Chapter 1 - Introduction to Data and Telecommunications

Table of Contents

1.1. Data Communications 1

Components 3

Data Representation 4

Data Flow 5

1.2. Networks 6

Network Criteria 6

Physical Structures 6

Categories of Networks 9

Internetworks 10

1.3 The Internet 11

The Internet Today 11

1.4 Protocols and Standards 12

Protocols 12

Standards 12

Standards Organizations 13

1.1. Data Communications

Telecommunication – Communication at a distance

Data – Information presented in whatever format is agreed upon by the parties involved

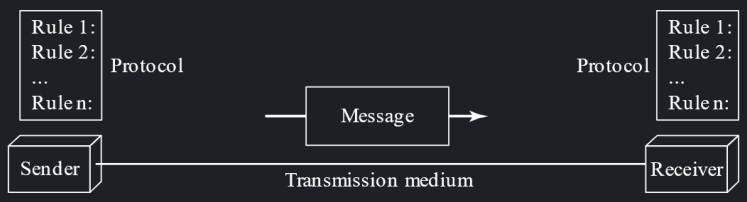
Data communication – Transmission of data between two devices via some form of transmission medium, such as a wire cable.

Data communication takes place with the help of some protocols, and these protocols are what we will be studying. All of these protocols are helping each other to transmit data.

For data communication to occur, the communicating devices must be in a system of hardware and software. The effectiveness of the communication depends on four things:

- **Delivery** – Data must be delivered to the correct destination and nowhere else. This can become very complicated and involve a lot of protocols, especially with multiple users being connected and multimedia data being transferred, such as with video conferencing.
- **Accuracy** – Data must be delivered without errors. The protocols used to transfer data via the internet are in themselves unreliable. Thus, we need some error-control mechanisms and flow-control mechanisms. This involves error-detection and error-correction.
- **Timeliness** – The data must be delivered on time, since data that arrives late might be useless. Consider live video or audio transmission. This data has to be transmitted as soon as it is produced, in the same order in which it is produced and without significant delays. Such transmission is called real-time transmission.
- **Jitter** – Jitter refers to the variations in packet delivery time. Consider video packets being sent where some packets have a 30ms delay while others have a 40ms delay. This will cause an uneven video quality.

Components



A data communication system has five components:

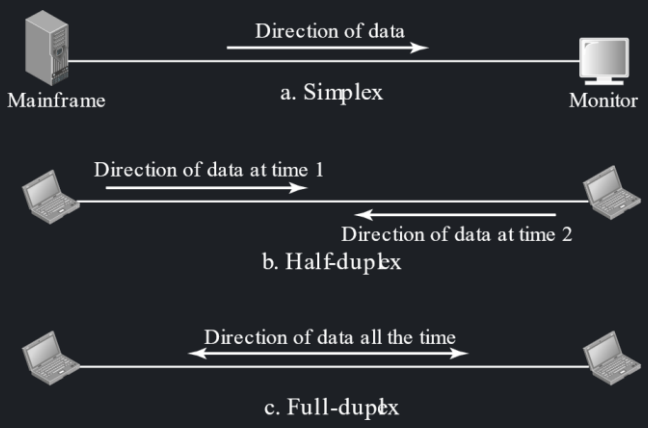
- **Message** – This refers to the data in any format.
- **Sender**
- **Receiver**
- **Transmission Medium** – This refers to the path, either wired or wireless, via which the message is transmitted.
- **Protocols** – These are a set of rules that govern the data transmission. It is an agreement between the two parties on how the data should be communicated, so that both parties can understand it.

Data Representation

Information can be in several formats.

- **Text** – Text is represented as bit patterns designed to represent text symbols. Popular coding systems for text include Unicode, ASCII, etc. ASCII uses just 7 bits and can thus represent a limited number of characters, while Unicode uses 16 bits and can represent any character in the world. Standards like these are required so devices at different places can communicate properly.
- **Numbers** – Numbers also use similar codes, which are directly converted to binary format.
- **Images** – Images are divided into extremely small pixels, each of which has a similar bit pattern. The value of the pattern depends on the colour of the pixel. Pure black and white would only need a single bit per pixel, while more colours need more bits. One method to represent these colours is RGB, where the intensity of red, green and blue light is measured to assign the bit pattern values. Each pixel is given an 8-bit value. Another method is YCM, for yellow, cyan and magenta.
- **Audio** – Audio is completely different, since it is continuous and is in the form of a signal.
- **Video** – Video can be like audio, a continuous signal, or a series of individual images arranged to convey an impression of motion.

Data Flow



Communication between two devices can be of three types:

- **Simplex** – Only one of the devices transmits data, while the other only receives. An example is the keyboard and display.
- **Half-Duplex** – Both devices transmit and receive data, but not at the same time. An example is walkie-talkies.
- **Full-Duplex** – Both devices transmit and receive data at the same time. Examples include any form of phone calls.

1.2. Networks

A network is a group of devices, also called nodes, that can communicate with each other. A node can be any device that can send or receive data, such as a computer, a mobile phone, etc.

Network Criteria

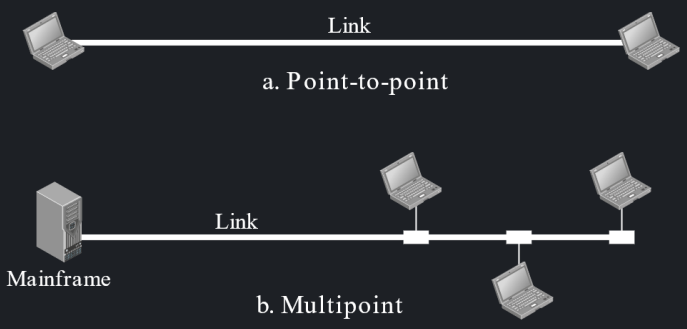
A network has to meet a few criteria, the most important of which are:

- **Performance** – Performance is measured using delay and throughput, which is the amount of data we are sending versus the amount of data we are receiving.
- **Reliability** – This is a measure of how frequently there is data loss and how well these failures are handled.
- **Security** – This has three parts:
    - Confidentiality - Protecting data from unauthorized access
    - Integrity - Protecting data from damage or invalid changes
    - Availability - Making the data available to valid users only. This is to prevent invalid users from taking up all system resources, which denies valid users the service in a denial-of-service (DOS) attack.

There are protocols that are more reliable, but have worse performance and vice versa. Which protocol needs to be used depends on the application. For example, a banking application must be extremely reliable. It cannot have any missing data. However, video conferencing applications need better performance for real-time transmission, since even if some data is lost, users can adjust.

Physical Structures

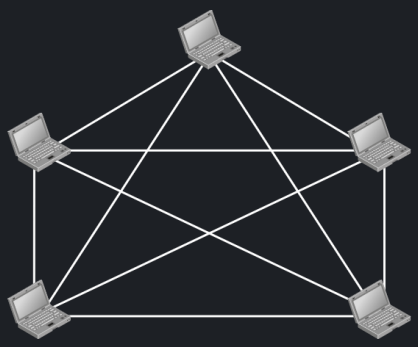
Types of Connection:



- **Point-to-Point** – A dedicated link between two devices
- **Multipoint (Multidrop)** – A single link shared between multiple devices

Physical Topology

Physical topology defines how the network is physically laid out. Two or more devices connect via a link, and two or more links form a topology.



- **Mesh Topology** – Every device on the network is connected to every other device.

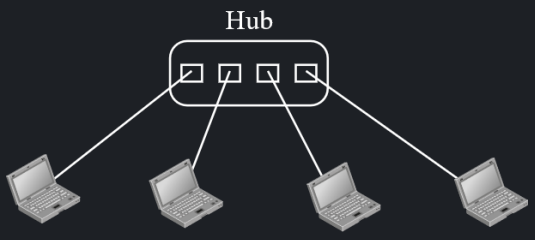
  ☑ Privacy

  ☑ Easy fault detection

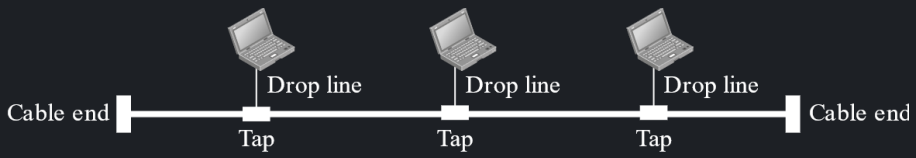
  ☑ Prevention of the system being affected if one link is damaged

  ☑ Elimination of traffic problems

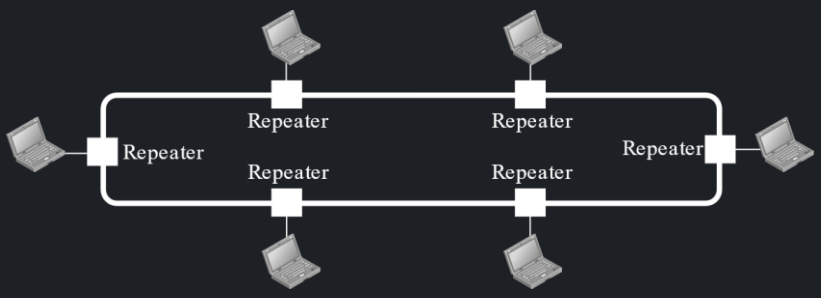
  ☒ Connections are difficult to manage and expensive, especially for physical connections, if the network is very large



- **Star Topology** – Every device is connected to a central device called the hub.
  - ☑ Easy to add or remove devices
  - ☑ Prevents the entire system being affected if one line is defective
  - ☑ Makes fault identification easy
  - ☒ If the hub goes down, the entire system is dead



- **Bus Topology** – All the devices are connected to a single long link. Each device is connected to the main cable via a drop line, and the connection is called a tap.
  - ☑ Easy to connect devices
  - ☑ Less wiring involved
  - ☑ Cable can be laid in an efficient manner
  - ☒ Signal becomes weaker the further it goes, meaning there is a limit
  - ☒ Damage to the cable will stop the system
  - ☒ Fault detection is difficult



- **Ring Topology** – Each device has a point-to-point connection with the two devices on either side of it. Signals are passed from device to device in a ring until the destination is reached.
  ☑ Each device acts as a repeater, keeping the signal strong
  ☑ Fault identification is easy
  ☑ Easy to change the configuration of the topology
  ☒ A break in the ring disables the network

Categories of Networks

Networks are divided into three categories based on size, ownership, coverage and physical architecture: LAN, MAN and WAN. Metropolitan Area Networks (MANs) will not be discussed here.

Local Area Network (LAN)

LANs are usually privately owned by organizations for their private use and connect hosts in a single building, office or campus. Each host has a uniquely identifiable address in the LAN. A packet of data will carry both the source and destination hosts' addresses.

Wide Area Network (WAN)

WANs span large areas, like a city, country or even the world. They connect devices like routers, modems and switches. Organizations do not privately own WANs, but rather lease them from communication companies. WANs can be of two types:

- **Point-to-Point** – Two devices on completely different locations are connected using connecting devices, such as modems, with the actual connection being made using a WAN.

- **Switched** – This has more than two ends, and can be thought of as several point-to-point WANs connected via switches.

Internetworks

When two or more networks are connected to each other, they make an internetwork, or internet. When using a lower case ‘i’, this refers to a private connection, such as the LAN networks of two offices of a single company. When using an upper case ‘I’, this refers to the global Internet.

1.3 The Internet

```
=== Skipping Section: A Brief History - No Questions will be asked from here ===
```

The Internet Today

There is a hierarchical organization to the internet today. Individual users connect to ISPs. ISPs connect to regional ISPs via routers, which handle relatively small amounts of data. They in turn connect to national ISPs. National ISPs allow different countries to be connected via network access points, which handle humongous amounts of data.

1.4 Protocols and Standards

Protocols

Protocols govern what data is communicated, how it is communicated and when it is communicated. A protocol has three main elements:

- **Syntax** – The format of the data, such as how many bits to use for the address
- **Semantics** – The meaning of the different sections of bits
- **Timing** – When should the data be sent and how fast

A few commonly known internet protocols are:

IPv4 IPv6 HTTP HTTPS TCP FTP SSH DNS POP IMAP

Standards

Standards are essentially guidelines that manufacturers must follow so that products from different manufacturers are able to work together. Standards fall into two categories:

- **De facto** – These are not approved by an organized body, but are generally followed
- **De jure** – These are set by an officially recognized body

Standards Organizations

Standards are created by certain organizations, and the one responsible for internet standards is called the Internet Society (ISOC). They are given technical advice by the Internet Architecture Board (IAB). The IAB has two subdivisions, the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF).