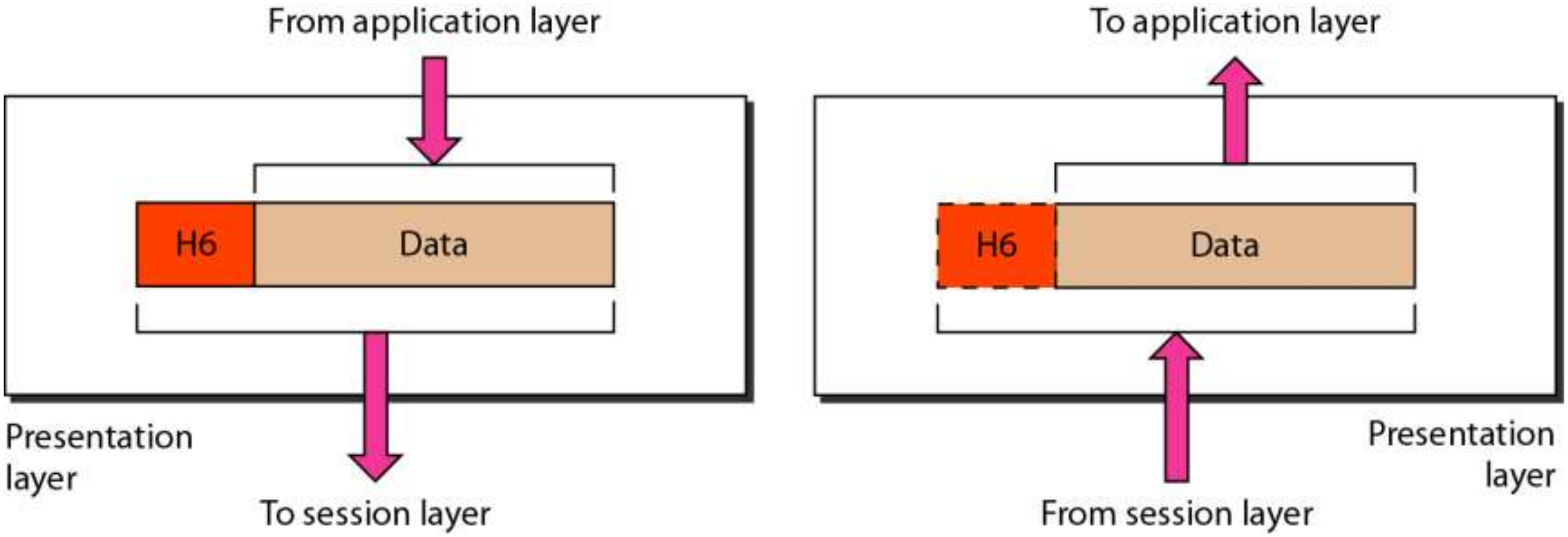


Session Layer



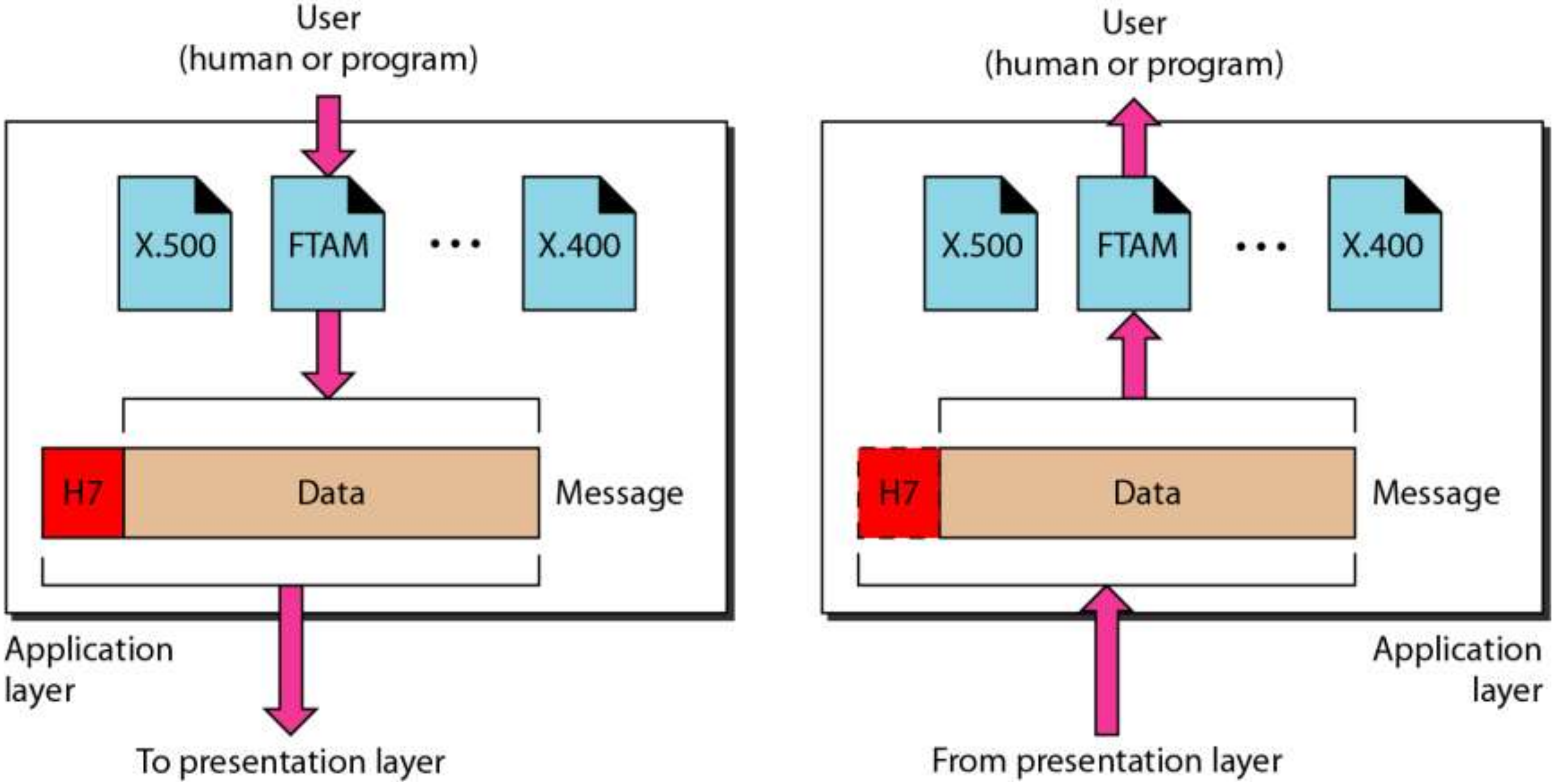
The session layer is responsible for dialog control and synchronization.

Presentation



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

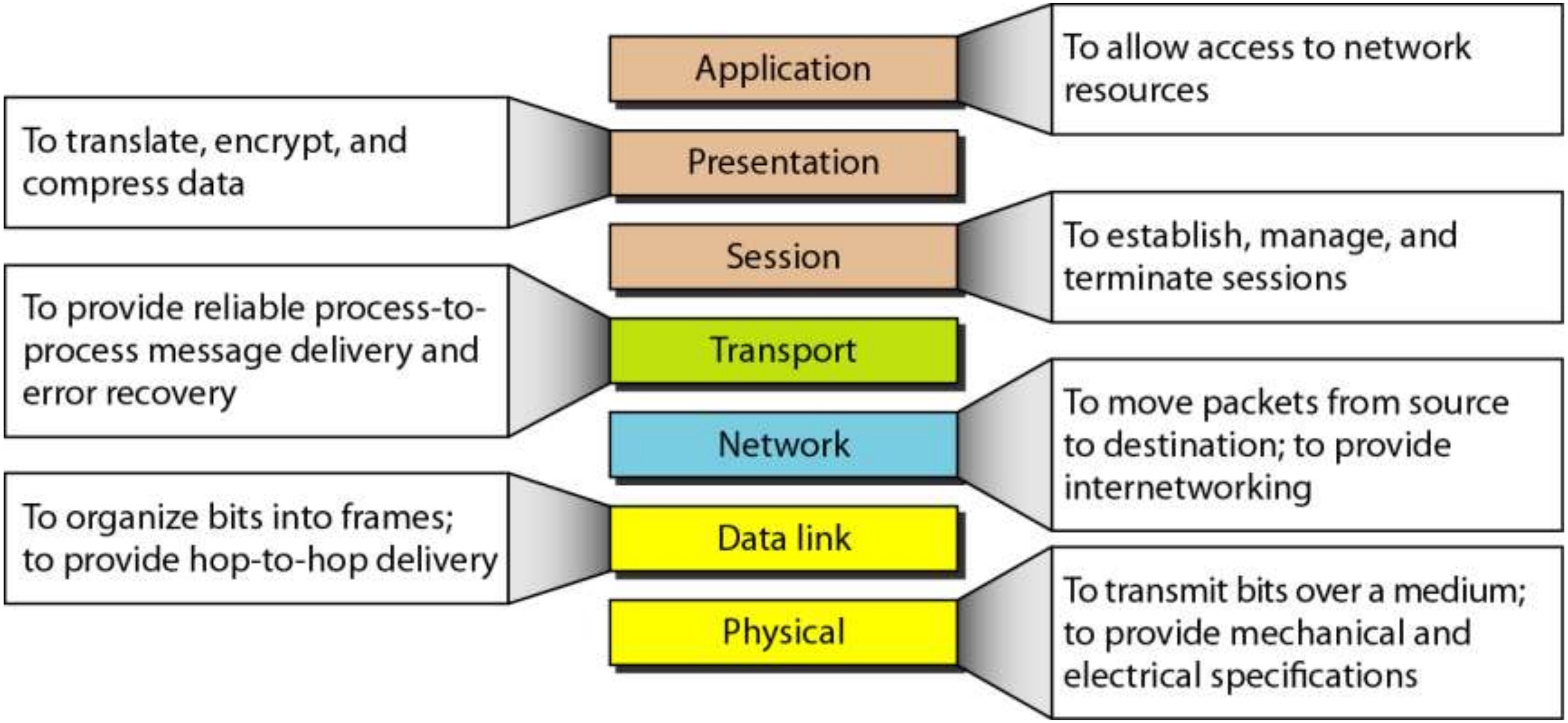
Application Layer



FTAM: File Transfer Access Management

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

Summary of Layers



Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide reliable process-to-process message delivery and error recovery

Network

To move packets from source to destination; to provide internetworking

Data link

To organize bits into frames; to provide hop-to-hop delivery

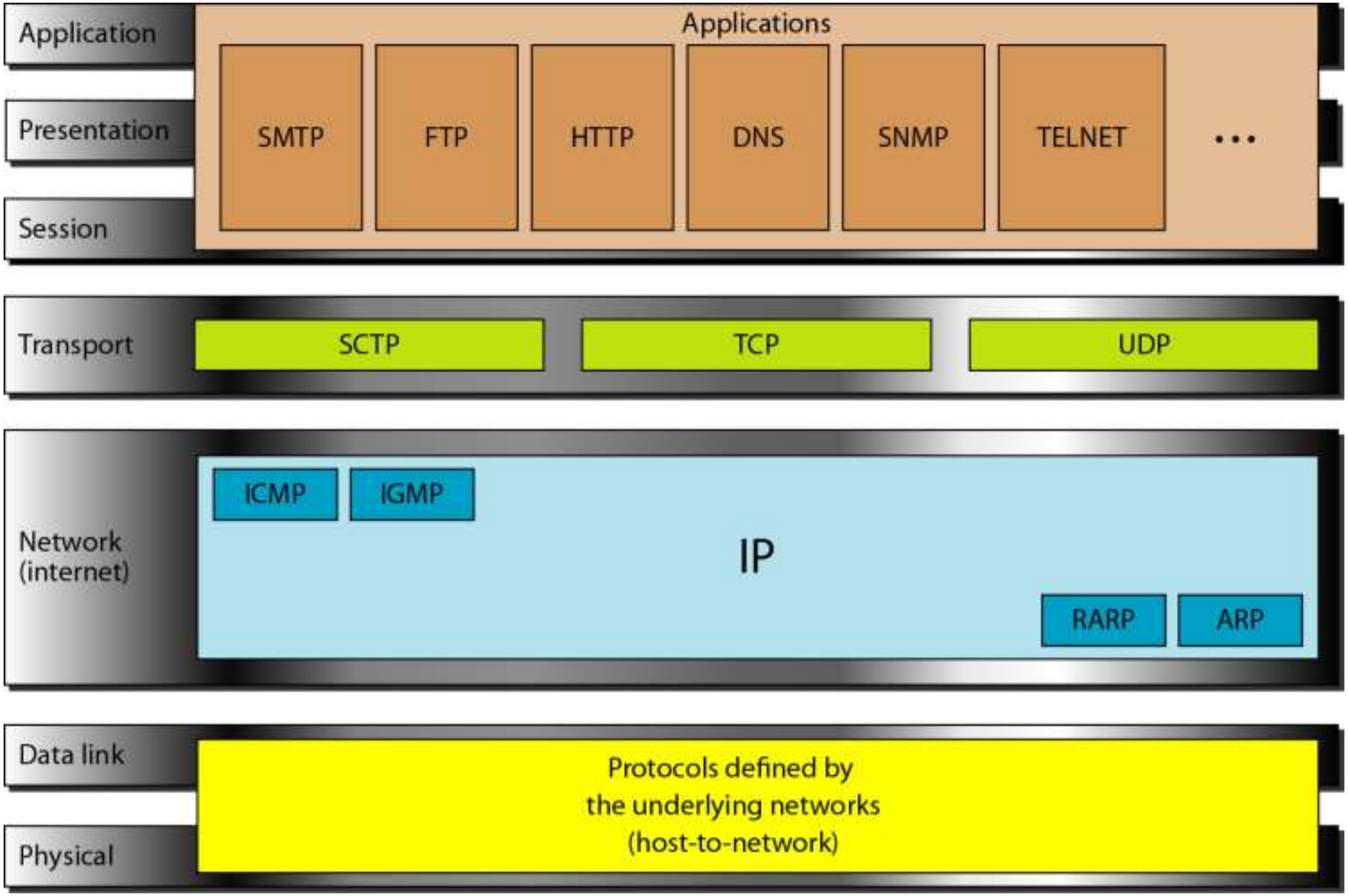
Physical

To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP Architecture

- 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 TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.

TCP/IP and OSI Model



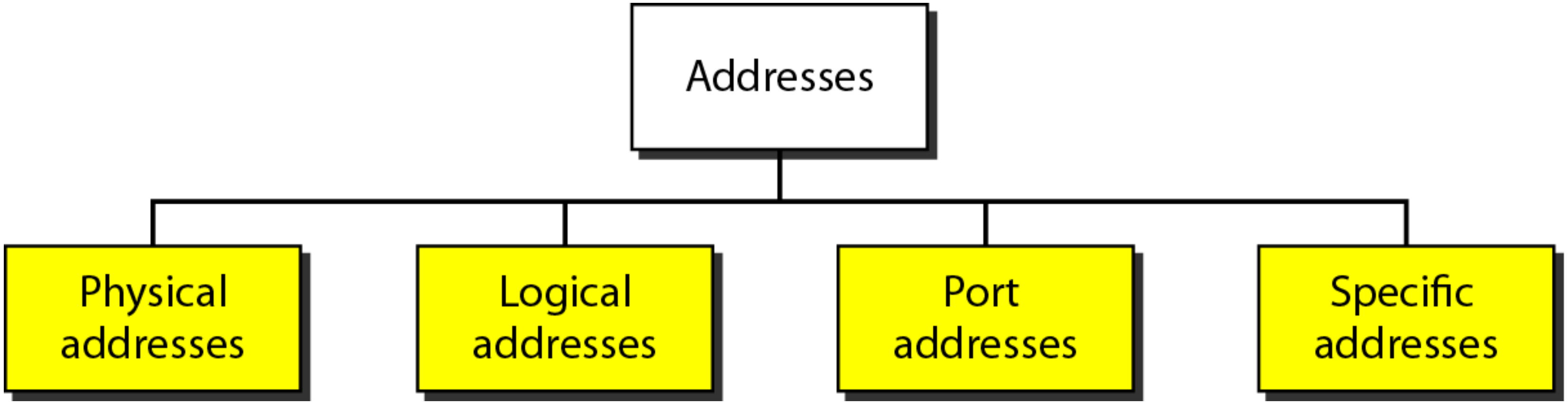
- **Physical and Data link Layers**
  - It supports all the standard and proprietary protocols. It does not define any specific protocol.
- **Network Layer**
  - TCP/IP supports the Internetworking Protocol. It uses four supporting protocols
    - **ARP: Address Resolution Protocol**
      - Logical Address --→ Physical Address
    - **RARP: Reverse Address Resolution Protocol**
      - Physical Address --→ Logical Address
      - It is used when a computer is connected to a network for first time or when a diskless computer is booted.
    - **ICMP**: Internet Control Message Protocol
    - **IGMP**: Internet Group Message Protocol

- **IP provides** unreliable and connectionless datagram delivery. It provides **Best Effort Delivery service**. Best Effort means that IP provides no error checking or tracking. IP does its best to get a transmission through to its destination, but with no guarantees.
- ICMP: it is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender.
- ICMP messages are divided into broad categories: **Query Messages** , which occur in pairs, help a host or a network manager get specific message information from a router or host. **Error Reporting** Messages helps to report errors.
- IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients.
- IGMP protocol gives the information about the membership status of hosts connected to the network.
- It uses concept of Multicasting (One --→ Many)

- Transport Layer
  - TCP: Transmission Control Protocol is a **Connection Oriented Protocol**. TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt. It reorders the transmission based on sequence numbers.
  - UDP: Adds only port address, checksum, error control and length information
  - SCTP (Stream Control Transmission Protocol): To meet the needs of some needs of some newer application such as voice over the Internet. It combines the best features of UDP and TCP.

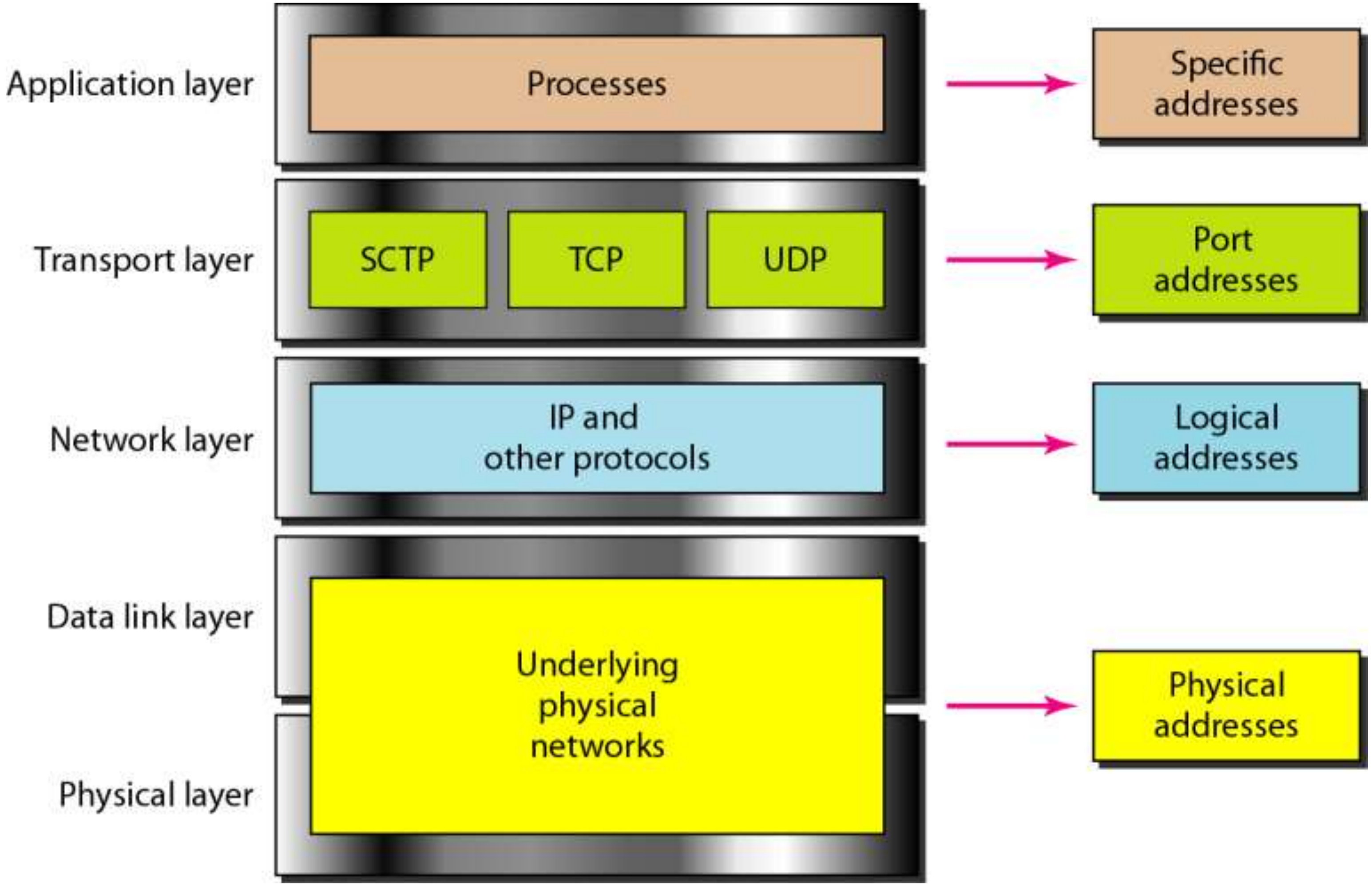
Addressing

- Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

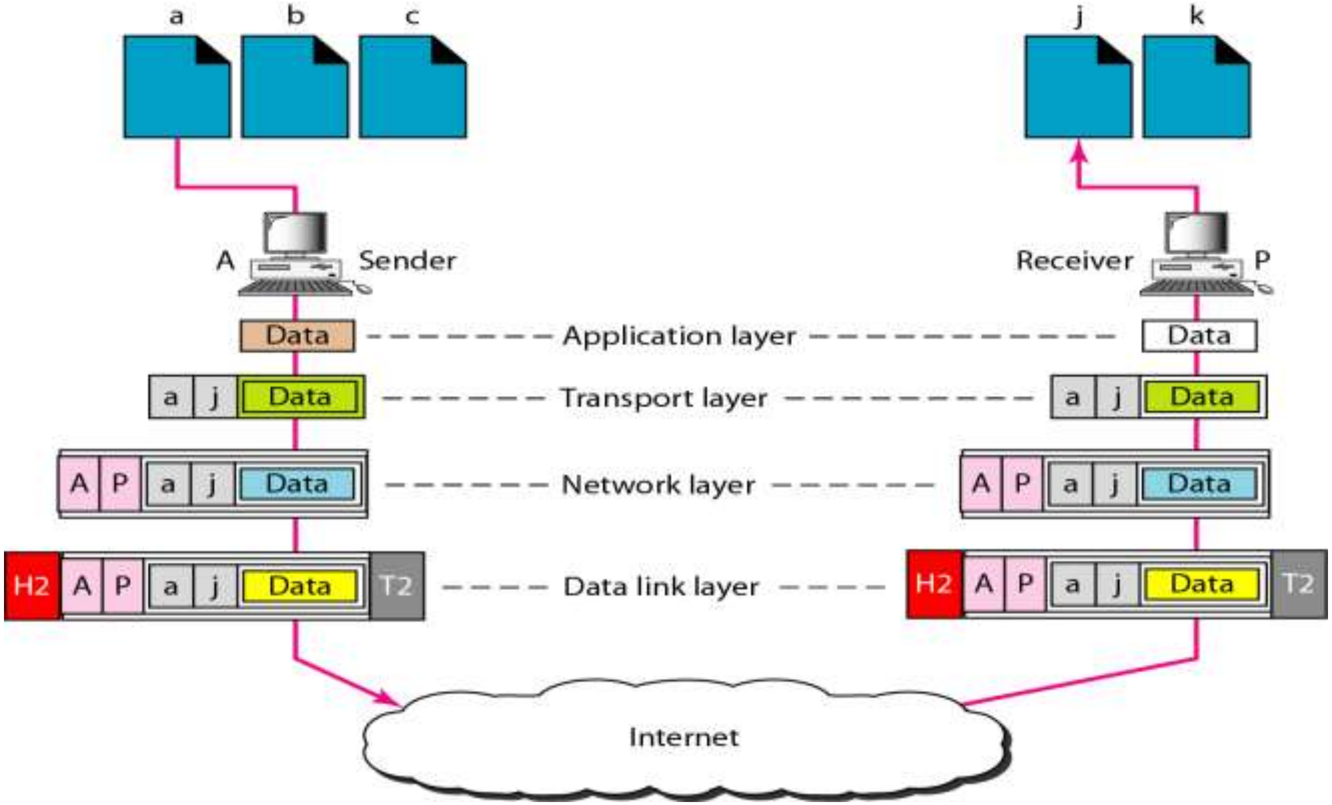


- Physical Address: It is also known as link address, is the address of a node defined by its LAN or WAN. It is included in the frame by the data link layer. It is the lowest level address.
- The size and format of these addresses vary depending on the network.
  - Ex. Ethernet uses a 6 byte physical imprinted on NIC card
  - Local Talk has a 1 byte dynamic address.
- Logical Address: it is necessary for universal communications that are independent of underlying physical networks. It is needed to identify each host uniquely.
  - Ex. IPV4 -→ 32bit, IPV6--→ 128bit address.
  - Developed by IETF
- Port Address: The label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length
  - The end objective of Internet communication is a process communicating with another process. Ex. FTP, Telnet
- Specific Addresses
  - Some applications have user-friendly addresses that are designed for that specific address. Example include the e-mail address and URL. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.

Relationship of layers and addresses in TCP/IP



Port Address



The physical addresses change from hop to hop,
but the logical and port addresses usually remain the same.

- Interface: The connection to a peripheral is often called the interface
- Interfacing : The process of providing all the proper interconnections between a computer and a peripheral is called Interfacing.

- https://www.youtube.com/watch?v=HOaIqQAeaik