Data Communication:

- Exchanging data over some transmission medium.
- Four important characteristics:
  1) Data delivery *safe* and *accurate* to the correct destination
  2) Timeliness: On time delivery without “jittering” (variation in arrival time) especially for audio and video data.

**Major components of DC:**

![Diagram of data communication components](image)

**Figure 1.1 Five components of data communication**

1.3

1) **Message**: Information to be communicated: text, numbers, pictures, audio, video.
2) **Senders**: devices that transmits the data messages: computers, telephones, TV stations, cameras, etc.
3) **Receivers**: devices that receives the data messages: computers, telephones, TV sets, etc.
4) **Transmission medium**: Physical links that carries the communicated data, TP, coaxial, fibers, radio waves, etc
5) **Protocol** for DC: Set of rules that govern DC, syntax and semantics.

**Data** are text, Numbers, Images, Audio, and video.
Data Flow:

Data flow between communication devices as follows:

a) **Simplex** (one way only).
b) **Half Duplex** (H/D) (Bidirectional on *one* links).
c) **Full Duplex** (F/D) (Bidirectional on *two* links).

Networks:

Set of nodes connected via physical links for the purpose of:

1) **Distributing Processing**: dividing a large task over a network of computers.
2) **Sharing Data vs. centralization**: shared access of data-banks (and other resources) among network of computers.
3) **Security and robustness**: distributed computers approach is for more security and reliability/dependability.

Network Criteria:

1) **Performance** *Response* time -- user level inquiry/response speed, function of network size, links' (medium) quality, and relays'
hardware and protocols. At a lower level, factors: packets' *throughput* (number of successful delivered packet per unit time) and *delay* (source-destination delay encountered by a packet travelling through the network--typically *dynamic*, i.e., varying with time) are also used to measure networks performance.

2) **Reliability**: How often the networks fail.

3) **Security**: *Privacy, integrity* and *authentication* of communication Data; *recovery* from breaches and data loss.

**Physical Structures:**
Types of connections:

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

1) **Point to Point**: *(P2P)*
   Dedicated link to be utilized only by end devices.

2) **Multipoint** (Multidrop): Many end devices share the link capacity.
Physical Topologies:

**Figure 1.4 Categories of topology**

### 1.7

A) Mesh:

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

Each device has dedicated point-to-point link to other devices. Fully connected mesh will have \[n(n-1)/2\] F/D links:

Where \(n\) = number of nodes

**Pros:** Fast communication (cable propagation delay), Robust (faulty node/link does not affect other nodes) and Privacy (Security--direct/private links). Easy to fault detect/isolate.

**Cons:** Cabling Space, fan-out ports, and $\text{cost}$.
B) Star:

Figure 1.6 A star topology connecting four stations

Devices are connected Point to Point to a central “Hub” (Controller Exchanger).

Pros: Less links and ports per node, two hops delay only—source to Hub and Hub to destination delays. Cost of the Hub installation/operation. Easy to maintain when nodes added/dropped nodes.

Cons: Not so robust (vulnerable center of control- The Hub!), more physical cables one per each node compared to the Bus!

C) Bus:

Figure 1.7 A bus topology connecting three stations

Multipoint link as “backbone” for a network where devices have drop line to tap into the bus

Pros: Less Cabling, one hop (source-destination cable) delay.

Cons: Scalability is limited and cable length dependent, which limit number of nodes on the bus due to signal power loss (attenuation) with distance, not so robust. Difficult fault isolation!
**C) Ring:**

*Figure 1.8  A ring topology connecting six stations*

Each station connects Point to Point with only two other stations (on its left and right), stations are connected to the ring via a *Repeater* (its exact function depends on the higher layer protocol, e.g., MAC).

**Pros**: Easy installation, better fault isolation (a dead node will be shorted and the ring remains functioning) and robustness (all nodes are still connected even when the ring breaks with one physical cable cut).

**Cons**: \(n/2\) hops communication delay on average, vulnerable to cuts.

**D) Hybrid**: Star of busses

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

Pros: Better domain separation management (domain security and speed), one hop delay (cable propagation delay).

Cons: Better robustness than the “star”, but still vulnerable to Hub failure!
E) **Pizza:** “star” inside a “ring”  
**Pros:** Better robustness (why?), still low cost, Delay is 1 hop to neighboring  
left/right nodes, or 2 hops to other nodes.  
**Cons:** The $\text{Cost}$ of adding more cabling than the Ring and Star, individually.

F) **Irregular:** “None of the above”! for WANs.
**Categories of Networks:**

**Local Area Networks (LAN): Few Kilometers**
Connects devices (PC’s, printers, servers.) within the same room, building, company, and campus.

Topologies most used are *bus, ring,* and *star.*

**Wide Area Networks (WAN): 100’s – 1000’s of Km**

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

1) **Switched:** End users connected via a cloud of switches (subnet).
2) **Point-to-Point:** Line leased from telephone company/ TV connecting users to the Internet Service Provider (ISP) for Internet access.
**Metropolitan Area Networks: MAN town/city**

High-speed backbone linking multiple LAN’s, Digital Subscriber Line (DSL), TV cables, FDDI, DQDB.
The Internet:

Huge number of interconnected Networks (>100000’s) private organized, e.g.’ government, schools, research facilities, in many countries.

Collection of LAN’S, MAN’S and WAN’s.

- The internet protocol stack is the (TCP-UDP)/IP.
- End users use the internet via Internet Service providers (ISPs) which are of the following hierarchies:

![Diagram of ISP hierarchy]

- Sprint Link, MCI Link, AGIS, PSI Net
- Network Access Point (NAP)
Protocols and Standards: A “protocol” is a set of rules that govern a communication between two nodes.

Elements:
- **Syntax**: PDU format
- **Semantics**: The meaning of each PDU’s field
- **Timing**: Synchronization of communication when PDU is to be transferred and its data rate.

A standard is set of guidelines to users and manufactures to ensure interconnectivity.

Types:
1) **De facto**: not approved but widely used (e.g., TCP/IP)
2) **De jure**: approved by recognized body (ISOOSI, IEEE 802.X).
Network Models

Network Architecture:

A) **Hardware (H/W):** at the core of any network; e.g.) Tx/Rx devices, modems, codecs, physical links, switches,

B) **Software (S/W):** to derive the core H/W to communicate end users. The S/W is as complex as its task. Hence it is divided into subtasks each of which is confined to a set of related processes to perform a specific function.

- Each subtask software module is called a “Layer”
- Layers are *stacked* over each other forming the net model stack, e.g., ISO, TCP/IP,

Each Layer has a “Peer-to-Peer” protocol that seems to represent (and carry out) the rest of the network task, for the immediate layer above it, yet it does only a *specific* part and delegate the rest to the layer beneath it (except for the physical layer). It also has an *interface* that defines the *services* that is provided to the layer above it.

**Encapsulation:** Each layer has its own protocol data unit (PDU) that is passed (as a parameter) to the layer beneath, which in turn adds a “**header** (at layer 2 also adds *trailer*) before assign t to the next layer (except the physical layer

<table>
<thead>
<tr>
<th>PDU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
</tr>
<tr>
<td>…</td>
</tr>
<tr>
<td>Trailer</td>
</tr>
</tbody>
</table>

Why “header” and “trailer”?????????????????????????

Physical movement of information PDU is “vertical” yet the user thinks (At each peer –to-peer) layer that info moves” horizontal” (virtual pipe).