CS-206 Computer Networks

SYLLABUS

Introduction to Internetworking and TCP/IP.

Addressing and Routing: Logical Addressing- IPv4 Addresses, IPv6 Addresses. Internet protocol- Internetworking, IPv4, IPv6, transition from IPv4 to IPv6. Address Mapping- ARP, RARP, BOOTP, DHCP, Error Reporting- ICMP. Multicasting-IGMP. Routing- Delivery, Forwarding, Intra and Inter-domain routing, Unicast Routing Protocols-Distance Vector Routing, Link State Routing, Path Vector Routing. Multicast Routing protocols.

TCP and UDP: Process to process delivery- Client/Server Paradigm, Multiplexing and De-multiplexing, Connectionless Versus Connection-Oriented Service, Reliable Versus Unreliable. UDP- Well-Known Ports for UDP, User Datagram, UDP Operation, Use of UDP.TCP- TCP Services, TCP Features, Segment, A TCP Connection, Flow Control, Error Control. Congestion Control- Network performance, Open loop congestion control, Closed loop congestion control, Congestion control in TCP, Quality of Service.

Network Applications: DNS- Name space, Distribution of name space, DNS in the Internet, resolution, DDNS. Remote logging- TELNET, Electronic Mail- SMTP, POP, IMAP, File Transfer- FTP, WWW, HTTP, Network Management: SNMP .

Network Security: Security services- message confidentiality, message integrity, Message authentication, Digital signature, Entity authentication, Key management- Symmetric, Asymmetric. Security in the Internet: IPSec, TLS, PGP, VPN and Firewalls.

Suggested Readings

1. B. A. Forouzan, Data Communications and Networking, TMH .
2. A. S. Tanenbaum, Computer Networks, PHI.
3. A. Forouzan, TCP/IP Protocol Suite, 4th Edition, McGraw Hill, 2010.

Lecture 0

Introduction to Data Communication and Computer Network

Dr. Vandana Kushwaha

Department of Computer Science

Institute of Science, BHU, Varanasi

Data Communication

- **Data communication** is the **exchange** of **data** between **two** or **more devices** via some form of **transmission medium** such as a **wired/wireless** medium.
- **Fundamental characteristics** of effective data communications :

  a. ***Delivery***

  b. ***Accuracy***

  c. ***Timeliness***

Fundamental Characteristics of Data Communication

a. Delivery.

The system **must deliver** data to the **correct destination**.

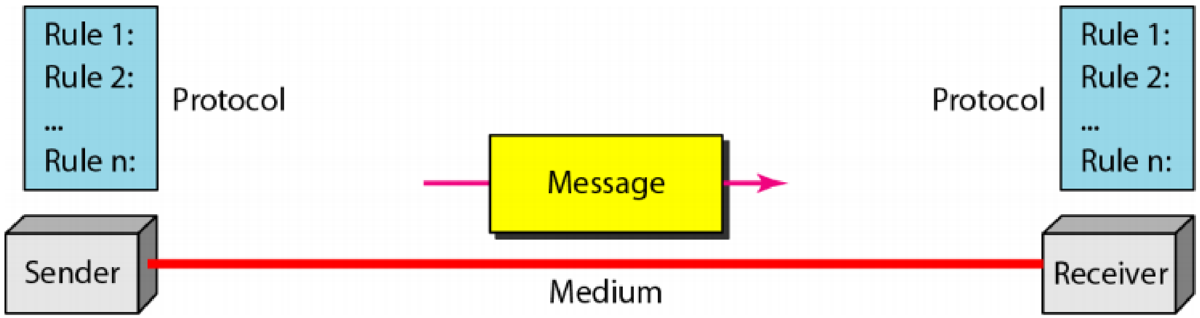
b. Accuracy.

The system **must deliver** the data **accurately.** Data that have been altered in transmission and left uncorrected are **unusable.**

c. Timeliness.

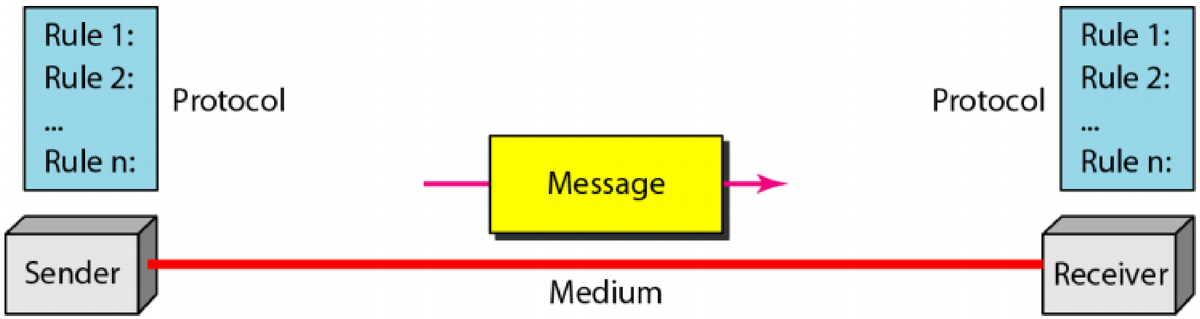
The system **must deliver** data in a **timely manner**. In the case of **real time video** and **audio**, **timely delivery** means **delivering data** as they are **produced,** in the **same order** that they are **produced**, and without significant **delay.**

Components of Data Communications System



- **Sender**. The **sender** is the **device** that **sends** the data **message.** It can be a *computer, workstation, telephone handset, video camera*, and so on.
- **Receiver.** The **receiver** is the **device** that **receives** the **message.** It can be a *computer, workstation, telephone handset, television,* and so on.
- **Transmission medium.** The **transmission medium** is the **physical/virtual 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.*

Components of Data Communications System



- **Message.** The **message** is the **information (data)** to be **communicated**. Popular forms of information include *text, numbers, pictures, audio*, and *video.*

- **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.**

Data Transmission Mode

Communication between **two devices** can be in three different possible modes:

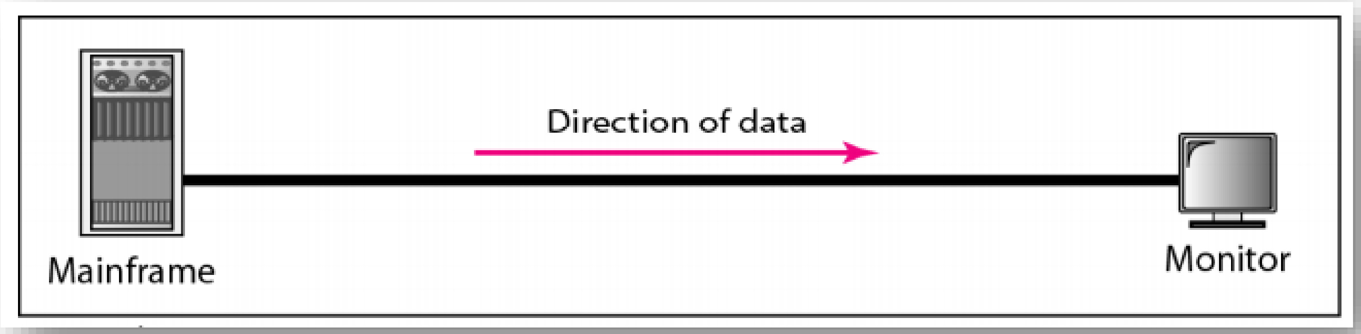
a. ***Simplex***

b. ***Half-duplex***

c. ***Full-duplex.***

a. Simplex:

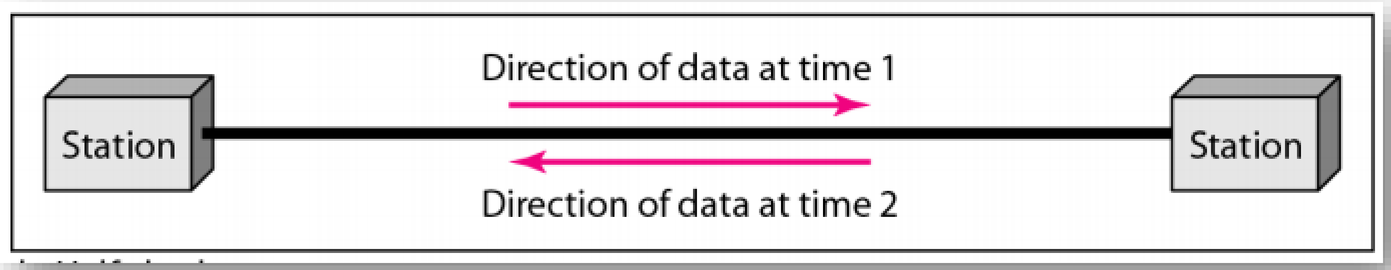
- In **simplex mode**, the communication is **unidirectional,** as on a **one-way street.**
- **Only one** of the two devices on a link **can transmit**; the **other** can **only receive.** **Keyboards** and **traditional monitors** are examples of **simplex devices.**



Data Transmission Mode

b. Half-Duplex:

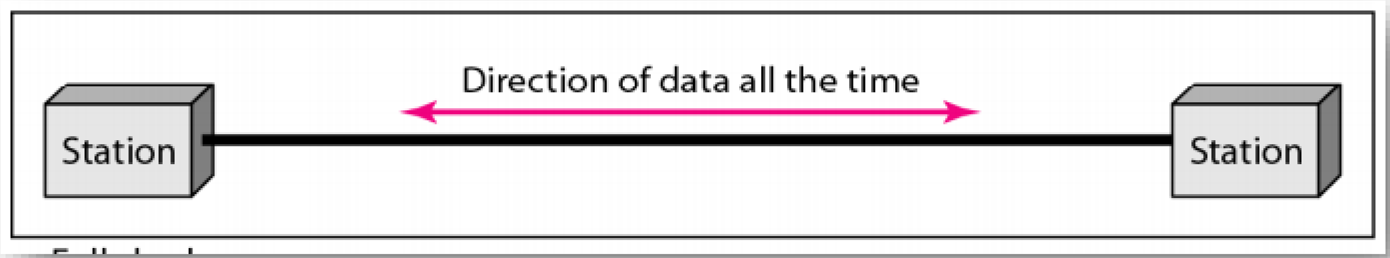
- In **half-duplex mode**, each station can **both transmit and receive**, but **not** at the **same time.**
- When **one device** is **sending,** the **other** can **only receive**, and **vice versa.**
- **Walkie-talkies** is a **half-duplex** system.



Data Transmission Mode

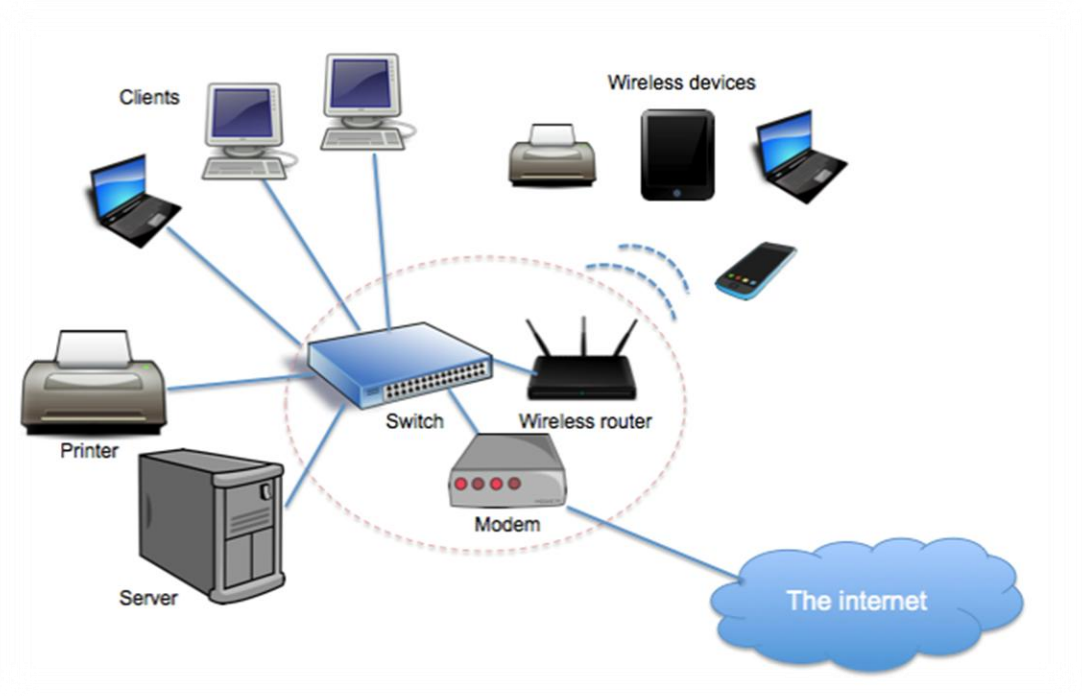
c. Full-Duplex:

- In **full-duplex mode** (also called **duplex)**, **both stations** can **transmit and receive simultaneously.**
- One common **example** of **full-duplex communication** is the **telephone network.**



Network

- A **network** is a **set of devices** (often referred to as **nodes/hosts/stations**) **connected** by **communication links.**
- **A node** can be a *computer, printer*, or any other device capable of **sending** and/or **receiving** data generated by other nodes on the network.
- **A link** is a *communications pathway* that *transfers data* from one device to another.



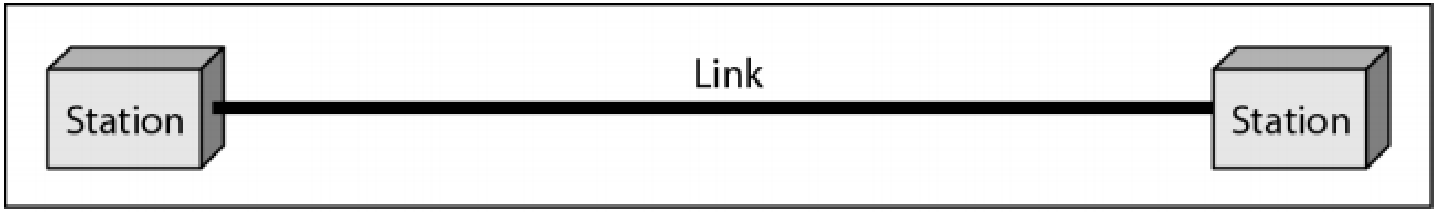
Type of Connection

There are **two** possible **types** of **connections:**

a. ***Point-to-point***

b. ***Multipoint.***

a. **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.**

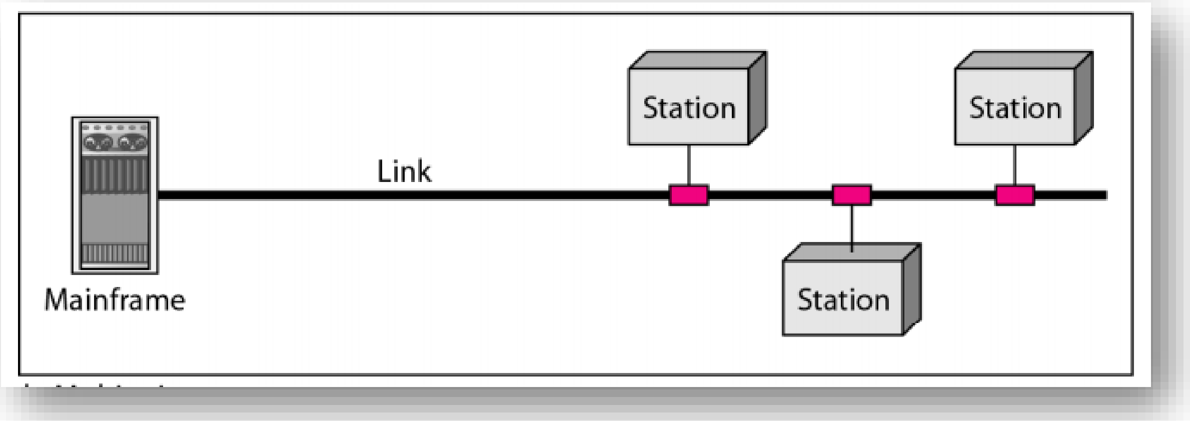


a. Point-to-point

Type of Connection

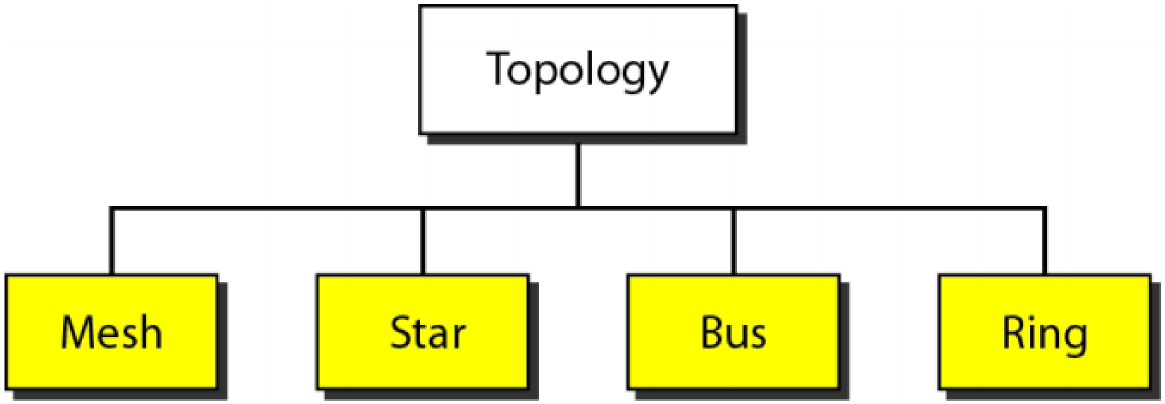
b. Multipoint:

- A **multipoint 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**.

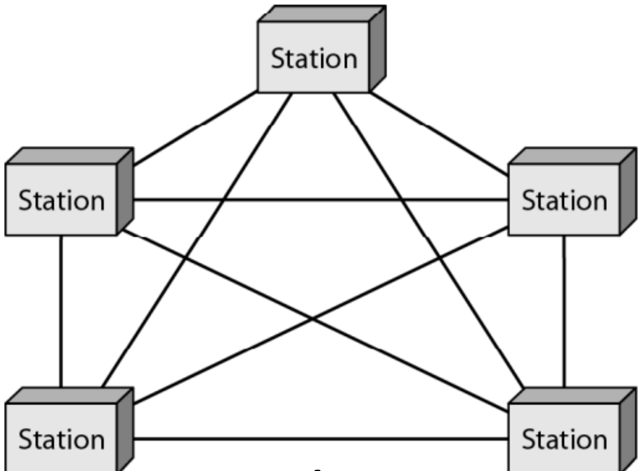


Physical Topology

- The term **physical topology** refers to the way in which a **network** is **laid out physically.**
- 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 **four basic topologies** possible: *mesh, star, bus, and ring.*

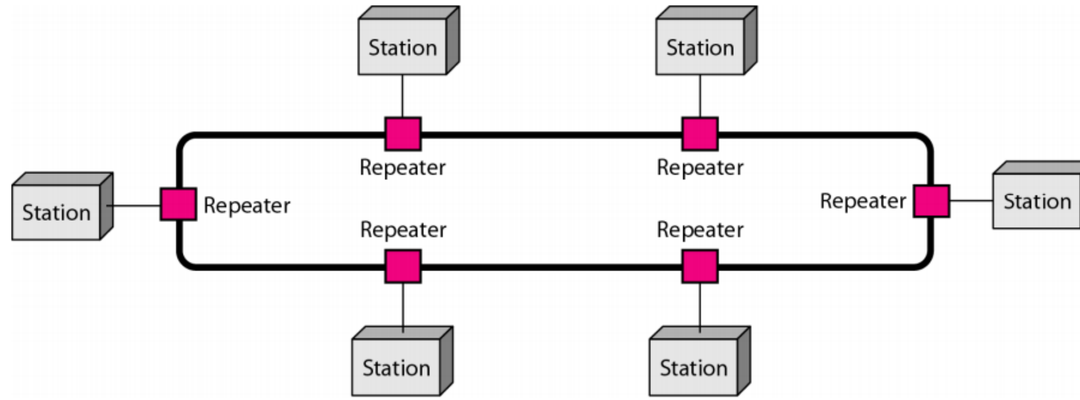


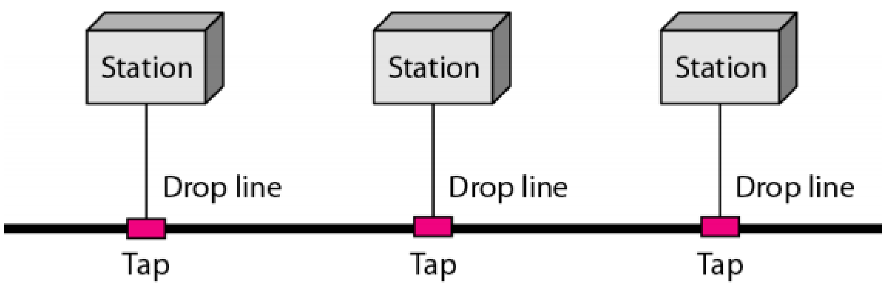
Physical Topology



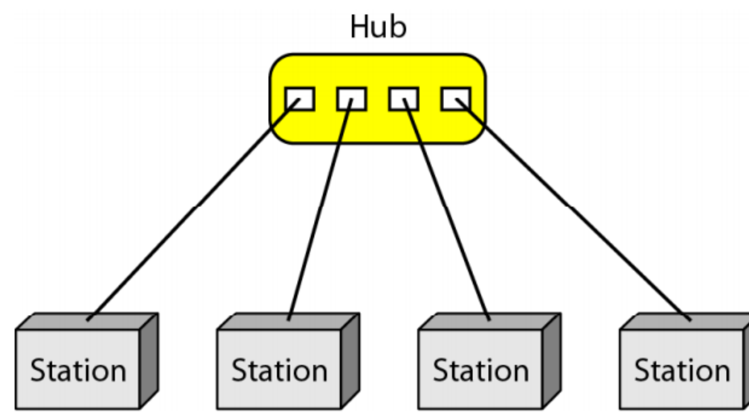
Mesh

Ring





Bus



Star

Categories of Networks

- **Networks** are generally referring to **two primary** categories:
  - **Local-area networks(LAN)**
  - **Wide-area networks(WAN)**
- A LAN normally covers a **small geographical** area. A **local area network** (LAN) is usually **privately owned** and **links** the **devices** in a *single office, building, or campus.*
- A WAN provides **long-distance transmission** of *data, image, audio and video* information over **large geographic areas** that may comprise a **country,** a **continent** or even the **whole world.**

Network Models: OSI Model

- The **International Standards Organization (ISO**) is a multinational body established in 1947, 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.**

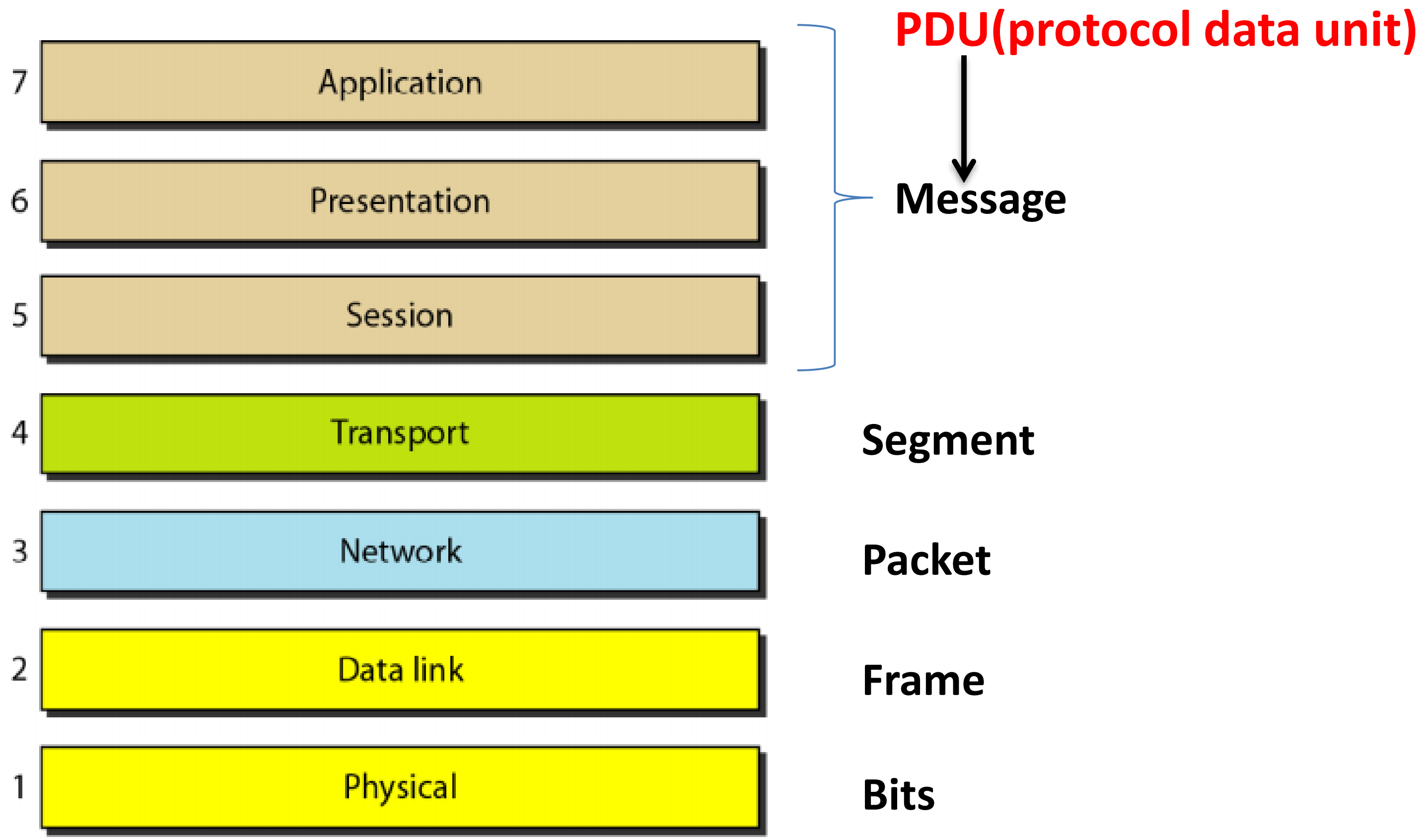
- An **open system** is a **set of protocols** that allows any two different systems to **communicate** regardless of their **underlying architecture**.

- The **purpose** of the **OSI model** is to show how to **facilitate communication between different systems** without requiring changes to the logic of the underlying hardware and software.

- The **OSI model** is not a protocol; it is a **conceptual model** for understanding and designing a **network architecture.**

OSI Model

- The **OSI model** is a **layered framework** for the **design of network systems** that allows **communication** between all types of computer systems.

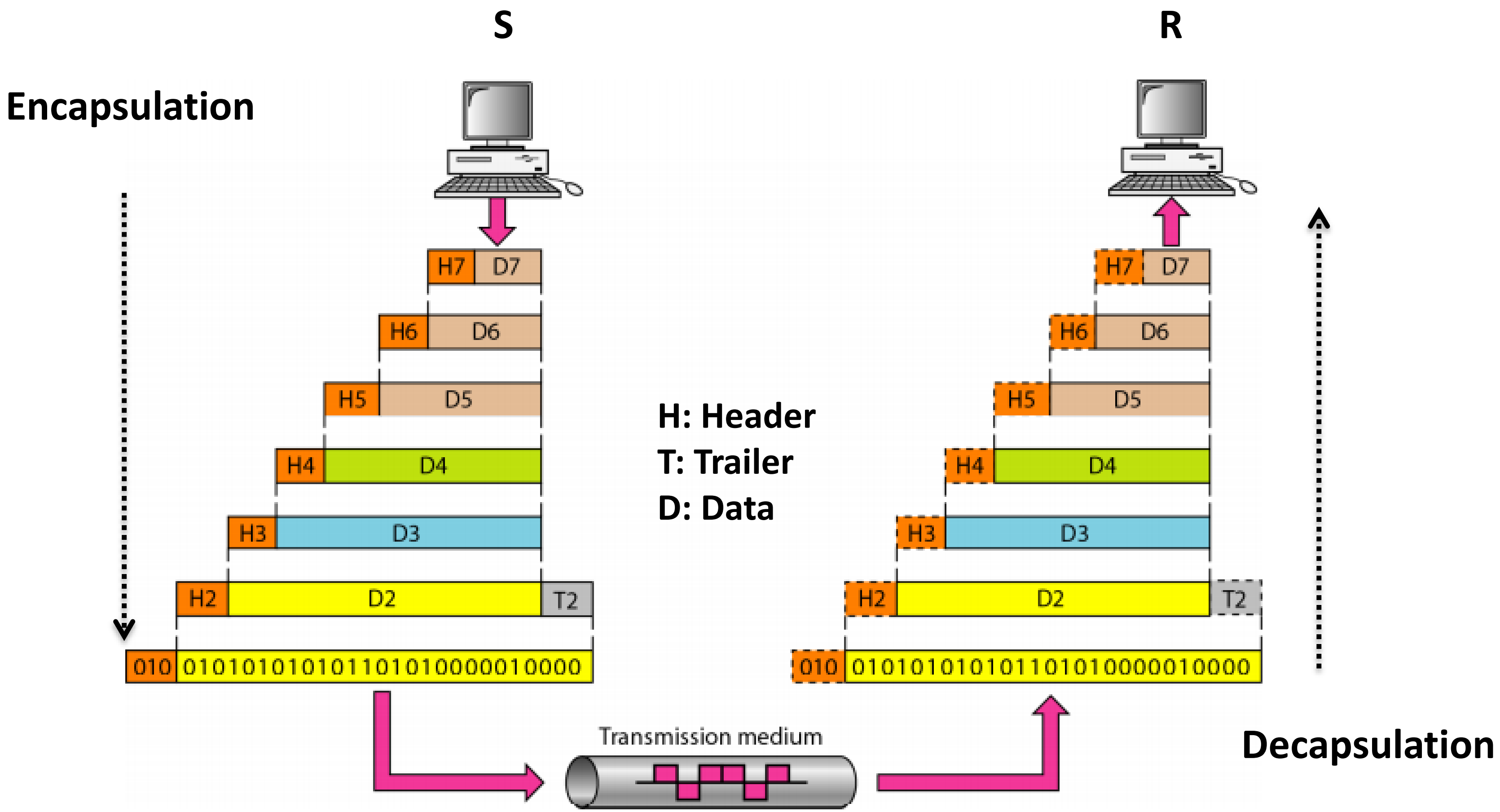


All **People** **Seem** **To** **Need** **Data** **Processing**

Exchange of data using the OSI Model

- **OSI model** consists of **seven** separate but related **layers,** each of which having **different functionality** to support data communication.
- The process starts at **layer 7** (the **application layer**), then moves from **layer to layer** in **descending**, sequential order.
- At each layer, **a header**, or possibly **a trailer,** can be **added** to the **data unit.**
- Commonly, the **trailer** is added only at **layer 2.**
- When the formatted **data unit** passes through the **physical layer** (layer 1), it is changed into an **electromagnetic signal** and **transported** along a **physical link.**

Exchange of data using the OSI Model

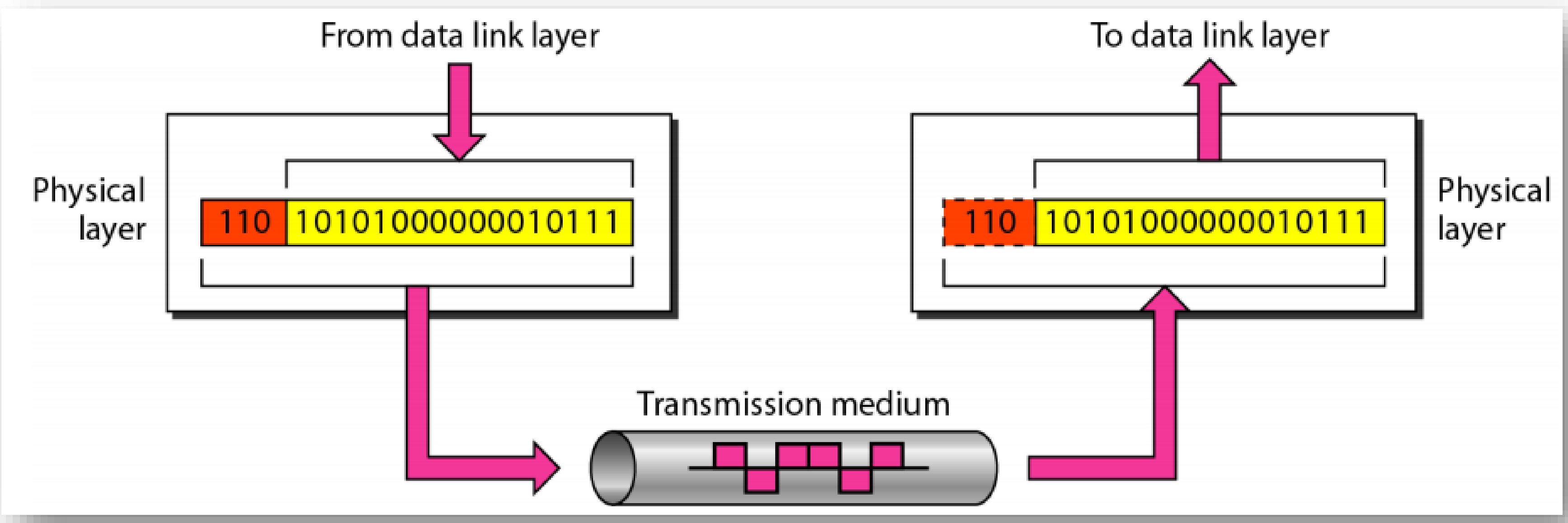


Functionalities of Layers in OSI Model

1. Physical Layer

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

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



Physical Layer Issues

a. **Physical characteristics of interfaces and medium**.

- The **physical layer** defines the **characteristics** of the **interface** between the **devices** and the **transmission medium.** Eg. Type of medium, type of connector etc.

b. Representation of bits.

- The **physical layer data** consists of a **stream of bits** (sequence of 0s or 1s) with no interpretation.
- To be transmitted, **bits** must be **encoded** into **signals--***electrical* or *optical*. The **physical layer** defines the **type of encoding** (how **0s** and **1s** are **changed** to **signals**).

c. Data rate.

- The **transmission rate**-the **number of bits sent each second**-is also defined by the **physical layer.**

Physical Layer Issues

d. Synchronization of bits.

The **sender** and **receiver** not only must use the same bit rate but also must be **synchronized** at the **bit level.**

e. Line configuration.

The **physical layer** is concerned with the **connection of devices** to the **media**; it may be **point-to-point** configuration or **multi-point.**

f. Physical topology.

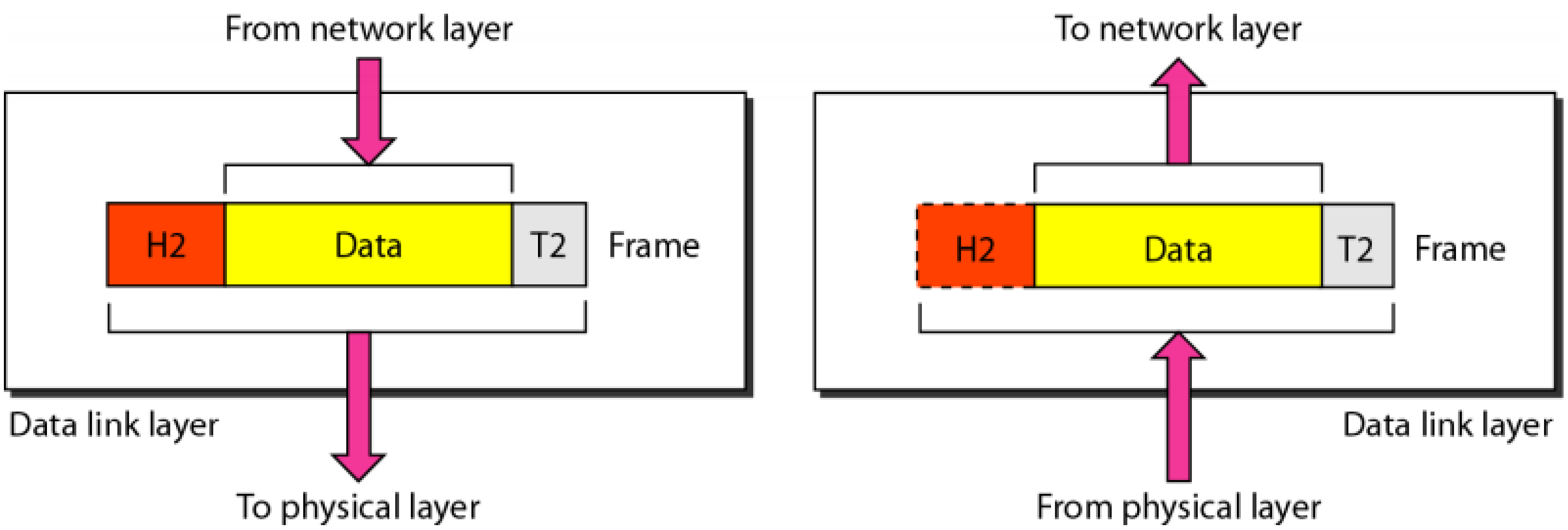
The **physical topology** defines how devices are connected to make a network. Ex. Mesh, Star, Ring, Bus, or a hybrid topology.

g. Transmission mode.

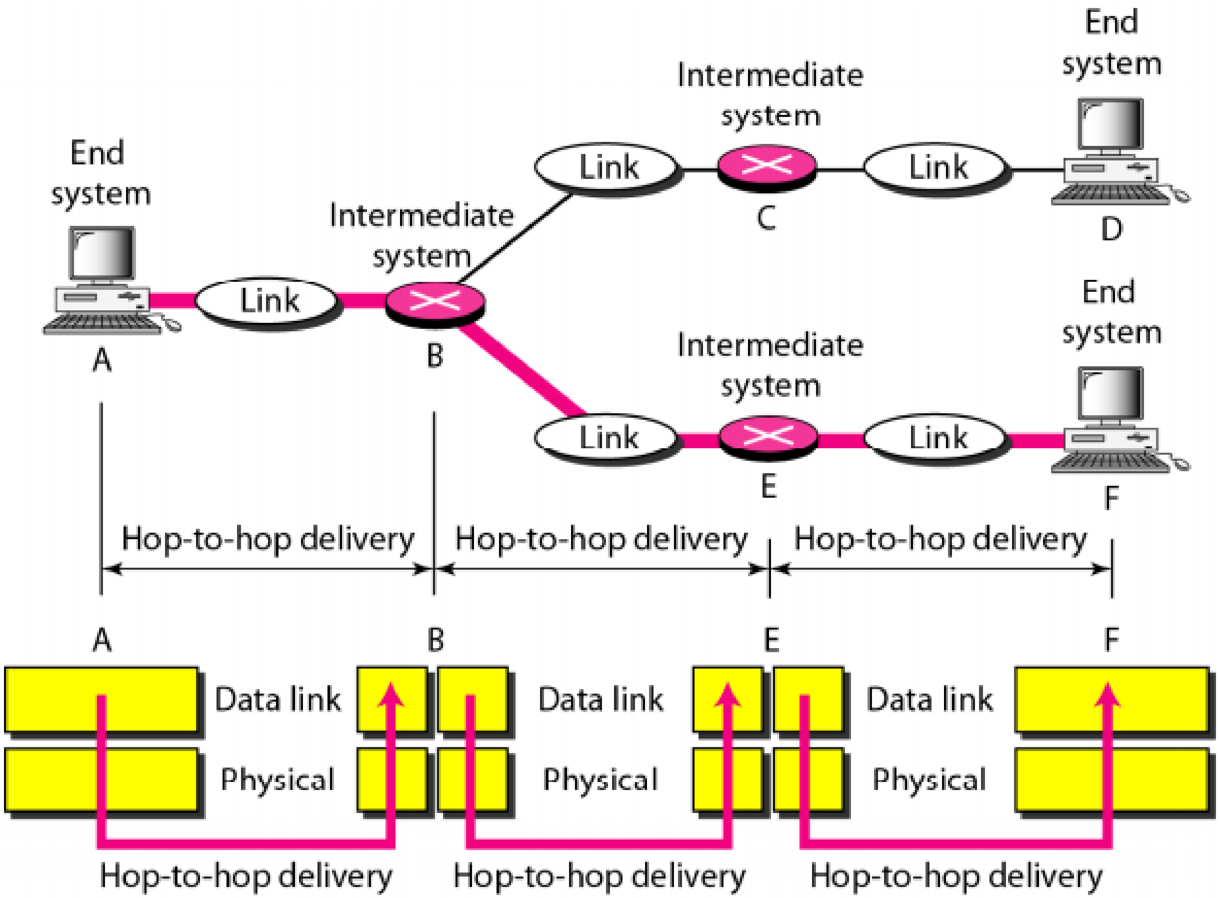
The **physical layer** also defines the **direction** of **transmission** between two devices: *simplex, half-duplex, or full-duplex.*

Data Link Layer

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



Hop-to-hop delivery



Data Link Layer Issues

1. **Framing**

- The **data link layer** divides the stream of bits received from the **network layer** into manageable data units called **frames.**

2. Physical addressing

- If frames are to be distributed to different systems on the network, the **data link layer** adds a **header** to the **frame** to define the **sender** and/or **receiver** of the **frame.**

3. Flow control.

- If the **rate** at which the **data** are **absorbed by the receiver** is **less** than the **rate** at which **data are produced** in the **sender**, the **data link layer** imposes **a flow control mechanism** to avoid **overwhelming** the **receiver.**

Data Link Layer Issues

4. Error control.

- The **data link layer** adds **reliability** to the **physical layer** by adding **mechanisms** to **detect** and **retransmit damaged** or **lost frames**.

- **Error control** is normally **achieved** through a **trailer** added to the end of the **frame.**

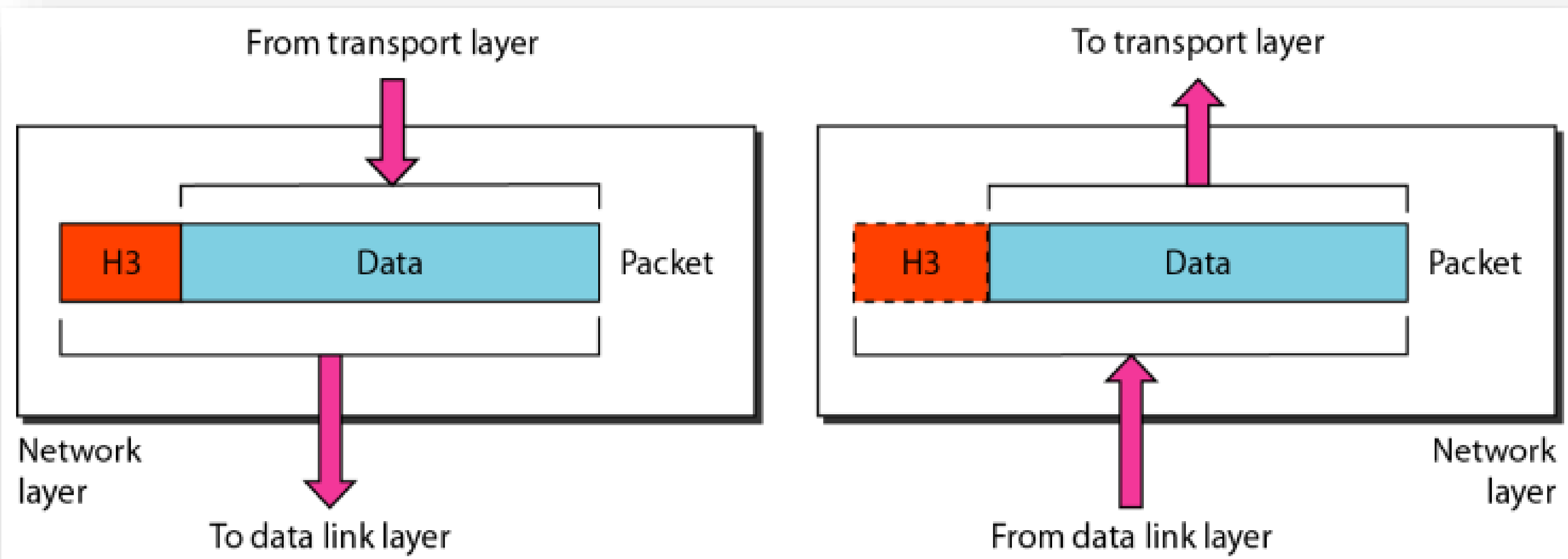
5. Access control.

- When two or more devices are connected to the **same link**, **data link layer** protocols are necessary to determine **which device** has **control over the link** at any given **time.**

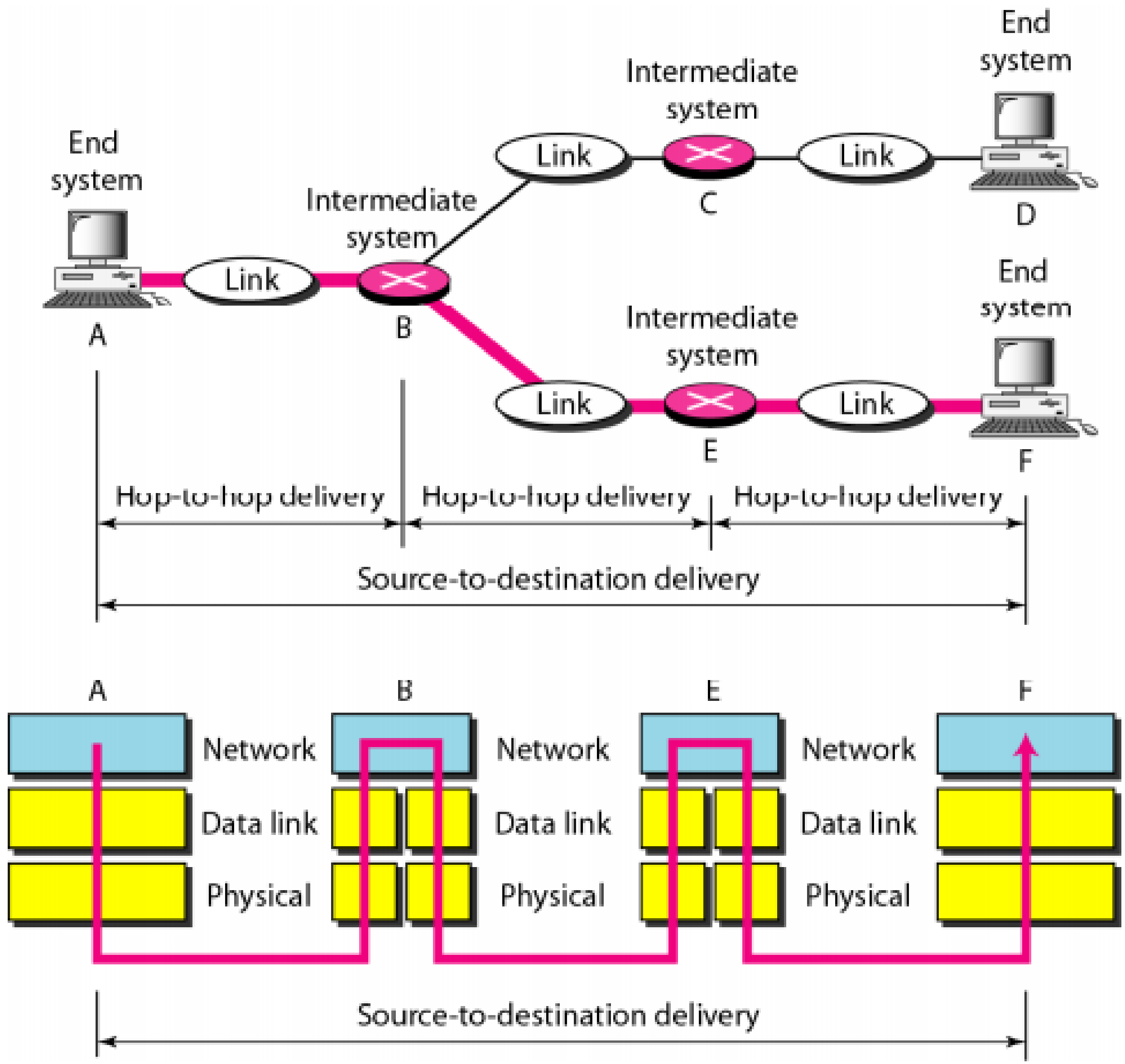
Network Layer

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

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



Source-to-destination delivery



Network Layer Issues

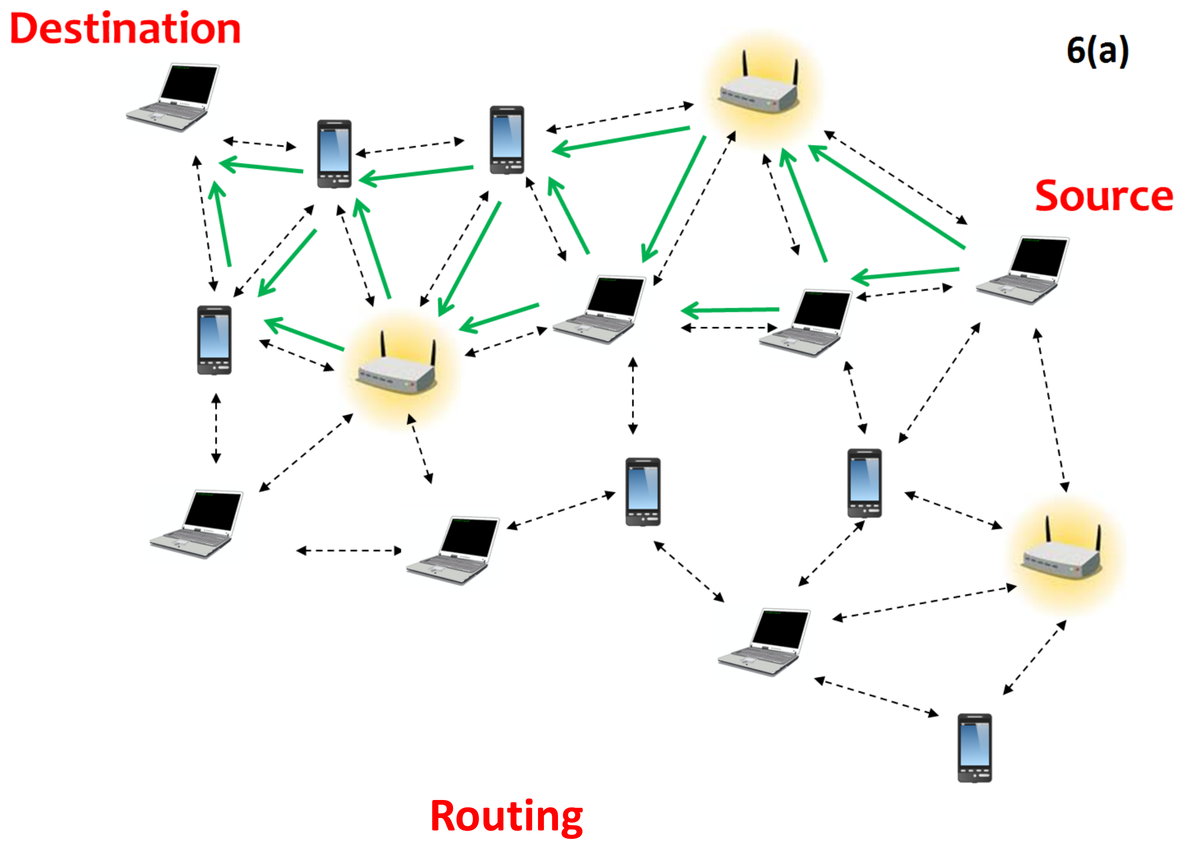
1. **Logical (IP)addressing**.

- The **network layer** adds a **header** to the **packet** coming from the **upper layer(Transport Layer)** that, among other things, includes the **logical (IP) addresses** of the **sender** and **receiver.**

2. Routing.

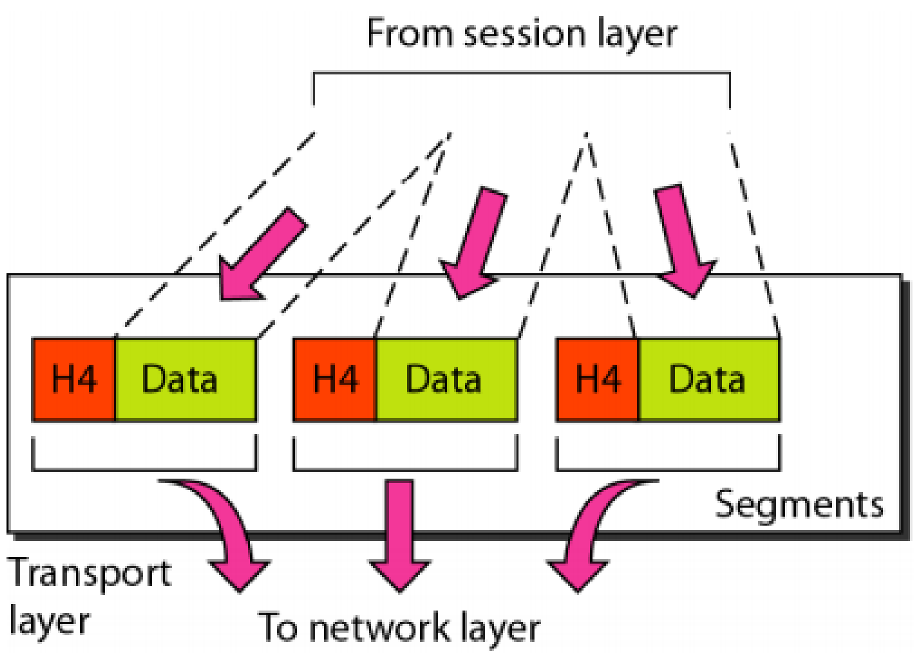
- When **independent networks** or **links** are connected to create **internetworks** or a **large network**, the **connecting devices** **route** the **packets** to their **final destination**. using an **optimal path** from **source** to **destination.**

Network Layer Issues



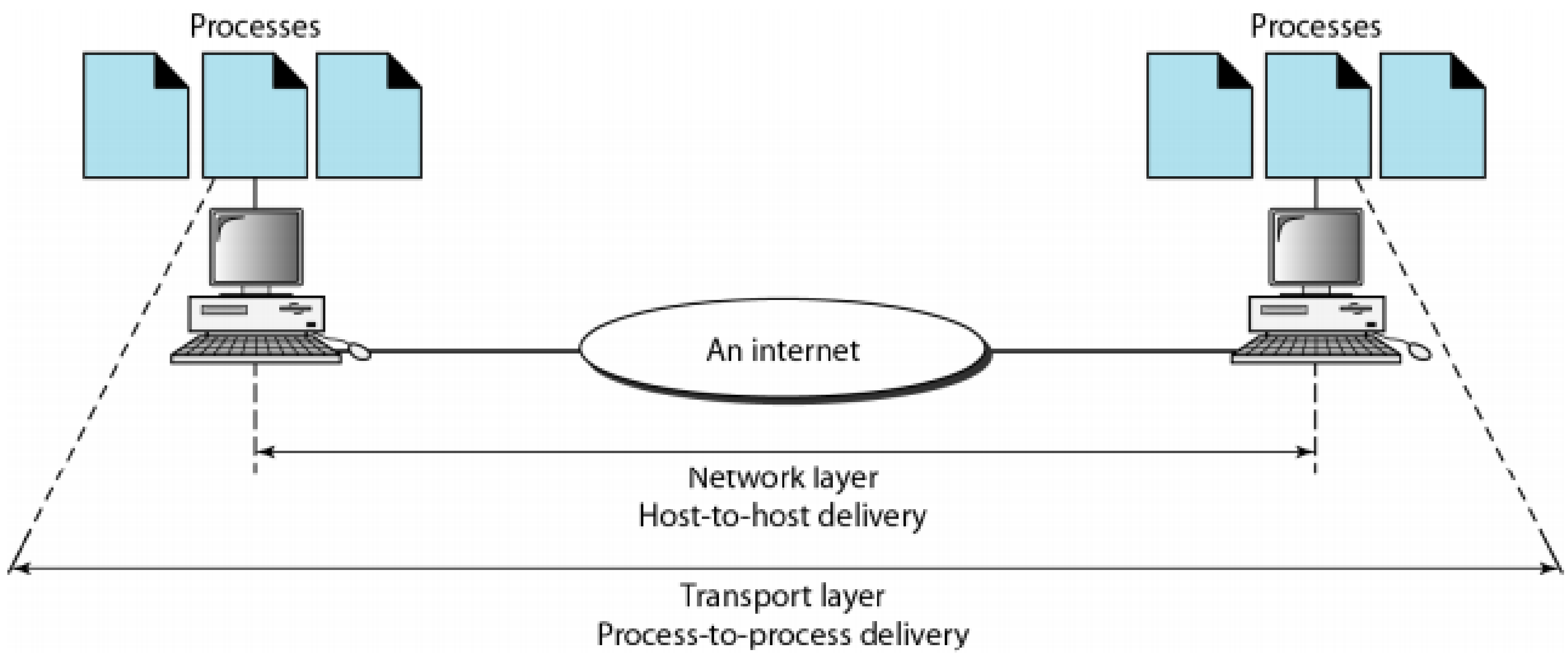
Transport layer

- The **transport layer** is responsible for **process-to-process delivery** of the **entire message**.
- A **process** is an **application program** running on a host. E.g. **FTP, HTTP.**
- The **transport layer** ensures that the whole **message** arrives intact and in order, overseeing both **error control** and **flow control** at **the source-to-destination level**.



Process-to-process delivery of a message

HTTP Client FTP Client HTTP Server FTP Server



Transport layer Issues

a. Port addressing. Source-to-destination delivery means delivery not only from one computer to the next but also from a **specific process** (running program) on one computer to a **specific process** (running program) on the other.

b. Segmentation and reassembly. A **message** is divided into **transmittable segments**, with each segment containing a **sequence number**. These numbers enable the **transport layer** to **reassemble** the **message** correctly upon arriving at the **destination** and to identify and replace packets that were lost in transmission.

c. Flow control. The transport layer is responsible for **flow control**. However, flow control at this layer is performed **end to end** rather than across a single link.

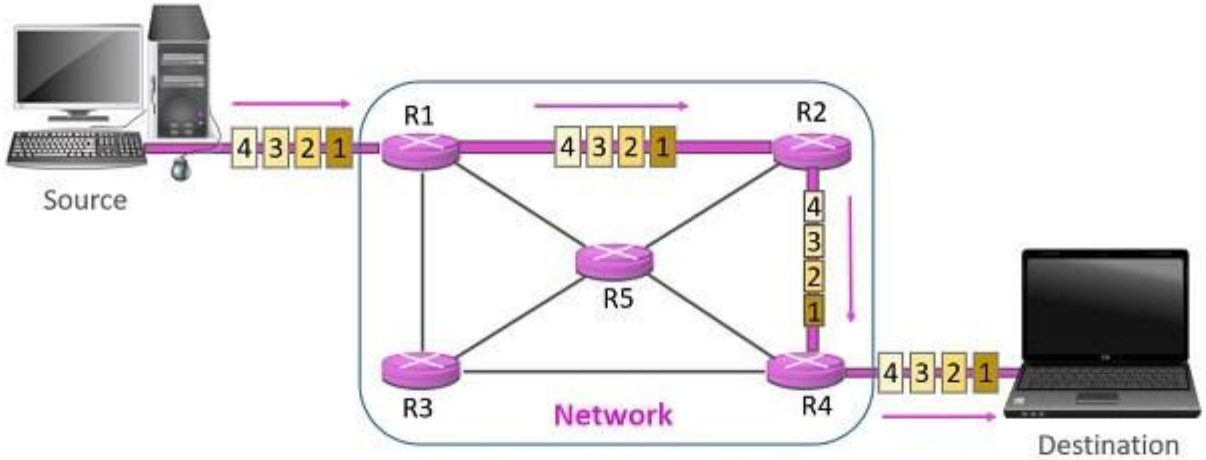
d. Error control. The transport layer is responsible for **error control**. However, error control at this layer is performed **process-to-process** rather than across a single link.

Transport layer Issues

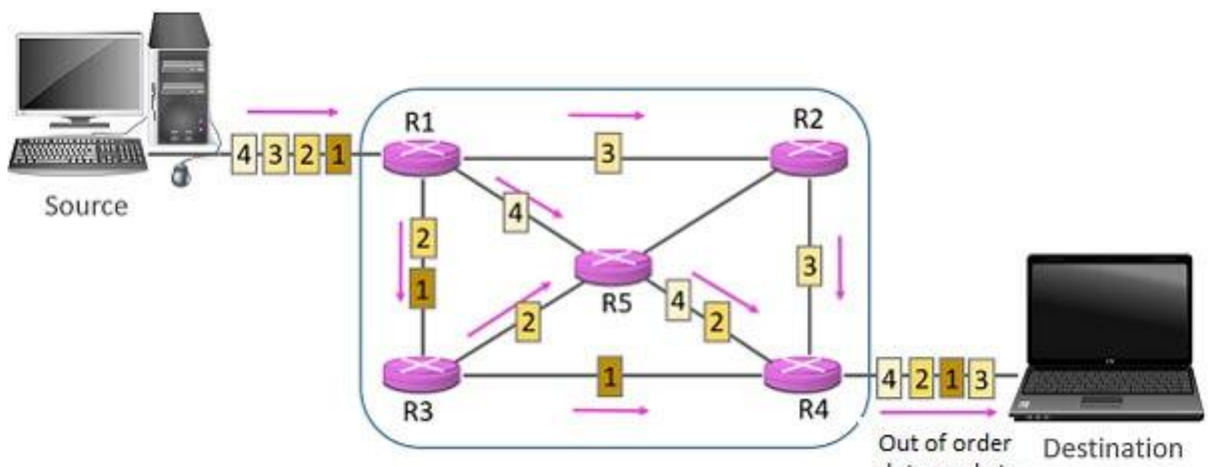
e. Congestion Control: Due to **increased network traffic** packet may be **delayed** or **lost.** To resolve such situation **congestion control** techniques are used.

f. Connection control. The transport layer can be either connectionless or connection oriented.

- A **connectionless** transport layer treats **each segment** as an **independent packet** and delivers it to the transport layer at the destination machine.
- A **connection oriented** transport layer **makes a connection** with the transport layer at the destination machine first before delivering the packets. After all the **data are transferred**, the connection is **terminated.**



Connection Oriented Service



Connectionless Service

Session Layer

- The **session layer** is the **network dialog controller**.
- It establishes, maintains, and synchronizes the interaction among communicating systems.

a. Dialog control.

- The **session layer** tracks the dialogs between systems, which are also called **sessions**.
- This layer **manages** a **session** by initiating the **opening** and **closing** of **sessions** between **end-user application processes.**

Session Layer

b. **Synchronization**.

- The **session layer** allows a **process** to add **checkpoints**, or **synchronization points**, to a **stream** of data.
- **Example:** If a system is sending a **file** of **800 pages**, adding **checkpoints** after **every 50 pages** is recommended.
- This ensures that **50 page unit** is **successfully received** and **acknowledged.**
- This is **beneficial** at the **time of crash** as if a **crash happens** at **page number 110**; there is **no need to retransmit** 1 to100 pages.
- Thus if a **failure occurs**, communication can **resume from the last checkpoint** instead of **restarting** from **scratch.**

Presentation Layer

- The **presentation layer** is concerned with the **syntax** and **semantics** of the **information exchanged** between two systems.
- **The presentation layer is responsible for:**
  - ***Translation,***
  - ***Compression,***
  - ***Encryption.***

a. Translation.

- The **processes** (running programs) in **two systems** are usually exchanging information in the form of character strings, numbers, and so on.
- The **information** must be **changed** to **common format**(bit streams) before being transmitted. **Ex-** EBCDIC to ASCII conversion.

Presentation Layer

c. Encryption.

- A system must be able to ensure **privacy.**
- **Encryption** means that the sender transforms the original information to another form and sends the resulting message out over the network.
- **Decryption** reverses the original process to transform the message back to its original form.

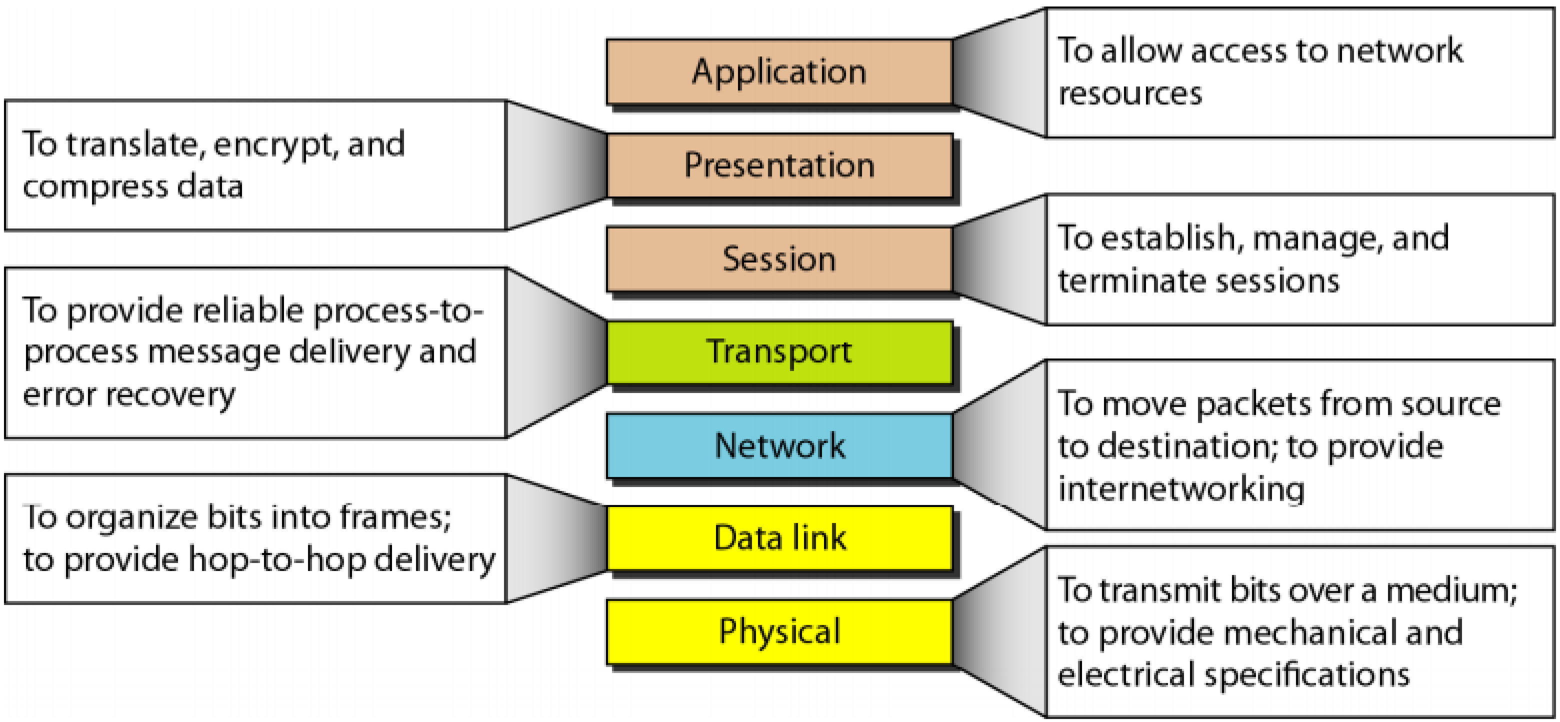
d. Compression.

- **Data compression** reduces the number of bits contained in the information by this reduce the bandwidth requirement of the data.
- It is **very important** in the transmission of **multimedia** such as text, **audio**, and **video.**

Application Layer

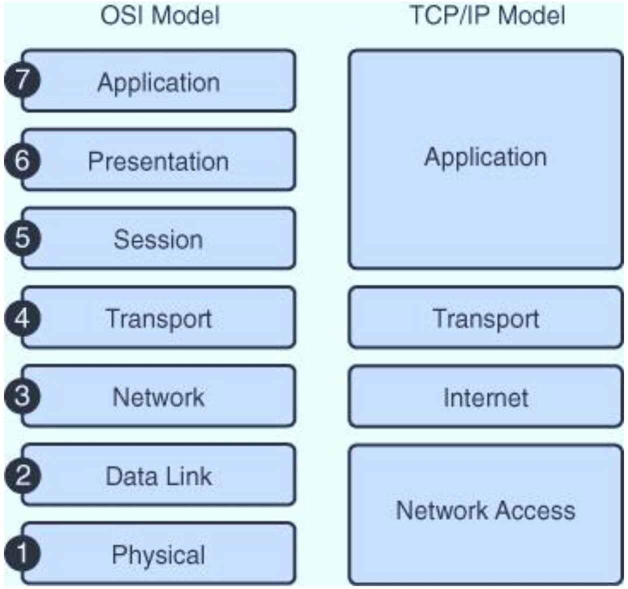
- The **application layer** enables the **user,** whether human or software, to access the network.
- It provides **user interfaces** and **support** for **services** such as **electronic mail, remote file access** and **transfer** and other types of distributed information services.
- A few **examples** of **application layer protocols** are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Remote Login(TELNET), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol(SNMP) and Domain Name System (DNS).

Summary of layers



TCP/IP Model

- The **OSI Model** we just looked at is just a **reference/logical model.**
- The **TCP/IP protocol suite** was developed prior to the **OSI model.**
- **TCP/IP model** was designed and developed by **Department of Defense (DoD)** in **1960s** and is based on standard protocols.
- **TCP/IP protocol suite** is made of **four layers**: **Network Access Layer**(Physical+Data link), **Internet Layer, Transport Layer and Application Layer.**



ADDRESSING

Three levels of **addresses** are used in an internet employing the **TCP/IP protocols:**

1. **Physical (MAC) address at Data Link layer**

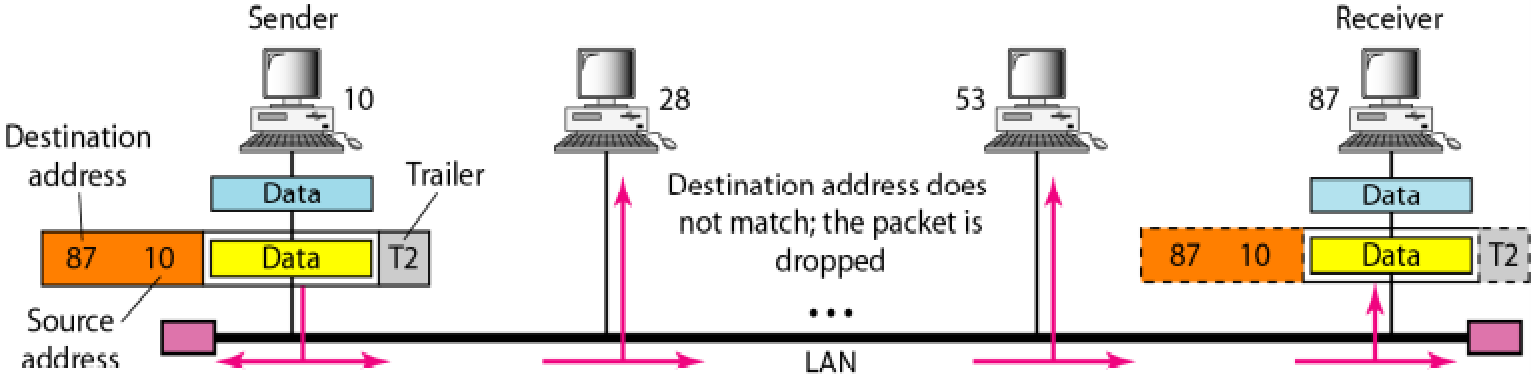
2. **Logical (IP) address at Network Layer**

3. **Port address at Transport Layer**

1. Physical(MAC) Addresses:

- The **physical address**, also known as the **link address**, is the **address of a node** as defined by its **LAN** or **WAN.**
- It is included in the **frame** used by the **data link layer.**
- The **size** and **format** of these **addresses** vary depending on the network.
- Example, **Ethernet** uses a **6-byte** (48-bit) **physical address** that is imprinted on the **network interface card (NIC).**
- **LocalTalk (Apple),** however, has a **1-byte dynamic address** that changes each time the station comes up.

Physical addresses Example



Numerals: Physical Address

Logical (IP)Addresses

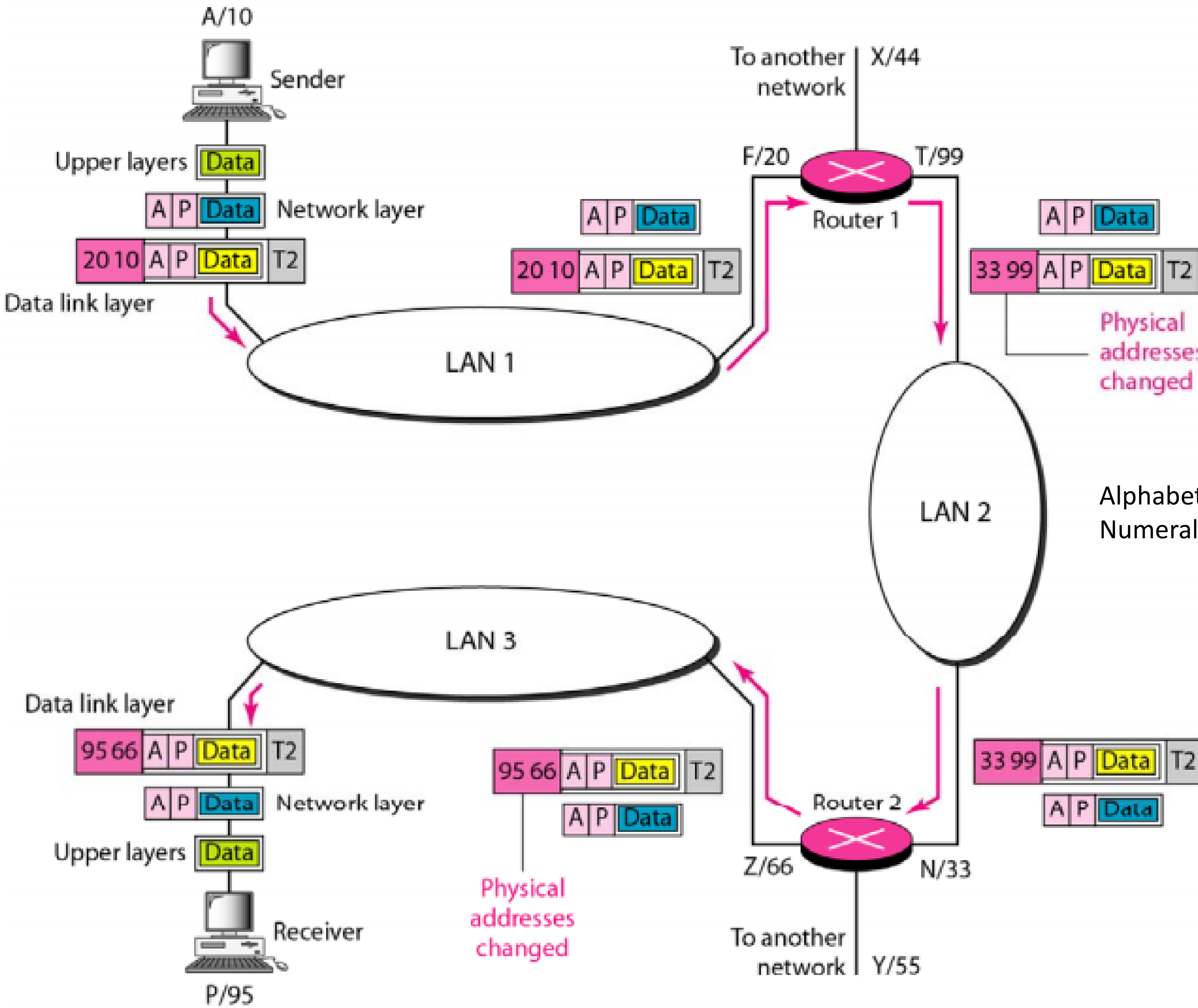
- **Logical(IP) addresses** are necessary for **universal(global) communications** that are independent of underlying physical networks.
- **Physical addresses** are not adequate in an **internetwork environment** where different networks can have different address formats.
- A **universal addressing** system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
- The **logical addresses** are designed for this purpose.
- A **logical(IP) address** in the Internet is currently a **32-bit address(IPv4)** that can uniquely define a host connected to the Internet.
- **IPv6** uses **128-bit** IP address.

Port Addresses

- The **IP address** and the **MAC address** are necessary for data to travel from a source to the destination host.
- However, arrival at the **destination host** is not the final objective of data communications on the Internet.
- Computers are devices that can run **multiple processes** at the same time.
- The end **objective** of Internet communication is a **process communicating with another process**.
- For **example,** computer **A** can communicate with computer **C** by using **TELNET**.
- At the same time, computer **A** communicates with computer **B** by using the File Transfer Protocol (**FTP**).
- For these **processes** to receive data simultaneously, we need a method to differentiate the different processes.

Port Addresses

- In the **TCP/IP** architecture, the address assigned to a process is called a **port address**.
- A **port address** in TCP/IP is **16 bits** in length.
- **Port Addresses/IP Addresses Example**
- Figure on next slide 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) fo**r each connection.
- The **physical addresses** will change from hop to hop, but the **logical** and **port addresses** usually remain the same.



Alphabets: Logical address
Numerals: Physical address

Port addresses