S.Y.B.Sc.IT - SEM III

COPMUTER NETWORKS (PUSIT303)

By,

Nikita Madwal

❖ REFERENCE BOOK

1. Data Communication and Networking, Behrouz A. Forouzan, Tata McGraw Hill, Fifth Edition, 2013

2. Computer Networks, Andrew Tanenbaum, Pearson, Fifth Edition, 2013

3. TCP/IP Protocol Suite, Behrouz A. Forouzan, Tata McGraw Hill, Fourth Edition, 2010

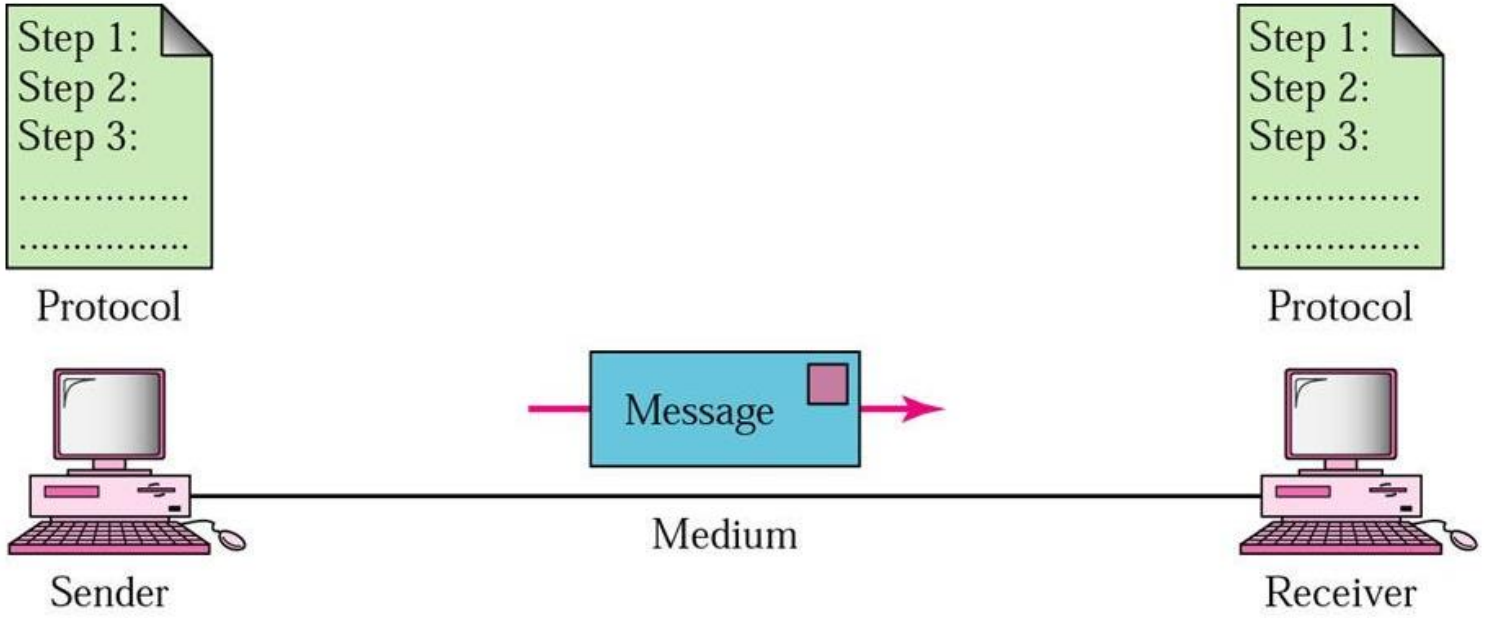
UNIT 1

1. INTRODUCTION

1. INTRODUCTION

Data Communication

- Data communications are the **exchange of data between two devices via some form of transmission medium such as a wire cable.**



- The **effectiveness of a data communications system depends** on **four fundamental characteristics** are :

- 1. **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.
- 2. **Accuracy :**
  - The **system must deliver** the **data accurately**.
  - **Data** that **have been altered (change) in transmission and left uncorrected** are **unusable**.

- 3. **Timeliness :**
  - The **system must deliver data** in a **timely manner**.
  - Data **delivered late** are **useless**.
  - In the **case of video and audio**, **timely delivery means delivering data as they are produced**, in the same order that they are produced, and **without significant delay**.
  - This kind of delivery is **called real-time transmission.**
- 4. **Jitter :**
  - Jitter refers to the **variation in the packet arrival time**.
  - It is the **uneven delay in the delivery of audio or video packets**.
  - For example, let us assume that video packets are sent every 30-ms. If some of the packets arrive with 30-ms (milliseconds) delay and others with 40-ms delay, an uneven quality in the video is the result.

❖Five components of data communication system

- **1. Message**
  - The message is **the information (data) to be communicated**.
  - Popular forms of **information include text, numbers, pictures, audio, and video.**
- **2. Sender**
  - The **sender** is the **device** that **sends the data message**.
  - It **can be a computer, workstation, telephone handset, video camera**, and so on.
- **3. Receiver**
  - The **receiver** is the **device** that **receives the message**.
  - It can be a **computer, workstation, telephone handset, television, and so on**.

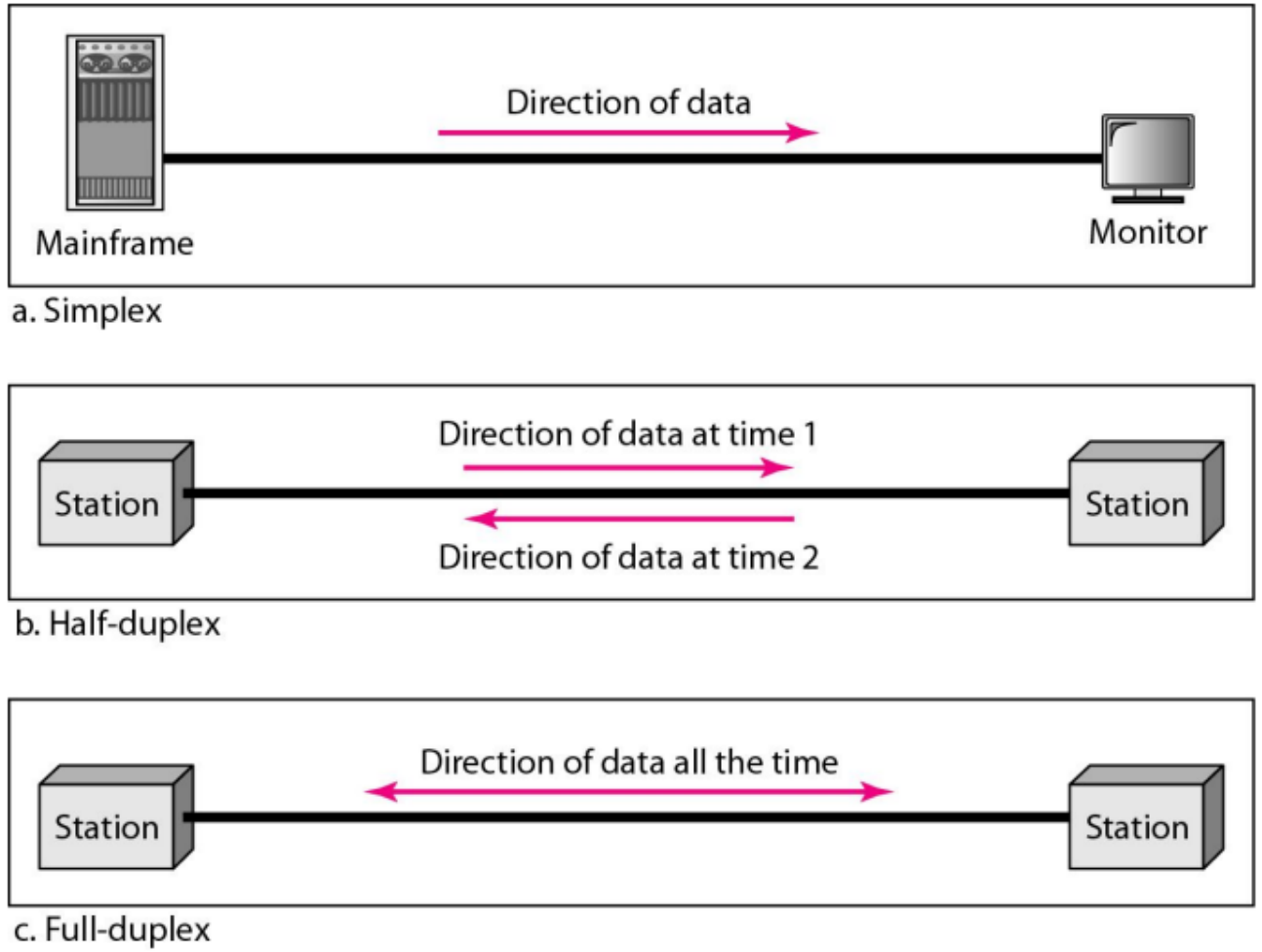
- **4. Transmission medium**
  - The transmission medium is the **path by which a message travels from sender to receiver**.
  - Some examples of transmission media include **twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves**
- **5. Protocol.**
  - A protocol is a **set of rules** that **govern (control) data communications**.
  - It represents an agreement between the communicating devices.
  - **Without a protocol**, two devices **may be connected <u>but not communicating</u>**, just as a person speaking French cannot be understood by a person who speaks only Japanese.

❖Data Representation

- Information today comes in different forms such as text, numbers, images, audio, and video.

❖Data Flow (Transmission Modes)

- The data can flow between the two devices in the following ways.
- 1. Simplex 2. Half Duplex 3. Full Duplex



❖1. Simplex

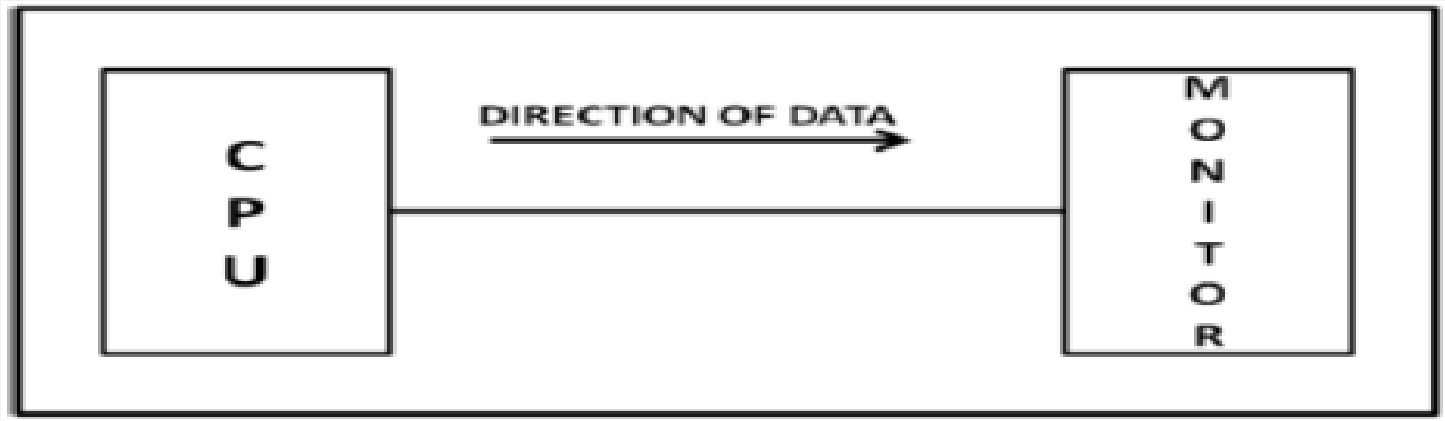


Figure: Simplex mode of communication

- 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**.
- Here, the **entire capacity** of the channel to **send data in one direction.**

❖2. Half Duplex

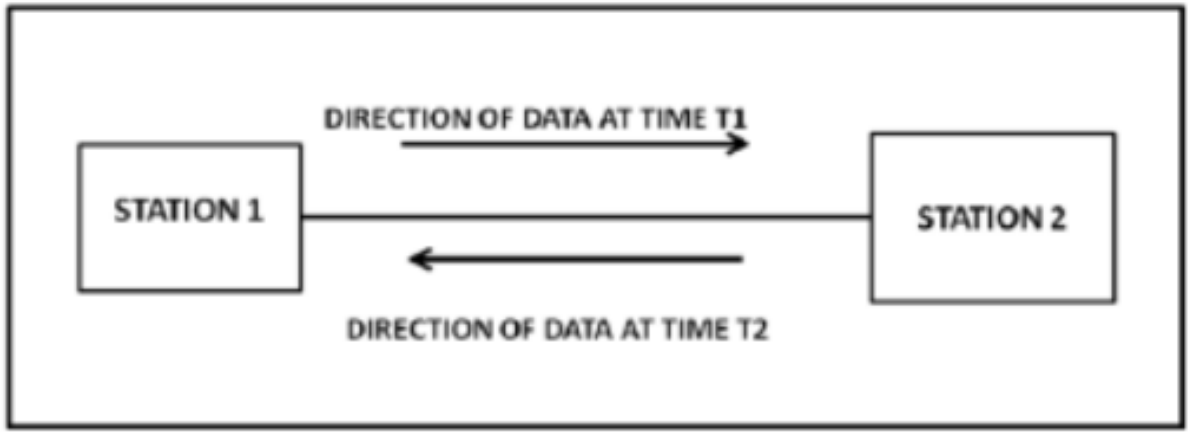


Figure: Half Duplex Mode of Communication

- 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.
- Example: **A walkie-talkie**.
- The **entire capacity** of the channel can be **utilized for each direction**.

- **3. Full Duplex**

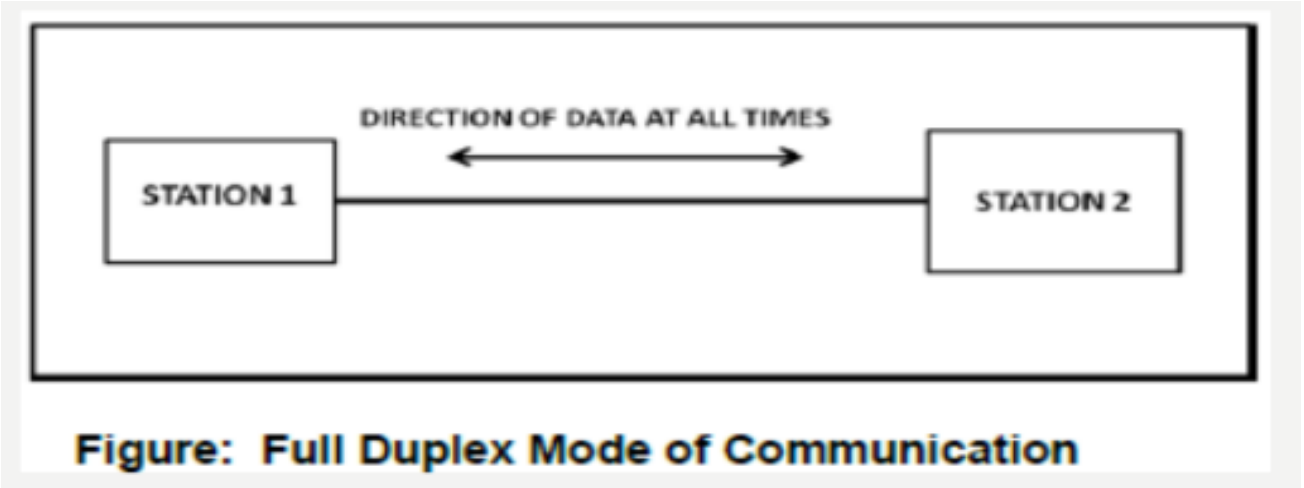


Figure: Full Duplex Mode of Communication

- In Full duplex mode, **both stations can transmit and receive simultaneously i.e. at same time.**
- In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other directions.
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.
- Example: **mobile phones**

Networks

- A network is the **interconnection of a set of devices capable of communication**.
- In this definition, **a device can be a host** (or an **end system** as it is sometimes called) such as a **large computer, desktop, laptop, workstation, cellular phone, or security system**.
- A **device** in this definition **can** also be a **connecting device such as a router**, which **connects the network to other networks**, a ***switch***, which ***connects devices together***, a **modem** (**modulator-demodulator**), which changes the form of data, and so on.
- These **devices** in a network **are connected using wired or wireless transmission media** such as **cable or air**. When we connect two computers at home using a plug-and-play router, we have created a network, although very small.

❖Network Criteria

- A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

- **1. Performance**
  - Performance can be measured in many ways, including **transit time and response time**.
  - **Transit time** is the ***amount of time required for a message to travel from one device to another.***
  - **Response time** is the ***elapsed time between an inquiry and a response***.
  - The **performance of a network depends** on a number of factors, including the **number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.**

- Performance is often evaluated by two networking metrics: **throughput and delay.**
- **Throughput** is a measure of **how many units of information a system can process in a given amount of time**.
- **We often need more throughput and less delay**. However, these two **criteria are often contradictory**.
- If we try to send **more data** to the network, we may **increase throughput but we increase the delay** because of traffic congestion in the network.

- **2. Reliability**

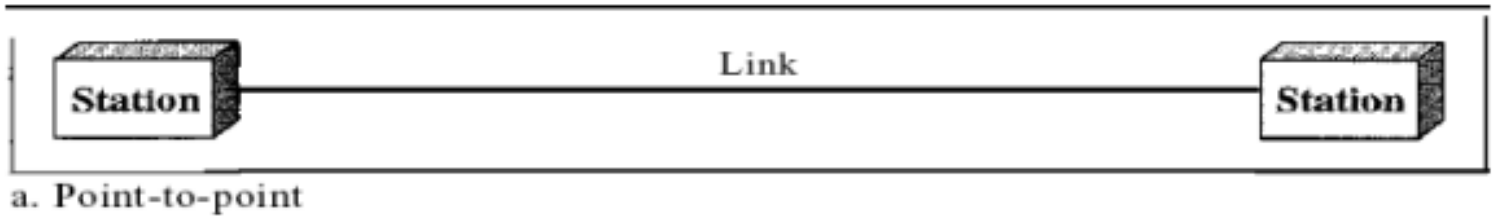
- In addition to accuracy of delivery, network **reliability is measured** by the **frequency of failure**, the **time it takes a link to recover from a failure**, and the **network's robustness in a catastrophe**.

- **3. Security**
  - Network security issues include **protecting data from unauthorized access**, **protecting data from damage and development**, and implementing policies and procedures for recovery from breaches(breaking or violating) and data losses.

❖Types of Connection

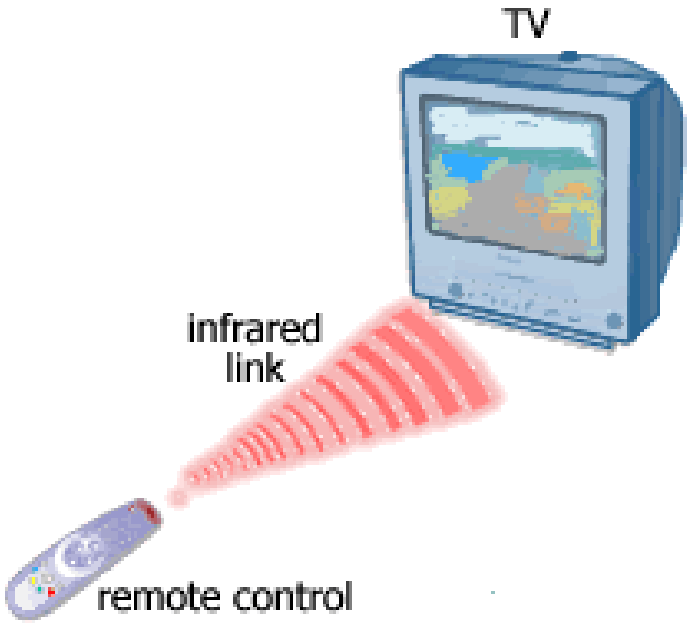
- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.
- **There are two possible types of connections: point-to-point and multipoint**

❖1. Point – to – Point

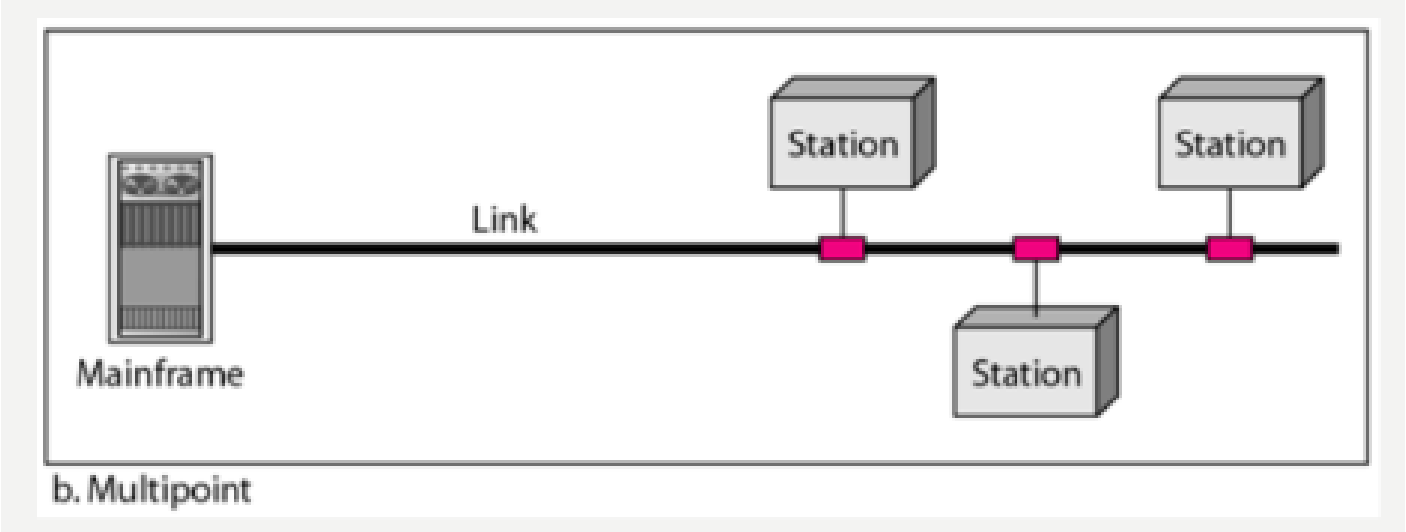


a. Point-to-point

- 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**.
- Most point-to-point connections **use an actual length of wire or cable to connect the two ends**, but other options, such as **microwave or satellite links, are also possible**.
- When we change television channels by infrared remote control, we are establishing a point-to- point connection between the remote control and the television's control system.



❖2. Multipoint

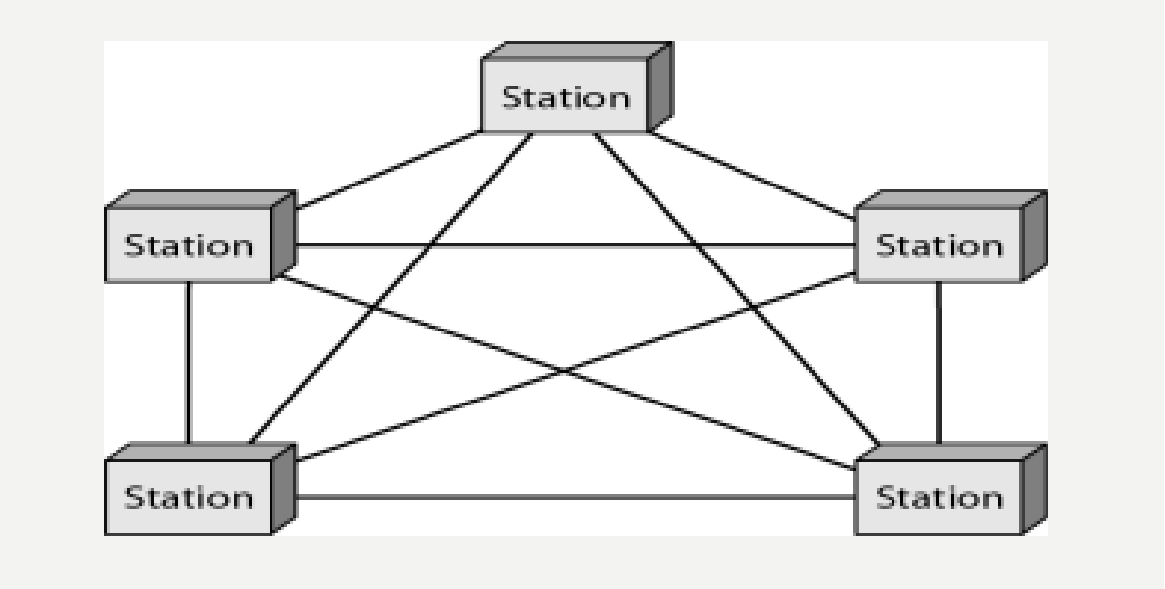


- A multipoint (also called multidrop) **connection is one** in which **more than two specific devices share a single link** .
- In a multipoint environment, the **capacity of the channel is shared**, either spatially or temporally.
- If several devices can use the link simultaneously, it is a spatially shared connection.

❖Physical Topology

- The **structure of a network** is **referred** as **topology**.
- The term physical topology refers to the way in which a **network is laid out physically**. Two or more devices connect to a link; two or more links form a topology.
- 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.
- However, the **complete physical structure of the cable** (or transmission media) is **called the physical topology**.
- The **physical topology of a network refers** to the **configuration of cables, computers, and other peripherals**.
- There are **four basic topologies** possible: ***mesh, star, bus, and ring***.

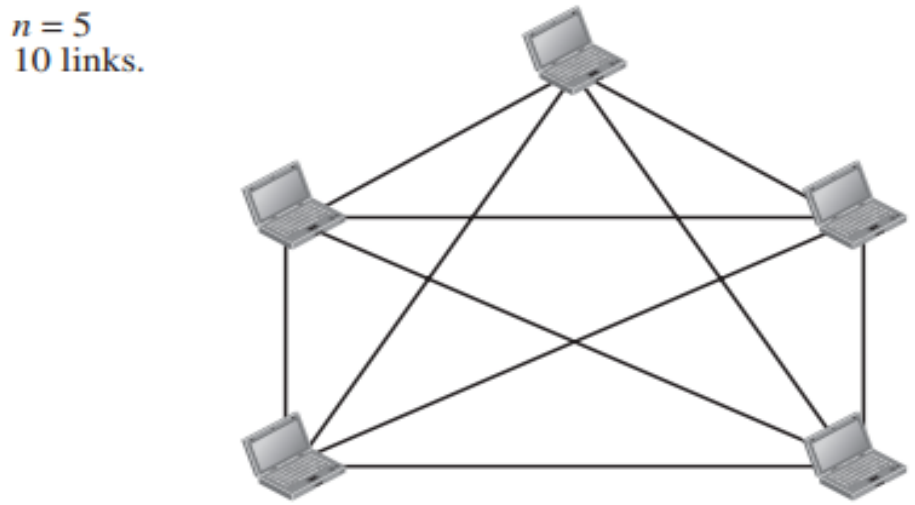
- **1. Mesh Topology**



- In Mesh Topology, **each and every nodes are interconnected with one another**.
- Every device has a **dedicated point-to-point link** to every other device.
- Every **device is connected to another via dedicated channels**. These channels are **known as links**.

- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node.
- Node 1 must be connected to n – 1 nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n – 1 nodes.
- **We need n (n – 1) physical links**.
- To accommodate that many links, every device on the network must have n – 1 input/output (I/O) ports (see Figure 1.4) to be connected to the other n – 1 stations.

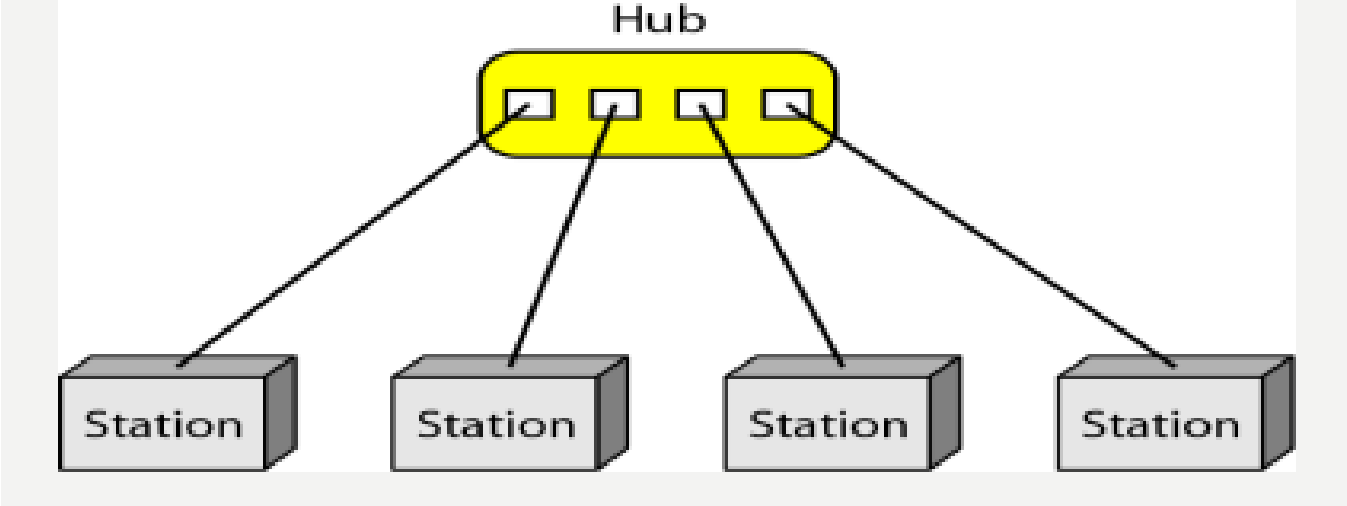
Figure 1.4 *A fully connected mesh topology (five devices)*



- **Advantage**
- The use of dedicated links **guarantees that each connection can carry its own data load**, thus **eliminating the traffic** problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If **one link becomes unusable**, it **does not disable/stop** the **entire system**.
- **Privacy or security** : When every **message travels along a dedicated line**, only the **intended recipient sees it**. ***Physical boundaries prevent*** other users from ***gaining access to messages***.
- point-to-point links **make fault identification and fault isolation easy**. **Traffic** can be **routed to avoid links with suspected problems**. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

- **Disadvantage**
- Disadvantages of a mesh are related to the **amount of cabling and the number of I/O ports required**.
- Installation and reconnection are difficult.
- The **total bulk of the wiring can be greater** than the available space (in walls, ceilings, or floors) can accommodate.
- The hardware required to connect each link (I/O ports and cable) can be expensive.
- **Application**
- One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

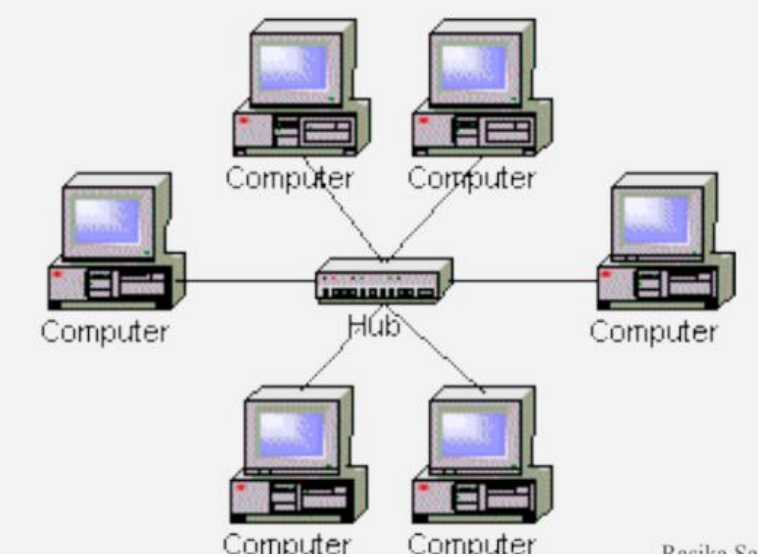
- **2. Star Topology**



- In a star topology, **each device has a dedicated point-to-point link** *only to a central controller*, usually *called a hub*.
- The **devices are not directly linked to one another**.
- A star topology does not allow direct traffic between devices.
- The controller acts as an exchange: If **one device wants to send data to another**, *it sends the data to the controller*, which then **relays the data to the other connected device**.

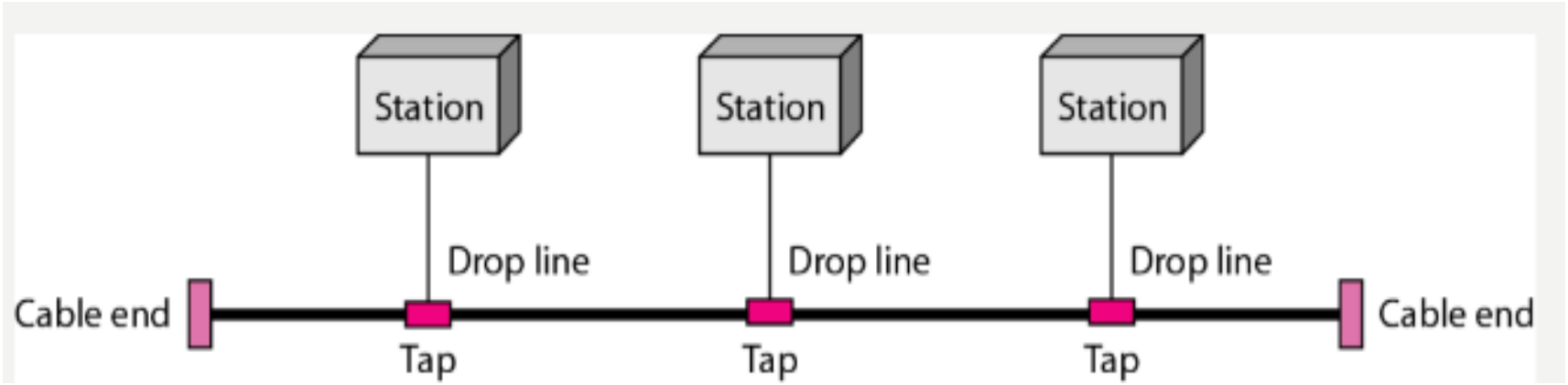
- **Advantages**
- A star topology is **less expensive than a mesh topology**.
- In a star, **each device needs only one link** and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.
- **Far less cabling needs to be housed**, and additions, moves, and deletions involve only one connection: between that device and the hub.
- **Robustness:** If **one link fails**, *only that link is affected*. All other links remain active.
- This factor also lends itself to easy fault identification and fault isolation.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.

- **Disadvantages**
- **Single point of failure :** star topology is the **dependent on the hub**. If the *hub goes down, the whole system is dead*.
- Although a star requires **far less cable than a mesh**, each node must be linked to a central hub. For this reason, often *more cabling is required in a star than in some other topologies (such as ring or bus).*
- **Application**
- The star topology is used in local-area networks (LANs).
- High-speed LANs often use a star topology with a central hub.



NIKITA MADWAL

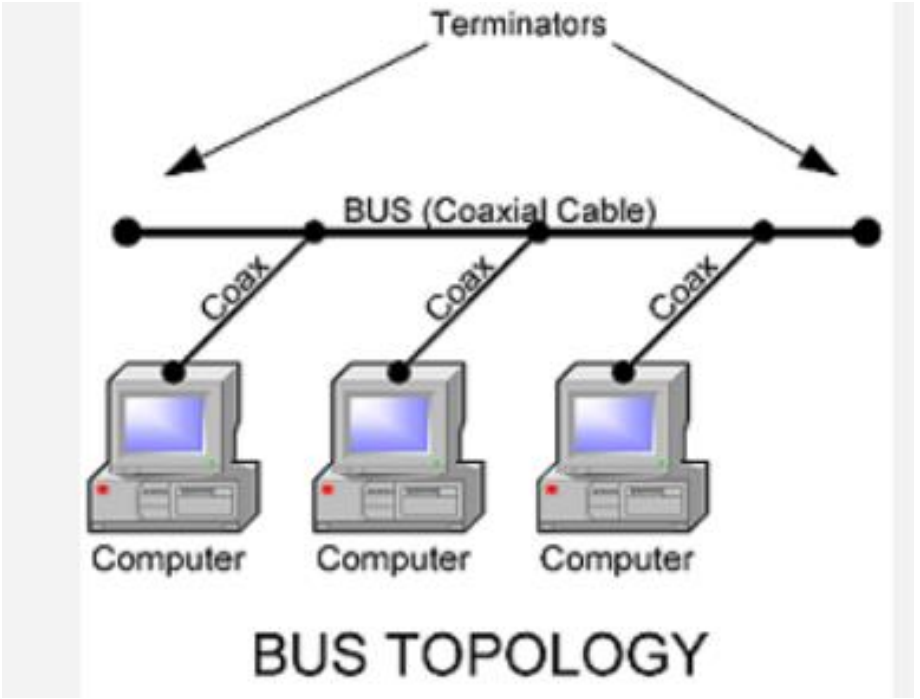
- **3. Bus Topology**



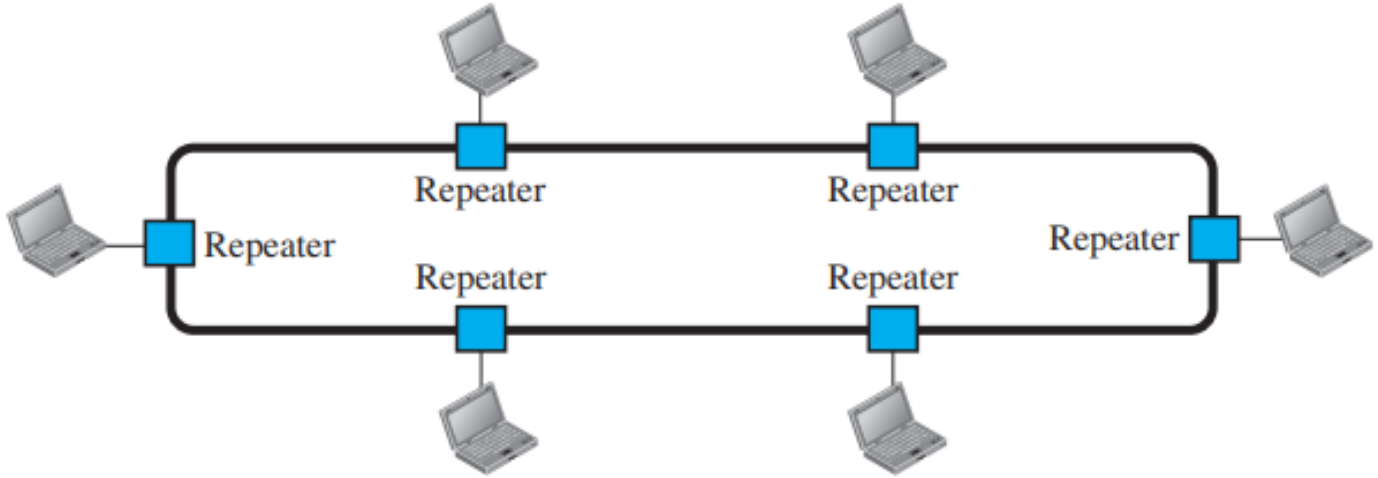
- A bus topology is multipoint. **One long cable acts as a backbone to link all the devices in a network.**
- Nodes are **connected** to the bus cable by **drop lines and taps**.
- A **drop line** is a connection **running between the device and the main cable**.
- A **tap** is a connector that either splices (connect) into the main cable or punctures (disconnect) the covering of a cable to create a contact with the metallic core.

- **Advantages**
- Ease of installation.
- Bus uses **less cabling than mesh or star topologies**.
- In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated.
- Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.
- Bus topology costs very less.

- **Disadvantages**
- **Difficult reconnection and fault isolation**.
- **Scalability Problem :Difficult to add new devices.** Adding new devices may therefore require modification or replacement of the backbone.
- A **fault or break in the bus cable stops all transmission**, even between devices on the same side of the problem.
- Bus topology was the one of the first topologies used in the design of early local area networks.
- **Application**
- Ethernet LANs can use a bus topology.



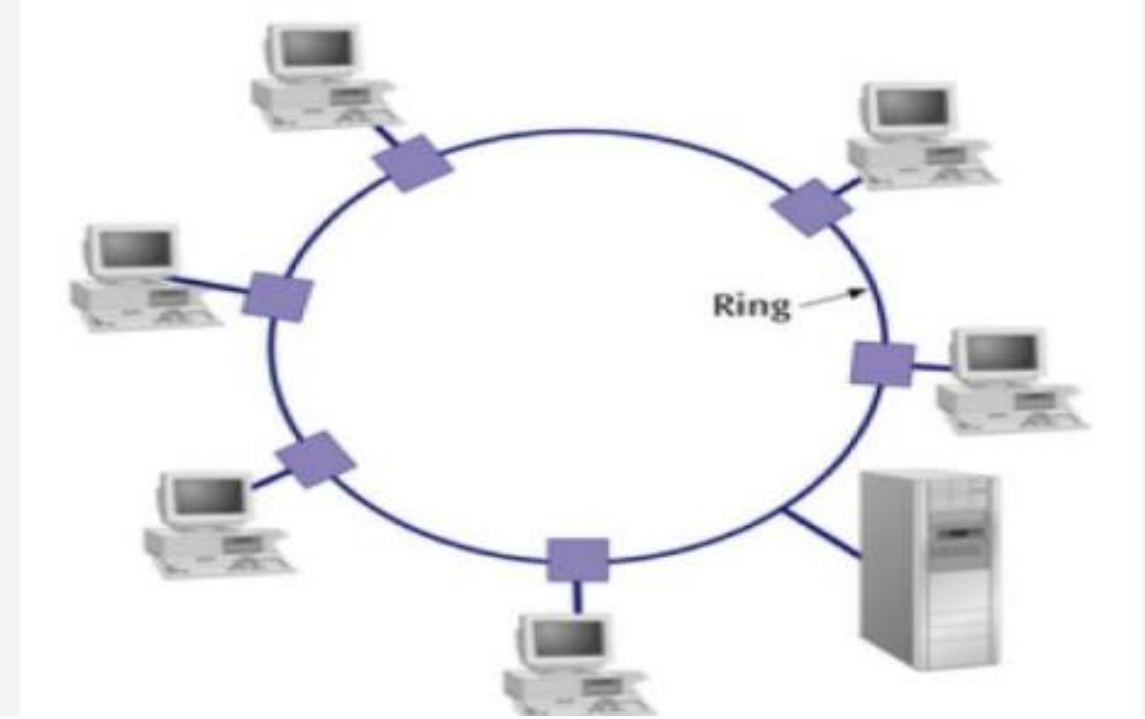
- **4. Ring Topology**



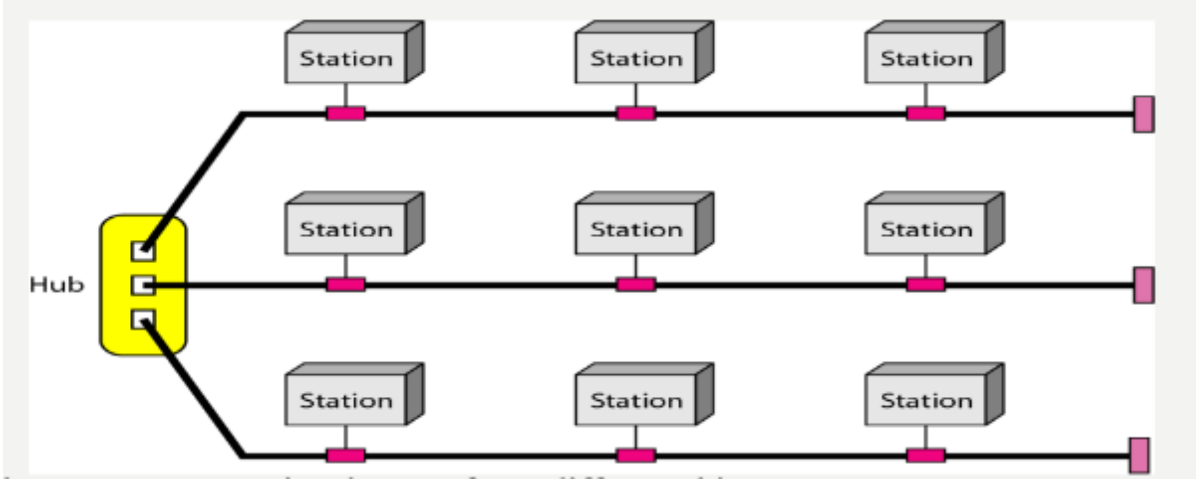
- In a ring topology, **each device has a dedicated point-to-point connection with only the two devices on either side of it**.
- A **signal is passed** along the ring in **one direction**, from device to device, **until it reaches its destination**.
- Each device in the **ring incorporates a repeater**.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

- **Advantages**
- Easy to install and reconfigure.
- Each device is **linked to only its immediate neighbors**
- To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).
- In addition, fault isolation is simplified.
- Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.
- **Disadvantages**
- unidirectional traffic can be a disadvantage.
- In a simple ring, **a break in the ring** (such as a disabled station) can **disable the entire network**.

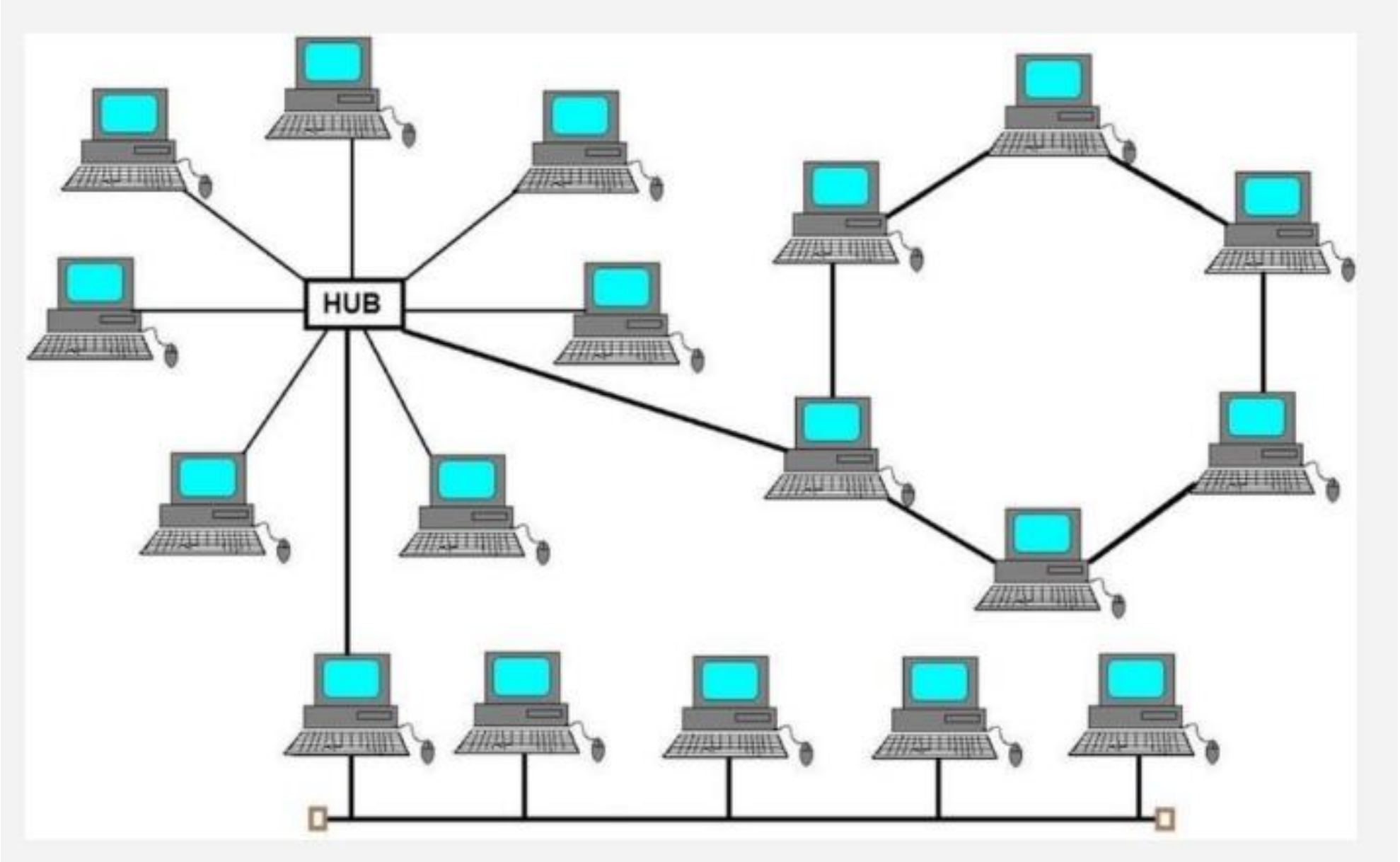
- **Application**
- Ring topology was prevalent when IBM introduced its local-area network, Token Ring.
- Today, the need for higher-speed LANs has made this topology less popular.



- **5. Hybrid Topology**



- Hybrid, as the name suggests, is **mixture of two different things**.
- Similarly in this type of topology we integrate two or more different topologies to form a resultant topology which has good points(as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology.
- This combination of topologies is done according to the requirements of the organization.
- For example, if there exists a ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology.

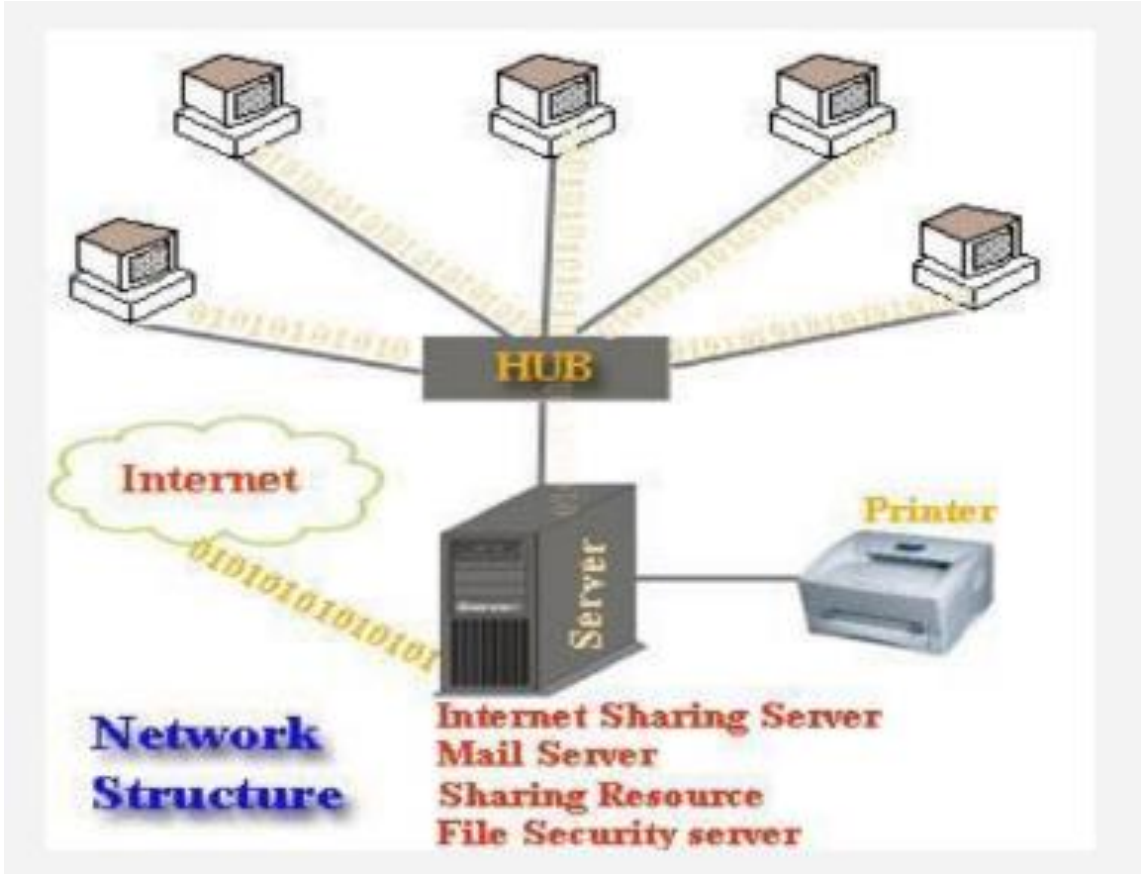


NIKITA MADWAL

Network Types

- After defining networks in the previous section and **discussing their physical structures**, we need to **discuss different types of networks** we encounter in the world today.
- We use a few criteria such as size, geographical coverage, and ownership to make this distinction.
- **Two types of networks**:
- 1) LANs
- 2) MANs
- 2) WANs

- **1. Local Area Network**

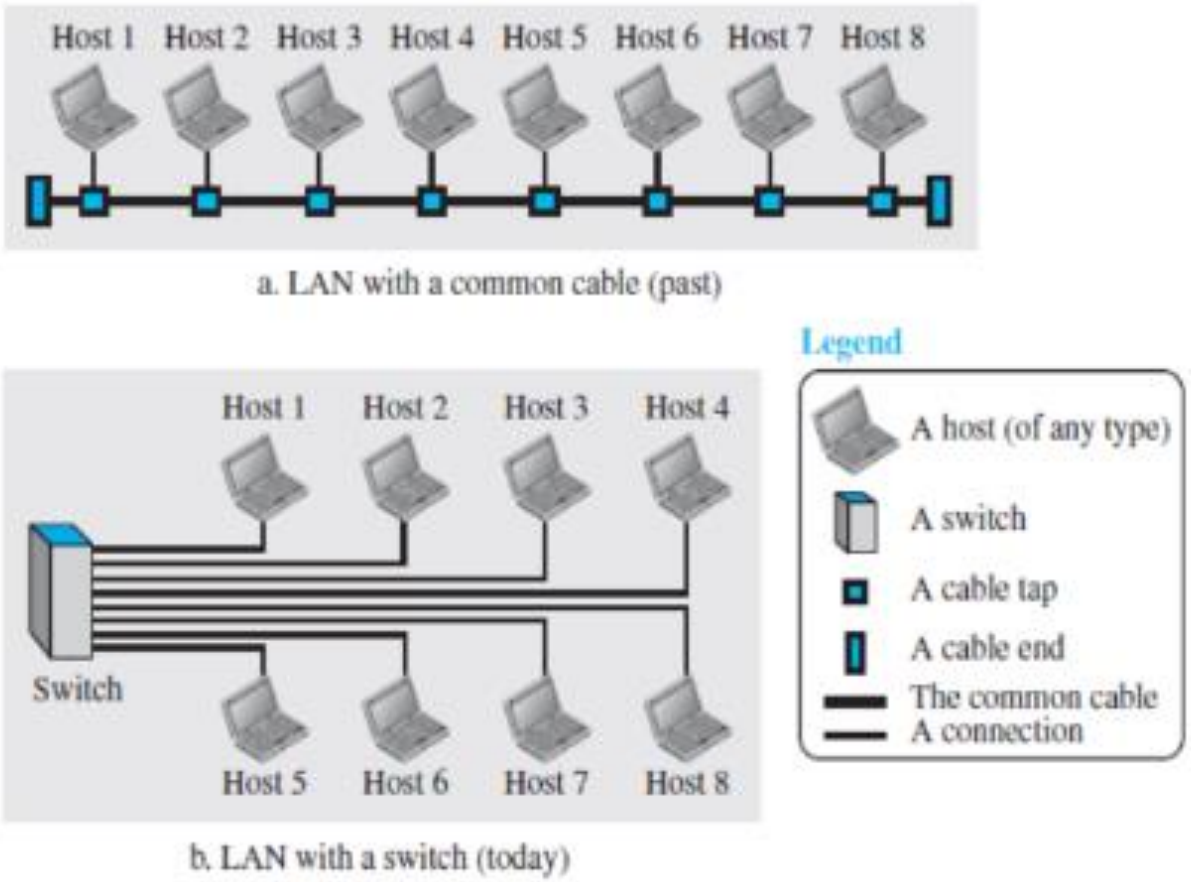


- A local area network (LAN) is **usually privately owned and connects some hosts in a single office, building, or campus**.
- Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices.

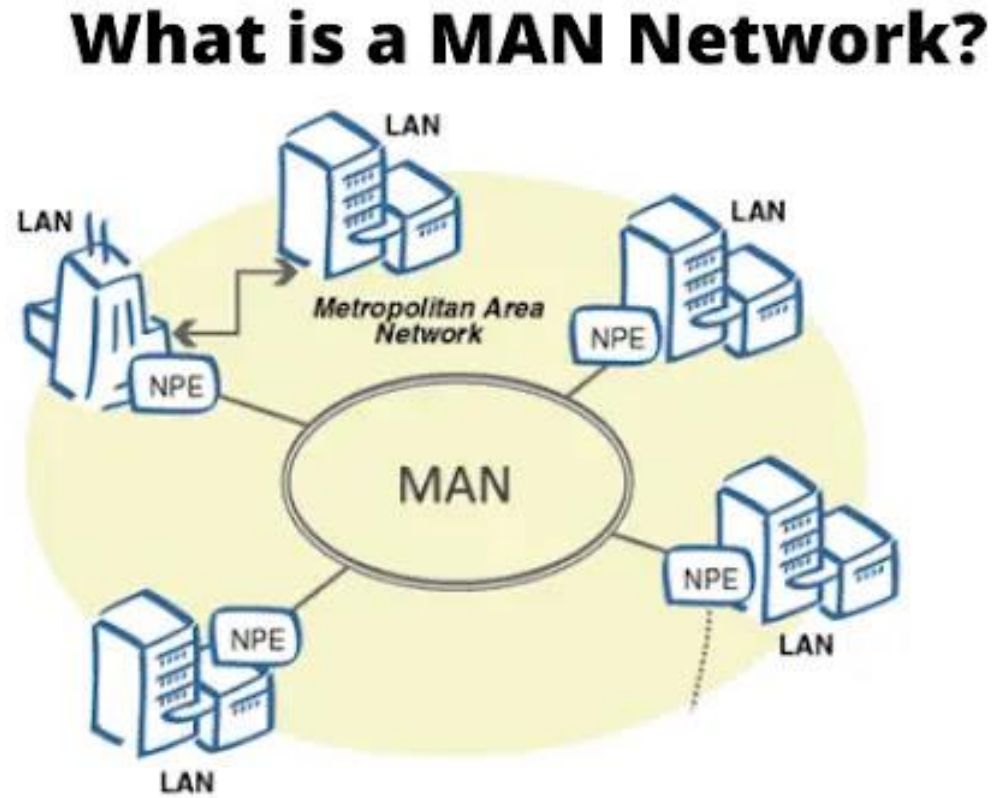
- Each **host in a LAN has an identifier, an address**, that **uniquely defines the host in the LAN**.
- A **packet sent by a host to another host carries** both the **source host's and the destination host's addresses.**
- **In the past**, **all hosts in a network** were **connected through a common cable**, which meant that a **packet sent from one host to another was received by all hosts.**
- The **intended recipient kept the packet**; the **others dropped the packet**.
- Today, most LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.
- The switch alleviates (reduce) the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them.
- Figure 1.8 shows a LAN using either a common cable or a switch.

- When LANs were used in isolation (which is rare today), they were designed to allow resources to be shared between the hosts.
- LANs today are connected to each other and to WANs to create communication at a wider level.

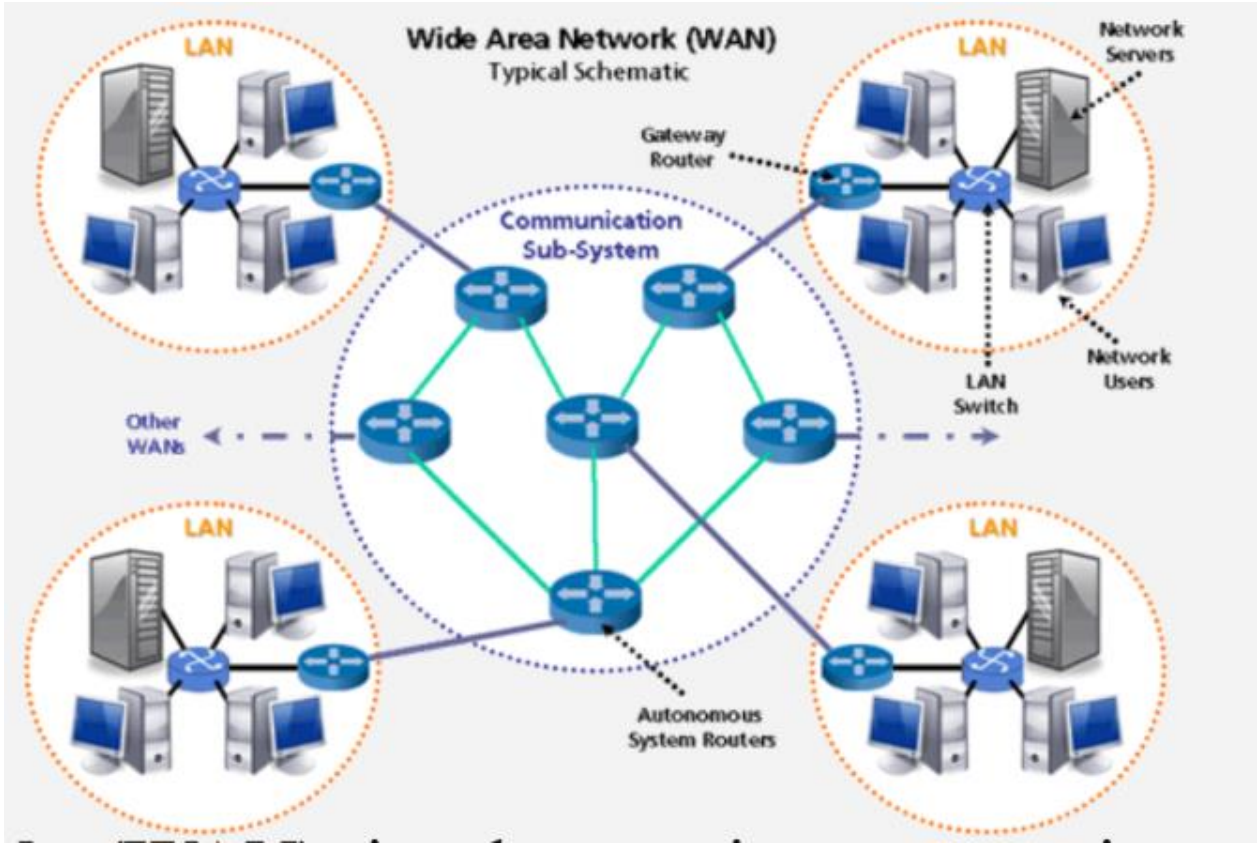
Figure 1.8 *An isolated LAN in the past and today*



- **2. Metropolitan Area Network**
- The Metropolitan Area Network (MAN) is a network type that covers the **network connection of an entire city or connection of a small area**
- The area covered by the network is connected using a wired network, like data cables.
- This **type of network is large than a LAN**
- MAN network **works in between LAN and WAN**
- In MAN, mostly used **medium is optical fibers** which results in high-speed connectivity.

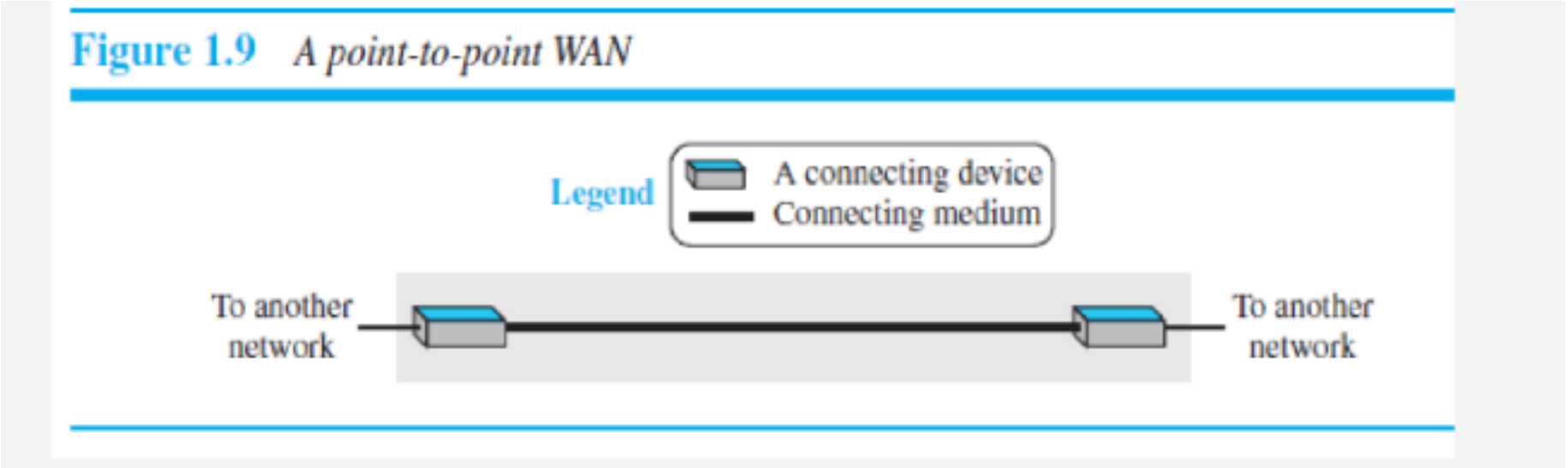


- **3. Wide Area Network**



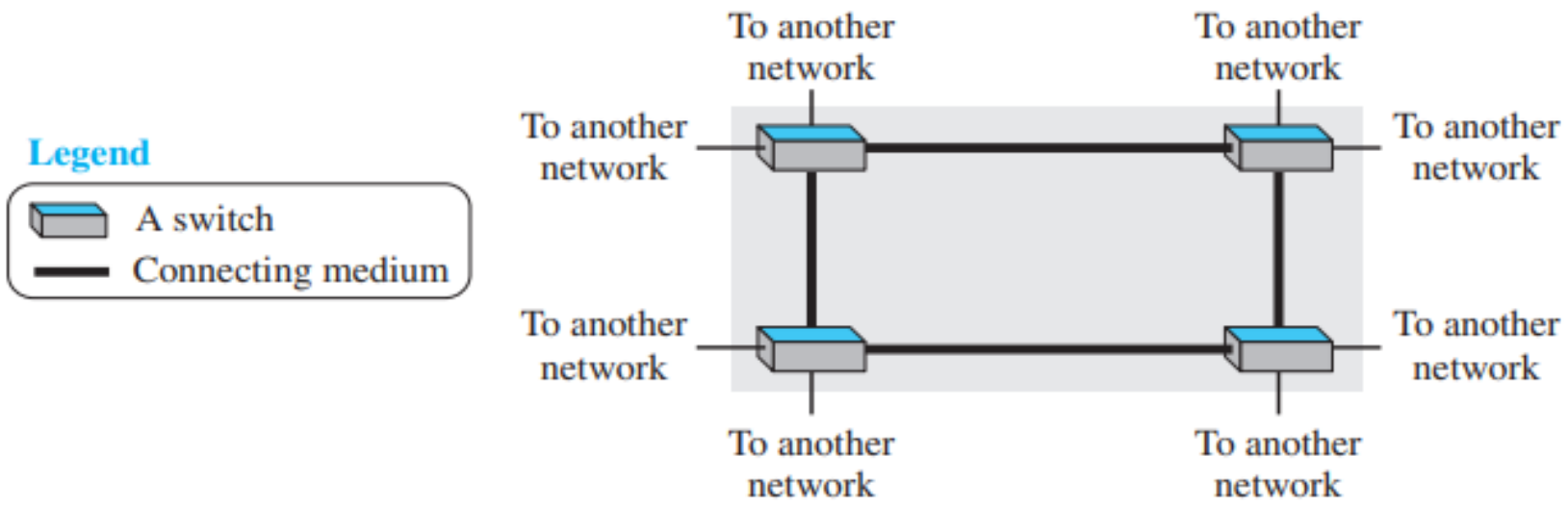
- A wide area network (WAN) is also an **interconnection of devices capable of communication.**
- However, there are some differences between a LAN and a WAN. A **LAN is normally limited in size**, spanning an office, a building, or a campus; a **WAN has a wider geographical span**, spanning a town, a state, a country, or even the world. A **LAN interconnects hosts**; a **WAN interconnects connecting devices such as switches, routers, or modems.**

- A **LAN is normally privately owned by the organization that uses it**; a **WAN is normally created and run by communication companies and leased by an organization that uses it.**
- Two distinct examples of WANs today: point-to-point WANs and switched WANs.
- **1. point – to – point WAN**
- A point-to-point WAN is a **network that connects two communicating devices through a transmission media (cable or air).**
- Figure 1.9 shows an example of a point-to-point WAN.



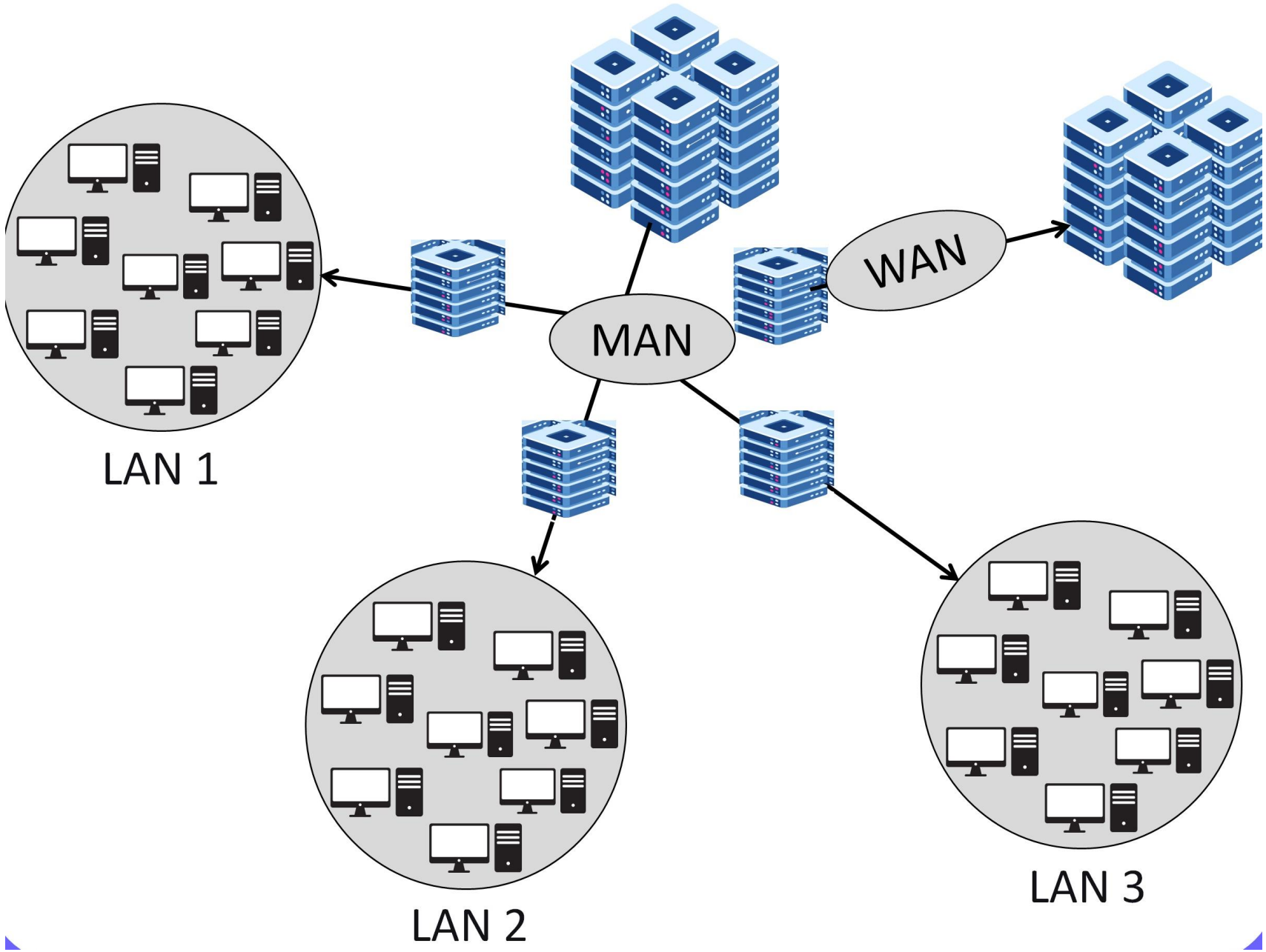
- **2. Switched WAN**
- A **switched WAN is a network** with **more than two ends**.
- A switched WAN, is used in the backbone of global communication today.
- A switched WAN is a **combination of several point-to-point WANs** that are connected by switches.
- Figure 1.10 shows an example of a switched WAN.

Figure 1.10 *A switched WAN*



Difference between LAN , MAN and WAN

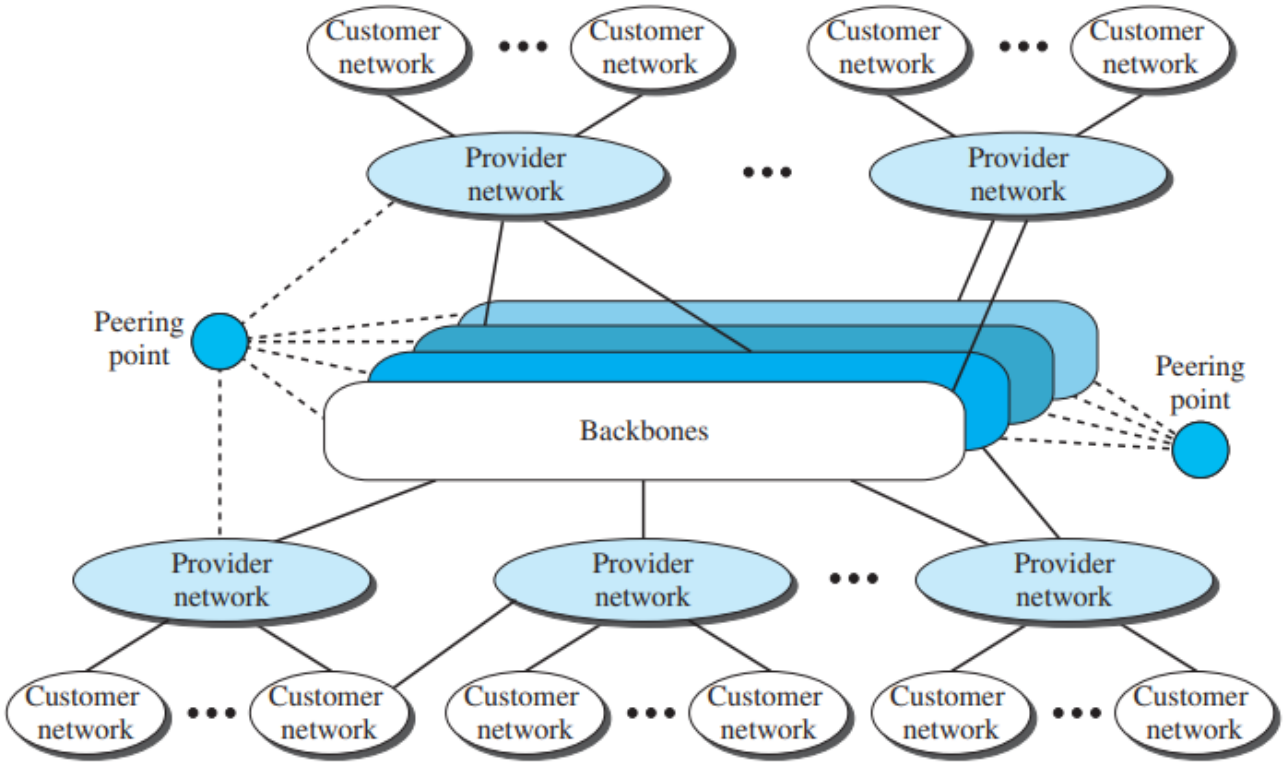
Parameter	LAN	MAN	WAN
Full Form	Local Area Network.	Metropolitan Area Network.	Wide Area Network.
Definition & Meaning	LAN covers small areas such as the same office or building.	MAN covers a large area such as a city or town.	WAN can cover a large geographical area such as country, continent, etc.
Delay in Propagation	It faces a very short propagation delay.	It faces a moderate propagation delay.	It faces a high propagation delay.
Speed	The Internet speed provided through LAN is fast.	MAN provides a modest Internet connection speed.	WAN provides a slow Internet connection.
Congestion	Congestion is less in the LAN network.	It is more in MAN.	Congestion is more in WAN when compared to LAN and MAN.
Design & Maintenance	LAN's design and maintenance are easy.	While MAN's design and maintenance are difficult than LAN.	Whereas WAN's design and maintenance are also difficult than LAN as well MAN.


WAN
MAN
LAN 1
LAN 2
LAN 3

Internet

- An internet (note the **lowercase i**) is **two or more networks that can communicate with each other.**
- The most notable internet is called the Internet (**uppercase I**), and is **composed of thousands of interconnected networks.**

Figure 1.15 *The Internet today*



- Figure 1.15 shows a **conceptual** (not geographical) **view of the Internet**.
- The figure shows the **Internet as several backbones, provider networks, and customer networks.**
- At the **top level, the backbones** are **large networks** owned **by some communication companies** such as Sprint, Verizon (MCI), AT&T (American Telephone & Telegraph) , and NTT.
- The **backbone networks are connected through some complex switching systems, called peering** points.
- At **the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee**.
- The provider networks are connected to backbones and sometimes to other provider networks.
- The ***customer networks are networks*** at the edge of the Internet that actually use the services provided by the Internet.
- They ***pay fees to* provider networks *for receiving services***.

- **Backbones and provider networks** are also called **Internet Service Providers (ISPs).**
- The backbones are often referred to as international ISPs; the provider networks are often referred to as national or regional ISPs.

❖Accessing the Internet

- The Internet today is an internetwork that allows any user to become part of it.
- The user, however, needs to be physically connected to an ISP.
- The physical connection is normally done through a point-to-point WAN.
- In this section, we briefly describe how this can happen

- **1. Using Telephone Networks**
- Today most residences and small businesses have telephone service, which means they are connected to a telephone network.
- Since most telephone networks have already connected themselves to the Internet, one option for residences and small businesses to connect to the Internet is to change the voice line between the residence or business and the telephone center to a point-to-point WAN. This can be done in two ways.
- 1) Dial-up service.
- 2) DSL Service.
- **1. Dial-up service.**
- The first solution is to add to the telephone line a modem that converts data to voice.
- The **software installed on the computer dials the ISP and imitates making a telephone connection.**

- Unfortunately, the **dial-up service is very slow, and when the line is used for Internet connection, it cannot be used for telephone (voice) connection.**
- It is only useful for small residences.
- **2. DSL Service.**
- Since the advent of the Internet, some telephone companies have upgraded their telephone lines to provide **higher speed Internet services to residences or small businesses.**
- The DSL service also allows the line to be used **simultaneously for voice and data communication.**

- **2. Using Cable Network**
- More and more residents over the last two decades have begun using able TV services instead of antennas to receive TV broadcasting.
- The **cable companies** have been **upgrading their cable networks and connecting to the Internet.**
- A residence or a small business can be connected to the Internet by using this service.
- It provides a higher speed connection, but the **speed varies depending on the number of** neighbors that use the same cable.

- **3. Using Wireless Networks**
- **Wireless connectivity has recently become increasingly popular.**
- A household or a small business can use a combination of wireless and wired connections to access the Internet.
- With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.

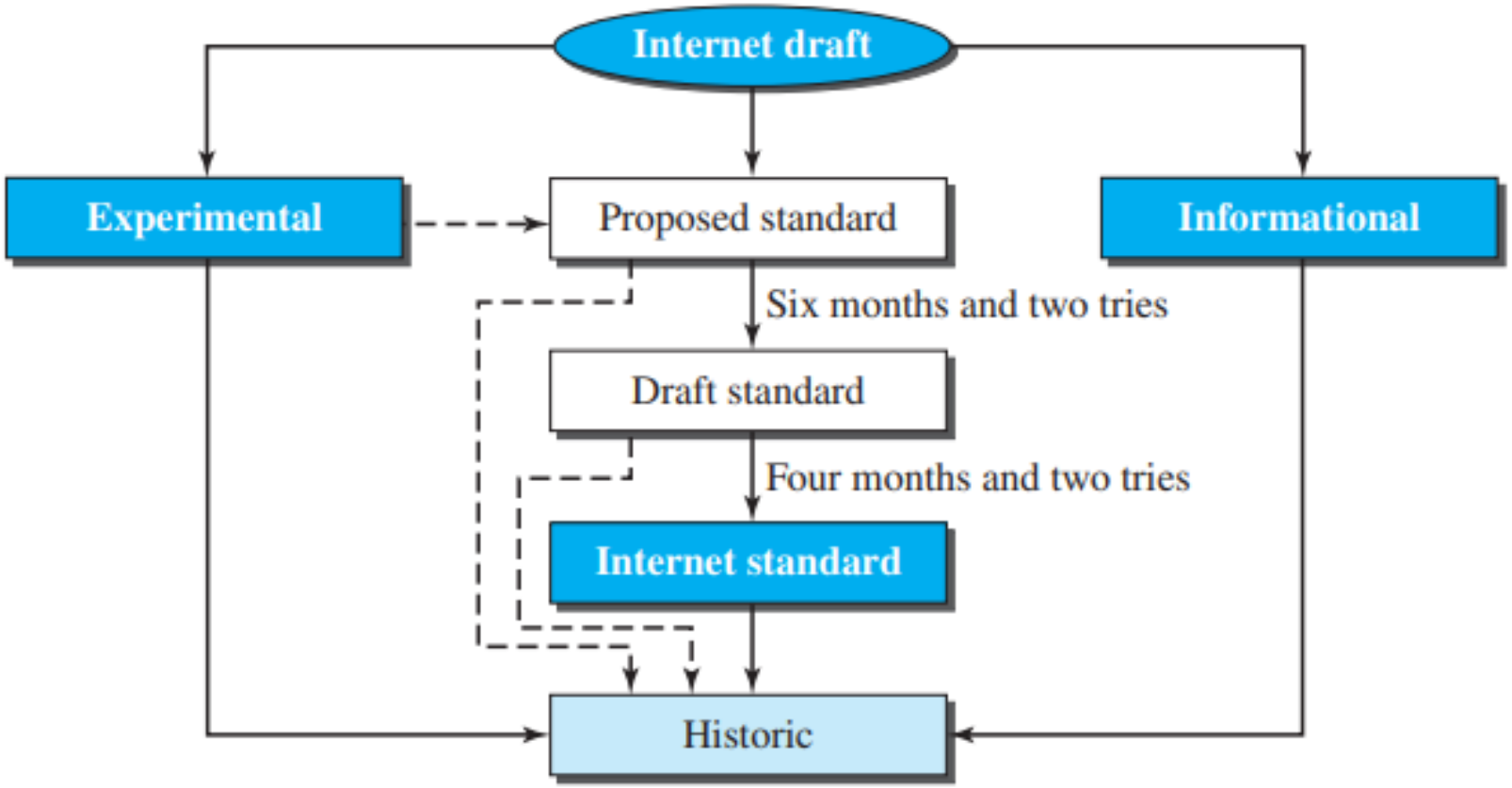
- **4. Direct Connection to the Internet**
- A **large organization or a large corporation can itself become a local ISP and be connected to the Internet.**
- This can be done if the **organization or the corporation leases a high- speed WAN from a carrier provider and connects itself to a regional ISP.**
- For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

Standards and Administration

- **1. Internet Standards**
- An Internet standard is a **thoroughly tested specification that is useful to and adhered to by those who work with the Internet.**
- It is a **formalized regulation that must be followed**.
- 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** (a work in progress) with no official status and a six-month lifetime.

- Upon recommendation from the Internet authorities, **a draft may be published as a Request for Comment (RFC).**
- 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.

- **Maturity Levels**
- An RFC, during its lifetime, falls into one of **six maturity levels**: proposed standard, draft standard, Internet standard, historic, experimental, and informational (see Figure 1.16).



- **Proposed Standard.**

- A proposed standard is a specification that is **stable, well understood, and of sufficient interest to the Internet community.**
- At this level, the **specification is usually tested and implemented by several different groups.**

- **Draft Standard.**

- A ***proposed standard*** is **elevated to *draft standard*** status **after** at **least two successful independent and interoperable implementations**.
- Barring difficulties, a draft standard, with **modifications if specific problems are encountered**, **normally becomes an Internet standard**.

- **Internet Standard.**
- A ***draft standard*** **reaches** ***Internet standard*** status **after demonstrations of successful implementation.**
- **Historic.**
- The historic RFCs are significant from a historical perspective.
- They either have been **superseded by later specifications or have never passed** the necessary maturity levels to become an Internet standard.
- **Experimental.**
- An RFC classified as experimental describes work related to an experimental situation that **does not affect the operation of the Internet.**
- Such an RFC **should not be implemented in any functional Internet service.**

- **Informational.**

- An RFC classified as informational contains **general, historical, or tutorial information related to the Internet.**
- It is usually written by someone in a non-Internet organization, such as a vendor.

❖Requirement Levels

- RFCs are classified into five requirement levels: required, recommended, elective, limited use, and not recommended**.**

➢Required

- An RFC is labeled required if **it must be implemented by all Internet systems** to achieve minimum conformance. For example, IP and ICMP are required protocols.

➢Recommended

- An RFC labeled recommended is **not required for minimum conformance; it is recommended because of its usefulness.** For example, FTP and TELNET are recommended protocols.

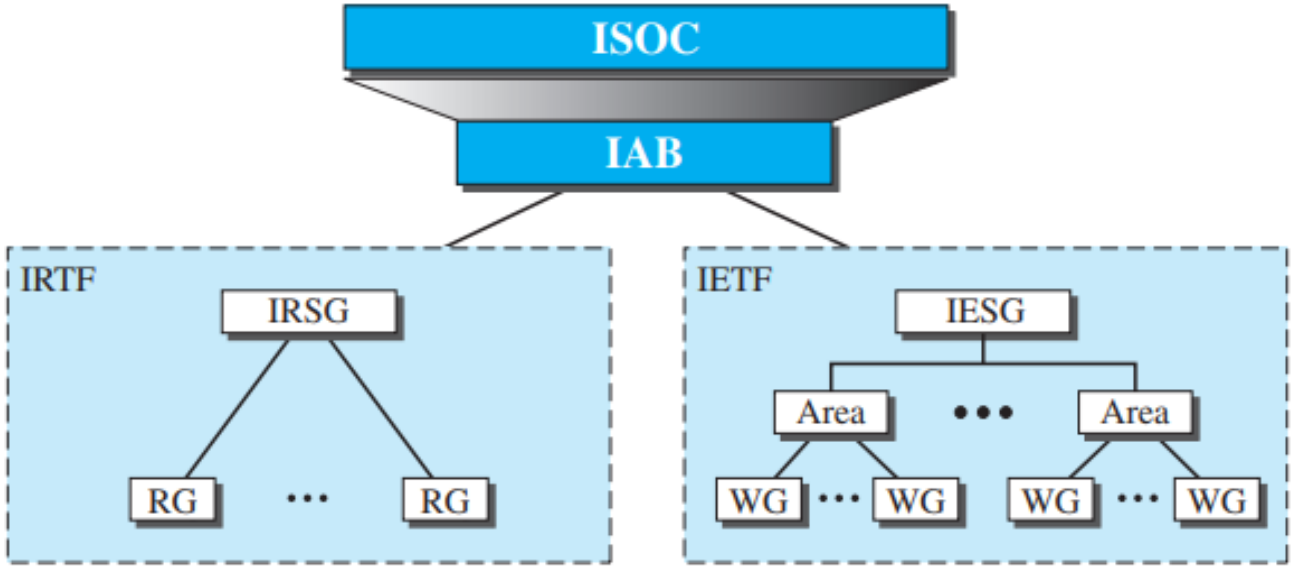
- **Elective**
  - An RFC labeled elective is **not required and not recommended**. However, a **system can use it for its own benefit**.
- **Limited Use**
  - An RFC labeled limited use **should be used only in limited situations**.
  - Most of the experimental RFCs fall under this category.
- **Not Recommended**
  - An RFC labeled **not recommended is inappropriate for general use**.
  - Normally a historic (deprecated) RFC may fall under this category.

RFCs can be found at http://www.rfc-editor.org

2. Internet Administration

- The Internet, with its roots primarily in the research domain, has evolved and gained a broader user base with significant commercial activity.
- Various groups that coordinate Internet issues have guided this growth and development.
- Figure 1.17 shows the general organization of Internet administration.

Figure 1.17 *Internet administration*



ISOC

- The **Internet Society** (ISOC) is an international, nonprofit organization formed in 1992 to provide **support for the Internet standards process.**
- ISOC **accomplishes** this **through maintaining and supporting other Internet administrative bodies such a IAB, IETF, IRTF, and IANA** (see the following sections).
- ISOC also **promotes research and other scholarly activities relating to the Internet.**

➢IAB

- The **Internet Architecture Board** (IAB) is the **technical advisor to the ISOC.**
- The main purposes of the IAB are to **oversee the continuing development of the TCP/IP Protocol Suite and to serve in a technical advisory capacity to research members of the Internet community**.
- IAB **accomplishes this through its two primary components**, the **Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF).**
- Another responsibility of the IAB is the editorial management of the RFCs, described earlier.
- IAB is also the external liaison between the Internet and other standards organizations and forums.

➢IETF

- The **Internet Engineering Task Force** (IETF) is a forum of working groups **managed by the Internet Engineering Steering Group (IESG).**
- IETF is **responsible for identifying operational problems and proposing solutions to these problems.**
- IETF also **develops and reviews specifications intended as Internet standards.**
- The working groups are collected into areas, and each area concentrates on a specific topic.
- **Currently nine areas have been defined**.
- The areas include applications, protocols, routing, network management next generation (IPng), and security.

➢IRTF

- The **Internet Research Task Force** (IRTF) is a forum of **working groups managed by the Internet Research Steering Group (IRSG).**
- IRTF **focuses on long-term research topics related to Internet protocols, applications, architecture, and technology.**

Network Models

- A **network** is a **combination of hardware and software that sends data from one location to another.**
- The **hardware consists of the physical equipment that carries signals from one point of the network to another.**
- The **software consists of instruction sets that make possible the services that we expect from a network.**

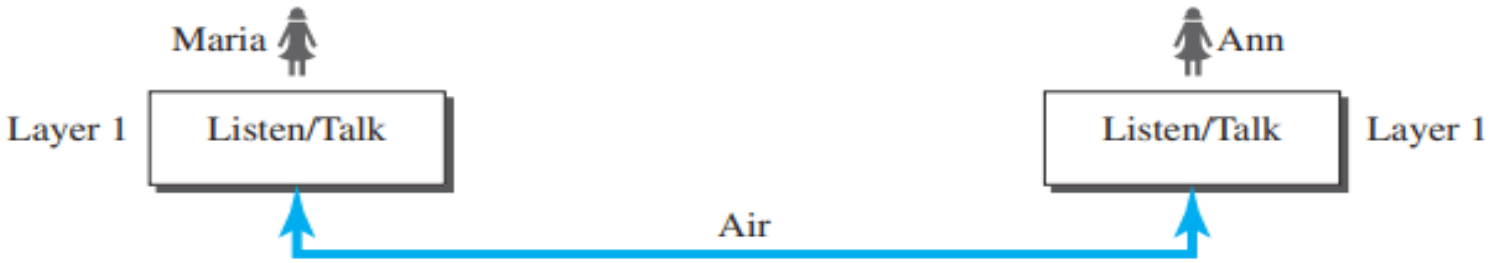
Protocol Layering

- In data communication and networking**, a protocol defines the rules that both the sender and receiver and all intermediate devices need to follow to be able to communicate effectively.**
- When **communication is simple**, we may need only **one simple protocol;**
- When the **communication is complex**, we may **need to divide the task between different layers, in which case we need a protocol at each layer, or protocol layering**.

❖Scenarios

- There are two simple scenarios to better understand the need for protocol layering.
- **1. First Scenario**
- In the first scenario, **communication is so simple that it can occur in only one layer.**
- Assume Maria and Ann are neighbors with a lot of common ideas. Communication between Maria and Ann takes place in one layer, **face to face, in the same language**, as shown in Figure 2.1.

Figure 2.1 *A single-layer protocol*



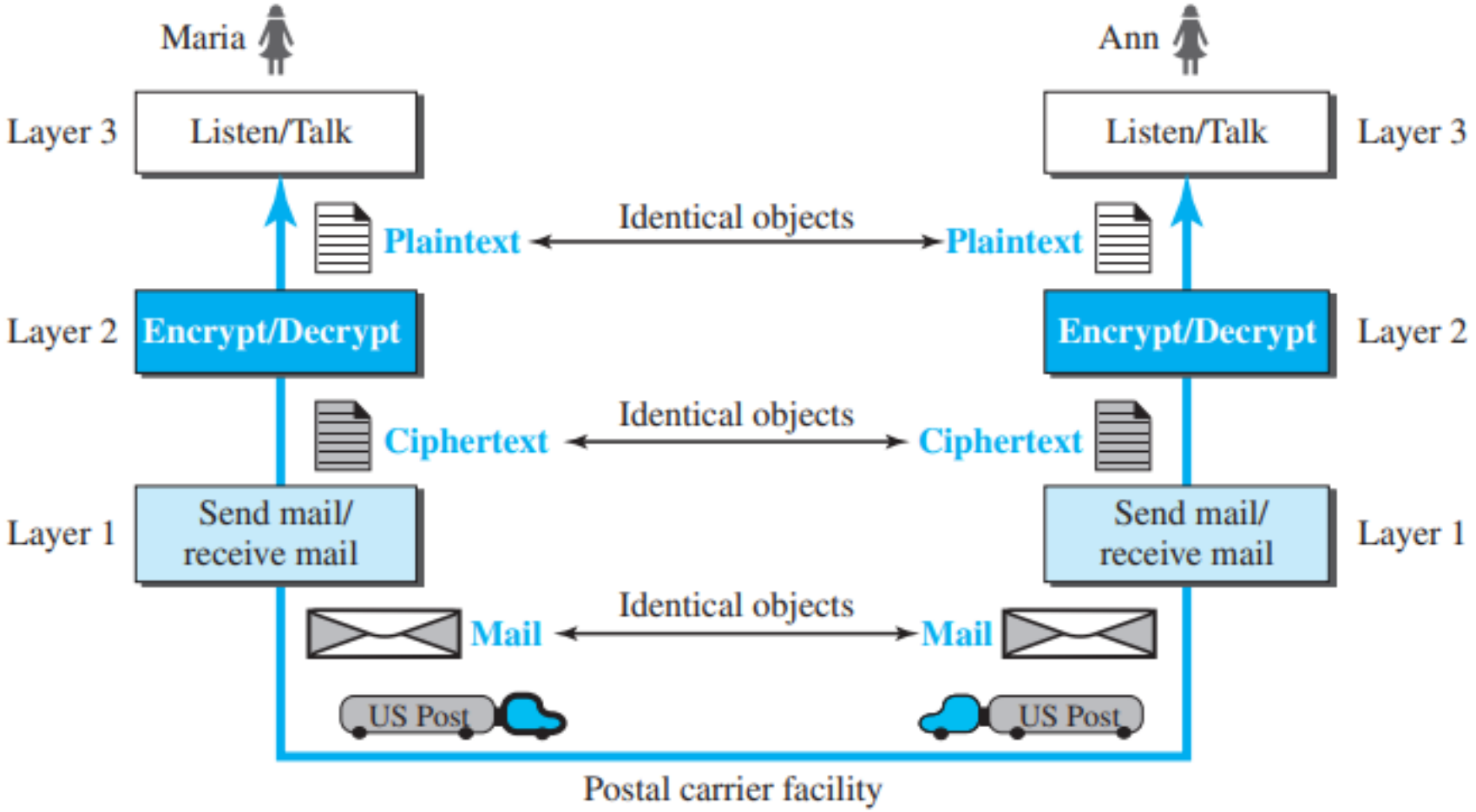
- Even in this simple scenario, we can see that a **set of rules needs to be followed.**
- **First**, Maria and Ann know that they **should greet each other** when they meet.
- **Second**, they know that they should **confine their vocabulary to the level of their friendship**(*they should use proper words for communication*).
- **Third**, each party knows that she should **refrain from speaking when the other party is speaking**.(*If one person is speaking other should remain silent and listen to that person and vice versa*.)
- **Fourth**, each party knows that the **conversation should be a dialog (*bidirectional*), not a monolog** (***unidirectional***): *both should have the opportunity to talk about the issue.*
- **Fifth**, they should **exchange some nice words when they leave** (*should properly terminate their conversation*).

- We can see that the **protocol used by Maria and Ann is different** from the **communication between a** professor and the students in a lecture hall**.**
- The **communication in the second case is mostly monolog**; the professor talks most of the time unless a student has a question, a situation in which the protocol dictates that she should raise her hand and wait for permission to speak.
- In this case, the communication is normally very formal and limited to the subject being taught.

- **2. Second Scenario**
- In the second scenario, we assume that Ann is offered a higher-level position in her company, but needs to move to another branch located in a city very far from Maria.
- The two friends still want to continue their communication and exchange ideas because they have come up with an innovative project to start a new business when they both retire.
- They decide to continue their **conversation using regular mail through the post office.**
- However, they do not want their ideas to be revealed by other people if the letters are intercepted. **They agree on an encryption/decryption technique.**
- The **sender of the letter encrypts** it to make it unreadable by an intruder(attacker); the **receiver of the letter decrypts it to get the original letter.**

- We assume that Maria and Ann use one technique that makes it hard to decrypt the letter if one does not have the key for doing so.
- Now we can say that the communication between Maria and Ann takes place in three layers, as shown in Figure 2.2.
- We assume that **Ann and Maria each have three machines (or robots) that can perform the task at each layer**.

Figure 2.2 *A three-layer protocol*



- Let us assume that **Maria sends the first letter to Ann**. Maria talks to the machine at the **third layer** as though the machine is Ann and is listening to her.
- The **third layer machine** listens to what Maria says and **creates the plaintext** (a letter in English), which is **passed to the second layer machine.**
- The **second layer** machine **takes the plaintext, encrypts it, and creates the cipher text**, which is **passed to the first layer machine**.
- The **first layer machine**, presumably a robot, **takes the cipher text, puts it in an envelope, adds the sender and receiver addresses, and mails it**.
- At Ann's side, the **first layer machine picks up the letter from Ann's mail box, recognizing the letter from Maria** by the sender address.
- The **machine takes out the cipher text from the envelope** and **delivers it to the second layer** machine.

- The **second layer machine decrypts the message, creates the plaintext,** and **passes the plaintext to the third-layer machine**.
- The **third layer machine takes the plaintext and reads it as though Maria is speaking.**
- **Protocol layering enables** us to **divide a complex task into several smaller and simpler tasks.**
- For example, in Figure 2.2, *we could have used only one machine to do the job of all three machines.*
- However, if Maria and Ann decide that the *encryption/ decryption done by the machine is not enough to protect their secrecy, they would have to change the whole machine.*

- In the *present situation*, they *need to change only the second layer machine; the other two can remain the same. This is referred to as* ***modularity.***
- **Modularity in this case means independent layers**.

- If two machines provide the same outputs when given the same inputs, they can replace each other.
- For example, Ann and Maria can buy the second layer machine from two different manufacturers.
- As long as the two machines create the same ciphertext from the same plaintext and vice versa, they do the job.
- One of the **advantages of protocol layering** is that **it allows us to separate the services from the implementation**.
- A **layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer**; we don't care about how the layer is implemented.
- For example, Maria may decide not to buy the machine (robot) for the first layer; she can do the job herself.
- As long as Maria can do the tasks provided by the first layer, in both directions, the communication system works.

- Another **advantage of protocol layering**, which cannot be seen in our simple examples but reveals itself when we discuss protocol layering in the Internet, is that **communication does not always use only two end systems; there are intermediate systems that need only some layers, but not all layers.**
- **If we did not use protocol layering**, we **would have to make each intermediate system as complex as the end systems, which makes the whole system more expensive.**

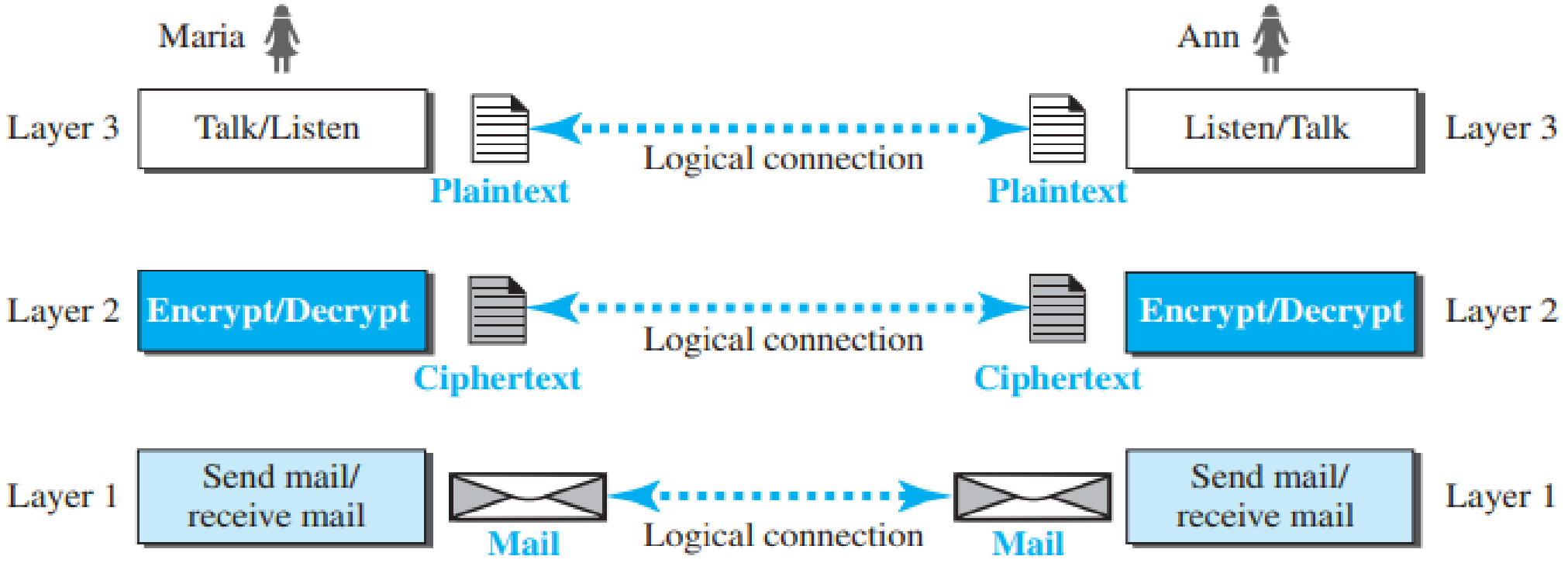
- Is there any **disadvantage to protocol layering**?
- One can argue that having a **single layer makes the job easier**. There is no need for each layer to provide a service to the upper layer and give service to the lower layer.
- For example, Ann and Maria could find or build one machine that could do all three tasks.
- However, as mentioned above, if one day they found that their code was broken, each would have to replace the whole machine with a new one instead of just changing the machine in the second layer.

- **Principles of Protocol Layering**
- There are two principles of protocol layering.
- **1. first Principle**
- The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform **two opposite tasks, one in each direction.**
- For example, the third layer task is to listen (in one direction) and talk (in the other direction).
- The second layer needs to be able to encrypt and decrypt.
- The first layer needs to send and receive mail.

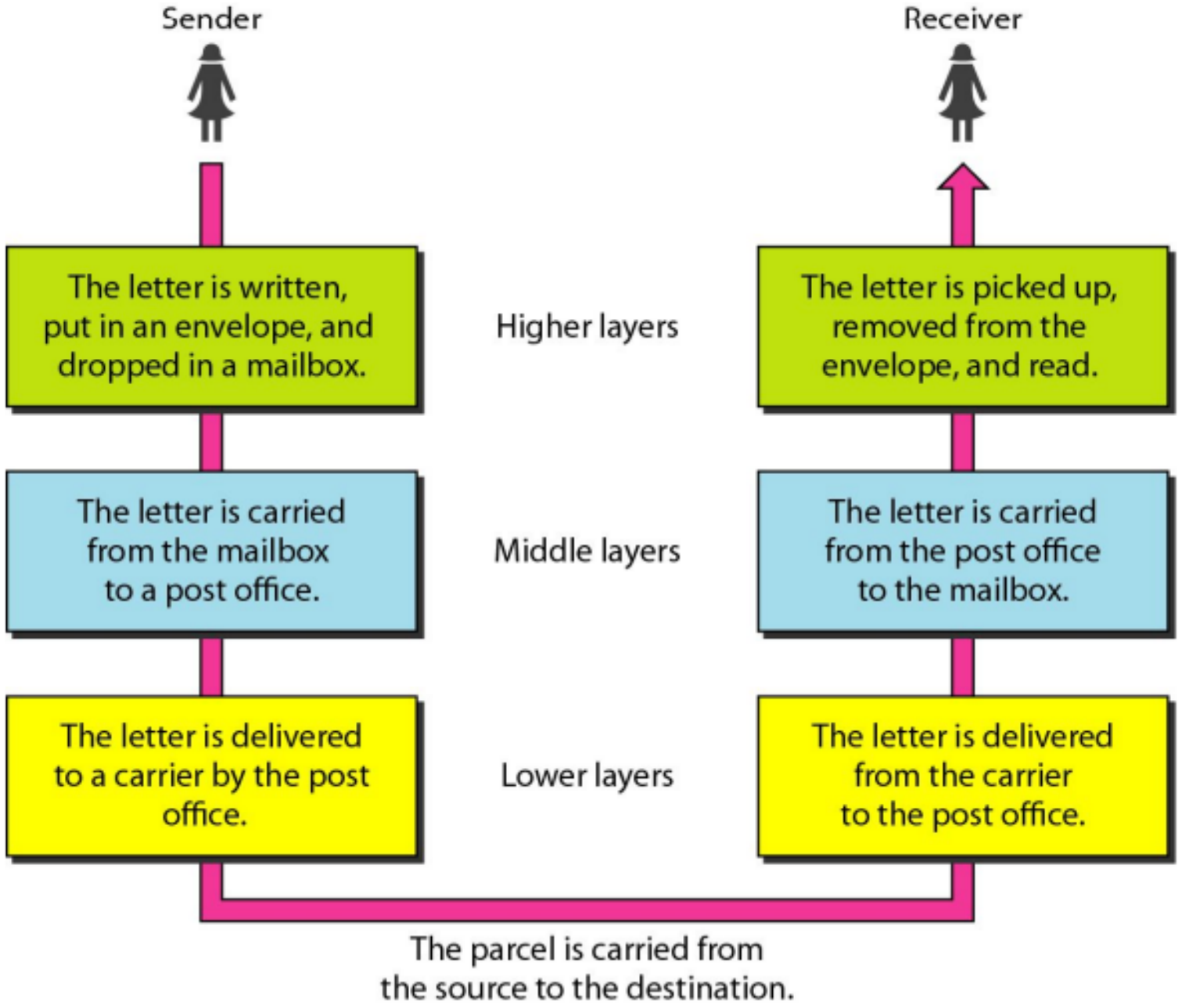
- **2. Second Principle**
- The second principle that we need to follow in protocol layering is that the **two objects under each layer at both sites should be identical**.
- For example, the object under layer 3 at both sites should be a plaintext letter.
- The object under layer 2 at both sites should be a cipher text letter.
- The object under layer 1 at both sites should be a piece of mail.

- **Logical Connection**
- After following the above two principles, we can think about logical connection between each layer as shown in Figure 2.3.
- This means that **we have layer-to-layer communication**.
- Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.
- We will see that the concept of logical connection will help us better understand the task of layering we encounter in data communication and networking.

Figure 2.3 *Logical connection between peer layers*



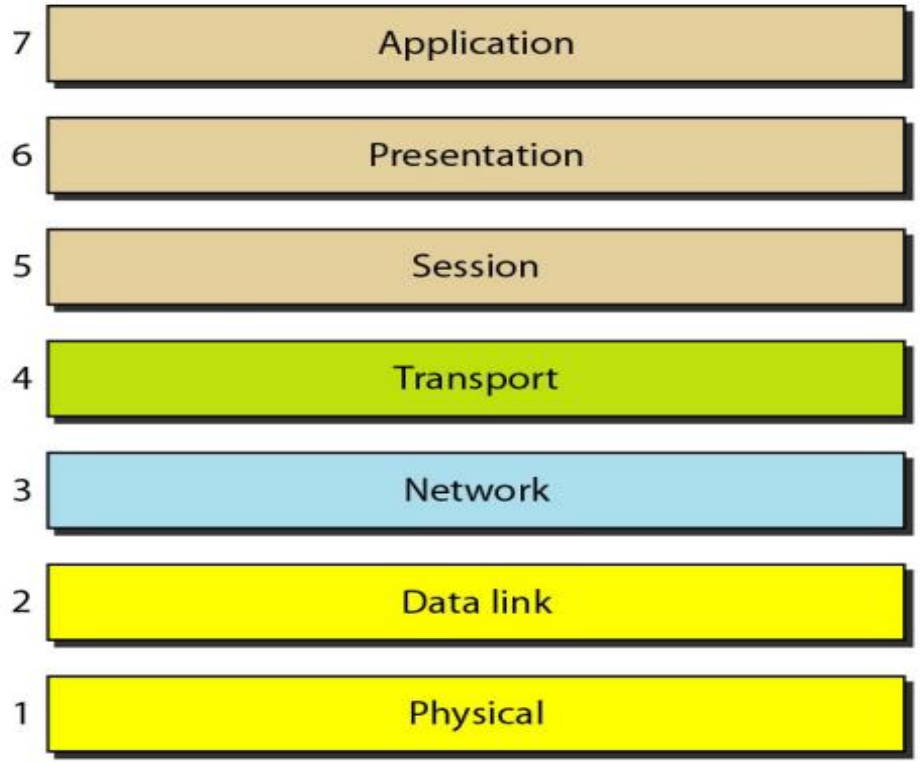
- The **main objective** of a **computer network** is to *be able to transfer the data from sender to receiver.*
- This **task can be done by** *breaking it into small sub tasks, each of which are well defined.*
- Each subtask will have its own process or processes to do and will take specific inputs and give specific outputs to the subtask before or after it. In more technical terms we can call these sub tasks as layers.
- In general, *every task or job can be done by dividing it into sub task or layers*. Consider the example of sending a letter where the sender is in City A and receiver is in city B.
- The process of sending letter is shown below:


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.

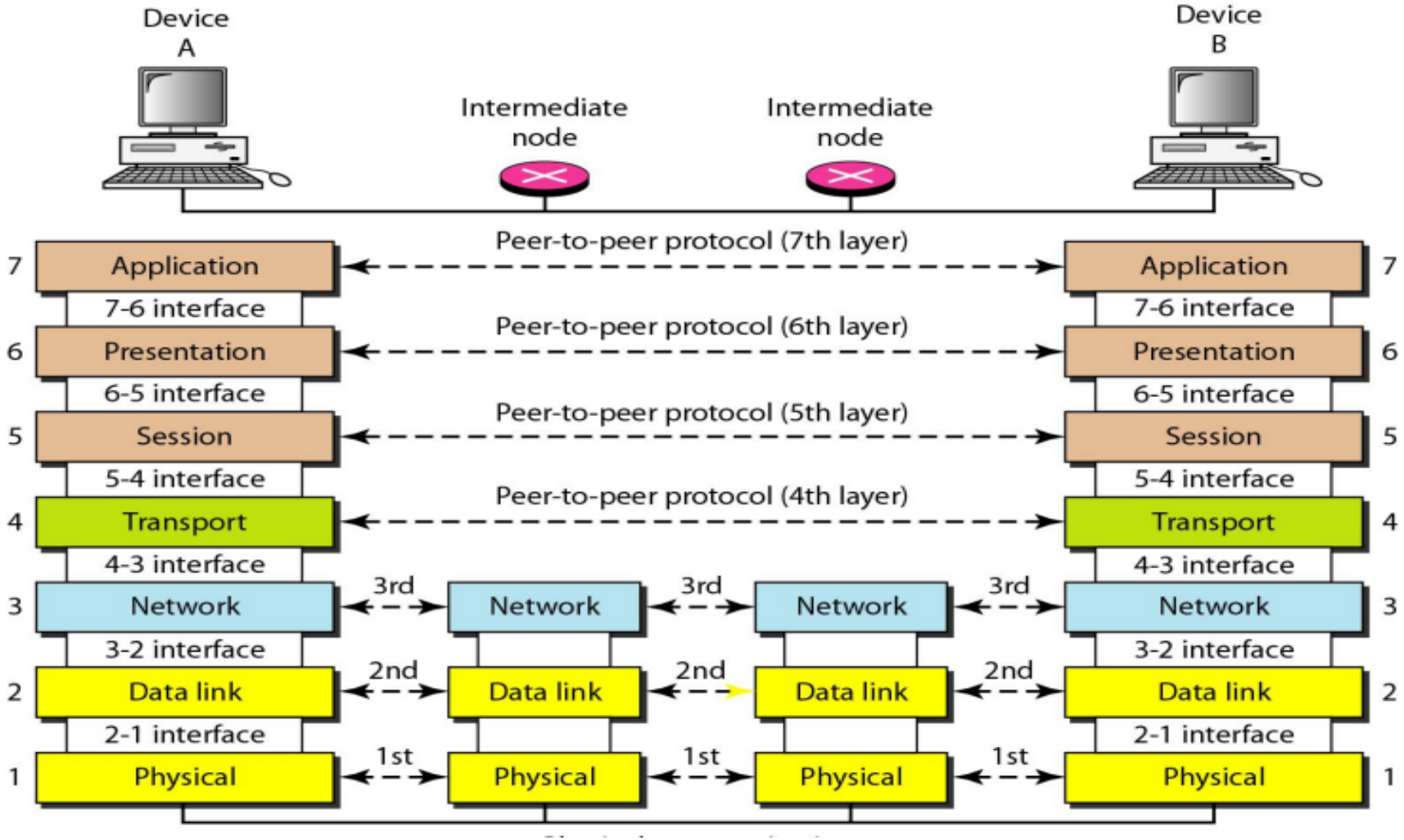
The OSI Model

- 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 model**.
- 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 model for understanding and designing a network architecture** that is flexible, robust, and interoperable(**able to communicate and exchange data**).
- *ISO is the organization. OSI is the model*.

- The **OSI model** is a **layered framework for the design of network systems that allows communication between all types of computer systems**.
- It **consists of seven separate but related layers**, each of which defines a part of the process of moving information across a network.
- Seven layers of the OSI model



- **Layered Architecture**



- In order for data to travel from the source to the destination, each layer of the OSI model at the source must communicate with its peer layer at the destination. This form of communication is referred to as peer-to-peer.

7. Application Layer

- The application layer **enables the user to communicate its data to the receiver by providing certain services**.
- The application layer enables the user, whether human or software, to **access the network**.
- It provides protocols that **allow software to send and receive information and present meaningful data to users.**
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- When a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back.
- **The application layer is responsible for providing services to the user**

➢ Responsibilities / Function

- **1.Network virtual terminal.**
- A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- To do so, the application creates a software emulation of a terminal at the remote host. **The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa.**
- **2.File transfer, access, and management.**
- This application allows a user to **access files in a remote host** (to make changes or read data), to **retrieve files from a remote computer** for use in the local computer, and to **manage or control files** in a remote computer locally.
- **3.Mail services.**
- This application provides the basis for **e-mail forwarding and storage**.

- **4.Directory services.**
- This application provides **distributed database sources and access for global information about various objects and services.**

➢**The various protocols used in this layer are:**

- DNS (Domain Name System),
- SMTP (Simple Mail Transfer Protocol),
- FTP (File Transfer Protocol),
- POP (Post Office Protocol),
- HTTP (Hyper Text Transfer Protocol), etc.

➢**The various devices used in this layer are:**

- PC's (Personal Computer),
- Phones,
- Servers,

6. Presentation Layer

- The presentation layer is concerned with the **syntax and semantics of the information exchanged between two systems**.
- It defines **how two devices should encode, encrypt, and compress data so it is received correctly on the other end**.
- **The presentation layer is responsible for translation, compression, and encryption.**

Responsibilities/Functions

- **1.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 bit streams before being transmitted.**
- The presentation layer **at the sender changes the information from its sender-dependent format into a common format**.
- The presentation layer **at the receiving** machine **changes the common format into its receiver-dependent format**.

- **2.Encryption.**
- **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.**
- **3.Compression.**
- Data compression **reduces the number of bits** contained in the information.
- Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

➢**The various protocols used in this layer are:**

- AFP (Apple Filing Protocol),
- SSL (Secure Socket Layer),
- TLS (Transport Layer Security),
- NDR (Network Data Representation),
- Tox protocol, etc.

5. Session Layer

- The session layer **creates communication channels, called sessions, between devices.**
- It is responsible for **opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends.**
- The session layer can **also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.**
- It establishes, maintains, and synchronizes the interaction among communicating systems.
- **The session layer is responsible for dialog control and synchronization.**

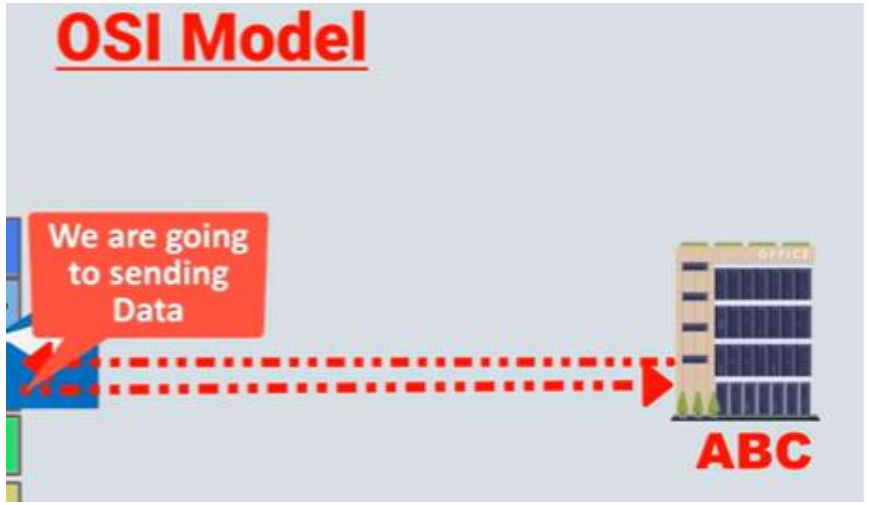
➢ Responsibilities / Functions

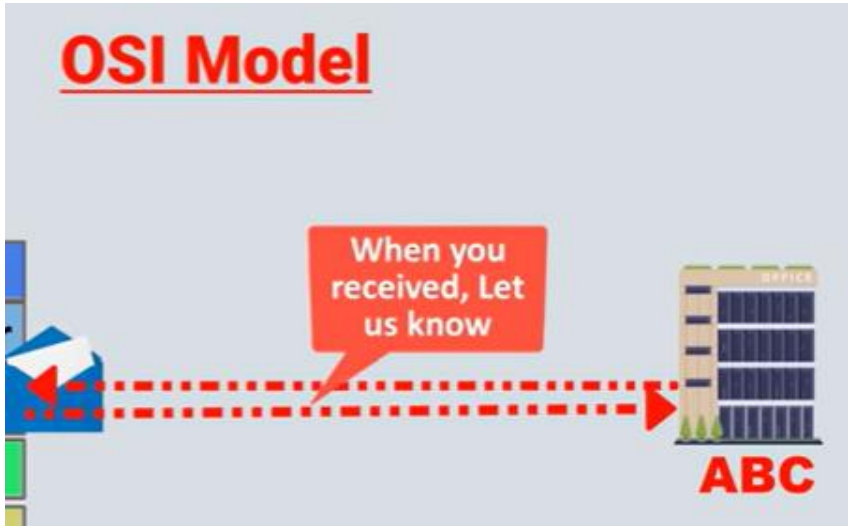
- **1.Dialog control.**
- The session layer allows two systems to enter into a dialog.
- The session layer establishes a session between the communicating devices called dialog and synchronizes their interaction.
- It is the responsibility of the session layer to establish and synchronize the dialogs.
- It is also called the network dialog controller.
- 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.
- **2.Synchronization.**
- The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

- The **checkpoints or synchronization points is a way of informing the status of the data transfer**.

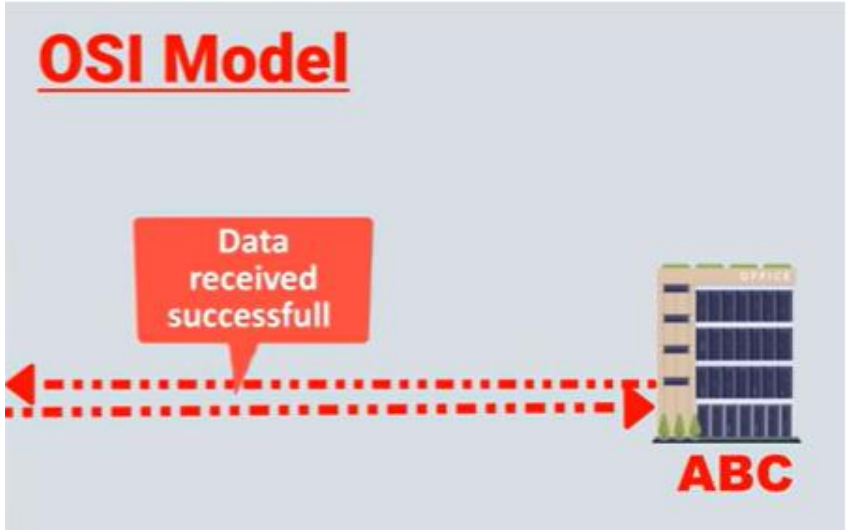
➢ **The various protocols used in this layer are :**

- PAP (Password Authentication Protocol)
- PPTP (Point-to-Point Tunneling Protocol)
- RPC (Remote Procedure Call Protocol)


OSI Model
We are going to sending Data
ABC


OSI Model
When you received, Let us know
ABC


OSI Model
Data lost Or Unsuccessfull
ABC


OSI Model
Data received successfull
ABC

4. Transport Layer

- **The transport layer is responsible for the delivery of a message from one process to another**.
- The transport layer takes data transferred in the session layer and **breaks it into "segments" on the transmitting end**.
- It is responsible for **reassembling the segments on the receiving end**
- The transport layer **carries out flow control**, **sending data at a rate that matches the connection speed of the receiving device**, and ***error control, checking if data was received incorrectly and if not, requesting it again***.

➢Responsibilities /Functions

- **1.Service-point addressing.**
- Computers often run several programs at the same time. For this reason, 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.
- The transport layer **header must therefore include a type of address called a service-point address (or port address**).
- A Port Address is the name or label given to a process. It is a 16 bit address. Ex. TELNET uses port address 23, HTTP uses port address 80.
- **2.Segmentation and reassembly.**
- A message is **divided into transmittable segments**, with each **segment containing a sequence number**.

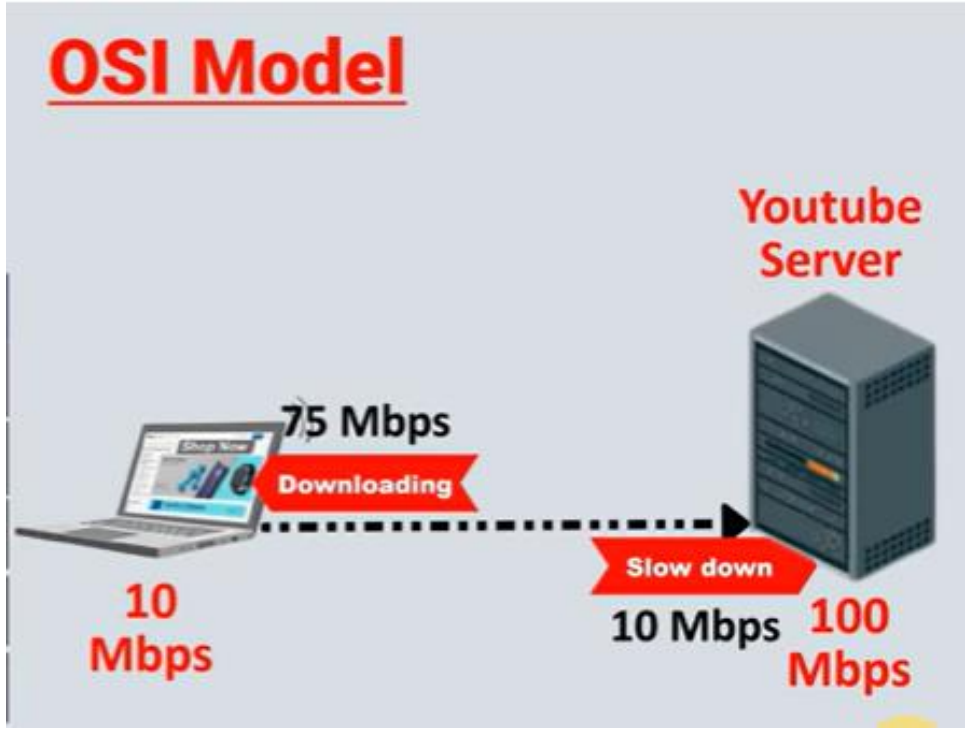
- These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.
- **3.Connection control.**
- The transport layer can be either connectionless or connection oriented.
- A **connectionless** 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.
- **4.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.

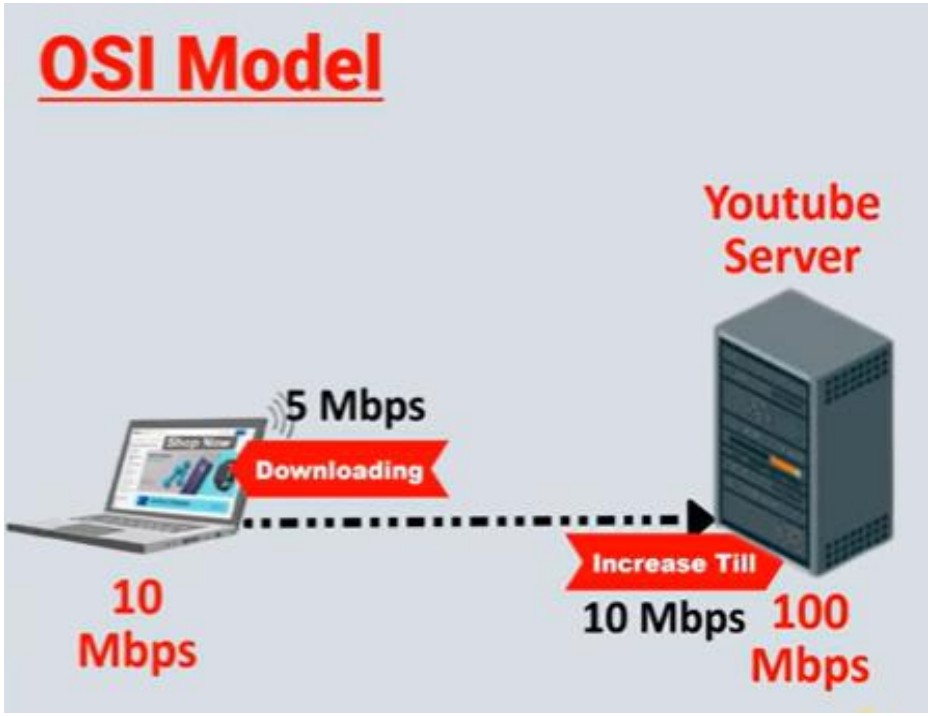
- **5.Error control.**
- The sending transport layer makes sure that the **entire message arrives at the receiving transport layer without error** (damage, loss, or duplication).
- Error correction is usually achieved through retransmission.

➢ **The various protocols used in this layer are :**

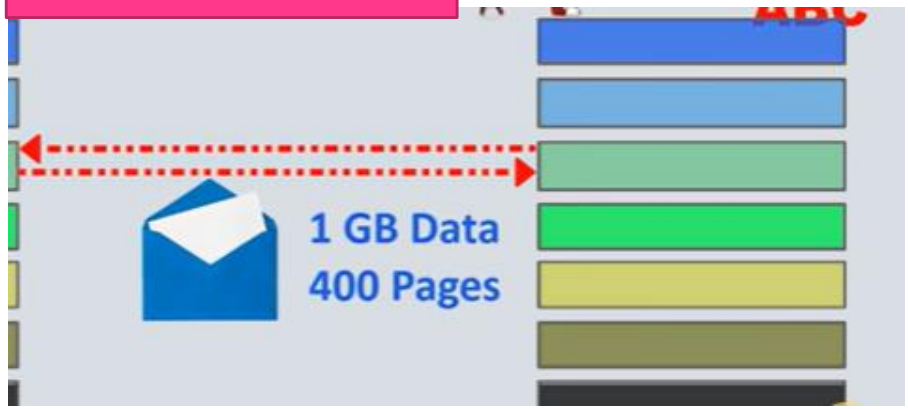
- TCP (Transmission Control Protocol),
- UDP (User Datagram Protocol), etc.

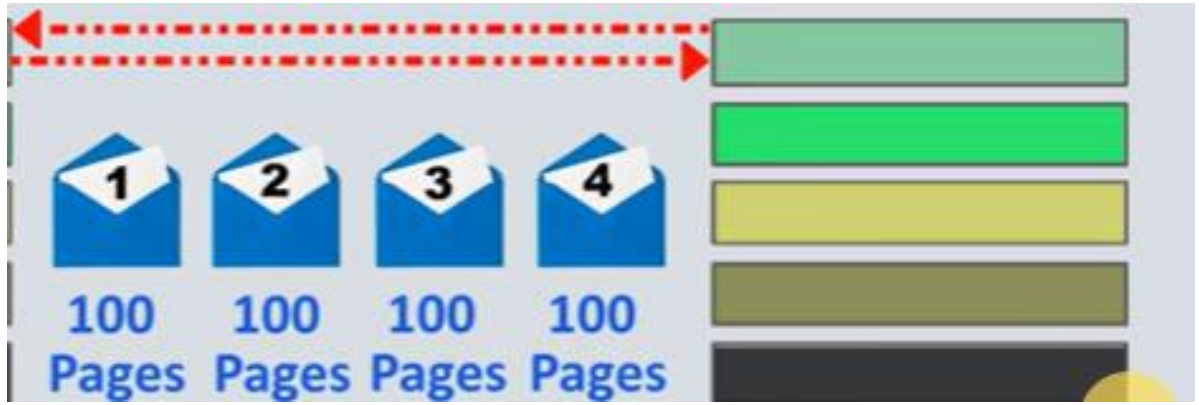
Flow Control





Segments





3. 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.**

Responsibilities/Functions

- **1.Logical addressing.**
- The network layer **uses logical address commonly known as IP address to recognize devices on the network.**
- The network layer adds a header to the packet coming from the upper layer that, among other things, **includes the logical addresses of the sender and receiver.**
- **2.Routing.**
- When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.
- Routing simply means **determining the best (optimal) path out of multiple paths from the source to the destination**. So the network layer must choose the best routing path for the data to travel.

- If many devices are connected to the same router then there is a change of packet drop because a router may not be able to handle all the requests. So, **the network layer controls the congestion on the network as well.**
- This process of finding the best path is called as Routing.
- It is done using routing algorithms.

➢ **The various protocols used in this layer are :**

- IPv4 (Internet Protocol version 4),
- IPv6 (Internet Protocol version 6),
- ICMP (Internet Control Message Protocol),
- IPSEC (IP Security),
- ARP (Address Resolution Protocol),
- MPLS (Multiprotocol Label Switching), etc.

➢ **The various devices used in this layer are :**

- Routers

2. Data Link Layer

- The data link layer **establishes and terminates a connection between two physically-connected nodes on a network.**
- **The data link layer is responsible for moving frames from one hop (node) to the next.**

➢Responsibilities/Functions

- **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.**
- The Data link layer appends the **physical address in the header of the frame** before sending it to physical layer.
- The physical address contains the **address of the sender and receiver**.
- **3.Error control.**
- The data link layer adds reliability to the physical layer **by adding mechanisms to detect and retransmit damaged or lost frames.**

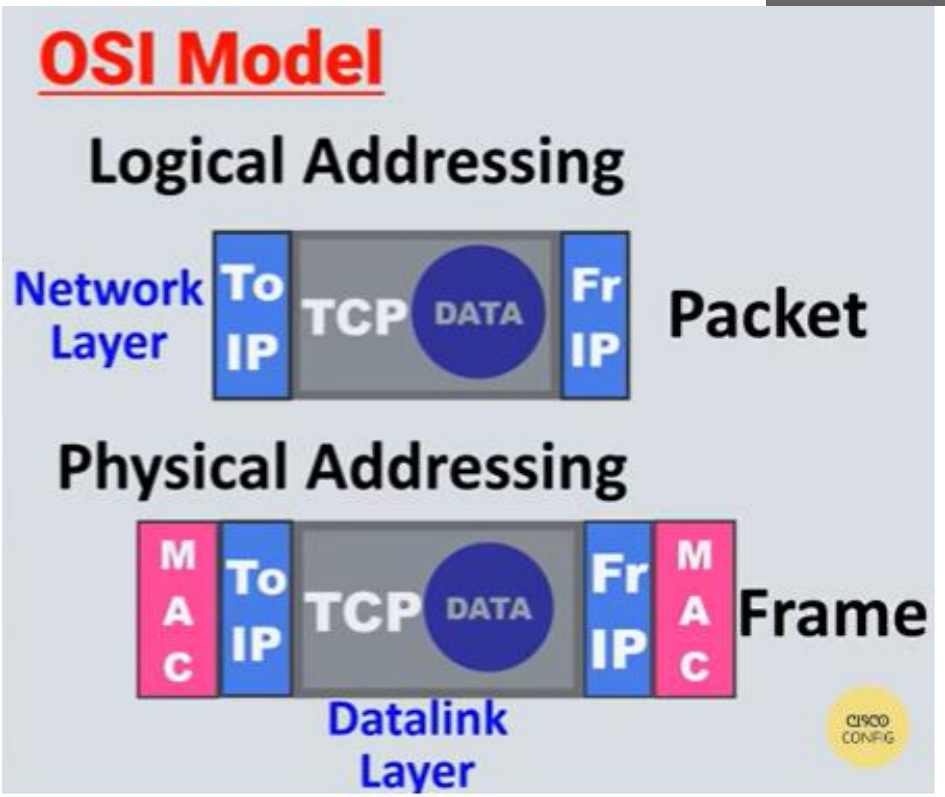
- **4.Access control.**
- The data link layer imposes access control mechanism to **determine which device has right to send data in an multipoint connection (two or more device) scenario**.

➢**The various protocols used in this layer are :**

- PPP (Point-to-Point Protocol),
- Frame Relay,

➢**The various devices used in this layer are :**

- Bridges,
- Switches,
- NIC cards (Network Interface Cards), etc.



1. Physical Layer

- **The physical layer is responsible for the physical cable or wireless connection between network nodes**.
- The physical layer is **responsible for movements of individual bits from one hop (node) to the next**.
- It defines the connector, the electrical cable or wireless technology connecting the devices, and is **responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.**

Responsibilities/Functions

- **1.Physical characteristics of interfaces and medium.**
- The physical layer defines the **characteristics of the interface between the devices and the transmission medium.**
- It also defines the **type of transmission medium**. (which type of transmission medium is used)
- **2.Representation of bits.**
- The physical layer **data consists of a stream of bits (sequence of 0s or 1s).**
- To be transmitted, bits must be **encoded into signals--electrical or optical**.
- The physical layer defines the type of encoding (how 0s and 1 s are changed to signals).

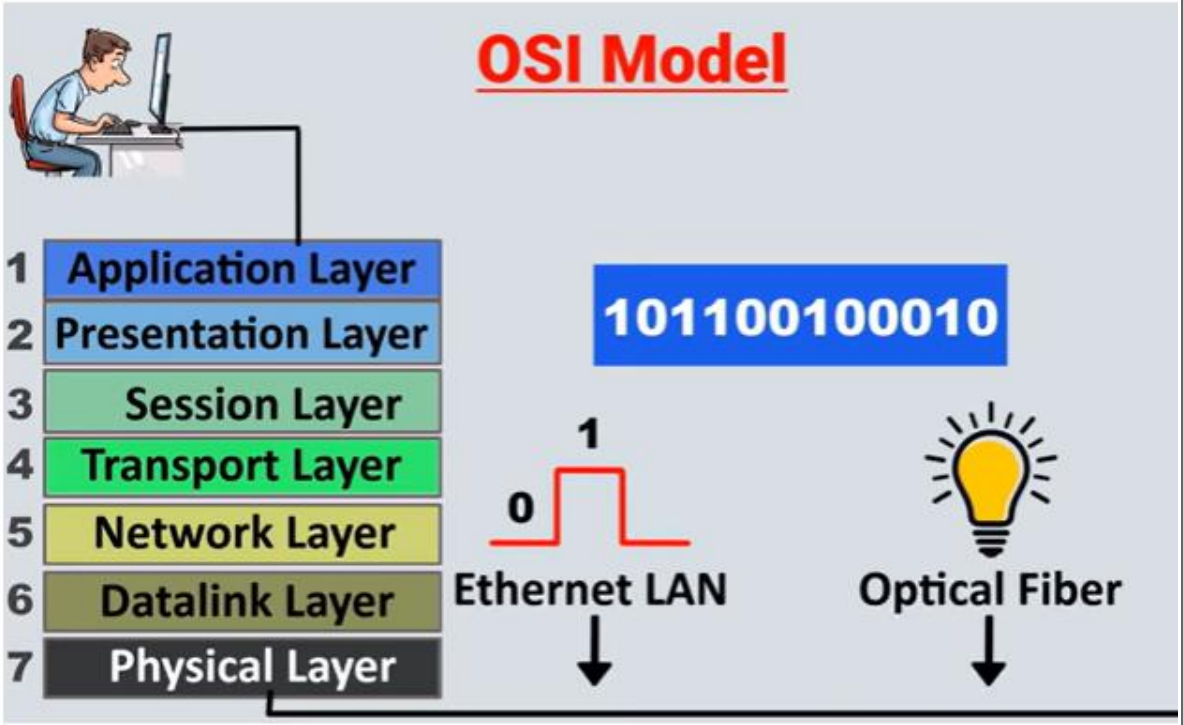
- **3.Data rate.**
- It is the responsibility of the physical layer **to maintain the defined data rate**.
- **4.Synchronization of bits.**
- The sender and receiver not only must use the same bit rate but also **must be synchronized at the bit level.**
- **5.Line configuration.**
- The physical layer defines the **nature of the connection .i.e. a point to point link, or a multi point link**.
- **6.Physical topology.**
- The physical topology **defines how devices are connected to make a network.**
- Devices can be connected by using a mesh topology , a star topology , a ring topology , a bus topology, or a hybrid topology .
- **7.Transmission mode**.
- The physical layer also defines the **direction of transmission between two devices**: simplex, half-duplex, or full-duplex.

- **The various protocols used in the physical layer are :**

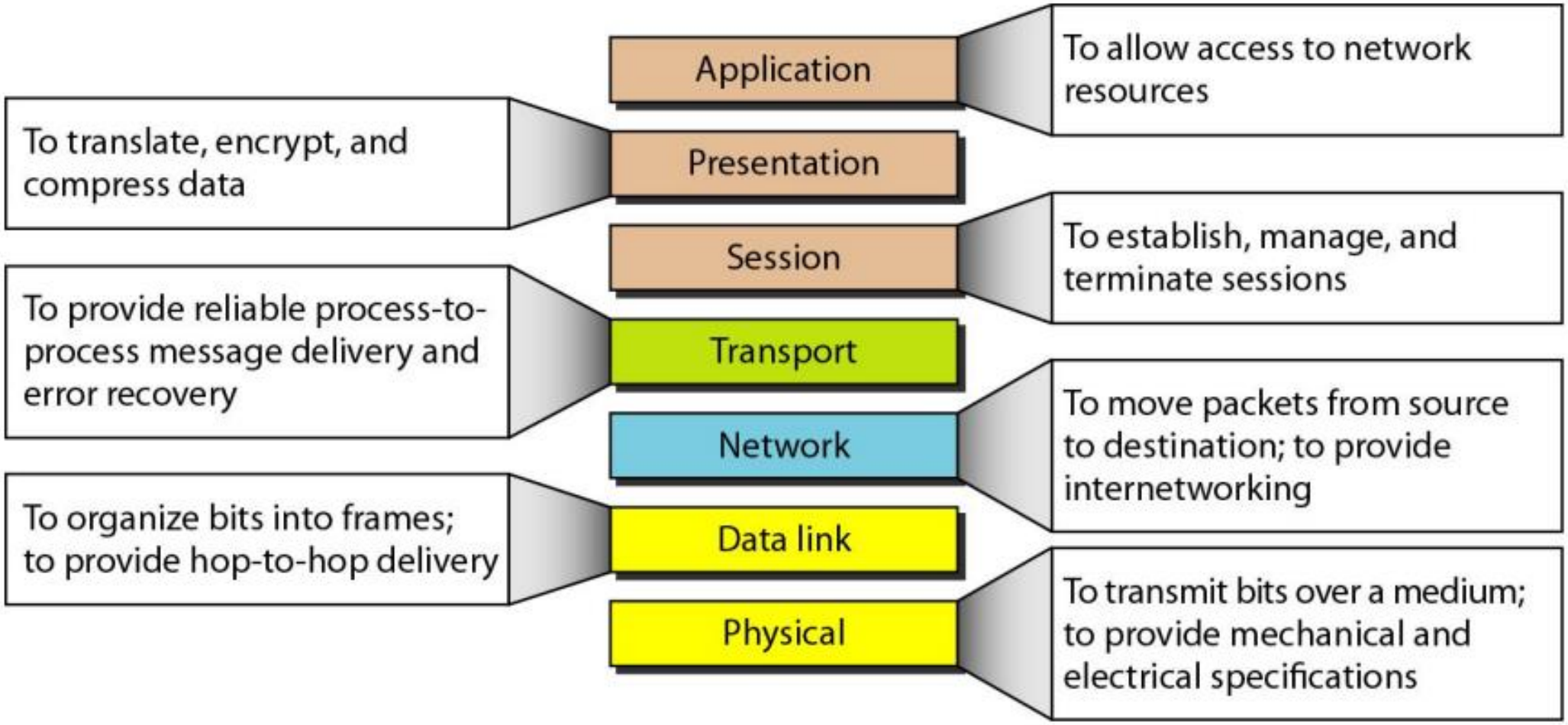
- Digital Subscriber Line.
- Integrated Services Digital Network.
- Ethernet, etc.

- **The various devices used in the physical layer are :**

- Network adapters,
- Hubs,
- Cables,
- Repeaters,
- Modem, etc.



Summary Of Layers



Layer 7: Application

Preparing requests
Protocols: HTTP, HTTPS, DNS
Data: Requests

Layer 5: Session

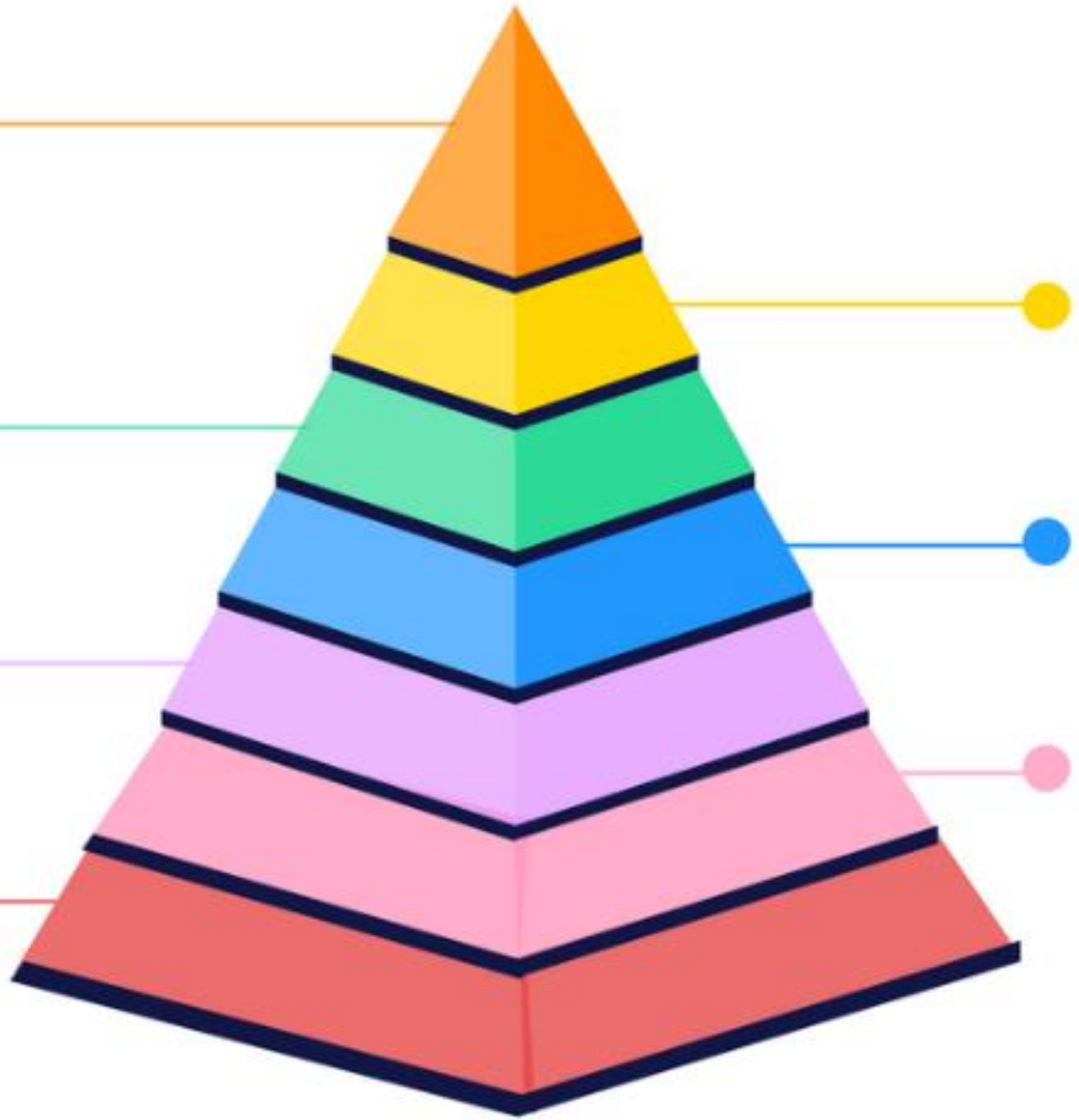
Creating communication channels (sessions) between devices
Protocols: RPC
Data: Requests

Layer 3: Network

Breaks segments into network packets and finds best route for sending packets.
Protocols: IP, NAT, ARP
Data: Packets

Layer 1: Physical

Converts data into physical signals
Data: Optics (Fibre), Electricity



Layer 6: Presentation

Data format
eg. encryption and compression
Protocols: TLS, SSL
Data: Requests

Layer 4: Transport

Breaks requests down into pieces that can be sent over the network and handles the sending of those
Protocols: TCP, UDP
Data: Segments

Layer 2: Data Link

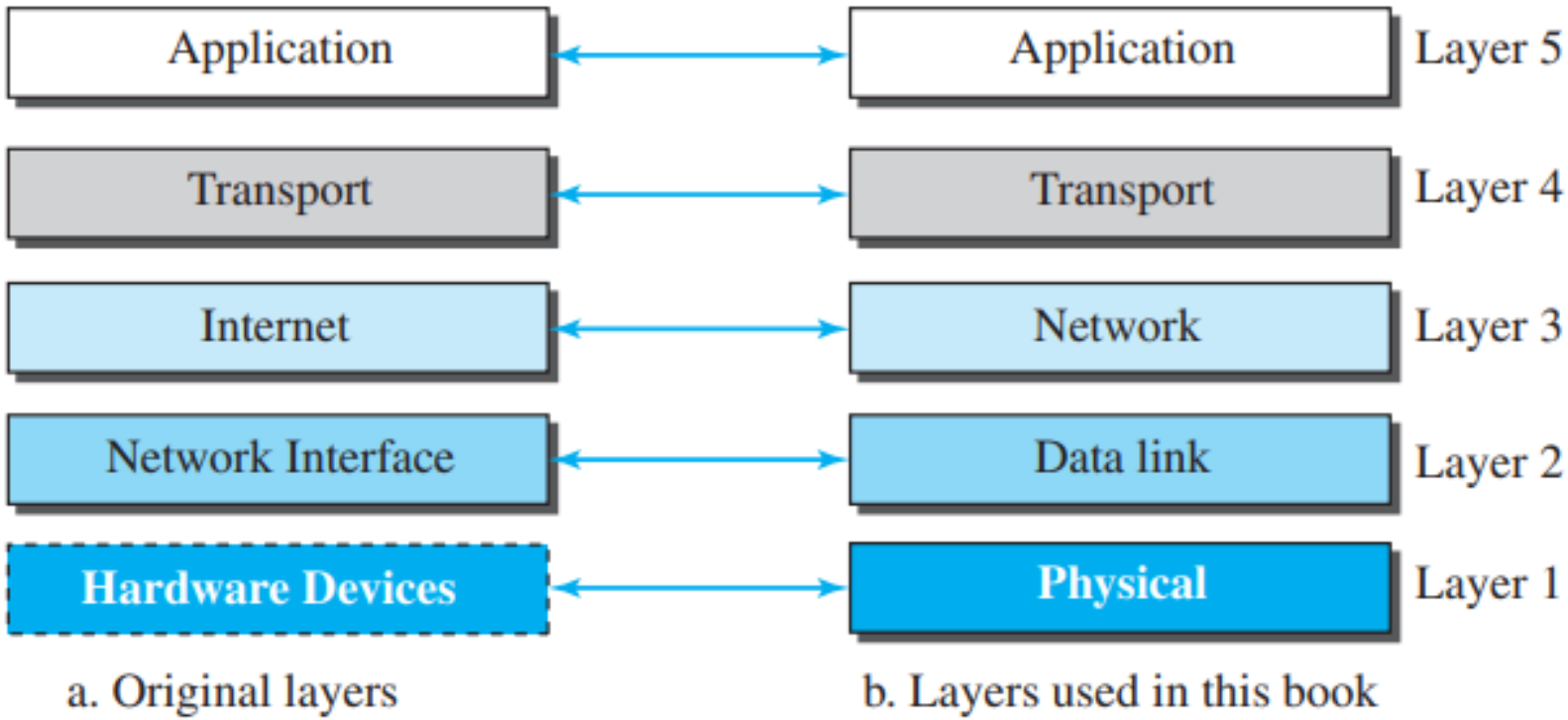
Establishes connections between physical machines using MAC addresses
Breaks segments packets into frames and sends from source to destination
Protocols: Wifi, Ethernet
Data: Frames

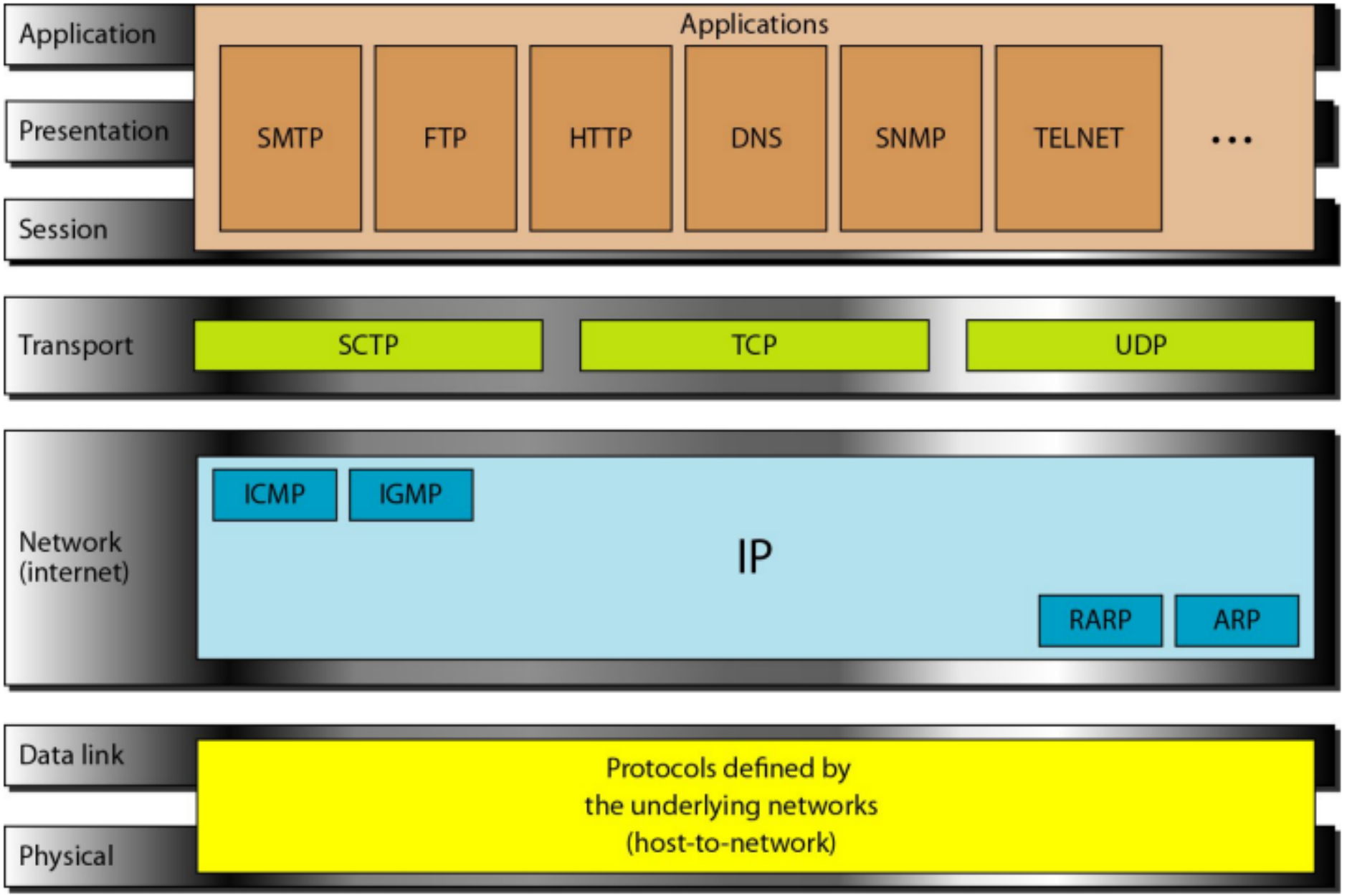
TCP/IP Suite

- TCP/IP(**Transmission Control Protocol/Internet Protocol**) is a protocol suite (a set of protocols organized in different layers) used in the Internet today.
- It is a **hierarchical protocol made up of interactive modules**, each of which provides a specific functionality.
- The term hierarchical means that **each upper level protocol is supported by the services provided by one or more lower level protocols**.
- It **existed even before the OSI model was developed.**
- The **original TCP/IP protocol suite was defined as four software layers** built upon the hardware. **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, an application**
- Figure 2.4 shows both configurations.

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

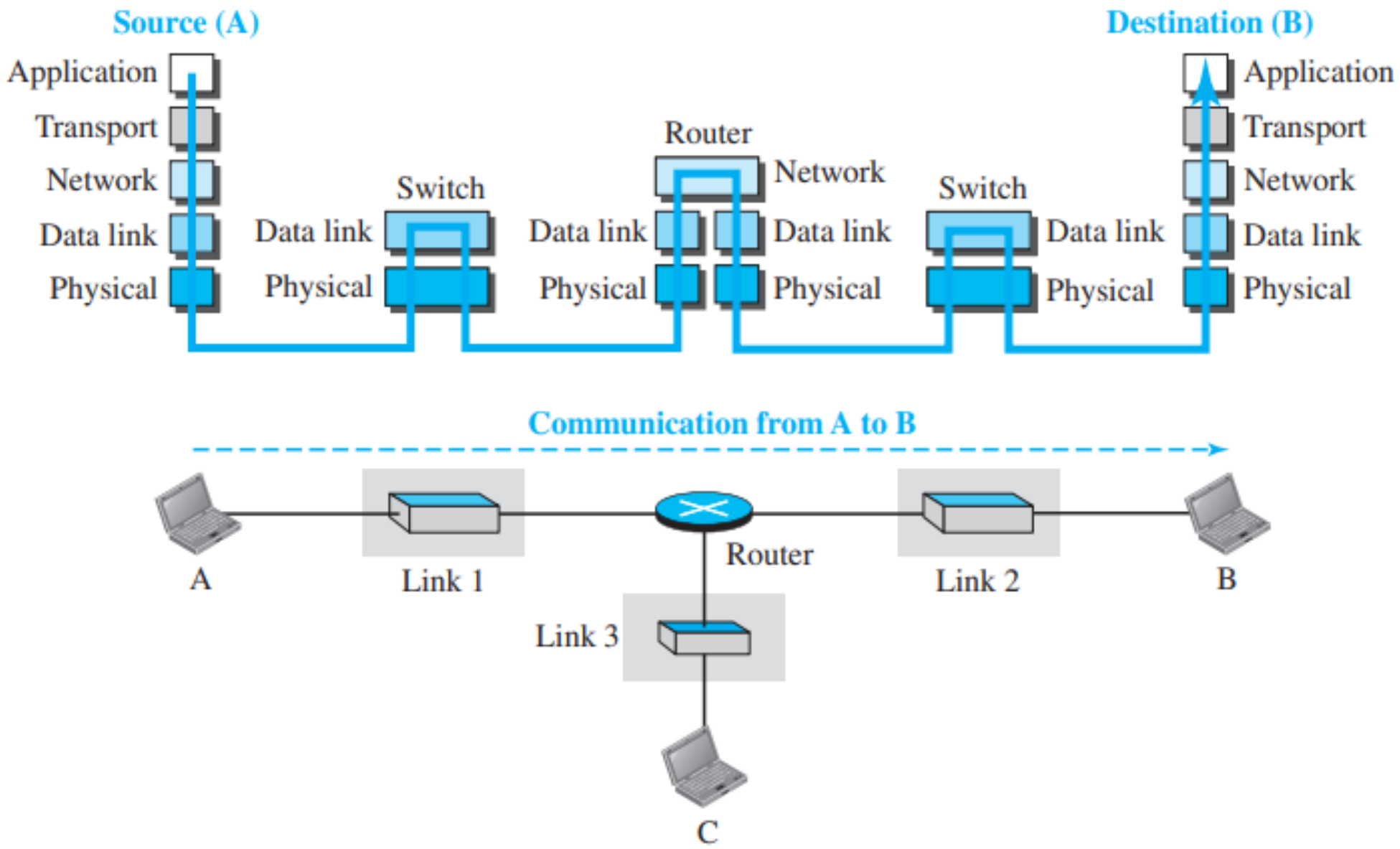



Application
Presentation
Session
Applications
SMTP
FTP
HTTP
DNS
SNMP
TELNET
...
Transport
SCTP
TCP
UDP
Network
(internet)
ICMP
IGMP
IP
RARP
ARP
Data link
Physical
Protocols defined by
the underlying networks
(host-to-network)

Layered Architecture

- To show how the layers in the TCP/IP protocol suite are involved in communication between two hosts, we assume that we want to use the suite in a small internet made up of three LANs (links), each with a link-layer switch.
- We also assume that the links are connected by one router, as shown in Figure 2.5.

Figure 2.5 *Communication through an internet*



- Let us assume that **computer A communicates with computer B.**
- As the figure shows, we have five communicating devices in this communication: ***source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B).***
- Each device is involved with a set of layers depending on the role of the device in the internet.
- The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.
- The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

- The **router is involved in only three layers**; there is no transport or application layer in a router as long as the **router is used only for routing.**
- Although a router is always involved in one network layer, it is involved in n combinations of link and physical layers in which n is the number of links the router is connected to.
- The reason is that each link may use its own data-link or physical protocol.
- For example, in the above figure, the router is involved in three links, but the **message sent from source A to destination B is involved in two links.**
- Each link may be using different link-layer and physical-layer protocols**; the router needs to receive a packet from link 1 based on one pair of protocols and deliver it to link 2 based on another pair of protocols.**

- **A link-layer switch in a link, however, is involved only in two layers, data-link and physical.**
- Although each switch in the above figure has two different connections, the connections are in the same link, which uses only one set of protocols. This means that, unlike a router, a link-layer switch is involved only in one data-link and one physical layer.

Description of Each Layer

❖5. Application Layer

- As Figure 2.6 shows, the logical connection between the two **application layers is end to- end.**
- The two application layers **exchange messages between each other as though there were a bridge between the two layers.**
- However, the communication is done through all the layers.
- Communication at the application layer is between two processes (two programs running at this layer).
- To communicate, **a process sends a request to the other process and receives a response.**
- Process-to-process communication is the duty of the application layer.

Sr. No.	Protocol	Function
1	Hypertext Transfer Protocol (HTTP)	As tool to access the World Wide Web (WWW).
2	Simple Mail Transfer Protocol (SMTP)	It is the main protocol used in electronic mail (e-mail) service.
3	File Transfer Protocol (FTP)	It is used for transferring files from one host to another.
4	Terminal Network (TELNET) and Secure Shell (SSH)	are used for accessing a site remotely.
5	Simple Network Management Protocol (SNMP)	is used by an administrator to manage the Internet at global and local levels.
6	Domain Name System (DNS)	is used by other protocols to find the network-layer address of a computer.
7	Internet Group Management Protocol (IGMP)	is used to collect membership in a group.

❖4. Transport Layer

- The logical connection at the **transport layer is also end-to-end**.
- The transport layer at the s**ource host gets the message from the application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols)**
- In other words, the transport layer is **responsible for giving services to the application layer**: to get a message from an application program running on the source host and deliver it to the corresponding application program on the destination host.
- There are a few transport-layer protocols in the Internet, each designed for some specific task.
- The transport layer contains three protocols:
- 1. TCP
- 2. UDP
- 3. SCTP

- **1) Transmission Control Protocol (TCP)** is a **connection-oriented** protocol that **first establishes a logical connection between transport layers at two hosts before transferring data.**
- It creates a logical pipe between two TCPs for transferring a stream of bytes.
- 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*), and congestion control to reduce the loss of segments due to congestion in the network.
- **2) User Datagram Protocol (UDP)**, is a **connectionless protocol** that **transmits user datagrams without first creating a logical connection**.
- In UDP, each user datagram is an independent entity without being related to the previous or the next one (the meaning of the term connectionless).

- UDP is a simple **protocol that does not provide flow, error, or congestion control.**
- Its simplicity, which means small overhead, is attractive to an application program that needs to send short messages and **cannot afford the retransmission of the packets involved in TCP, when a packet is corrupted or lost.**
- **3) *Stream Control Transmission Protocol (SCTP)*** is designed to respond to ***new applications that are emerging in the multimedia.***
- It provides support for newer applications such as voice over the Internet.
- It is a transport layer protocol that combines the ***best features of UDP and TCP.***

❖3. Network Layer

- The **network layer is responsible for creating a connection between the source computer and the destination computer.**
- The communication at the **network layer is host-to-host**.
- However, since there can be several routers from the source to the destination, the **routers in the path are responsible for choosing the best route for each packet.**
- The network layer is **responsible for host-to-host communication** and **routing 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 at the network layer.**
- IP also **defines the format and the structure of addresses used in this layer.**

- IP is also **responsible for routing a packet from its source to its destination**, which is achieved by each router forwarding the datagram to the next router in its path.
- The network layer **also includes unicast (one-to-one) and multicast (one- to-many) routing protocols.**
- A routing protocol does not take part in routing (it is the responsibility of IP), but it creates forwarding tables for routers to help them in the routing process.
- The network layer also has some auxiliary protocols that help IP in its **delivery and routing tasks.**
- The examples of such protocols are ICMP, IGMP, DHCP, ARP etc.

Sr. No.	Protocol	Function
1	Internet Control Message Protocol (ICMP)	helps IP to report some problems when routing a packet
2	Internet Group Management Protocol (IGMP)	helps IP in multitasking.
3	Dynamic Host Configuration Protocol (DHCP)	helps IP to get the network-layer address for a host.
4	Address Resolution Protocol (ARP)	helps IP to find the link-layer address(Hardware Address)of a host or a router when its network- layer address(IP) is given.
5	Reverse Address Resolution Protocol (RARP)	helps IP to find the network-layer address(IP)of a host or a router when its the link-layer address(Hardware Address) is given.

❖2. Data Link Layer

- An internet is made up of **several links (LANs and WANs) connected by routers.**
- There may be several **overlapping sets of links that a datagram can travel from the host to the destination.**
- The **routers are responsible for choosing the best links**.
- However, when the next link to travel is determined by the router, the **data-link layer is responsible for taking the datagram and moving it across the link.**
- The link can be a wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.
- There can be a different protocols used with any link type.

- In each case, **the data-link layer is responsible for moving the packet through the link.**
- TCP/IP **does not define any specific protocol for the data-link layer.**
- It supports all the standard and proprietary protocols.
- *Any protocol that can take the datagram and carry it through the link suffices for the network layer*. **The data-link layer takes a datagram and encapsulates it in a packet called a frame.**
- Each link-layer protocol may provide a different service.
- Some link-layer protocols provide complete error detection and correction, some provide only error correction.

❖1. Physical Layer

- The physical layer is **responsible for carrying individual bits in a frame across the link.**
- Although the physical layer is the **lowest level in the TCP/IP protocol suite**, the communication between two devices at the physical layer is still a logical communication because there is another, hidden layer, the transmission media, under the physical layer.
- **Two devices are connected by a transmission medium (cable or air).**
- The **transmission medium does not carry bits; it carries electrical or optical signals.**
- So the bits received in **a frame from the data-link layer are transformed and sent through the transmission media**
- There are **several protocols that transform a bit to a signal.**

Hardware Devices Used for Networking

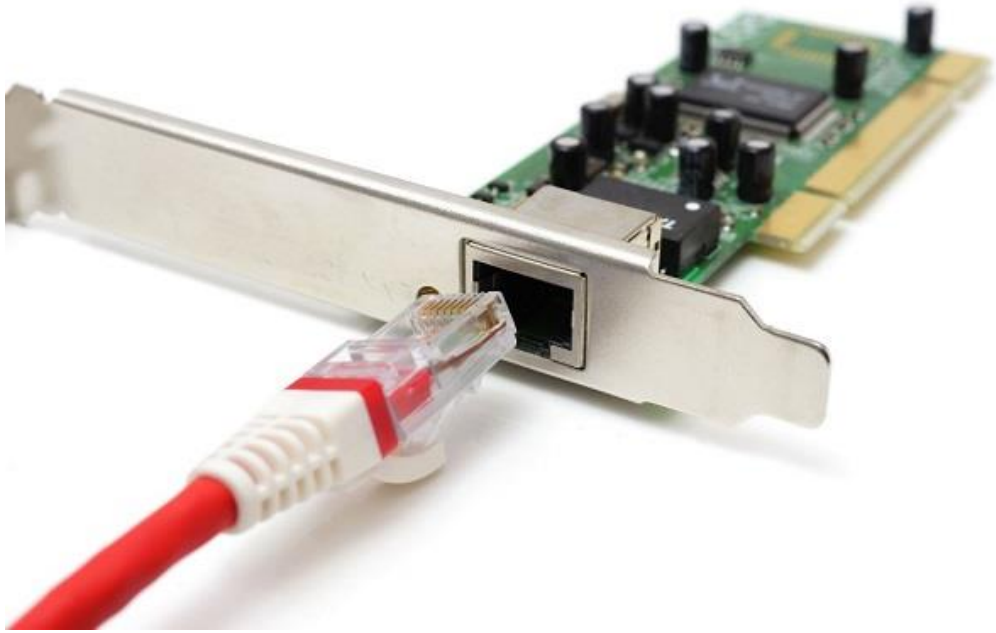
- **Networking hardware**, also known as **network equipment** or **computer networking devices**, are electronic devices which are required for **communication and interaction between devices on a computer network.**
- **Types of network devices** Here is the common network device list:

- NIC (Network Interface Card)
- Modem
- Hub
- Switch
- Router
- Bridge
- Gateway

NIC (Network Interface Card)

- For **any machine to connect to network**, it first **needs a Network Interface card**
- It is **used to connect computer or other device to the network**
- So to **create a network**, **NIC has a very important role**
- **Network interface card or NIC**, is also known as Ethernet card, network card, LAN card, network adapter or network adapter card (NAC) or Network Interface Unit(NIU) or Terminal Access Point (TAP).
- Any device which wants to connect to the network must contain a NIC card, even **switch and routers also consist NIC in order to connect to the network**
- It is a physical and data link layer device used by computers to connect to **Ethernet LAN** and communicate with other devices on the LAN.
- NIC provides physical connectivity between a device and a network .
- A **wired NIC** typically uses an **Ethernet cable to connect to the network** , While **wireless NIC** uses **radio waves to connect wirelessly**

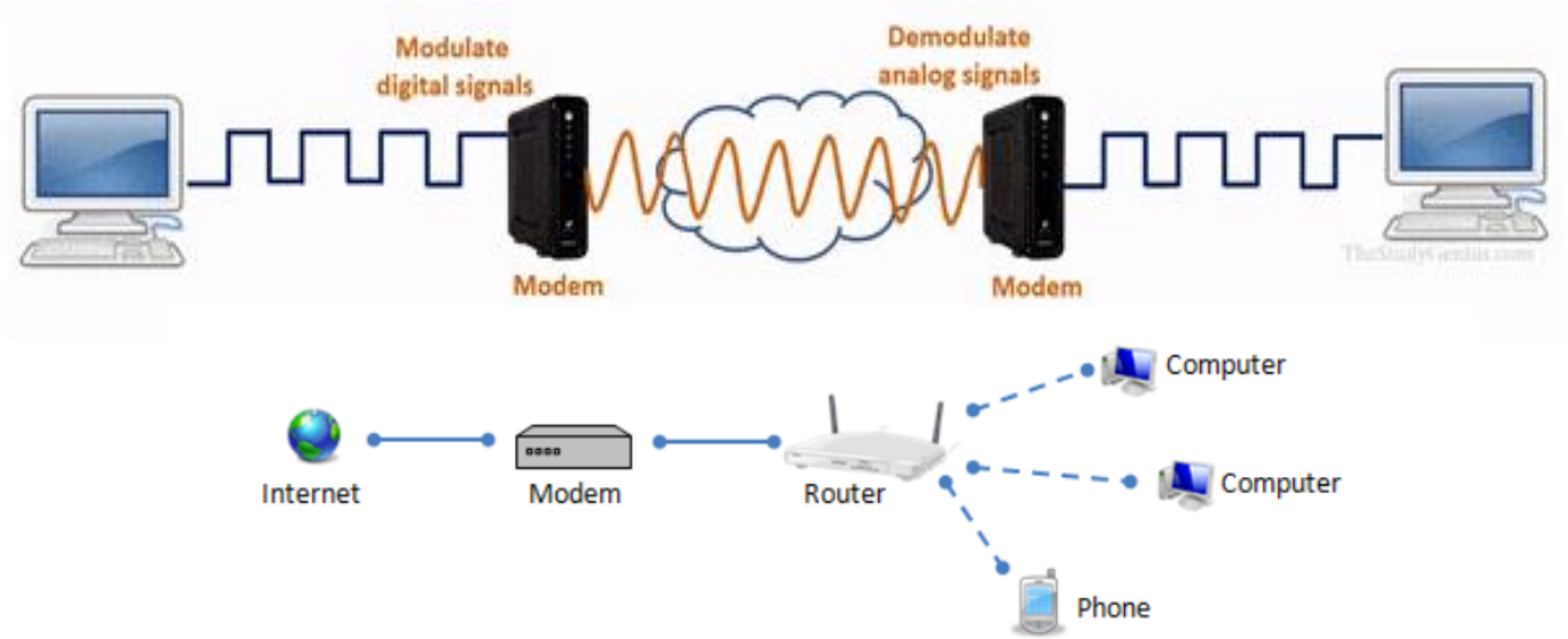
- Wired NIC



- Wireless NIC

Modem

- A modem is a **networking device** that is **used to connect the computer to the internet** where is **converts data signals into digital and analog forms.**
- It allows to **connect home network to internet** and **enables to access websites, send emails, stream videos and engage in other activities**
- In short, a modem **acts as an intermediary between the digital world of the computer** and the **analog world of the telephone line or cable network**, enabling the computer to communicate with other devices over the network
- It **modulates digital signals into analog signals** for transmission and **demodulates incoming analog signals back into digital signals**
- If we want access the internet in our home or business, we should have modem

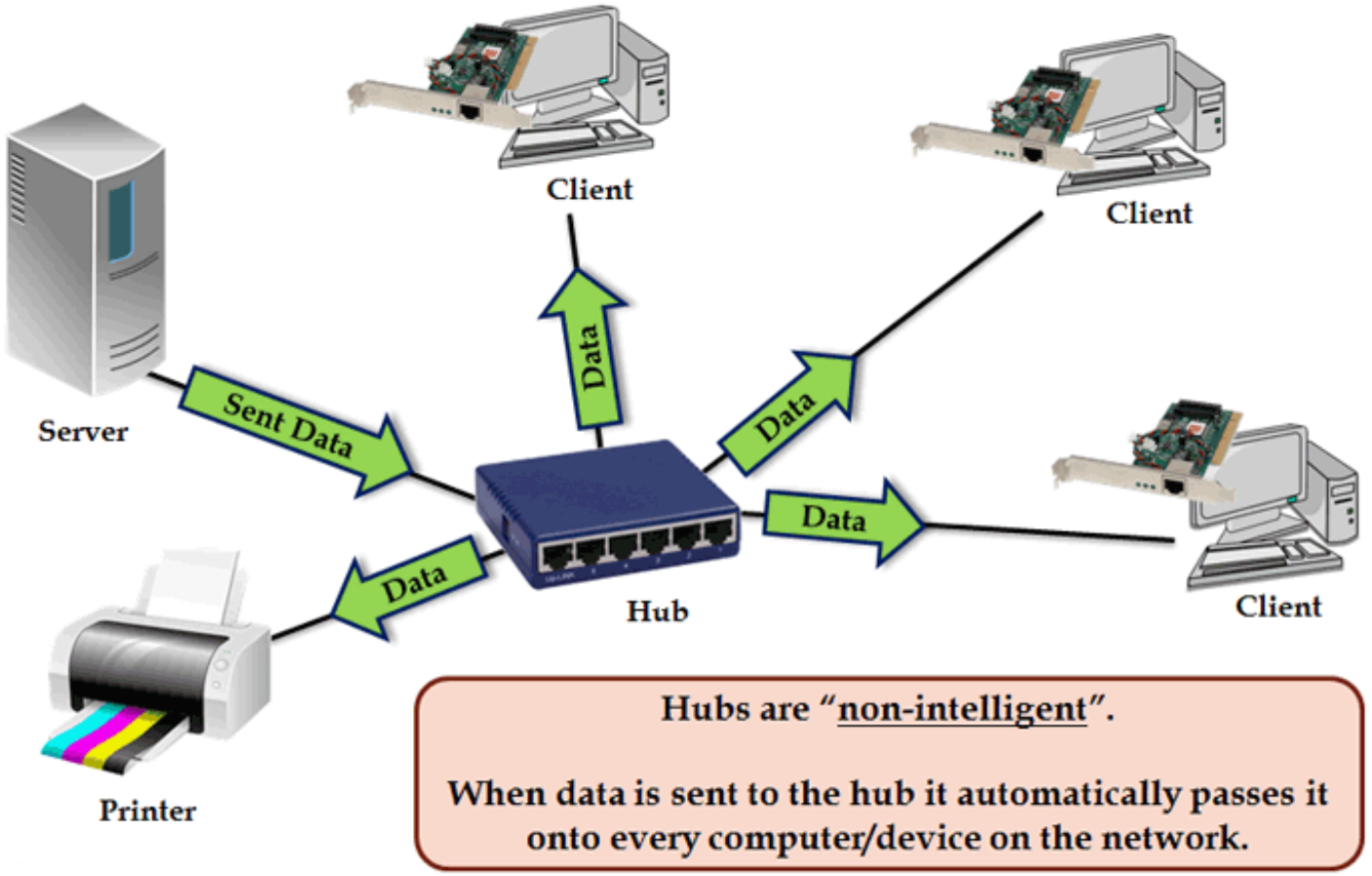


How a modem and router connect to each other, the Internet and devices on the network.

Hub

- Hub is a **physical layer device** which has multiple ports that are used to **connect multiple computers or segments of LAN together.**
- The data is **transferred in packets to entire computer network.**
- So when a host sends a data packet to a network hub, the **hub copies the data packet to all of its ports connected to.**
- Like this, **all the ports know about the data** and the **port for whom the packet is intended, claims the packet.**
- Hubs can be **passive or active**.

- **Passive hub allows the signal to be passed without any change**.
- ***Active Hubs amplify the signal as it moves from one device to another***. That helps to extend the range of network without using repeaters.
- **Disadvantages** of hub is that because of its working mechanism, a **hub is not so secure and safe**.
- Moreover, **copying the data packets on all the interfaces or ports makes it slower and more congested** which led to the use of network switch.



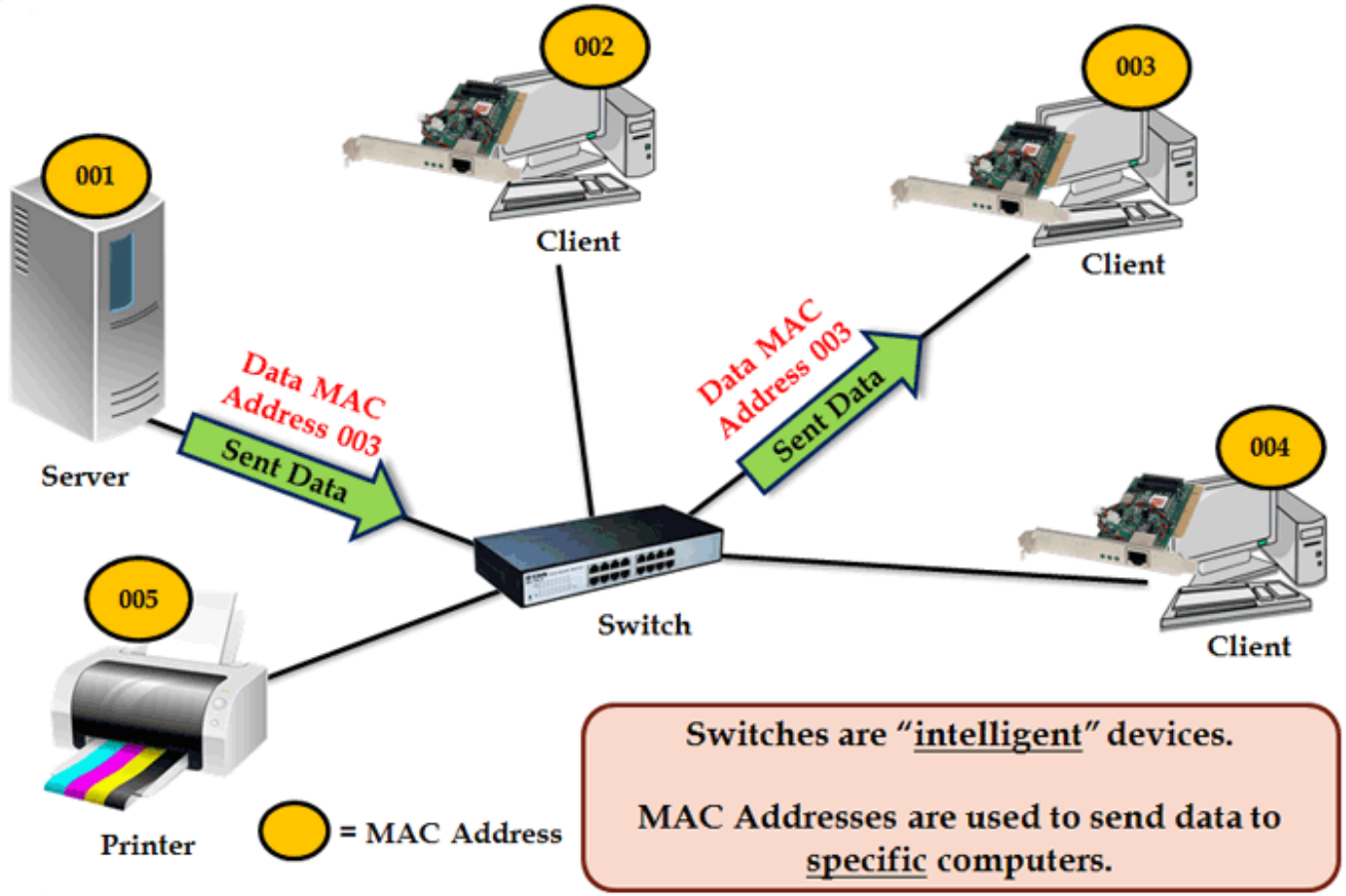
Hubs are "non-intelligent".

When data is sent to the hub it automatically passes it onto every computer/device on the network.

Switch

- Switch is a network device that **multiple ports , used to connect multiple devices and create a network**
- Switches are networking devices **operating at layer 2 or a data link layer**
- Switch is **more intelligent than a hub.**
- While **hub** just does the work of **data forwarding**, a **switch** does **'filter and forwarding' which is a more intelligent way of dealing with the data packets.**
- So, when a packet is received at one of the interfaces of the switch, it checks the destination address and transmits the packet to the correct receiver.
- Before forwarding, the **packets are checked for collision and other network errors**. This **technique is called packet switching technique.**

- A switch can **actually learn the physical addresses of the device that are connected to it**, store these physical address (called **MAC addresses) in its table**
- It is an intelligent device because it **has a memory where it maintains a table and stores the port number and MAC address of all devices**, which helps to identify every device on network



Switch L1 and Switch L2

➢Switch L1

- A physical layer switch, or Layer 1(L1) switch, **operates at the physical layer** of the OSI (Open System Interconnection) model.
- The easiest way to think of a Layer 1 switch is an electronic, programmable patch panel.
- It **simply establishes the physical connection between ports**.
- A Layer 1 switch **does not read, manipulate or use packet/frame headers to route the data.**

➢Switch L2

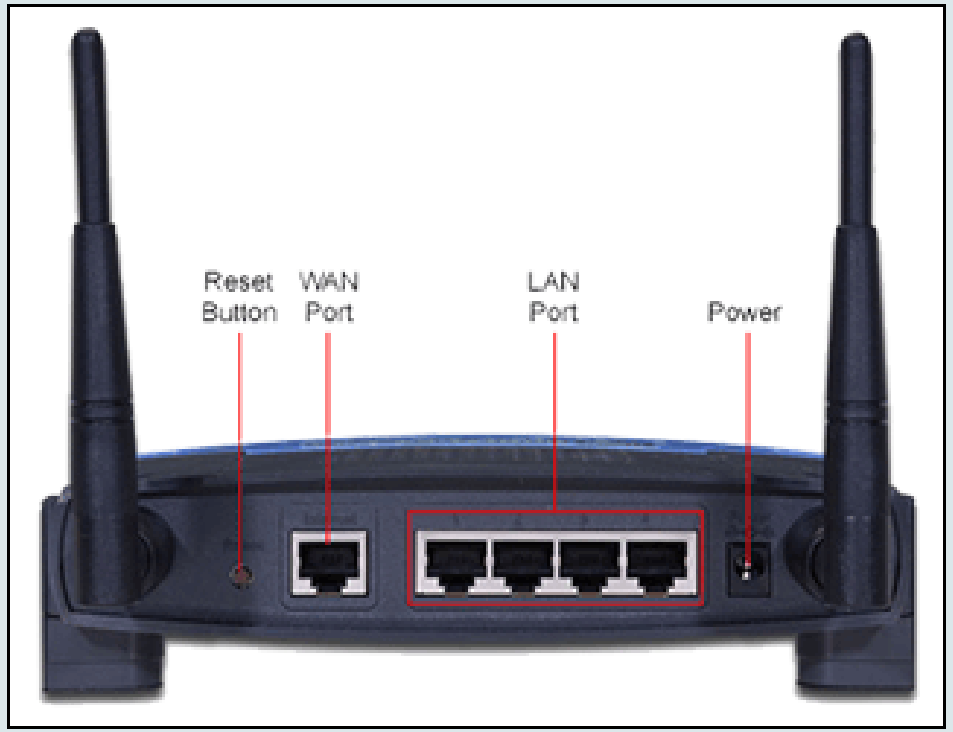
- A layer 2 switch is a type of network switch or device that **works on the data link layer** (OSI Layer 2)
- It connects **inputs and output ports by reading packet or frame headers and routes data** based on the location designated in the header.
- **It utilizes MAC Address to determine the path** through where the frames are to be forwarded.

Sr. No	Hub	Switch
1	Hub is a physical layer device i.e. layer 1.	Switch is a data link layer device i.e. layer 2.
2	In Hub, half duplex transmission technique is utilized.	In switch, full duplex transmission technique is utilized.
3	Hub follows broadcast transmission.	Switch follows three i.e., multicast, unicast, and broadcast type transmission.
4	Hub is not an intelligent device that sends message to all ports hence it is comparatively inexpensive.	While switch is an intelligent device that sends message to selected destination so it is expensive.
5	Hub is cheaper as compared to switch and router.	Switch is an expensive device than hub.
6	Hub does not allow packet filtering	Switch allows packet filtering

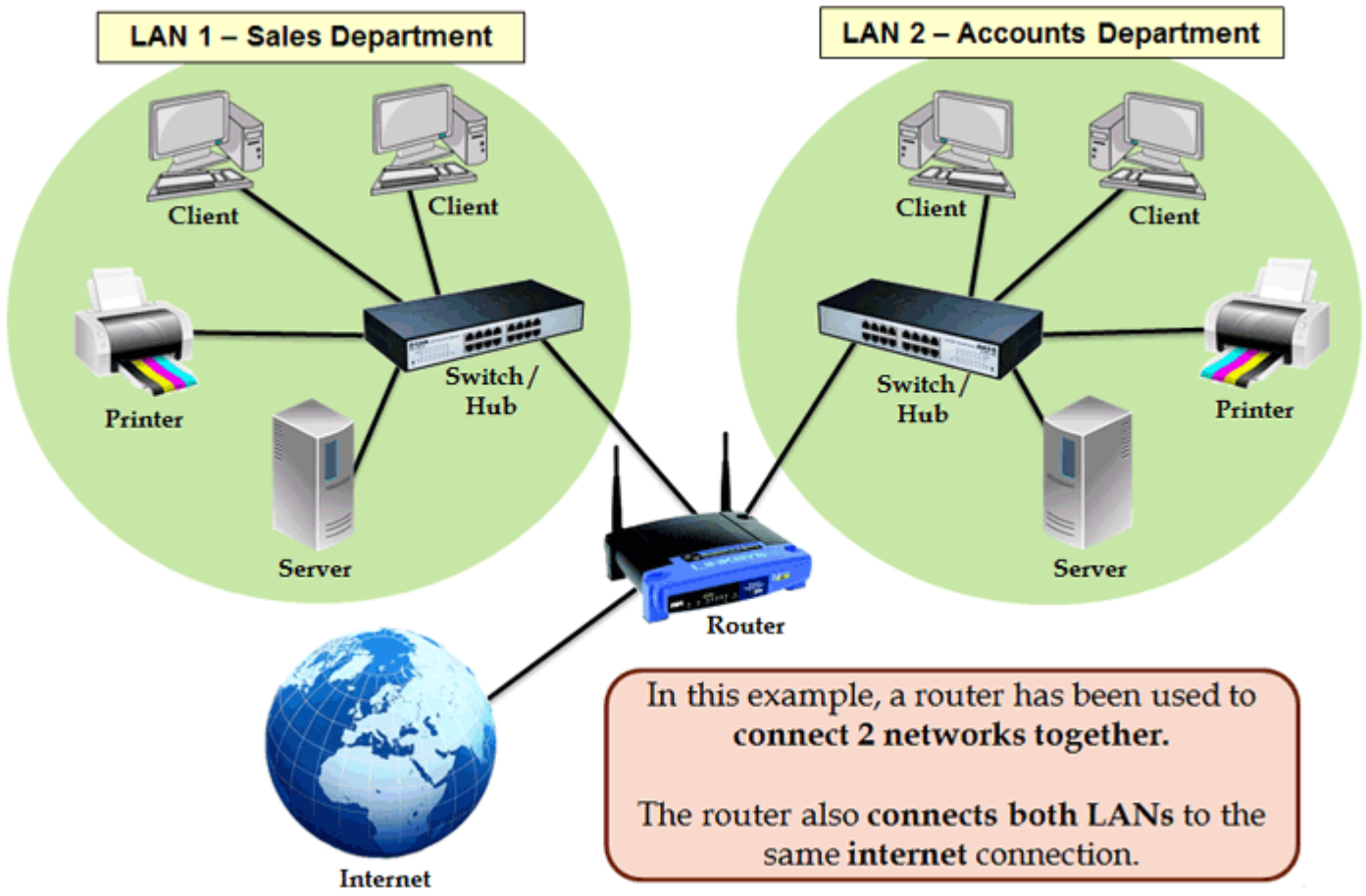
Router

- The internet is a group of networks , means many smaller and bigger network create the internet and **router is the only device that can connect to these network with each other.**
- A router is the **smartest or most complicated of the three.**
- Router is mainly a **Network Layer device.**
- It can work like a switch that **routes data packets based on their IP addresses.**
- Routers stores **IP addresses in routing table**
- The **routing table lists all of the different routes to other networks**
- The router will use the **routing table to determine the best route** to use when sending data to another network

- Routers normally **connect LANs with internet or other WANs together.**
- It has the capability to **repackage the data and send over another network.**
- There are many different types of **routers like WiFi router which can act as a combination router and modem**, converting an incoming broadband signal from your ISP.

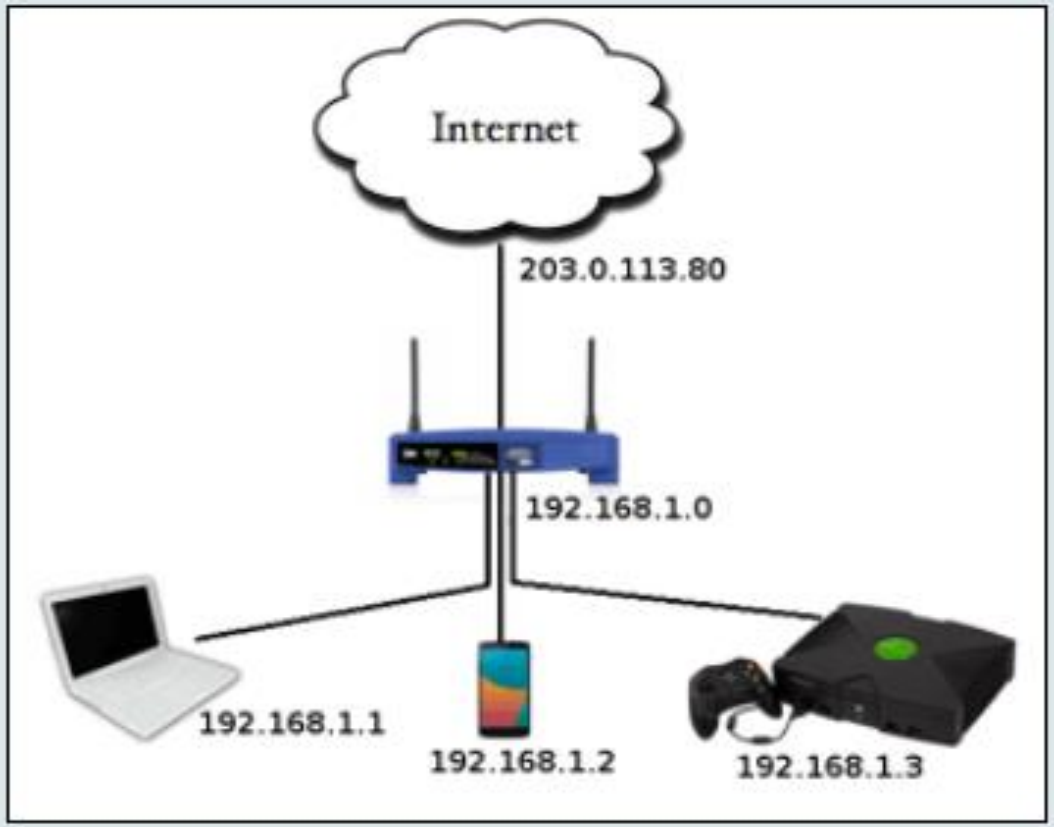


Routers allow computers on a LAN to share the same internet connection.



In this example, a router has been used to **connect 2 networks together.**

The router also **connects both LANs** to the same **internet** connection.

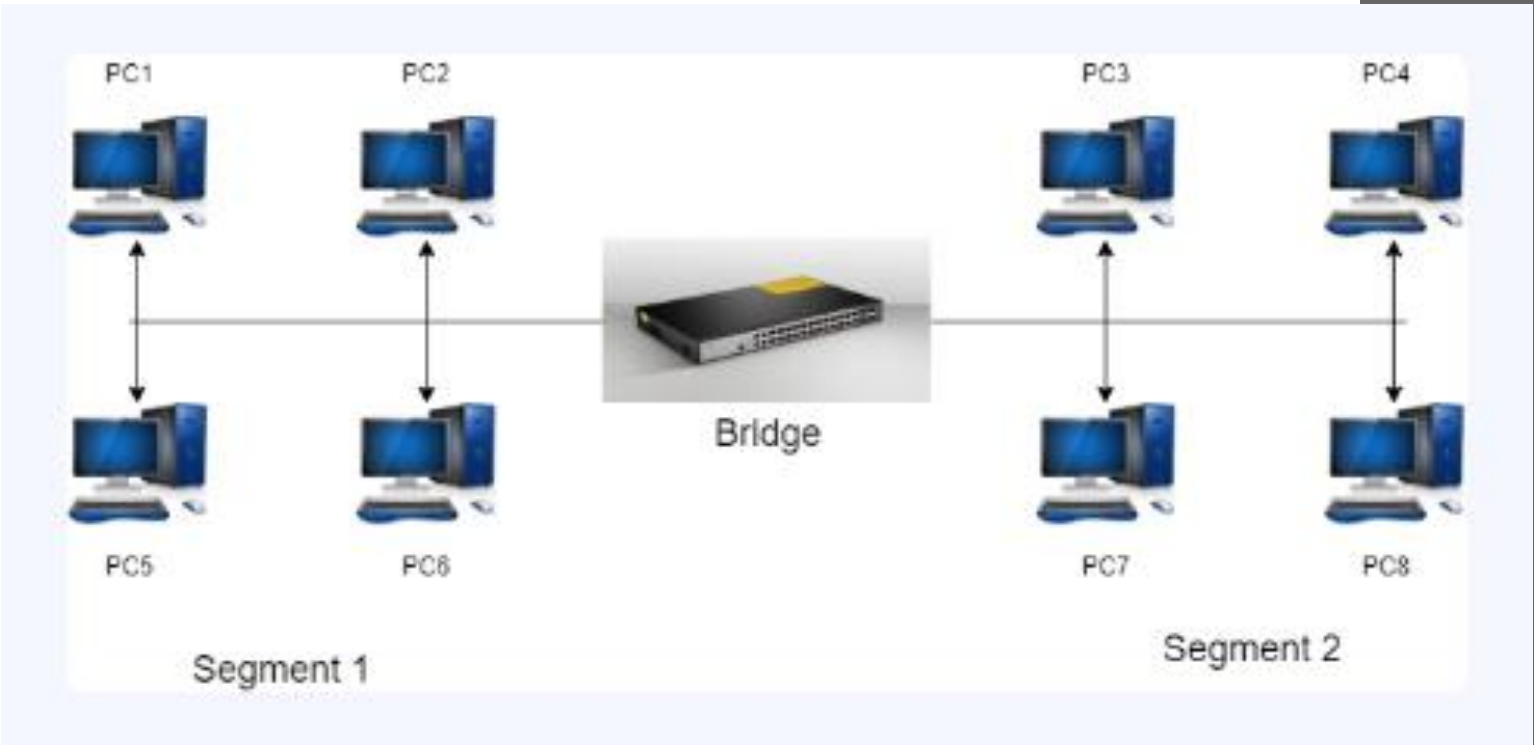


Routers use IP addresses to work out where to send packets of data.

Bridge

- It **operates at data link layer.**
- A bridge **connects two or more LANs.**
- Bridges can however **handle network that follow the same protocol.**
- It **Divide local area networks into multiple segments.**
- It **Maintains MAC address table** to discover new segments.
- A bridge in computer network **either blocks or forwards the data depending on the destination MAC address.**
- The address is written into each data frame.
- Like a hub, a modern bridge has multiple ports, but unlike hub, when a frame arrives, the bridge **extracts the destination address from the frame header and looks it up in a table** to see where to send the frame.

- The bridge only **outputs the frame on the port where it is needed** and can forward multiple frames at the same time.
- Filtering, forwarding and blocking of frames are functions of bridges.
- Bridges offer much better performance than hub



Gateway

- **Gateway** is a network device **used to connect two or more dissimilar networks.**
- That is **networks that use different protocols.**
- It **establishes** an intelligent **connection between a local network and an external network.**
- A gateway in networking is a network node that **acts as an entry and exit point to another network**, as **all data coming in and going out of a network must first pass through the gateway** in order to use routing paths.
- The gateway acts as a portal between two applications via protocol communications, **allowing them to share data on the same or other systems.**
- At home it could be the ISP which connects your computer to internet.

GATEWAY