COMPUTER NETWORKS

Module – I: INTRODUCTION AND PHYSICAL LAYER

Introduction: Data Communications: Components, Data representations, Data flow, Networks: Distributed Processing, Network Criteria, and Physical structures, Network models, Categories of Networks [LAN, WAN, MAN], Protocols and Standards. [1.1,1.2,1.3]

Network Models: The OSI Model: layered architecture, Peer to peer processes, and encapsulation, Layers in the OSI Model: [Brief description of all seven layers], TCP / IP Protocol Suite, Addressing: physical, logical and port addresses and specific address. [2.1,2.2,2.3]

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

1-1 DATA COMMUNICATIONS

- 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 cable.

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

- The effectiveness of a data communication system depends on four fundamental characteristics

1. Delivery : The data should be delivered to the correct destination and correct user.

2. Accuracy : The communication system should deliver the data accurately, without introducing any errors. The data may get corrupted during transmission affecting the accuracy of the delivered data.

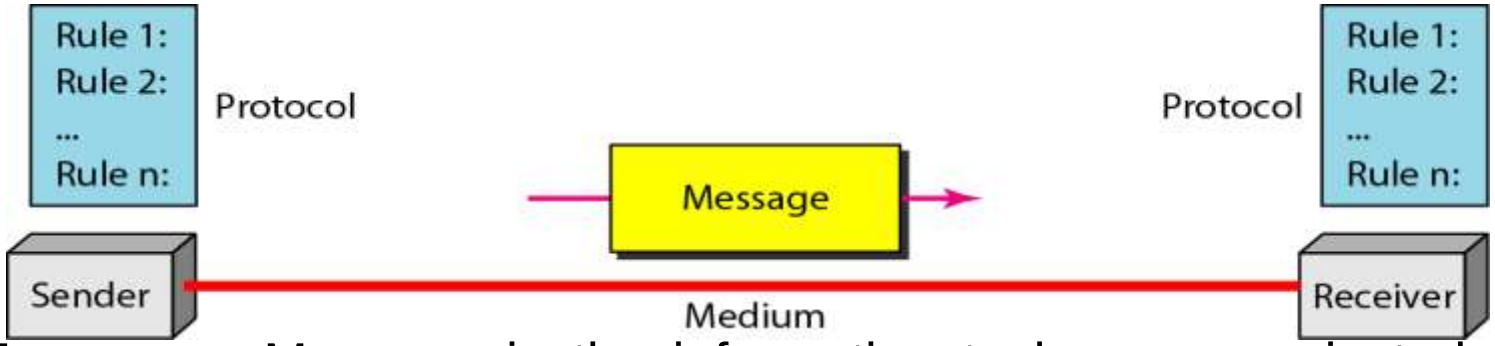
3. Timeliness : Audio and Video data has to be delivered in a timely manner without a delay; such a data delivery is called real time transmission of data.

4. Jitter: It is the variation in the packet arrival time. Uneven Jitter may affect the timeliness of data being transmitted

- Components
- Data Representation
- Data Flow

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

Five components of data communication



1. Message : Message is the information to be communicated by the sender to the receiver.

2. Sender : The sender is any device that is capable of sending the data.

3. Receiver : The receiver is a device that the sender wants to communicate the data (message).

4. Transmission Medium : It is the path by which the message travels from sender to receiver. It can be wired or wireless and many subtypes in both.

5. Protocol : set of rules used by the sender and receiver to communicate data. A protocol is a set of rules that governs data communication. A Protocol is a necessity in data communications without which the communicating entities are like two persons trying to talk to each other in a different language without know the other language.

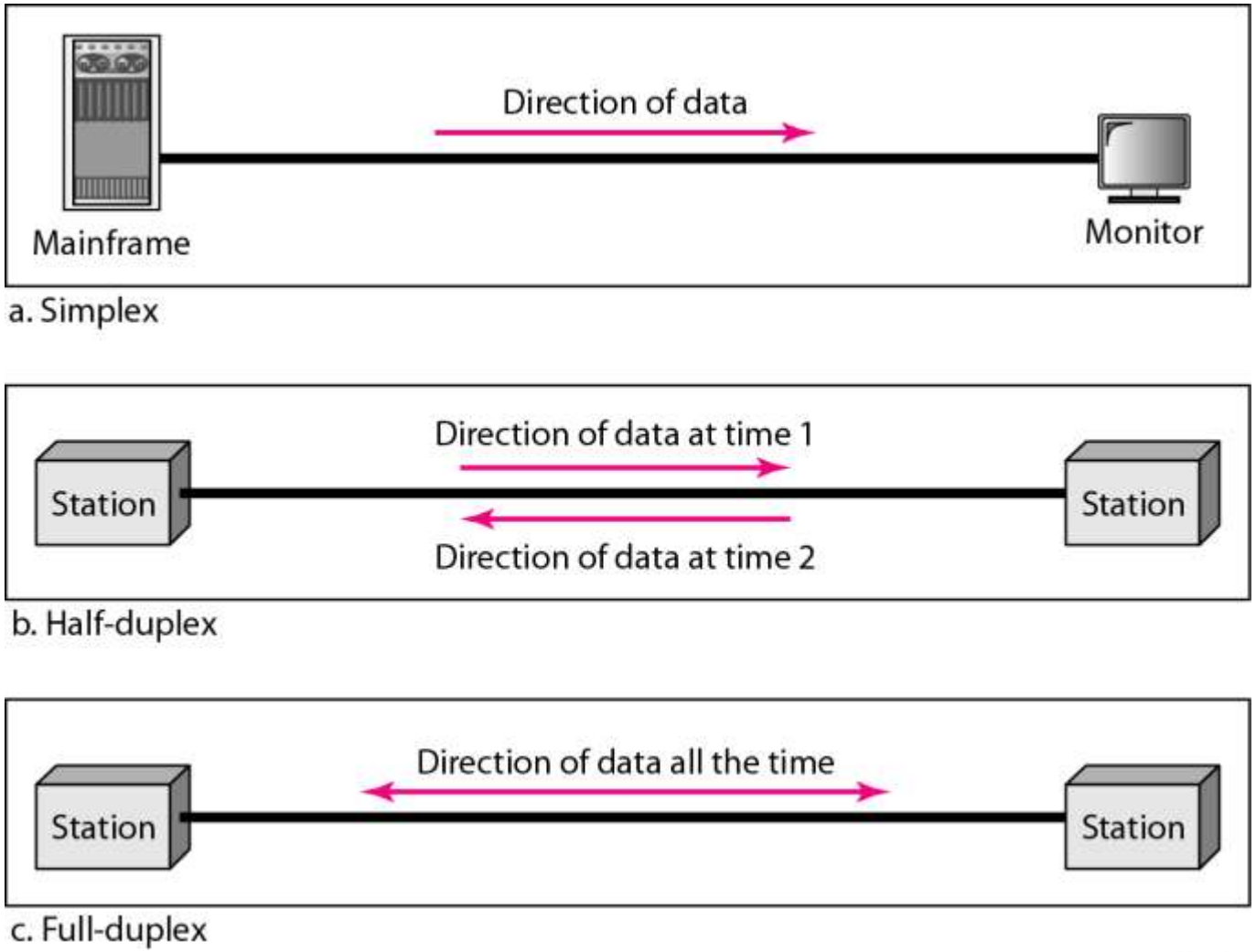
Data Representation

- **Text :**
  - A…Z, a…z, 0..9, etc
  - Text includes combination of alphabets in small case as well as upper case.
  - It is stored as a pattern of bits. encoding system used to represent text: ASCII, Unicode ,ISO
- ASCII
  - uses 7 bits
- Extended ASCII
  - uses 1 byte
- Unicode
  - Uses 16 bits
- ISO (International Organization for Standardization)
  - Uses 32 bits.
- **Numbers :**collection of digits from 0 to 9. It is stored as a pattern of bits.
- **Audio :**Data can also be in the form of sound which can be recorded and broadcasted. Audio data is continuous, not discrete.
- **Video :**Video refers to broadcasting of data in form of pictures

Images

- A Pixel is the smallest element of an image, a picture or image is represented as matrix of pixel elements.
- The pixels are represented in the form of bits.
- The size of an image depends upon the number of pixels (also called resolution)
- Commonly used Image formats : jpg, png, bmp, etc

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



Examples:

Keyboard

Walkie-talkies

Telephone

Two devices communicate with each other by sending and receiving data. The data can flow between the two devices in the following ways.

1. Simplex
2. Half Duplex
3. Full Duplex

Simplex :In Simplex, communication is unidirectional
Only one of the devices sends the data and the other one only receives the data.
Example: in the above diagram: a cpu send data while a monitor only receives data.

Half Duplex : In half duplex both the stations can transmit as well as receive but not at the same time. When one device is sending other can only receive and vice-versa (as shown in figure above.)
Example: A walkie-talkie

Full Duplex : In Full duplex mode, both stations can transmit and receive at the same time.
Example: mobile phones

1-2 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

Topics discussed in this section:

1. **Distributed Processing**
2. **Network Criteria**
3. **Physical Structures**
4. **Network Models**
5. **Categories of Networks**
6. **Interconnection of Networks: Internetwork**

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

1. Distributed Processing
   - Task is divided among multiple-computers
2. Network Criteria
   - Performance
     - Transit time and Response time
     - Depends on no. of users, type of medium etc
   - Reliability
     - Measured by frequency of failure,
     - The time it takes a link to recover from a failure
   - Security
     - Protecting data from unauthorized access

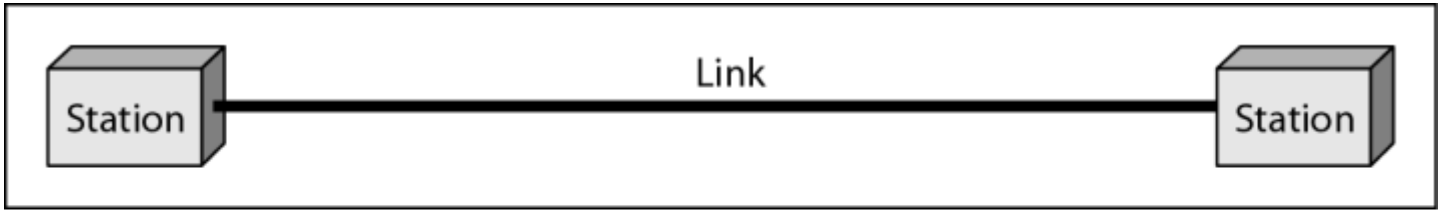
3.Physical Structures

- A network is two or more devices connected together through links.
- A link is a communications pathway that transfers data from one device to another.
- There are two types of connections
  - Point –to- point
  - Multipoint

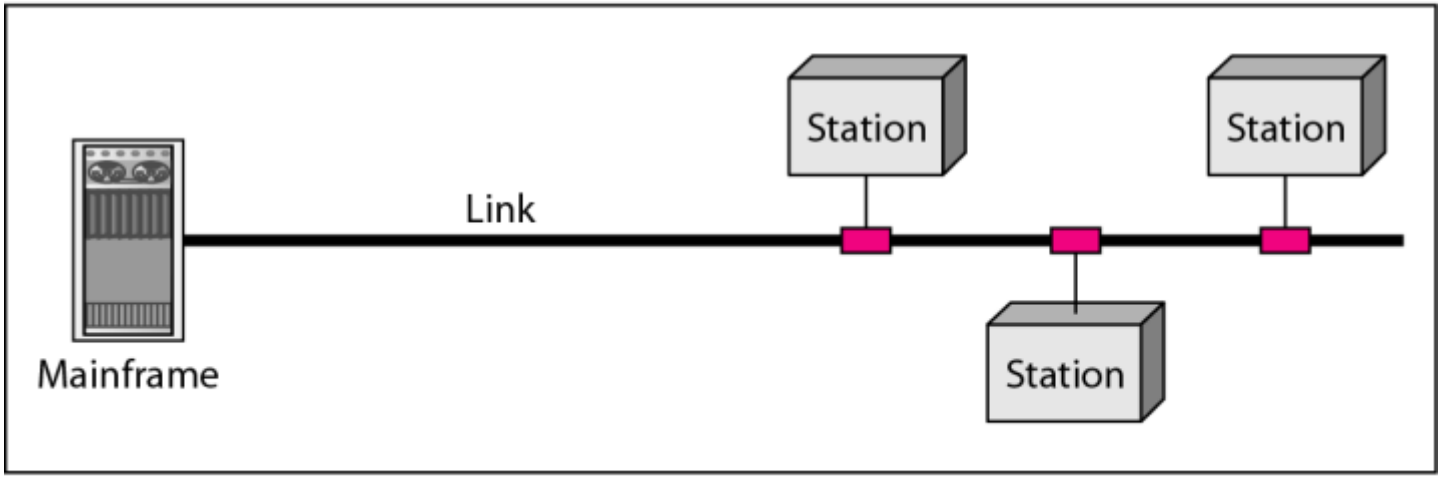
Point –to- point: provides dedicated link between two devices. The entire capacity of link is reserved for transmission between those two devices.

Multipoint : Is one where more than two devices share a single link. Capacity of link shared ,either spatially or temporally.

Figure 1.3 *Types of connections: point-to-point and multipoint*



a. Point-to-point



b. Multipoint

Physical topology

- The physical topology of a network is the geometric representation of the relationship of
  - all the links and
  - linking devices to one another.

Figure 1.4 *Categories of topology*

- There are four basic topologies
  - Mesh
  - Star
  - Bus
  - Ring

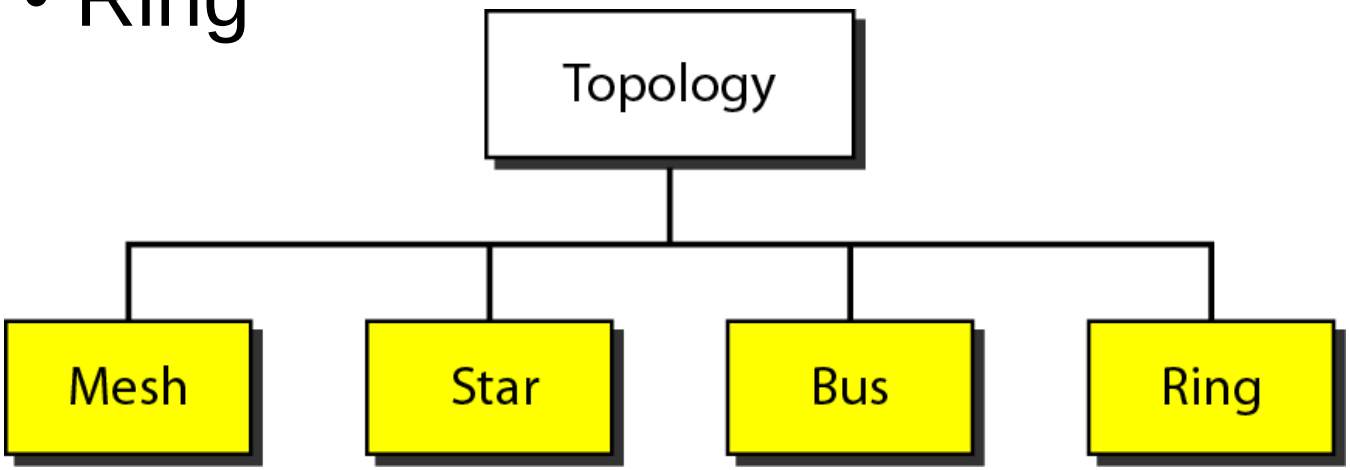
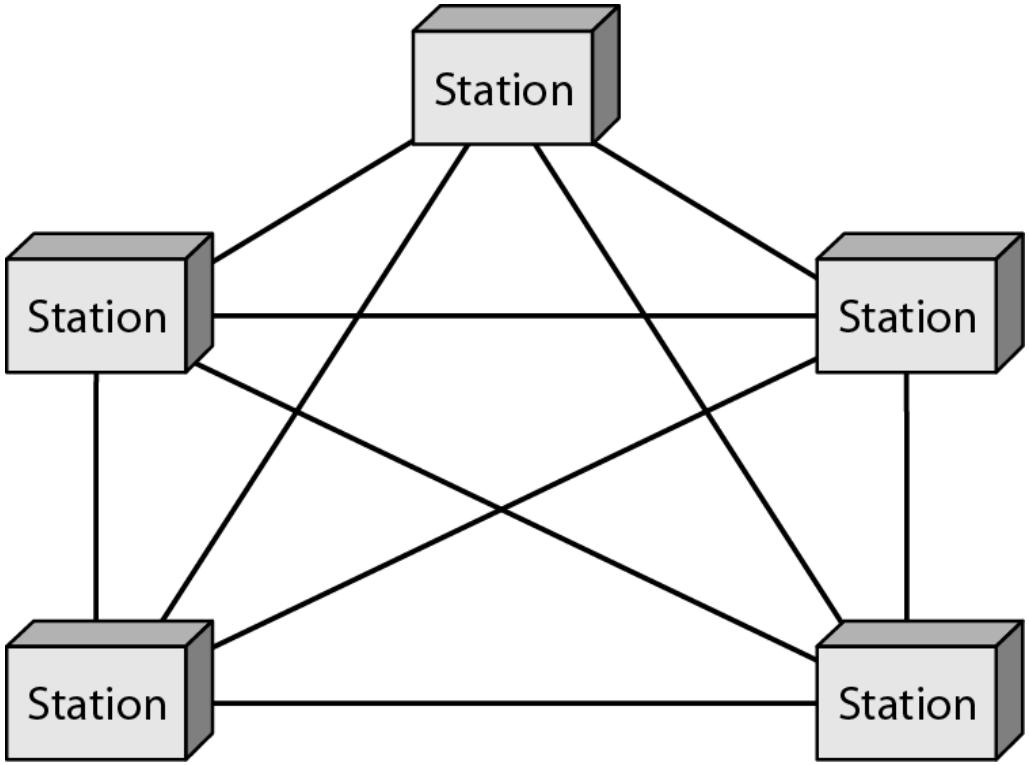


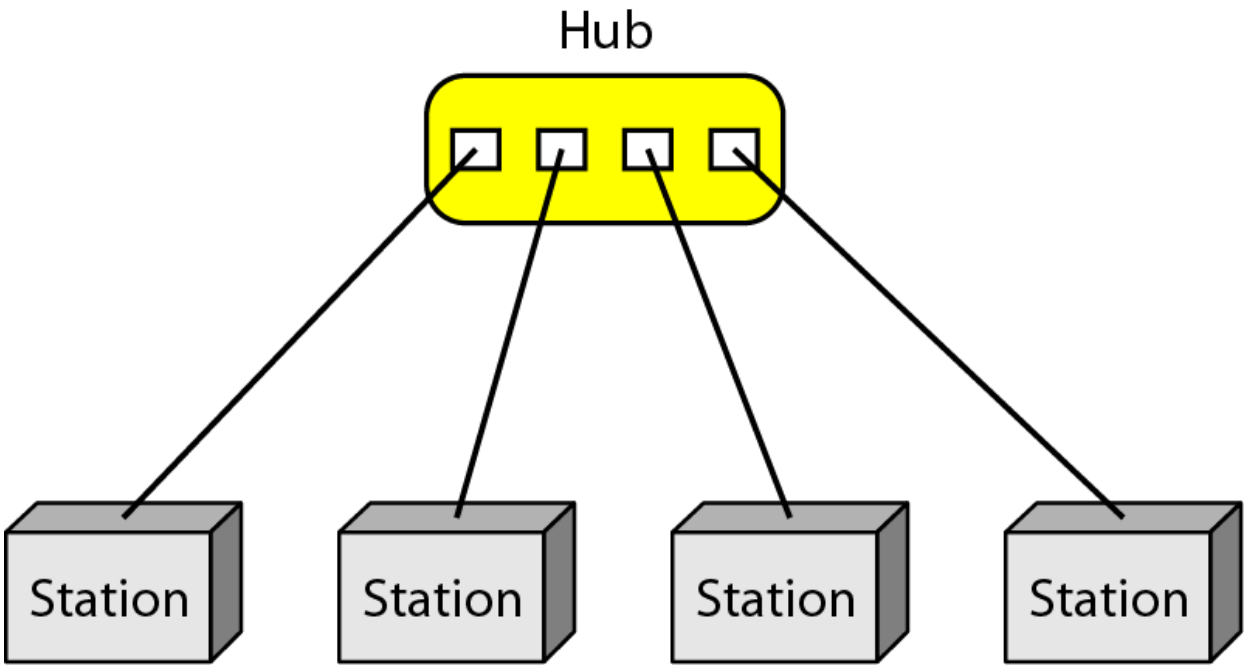
Figure 1.5 *A fully connected mesh topology (five devices)*



Mesh Topology

- Every device has a dedicated point-to-point link to every other device
- A fully connected mesh network has n(n-1)/2 physical channels to link n devices.
- **Advantages**
  - Dedicated links eliminates traffic problems
  - Robust- if one link becomes unusable, it does not affect the entire system
  - Secure
  - fault identification and isolation is easy
- **Disadvantages**
  - More cabling
  - More hardware

Figure 1.6 *A star topology connecting four stations*



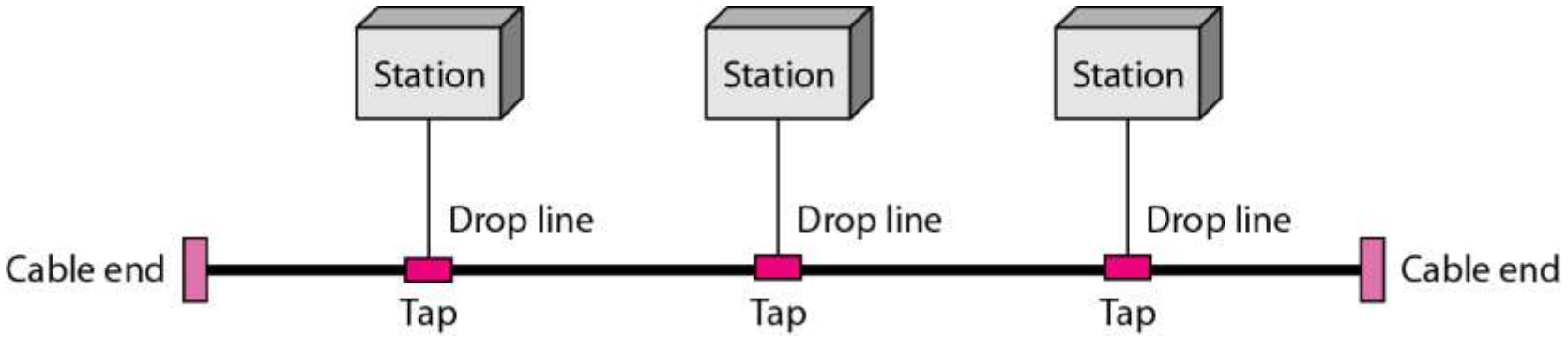
Star Topology

- Each device has a dedicated point-to-point link only to a central controller-hub
- The controller acts as an information exchanger
- **Advantages**
  - Less expensive than mesh
  - Robustness
  - Easy fault detection and isolation

  Disadvantage:

  Failure of hub leads to failure of entire ntwork

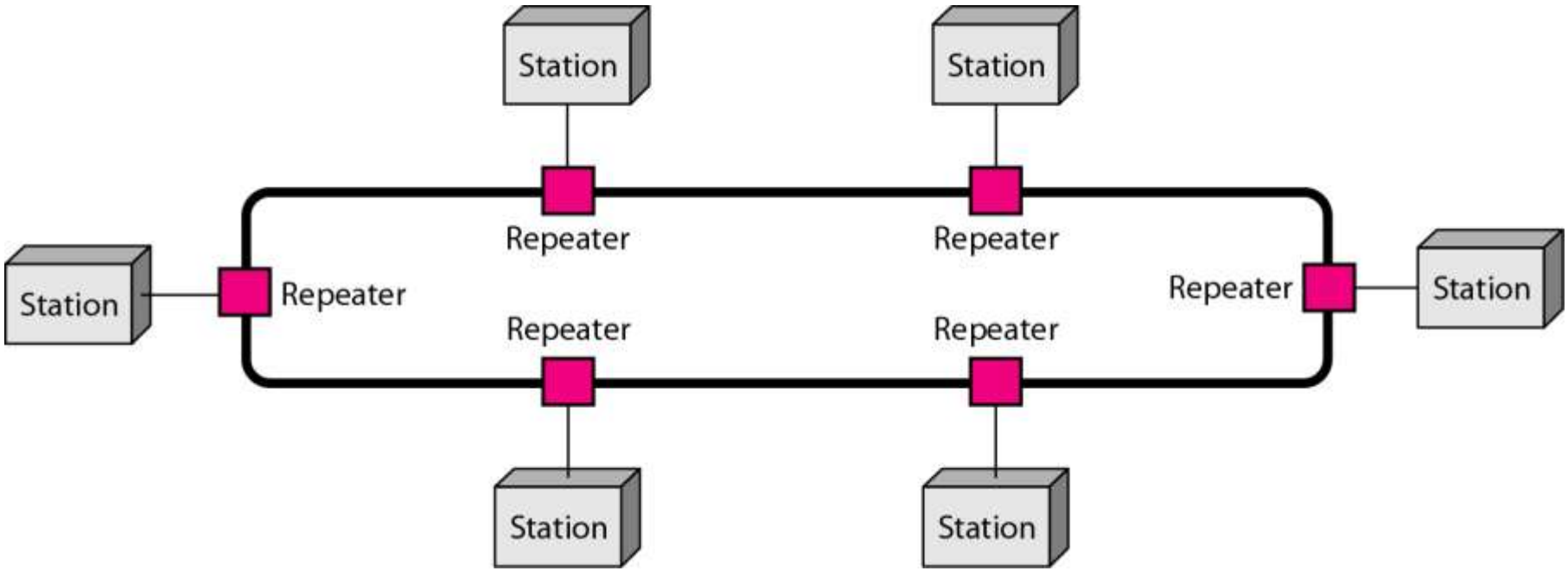
Figure 1.7 *A bus topology connecting three stations*



Bus Topology

- A bus topology is a multipoint.
- One long cable acts as a backbone to link all the devices in a network.
- Weaker signal
- **Advantages**
  - Ease of installation
  - Less cabling than mesh or star
- **Disadvantages**
  - Difficult reconnection and fault isolation

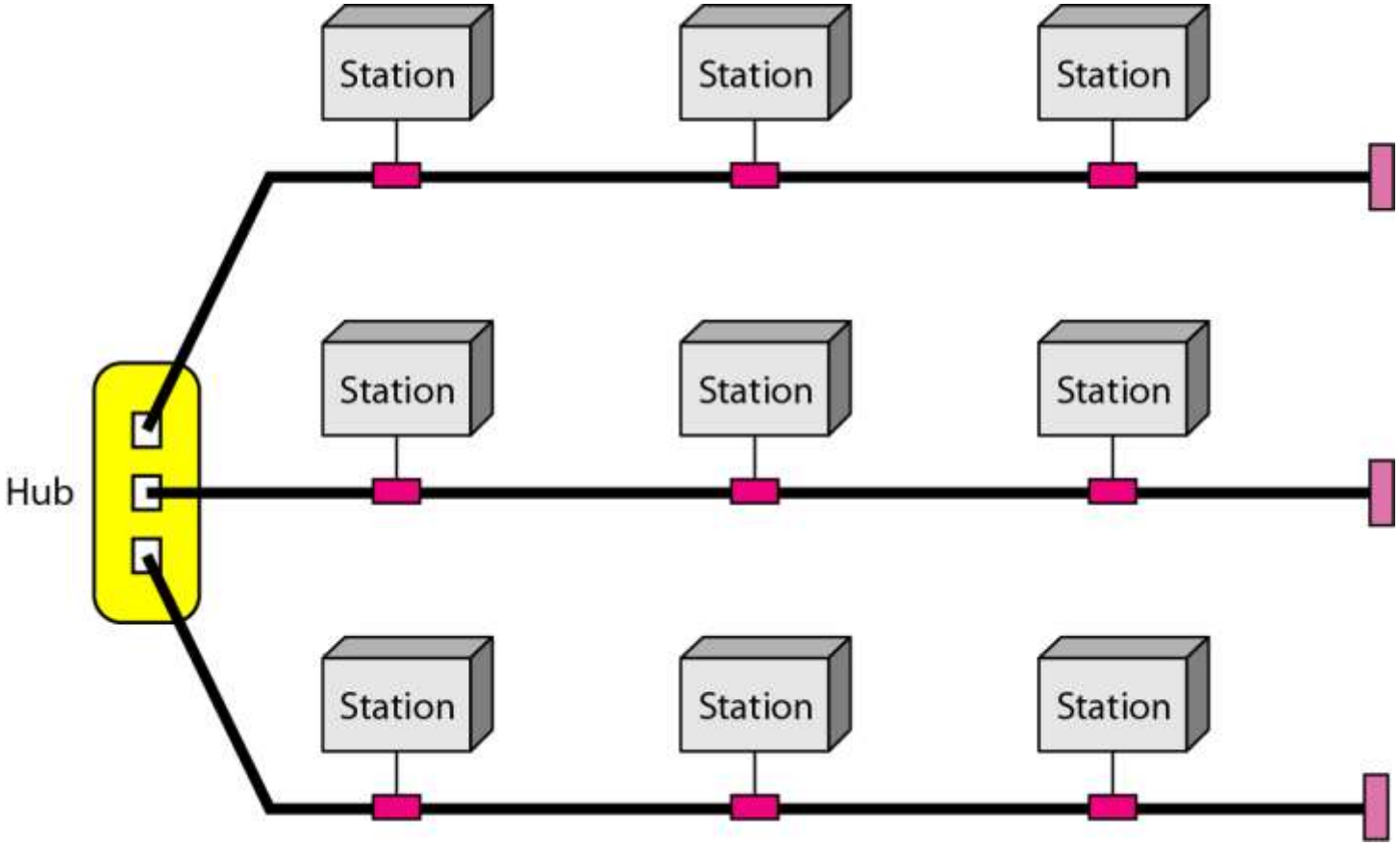
Figure 1.8 *A ring topology connecting six stations*



Ring Topology

- Each device has a dedicated point-to-point connection only with the two devices on either side of it.
- Each device in the ring incorporates a repeater
- The repeater regenerates the bits and passes them to destination
- **Advantages**
  - Easy to install and reconfigure
  - To add or delete a device requires changing only two connections
  - Fault isolation is simplified
- **Disadvantages**
  - Unidirectional traffic
  - Break in ring can disable the entire network

Figure 1.9 *A hybrid topology: a star backbone with three bus networks*



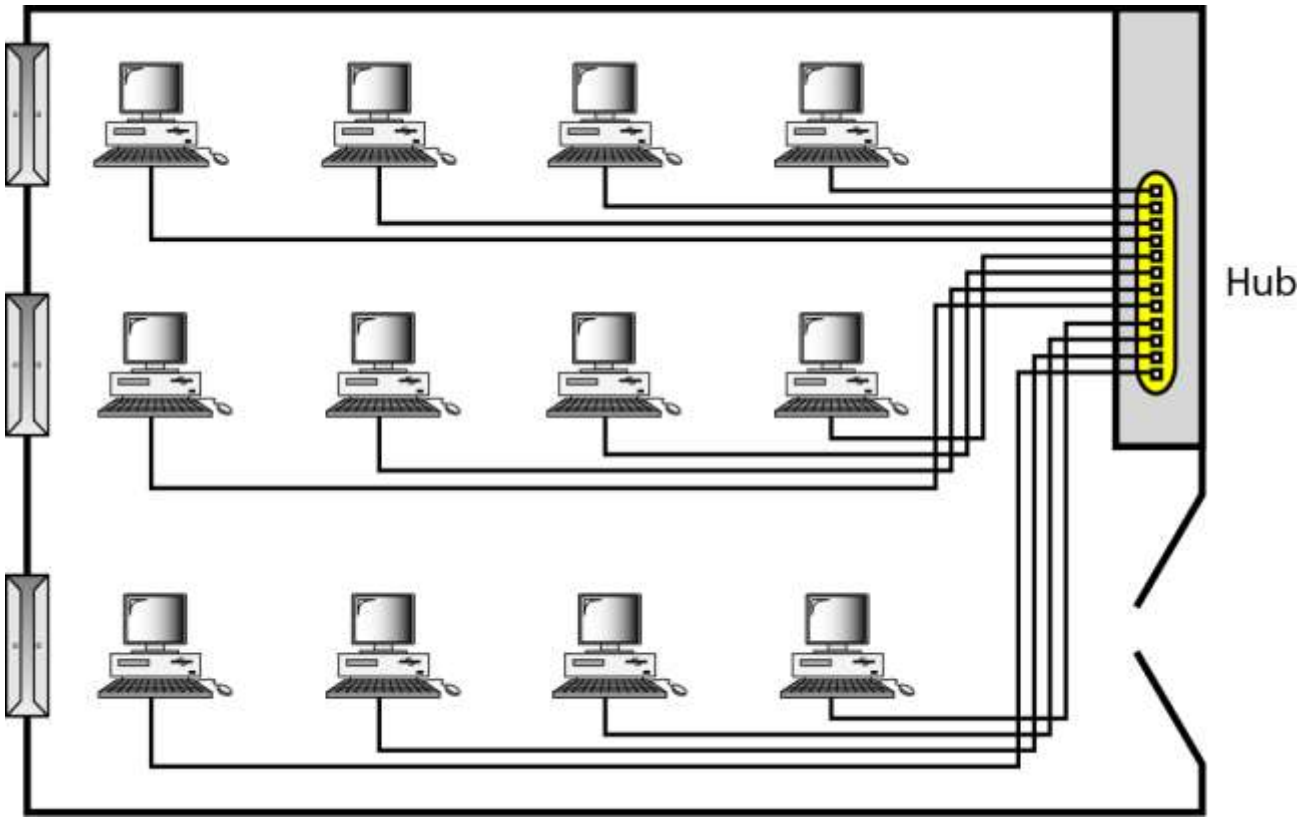
5. Categories of Networks

- Determined by
  - Size
  - Ownership
  - Distance
  - Physical architecture
- **LAN**
- **MAN**
- **WAN**

LAN- Local Area Networks

- Privately owned
- For a single office, building
- Size is limited to a few kilometers
- Resource shared between PC and workstation
- SW can store in central server

Figure 1.10 *An isolated LAN connecting 12 computers to a hub in a closet*



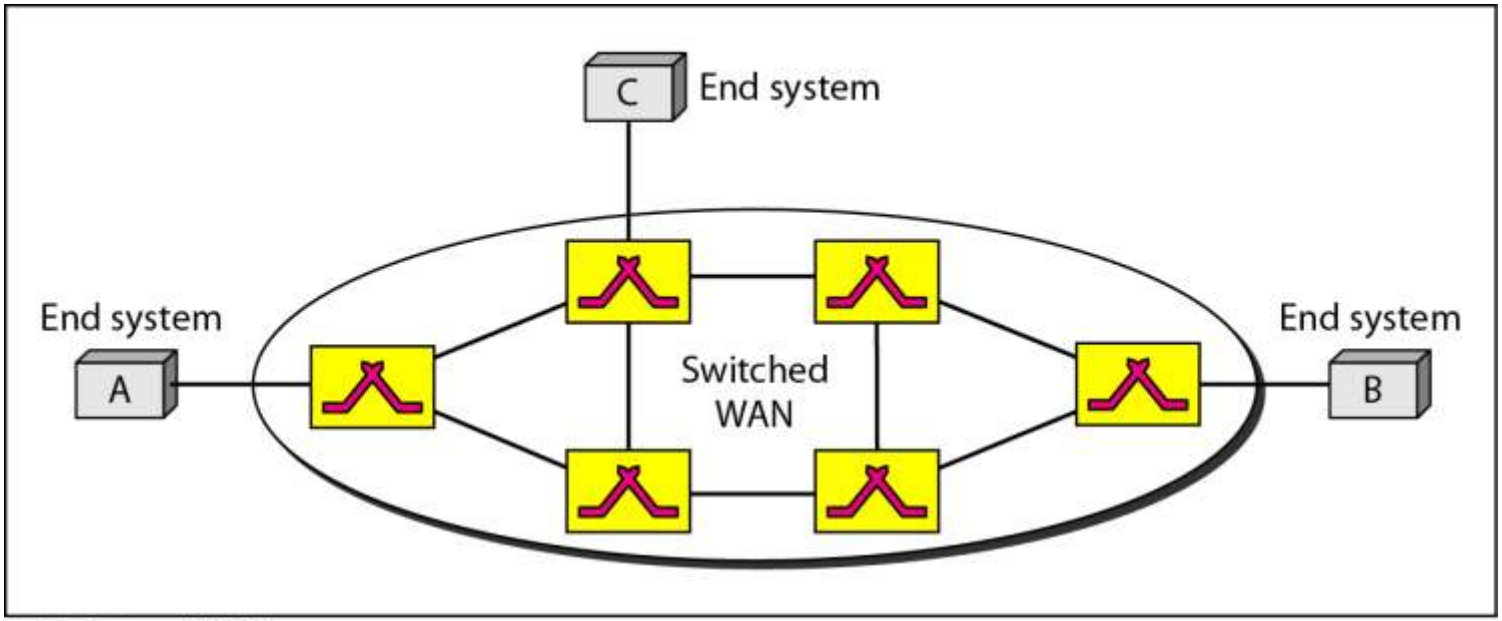
MAN – Metropolitan Area Network

- MAN is designed to extend over an entire city.
  - Ex: Cable Television Network
- Connecting several LANs
  - Company network in city
- Owned by privately or public company
- Many telephone companies provide a popular MAN service called Switched Multi-megabit Data Services (SMDS)

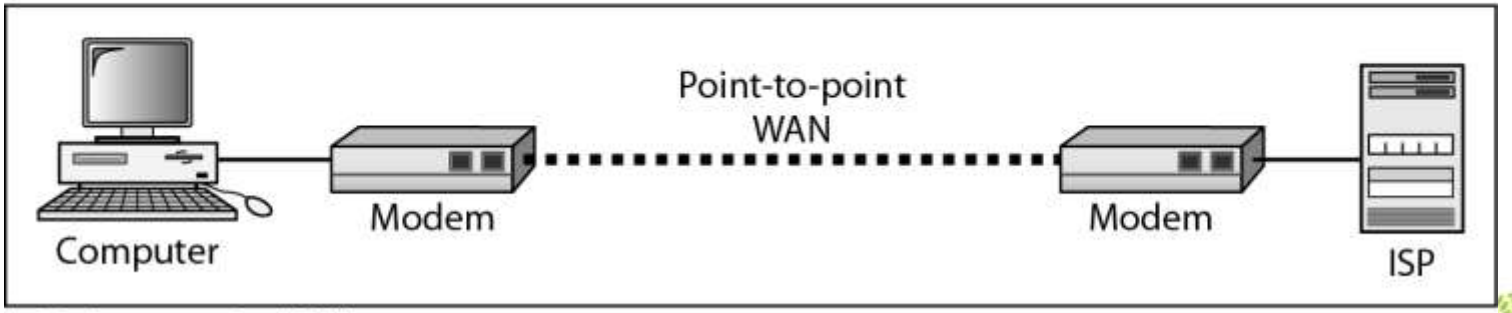
WAN-Wide Area Network

- WAN provides long-distance transmission of data, voice, image and video information
- WANs may utilize public or private communication equipment
- A WAN that is owned and used by a single company is often referred to as an *enterprise network*.

Figure 1.11 *WANs: a switched WAN and a point-to-point WAN*

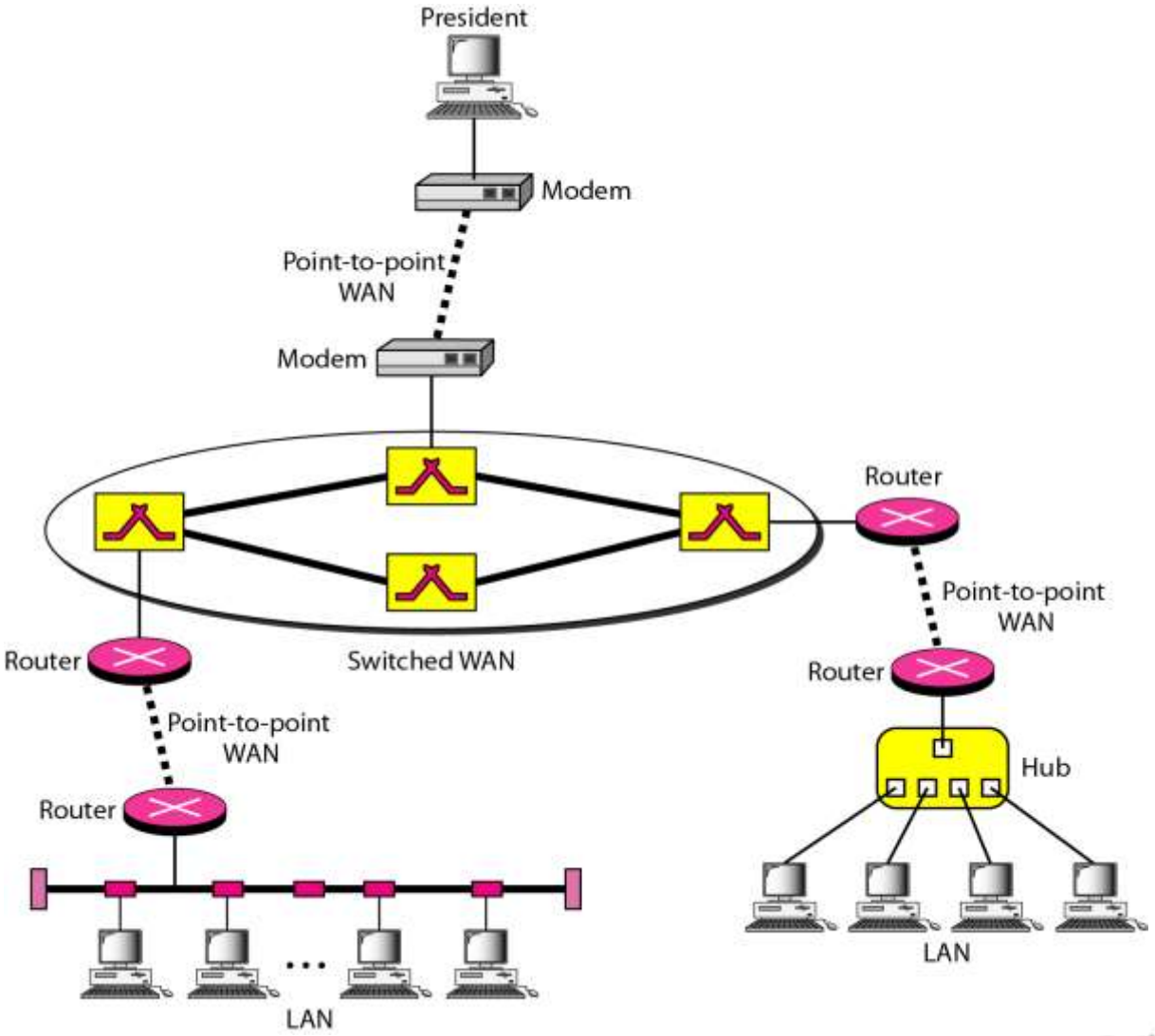


a. Switched WAN



b. Point-to-point WAN

Figure 1.12 *A heterogeneous network made of four WANs and two LANs*



1-3 PROTOCOLS AND STANDARDS

Topics discussed in this section:

Protocols
Standards
Standards Organizations
Internet Standards

Dr. Chandrappa S
NAGARJUNA
COLLEGE OF ENGINEERING & TECHNOLOGY

Protocols

- It is a set of rules that governs data communications.
- A protocol defines
  - What is communicated,
  - How it is communicated and
  - When it is communicated
- Key elements of a protocol are
  - Syntax
    - Refers to structure of data

  - Semantics
    - Meaning of each section of bits
  - Timing
    - Refers to two characteristics
      - When data should be sent
      - How fast they can be sent

Standards

- Data communication standards fall into two categories
  - De facto
    - Standards that have not been approved by an organized body
  - De jure
    - Those that have been legislated by an officially recognized body are de jure standards (ANSI)

Standards Organizations

- ISO (International Organization for Standardization)
- ITU-T (International Telecommunication Union)
  - CCITT (Consultative Committee for International Telegraphy and Telephony)
- ANSI (American National Standards Institute)
- IEEE (Institute of Electrical and Electronics Engineers)
- EIA (Electronic Industries Association)

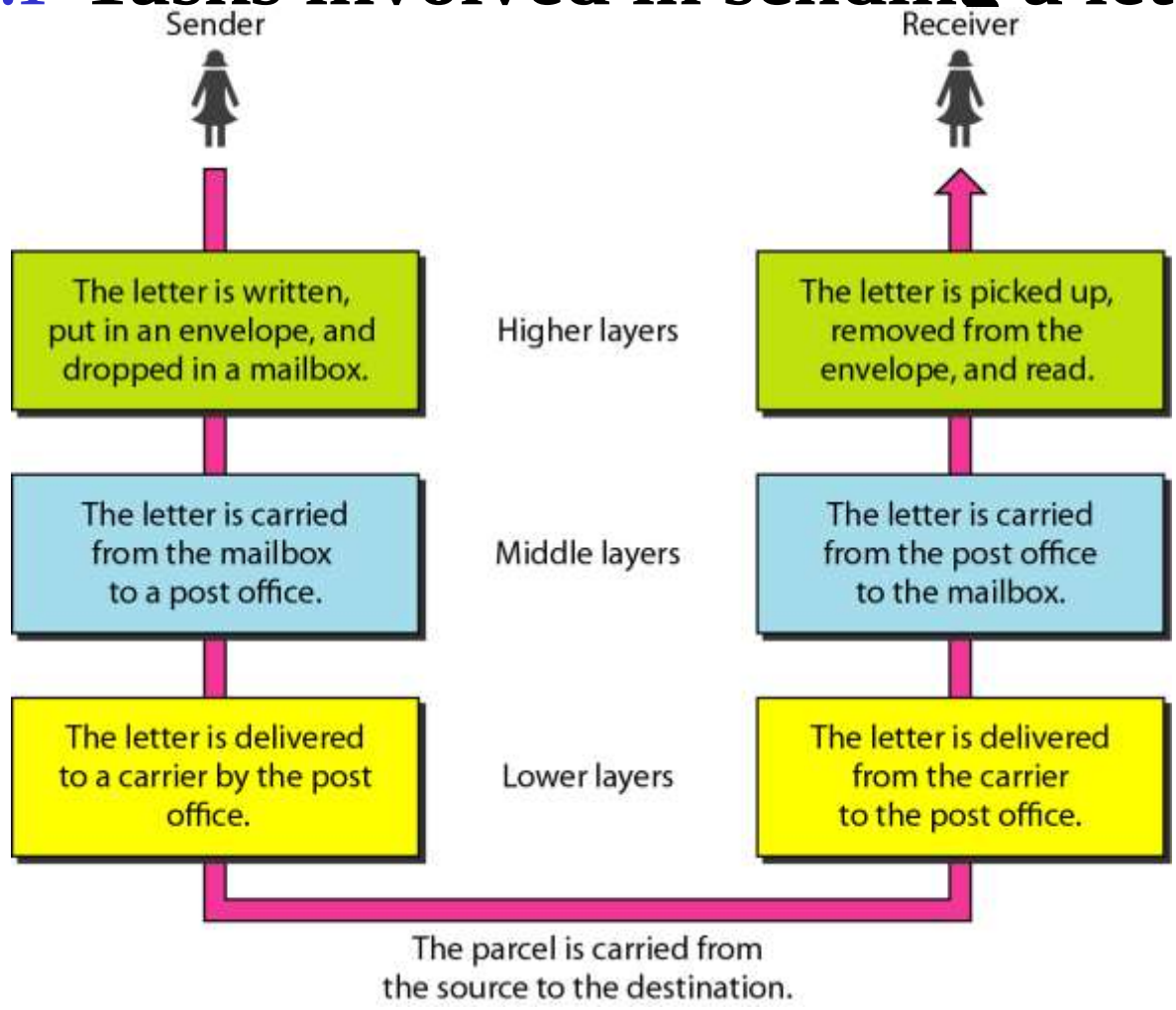
Chapter 2

Network Models

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

2-1 LAYERED TASKS

Figure 2.1 Tasks involved in sending a letter

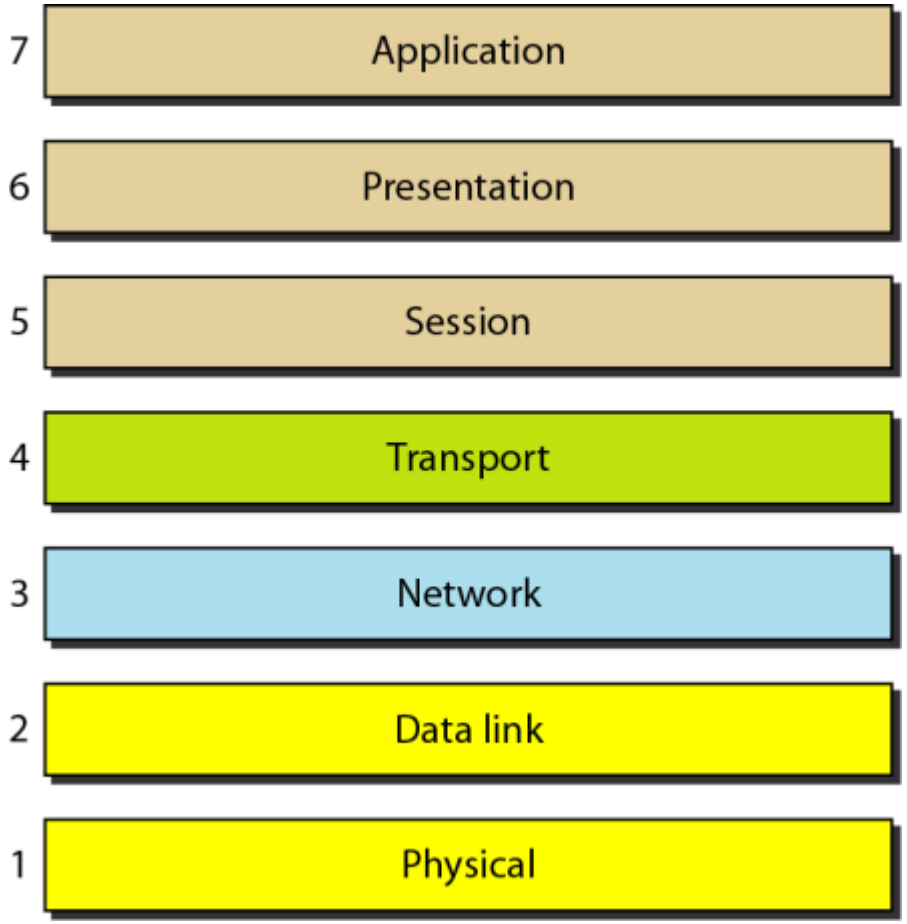


2-2 THE OSI (Open System Interconnection) MODEL

1. ***Developed by ISO (International Standard Organization)***
2. ***It was first introduced in the year 1970s.***
3. ***Open System refers to a set protocols that allows two computers to communicate regardless of underlying architecture.***
4. ***OSI is not a protocol; but it is a model for understanding network architecture that is robust and flexible.***

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

Figure 2.2 *Seven layers of the OSI model*



Provides User interface operations, data generation, processing, maintenance, transmission and reception

Designed to handle the data translation, encryption and decryption

Designed to establish, maintain and synchronize session

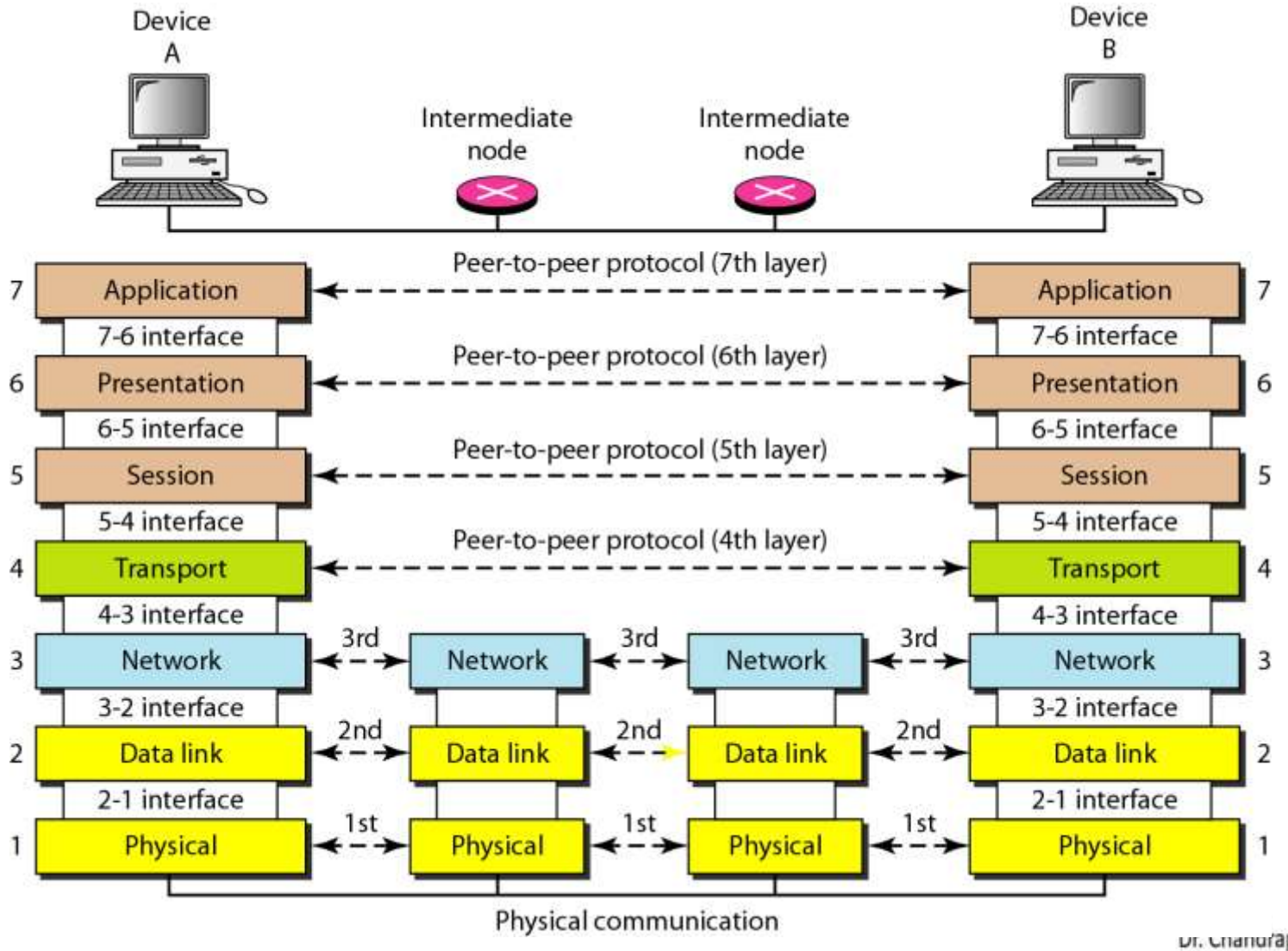
converting message into transmittable segment and transforming segments

Generates package from segment, Add source and destination IP address

Generates frame from packet, Add source and next node mac address

Convert frame into bits

Figure 2.3 *The interaction between layers in the OSI model*



- The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7).
- Figure 2.3 shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.
- Each layer defines functions which are distinct from other layers.
- Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.
- Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is governed by an series of rules called **protocols**. The processes on each machine that communicate at a given layer are called **peer-to-peer processes**
- **Interfacing:** each pair of adjacent layers are interfaced.
- It helps for exchange of the data and network information
- **Organization of layers**: Layers 1, 2, and 3-physical, data link, and network-are network support layers;
- Layers 5, 6, and 7-session, presentation, and application-are user support layers;
- Layer 4, the transport layer, links the two subgroups

Application (7)	SMTP, FTP, Telnet
Presentation (6)	Format Data, Encryption
Session (5)	Start & Stop Sessions
Transport (4)	TCP, UDP, Port Numbers
Network (3)	IP Address, Routers
Data Link (2)	MAC Address, Switches
Physical (1)	Cable, Network Interface Cards, Hubs

Dr. Chandrappa S
NAGARJUNA
COLLEGE OF ENGINEERING & TECHNOLOGY

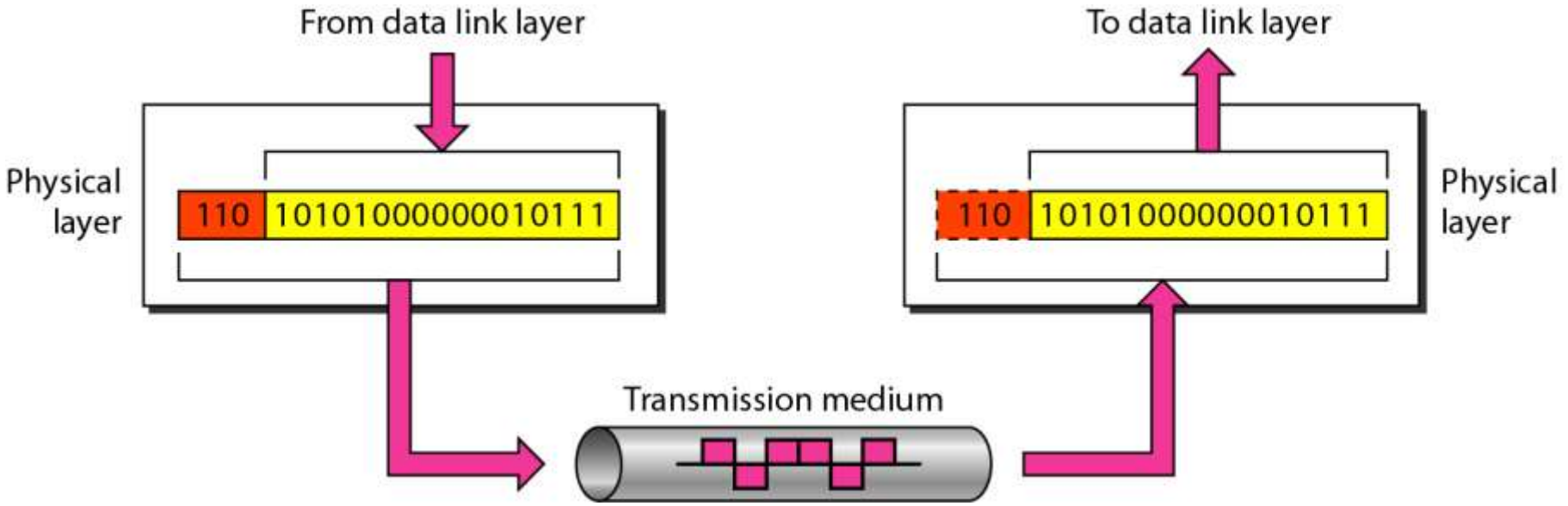
2-3 LAYERS IN THE OSI MODEL

Topics discussed in this section:

Physical Layer
Data Link Layer
Network Layer
Transport Layer
Session Layer
Presentation Layer
Application Layer

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

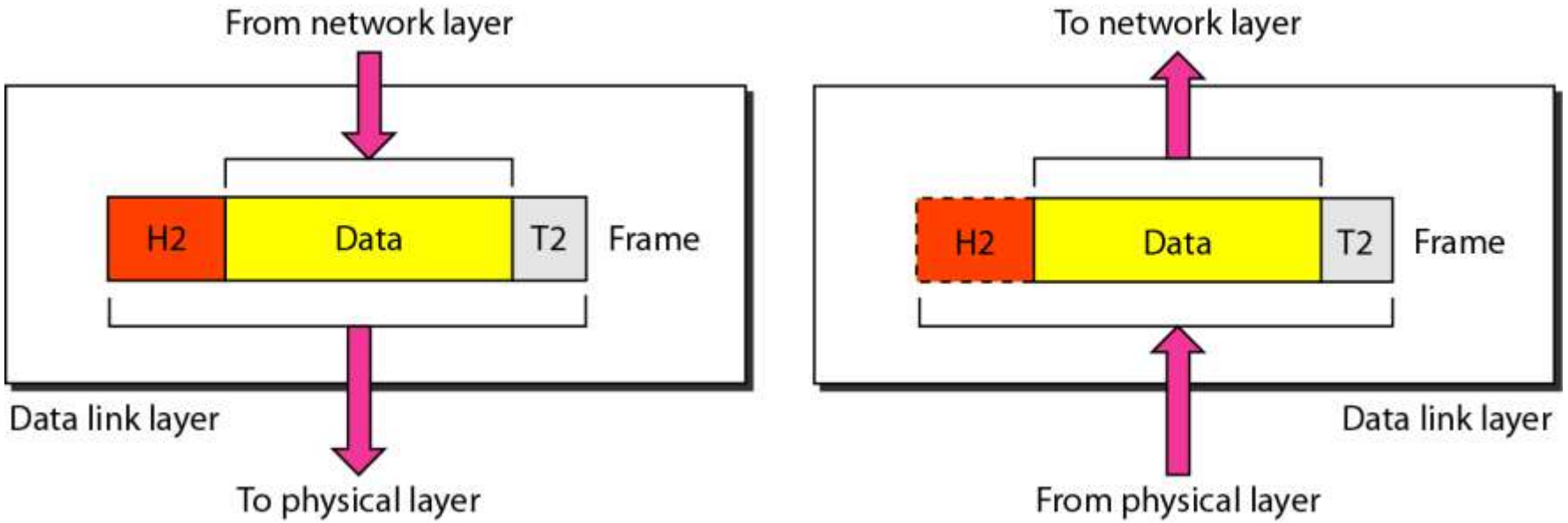
Figure 2.5 *Physical layer*



Physical layer functionalities

- **Define Physical characteristics of interfaces and medium.** Defining the Characteristics of the interface between the devices and the transmission medium.
- **Representations of the bits** : Sequences of 1's and 0's and encoding these bits into signals.
- **Data rate :** No. of bits send per second
- **Line Configuration :** defines how the devices are connected to the media.
  - Point to point
  - Multi point
- **Physical Topology :** Defines the structure of a network.
- **Transmission mode:** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Figure 2.6 *Data link layer*



Data link layer functionalities

Responsible for hop to hop delivery

- **Framing :** The data link layer **divides the stream of bits** received from the network layer **into manageable data units called frames**.
- **Physical Addressing :** Adding sender and receiver addressing information to the frame
- **Flow Control :** if rate of data absorbed by receiver is less than rate of data sent by sender then **it will Control the flow of data to avoid bottleneck.**
- **Error Control : detect and retransmit damaged or lost frames.** It also uses a mechanism to recognize duplicate frames.
- **Access Control :** when two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has the control over the link.

Node-to-node delivery

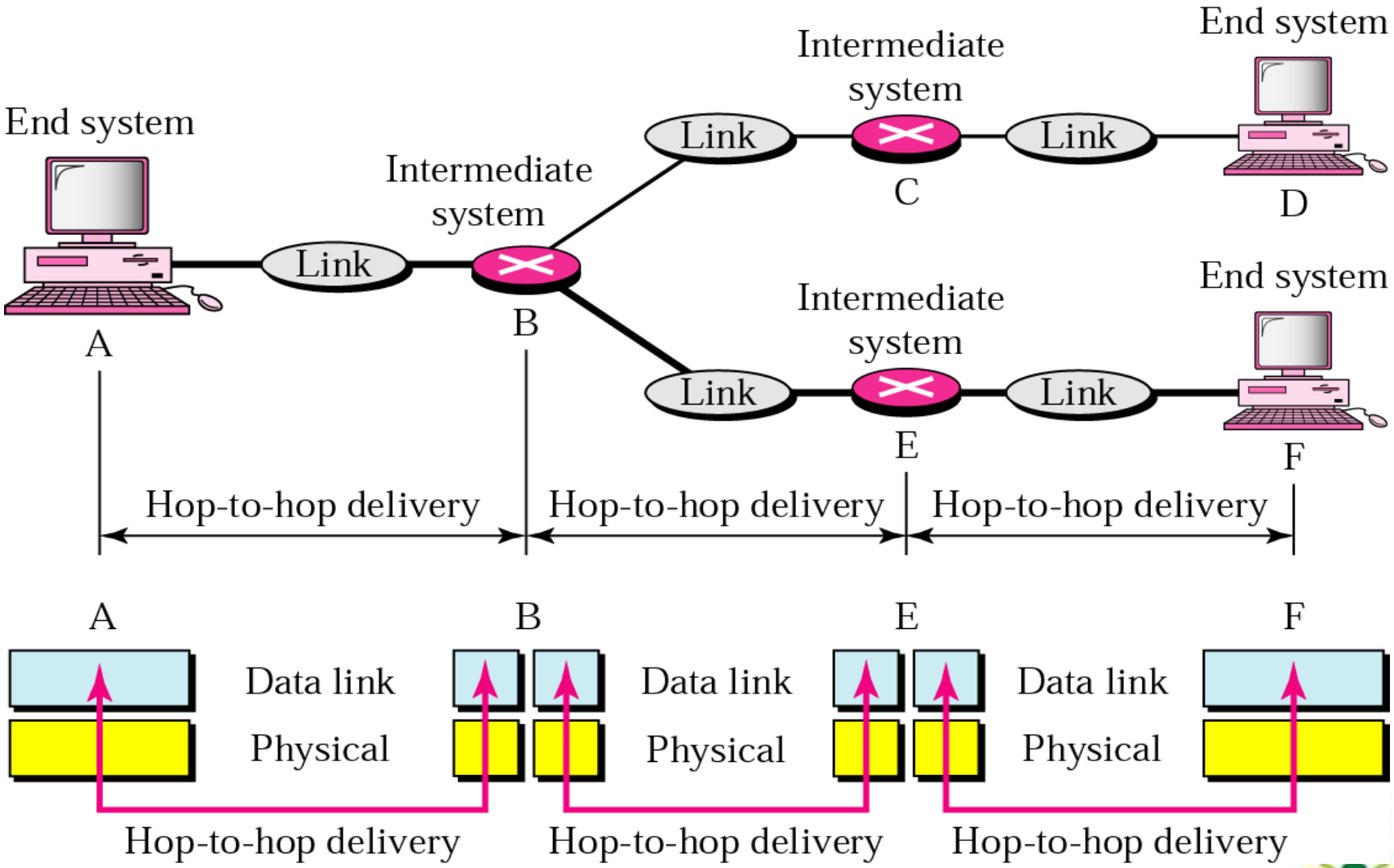
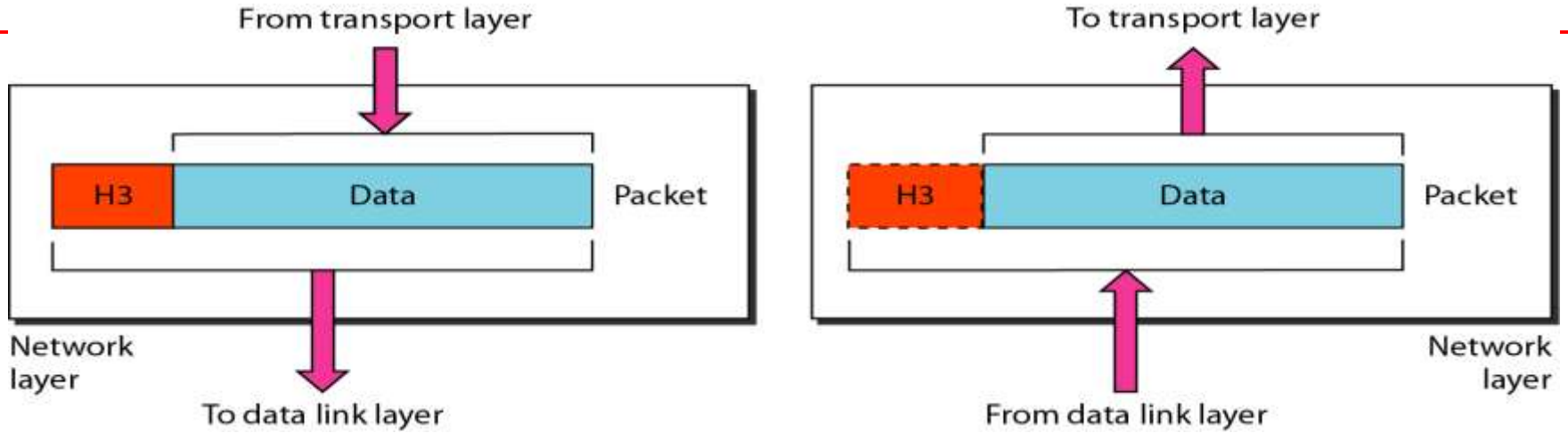


Figure 2.8 *Network layer*



- **The network layer is responsible for creating a connection between th e source computer and the destination computer. The communication at the network layer is host-to-host**
- **The network layer is responsible for the delivery of packets from the o riginal source to the final destination.**
- **Network layer is responsible for host-to-host communication and routi ng the packet through possible routes.**
- **The network layer in the Internet includes the main protocol, Internet Protocol (IP), that defines the format of the packet, called a datagram a t the network layer.**

Network layer functionalities

- **Responsible for source to destination delivery of packet across multiple networks/l**inks**.**
- **Logical Addressing :** Adding sender and receiver addressing information to the Packet.
- **Routing** : Forwarding the packets to destination using the networks/links. Router or switches are responsible for forwarding these packets to destination station.
- IP is a **connectionless protocol that provides no flow control, no error control, and no congestion control services.**
- The network layer also includes unicast (one-to-one) and multicast (one-to-many) routing protocols.

- The Internet Control Message Protocol (ICMP) helps IP to report some problems when routing a packet.
- The Internet Group Management Protocol (IGMP) is another protocol that helps IP in multitasking.
- The Dynamic Host Configuration Protocol (DHCP) helps IP to get the network-layer address for a host.
- The Address Resolution Protocol (ARP) is a protocol that helps IP to find the link-layer address of a host or a router when its network-layer address is given.

Figure 2.9 *Source-to-destination delivery*

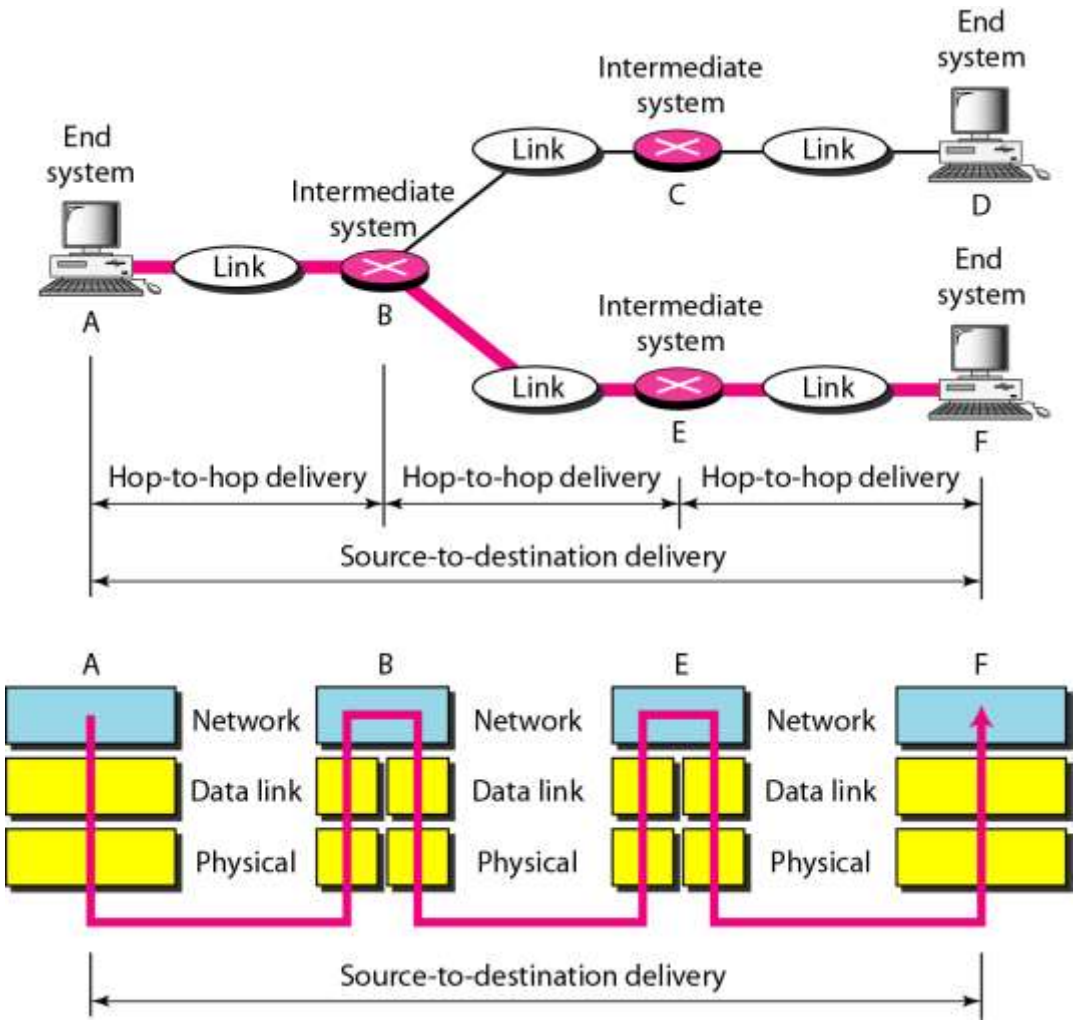
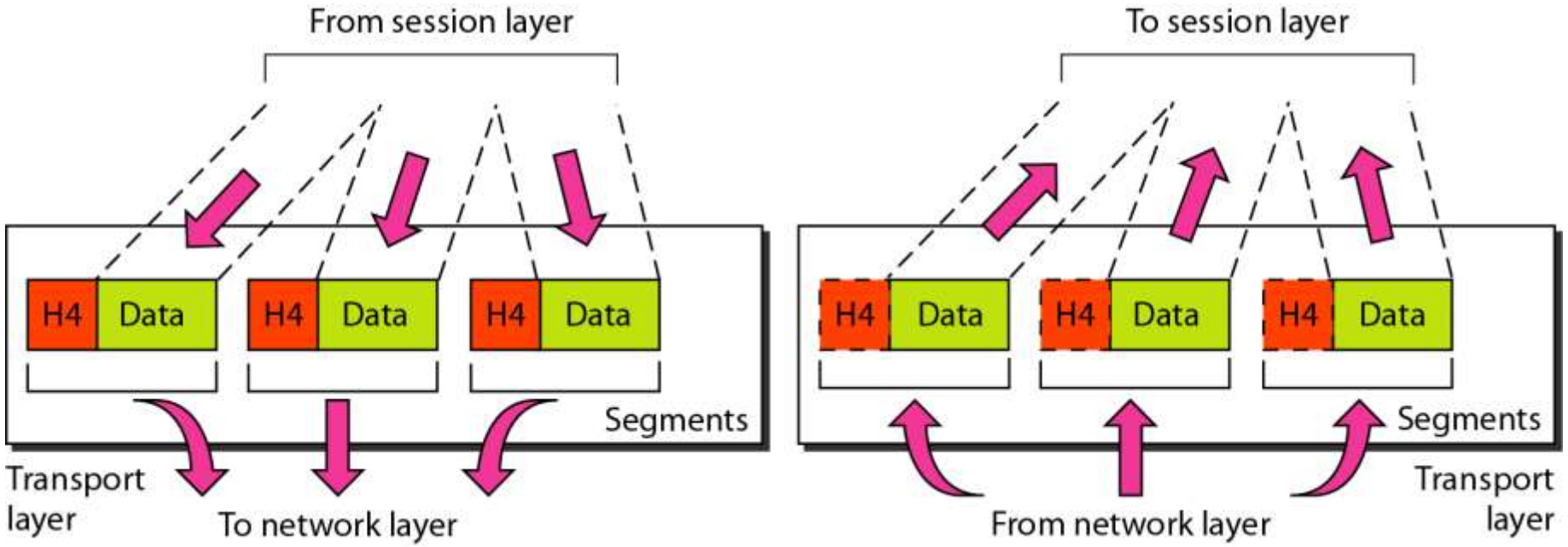


Figure 2.10 *Transport layer*



Transport layer functionalities

- **Responsible for process to process delivery**
- **Service Point Addressing/port addressing :** Specifying port address of receiver process.
- **Segmentation and Reassembly :** Dividing a message into transmittable segments, with each segments containing a sequence number.
- **Connection Control :**
  - **Connection Oriented:** Transmission Control Protocol (TCP), is a connection-oriented protocol that first establishes a logical connection between transport layers at two hosts before transferring data
  - **Connection less:** User Datagram Protocol (UDP), is a connectionless protocol that transmits user datagrams without first creating a logical connection.
- **Flow Control :** TCP provides flow control (matching the sending data rate of the source host with the receiving data rate of the destination host to prevent overwhelming the destination)
- **Error Control :** to guarantee that the segments arrive at the destination without error and resending the corrupted ones
- Congestion control to reduce the loss of segments due to congestion in the network
- UDP is a simple protocol that does not provide flow, error, or congestion control

Figure 2.11 *Reliable process-to-process delivery of a message*

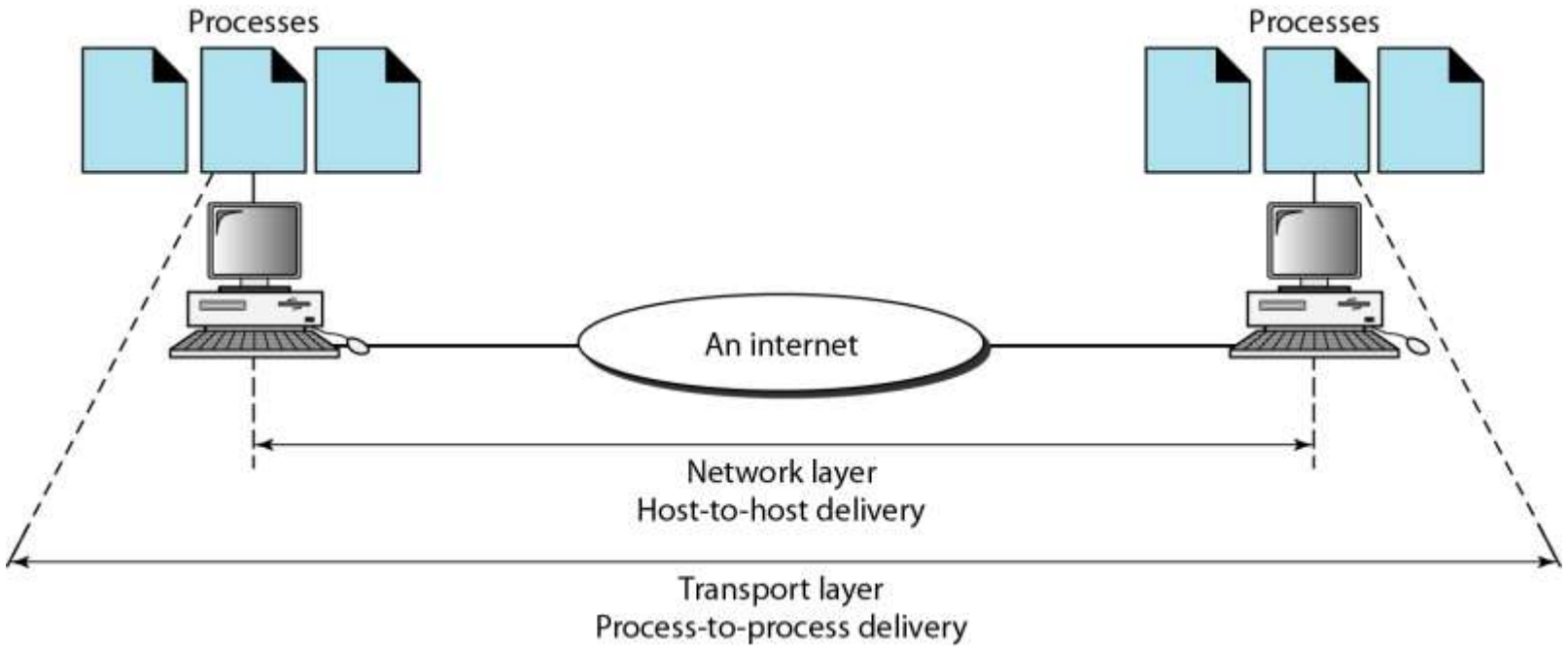
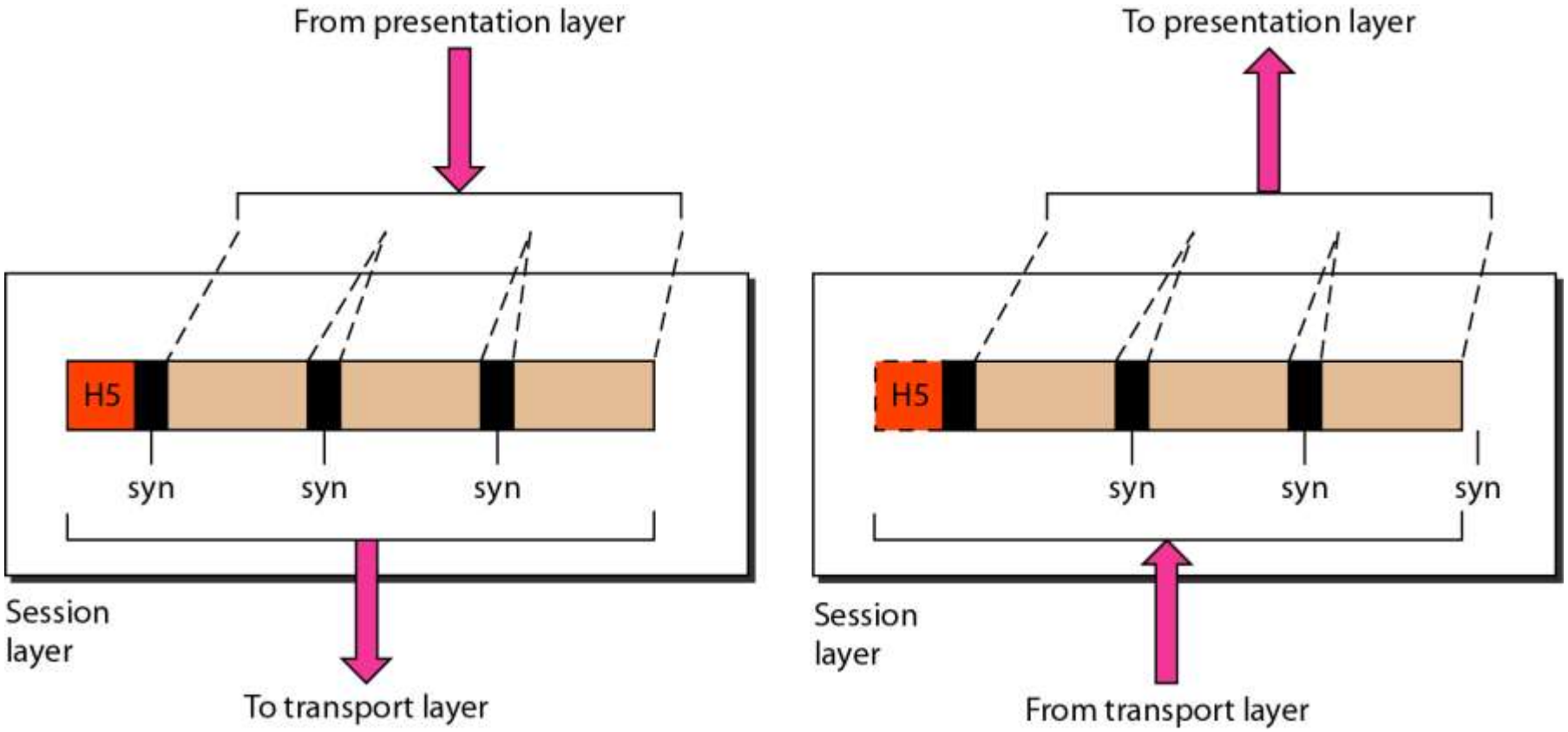


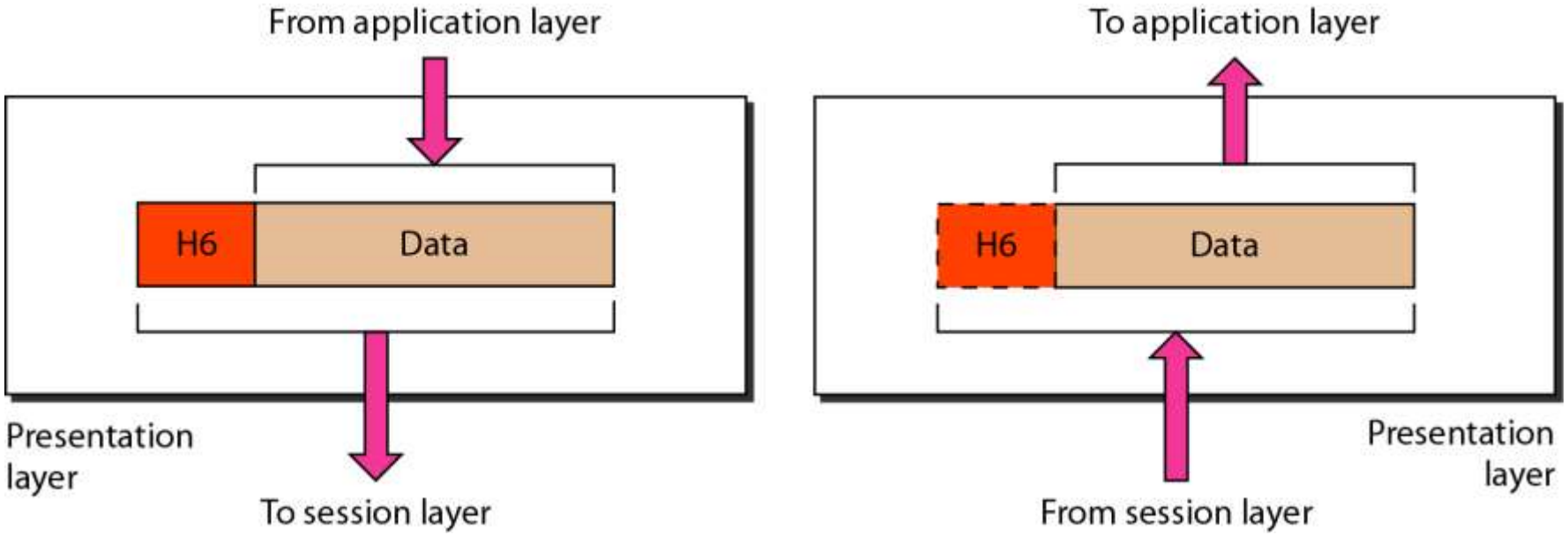
Figure 2.12 *Session layer*



Session layer functionalities

- **It establishes , maintaining and synchronizes the interaction among communicating systems. It is called dialog controller**
- **Dialog Control :** It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization :** Adding the check points to the data. Ensure that each data unit is received and acknowledged independently.

Figure 2.13 *Presentation layer*

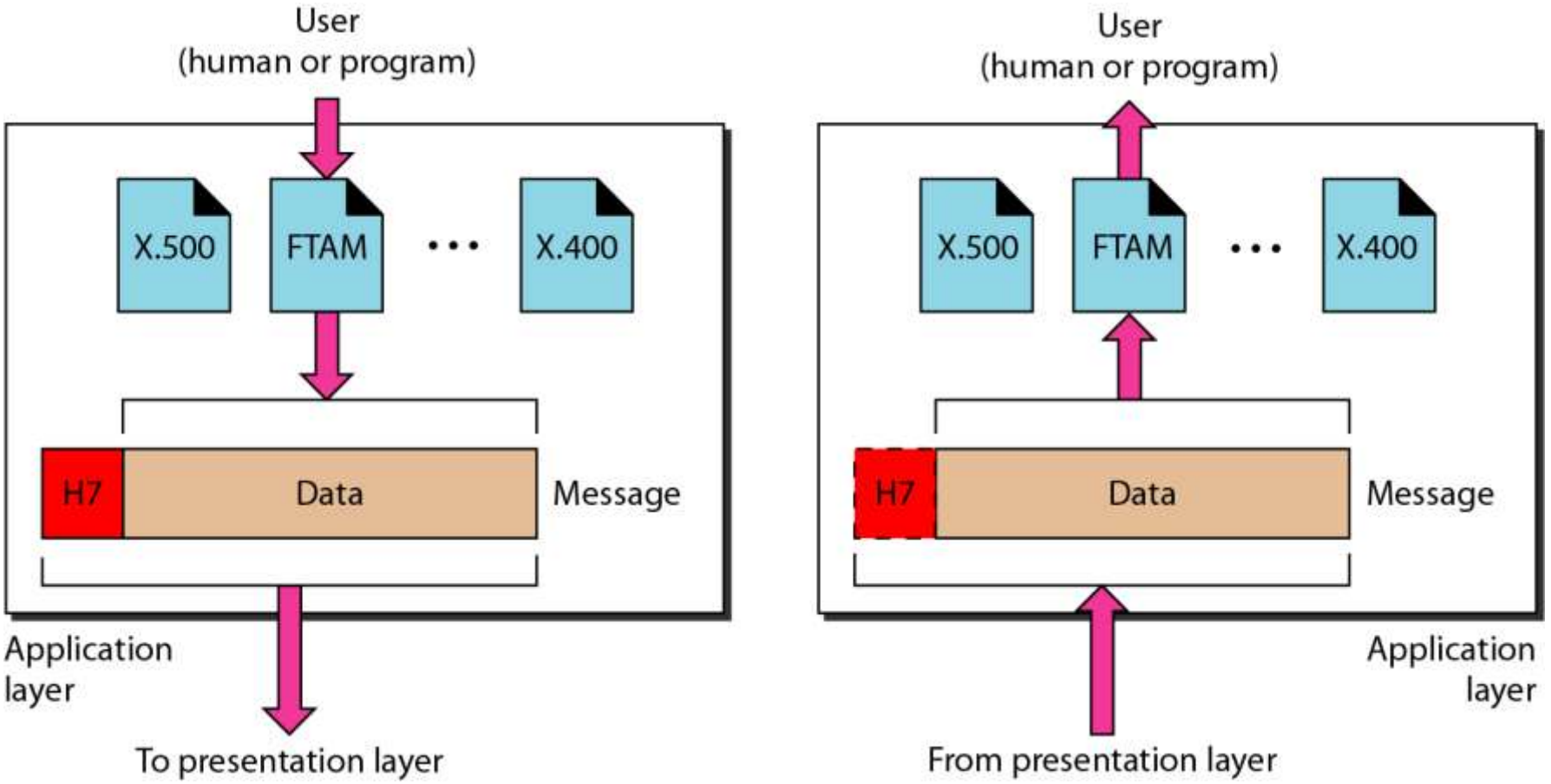


Presentation layer functionalities

- **Translation :** Changing information of the sender into its receiver – dependent format.
- **Encryption :** Sending original information in another form for security of the information.
- **Compression:** Reducing the data size for effective transmission.

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

Figure 2.14 *Application layer*



Application layer functionalities

- **It provides user interfaces and support for services such as electronic mail , remote file access and transfer.**
- **File Transfer ,access and management :** Allowing user to access remote computer files.
- **Mail Services :** Email forwarding and storage.

The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.

Ex: The Hypertext Transfer Protocol (HTTP) is a vehicle for accessing the World wide Web (WWW).
The Simple Mail Transfer Protocol (SMTP) is the main protocol used in ele ctronic mail (e-mail) service.
The File Transfer Protocol (FTP) is used for transferring files from one hos t to another.
The Terminal Network (TELNET) and Secure Shell (SSH) are used for ac cessing a site remotely.
The Domain Name System (DNS) is used by other protocols to find the net work-layer address of a computer.
The Simple Network Management Protocol (SNMP) is used by an administ rator to manage the Internet at global and local levels

Encapsulation and Decapsulation

Figure 2.8 *Encapsulation/Decapsulation*

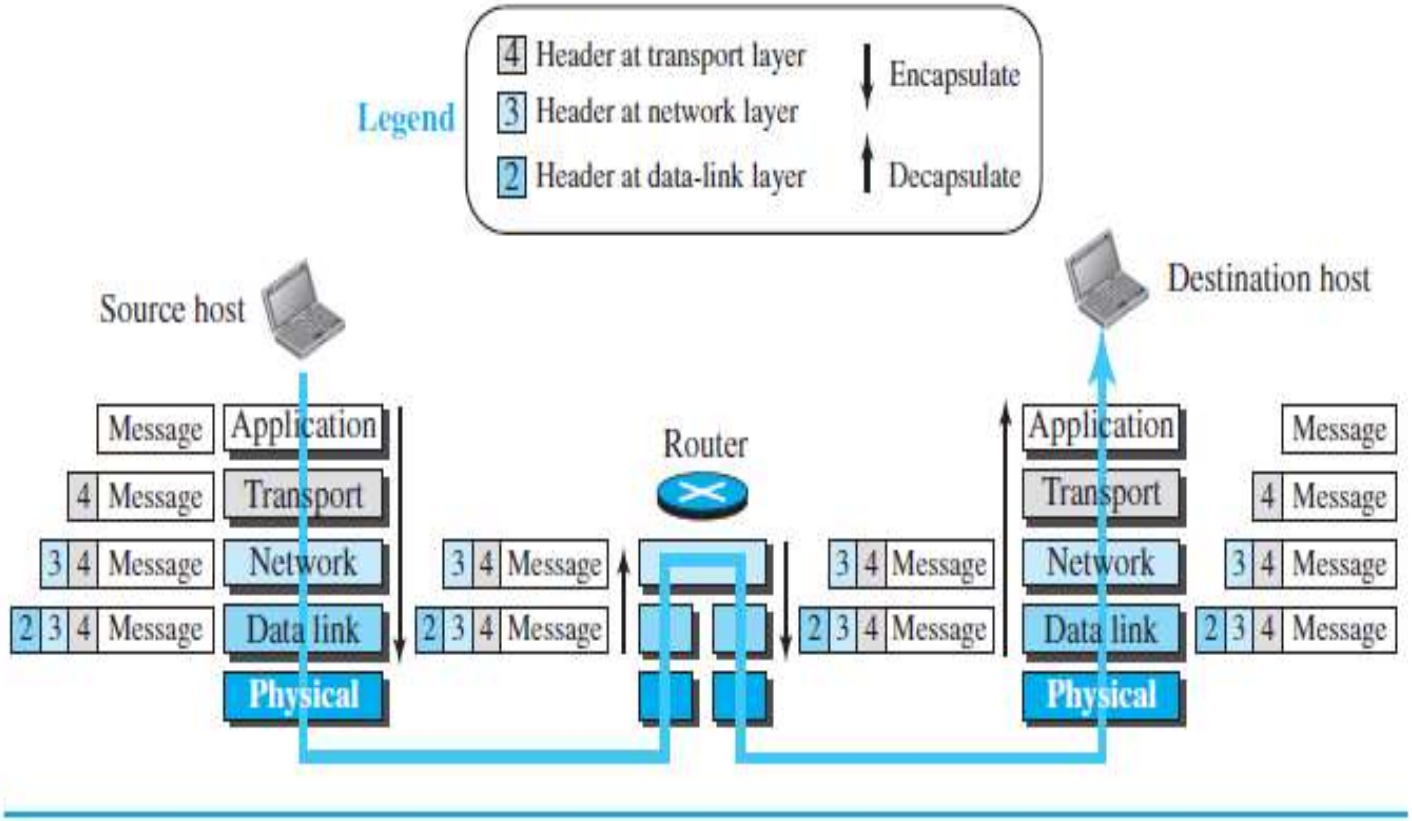
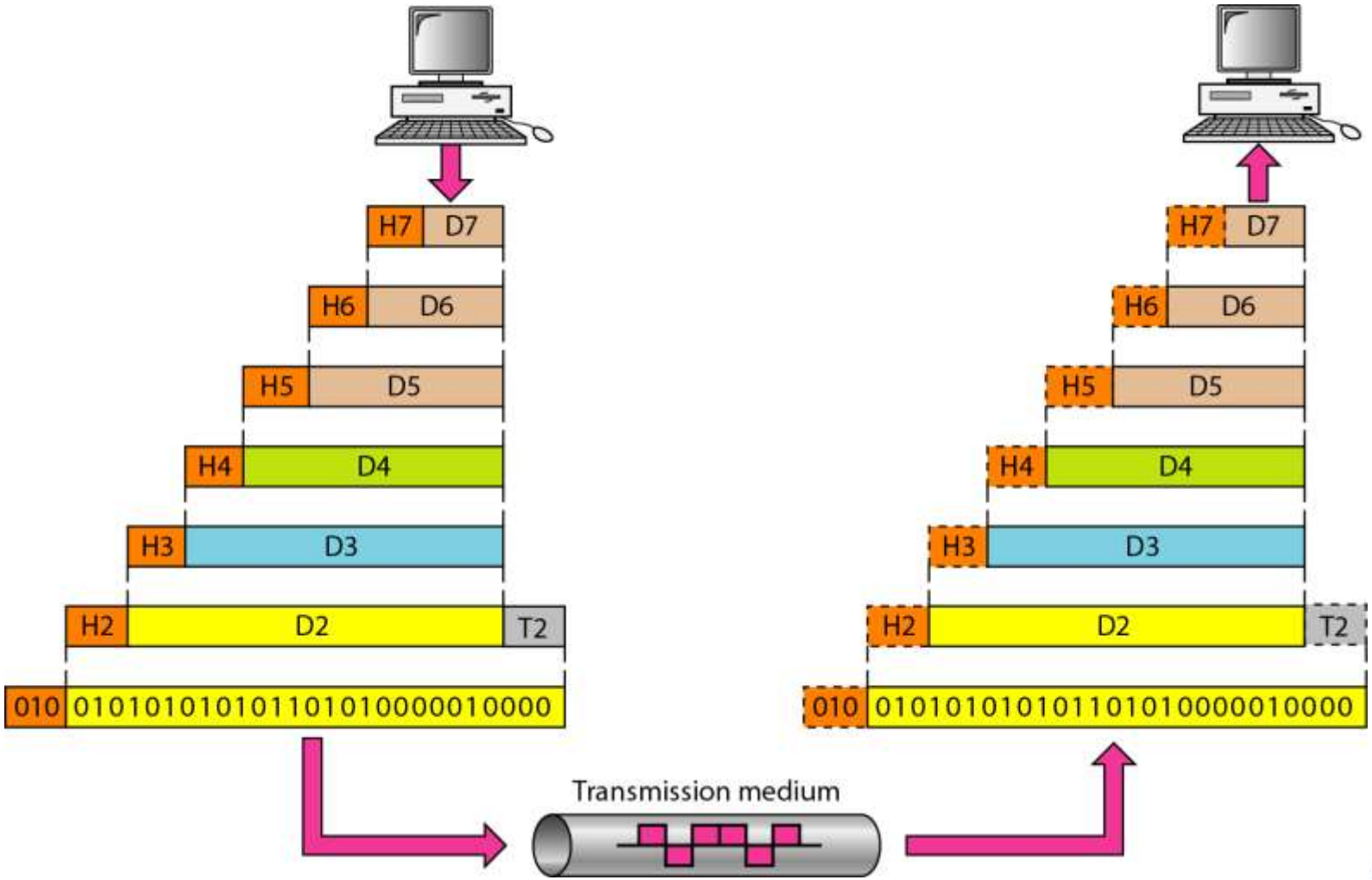


Figure 2.4 *An data exchange using the OSI model-Encapsulation and DE capsulation*



Encapsulation at the Source Host

At the source, we have only encapsulation.

1. **At the application layer, the data to be exchanged is referred to as a *message. A*** message normally does not contain any header or trailer, we refer to the whole as the message. The message is passed to the transport layer**.**

2. **The transport layer takes the message as the payload,** the load that the transport layer should take care of.

- It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-to end delivery of the message, such as information needed for flow, error control, or congestion control.

3.The network layer takes the transport-layer packet as data or payload and adds its own header to the payload.

The header contains the addresses of the source and destination hosts and some more information used for error checking of the header, fragmentation information, and so on.

4. **The data-link layer takes the network-layer packet as data or payload and adds its** own header, which contains the link-layer addresses of the host or the next hop (the router).

Decapsulation and Encapsulation at the Router

1. **After the set of bits are delivered to the data-link layer, this layer decapsulates the** data from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the data is to be delivered.
3. The datagram is then passed to the data-link layer of the next link
4. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host

- At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer.

2-4 TCP/IP PROTOCOL SUITE

- *It is also called Internet Protocol Suite, consists of set of communication protocols used for the Internet and other similar networks.*
- *Two most important Protocols : TCP & IP.*
- *The original TCP/IP protocol suite consisting four layers:*

1. *host-to-network layer → physical + data link layer of OSI*
2. *Internet → Network Layer of OSI*
3. *Transport → Transport layer of OSI.*
4. *application→ Session + Presentation + application of OSI model.*

Figure 2.4 *Layers in the TCP/IP protocol suite*

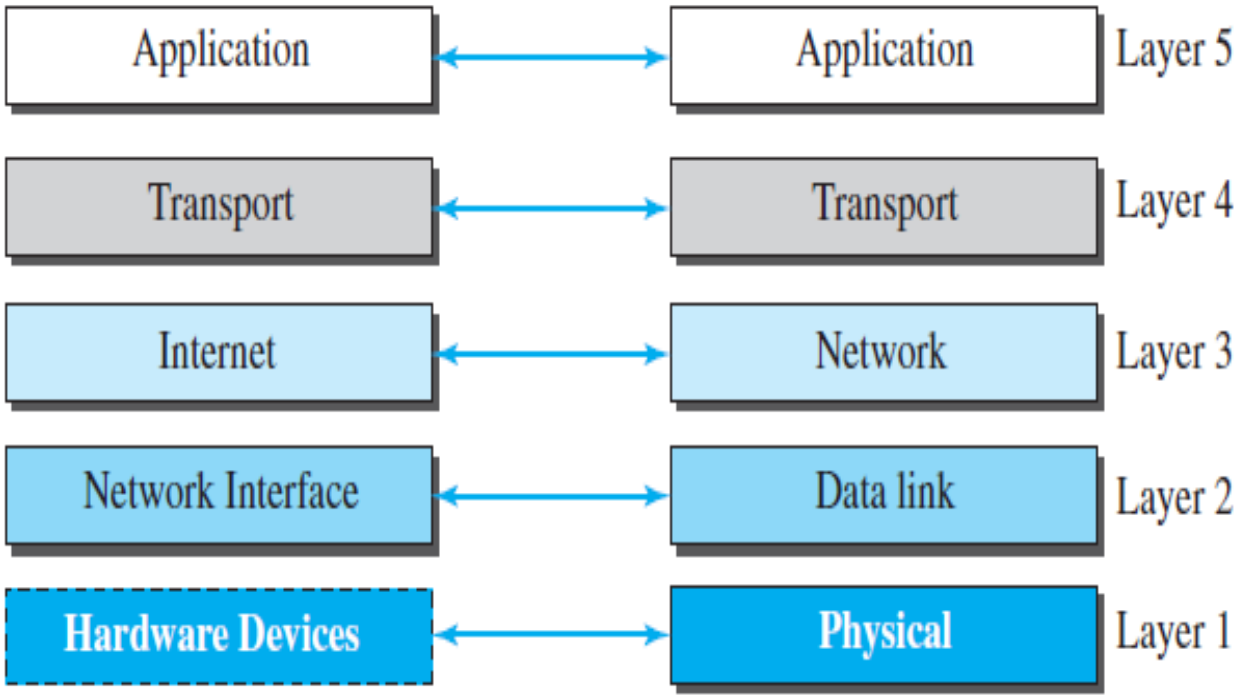
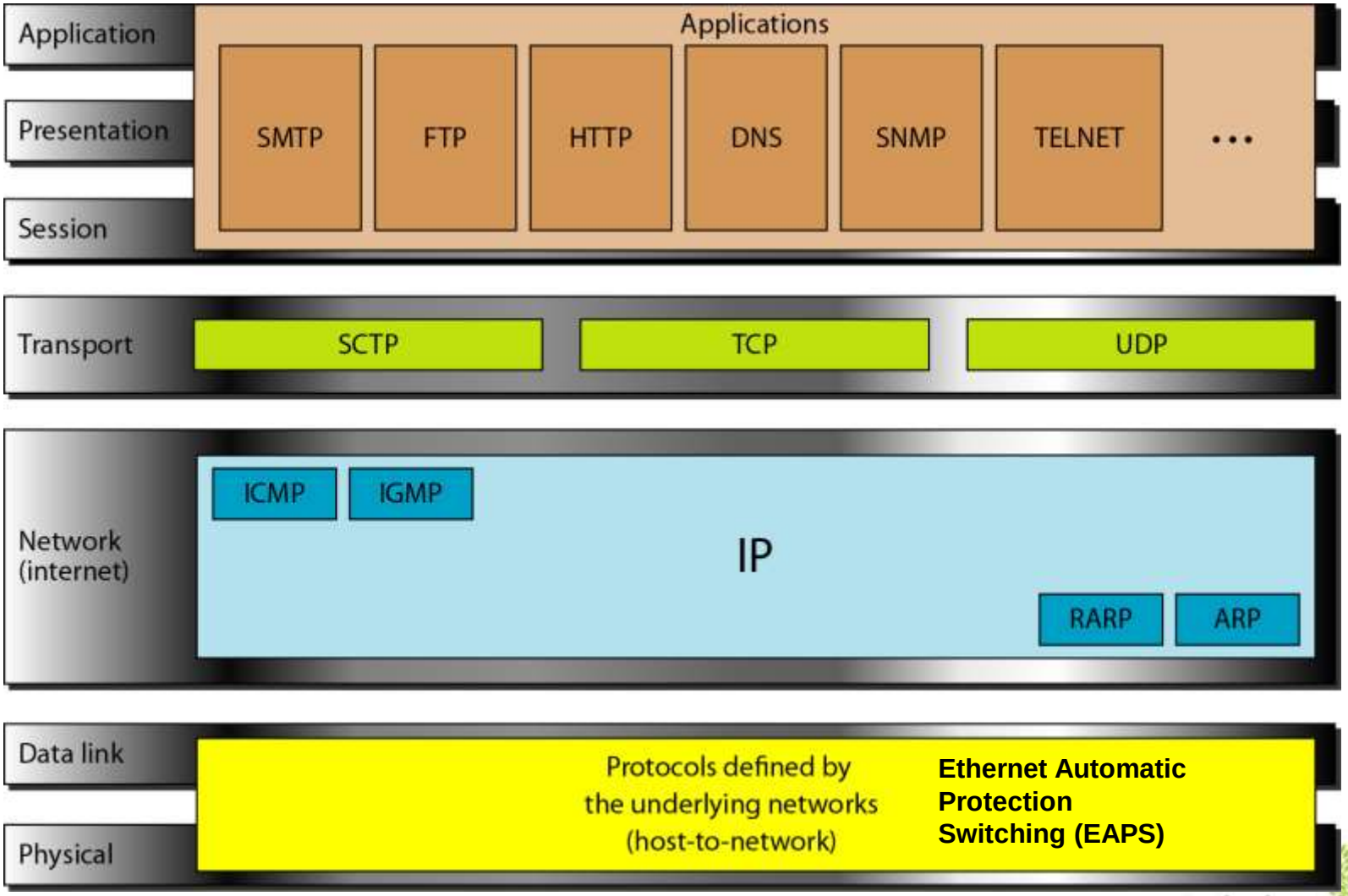


Figure 2.16 *TCP/IP model*



TCP/IP Layers

- **Physical and Data Link Layers :**
  It supports all the standard protocols
- **Network Layers :**
  - **Internet Protocol (IP) :** Used to send datagram (packets) from the source host to the destination host based on its address.
    - **Unreliable and connection less**
    - **IP data is called datagrams**
  - **Address Resolution Protocol (ARP) :** Used to find physical address when its internet address is known.
  - **Reverse Address Resolution Protocol (RARP):** Used to find internet address when its physical address is known.
- **Internet Control Message Protocol (ICMP) :**used by hosts and gateways to send notification of datagram problems back to the sender **.** Used to send query and error reporting messages.
- **Internet Group Message Protocol: The** Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

TCP/IP Layers

- **Transport Layers : UDP and TCP protocols** responsible for delivery of a message from a process (running program) to another process
  - **User Datagram Protocol :** Used to send short messages sometimes known as datagram. Process to Process protocol that adds only port address , checksum , error control and length information to the data.
    - **UDP does not guarantee reliability or ordering**
  - **Transmission Control Protocol :**
    - **Connection oriented and reliable**
    - **Data is called segments**
    - **reordering of the segments**
  - **Stream Control Transmission Protocol : Newer application support, such as voice over network.**
- **Application Layer :** Equivalent to combined session , presentation and application layers of the OSI model.

2-5 ADDRESSING

Four levels of addresses : physical, logical, port, and specific.

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
Specific Addresses

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

Figure 2.17 *Addresses in TCP/IP*

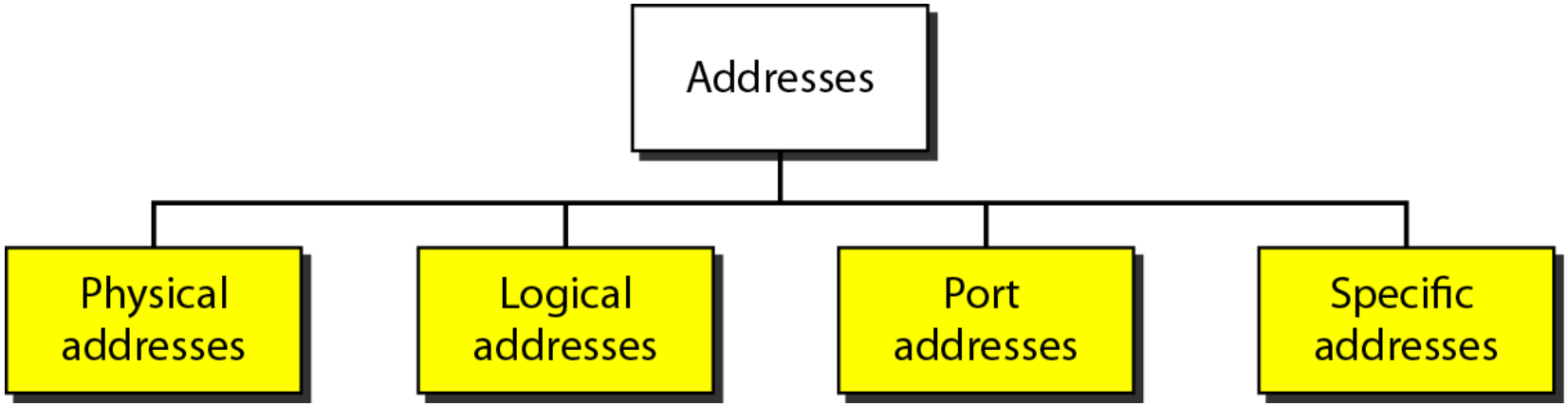
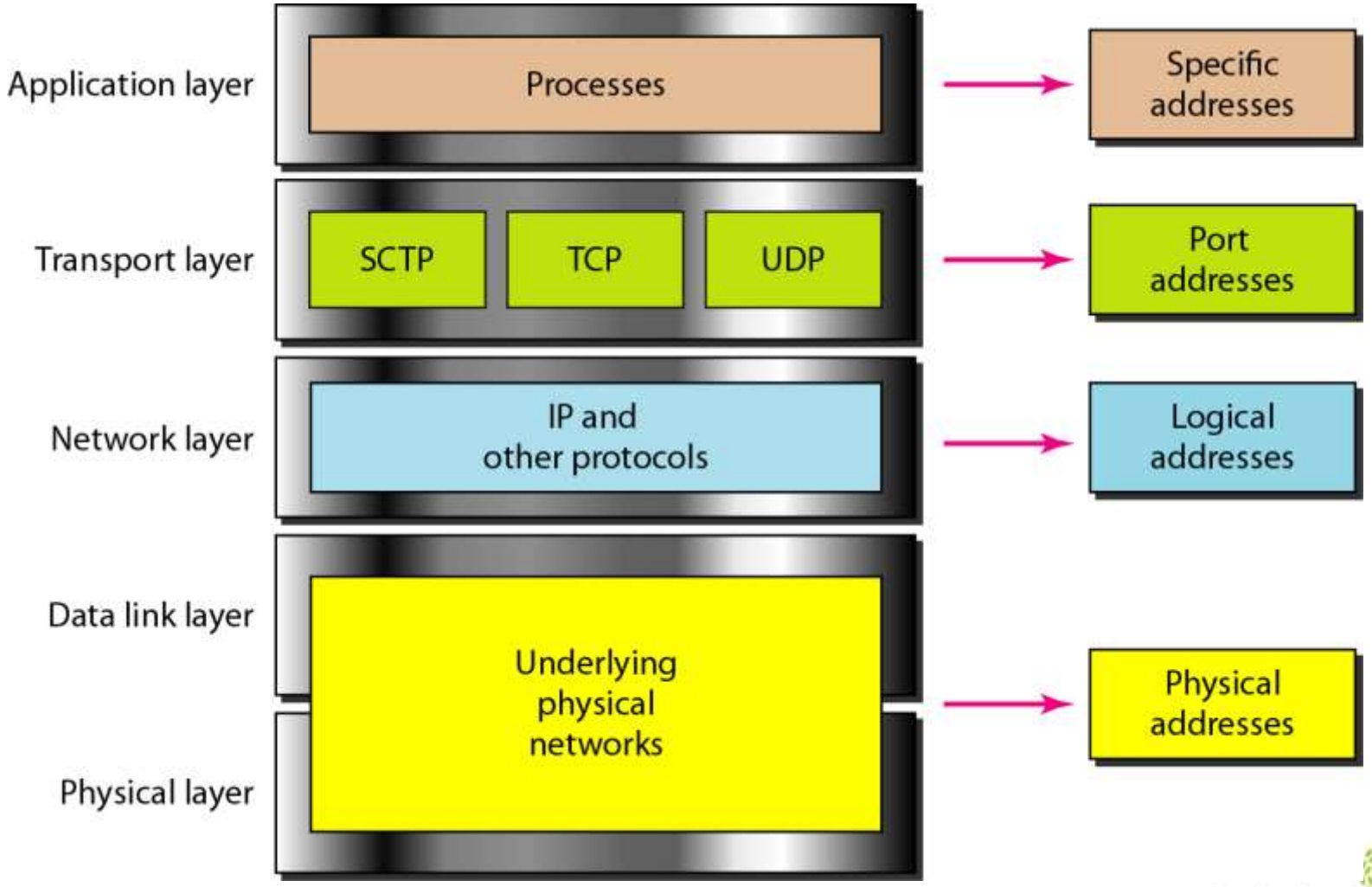


Figure 2.18 *Relationship of layers and addresses in TCP/IP*



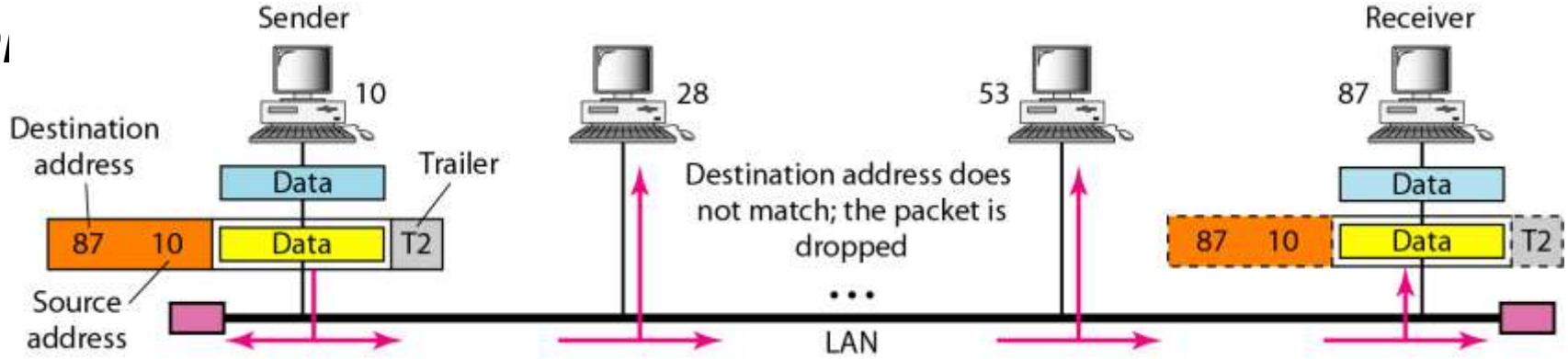
physical address

most local-area networks uses a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

In Figure shown below. a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with p



Logical Addresses

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

IPv4 address consists of 32 bits which limits the address space to 4294967296 (2^{32}) possible unique addresses.

IPv4 addresses are represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address.

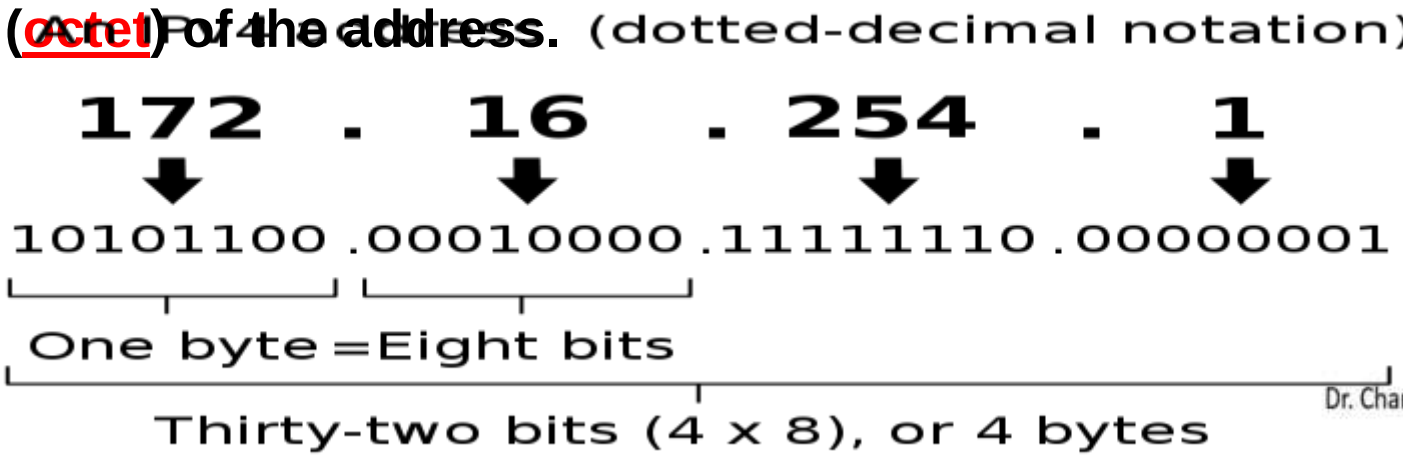
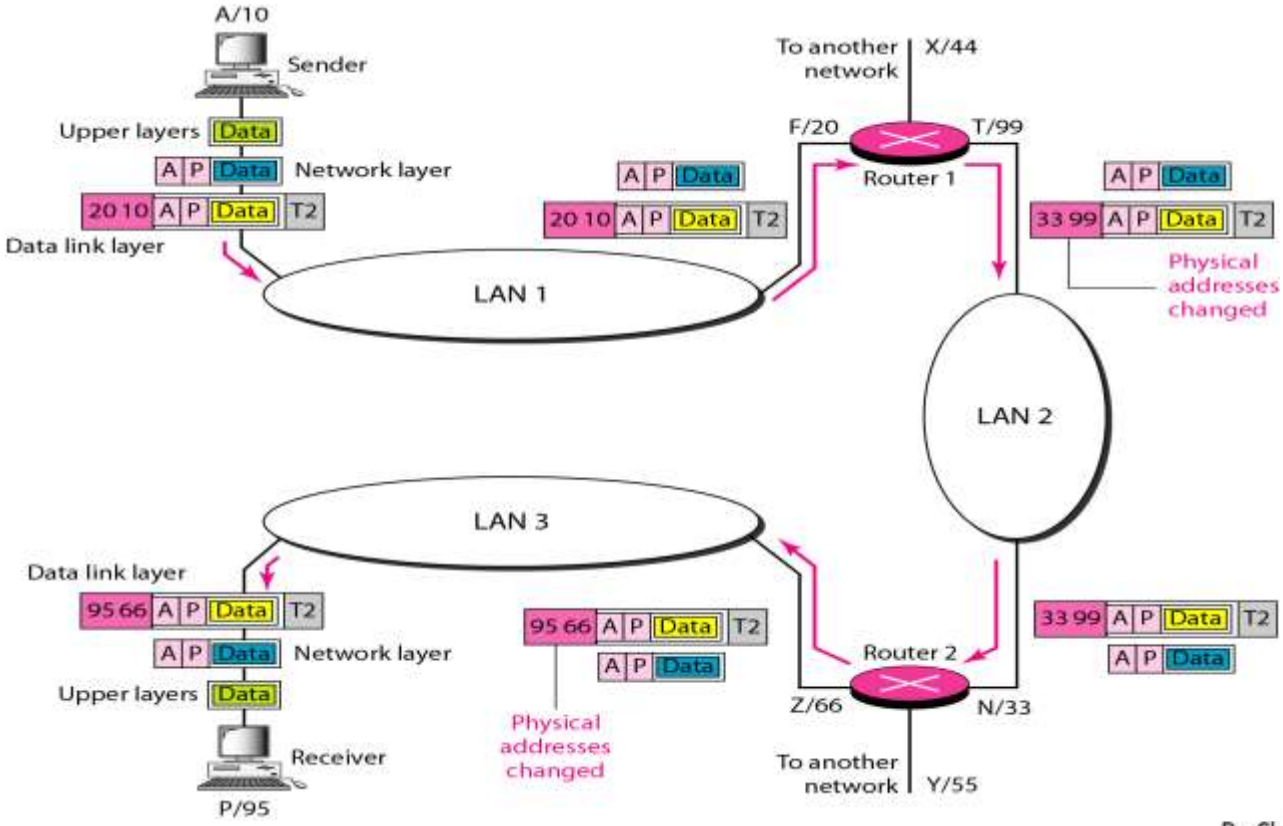


Figure 2.20 *IP addresses*

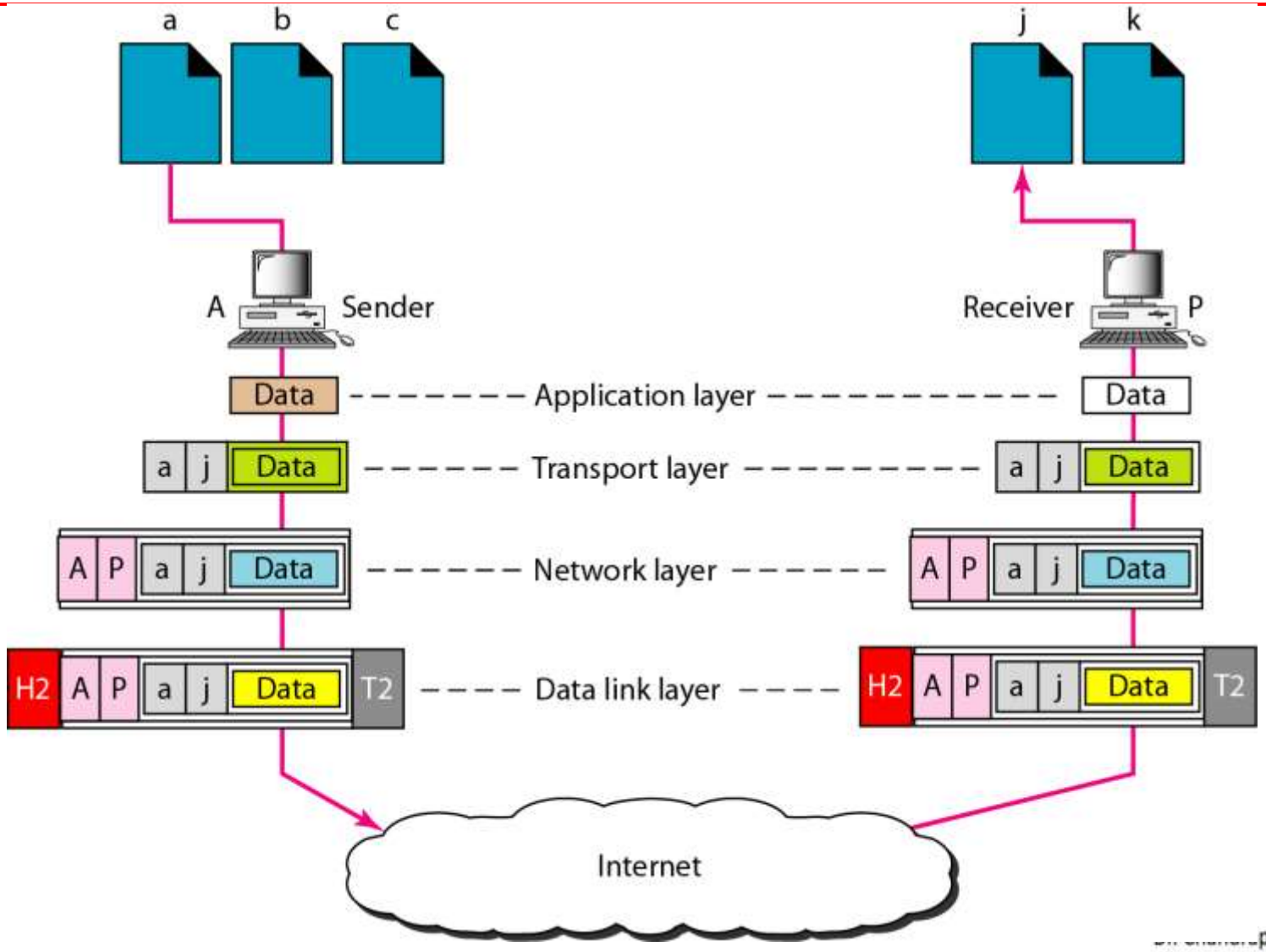
Figure 2.20 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.



port addressing

Figure 2.21 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Figure 2.21 *Port addresses*



A port number is a way to identify a specific process to which message is to be forwarded

A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented as one single number.

Dr. Chandrappa S
NAGARJUNA
College of Engineering & Technology

Specific Addresses

Some applications have user-friendly addresses that are designed for that specific address.

Examples include the e-mail address (for example, chandrucs21@gmail.com)

REVIEW QUESTIONS

1. Differentiate between data & information. What are the different forms in which data can be represented?
2. What are the characteristics of data communication?
3. What are the components of a data communication system?
4. Define computer network and categorize.
5. Explain protocols and standards in details
6.What is physical topology of network? Explain types of physical topology of network.
7.What is internet ? Explain history of internet and internet today.