# 19CAB09 – DATA COMMUNICATION AND NETWORKS

Prepared by

S.NITHYANANTH, ASP

DEPARTMENT OF MCA

MUTHAYAMMAL ENGINEERING COLLEGE,RASIPURAM.

# OBJECTIVES

- To understand networking concepts and basic communication model.
- To understand network architectures and components required for data communication.
- To analyze the function and design strategy of physical, data link, network layer and transport layer.
- To Acquire knowledge of various application protocol standard developed for internet.

# UNIT I NETWORK FUNDAMENTALS

Introduction to Networks – Categories of Networks -Communication model –Data transmission concepts and terminology – Protocol architecture – Protocols – OSI – TCP/IP – LAN Topology - Transmission media.

# UNIT II DATA LINK LAYER

Data link control – Error Detection – VRC – LRC – CRC – Checksum – Error Correction – Hamming Codes – MAC – Ethernet, Token ring , Token Bus – Wireless LAN - Bluetooth – Bridges.

# UNIT III

# NETWORK LAYER

Network layer – Switching concepts – Circuit switching – Packet switching – IP Addressing –IPV4, IPV6 – Routing Protocols – Distance Vector – Link State.

# UNIT IV

# TRANSPORT LAYER

Transport layer – service – Connection establishment – Flow control – Transmission control protocol – Congestion control and avoidance – User datagram protocol - Transport for Real Time Applications (RTP).

# UNIT V APPLICATIONS

Applications - DNS – E-Mail Protocols – WWW – SNMP – SMTP - Security – Threats and Services- Cryptography -DES-RSA- Web security -SSL .

# OUTCOMES

- Able to trace the flow of information from one node to another node in the network.
- Able to Identify the components required to build different types of networks.
- Able to understand the functionalities needed for data communication into layers.
- Able to choose the required functionality at each layer for given application.
- Able to understand the working principles of various application protocols.
- Acquire knowledge about security issues and services available.

# REFERENCES

1.Forouzan, “ Data Communication and Networking”, Fifth Edition , TMH 2012

2. Larry L. Peterson & Bruce S. Davie, “Computer Networks – A systems Approach”, Fourth Edition, Harcourt Asia / Morgan Kaufmann, 2010.

3.William Stallings, “Data and Computer Communications”, Nineth Edition, Prentice Hall 2011.

4. Andrew S.Tannenbaum David J. Wetherall, “Computer Networks”Fifth Edition , Pearson Education 2011

5.James F. Kurose, Keith W. Ross, “Computer Networking: A Top-down Approach, Pearson Education, Limited, sixth edition,2012.

6. John Cowley, “Communications and Networking : An Introduction”, Springer Indian Reprint, 2010.

# UNIT – I

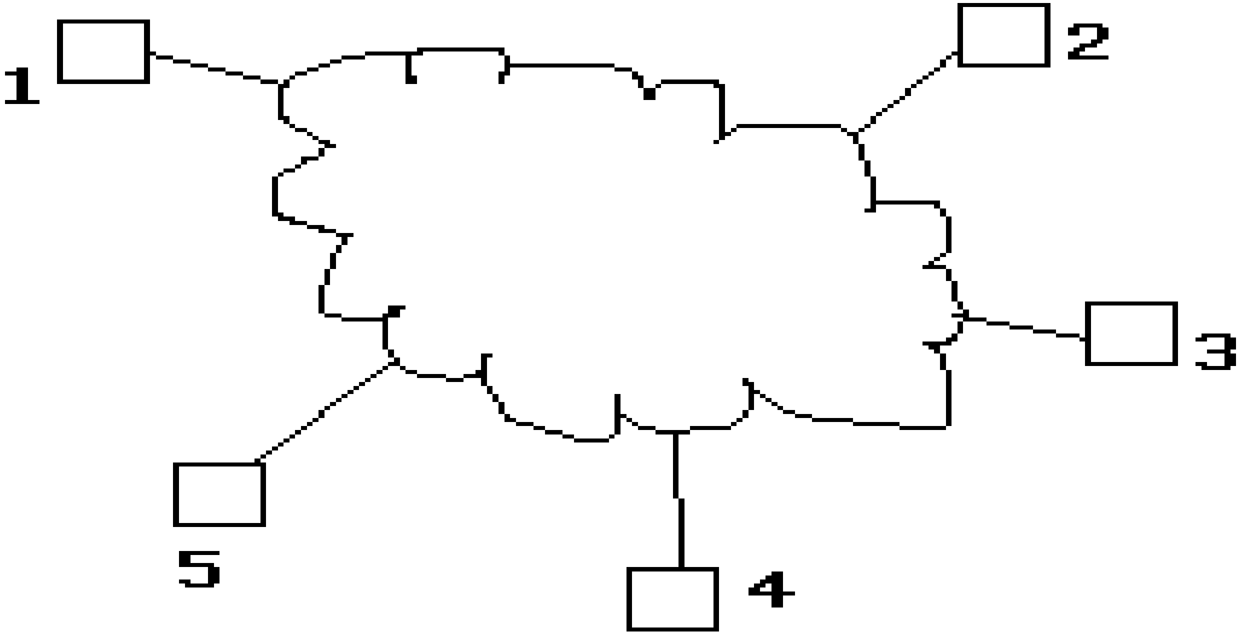
# NETWORK FUNDAMENTALS

# OVERVIEW

- Introduction to Networks
- Categories of Networks
- Communication Model
- Data Transmission Concepts and Terminology
- Protocol Architecture
- Protocols
- OSI
- TCP/IP
- LAN Topology
- Transmission Media

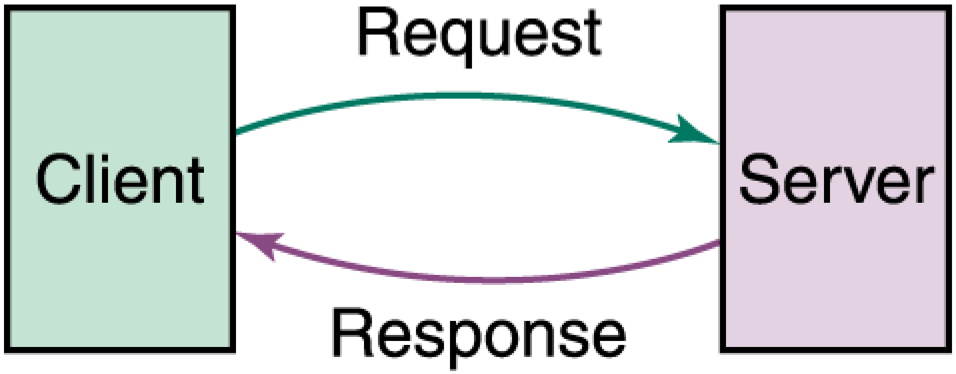
# Introduction to Networks

- *A Network: A group of devices that can communicate with each other over links.*
- *Each device is called a host. Each host has a unique address.*



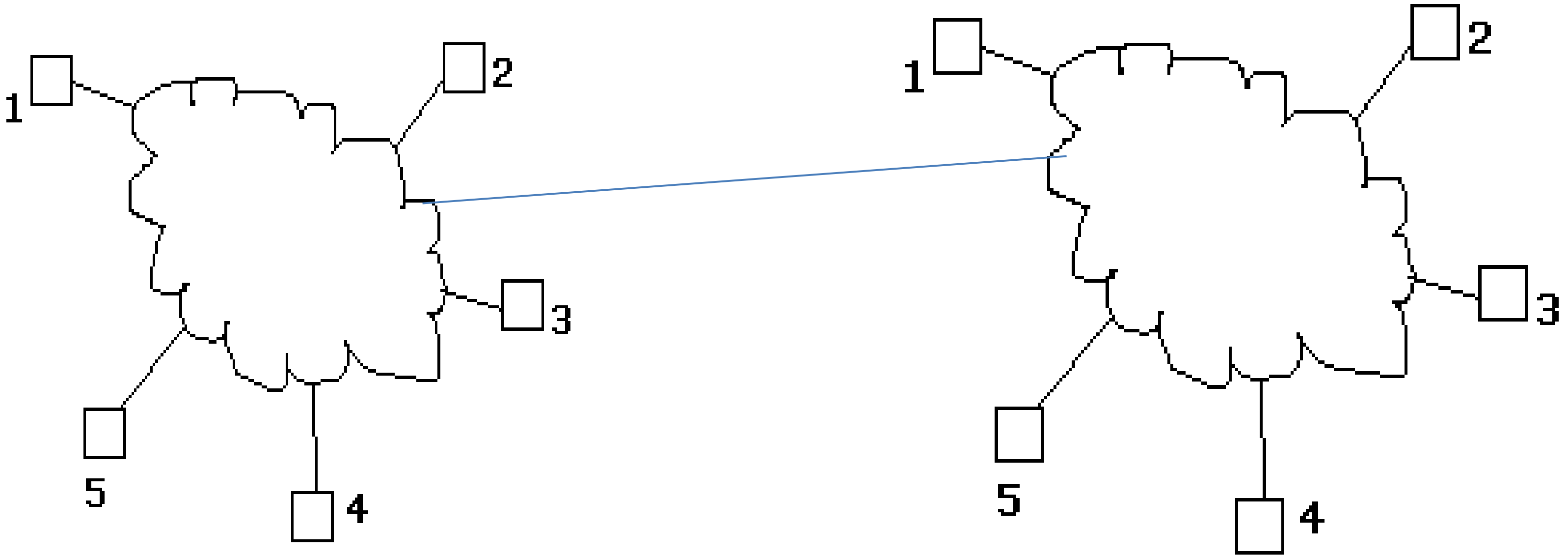
- **Network** is a connection between two or more devices.
- Which is connected by a communication links.
- A node can be computer, printer or any other devices which is capable of sending and receiving information at each other.

## *Example:*



# INTERNET

- **An internet**: **A network of networks or connection between two or more Networks is also known as internet.** each host has an address of the form **n/h** where **n is the network number** and **h is the number of the host on network n**.



# Uses of Network

- It is Used for

i) Business Application

ii) Home Application

iii) Mobile Users

iv) E-Mail

# Categories or Types of Network

- **There are Three Types:**

  **1. LAN - Local Area Network**

  **2. MAN - Metropolitan Area Network**

  **3. WAN – Wide Area Network**

## 1. LAN - Local Area Network

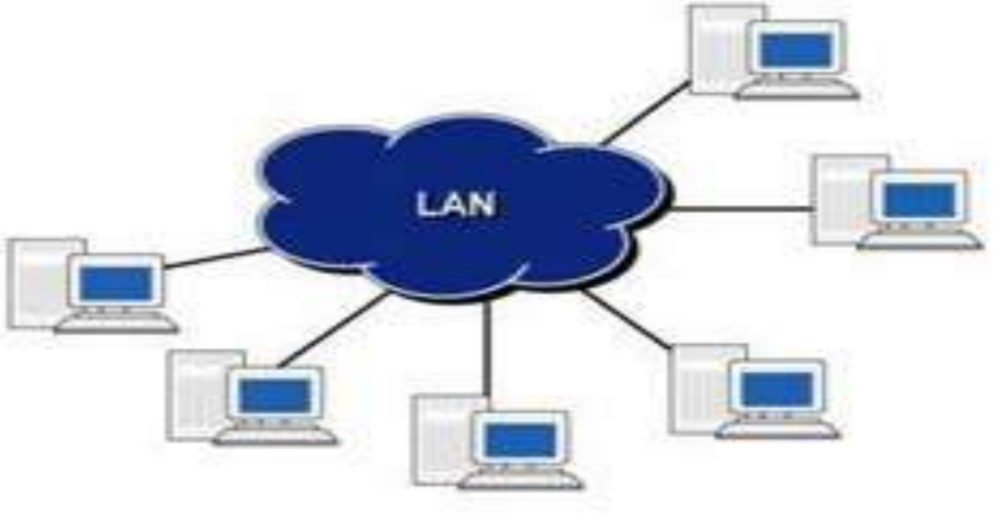
A LAN is Designed by Local Area Connections such as:

i) within Building

ii) within office

iii) within Campus

iv) within Specifi



## Advantages :

1) Sharing of Files.

2) Sharing of Programs.

3) Communication Exchange.

## Disadvantages :

1) Reliability.

2) Capacity.

3) High Cost.

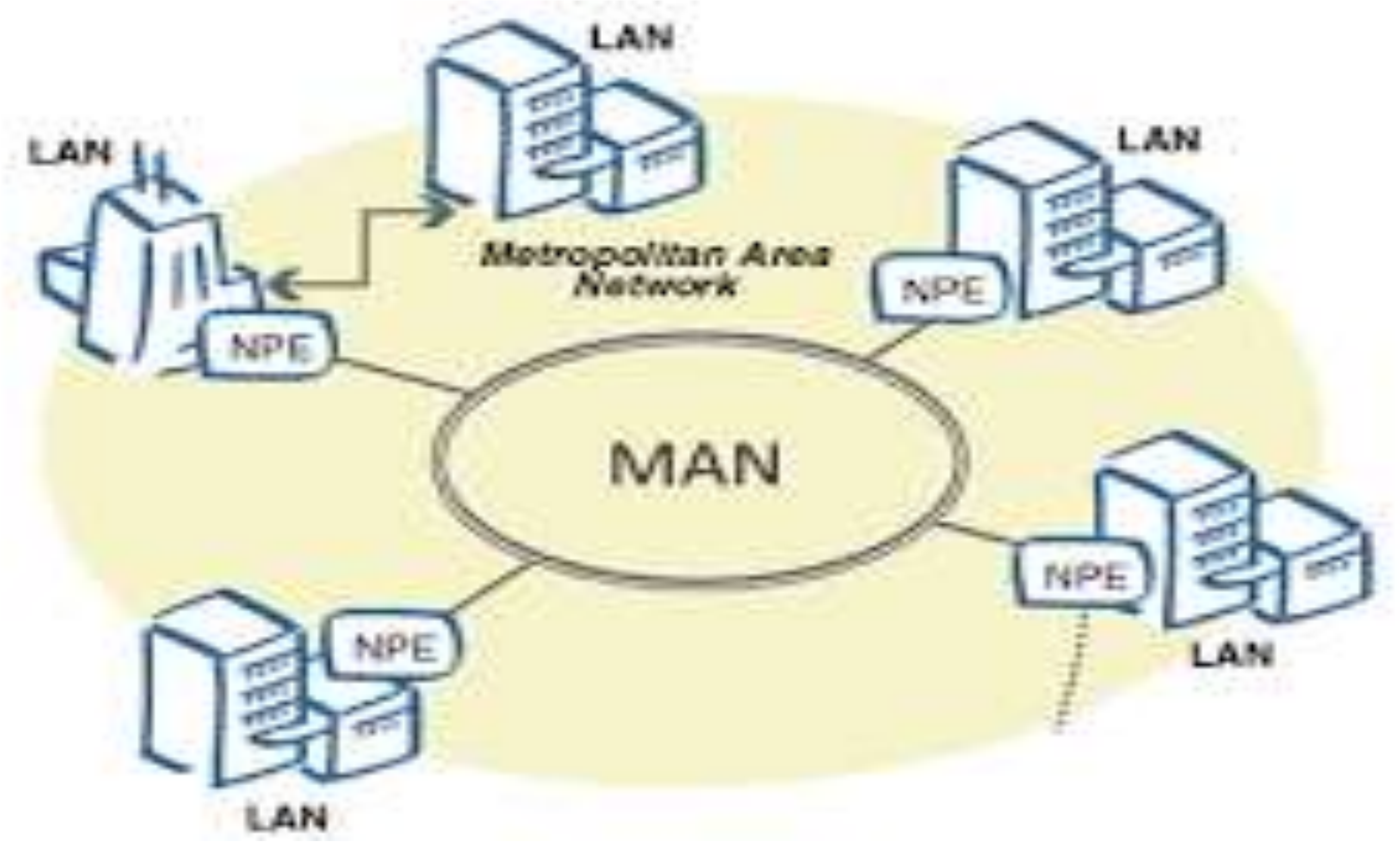
## 2. MAN - Metropolitan Area Network

A Metropolitan Area Network (**MAN**) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

- MAN supports up to 150 Kilometers Distance.
- Example:

→ Telephone Network

→  Cable TV



## Advantages :

1) High Bandwidth.

2) It support Large number of Clients.

3) Reduce the Errors.

## Disadvantages :

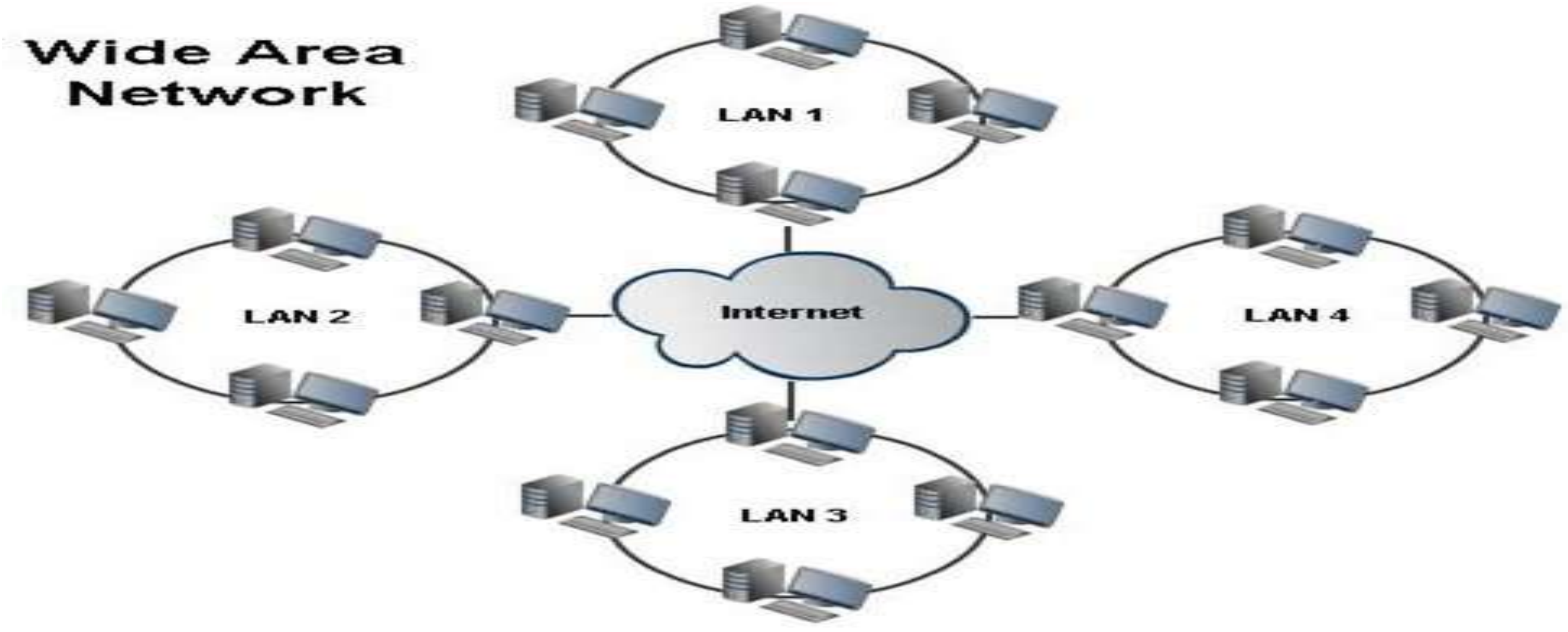
1) Large Space Requirements.

2) Slower Data Access.

3) High Cost.

## 3. WAN – Wide Area Network

- WAN Provide a Long Distance Transmission of Data.
- By Using WAN Exchange the Information from one country to another country.



# Components of Network

1) **Client** - Which gives the Request.

2) **Server** - Which gives the Response.

3) **Modems** - It Indicates Modulator / Demodulator.

4) **Router** - Which identifies the Path between Client & Server.

5) **Channels** - Which overcomes the Traffic problems.

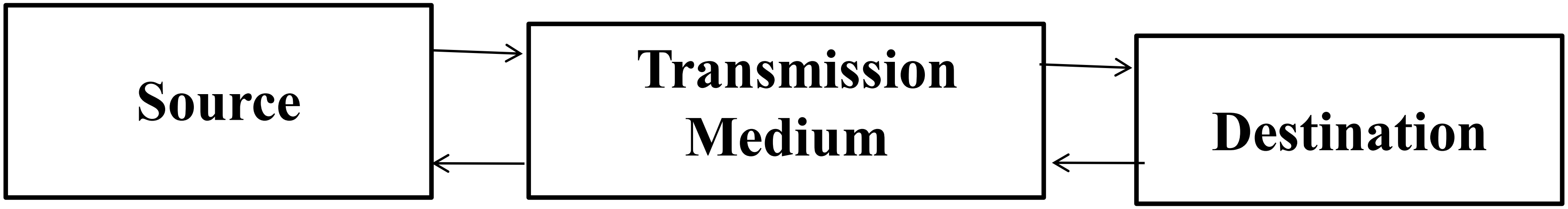
# Communication Model

- Data communications are exchange of data between **two devices via some transmission medium.**
- **It should be done in two ways**

  **i) Local** - It takes LAN Connection.

  **ii) Remote** - It takes Long distance like MAN & WAN.
- Data should be Transferred in the form of **0's and 1's**

# Block Diagram for Communication Model:



# Characteristics of Communication Model :

1) **Delivery** - The System must deliver the data to the correct Destination.

2) **Accuracy** - The System must deliver the data at Accurate way.

**3) Timeline -** The System must deliver the data at **Exact Time.**

**4) Jitter -** It refers to the variable in the **Perfect Arrival Time.**

## Components of Communication Model :

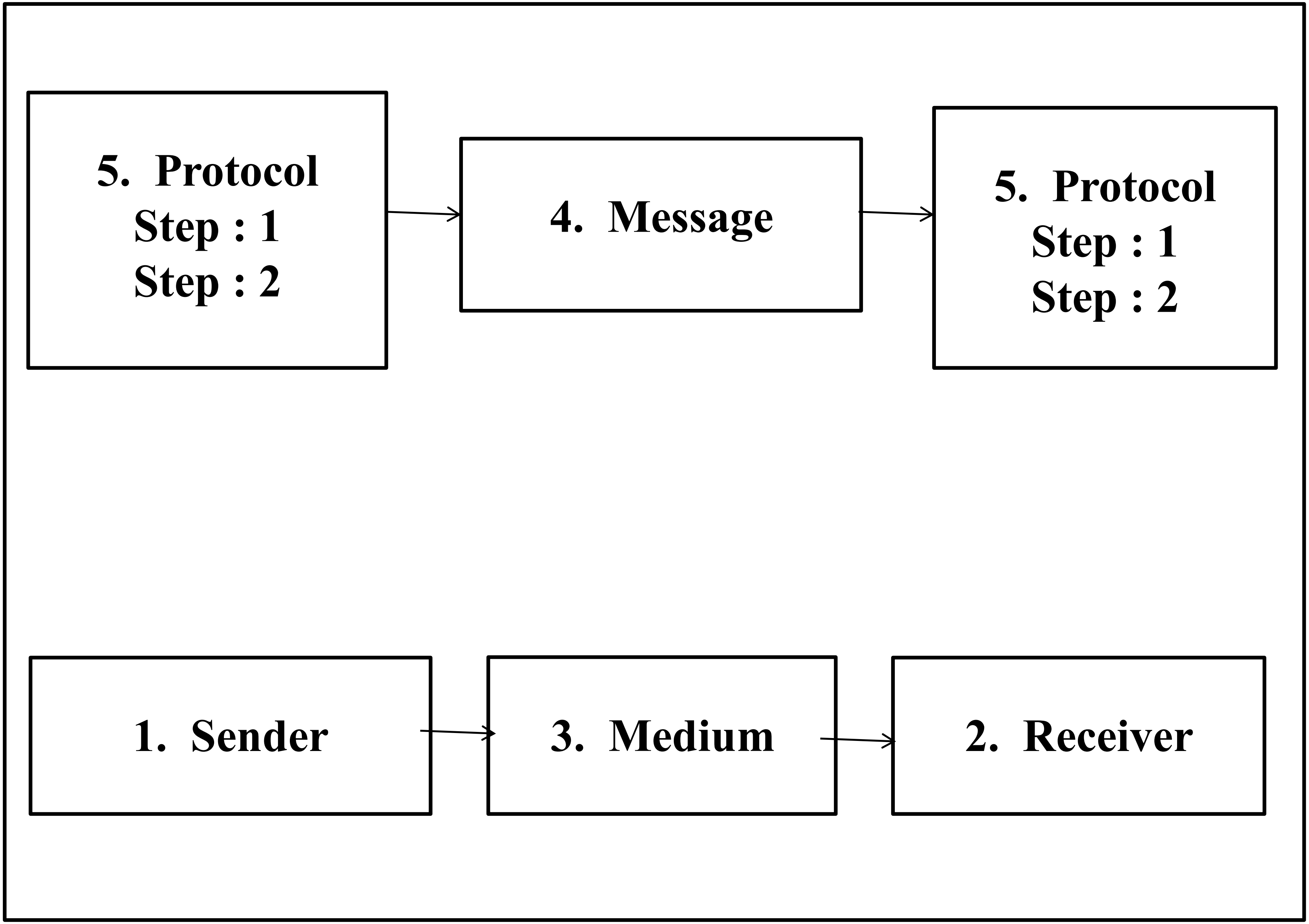
**i) Sender**

**ii) Receiver**

**iii) Medium**

**iv) Message**

**v) Protocol**



5. Protocol
Step : 1
Step : 2

4. Message

5. Protocol
Step : 1
Step : 2

1. Sender

3. Medium

2. Receiver

1. **Sender** : It is a device , that Sends the information to the Receiver.

2. **Receiver** : It is a device , that Receives the information from the Sender.

3. **Medium** : It is the physical path between Sender to Receiver.

4. **Message** : This is the passing Informations.

5. **Protocol** : It is a set of rules and regulations that “ Governed “ from data communication.

# Data Transmission Concepts and Terminology

- Data Transmission occurs between sender and receiver over some Transmission Medium or Transmission Media.
- Transmission Media may be classified into **Two Types :**

    **i) Guided Media [Wired Technology]**

    **ii) Unguided Media [Wireless Technology]**

## i) Guided Media (Wired Network)

- In Guided Media Signals are Passed in a “ same physical path”
- Example:

  i) Twisted pair Cable

  ii) Coaxial Cable

  iii) Fiber Optic Cable

## ii) Unguided Media (Wireless Network)

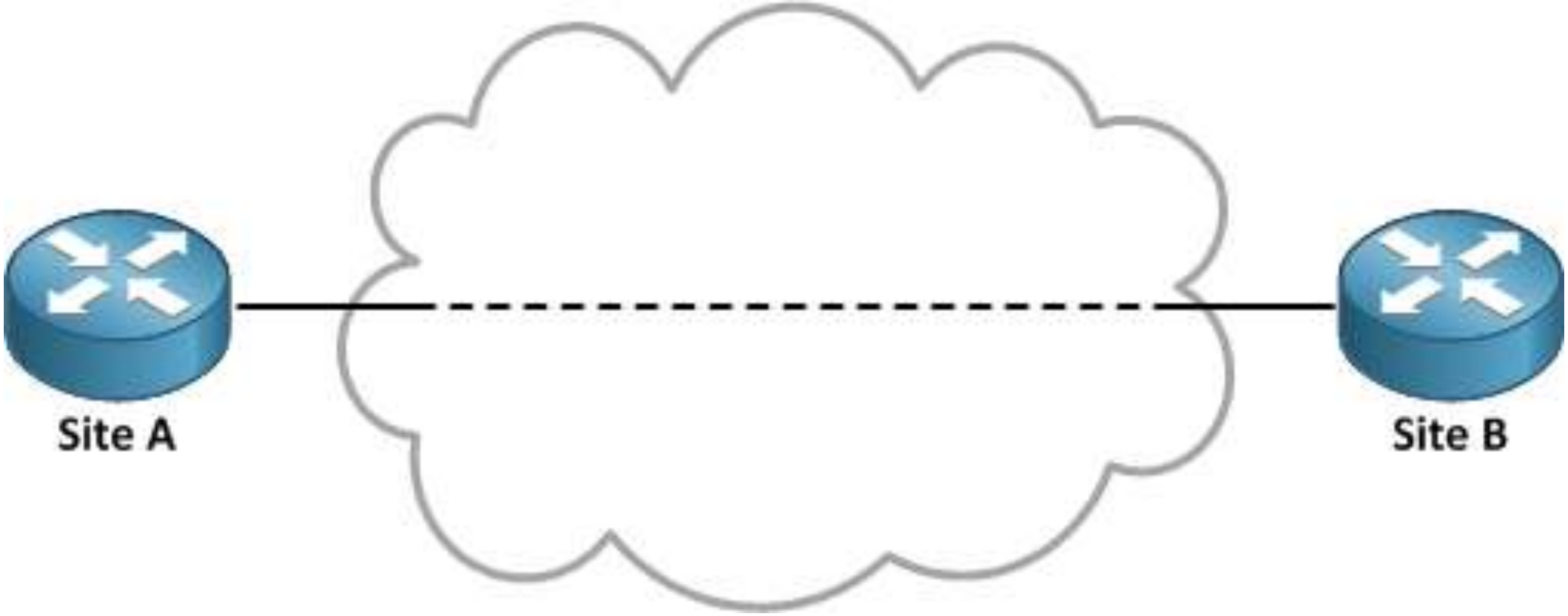
- In Unguided Media Signals are Passed in  the form of “ Electromagnetic Waves”
- Example :

i) Mobile phones

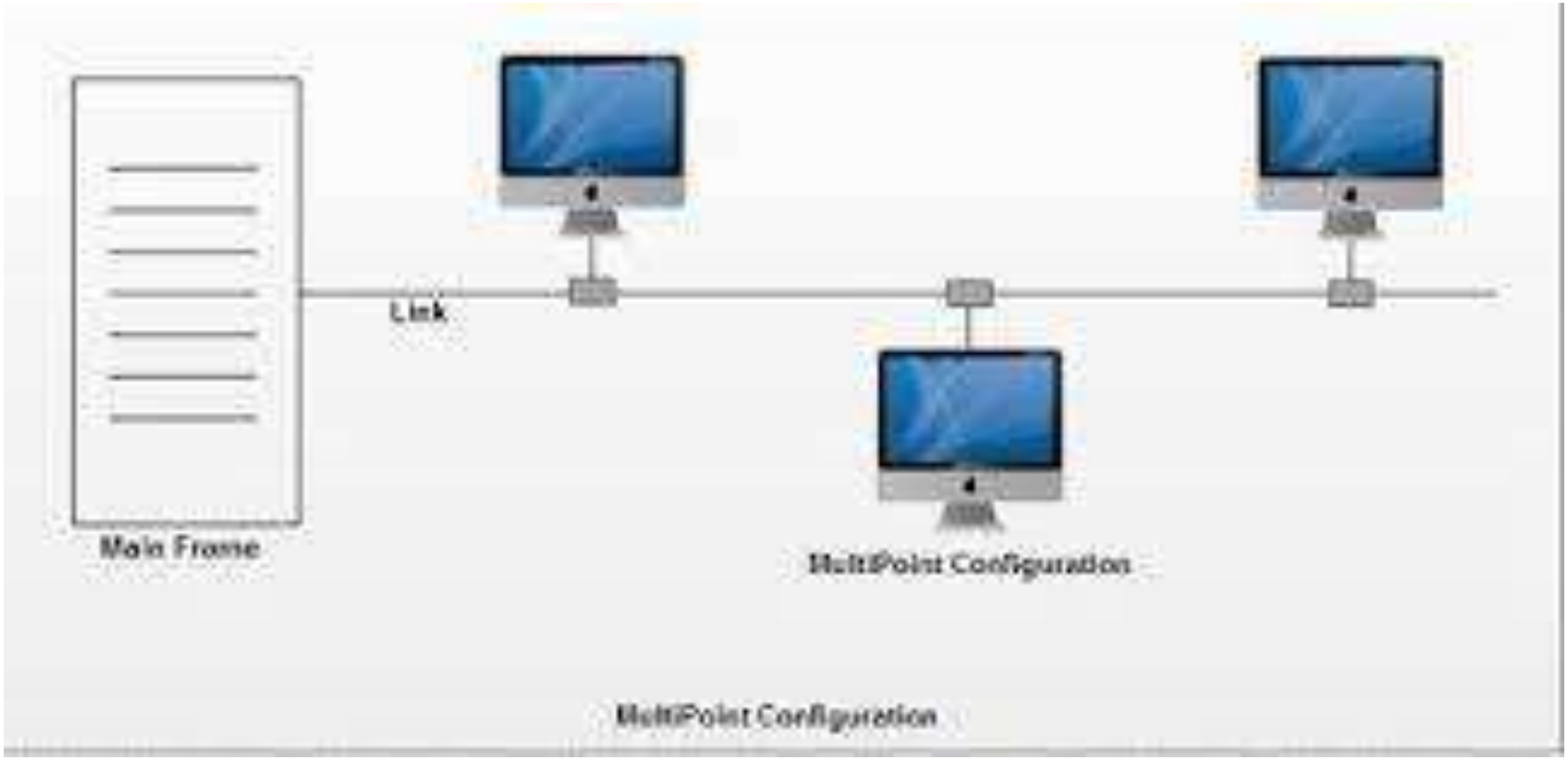
ii) Satellite microwave

iii) Infrared

- Point - to - Point Connection : It **Provides a dedicated links between two devices**.
- For example, a wired system that connects two computers together can be thought of a point-to-point link.



- **Multi - Point Connection : It is a link between two or more devices.** It is also known as Multi-Point configuration. The networks having multipoint configuration are called **Broadcast Networks.**



# Transmission Mode

- It refers to the direction of information flow between two devices.
- Data flow is the flow of data between 2 points.
- The direction of the data flow can be described as
  - Simplex Mode
  - Half-Duplex Mode
  - Full-Duplex Mode

- **Simplex:** Data flows in only one direction on the data communication line (medium).

  Examples are Radio and Television broadcasts.

- **Half-Duplex:** Data flows in both directions but only one direction at a time on the data communication line.

  Ex. Conversation on walkie-talkies.

- **Full-Duplex:** Data flows in both directions simultaneously. Modems are configured to flow data in both directions.

  Ex. Phone Conversation

# Data Flow

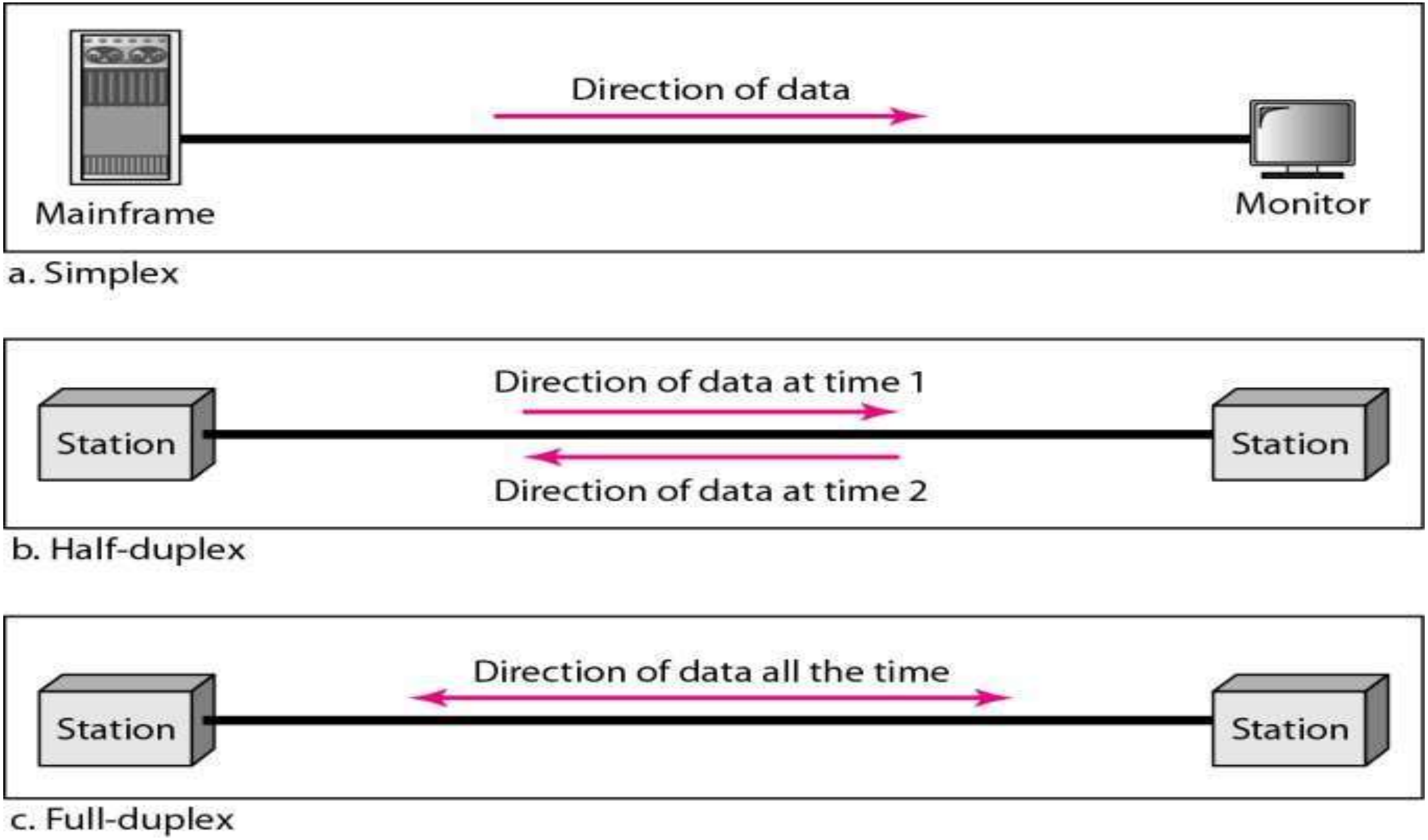


**Figure 1.2** ***Data flow (simplex, half-duplex, and full-duplex)***

# Protocol Architecture

- It is a layered structure of H/W and S/W that supports exchange of data b/w systems
- It supports distributed applications(E-Mail, File Transfer)
- Each layer of protocol architecture provides some set of rules
- There are 2 widely used protocol architecture

✓ TCP/IP Architecture

✓ OSI Model

# Protocol

- Protocol is a set of rules that govern data communication
- It represents **what** is communicated, **when** it is communicated and **how** it is communicated.
- There are 3 key elements

✓ Syntax

✓ Semantics

✓ Timing

# Syntax

- It represents **structure**, Format of data the order in which it is presented

Data may contain:

- First 8 bit -> Sender Address
- Second 8 bit -> Receiver Address
- Remaining bits-> message stream

## SEMANTICS

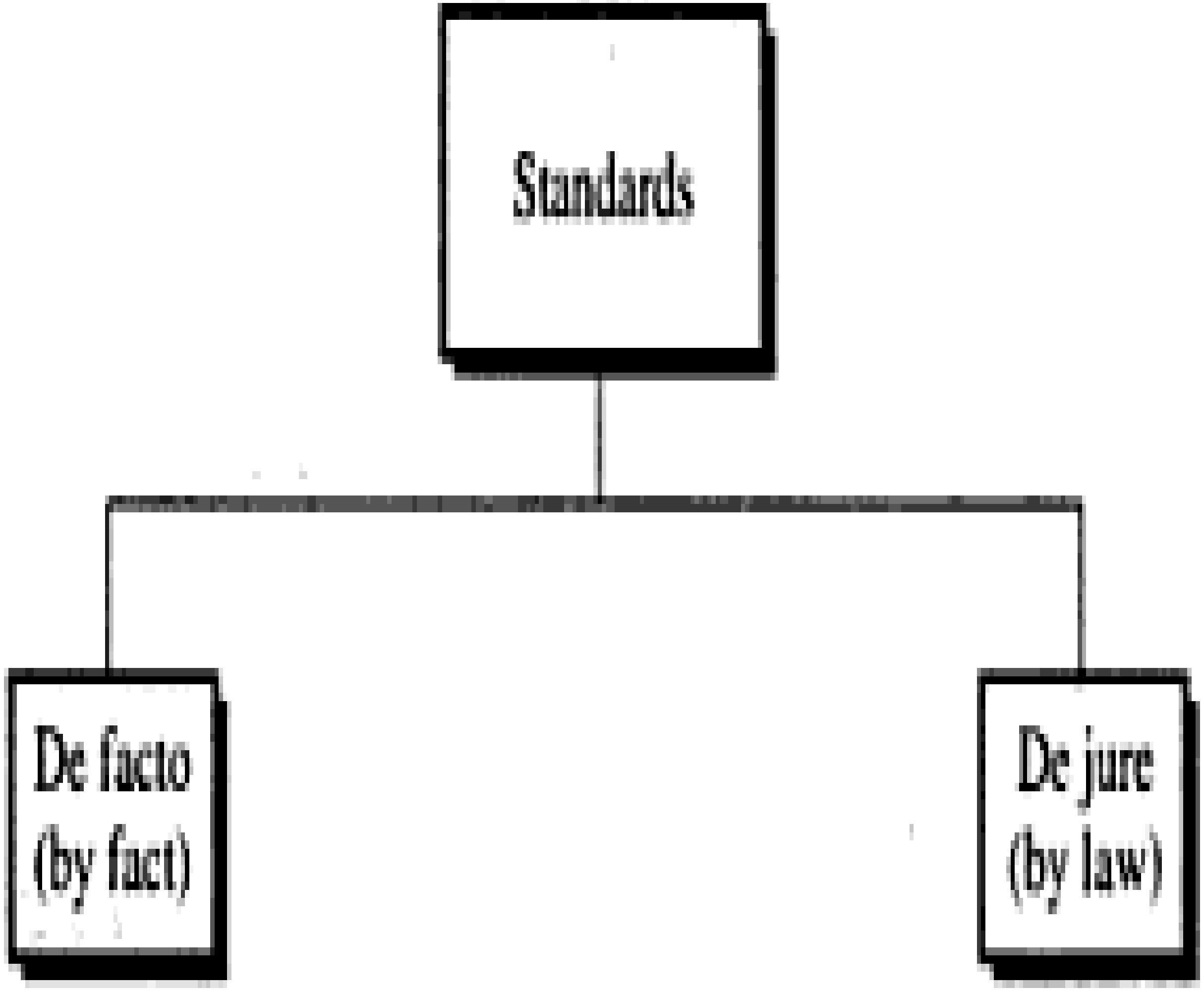
- It refers the **meaning** of each section of bit

## TIMING

- It refers when data sent and how fast it is sent (Says Characteristics)
- Ex:100Mbps

# Protocol Standards

- It provides **model for the development** of product regardless of individual manufacturer
- It falls in 2 categories


Standards
De facto (by fact)
De jure (by law)

# De Facto standard

- Not officially adopted but used widespread
- It has 2 categories
- Proprietary->Wholly owned by company
- Non-Proprietary->Group or communiy developed for public

# De Jure Standard

- A Standard Legislated by an officially recognized body

Standard Organizations:

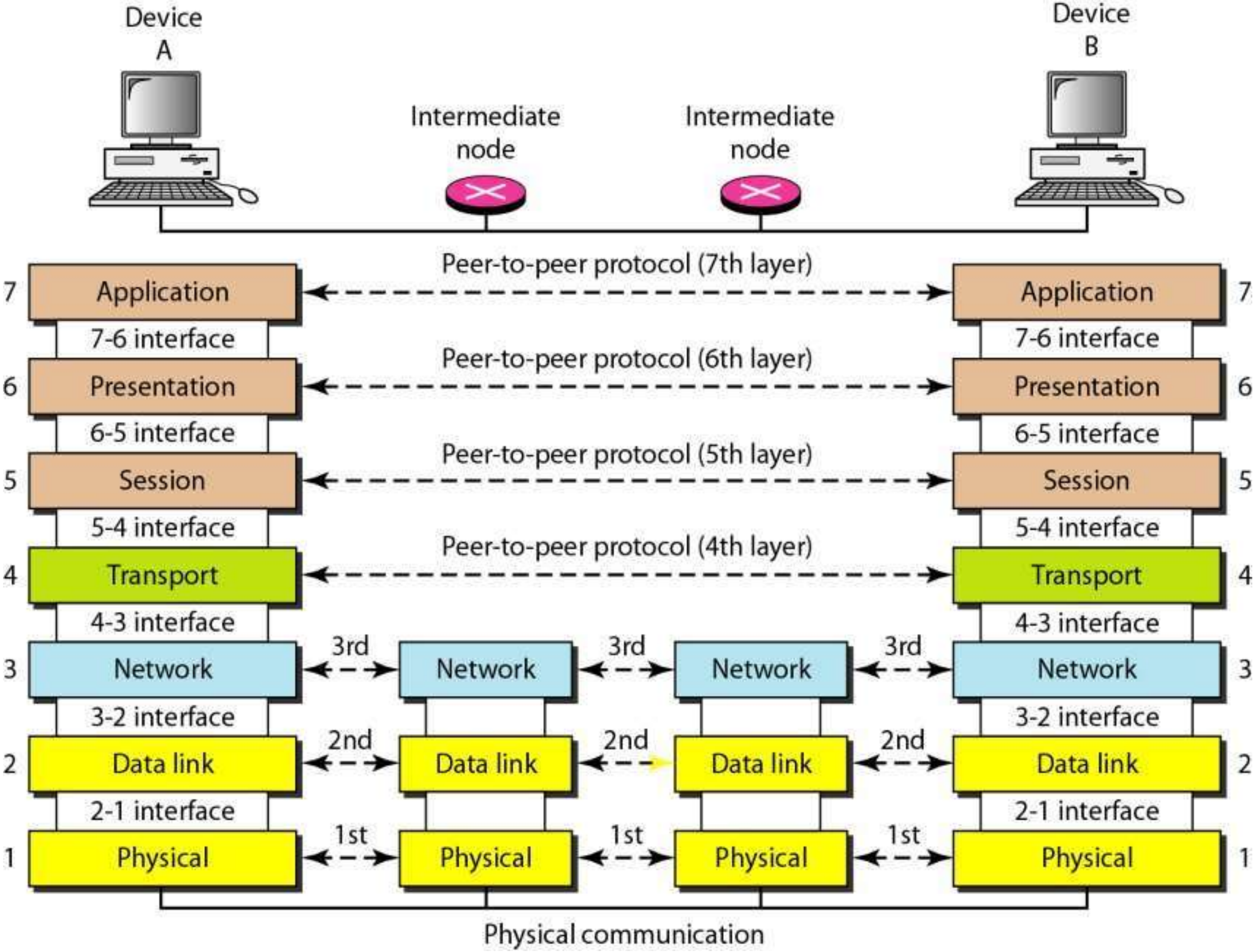
- International Standard Organization
- ANSI
- IEEE

# The OSI Model

- An ISO (International standard Organization) that covers all aspects of network communications is the **Open System Interconnection (OSI) model**.
- An open system is a model that allows any two different systems to communicate regardless of their underlying architecture (hardware or software).
- The OSI model is not a protocol; it is model for understanding and designing a network architecture that is flexible, robust and interoperable.

- The OSI model is a layered framework for the design of network systems that allows for communication across all types of computer systems.
- The OSI model is built of seven ordered layers:

1. **(Layer 1) Physical layer**
2. **(Layer 2) Data link layer**
3. **(Layer 3) Network layer**
4. **(Layer 4) Transport layer**
5. **(Layer 5) Session layer**
6. **(Layer 6) Presentation layer**
7. **(Layer 7) Application layer**

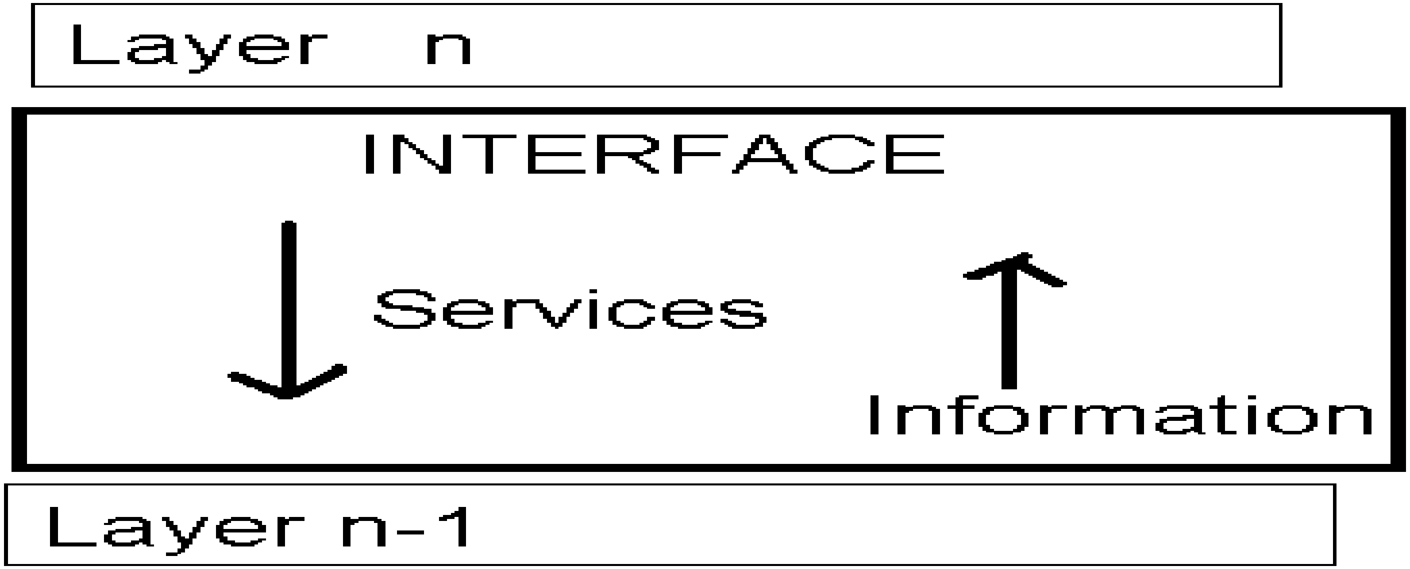

Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
Application 7
7-6 interface
Presentation 6
6-5 interface
Session 5
5-4 interface
Transport 4
4-3 interface
Network 3
3-2 interface
Data link 2
2-1 interface
Physical 1
3rd
3rd
3rd
Network
Network
2nd
2nd
2nd
Data link
Data link
1st
1st
1st
Physical
Physical
Physical communication

# Peer-to-Peer Process

- Within a single machine, each layer calls upon services of the layer just below it.
- Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4.
- Between machines, layer x on one machine communicates with layer x on another machine, by using a protocol (**this is Peer-to-Peer Process**).
- Communication between machines is therefore a peer-to-peer process using protocols appropriate to a given layer.

# Interfaces between Layers

- There is an interface between each pair of adjacent layers. This interface defines what information and services a layer must provide for the layer above it.



Layer n

INTERFACE

Services

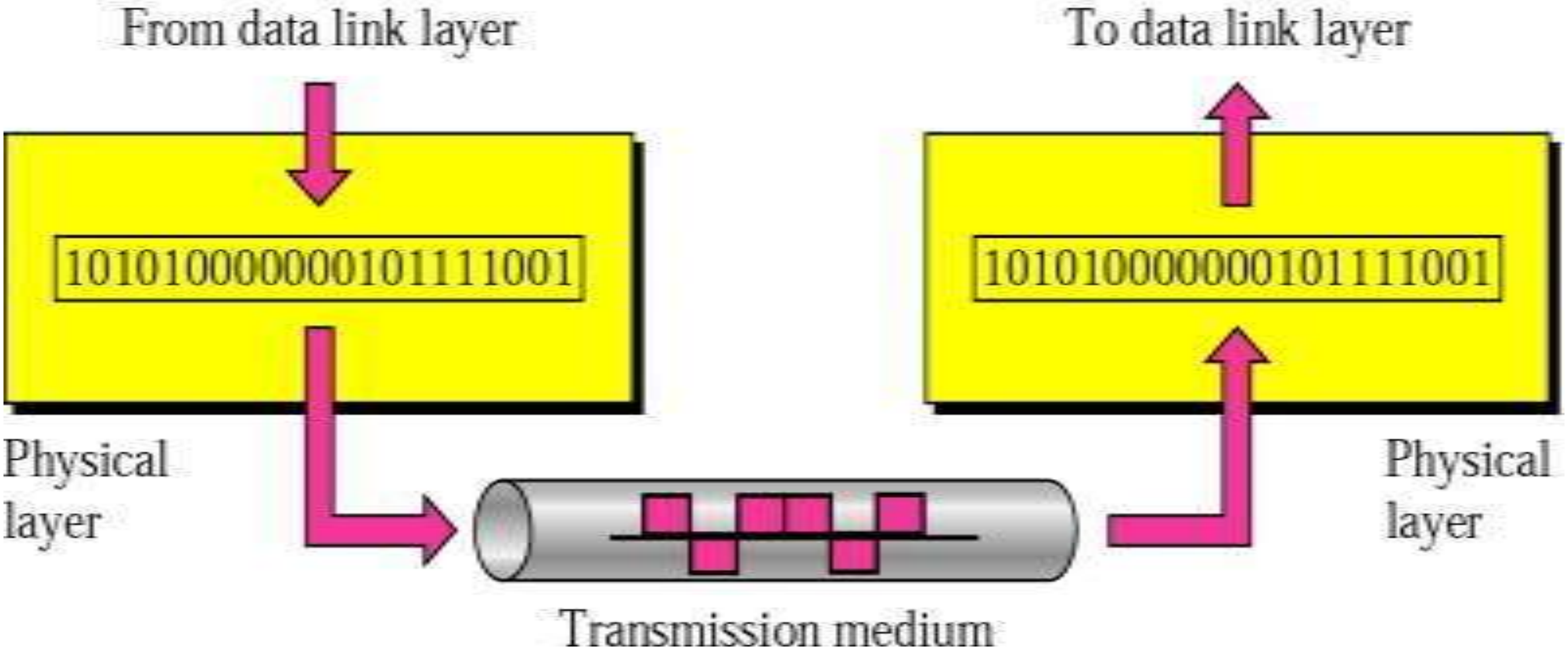
Information

Layer n-1

# Functions of Layers

## 1. Physical Layer

*The physical layer is responsible for transmitting* ***individual bits*** *from one node to the next.*



# Physical layer

The physical layer is concerned with the following:

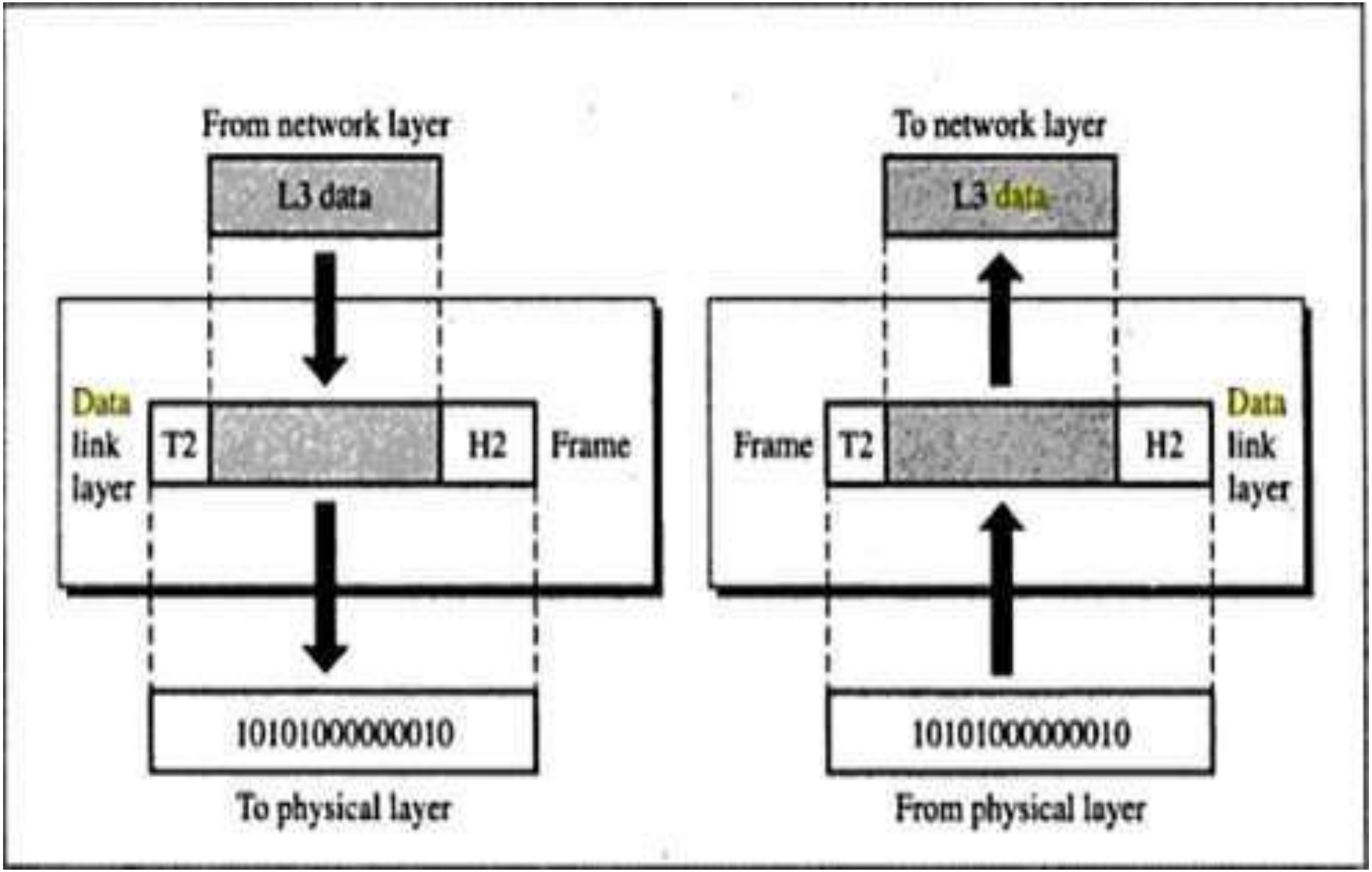
- **Physical characteristics of interfaces and media:** It define the type of transmission media
- **Representation of the bits:** the physical layer data consist of a stream of bits(0,1). The transmitted bits must be encoded into signals – **electrical or optical**. The physical layer defines the type of **encoding**.
- **Data rate:** The physical layer defines the **transmission rate**, the number of bits sent each second.

# Physical Layer

- Line configuration: the physical layer is concerned with the connection of devices to the medium.
- Physical topology – Ring, star
- Transmission Mode - Simplex, Half duplex Full Duplex

# 2. Data Link Layer

- It is responsible for **node-to-node** delivery of data.

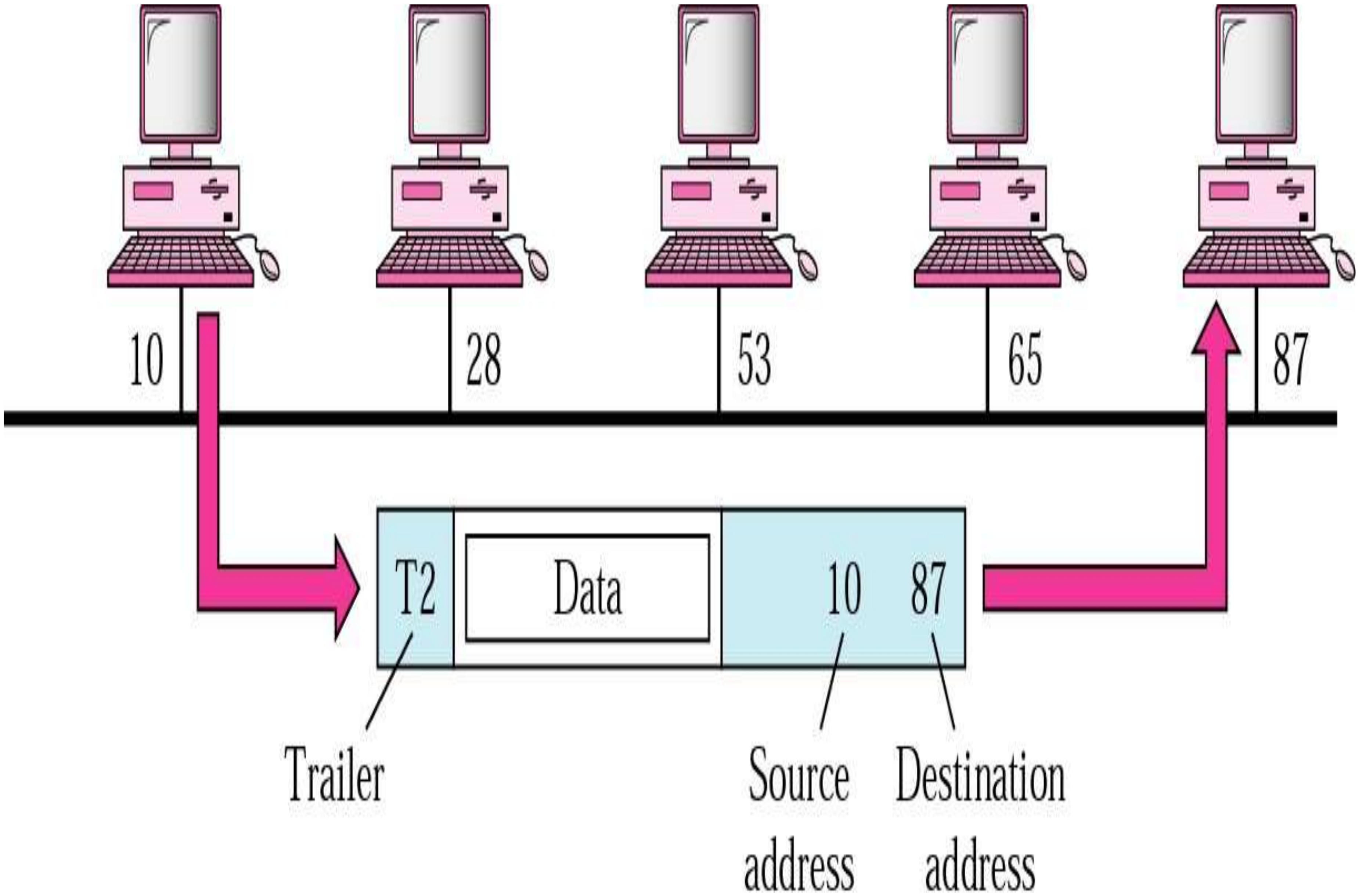


# Functions of the Data Link Layer:

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

- Physical addressing. If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender (source address) and/or receiver (destination address) of the frame.

- If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects one network to the next.


10
28
53
65
87
T2
Data
10
87
Trailer
Source address
Destination address

- Flow Control. If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.
- Error control. The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. Error control is normally achieved through a trailer to the end of the frame.

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

# 3. Network Layer

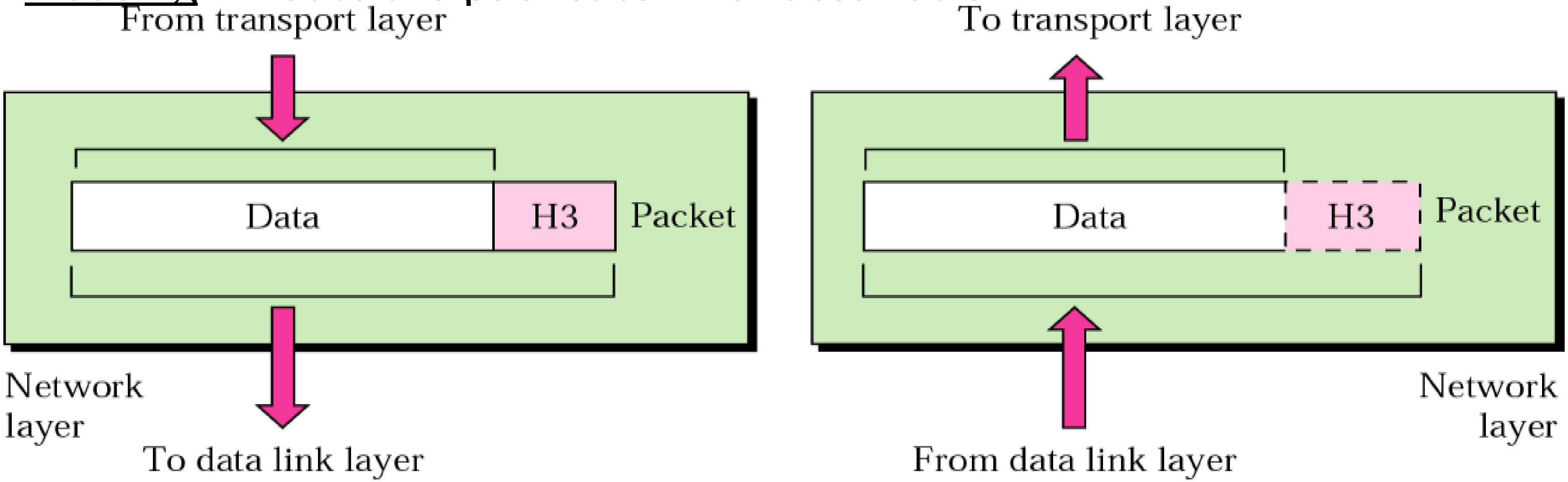
- The Network layer is responsible for the **source-to-destination delivery of a packet** possible across multiple networks.
- It converts **Frames into packets.**

- If **two systems are connected to the same link**, there is usually **no need for a network layer**. However, if the two systems are attached to different networks, there is often a need for the network layer to accomplish source-to-destination delivery.

# Network Layer

## Functions:

- <u>Logical addressing</u>-Physical addressing (May change) handle addressing problem locally
- If packet pass the network boundary, we need another addressing called logical addressing (Never change)
- <u>Routing</u> - Route the packet to final destination

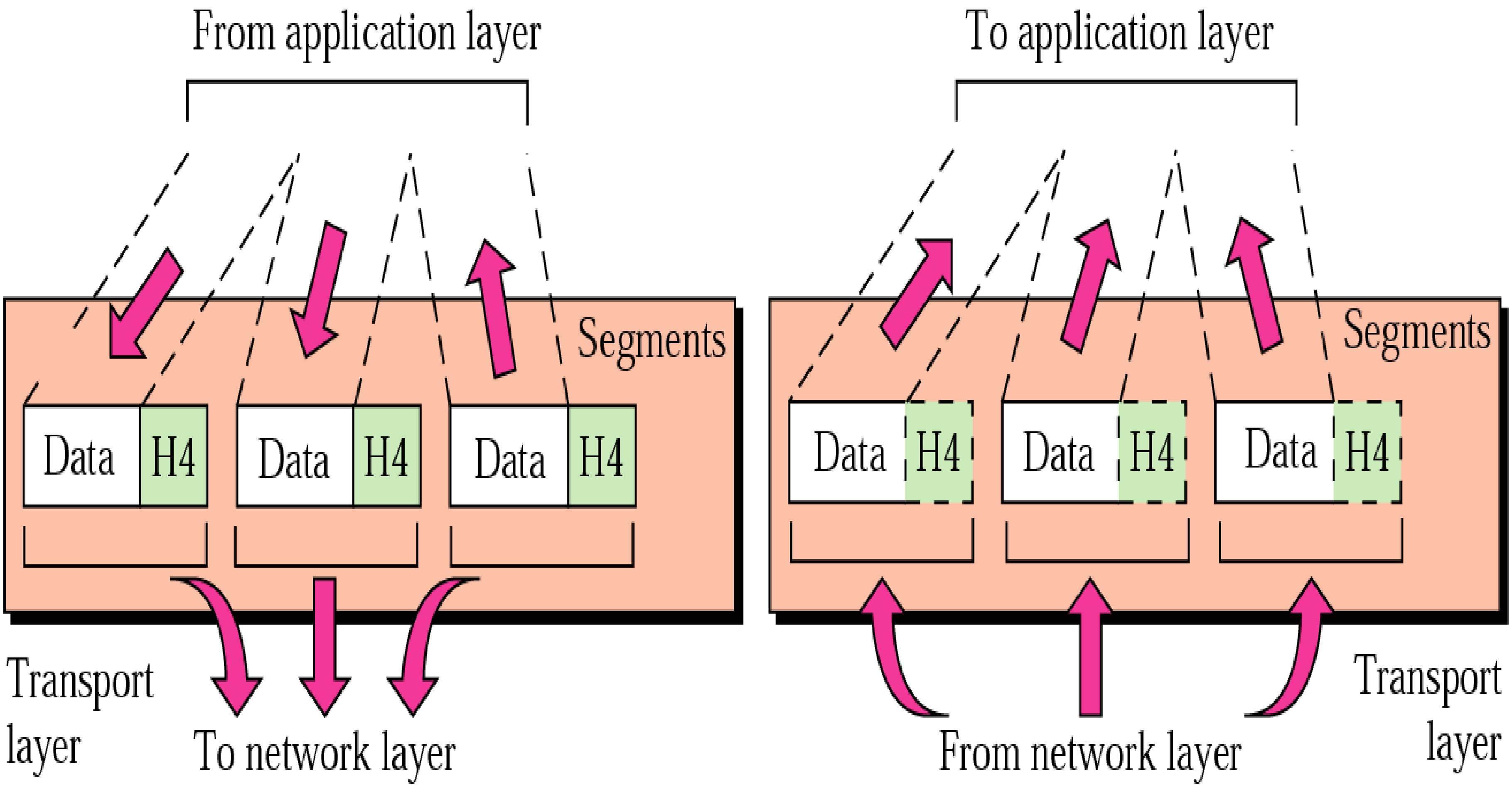


***The network layer is responsible for the delivery of packets from the original source to the final destination.***

# 4. Transport Layer

- The transport layer is responsible for **process-to-process or end-end** delivery of the entire message.
- The network layer oversees host-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
- The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the process-to-process level.

# *Transport layer*



***The transport layer is responsible for delivery of a message from one process to another.***

# Functions of the Transport layer

**Service point addressing:**

Computer often run several processes (running programs) at the same time. Process-to-process delivery means delivery from a specific process on one computer to a specific process on the other.

- The transport layer header include a type of address called **port address**.
- The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

# Cont..

,

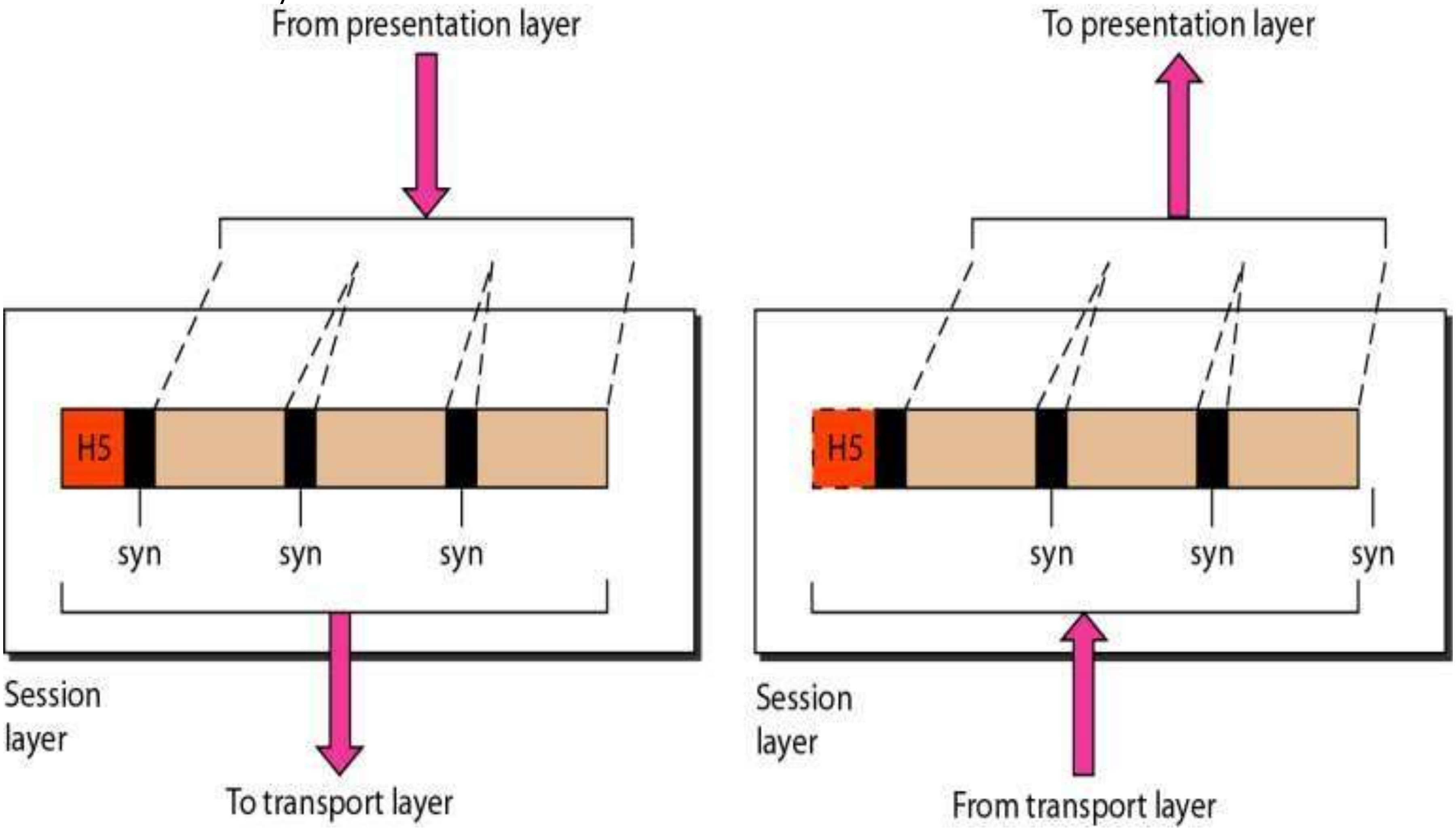
- **Segmentation and reassembly**: a message is **divided into transmittable segments**, each having a **sequence number**. These numbers enable the transport layer to reassemble the message correctly upon arrival at the destination.
- **Connection control**: The transport layer can be either connectionless 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.

# Functions of the transport layer

- **Flow control**: the transport layer performs a flow control end to end. The data link layer performs flow control across a single link.
- **Error control**: the transport layer performs error control end to end. The data link layer performs control across a single link.
- **Congestion control** concerns controlling traffic entry into a telecommunication networks so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. It should not be confused with flow control, which prevents the sender from overwhelming the receiver.

# 5. Session Layer

- The session layer is responsible for dialog control and synchronization.

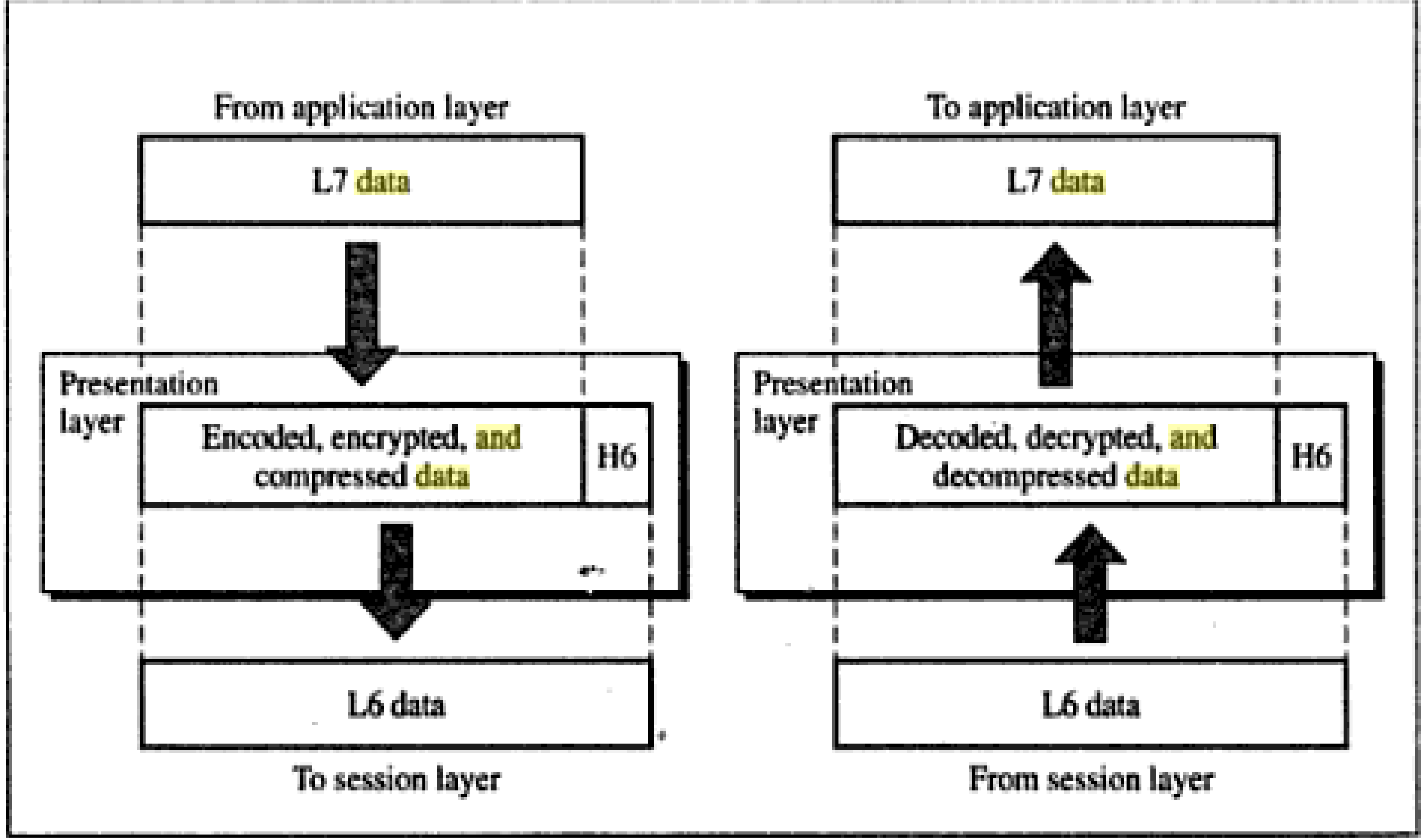


# Functions of Session Layer

- **Decision Control**:- Half duplex, Full Duplex
- **Synchronization**: Adding checkpoints to stream data.
- Ex: System sending 2000 pages.
- Add check point after each 100th page.
- So in case of failure no need to sent whole page.

# 6. Presentation Layer

- It is concerned with the syntax and semantics of the information exchanged b/w 2 devices.

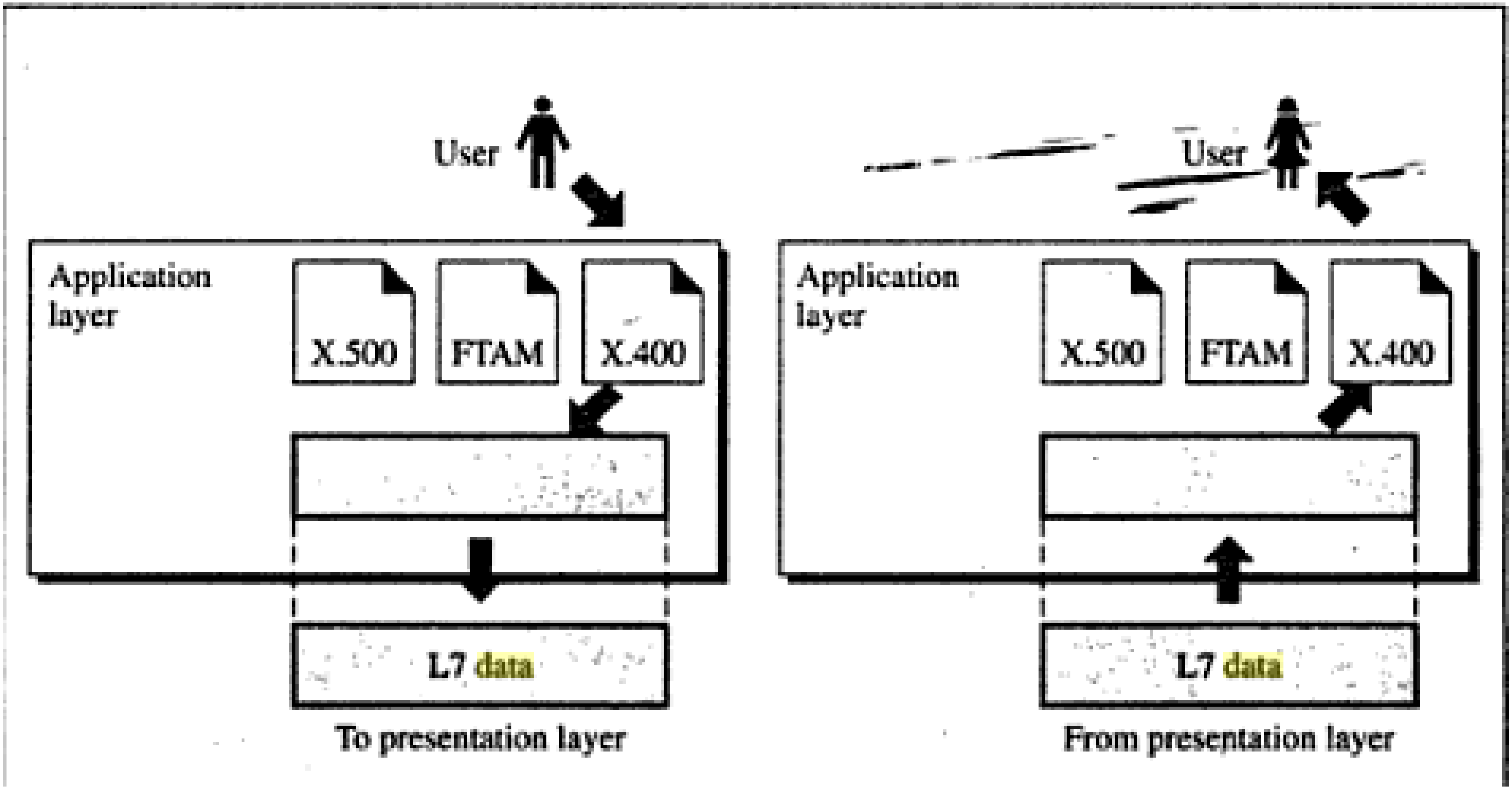


# Functions of Presentation Layer

- **Translation:** Interoperability b/w different encoding formats.
- **Encryption:** Converting plain to cipher text and vice versa.
- **Compression:** Reducing number of bits in multimedia data when transmitting.

# *7. Application layer*

The application layer is responsible for providing services to the user.



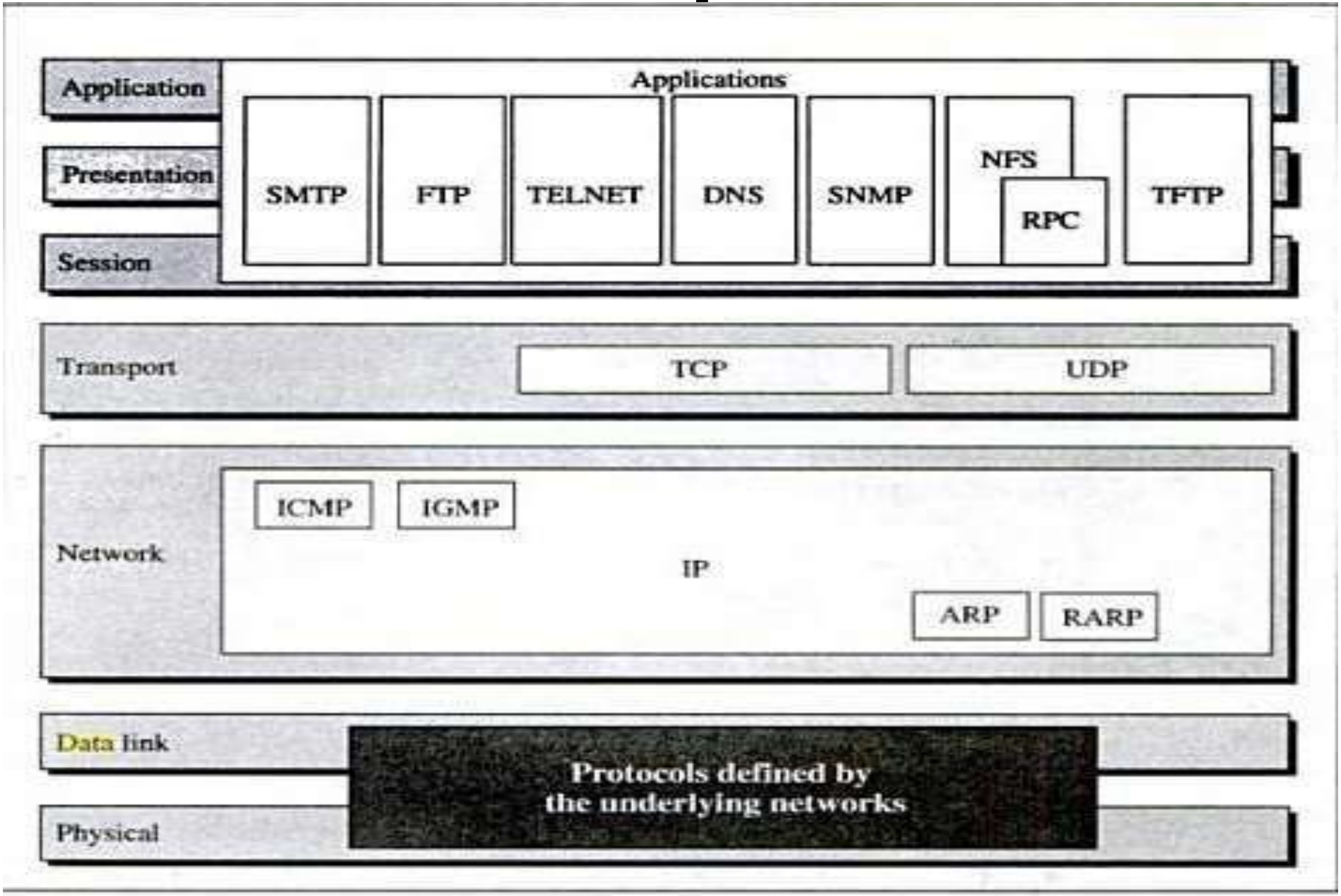
# Functions of Application Layer

- It provides user access to network.
- X.500-Directory service.
- X.400-Message handling service.
- **FTAM-** File Transfer Access and management.
- Network Virtual Terminal.

# TCP/IP Protocol

- Transmission Control Protocol / Internetworking Protocol is used in the internet and is developed **prior to the OSI** model.
- It would not match exactly with OSI model
- It is divided into layers.

# TCP/IP protocol



- It contains relatively independent protocols that can mixed and matched with depend on  needs of the system.

# LAN Topology

- It defines the Physical (or) Logical arrangement of Links in a Network.
- Topology refers to the layout of connected devices in a network.
- The Topology of the Network is Geometric Representation of the relationship between all Communication links.

# Types of Topology

i) Mesh Topology

ii) Star Topology

iii) Tree Topology

iv) Bus Topology

v) Ring Topology

vi) Hybrid Topology

# Types of Topology

## i) Mesh Topology

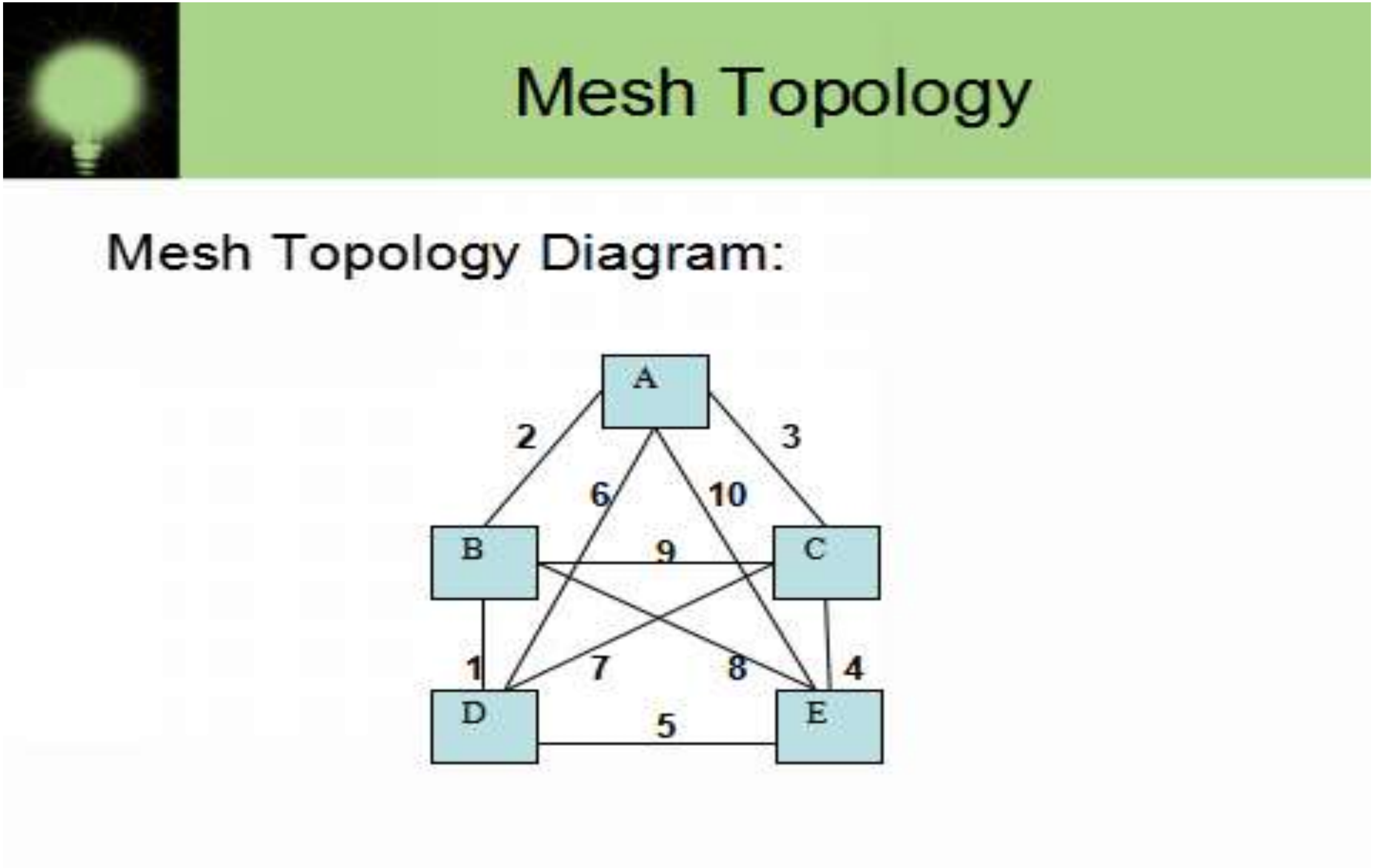
- Here every device has a direct point to point link between every other device.
- A fully connected mesh can have n(n-1)/2 physical channels to link n devices.

if n=5 (Number of Nodes)

5(5-1)/2 = 10 ( Communication Links)

- 5 Nodes are Connected by using 10 Communication Links

# Mesh Topology



Mesh Topology

Mesh Topology Diagram:

# Mesh Topology

**Advantages:**

- It eliminate the traffic problem.
- It is robustness.
- It has privacy and security.
- Fault can be easily found.

# Mesh Topology

**Disadvantages:**

- More number of cables to be  used.
- Every devices must be connected to some other devices. So installation process is very difficult.

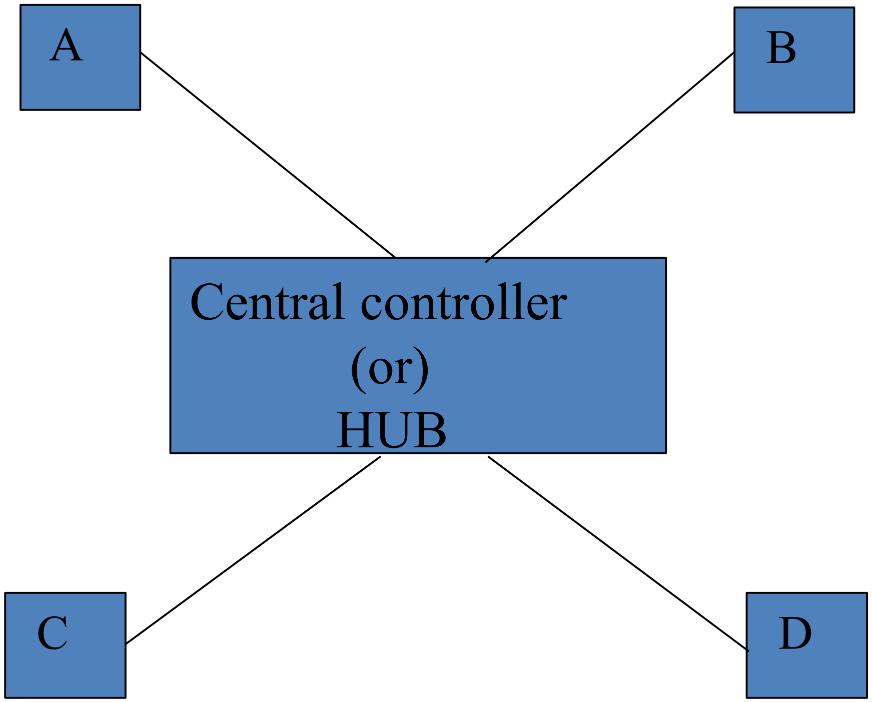
# Types of Topology

## ii)Star Topology:

- Each device has a dedicated point-to-point link between only a central controller or “HUB”.
- The devices are not directly linked to some other devices.
- If one device wants to send data to another device, it sends to the central controller and the Central controller send to other device.

# Star Topology

## Star Topology Diagram:



# Star Topology

**Advantages :**

- Less expensive than Mess topology.
- Less number of cables to be used.
- It is robustness.

# Star Topology

**Disadvantages:**

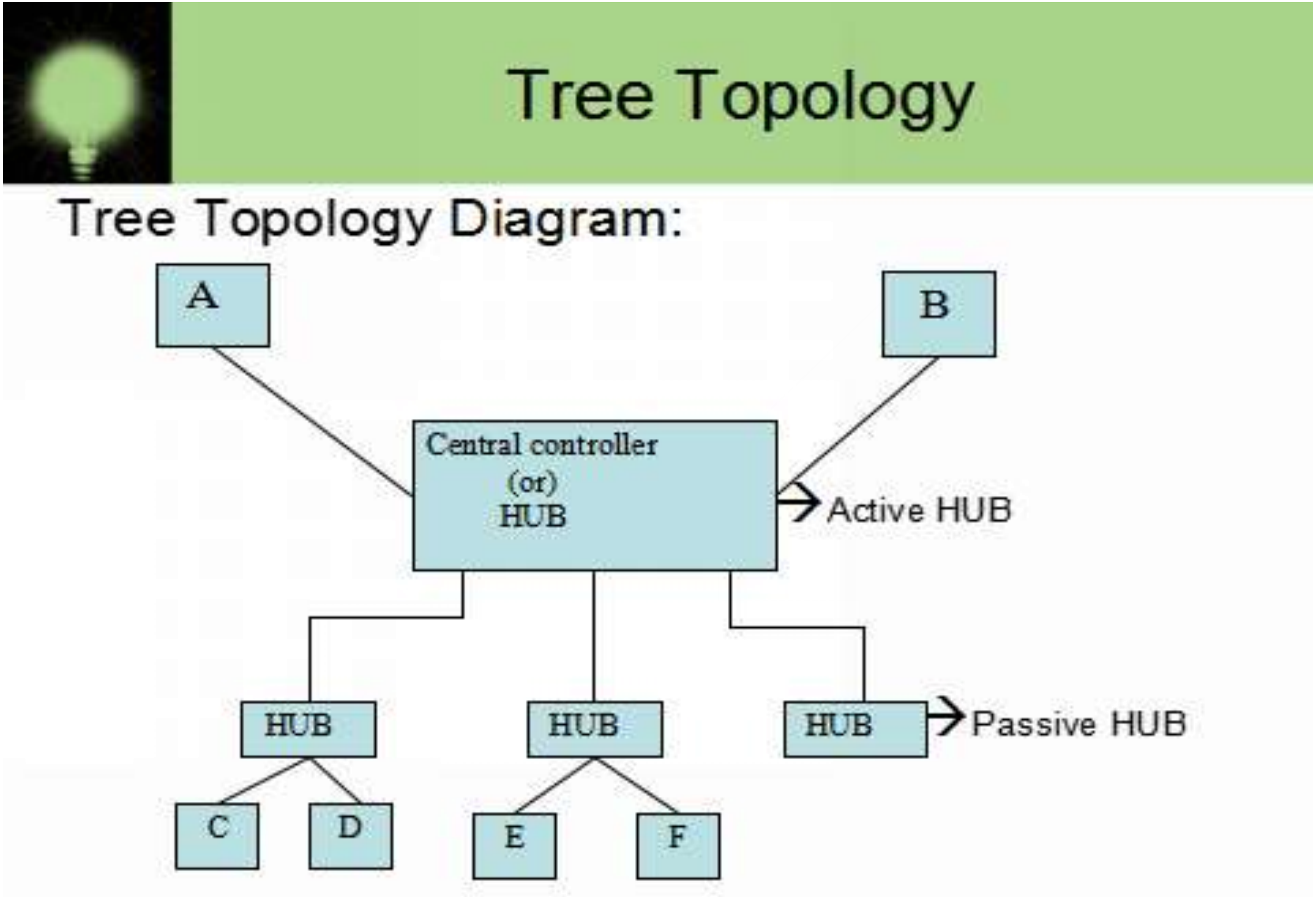
- Each device must connected to central controller.
- It require  more installation process.
- If central controller failure means all the devices should be failed.

# Types of Topology

## iii)Tree Topology:

- Tree topology has some variation from star topology.
- The nodes in the tree are linked to the central controller.
- The primary HUB in the tree is represented by “Active Hub”.
- The secondary HUB in the tree is represented by “Passive Hub”.

# Tree Topology



## Tree Topology

Tree Topology Diagram:

A

B

Central controller
(or)
HUB

Active HUB

HUB

HUB

HUB

Passive HUB

C

D

E

F

# Tree Topology

**Advantages:**

- It allows more devices to be attached in a single central controller.
- It allows the network to prioritize the communication.

# Tree Topology

**Disadvantages:**

- Each device must be linked to central controller.
- It require more installation processes.
- If central controller failure means entire system should fail down.

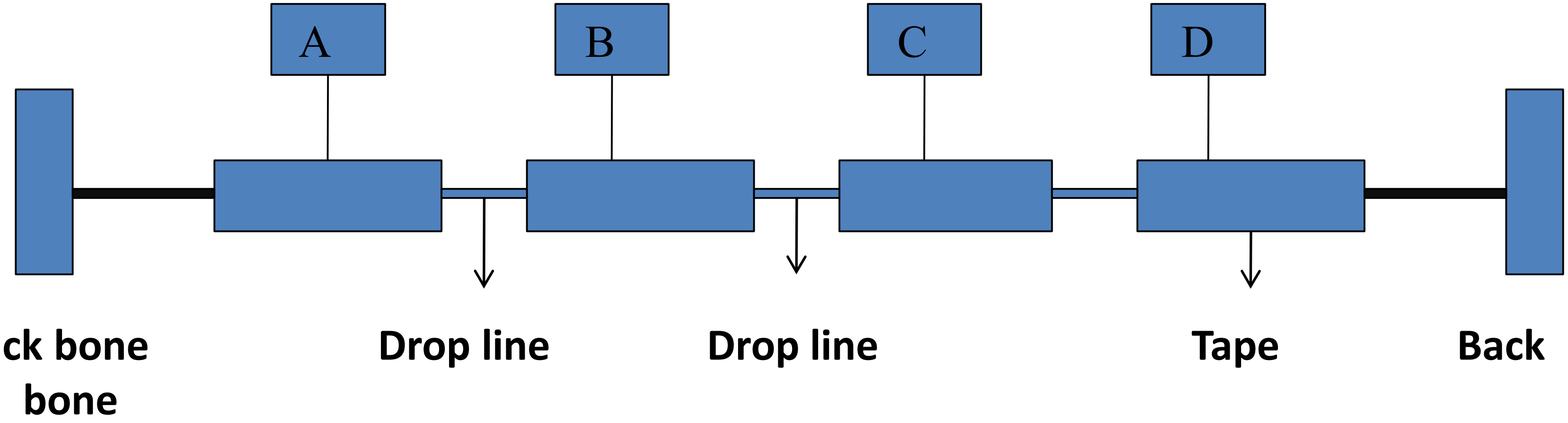
# Types of Topology

## iv)Bus Topology:

- A Bus topology describes the multipoint configuration.
- One long cable act as a backbone to link all the devices in a network.
- Devices are connected in a bus topology with the help of “Drop lines” and “Tapes”.

# Bus Topology

## Bus Topology Diagram:



# Bus Topology

**Advantages:**

- Installation process is very easy.
- Redundancy can be eliminated.
- Less number of cables to be used.

# Bus Topology

**Disadvantages:**

- Reconfiguration is very difficult.
- Very difficult to adding (or) deleting of a devices

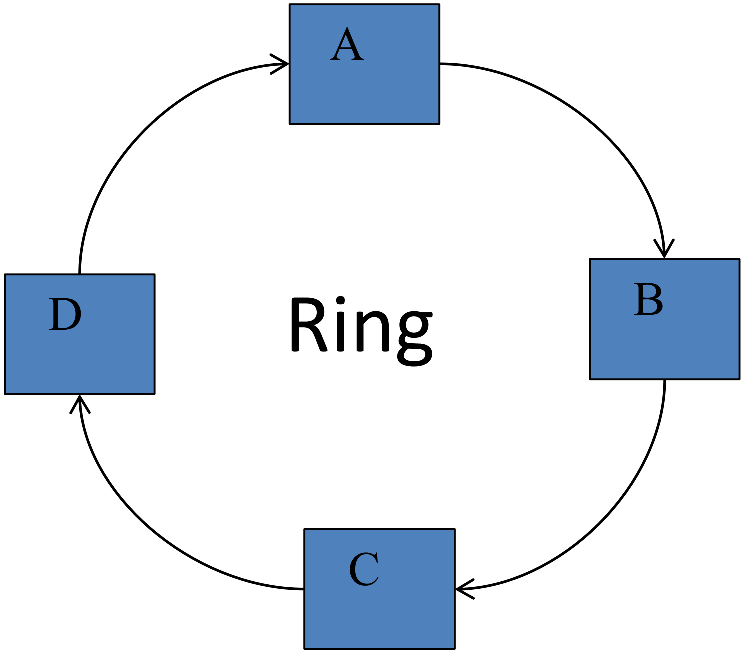
# Types of Topology

**v) Ring Topology:**

- In Ring Topology each device has dedicated point-to-point link between other devices.
- The signals are passed along the “ring” in only one direction from device to device.
- Each devices in a ring should have a “Repeater”.

# Ring Topology

**Ring Topology Diagram:**



# Ring Topology

**Advantages:**

- Easy to install and reconfigure.
- Fault can be easily identified.

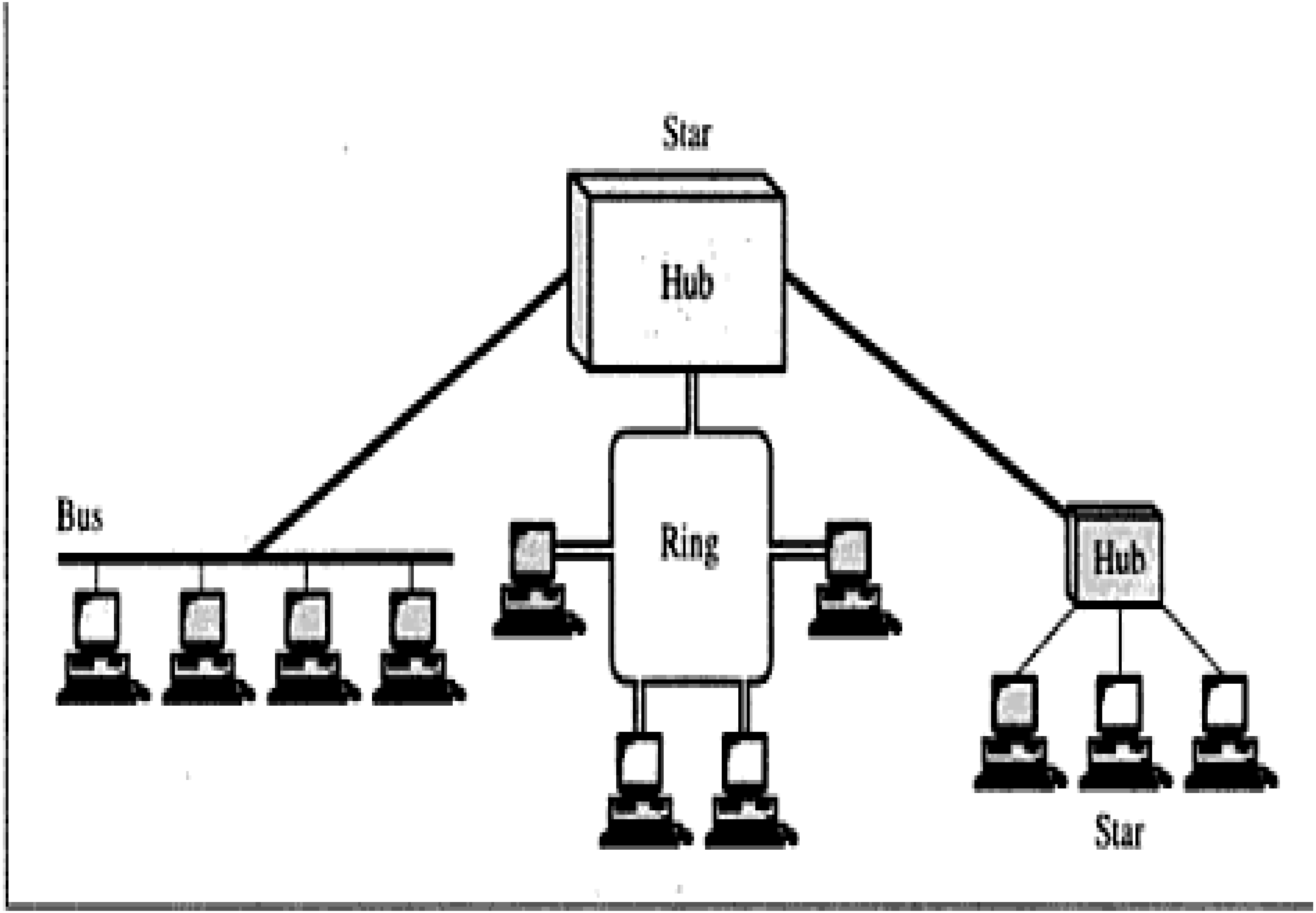
# Ring Topology

**Disadvantages:**

- It is unidirectional traffic.
- In rings if one device gets failure then the entire system should be failed.

## VI. Hybrid Topology

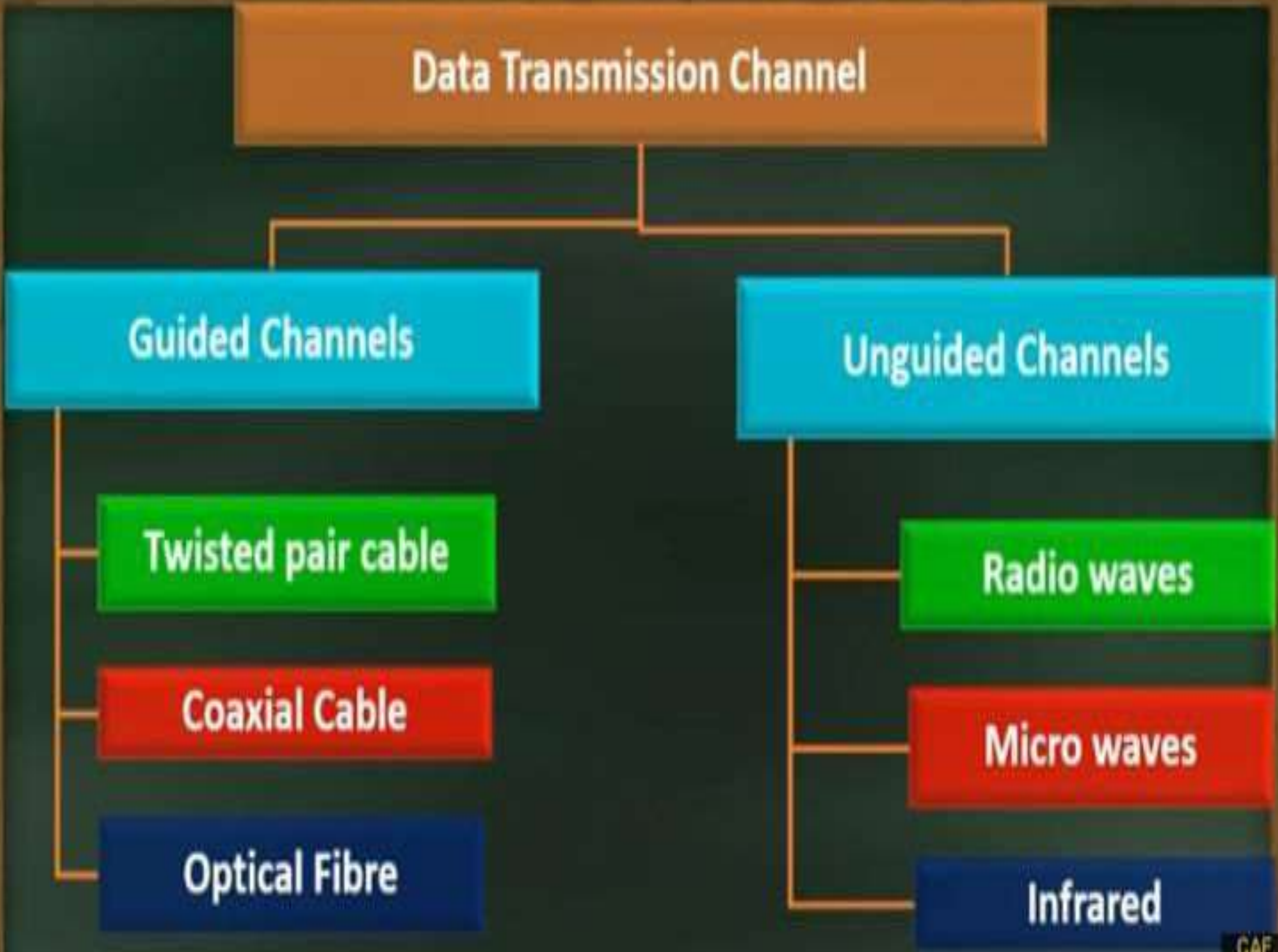
- Combination of all topology is called hybrid topology.


Star
Hub
Bus
Ring
Hub
Star

# Transmission Media

The physical path between transmitter and receiver.

- **Repeaters or amplifiers** may be used to extend the length of the medium.
- Communication of electromagnetic waves is *guided* or *unguided.*



Data Transmission Channel

Guided Channels

- Twisted pair cable
- Coaxial Cable
- Optical Fibre

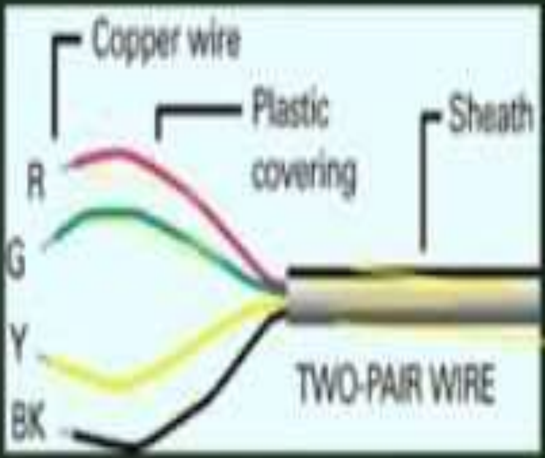
Unguided Channels

- Radio waves
- Micro waves
- Infrared

# Guided Media

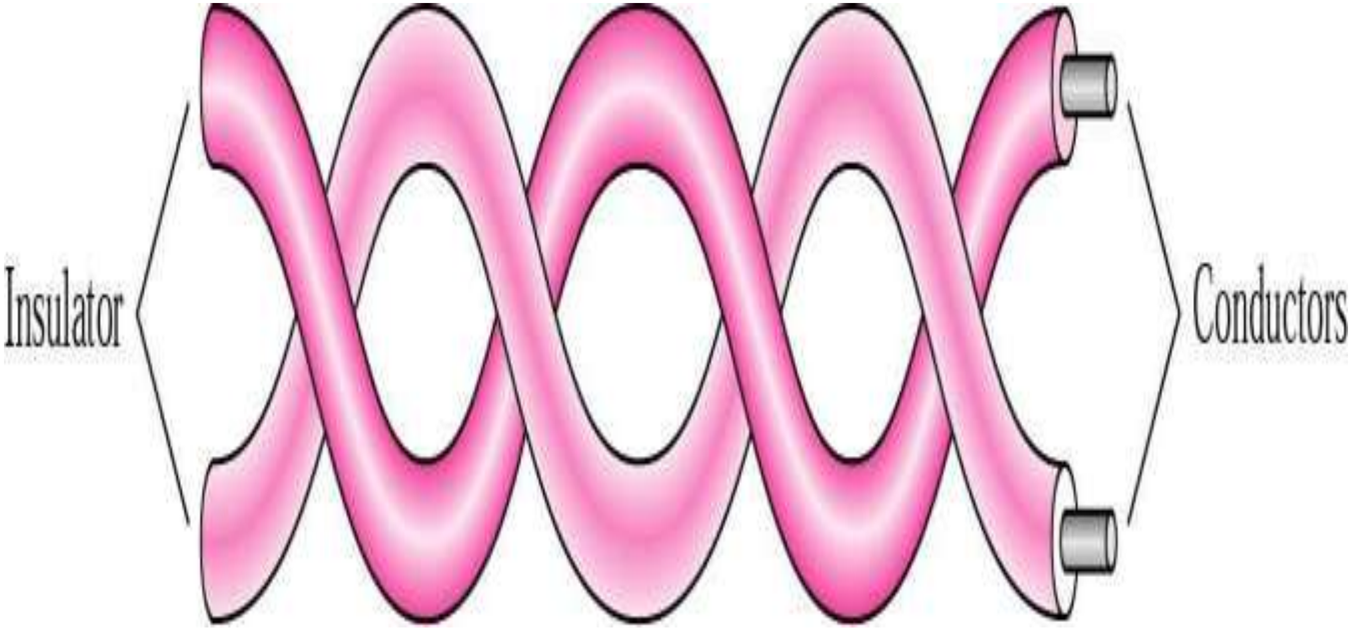
- Guided media provide a physical connection using wire or cable between two devices.
- A signal traveling through guided media is directed and contained within the physical limits of the medium

# Twisted pair cable

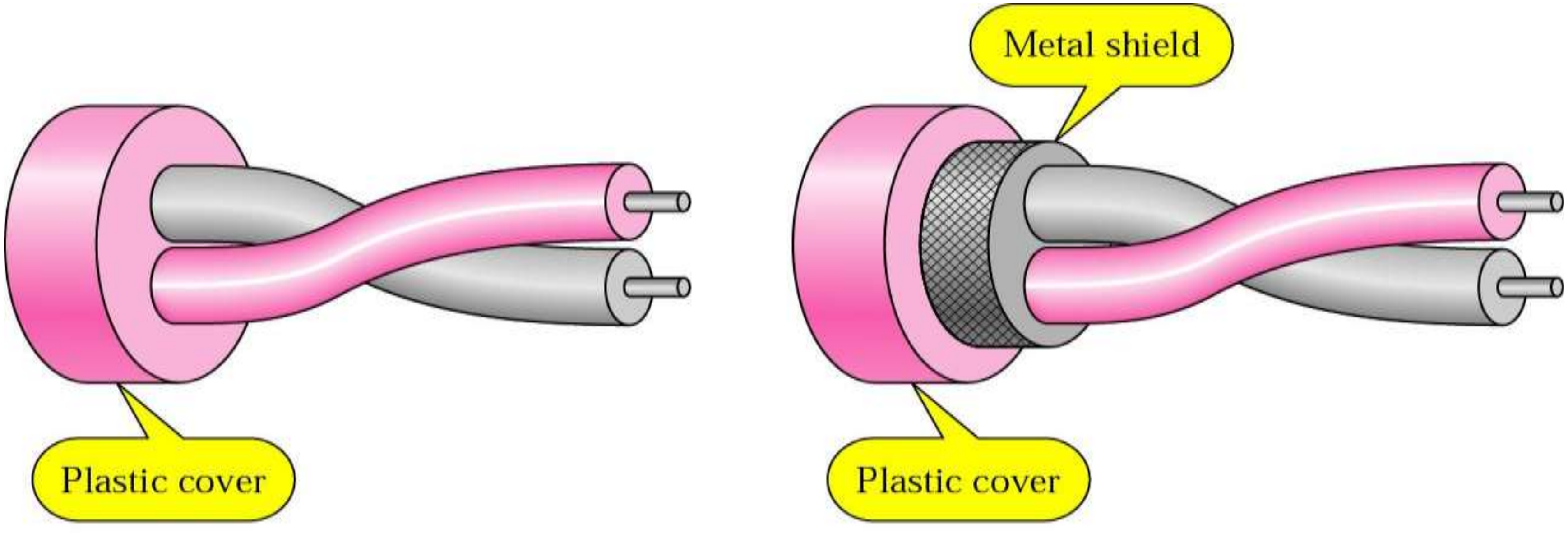


- This cable is the most commonly used and is cheaper than others.
- It is lightweight, cheap, can be installed easily, and they support many different types of network.
- A twisted pair cable consists of two conductors which are normally made of copper.
- Each conductor has its own plastic insulation typically 1 mm thick.
- These cables are twisted together.

# Twisted-pair cable

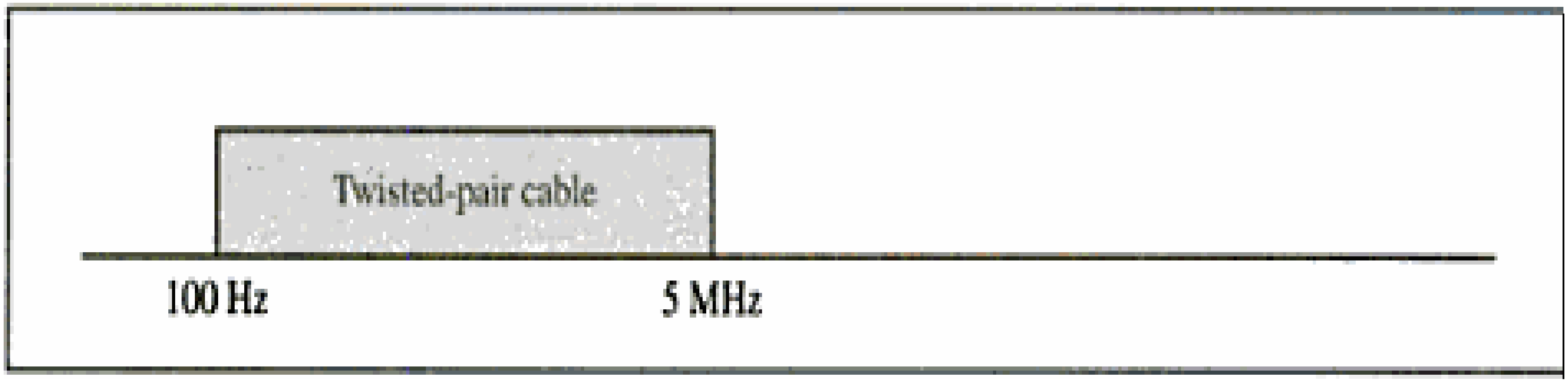


# *UTP and STP*



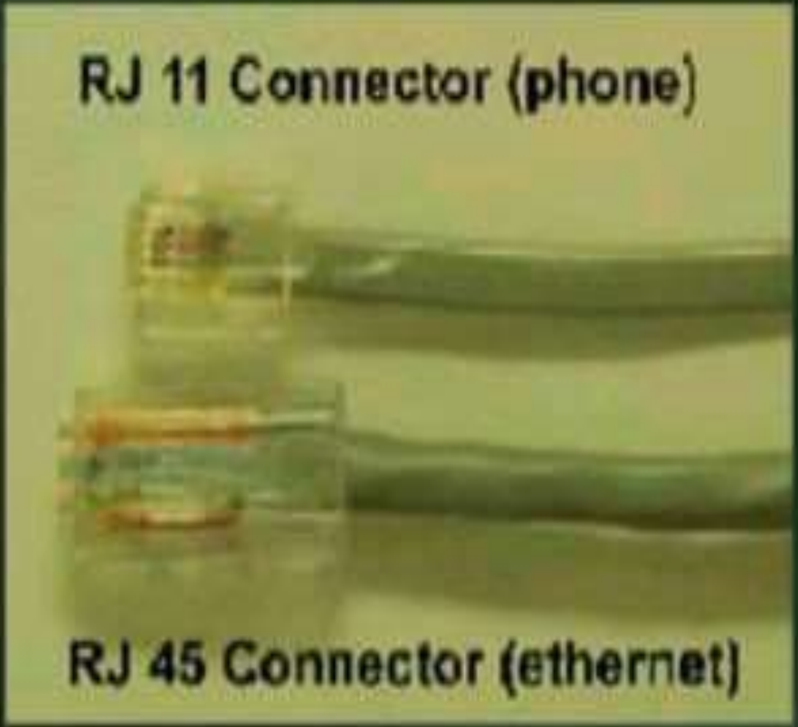
a. UTP

b. STP



## Unshielded Twisted Pair Cable

- It is the most common type of telecommunication which consists of two conductors usually copper, each with its own colour plastic insulator.



- Identification is the reason behind coloured plastic insulation.
- UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector and 4 pair cable use RJ-45 connector.

## Advantages :

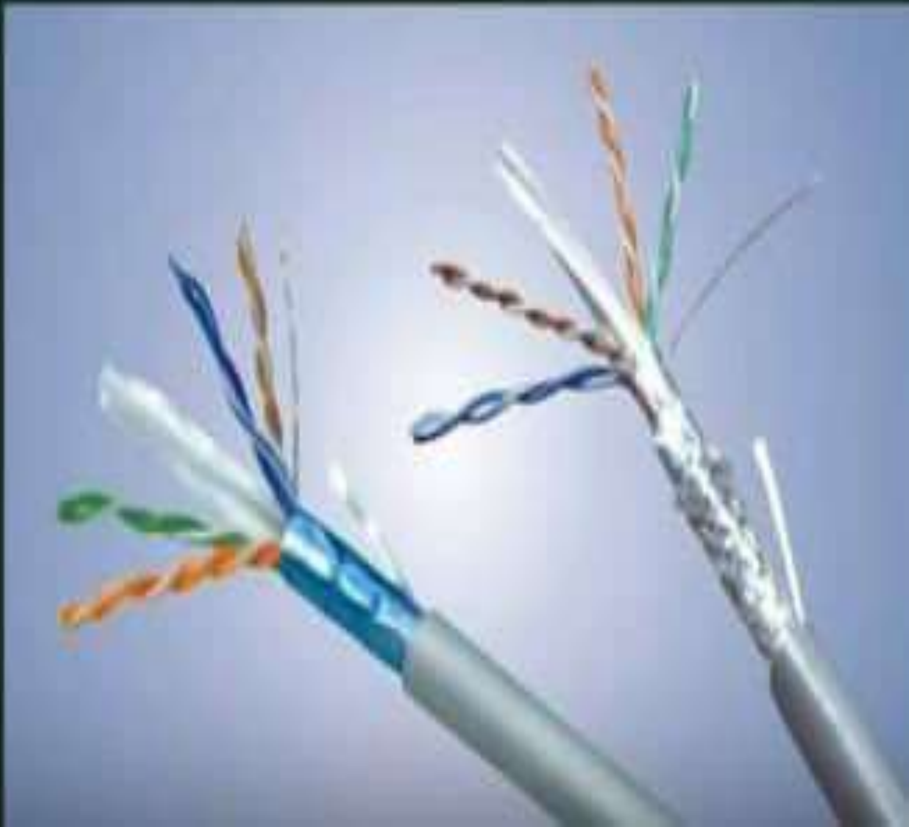
- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet

## Disadvantages :

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

## Shielded Twisted Pair Cable

- This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors.



- Electromagnetic noise penetration is prevented by metal casing.
- Shielding also eliminates crosstalk
- It is faster the unshielded and coaxial cable.
- It is more expensive than coaxial and unshielded twisted pair.

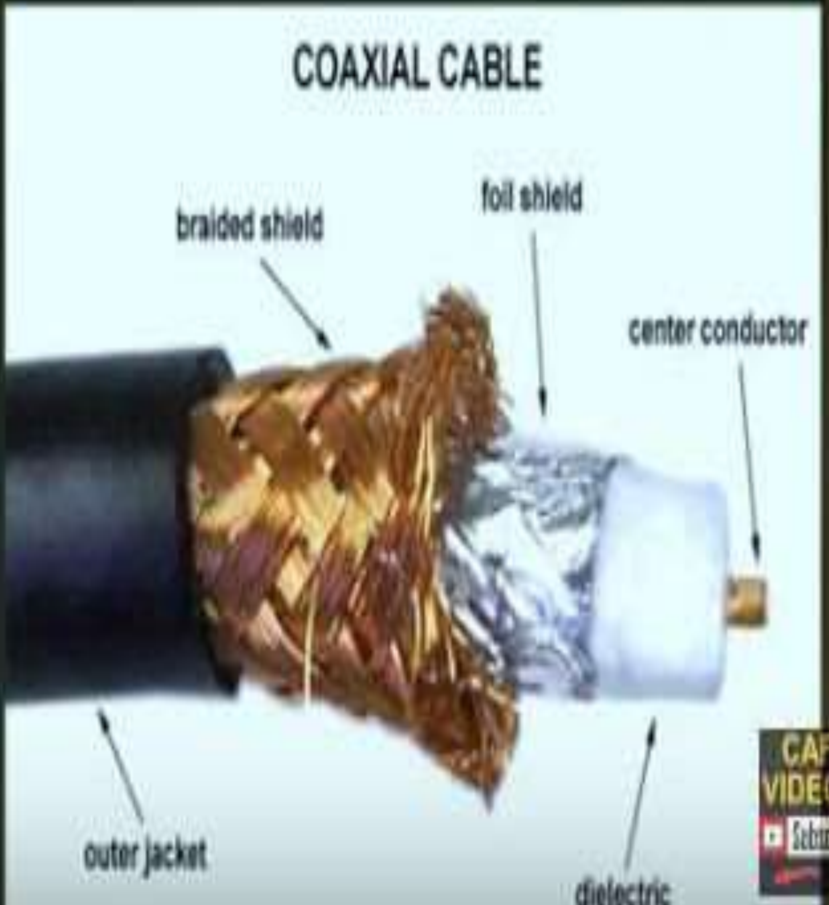
Advantages :

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission
- Increases the signalling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

## Disadvantages :

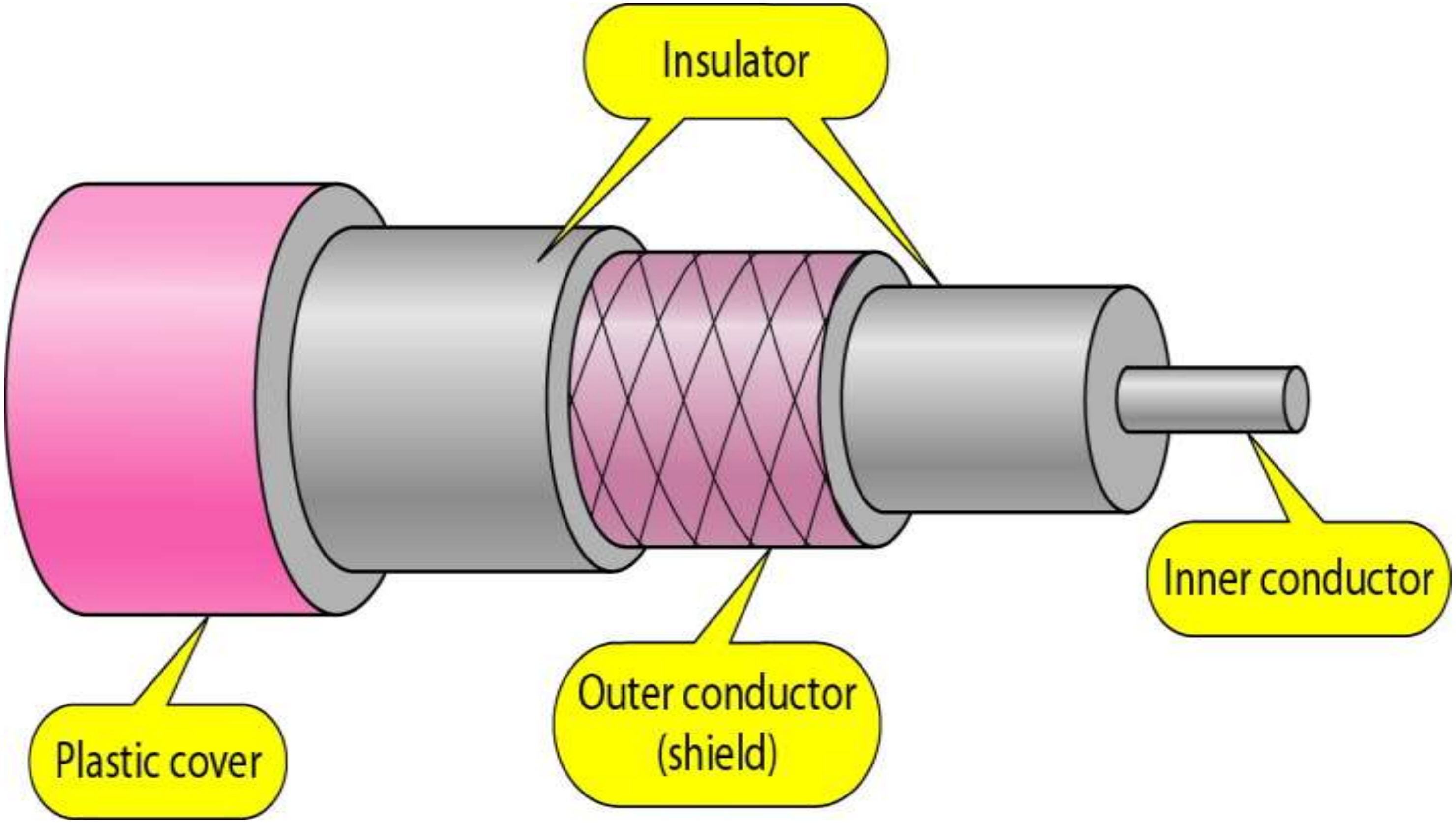
- Difficult to manufacture
- Heavy

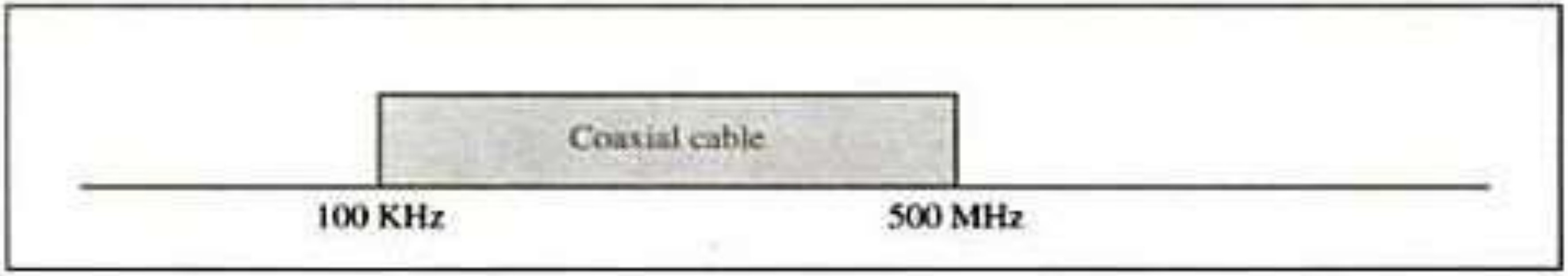
## Coaxial Cable



- Copper is used in this as centre conductor which can be a solid wire or a standard one.
- It is surrounded by PVC installation, a sheath which is encased in an

# Coaxial Cable



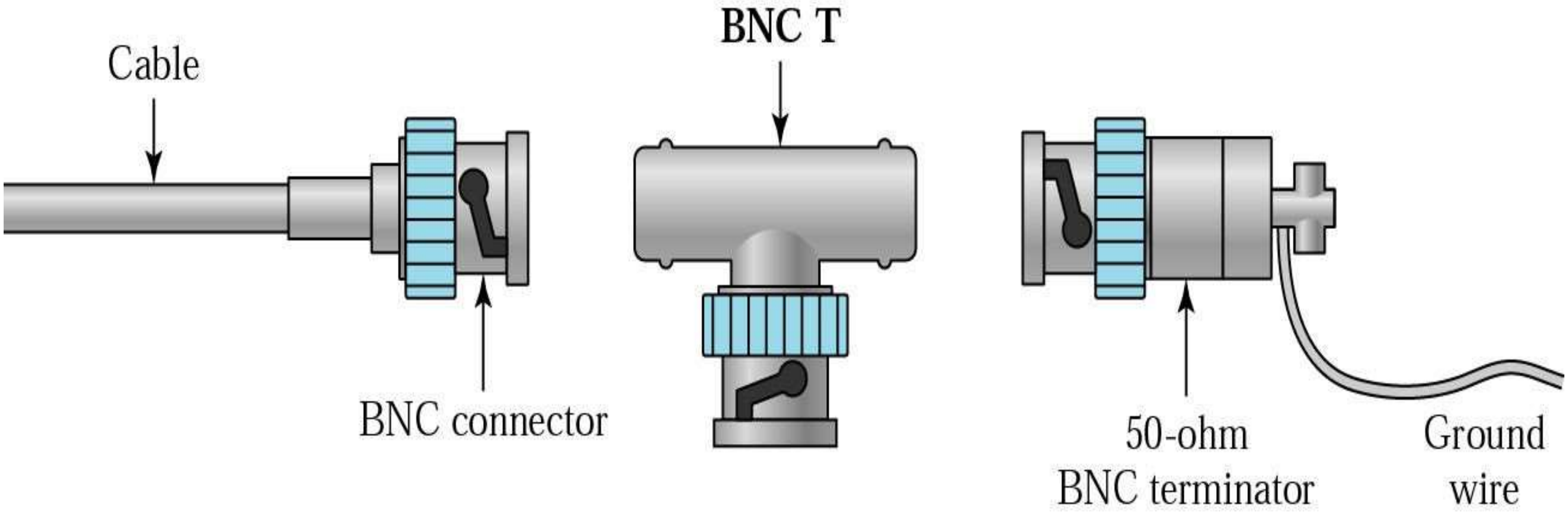


# BNC connectors

- To connect coaxial cable to devices, it is necessary to use coaxial connectors. The most common type of connector is the Bayone-Neill-Concelman, or BNC, connectors.

**There are three types: the BNC connector, the BNC T connector, the BNC terminator.**

Applications include cable TV networks, and some traditional Ethernet LANs like 10Base-2, or 10-Base5.



outer conductor of metal foil, braid or both.

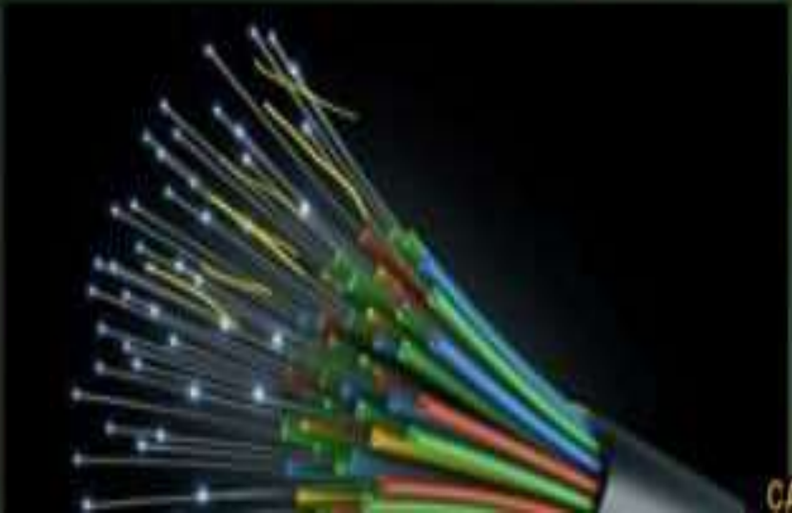
- Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit.
- The outer conductor is also encased in an insulating sheath.
- The outermost part is the plastic cover which protects the whole cable.

Advantages :

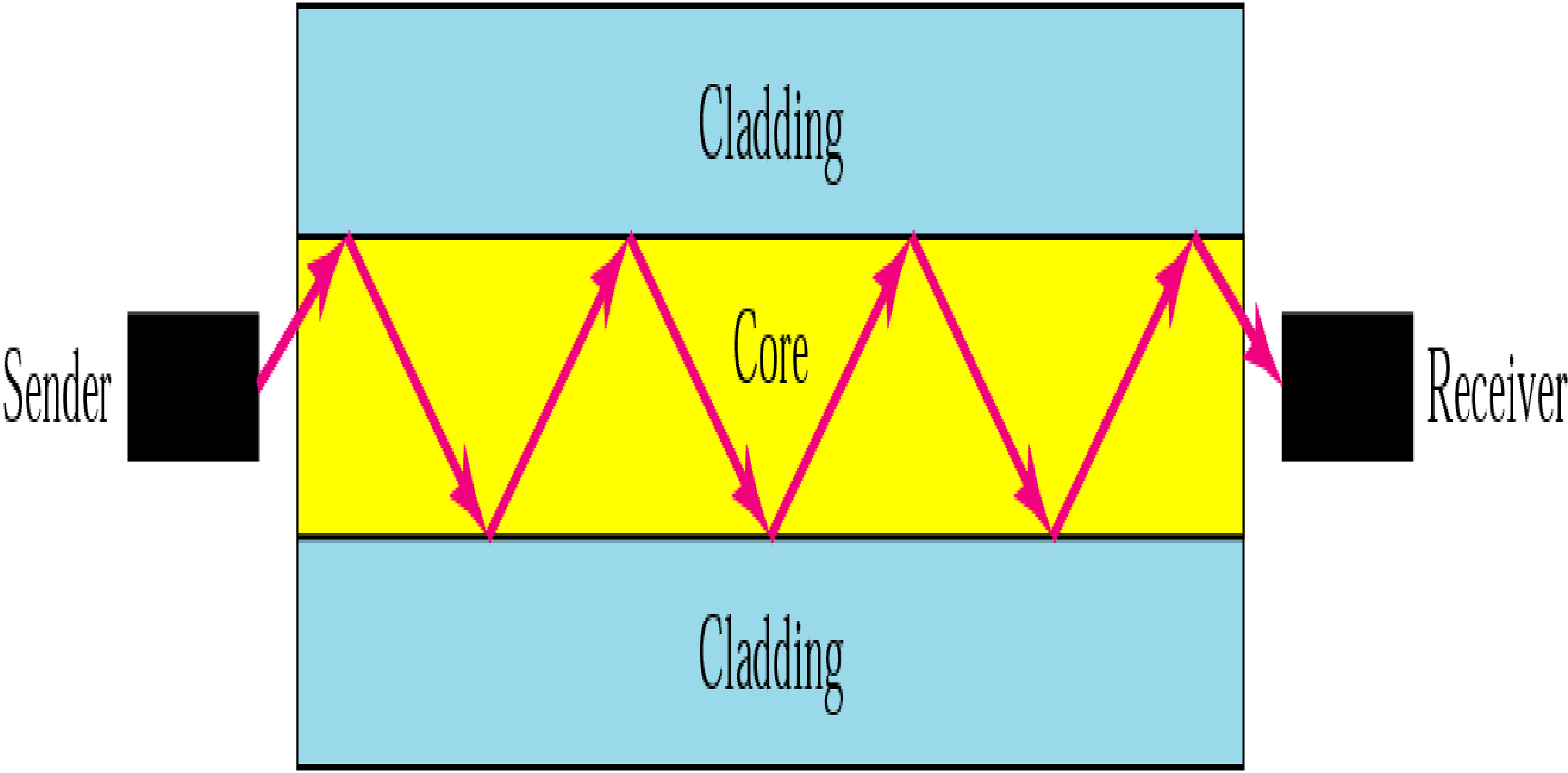
- Bandwidth is high
- Used in long distance telephone lines.
- Transmits digital signals at a very high rate of 10Mbps.
- Much higher noise immunity

# Optical Fibre

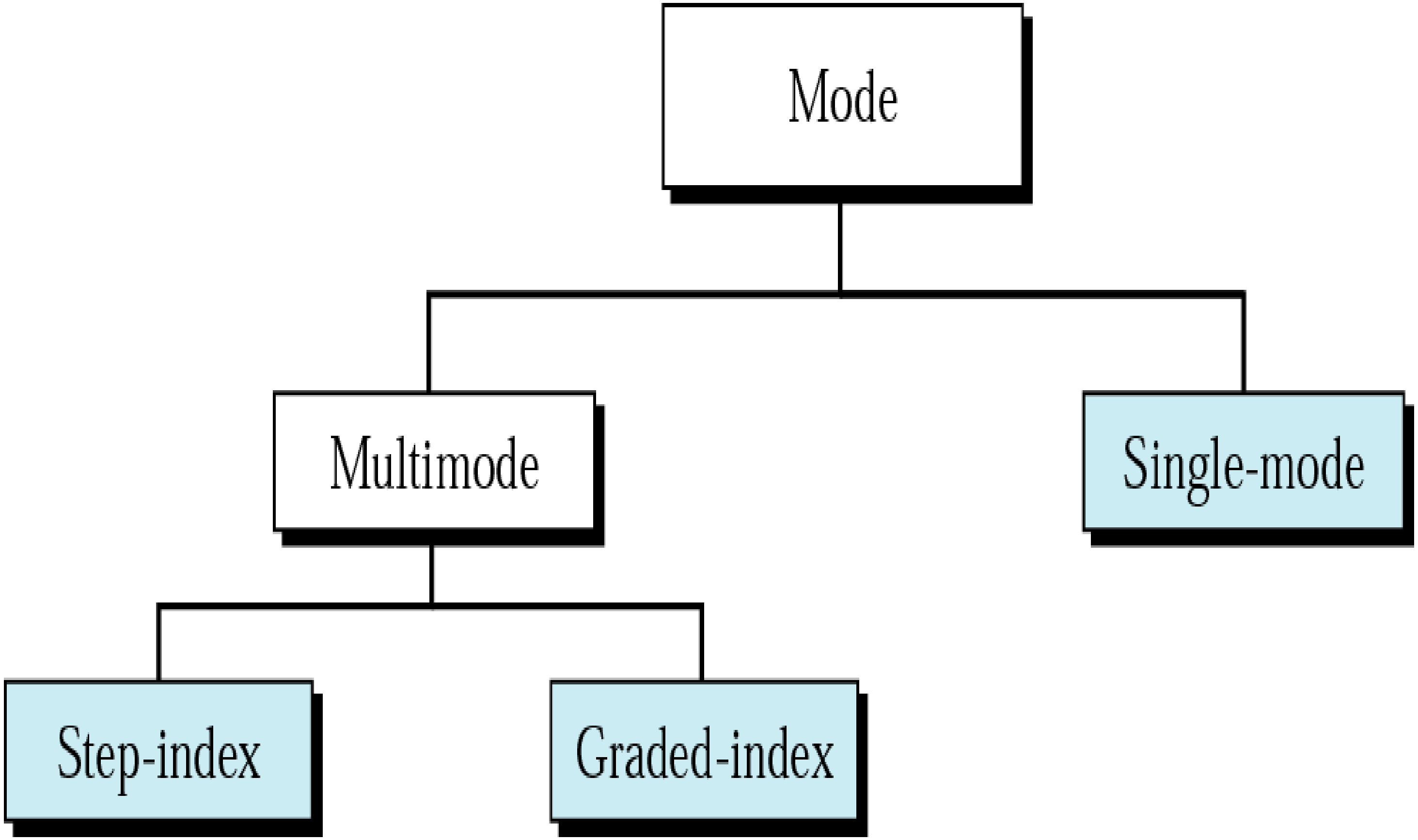
- A technology that uses glass (or plastic) threads (fibres) to transmit data.
- A fibre optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.
- Fibre optic cable has bandwidth more than 2 gbps (Gigabytes per Second)



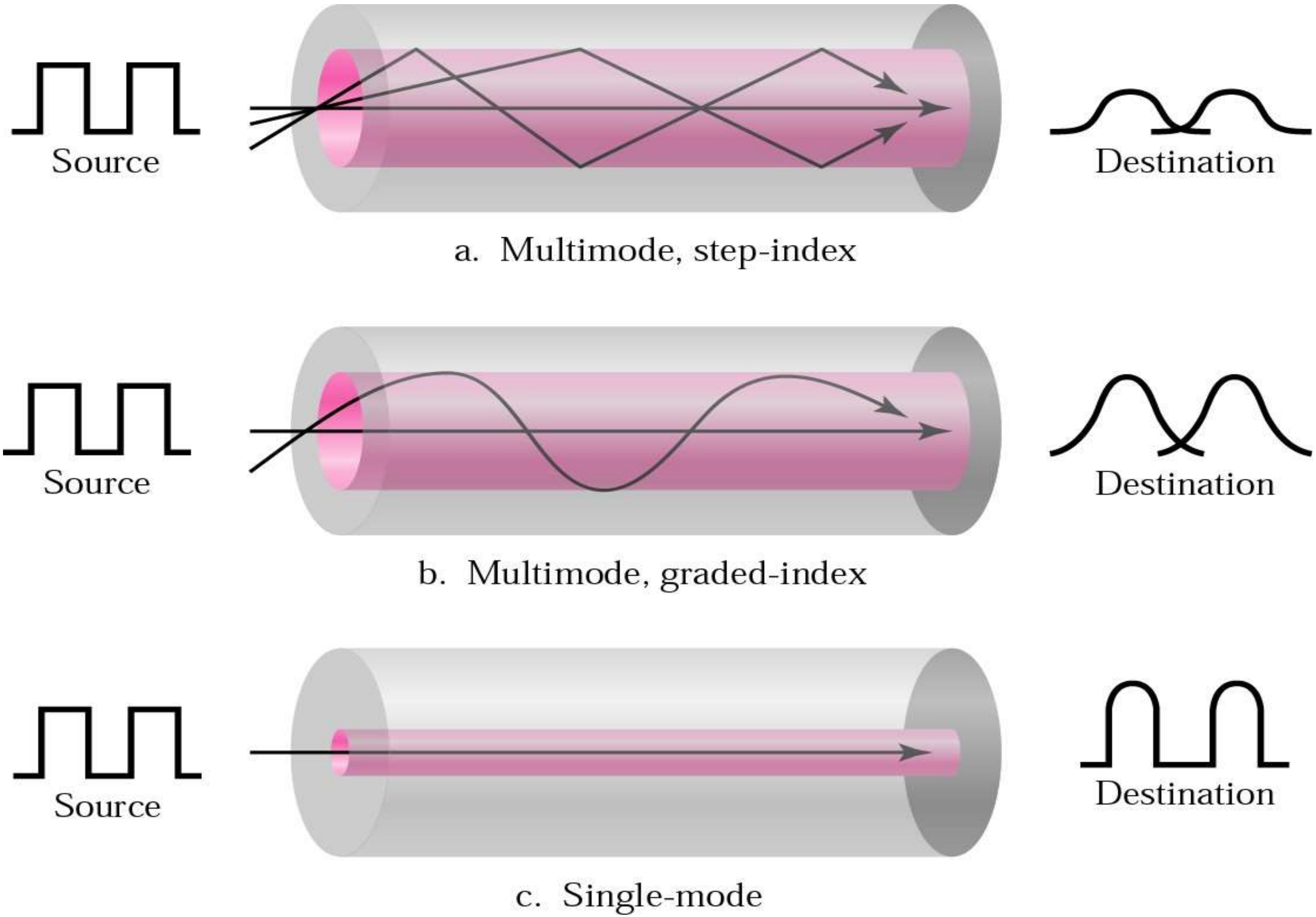
# Optical fibers



# Propagation Modes (Types of Optical Fiber )



# *Propagation Modes*



a. Multimode, step-index

b. Multimode, graded-index

c. Single-mode

## Advantages

- Provides high quality transmission of signals at very high speed.
- Used for both analog and digital signals.
- These cables are much lighter than the copper cables
- Its transmission distance is greater than the twisted pair and it can run for 50Kms without regeneration.
- These are not affected by electromagnetic interference, so noise and distortion is very less.

## Disadvantages

- It needs expertise which is not available everywhere. So it is difficult to install.
- Propagation of light is unidirectional and we need two fibers for bidirectional communication.
- It is expensive because the cables and interfaces used are relatively expensive.

# Unguided Media

- Unguided media is used for transmitting the signal without any physical media.
- It transports electromagnetic waves and is often called wireless communication.
- Signals are broadcast through air and received by all who have devices to receive them.

# Radio waves

- Radio frequency (RF) waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
- Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.

- Radio waves can be received both inside and outside the building.
- Radio waves are very useful in multicasting and hence used in AM and FM radios, cordless phones and paging.
- If the communication is between single source and destination then it is called unicast;
- on the other hand, if one source is transmitting signal and any destination that is in the range may be able to reach it then it is called broadcast.

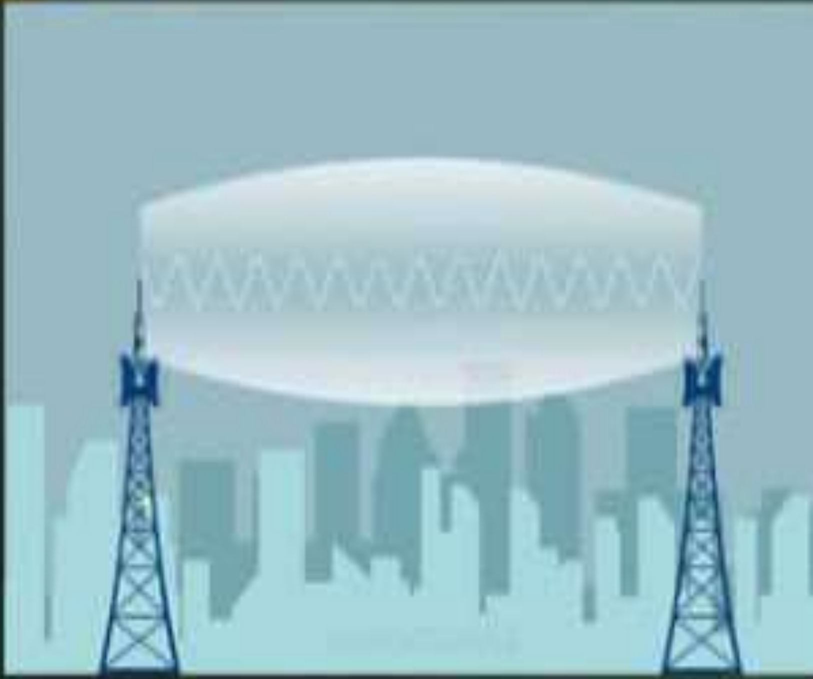
- Multicast is when a source transmits a signal for some specific group of destinations which may be more than one.

## Bluetooth

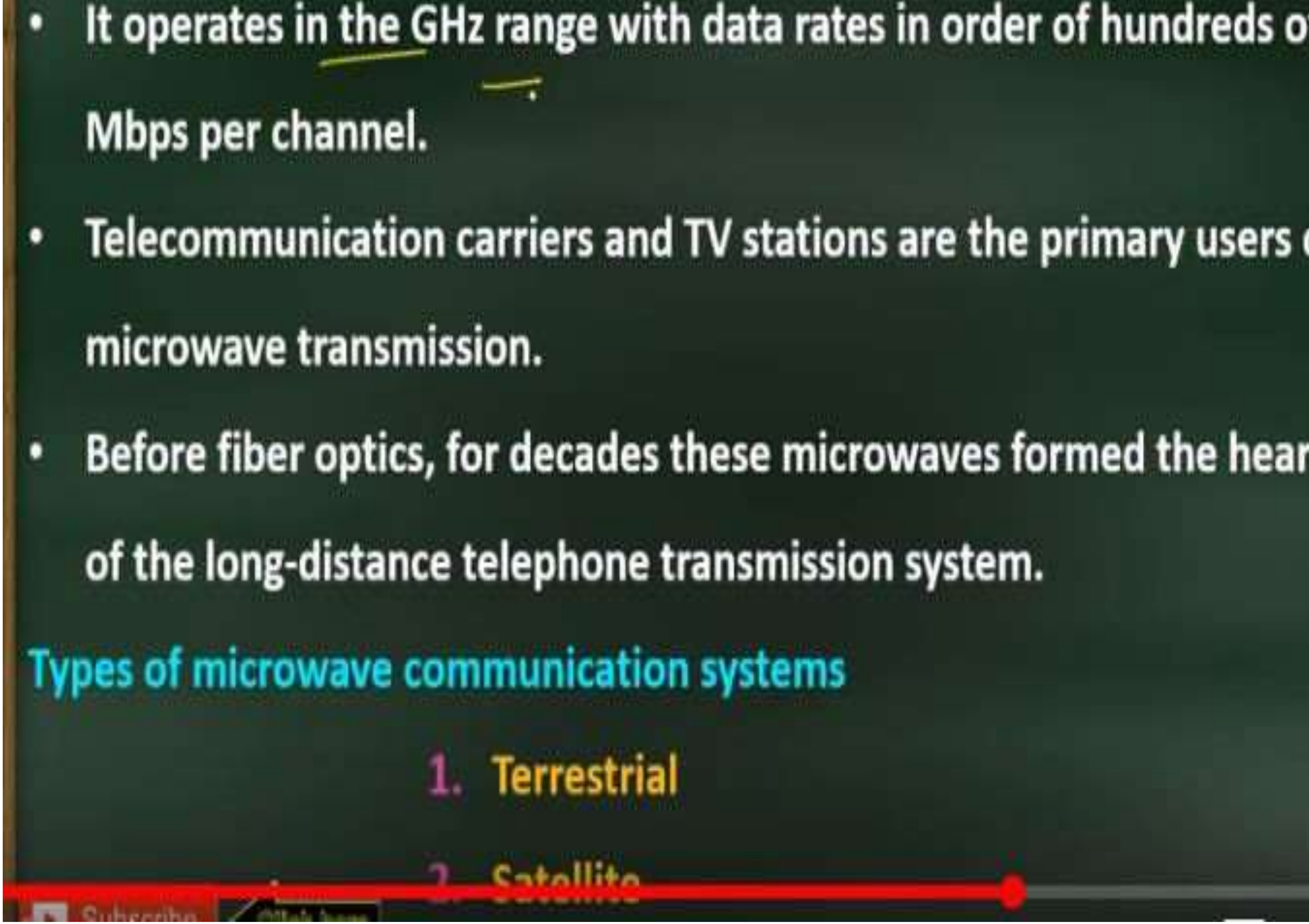
- Bluetooth is a very popular application of short wave length radio transmission in the frequency band of 2400 to 2480 MHz.
- It is a proprietary wireless technology standard used for exchanging data over short distances in mobile phones and other related devices.

- It allows wireless devices to be connected to wireless host which may be a computer over short distances. You may have it for transferring data between a mobile phone and a computer provided both have Bluetooth technology.

# Microwave Transmission



- Travels in straight lines and therefore narrowly focused concentrating all the energy into a beam.
- Periodic repeaters are necessary for long distances.
- For transmitting and receiving, antennas should be aligned accurately.
- Can not penetrate through buildings.

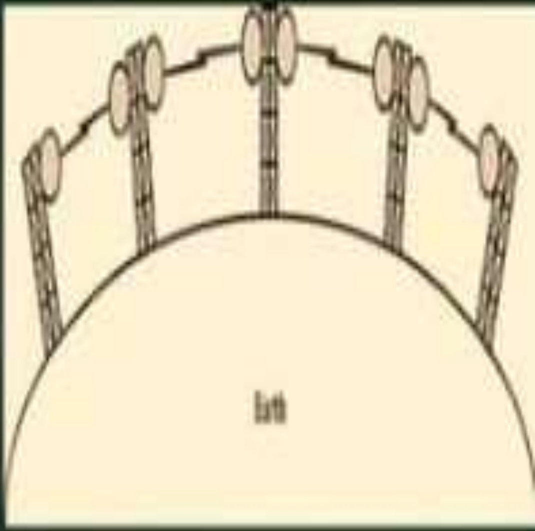


- It operates in the GHz range with data rates in order of hundreds o
  Mbps per channel.
- Telecommunication carriers and TV stations are the primary users
  microwave transmission.
- Before fiber optics, for decades these microwaves formed the hear
  of the long-distance telephone transmission system.

Types of microwave communication systems

1. Terrestrial
2. Satellite

## Terrestrial Microwave

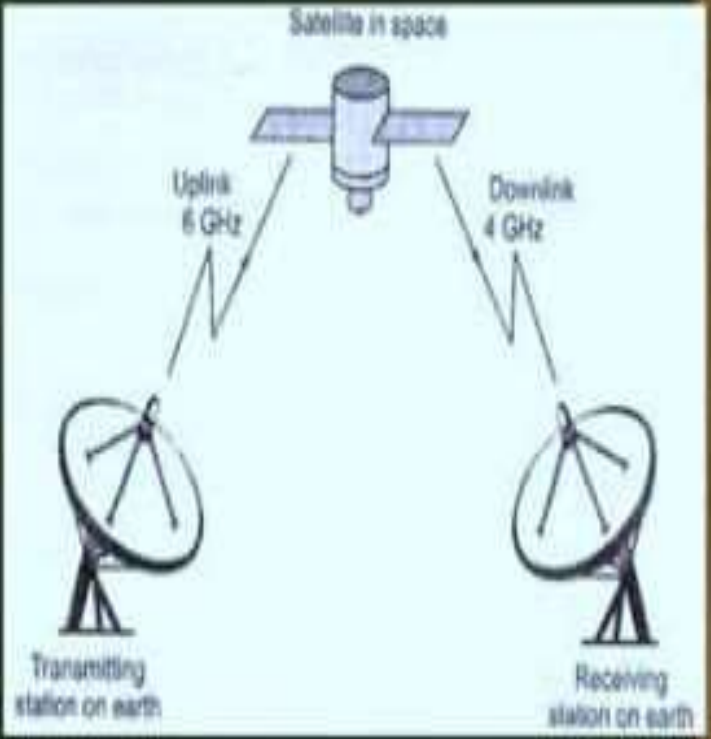


- The terrestrial microwave transmission typically uses the radio frequency spectrum 2 to 40 GHz.
- The transmitter is a parabolic dish (shaped like a bowl) and is mounted as high as possible to get the best frequency and transmission.
- An unblocked line of sight must be available between the source and the receiver.

- Terrestrial microwaves are used for both radio (voice) and television transmission.
- It can be expensive to adhere to the 30-mile line of sight requirement.
- The towers and repeaters can be fairly costly and there is a risk of interference from aeroplanes, birds and rain.

## Satellite Microwave

- This is a microwave relay station which is placed in outer space.
- The satellites are launched either by rockets or space shuttles carry them.



- The signals transmitted by earth stations are received, amplified, and retransmitted to other earth stations by the satellite.
- These are positioned 3600KM above the equator with an orbit

speed that exactly matches the rotation speed of the earth.

- As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.
- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.
- A single microwave relay station which is visible from any point.

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

## Infrared

- Infrared signals range between 300 Giga-Hertz to 400 Tera-Hertz.
- These can be used for short range communication.

- High range infrared rays cannot be used for long range communication as it cannot penetrate walls.
- Infrared signals are generated and received using optical transceivers.
- Infrared systems represent a cheap alternative to most other methods, because there is no cabling involved and the necessary equipment is relatively cheap.
- However, applications are limited because of distance limitations (of about one kilometer).

- It cannot be used outside building as rays of sun contain infrared which leads to interference in communication.
- Infrared having wide bandwidth can be used to transmit digital data with a very high data rate.

# THANK YOU

# UNIT II DATA LINK LAYER

Data link control – Error Detection – VRC – LRC – CRC – Checksum – Error Correction – Hamming Codes – MAC – Ethernet, Token ring , Token Bus – Wireless LAN - Bluetooth – Bridges.

# UNIT – II

## DATA LINK LAYER

# OVERVIEW

- **Data Link Control**
- **Error Detection**
- **VRC**
- **LRC**
- **CRC**
- **Checksum**
- **Error Correction**
- **Hamming Codes**
- **MAC**
- **Ethernet**
- **Token ring**
- **Token Bus**
- **Wireless LAN**
- **Bluetooth**
- **Bridges**

# Data Link Control

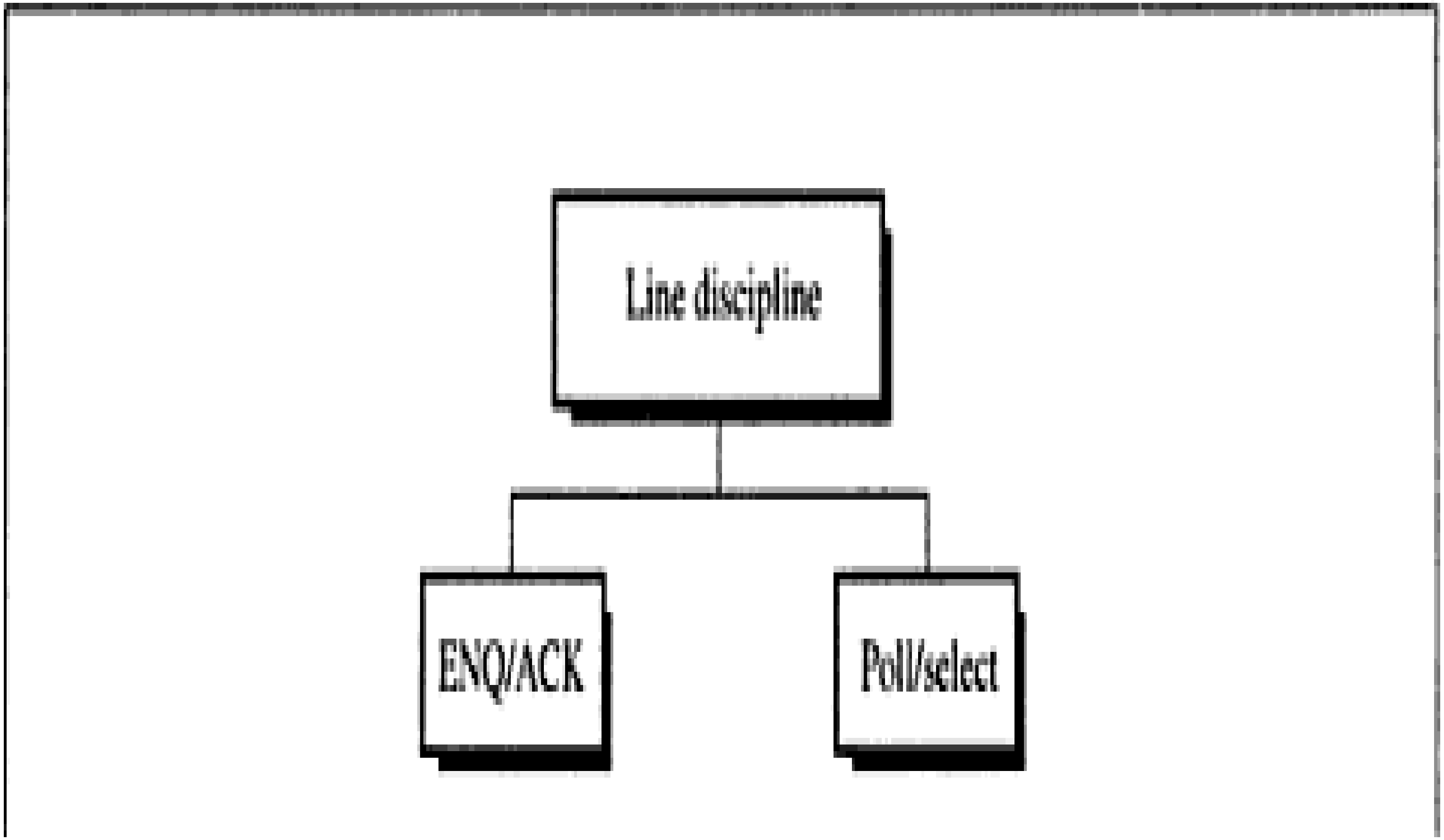
## Communication

- Minimum 2 devices are needed for data communication. So line discipline is necessary for co-operation b/w2 devices.
- The 2 important functions of data link layer is **flow control and error control.** This functions are otherwise called as Data link control.

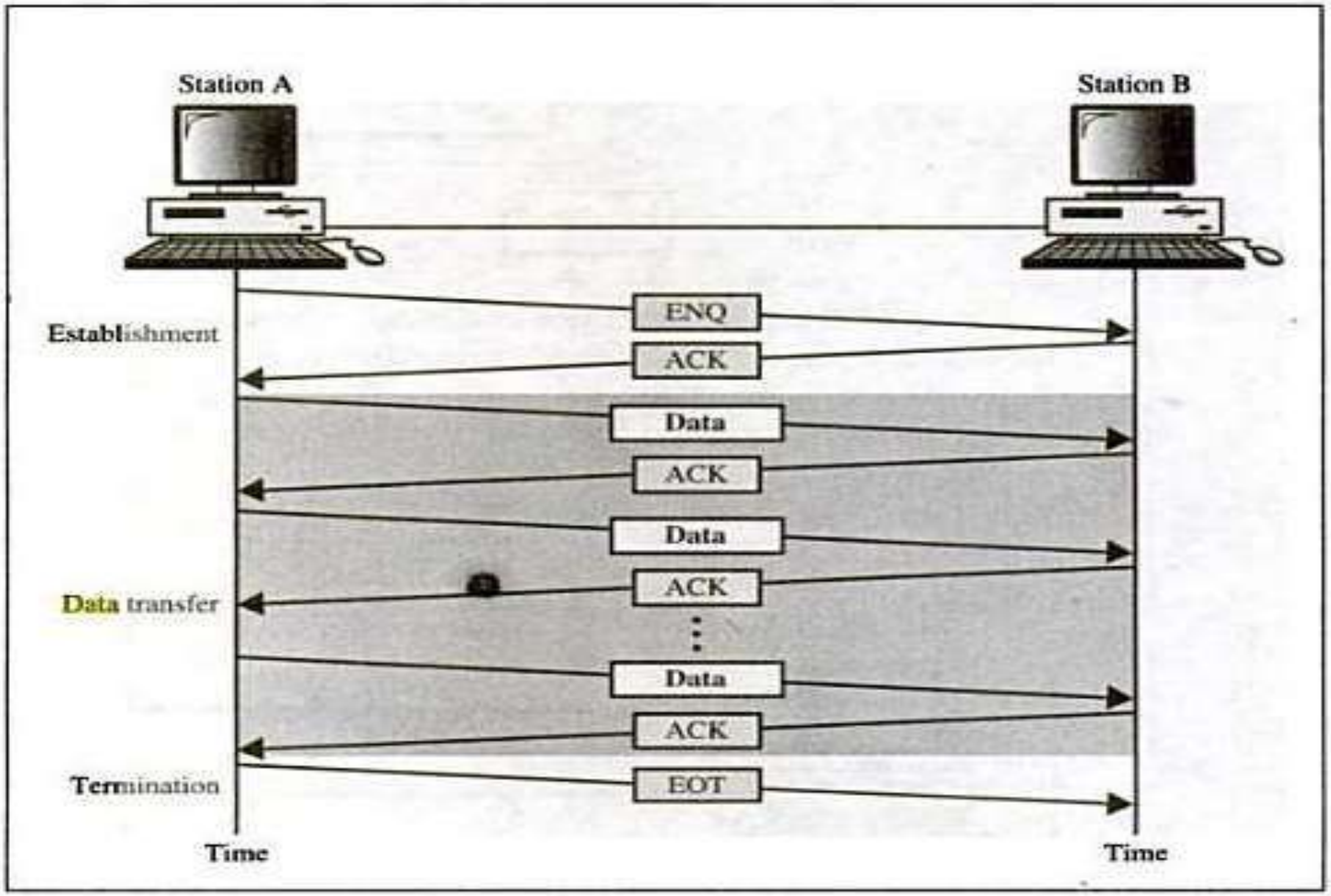
# Line Discipline

- It coordinates the link system
- It is done in 2 ways
  - ENQ (Enquiry)
    - Used in peer - peer communication
    - Enquire whether there is a required link b/w two devices
    - Check whether the intended device is capable to receive
  - ACK (Acknowledgment)
    - Used in Primary secondary communication
    - The intended device will acknowledge about its status to the receiver

# There are 2 categories in line discipline



# ENQ/ACK Line Discipline



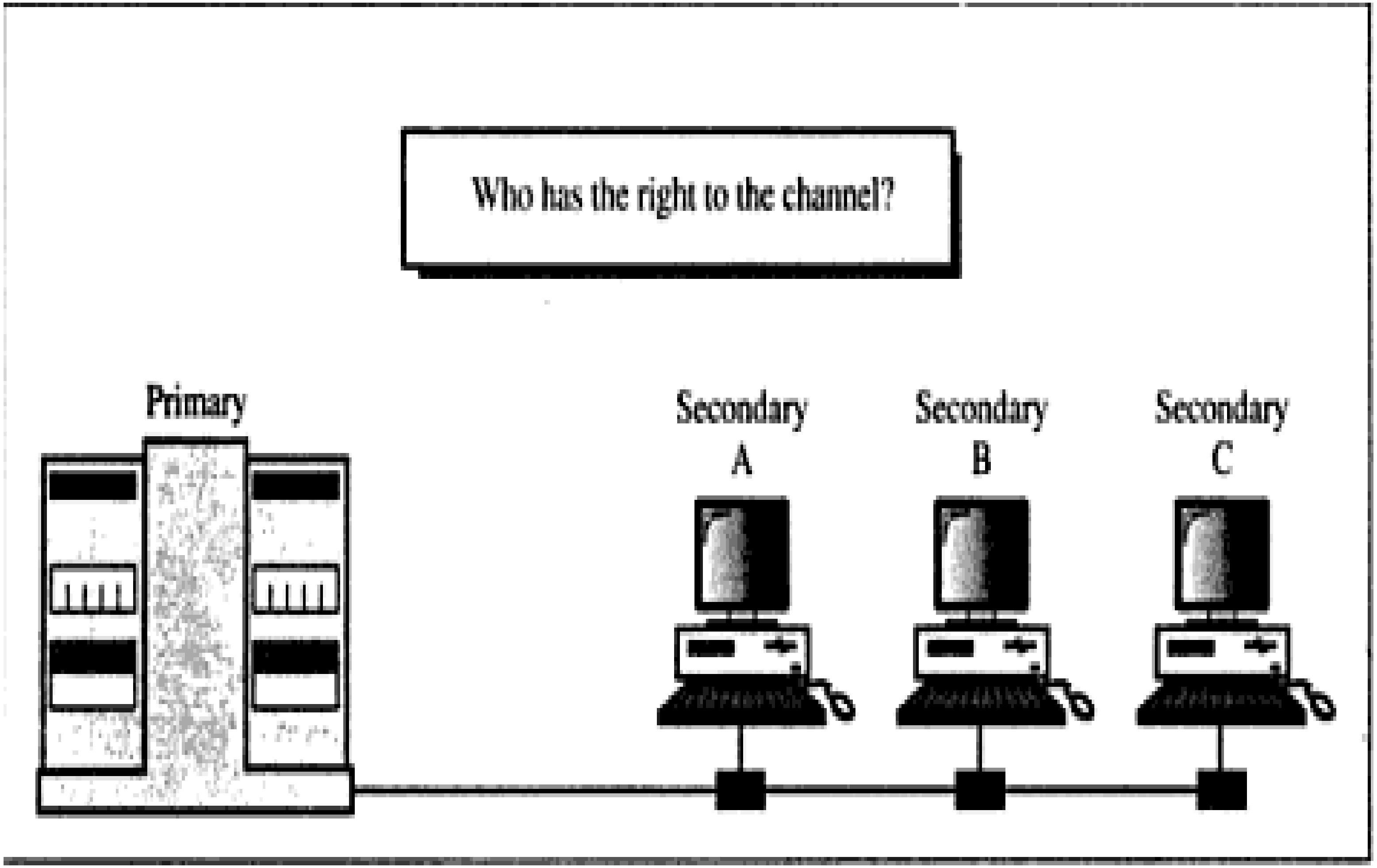
# Select

- □ It is a line discipline used in topologies with primary secondary relationship.

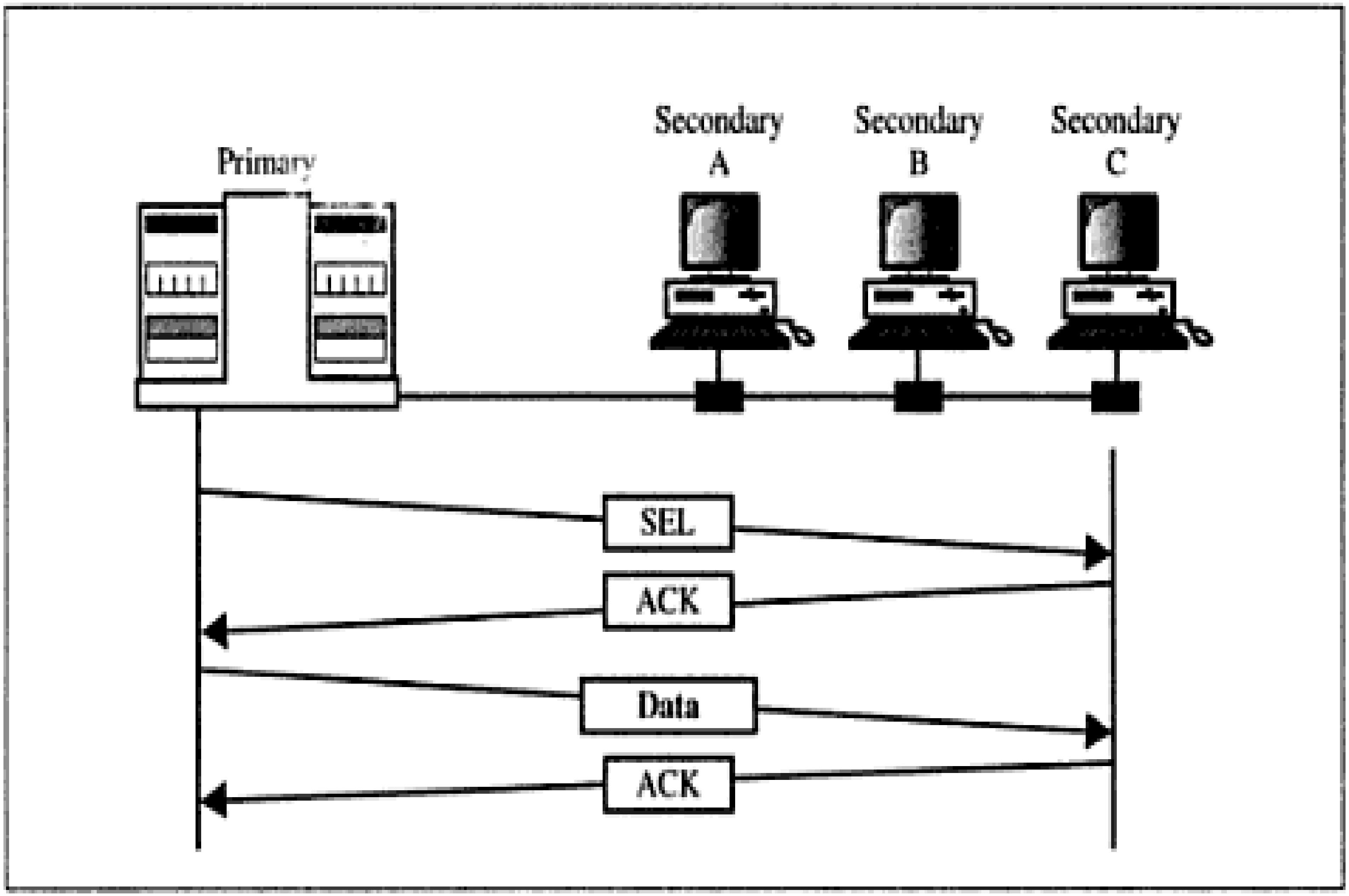
<u>Select</u>

- □ It is uses whenever the primary device has something to send.ie)Primary controls the link.

# Select


Who has the right to the channel?
Primary
Secondary A
Secondary B
Secondary C

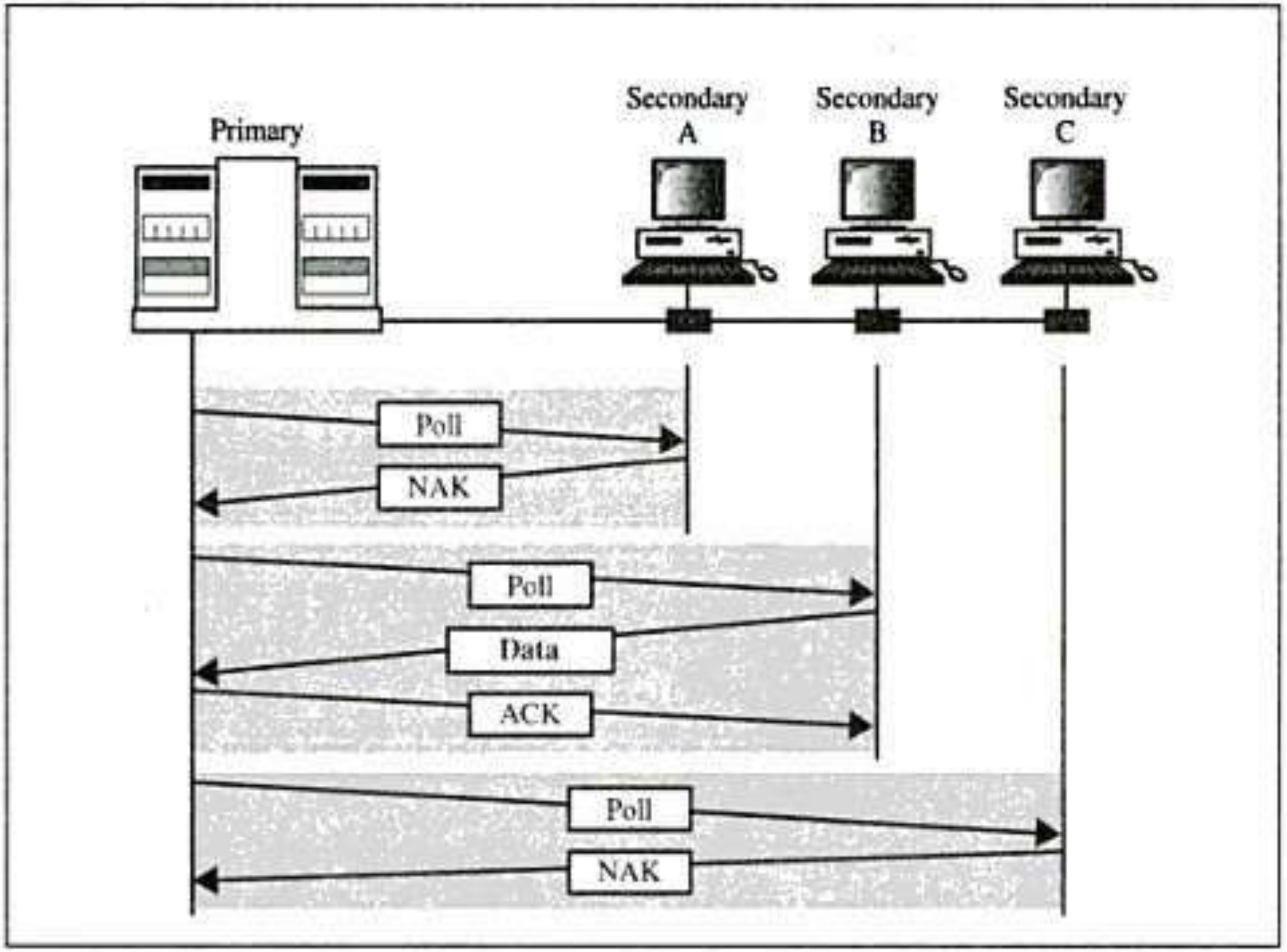
# Select


Secondary
A
Secondary
B
Secondary
C
Primary
SEL
ACK
Data
ACK

# Poll

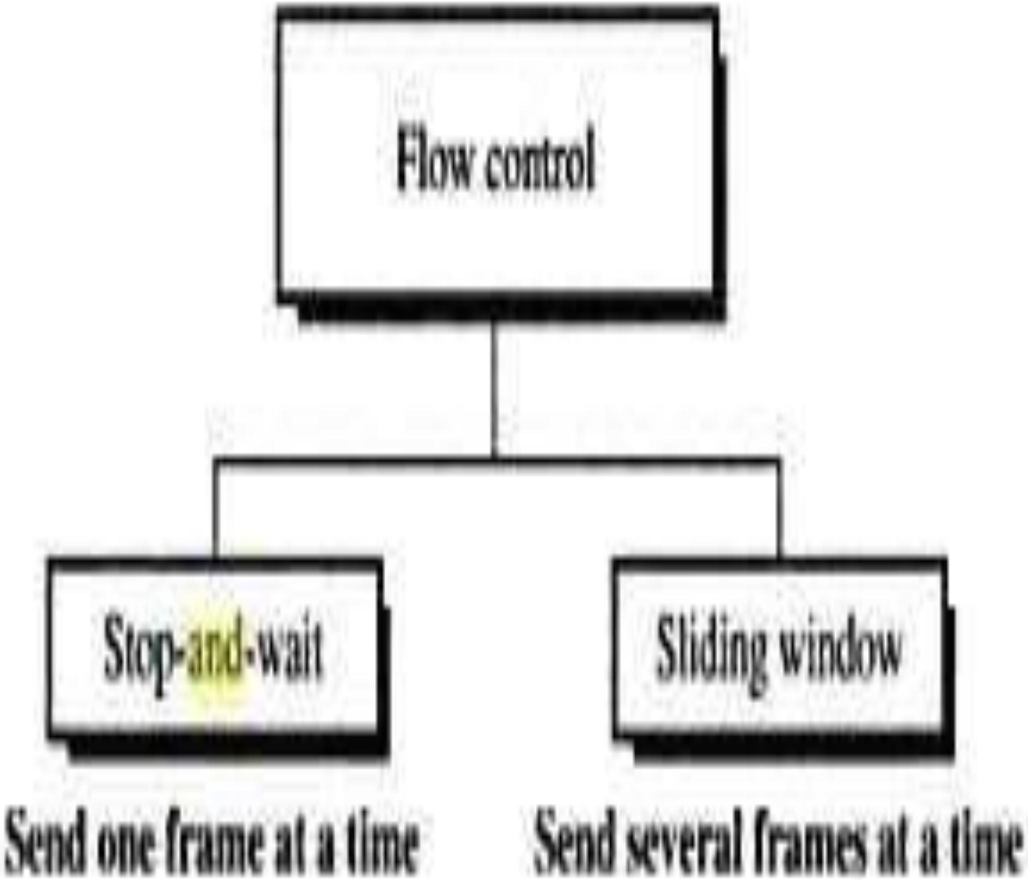
- The polling function is used by the primary device to Select transmissions from the secondary devices.
- If the primary device is ready to receive data , It ask each device in turn if it has anything to send.

# Poll


Primary
Secondary A
Secondary B
Secondary C
Poll
NAK
Poll
Data
ACK
Poll
NAK

# Flow Control

- It is a set of procedures to tell the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
- Two categories of flow control:
  - **Stop-and-wait**
    - Send one frame at a time.
  - **Sliding window**
    - Send several frames at a time.



Flow control

Stop-and-wait

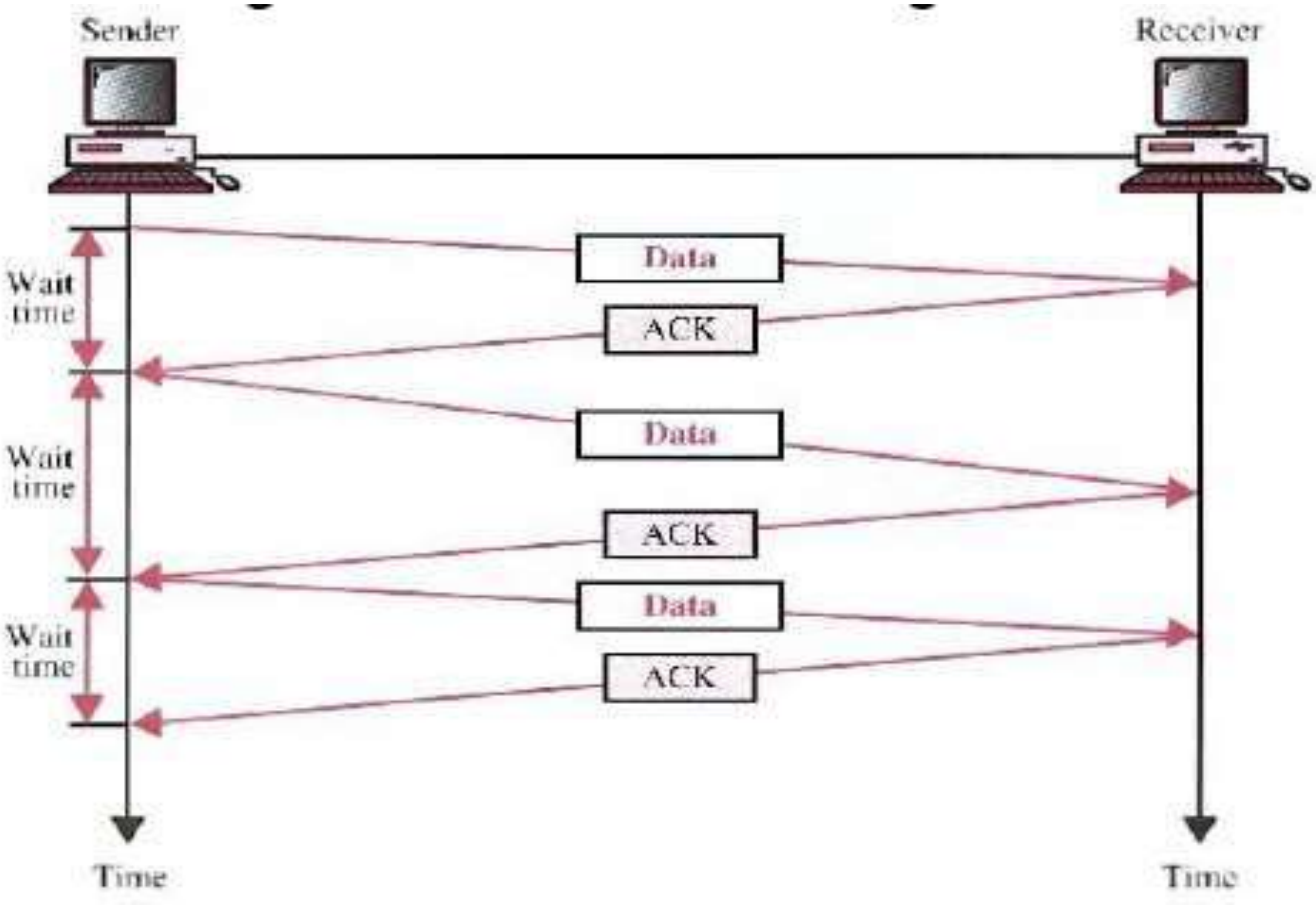
Send one frame at a time

Sliding window

Send several frames at a time

# Stop-and-wait

- Sender sends one frame and waits for an acknowledgement before sending the next frame.

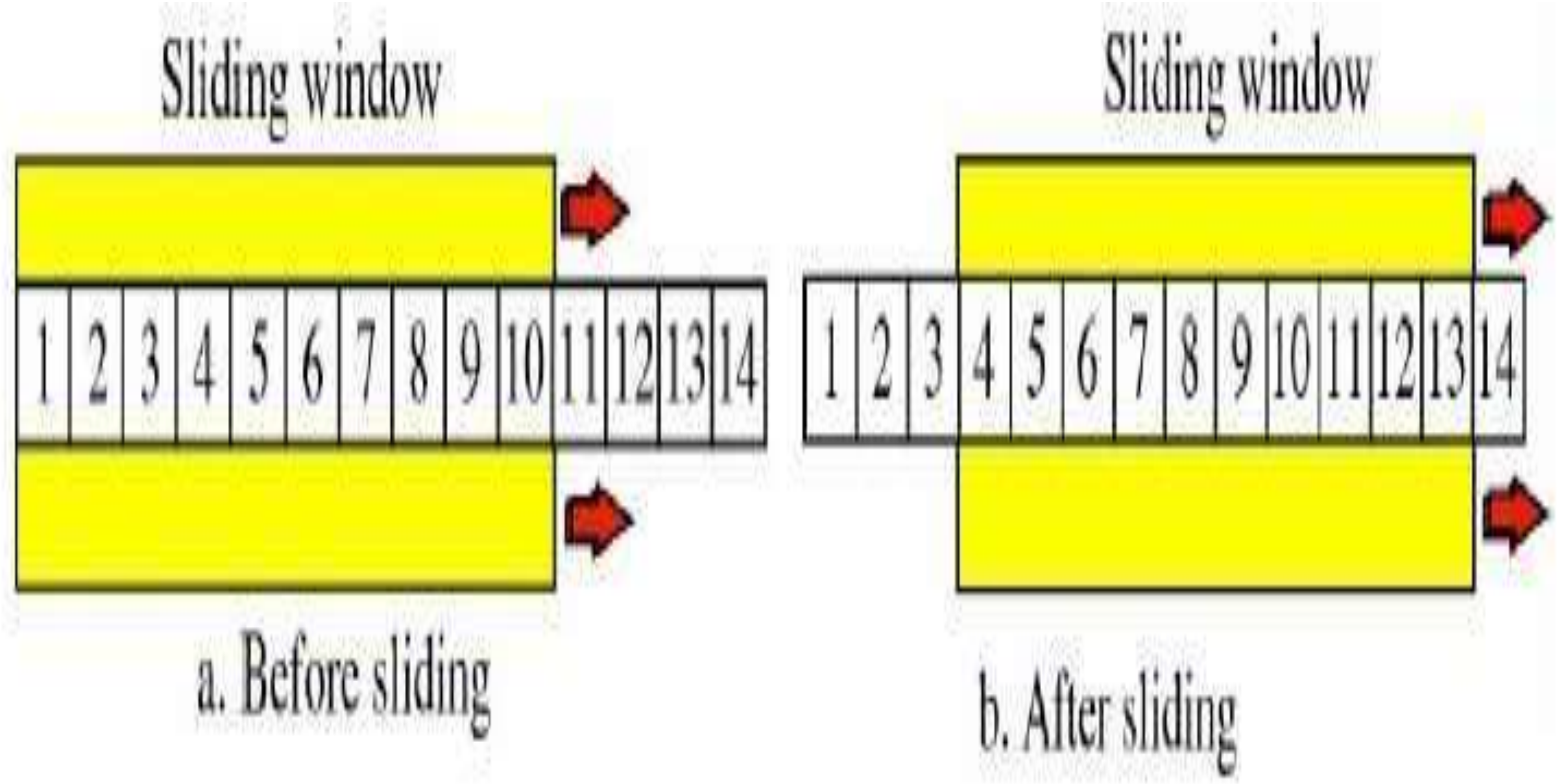


# Stop-and-wait

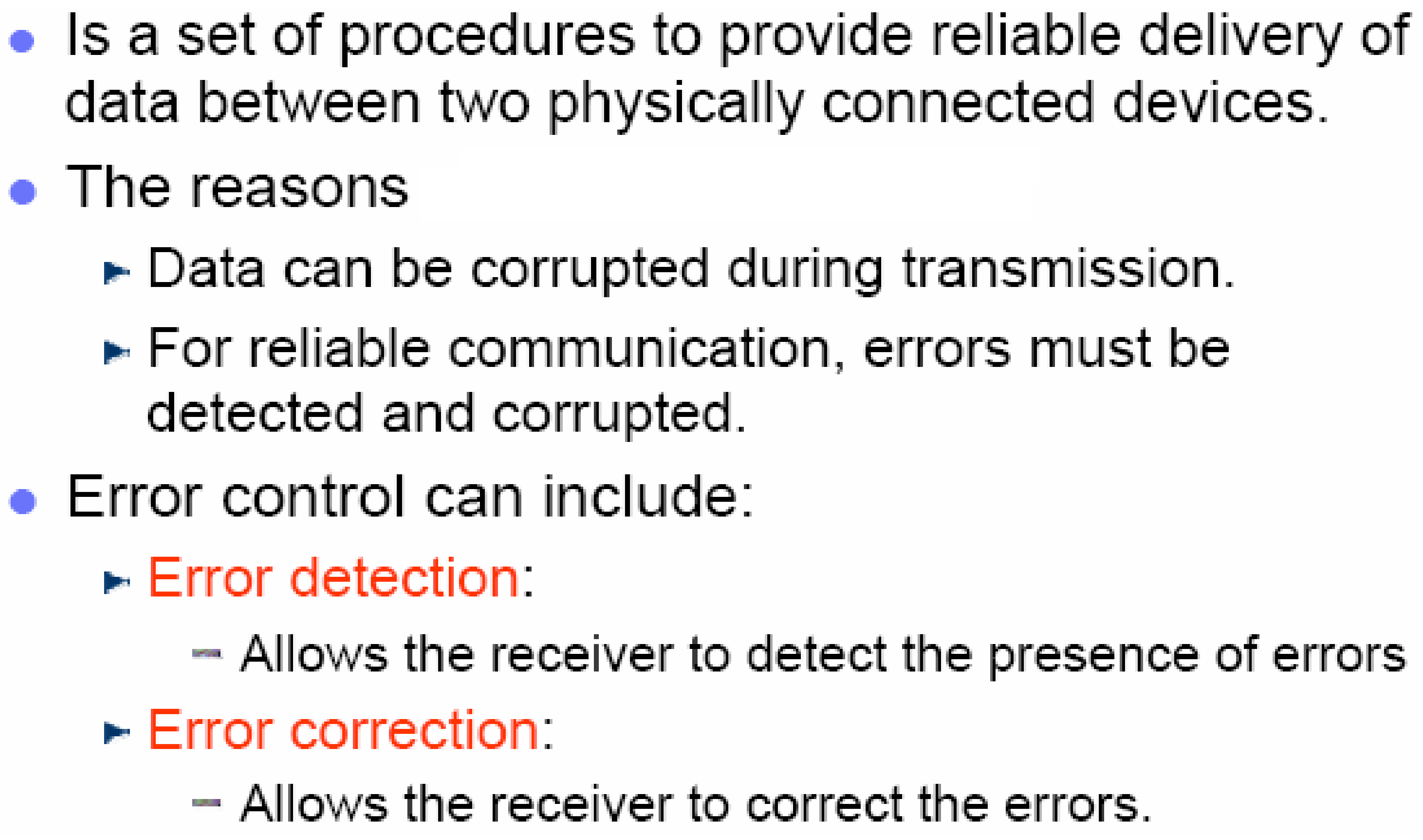
- Advantages:
  - Simplicity.
  - Each frame is checked and acknowledged before the next frame is sent.
- Disadvantages:
  - Slow.
    - Can add significantly to the total transmission time if the distance between devices is long.
  - Inefficiency
    - Each frame is alone on the line.

# Sliding Window

- Sender can send several frames before needing an acknowledgement.
- Advantages:
  - The link can carry several frames at once.
  - Its capacity can be used efficiently.

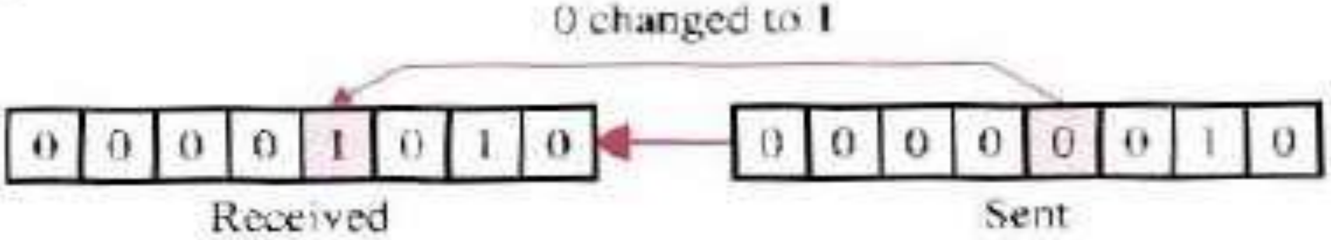


# Error Control

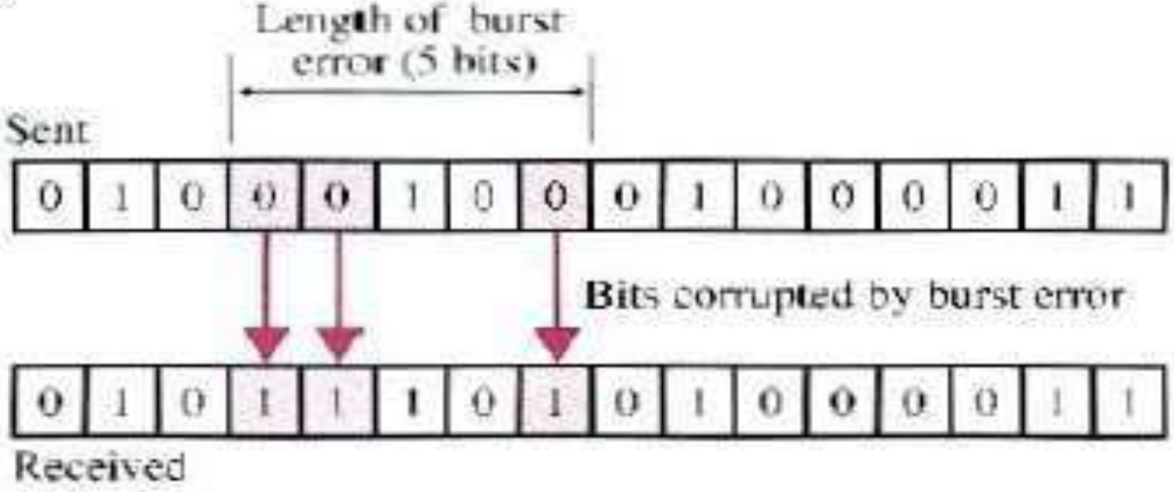


- Is a set of procedures to provide reliable delivery of data between two physically connected devices.
- The reasons
  - Data can be corrupted during transmission.
  - For reliable communication, errors must be detected and corrupted.
- Error control can include:
  - Error detection:
    - Allows the receiver to detect the presence of errors
  - Error correction:
    - Allows the receiver to correct the errors.

- Errors:
  - Can be caused by signal attenuation or noise.
  - Types of errors:
    - Single-bit error: only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.

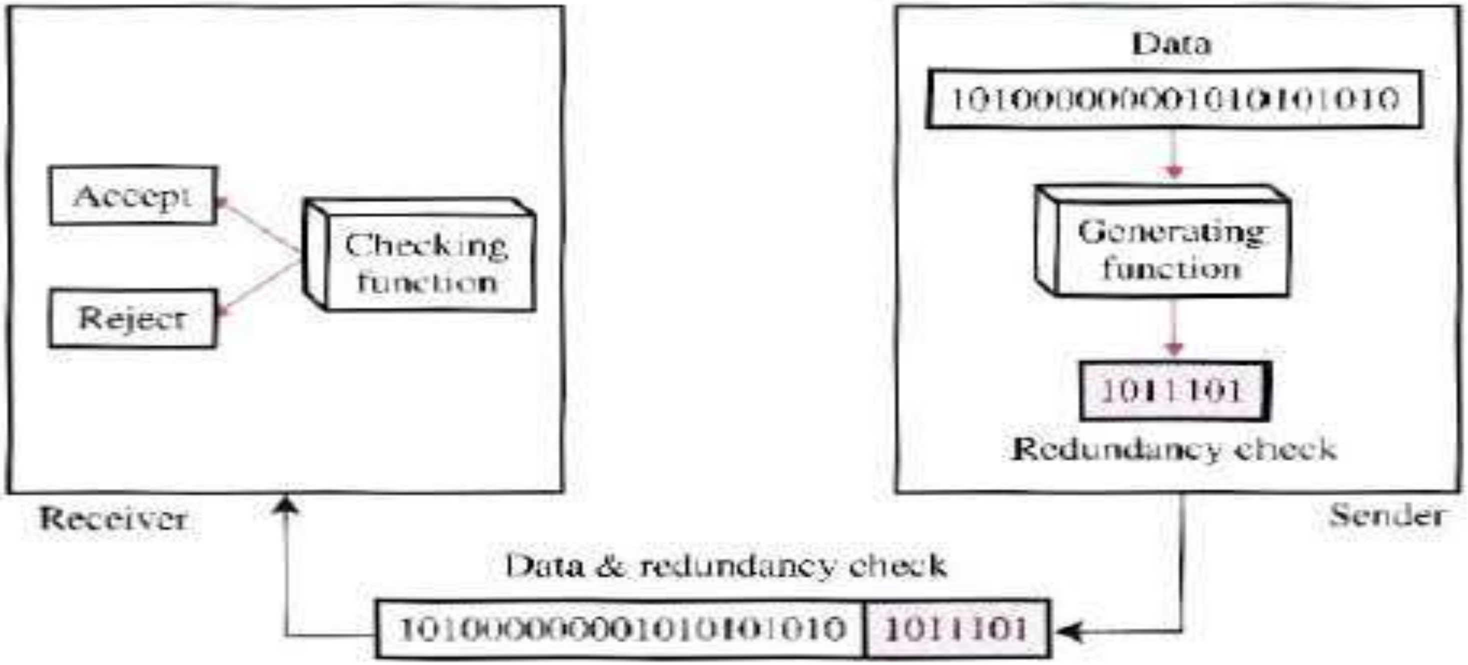


    - Burst-error: two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.



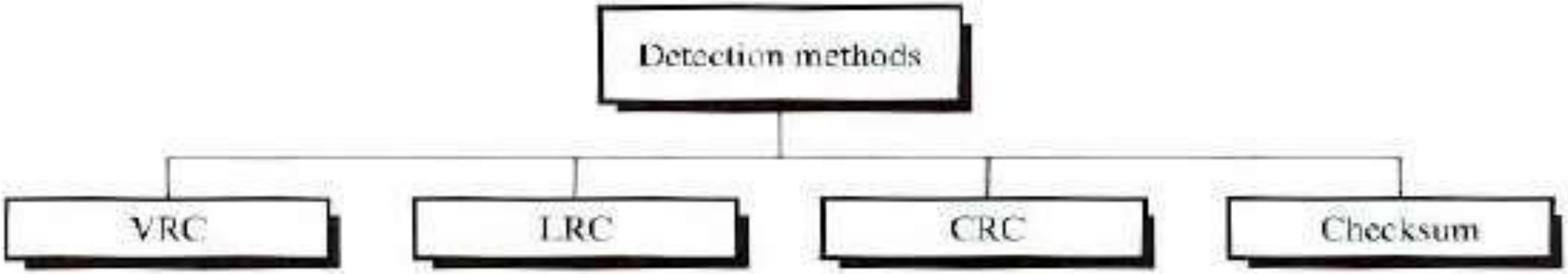
# Error Detection

- Error detection uses the concept of redundancy.
  - Adds extra bits for detecting errors at destination.
    - For efficiency, extra bits $k << n$ (information bits).
    - Generating function is used to generate these extra bits.



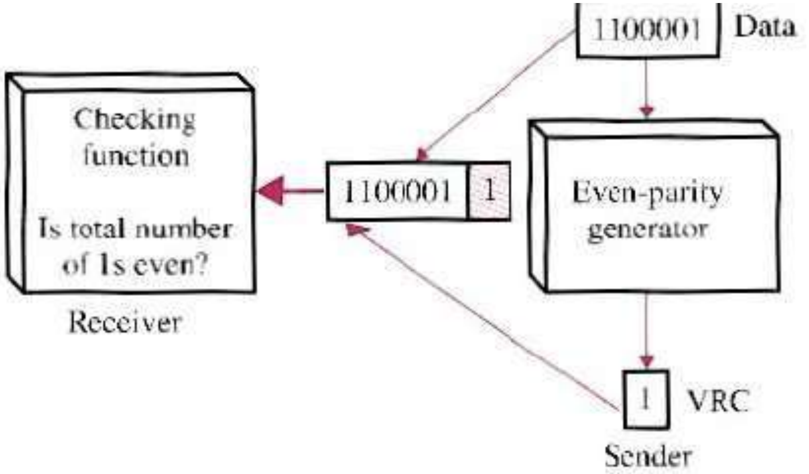
# Error Detection

- Four types of redundancy checks:



  - VRC: vertical redundancy check or parity check
  - LRC: longitudinal redundancy check
  - CRC: cyclic redundancy check
  - VRC, LRC, CRC used by data link layers.
  - Checksum used by higher-layer protocols.

- Vertical redundancy check (VRC):
  - Adds a parity bit to every data unit so that the total number of 1s becomes
    - even – even parity checking
    - odd – odd-parity checking



Even number of ones –add 0
Odd number of ones – add 1

- Example:
  - The word “cute” is coded in ASCII as:

| 1100011 | 1110101 | 1110100 | 1100101 |
|---|---|---|---|
| c | u | t | e |

  - Using even-parity checking, the sender will send:

    11000110 11101011 11101000 11001010

  - If the word is not corrupted during transmission:
    - The receiver counts the 1s in each character and comes up with (4, 6, 4, 4) – all even numbers.
  - If the word is corrupted during transmission, say:

    11010110 11101011 11101000 11000010

    - The receiver counts the 1s in each character and comes up with (5, 6, 4, 3).

Can detect all single-bit errors. Can detect burst errors only if the total number of errors in each data unit is odd.

## Longitudinal redundancy check (LRC):

- 2-dimensional parity checking.
  - Divides a block of bits into rows of *n* bits.
  - Calculates the even/odd parity for each column.
    - This results in an extra row of parity bits.

## Example:

- The word “cute” is coded in ASCII as:

  1100011 1110101 1110100 1100101
  c u t e

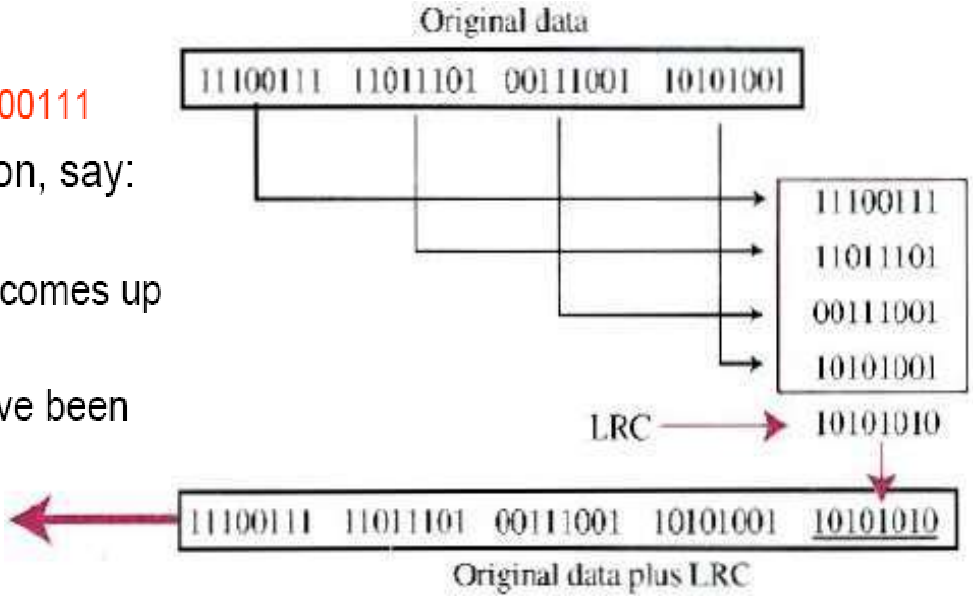
- Using LRC, the sender will send:

  1100011 1110101 1110100 1100101 0000111

- If the word is corrupted during transmission, say:

  1101101 0100101 1110100 1100001

  - The receiver calculates the LRC and and comes up with 1011001 ≠ 0000111.
  - 5 bits of LRC have changed – 5 errors have been detected.

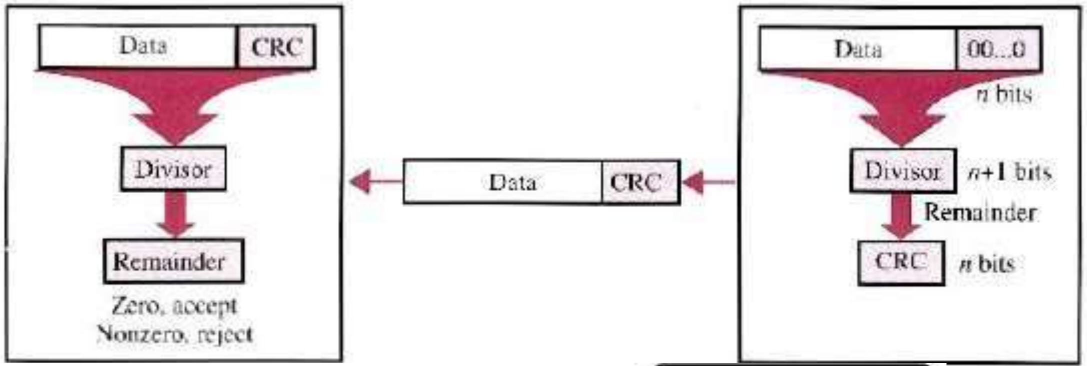


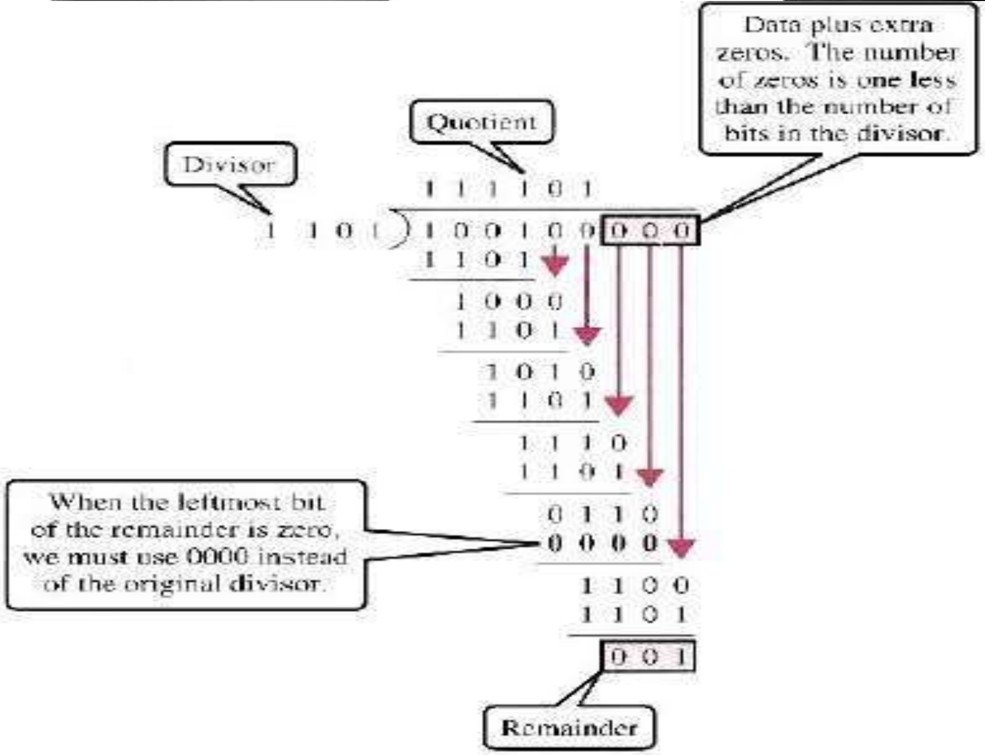
- Increases the likelihood of detecting burst errors.
- *n* bits LRC can detect a burst error of *n* bits.
- Errors may be undetected if:
  - Have even number of errors in that position.

- Cyclic redundancy check (CRC):
  - Based on binary division
    - Cf. VRC and LRC based on addition
  - Divides the data unit by predetermined divisor or generator using modulo-2 division.
  - CRC = remainder.
- CRC generator:
  - For *n*-bits data unit and *m*-bits divisor:
    - Forms dividend: *n*-bits + (*m*-1) bits of zeros.
    - Divides dividend by divisor.
    - Subtracting each bit of divisor without disturbing the next higher bit.

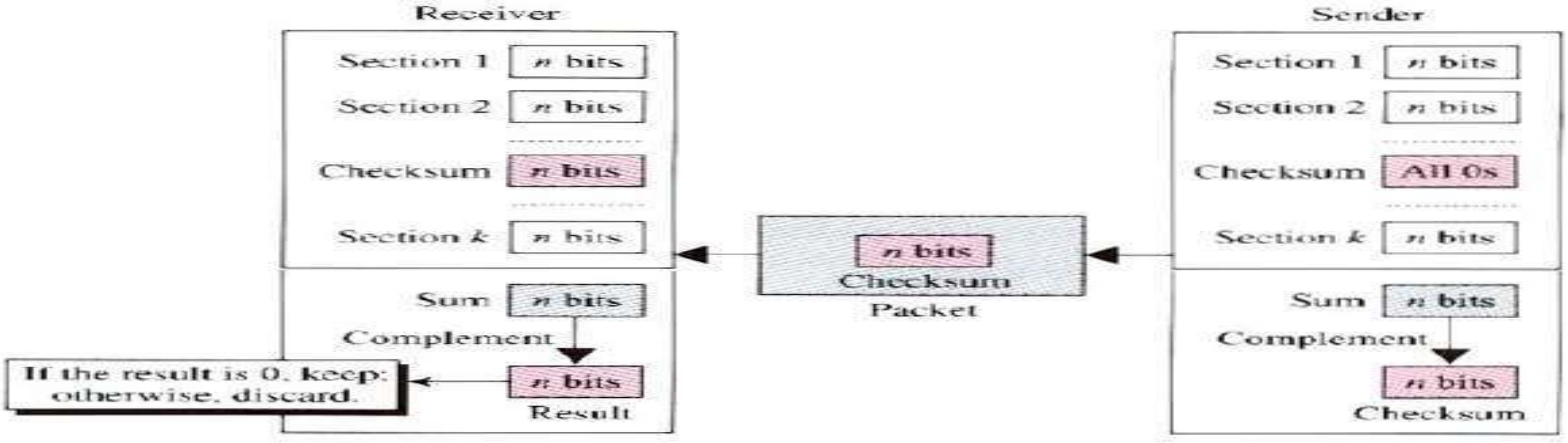
      1 – 1 or 0 – 0 = 0

      1 – 0 or 0 – 1 = 1
  - Sends data + CRC.

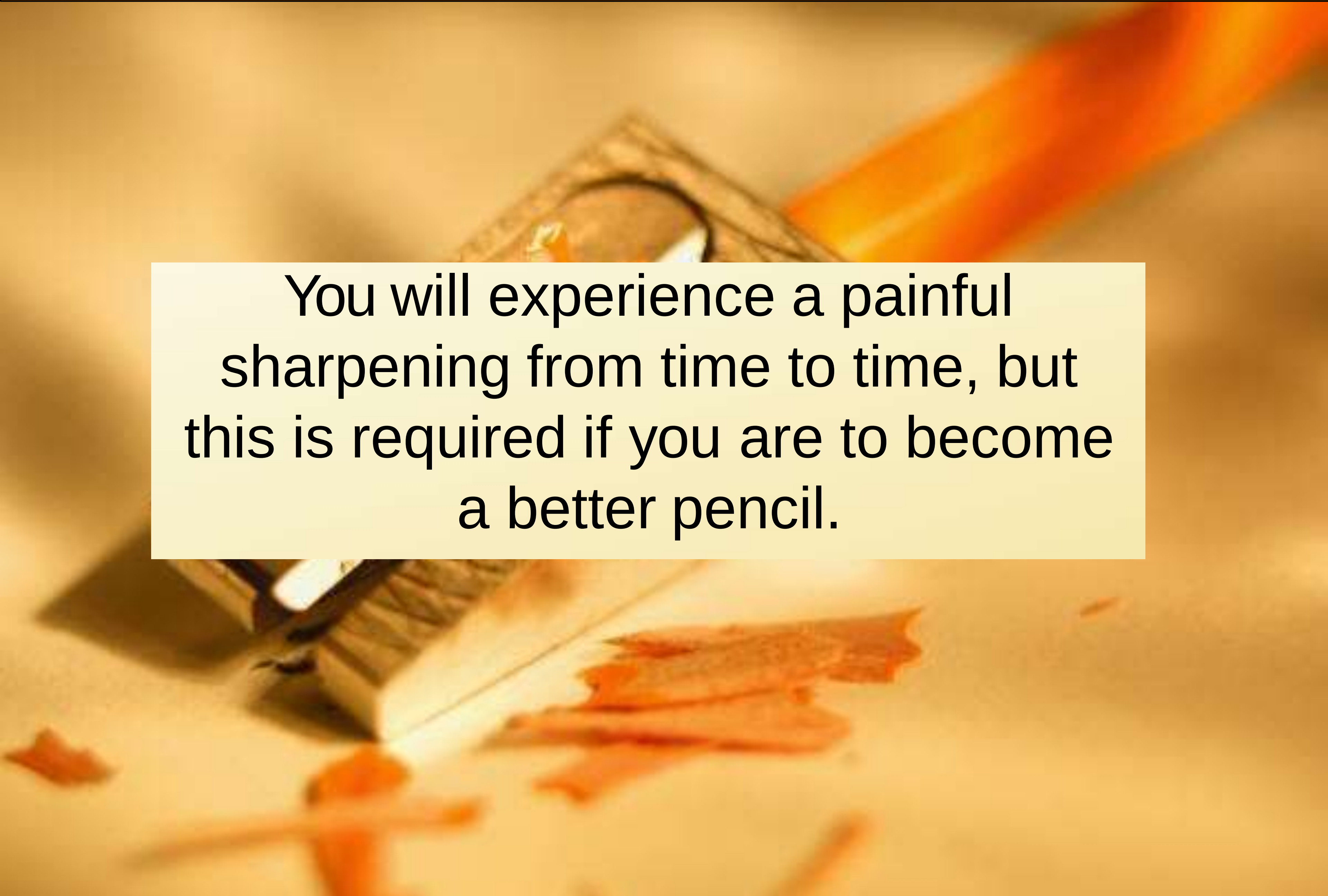



Data plus extra zeros. The number of zeros is one less than the number of bits in the divisor.
Quotient
Divisor
1 1 1 1 0 1
1 1 0 1
1 0 0 1 0 0 0 0 0
1 1 0 1
1 0 0 0
1 1 0 1
1 0 1 0
1 1 0 1
1 1 1 0
1 1 0 1
0 1 1 0
0 0 0 0
1 1 0 0
1 1 0 1
0 0 1
When the leftmost bit of the remainder is zero, we must use 0000 instead of the original divisor.
Remainder

- Checksum:



- Checksum generator (sender):
  - Divide data unit into segments of *n* bits (usually *n* = 16).
  - Add together all segments using one's complement to get the sum
  - Complement the sum to become the checksum.
  - Send the checksum with the data.
- Checksum checker (receiver):
  - Divide data unit into segments of *n* bits.
  - Add together all segments using one's complement to get the sum.
  - Complement the sum.
  - If the result is zero, accept the data, otherwise, reject the data.



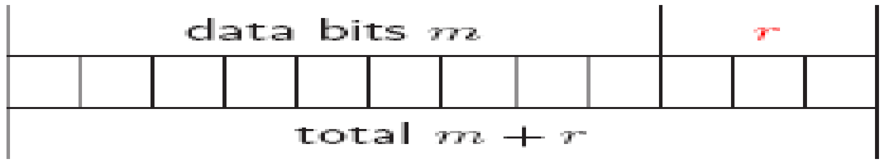
You will experience a painful sharpening from time to time, but this is required if you are to become a better pencil.

# Error Correction

- Error correction can be handled in two ways:
  - Receiver can ask the sender to retransmit the corrupted data unit.
  - Receiver can use an error-correcting code, which automatically correct certain errors.
    - Most error correction is limited to 1 – 3 bits errors.
    - Much more redundancy bits are needed to correct larger bit errors – often becomes inefficient to use.
  - The choice depends on the distance between devices and applications.

# Redundancy Bits

To calculate the number of redundancy bits $r$ required to correct a given number of data bits $m$, must find a relationship between $m$ and $r$



- $m + r$ bits $\Rightarrow$ r must indicate at least $m + r + 1$ different states
  - *Each state identifies a specific bit*
  - One of the states must indicate *no error*
- Therefore, if $m + r + 1$ states are needed and $r$ can identify $2^r$ states

$$2^r \geq m + r + 1$$

- The value of $r$ can be determined by using the value of $m$
- If $m = 7$ then the smallest $r$ is 4

$$2^4 \geq 7 + 4 + 1$$

| Data bits ($m$) | Redundancy bits ($r$) | Total bits ($m + r$) |
|---|---|---|
| 1 | 2 | 3 |
| 2 | 3 | 5 |
| 3 | 3 | 6 |
| 4 | 3 | 7 |
| 5 | 4 | 9 |
| 6 | 4 | 10 |
| 7 | 4 | 11 |

You have the ability to correct any mistakes you might make.

# Hamming Codes-Error correction

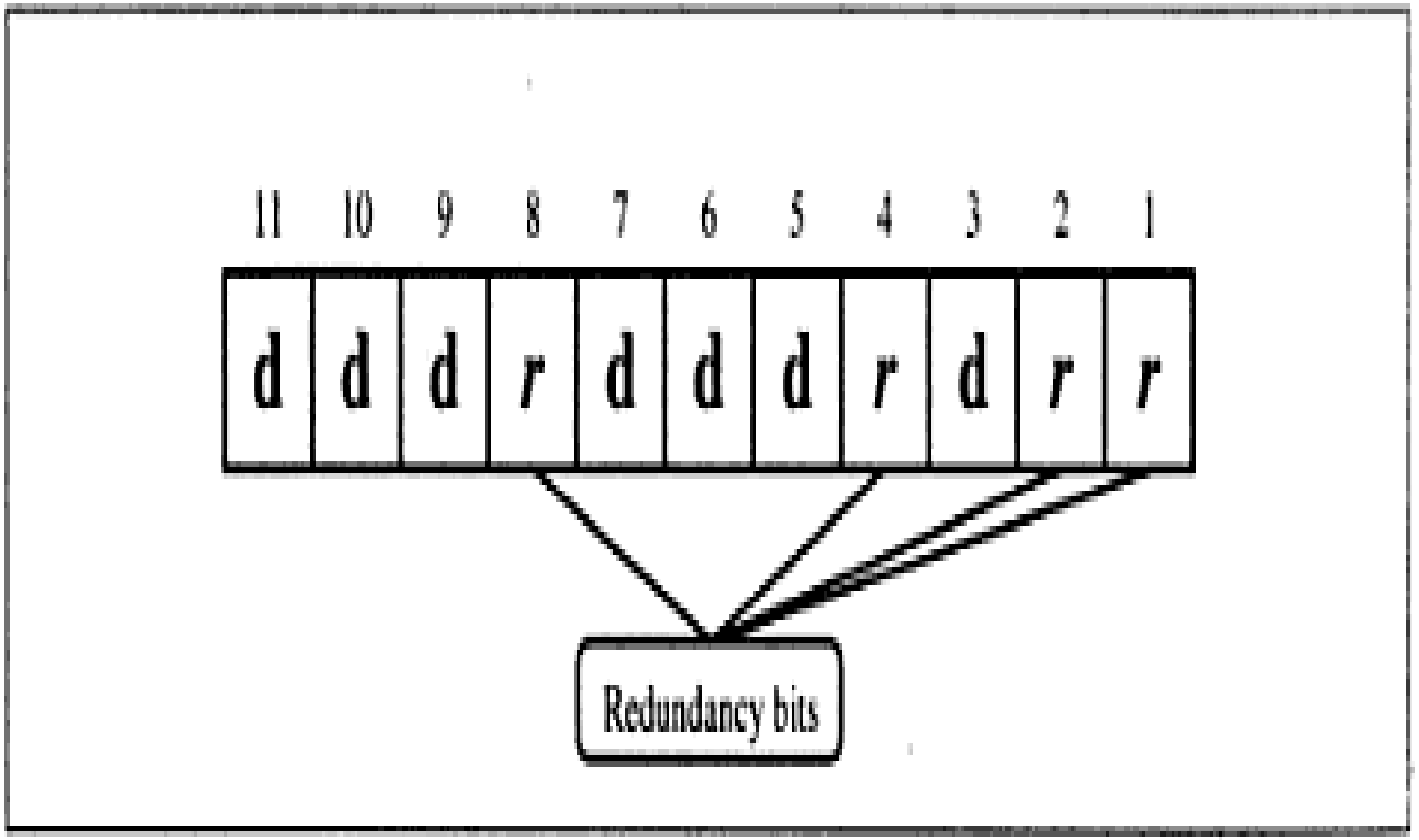
- Hamming codes, like polynomial codes, are appended to the transmitted message

- Hamming codes, unlike polynomial codes, contain the information necessary to locate a single bit error

# Calculating the Hamming Code

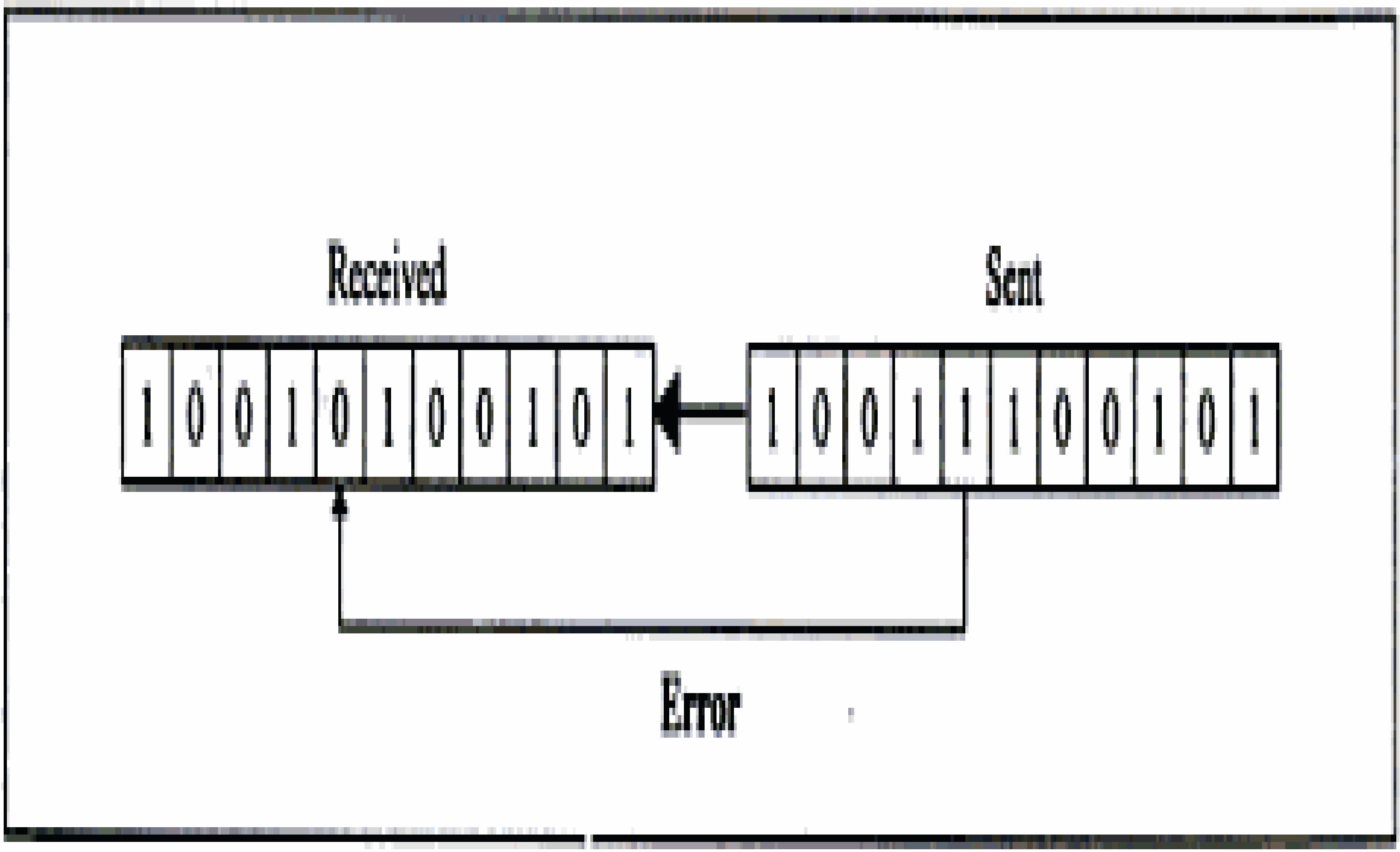
- The key to the Hamming Code is the use of extra parity bits to allow the identification of a single error. Create the code word as follows:
  - Mark all bit positions that are powers of two as parity bits. (positions 1, 2, 4, 8, 16, 32, 64, etc.)
  - All other bit positions are for the data to be encoded. (positions 3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, etc.)
  - Each parity bit calculates the parity for some of the bits in the code word. The position of the parity bit determines the sequence of bits that it alternately checks and skips.
    Position 1: check 1 bit, skip 1 bit, check 1 bit, skip 1 bit, etc. (1,3,5,7,9,11,13,15,...)
    Position 2: check 2 bits, skip 2 bits, check 2 bits, skip 2 bits, etc. (2,3,6,7,10,11,14,15,...)
    Position 4: check 4 bits, skip 4 bits, check 4 bits, skip 4 bits, etc. (4,5,6,7,12,13,14,15,20,21,22,23,...)
    Position 8: check 8 bits, skip 8 bits, check 8 bits, skip 8 bits, etc. (8-15,24-31,40-47,...)
    Position 16: check 16 bits, skip 16 bits, check 16 bits, skip 16 bits, etc. (16-31,48-63,80-95,...)
    Position 32: check 32 bits, skip 32 bits, check 32 bits, skip 32 bits, etc. (32-63,96-127,160-191,...)
    etc.
  - Set a parity bit to 1 if the total number of ones in the positions it checks is odd. Set a parity bit to 0 if the total number of ones in the positions it checks is even.

# Position of Redundancy bit in Hamming code



# Error

Figure 9.20 *Single-bit error*

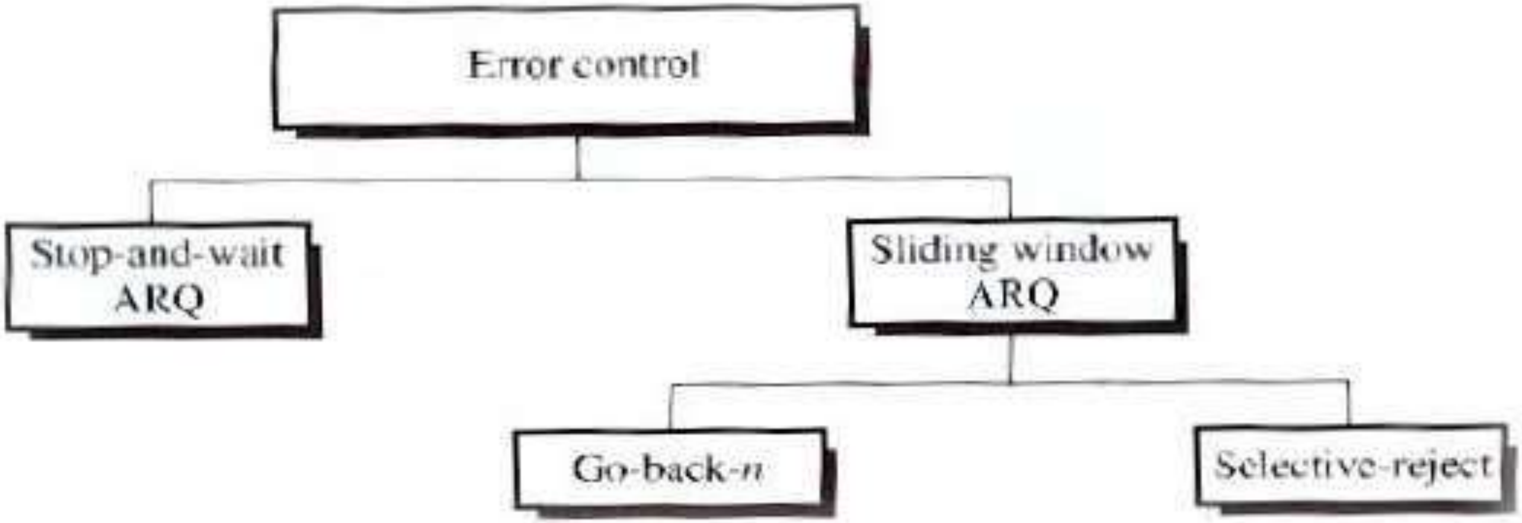


Received: 1 0 0 1 0 1 0 0 1 0 1

Sent: 1 0 0 1 1 1 0 0 1 0 1

# Error Control

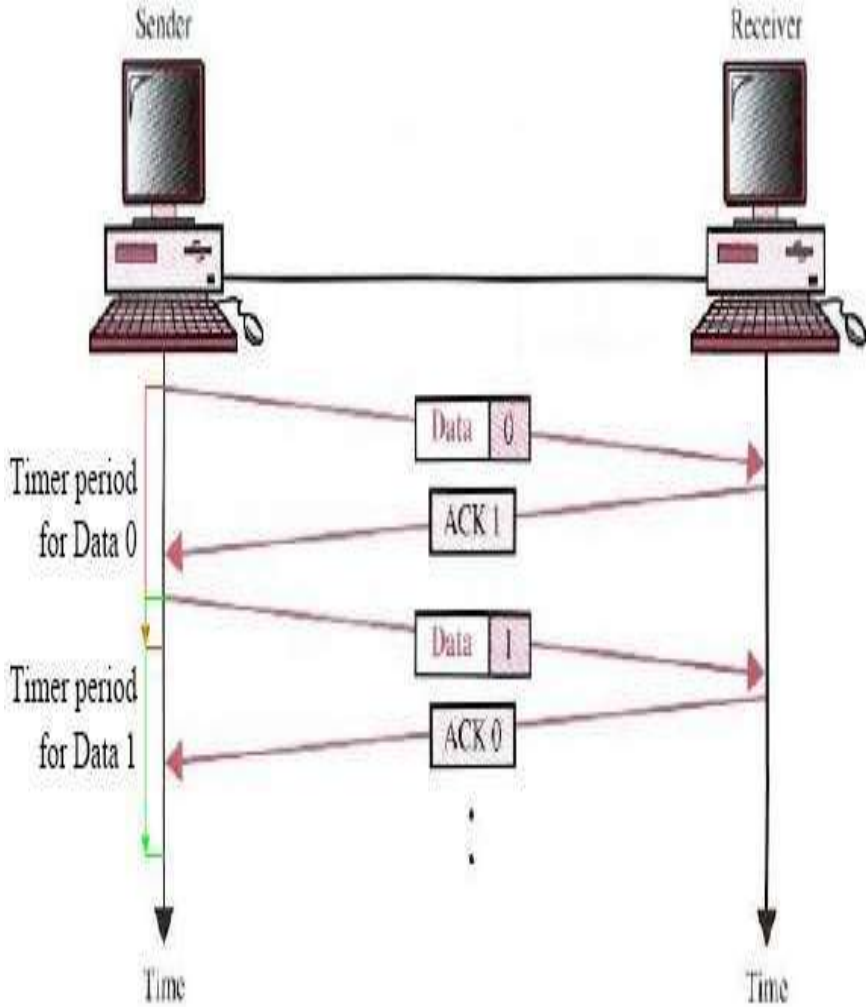
- Data link layer error control commonly uses:
  - CRC for error detection.
  - Data retransmission for error correction.
    - It returns a negative acknowledgement (NAK) and asks for the frame retransmission. This process is called Automatic Repeat Request (ARQ).
- Error control adds on to flow control.



# Stop-and-Wait ARQ

- Is an extension of stop-and-wait flow control to include data retransmission.
- ARQ needs to cater for three possible cases:
  - Corrupted frame.
  - Lost frame.
  - Lost of acknowledgement.

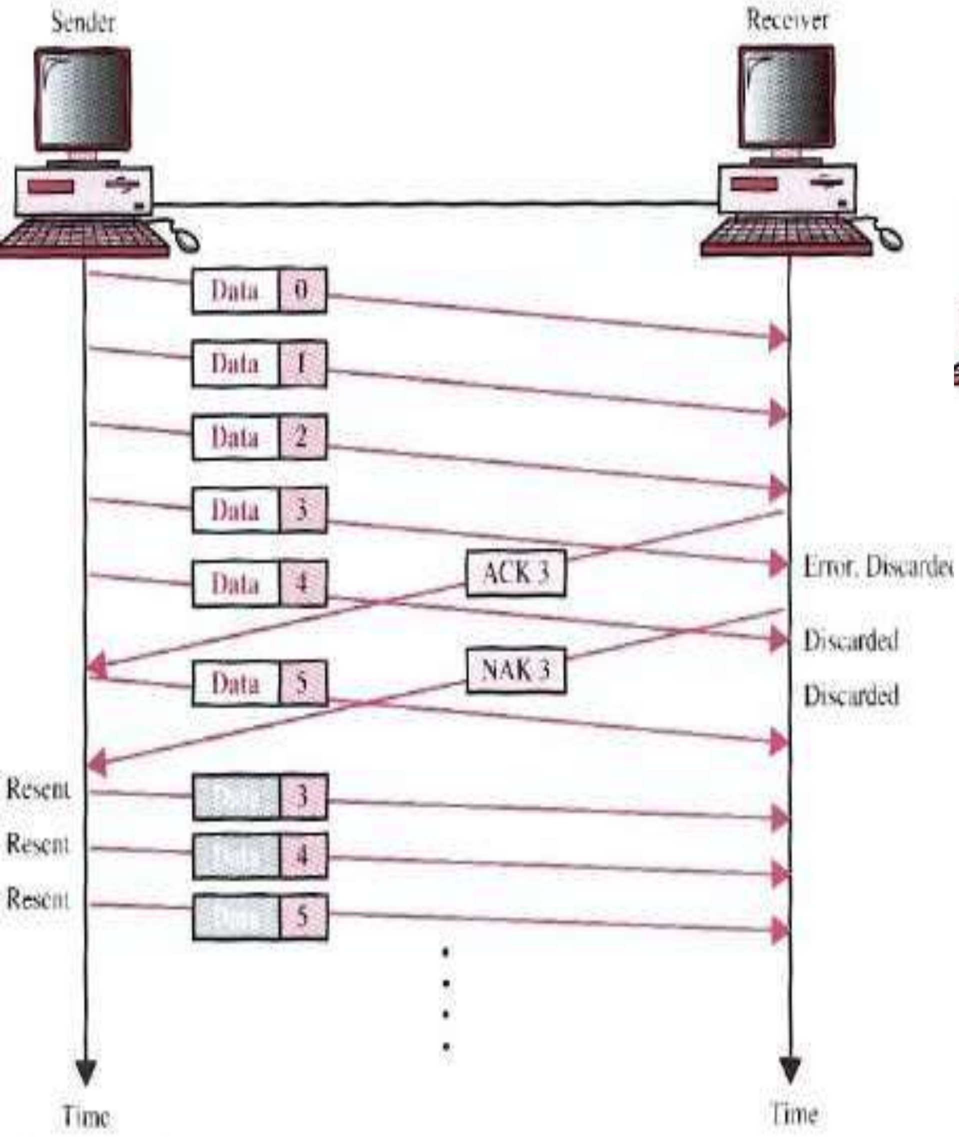
- Four features added onto basic flow control:
  - Sending device keeps a copy of the last frame transmitted until it is acknowledged.
  - Sending device is equipped with a timer.
    - Timer starts every time a frame is transmitted.
    - If the timer times out and the sender has not received an acknowledgement, then it assumes that the frame is lost and resends the frame again.
  - Numbering of data frames and ACK frames.
    - Allows the receiver to identify duplicate transmission.
  - Receiving device returns a NAK frame if it detects an error in a data frame.



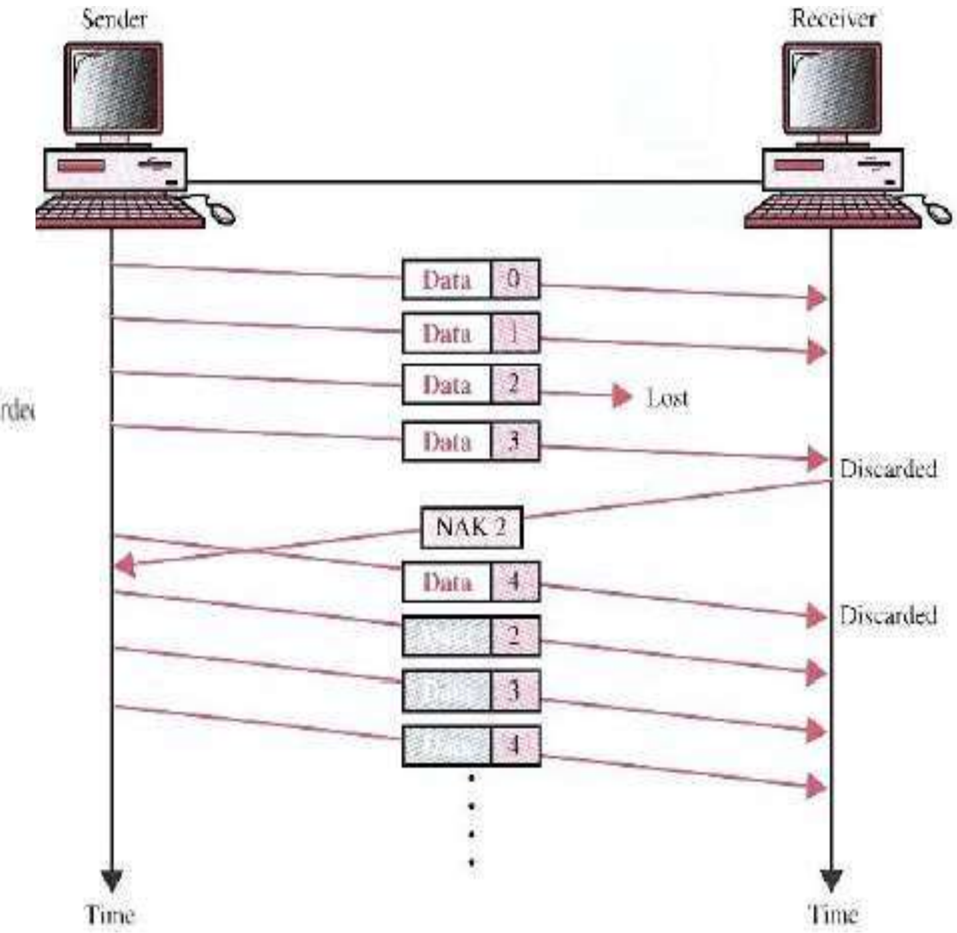
# Sliding windowARQ

- Is an extension of sliding window flow control to include data retransmission.
- Many frames are in transit following a corrupted or lost frame. Two possible options:
  - Ask for retransmission of all frames starting from the corrupted frame – go-back-n ARQ.
  - Ask for retransmission of only the corrupted frame – selective-reject ARQ.
- Stop-and-wait protocol is a special case of sliding-window protocol with a window size of 1.

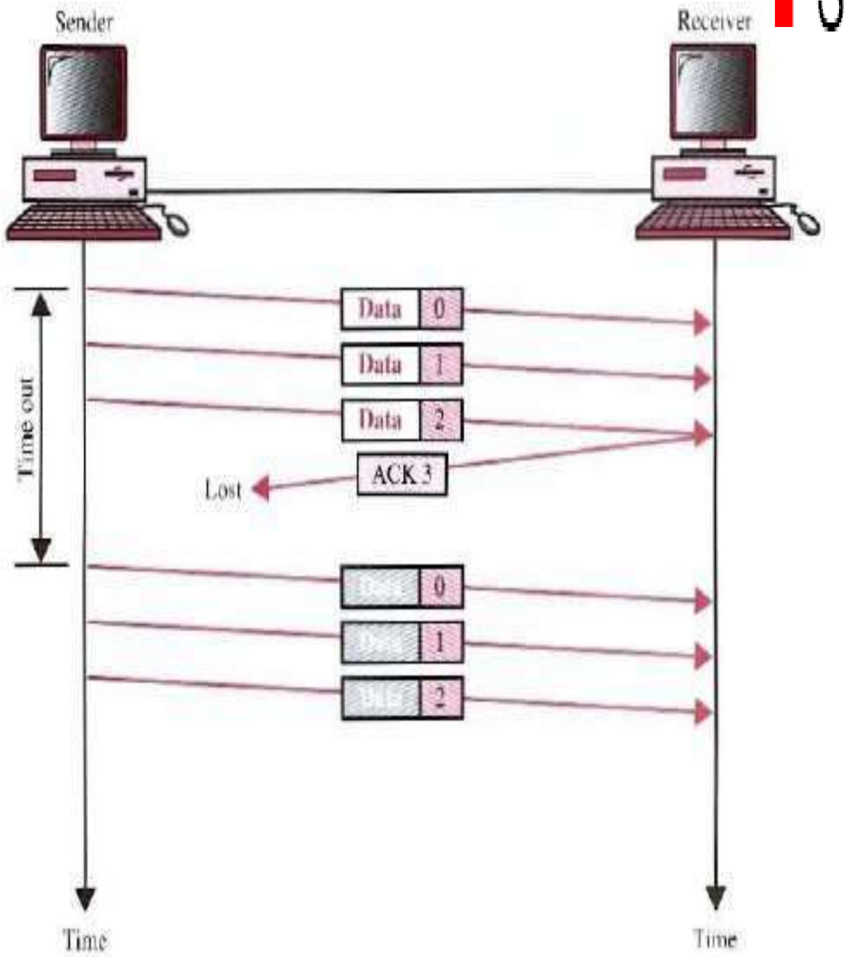
- Go-back-n, corrupted frame case:



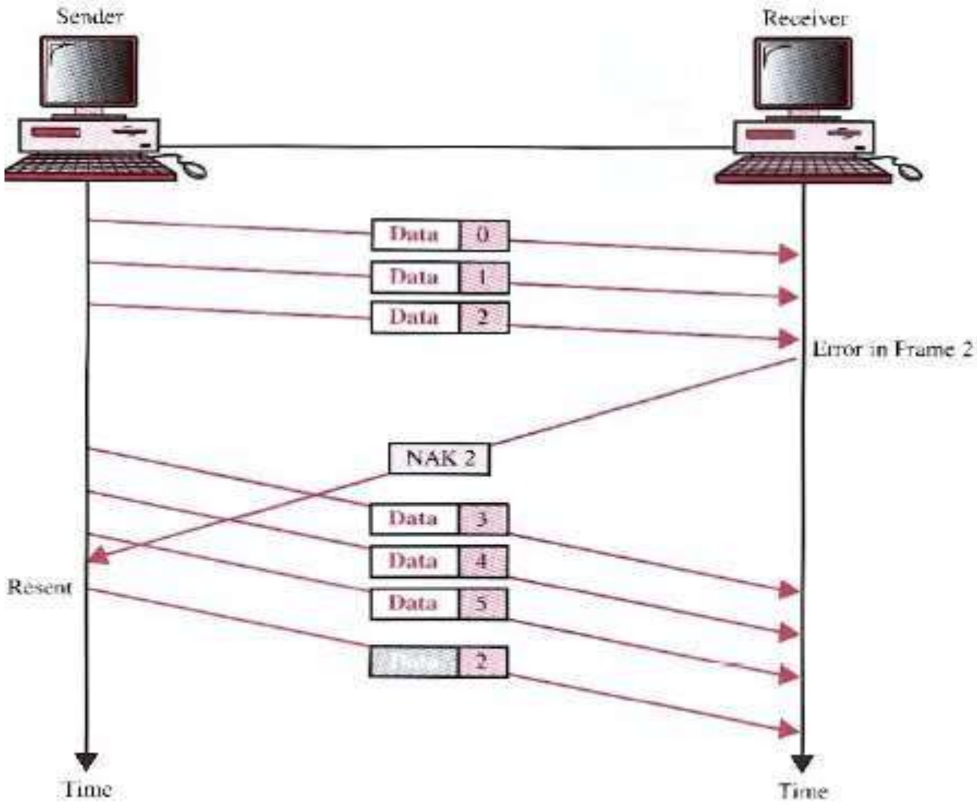
- Go-back-n, lost frame case:



- Go-back-n, lost ACK case:



- Selective-reject, corrupted frame case:



- Selective-reject, lost frame case:
  - Similar to corrupted frame case.
  - Lost frame is only detected after the next frame has been received correctly.
- Selective-reject, lost ACK case:
  - Similar to lost ACK case of go-back-n.
  - All frames from last ACK have to be retransmitted when the timer times out.

- Go-back-n vs. Selective-reject:
  - Selective-reject is expensive due to:
    - The need for extra logic to select specific frame for retransmission.
    - The need to buffer correctly received frames.
    - The complexity of sorting the received frames.
  - Go-back-n is much simpler and more commonly used.

# MAC

- IEEE has subdivided(Project 802) the data link layer into two sub layers:
  - Logical Link Control
  - Medium access control

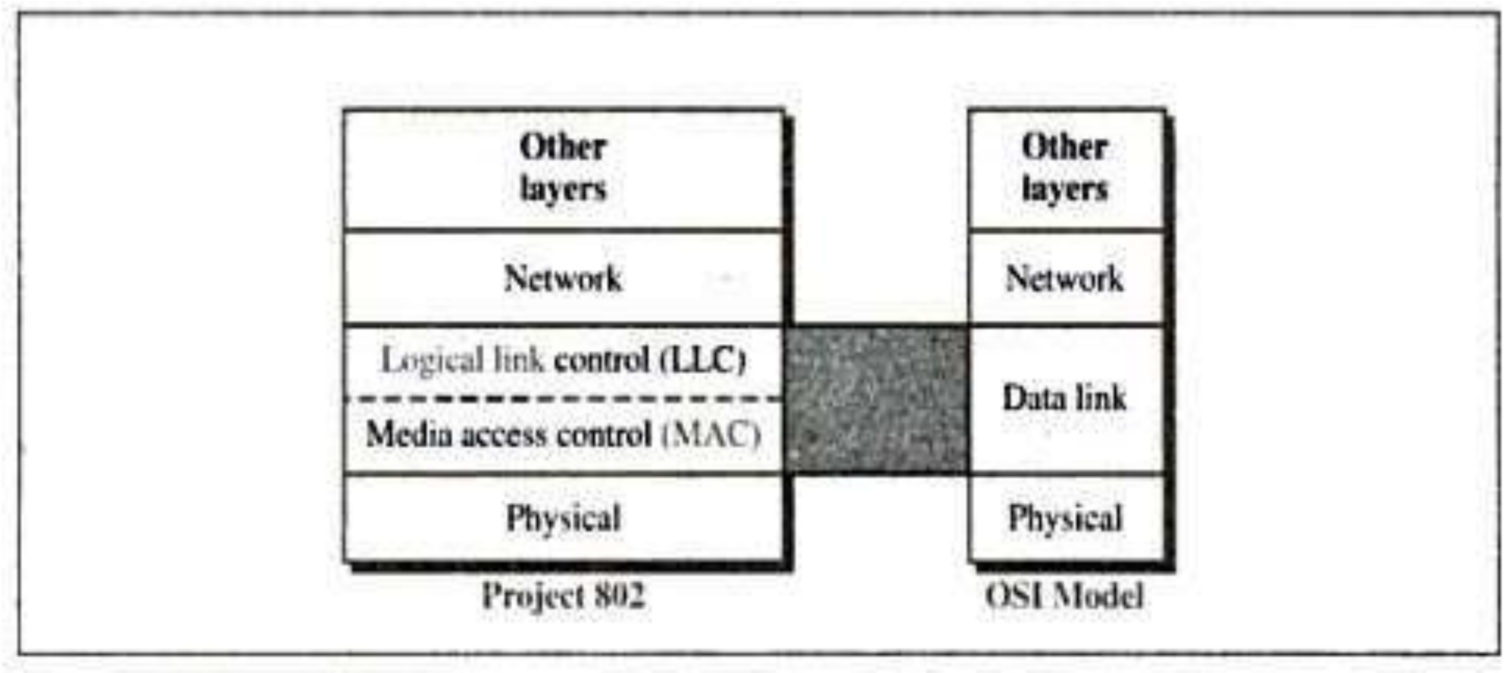
## Functions of MAC

- It resolves the contention of shared media
- It contains all information to move information from one place to another
- It contains the physical address of next station to route packet.
- MAC protocol are specific to LAN

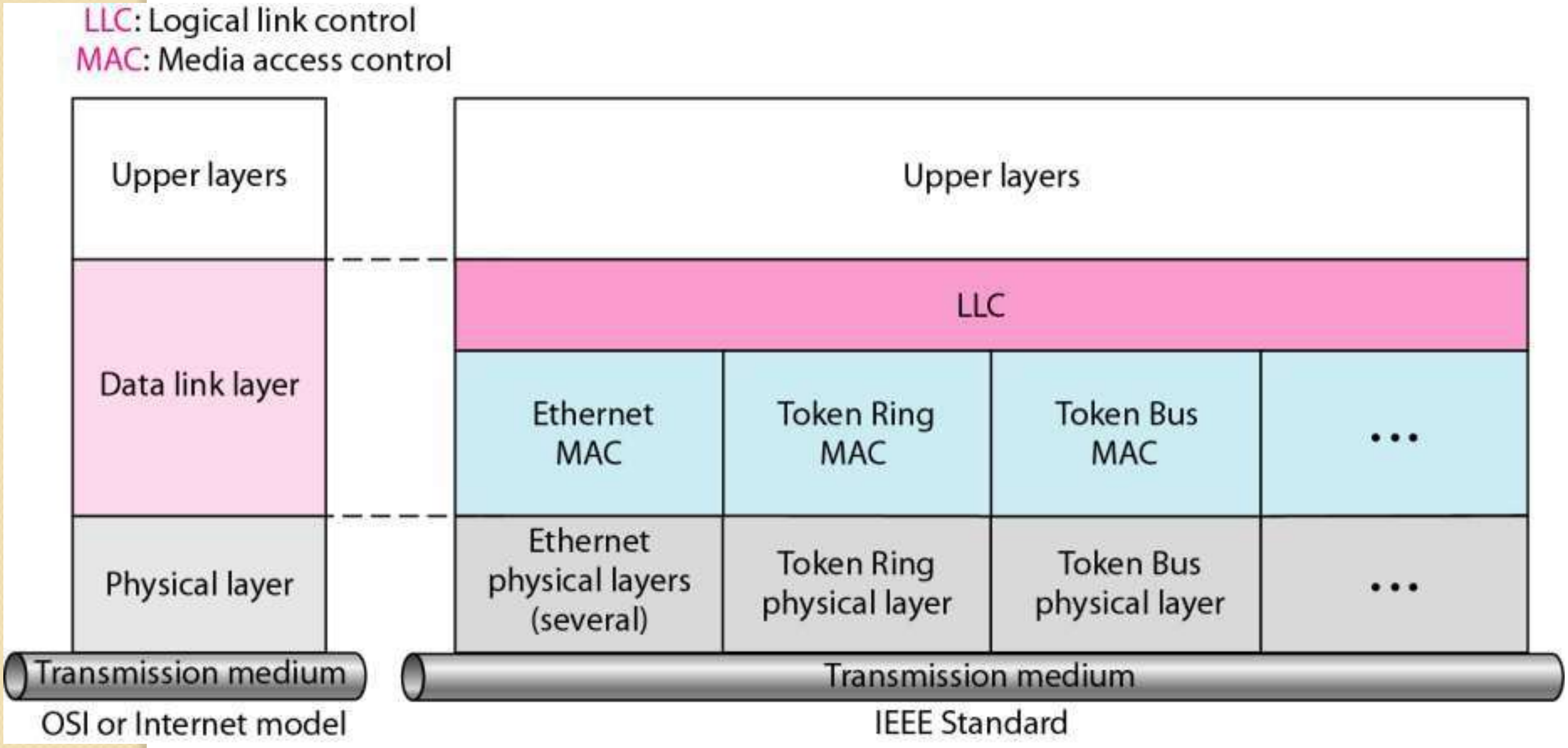
- The project 802 which governs internet working. Here each subdivision is identified by a number
- 802.1(internetworking)
- 802.2(LLC)

and MAC modules

- 802.3(CSMA/CD)
- 802.4(Tokenbus)
- 802.5(Tokenring)



# Figure 13.1 *IEEE standard for LANs*



LLC: Logical link control

MAC: Media access control

Upper layers

Data link layer

Physical layer

Transmission medium

OSI or Internet model

Upper layers

LLC

Ethernet MAC

Token Ring MAC

Token Bus MAC

• • •

Ethernet physical layers (several)

Token Ring physical layer

Token Bus physical layer

• • •

Transmission medium

IEEE Standard

# MAC protocol are specific to LAN

- LAN is a Local Area Network used for communication inside building
- Protocols for LAN are,
  - Ethernet
  - Token Ring
  - Token bus
  - FDDI

# IEEE STANDARDS

Ethernet: It is a LAN protocol that is used in Bus and Star topologies and implements CSMA/CD as the medium access method

- Original (traditional) Ethernet developed in 1980 by three companies: Digital, Intel, Xerox (DIX).

- In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers.
  - Current version is called IEEE Ethernet

- IEEE 802.3 supports LAN standard Ethernet
- IEEE802.3 defines two categories
  - Baseband
  - Broadband
- Base band has five different category
  - 10Base5
  - 10Base2
  - 10BaseT
  - 1Base5 etc.,
- Broad band has a category
  - 10Broad36

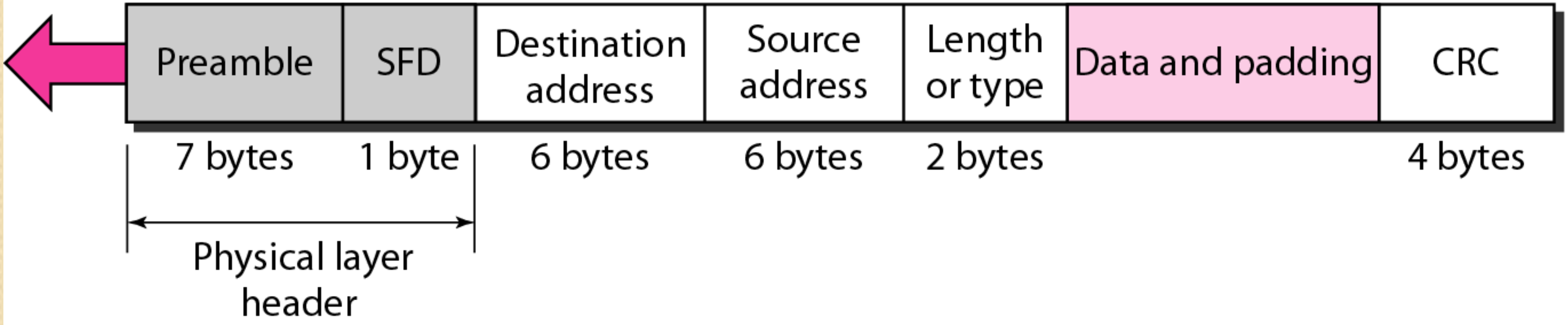
# Access Method:CSMA/CD

- When multiple user access the single line ,there is a danger of signals overlapping and destroying each other(Traffic) .such an overlap is called **Collisions.**
- To avoid this the access method used in Ethernet is carrier sense multiple access/collision detection
- In CSMA any workstation wishing to transmit must listen to existing traffic on the line
- If no voltage is detected ,line is considered idle
- CSMA cuts down the number of collisions, but cant eliminate. Collisions still occur if both station try to listen at a time.

## Figure 13.4 *802.3 MAC frame*

Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



| Preamble | SFD | Destination address | Source address | Length or type | Data and padding | CRC |
|---|---|---|---|---|---|---|
| 7 bytes | 1 byte | 6 bytes | 6 bytes | 2 bytes | | 4 bytes |

# IEEE Ethernet

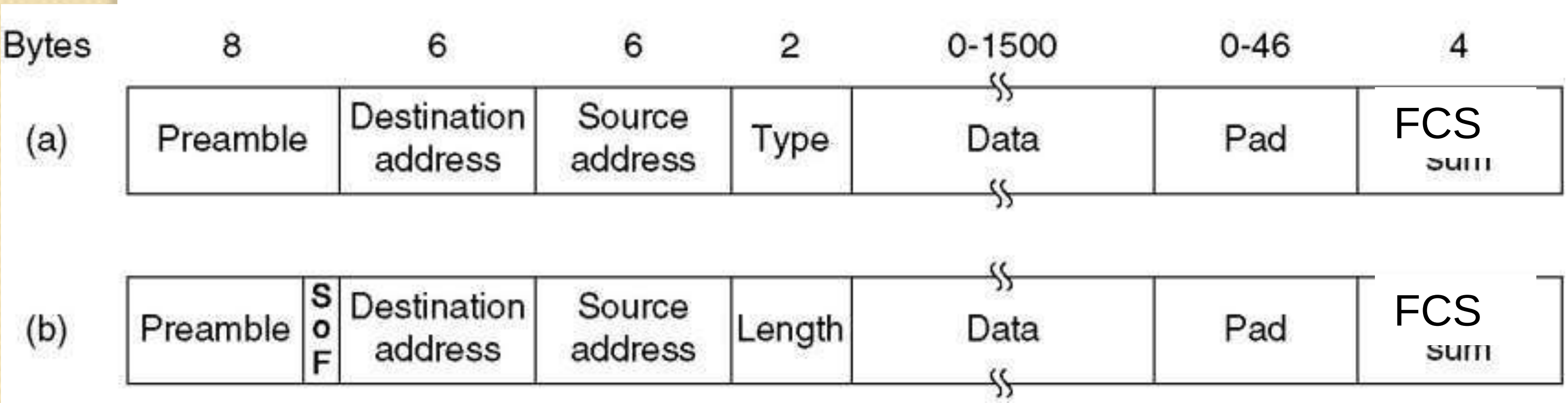
- In IEEE 802.3 Ethernet Data link layer is split into two sublayers:
  - Bottom part: MAC
    - The frame is called **IEEE 802.3**
    - Handles framing, MAC addressing, Medium Access control
    - **Specific implementation for each LAN p**rotocol
      - Defines **CSMA/CD** as the access method for Ethernet LANs and **Token passing** method for Token Ring.
    - Implemented in **hardware**
  - Top part: LLC (Logical Link Control)
    - The subframe is called **IEEE 802.2**
    - Provides **error and flow control** if needed
    - It makes the MAC sublayer transparent
      - Allows interconnectivity between different LANs data link layers
    - Used to multiplex multiple network layer protocols in the data link layer frame
    - Implemented in **software**

# Ethernet Provides Unreliable, connectionless Service

- **Ethernet data** link layer protocol provides **connectionless service** to the network layer
  - No handshaking between sending and receiving adapter.
- **Ethernet protocol provides *Unreliable* service to the network layer :**
  - Receiving adapter doesn't send ACK or NAK to sending adapter
  - This means stream of datagrams passed to network layer can have gaps (missing data)
    - Gaps will be filled if application is using reliable transport layer protocol
      - Otherwise, application will see the gaps

# Ethernet

- Ethernet Frame format



| Bytes | 8 | 6 | 6 | 2 | 0-1500 | 0-46 | 4 |
|---|---|---|---|---|---|---|---|
| (a) | Preamble | Destination address | Source address | Type | Data | Pad | FCS<br>sum |
| (b) | Preamble<br>SoF | Destination address | Source address | Length | Data | Pad | FCS<br>sum |

Frame formats. **(a) DIX Ethernet ,(b) IEEE 802.3.**

# Ethernet Frame

PREAMBLE

- 8 bytes with pattern 10101010 used to synchronize receiver, sender clock rates.
- In IEEE 802.3, eighth byte is start of frame (10101011)

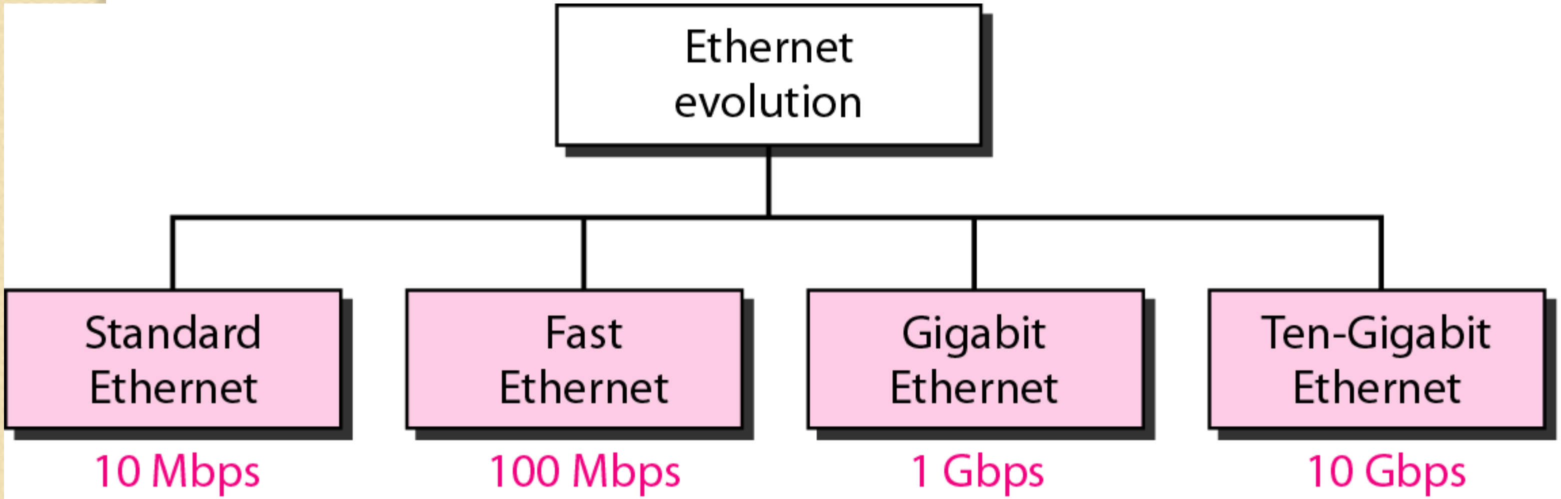
- Addresses: 6 bytes (explained latter)
- Type (DIX)
  - Indicates the type of the **Network layer protocol** being carried in the **payload (data)** field, **mostly IP** but others may be supported such as IP (**0800**), Novell IPX (**8137**) and AppleTalk (**809B**), ARP (**0806**) )
  - Allow **multiple network layer** protocols to be supported on a single machine (multiplexing)
  - Its value starts at **0600h (=1536 in decimal)**
- Length (IEEE 802.3): number of bytes in the **data field**.
  - Maximum 1500 bytes **(= 05DCh)**
- CRC: checked at receiver, if error is detected, the frame is **discarded**
  - CRC-32
- Data: carries data encapsulated from the upper-layer protocols
- Pad: Zeros are added to the data field to make the **minimum data length = 46 bytes**

# Ethernet address

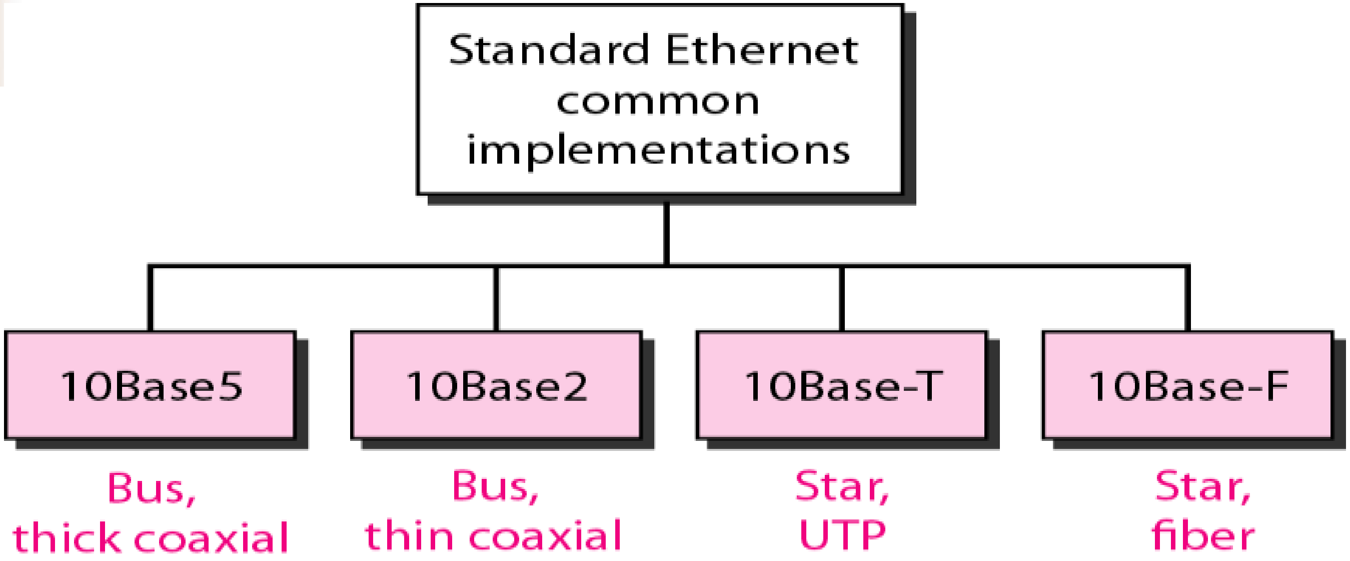
06-01-02-01-2C-4B

- Six bytes = 48 bits
- Flat address not hierarchical
- Burned into the NIC ROM
- First three bytes from left specify the vendor. Cisco 00-00-0C, 3Com 02-60-8C and the last 24 bit should be created uniquely by the company
- Destination Address can be:
  - Unicast: second digit from left is even (one recipient)
  - Multicast: Second digit from left is odd (group of stations to receive the frame – conferencing applications)
  - Broadcast (ALL ones) (all stations receive the frame)
- Source address is always Unicast

Figure 13.3 *Ethernet evolution through four generations*



# Categories of traditional Ethernet



Standard Ethernet common implementations

10Base5

Bus, thick coaxial

10Base2

Bus, thin coaxial

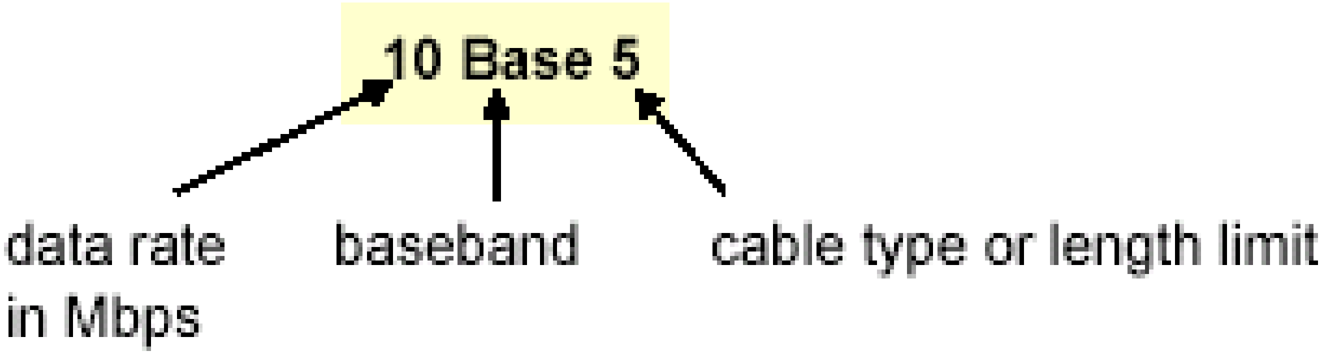
10Base-T

Star, UTP

10Base-F

Star, fiber

- <data rate><Signaling method><Max segment length or cable type>



10 Base 5

data rate in Mbps

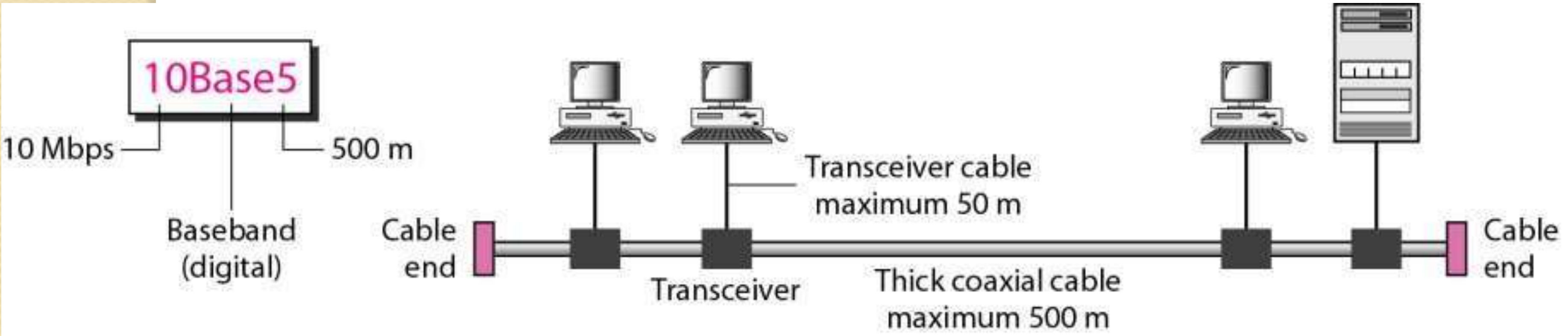
baseband

cable type or length limit

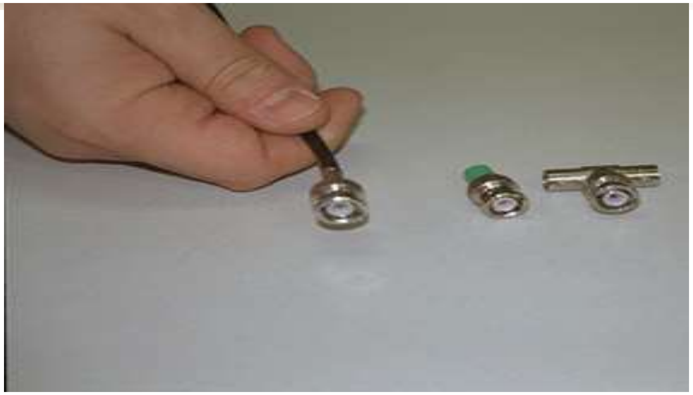
# IEEE 802.3 Cable Types

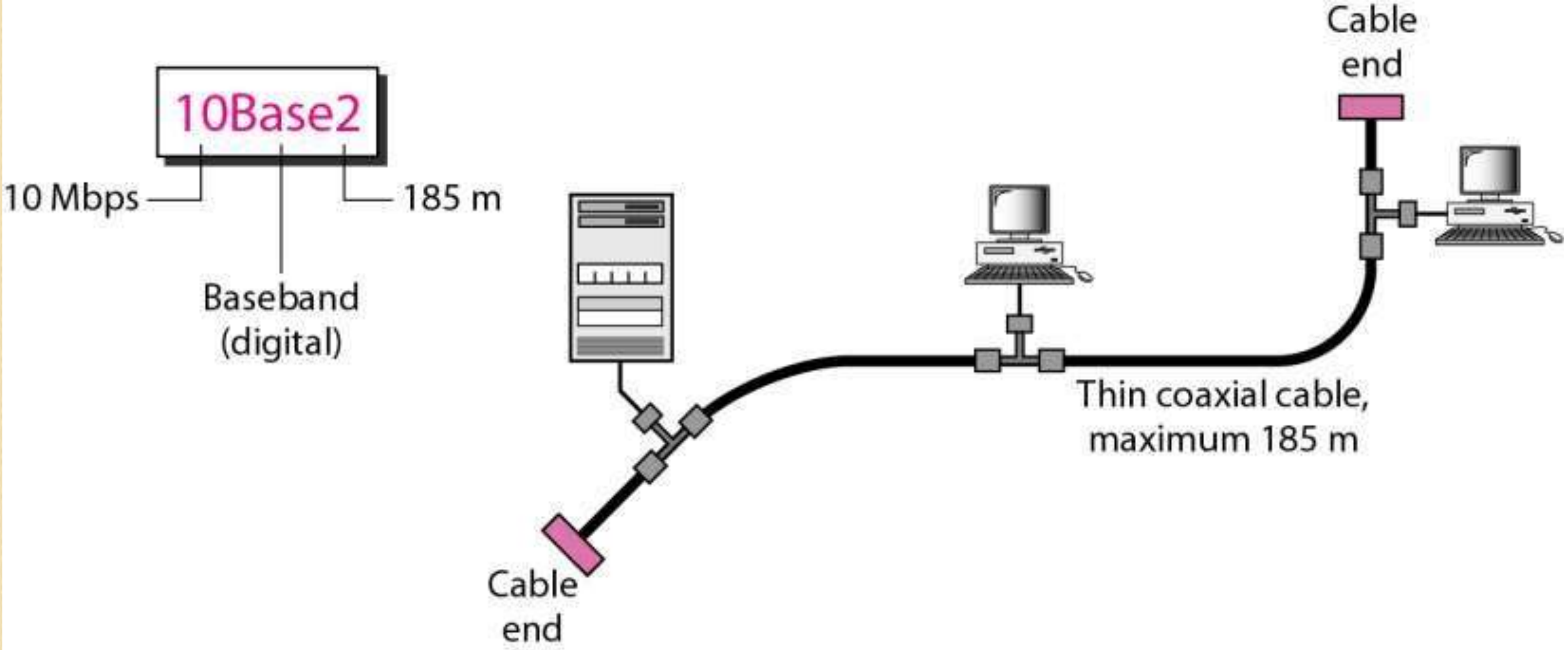
| **Name** | **Cable Max.** | **Max Cable Segment Length** | **Nodes /segment** | Toplogy |
|---|---|---|---|---|
| 10Base5 | thick coax | 500 meters | 100 | Bus |
| 10Base2 | thin coax | 185 meters | 30 | Bus |
| 10BaseT | twisted pair | 100 meters | 1 | Star |
| 10BaseF | Fiber Optic | 2Km | 1 | Star |

## Figure 13.10 *10Base5 implementation*



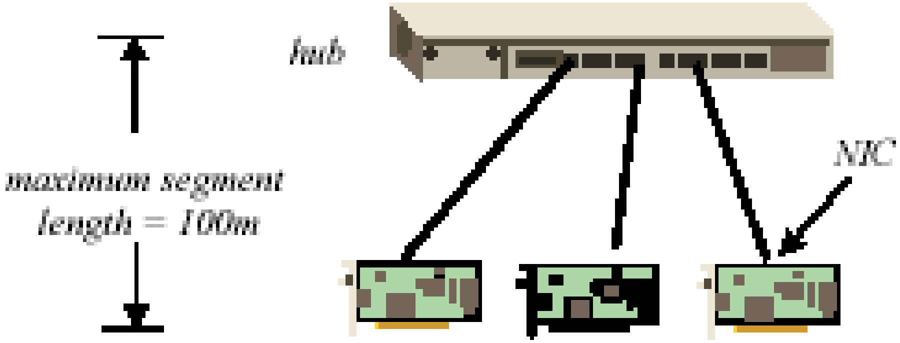
Connection of stations to the medium using 10Base2



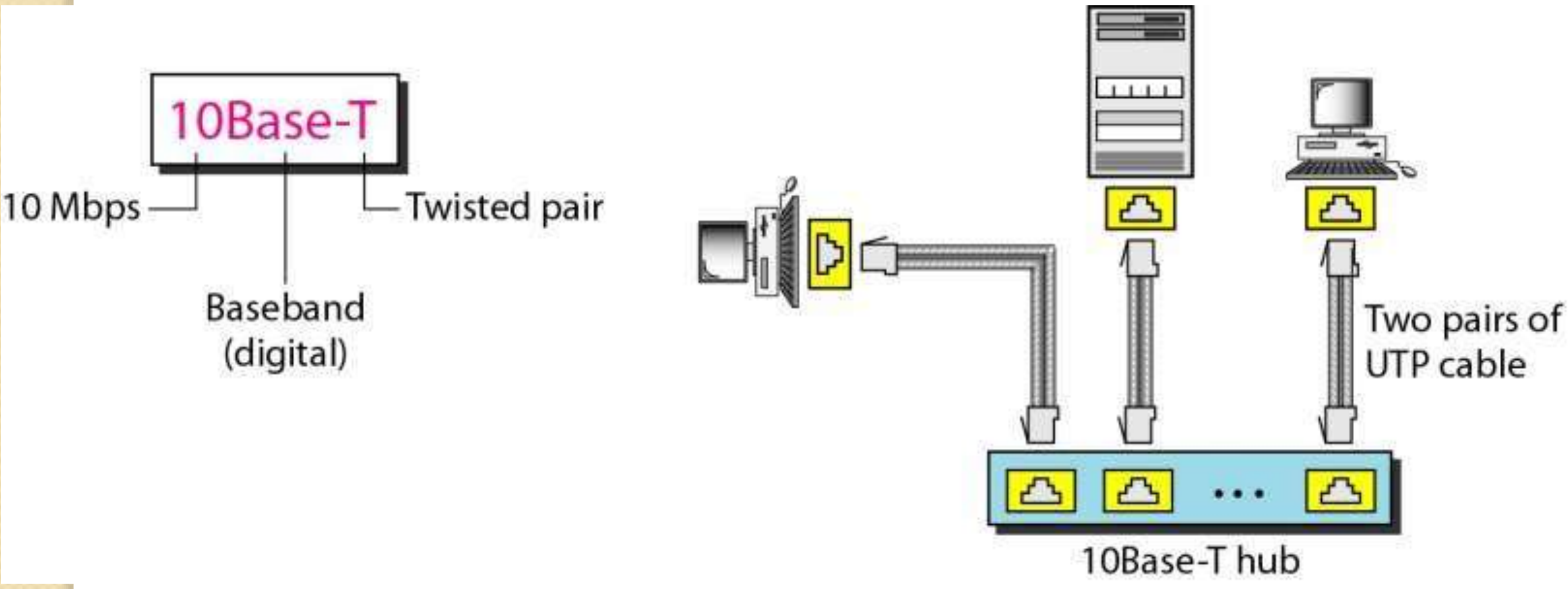


# 10BaseT

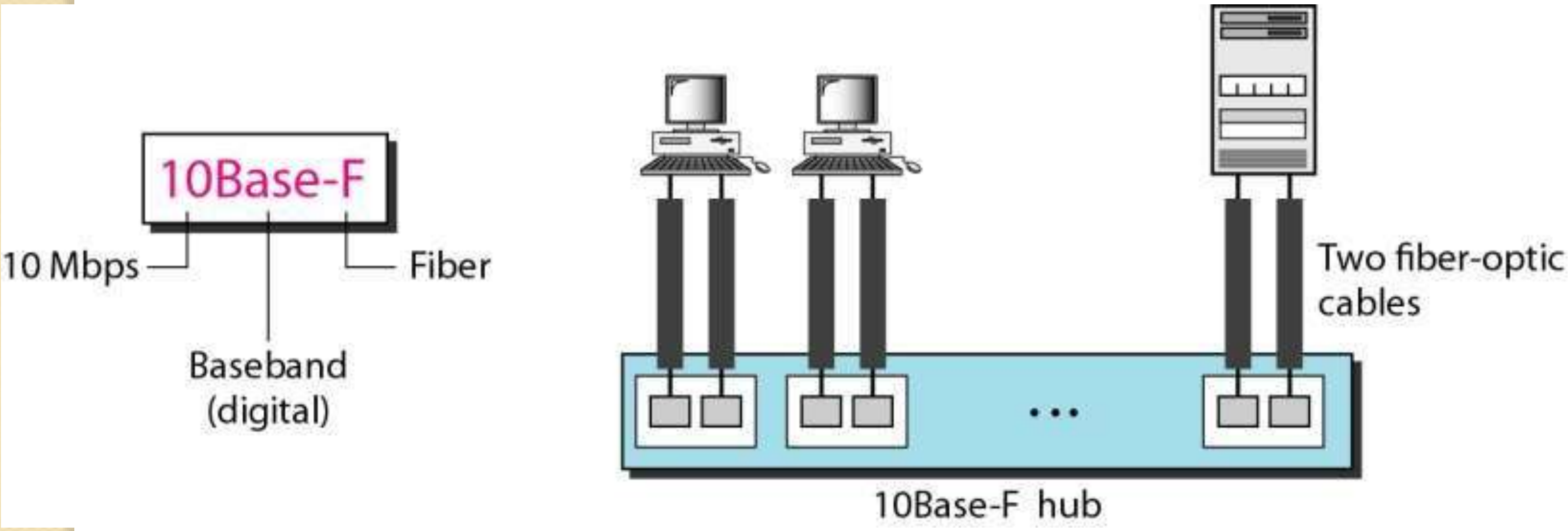
- Uses twisted pair Cat3 cable
- Star-wire topology
- A hub functions as a repeater with additional functions
- Fewer cable problems, easier to troubleshoot than coax
- Cable length at most 100 meters



## Figure 13.12 *10Base-T implementation*

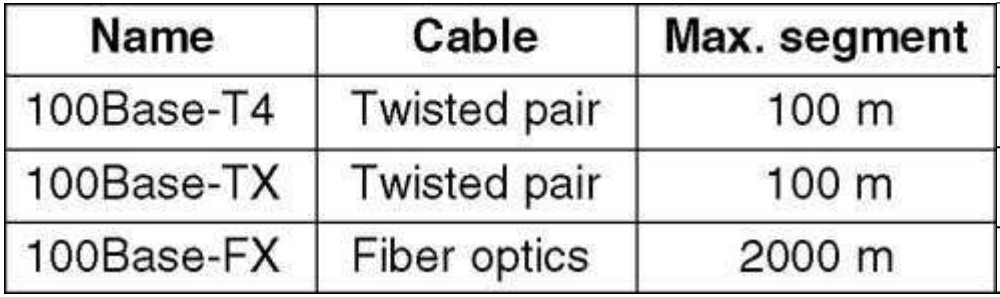


## Figure 13.13 *10Base-F implementation*



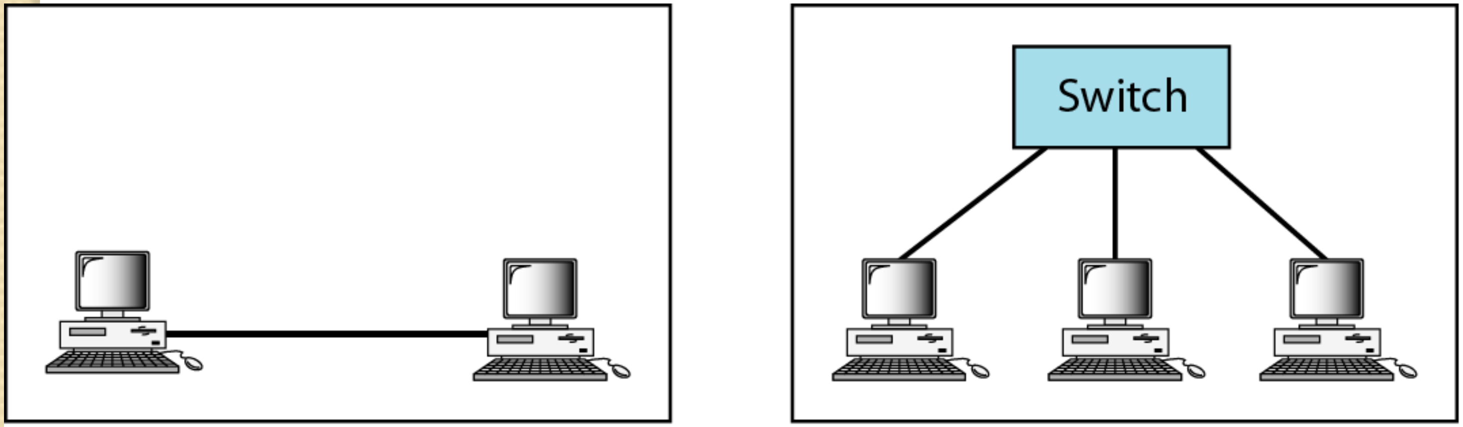
# Fast Ethernet

- 100 Mbps transmission rate
- same frame format, media access, and collision detection rules as 10 Mbps Ethernet
- can **combine 10 Mbps** Ethernet and Fast Ethernet on same network using a ***switch***
- media: twisted pair (CAT 5) or fiber optic cable (no coax)
- Star-wire topology
  - Similar to 10BASE-T



| Name | Cable | Max. segment | |
|---|---|---|---|
| 100Base-T4 | Twisted pair | 100 m | CAT 3 |
| 100Base-TX | Twisted pair | 100 m | CAT 5 |
| 100Base-FX | Fiber optics | 2000 m | |

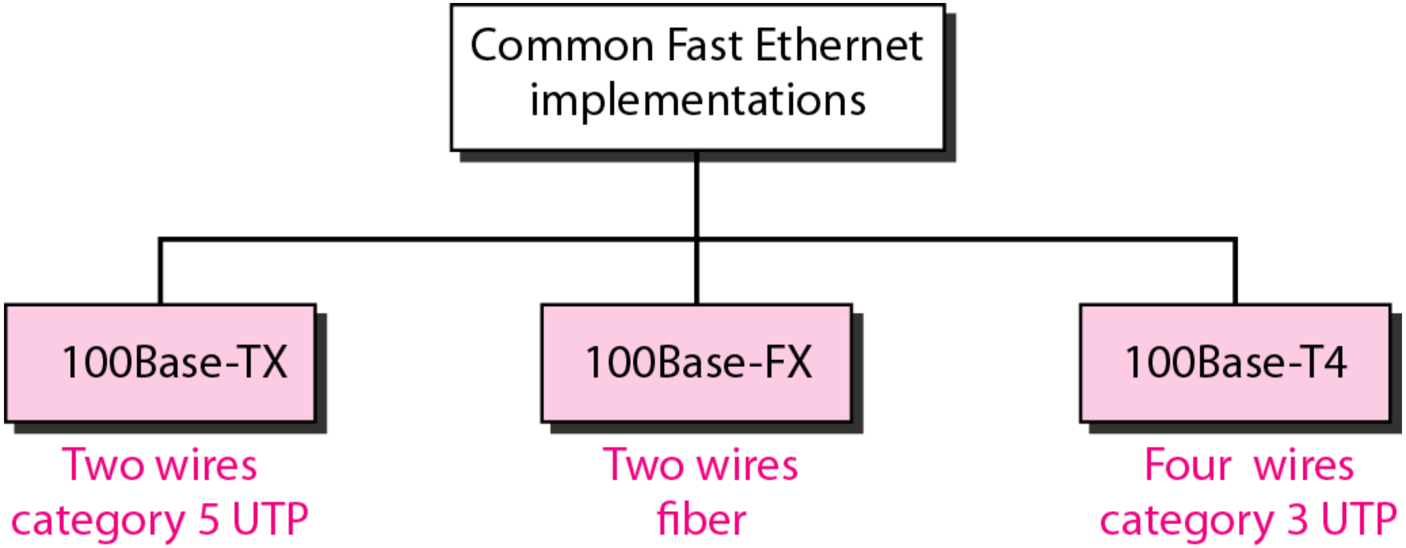
# Figure 13.19 *Fast Ethernet topology*



a. Point-to-point

b. Star

## Figure 13.20 *Fast Ethernet implementations*



Common Fast Ethernet implementations

100Base-TX

Two wires
category 5 UTP

100Base-FX

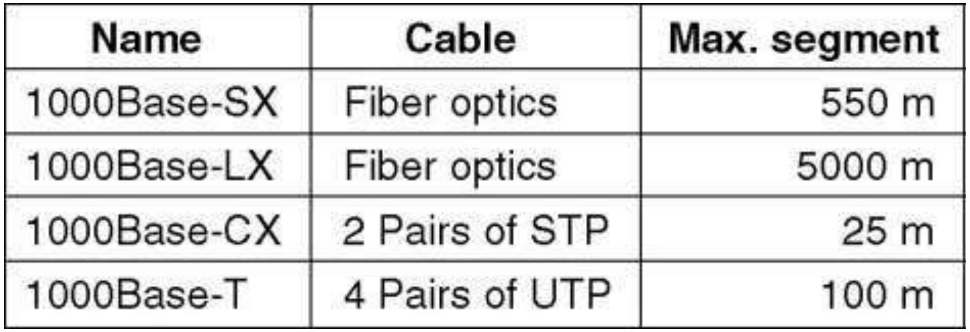
Two wires
fiber

100Base-T4

Four wires
category 3 UTP

# Gigabit Ethernet

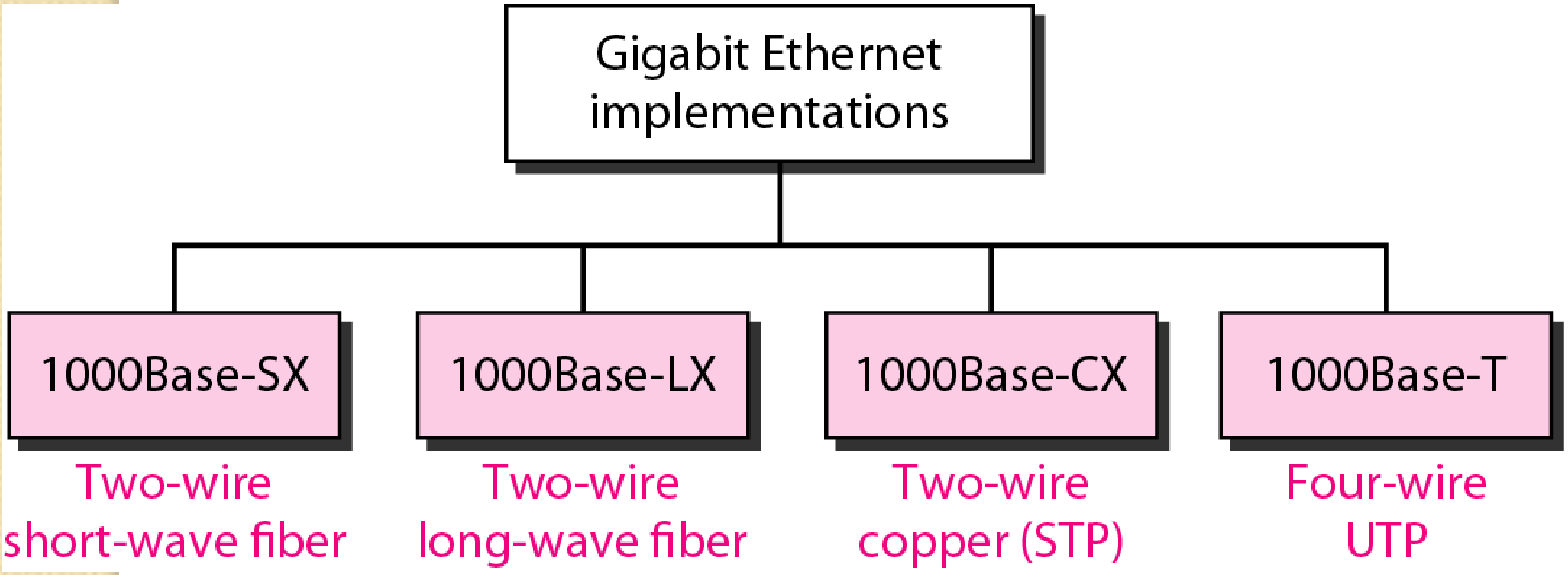
- Speed 1Gpbs
- Minimum frame length is 512 bytes
- Operates in full/half duplex modes mostly full duplex



| Name | Cable | Max. segment |
|---|---|---|
| 1000Base-SX | Fiber optics | 550 m |
| 1000Base-LX | Fiber optics | 5000 m |
| 1000Base-CX | 2 Pairs of STP | 25 m |
| 1000Base-T | 4 Pairs of UTP | 100 m |

In the full-duplex mode of Gigabit Ethernet, there is no collision;
the maximum length of the cable is determined  by the signal attenuation
in the cable.

## Figure 13.23 *Gigabit Ethernet implementations*



# 10Gbps Ethernet

- Maximum link distances cover 300 m to 40 km
- Full-duplex mode only
- No CSMA/CD
- Uses optical fiber only

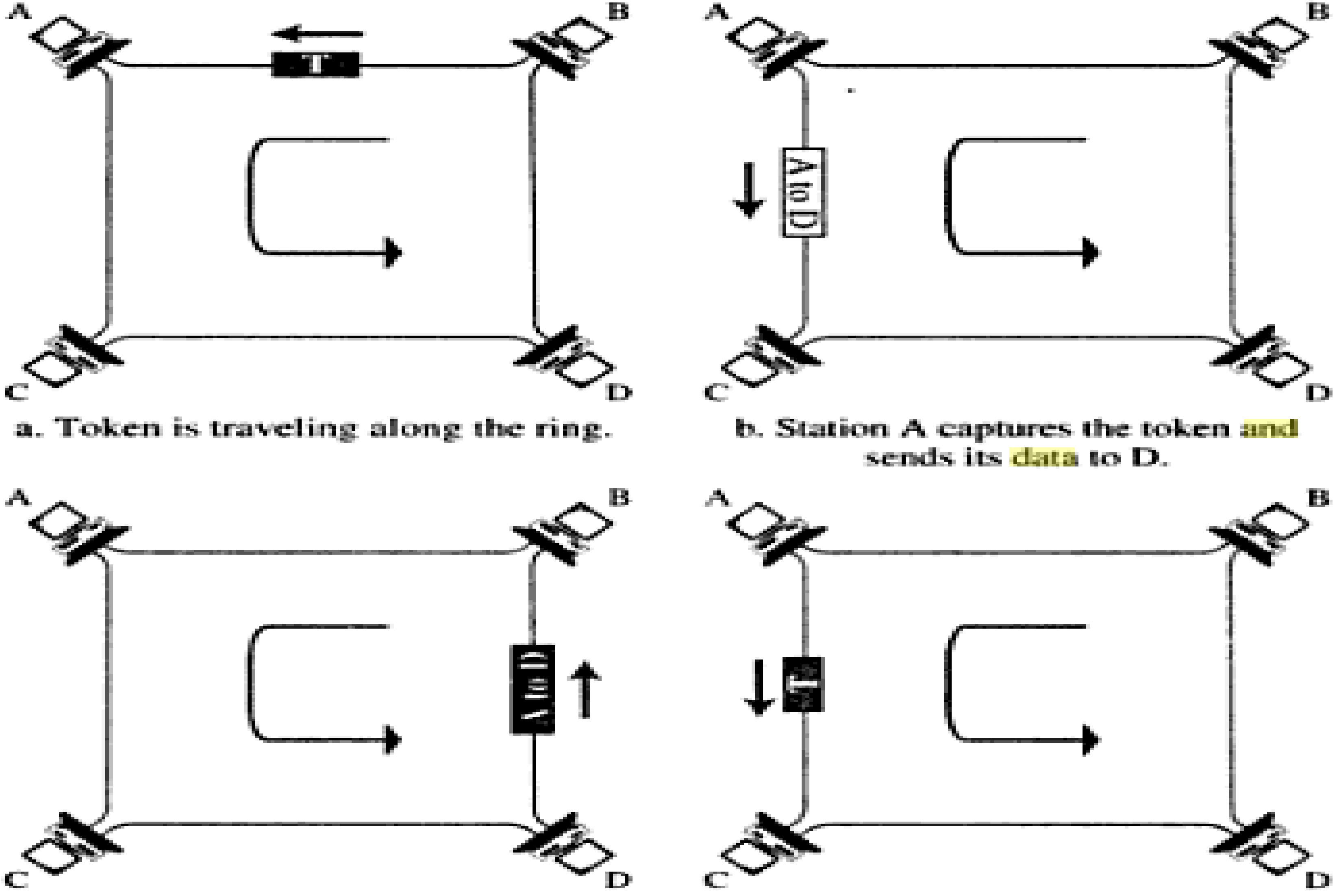
# Token Ring

- It allows each station to sent one frame .
- The access control mechanism used by Ethernet is inefficient sometimes because of collision.
- It solves the collision problem by passing token
- Initially a station waits for token, if a token is free the station may send a data frame

# Cont..,

- This frame proceeds around the ring ,being regenerated by each station .Each station examines the destination address finds the frame is addressed to another station and relays it to its neighbor.
- The intended recipient recognizes its own address and copies the message and set the address bit
- The token finally reach the sender and it recognizes that the data is delivered through address bit
- Token is passed from NIC to NIC

# Token Ring



a. Token is traveling along the ring.

b. Station A captures the token and sends its data to D.

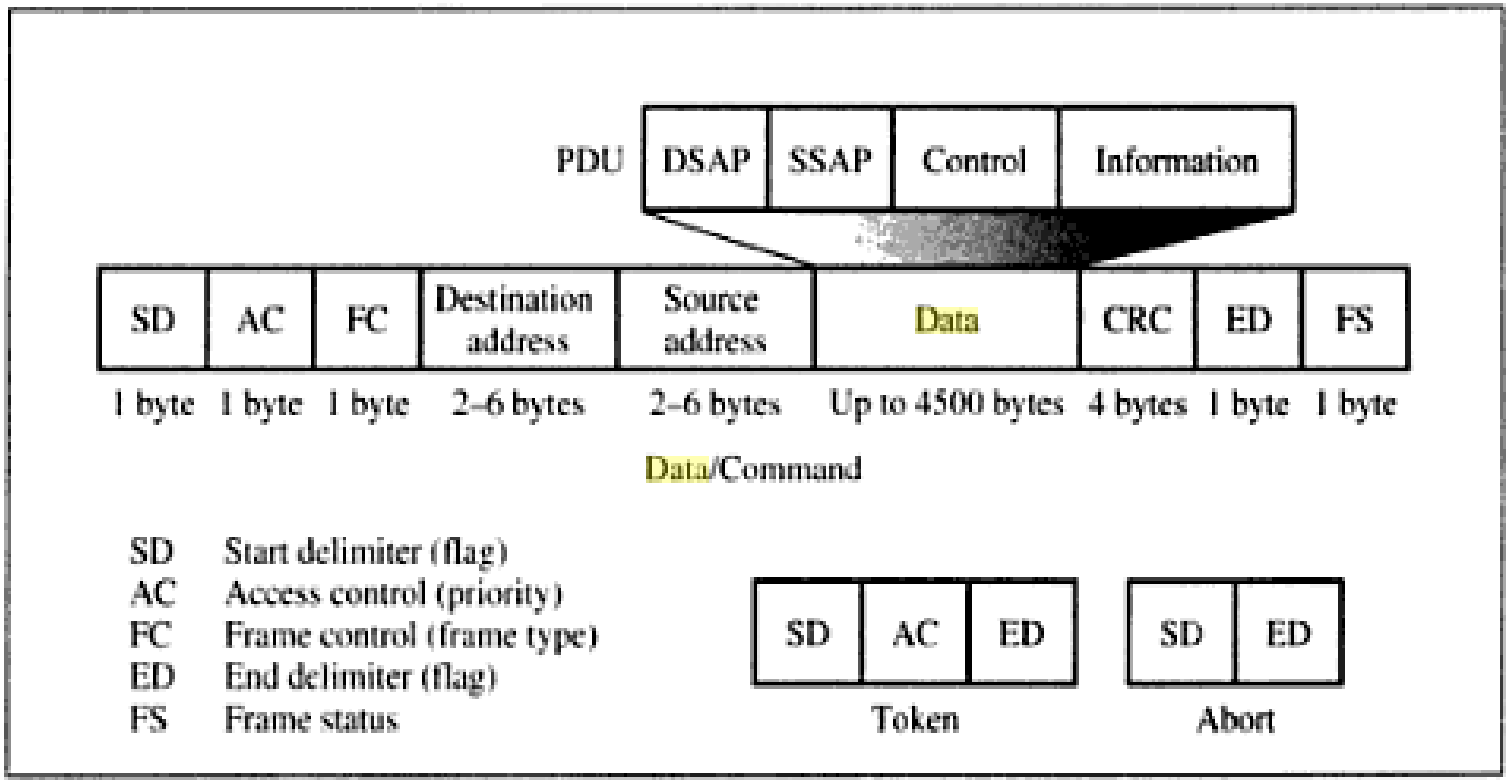
c. Station D copies the frame and sends the data back to the ring.

d. Station A receives the frame and releases the token.

# Token Bus

- It combines the feature of token ring and Ethernet

**Figure 12.22** *Token Ring frame*

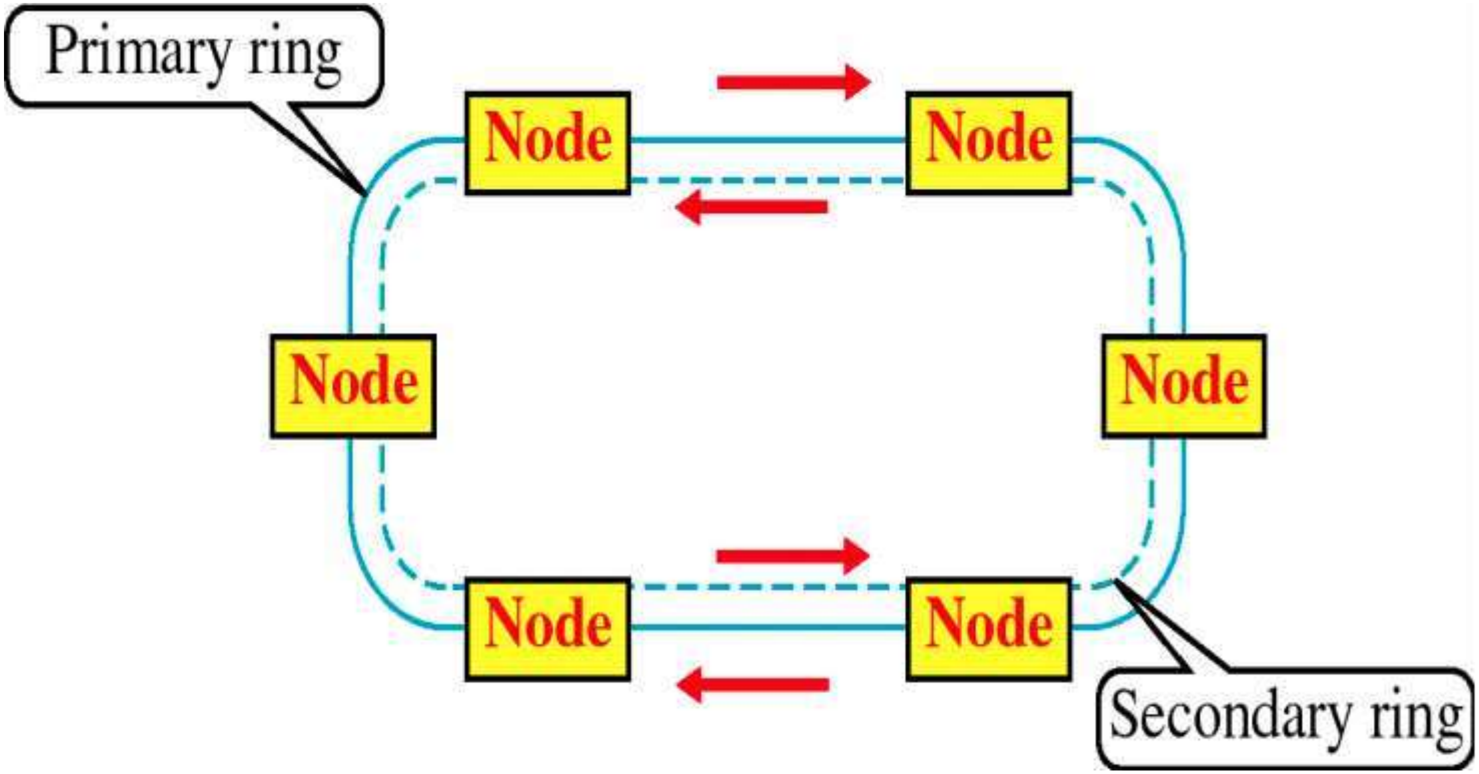


SD Start delimiter (flag)
AC Access control (priority)
FC Frame control (frame type)
ED End delimiter (flag)
FS Frame status

# FDDI

- Fiber Distributed Data Interface
- local area network protocol standardized by  ANSI
- 100-Mbps token passing
- Dual-ring LAN
- A high-speed backbone technology
- High bandwidth
- Optical fiber transmission
- Allows up to 1000 stations

# FDDI Architecture

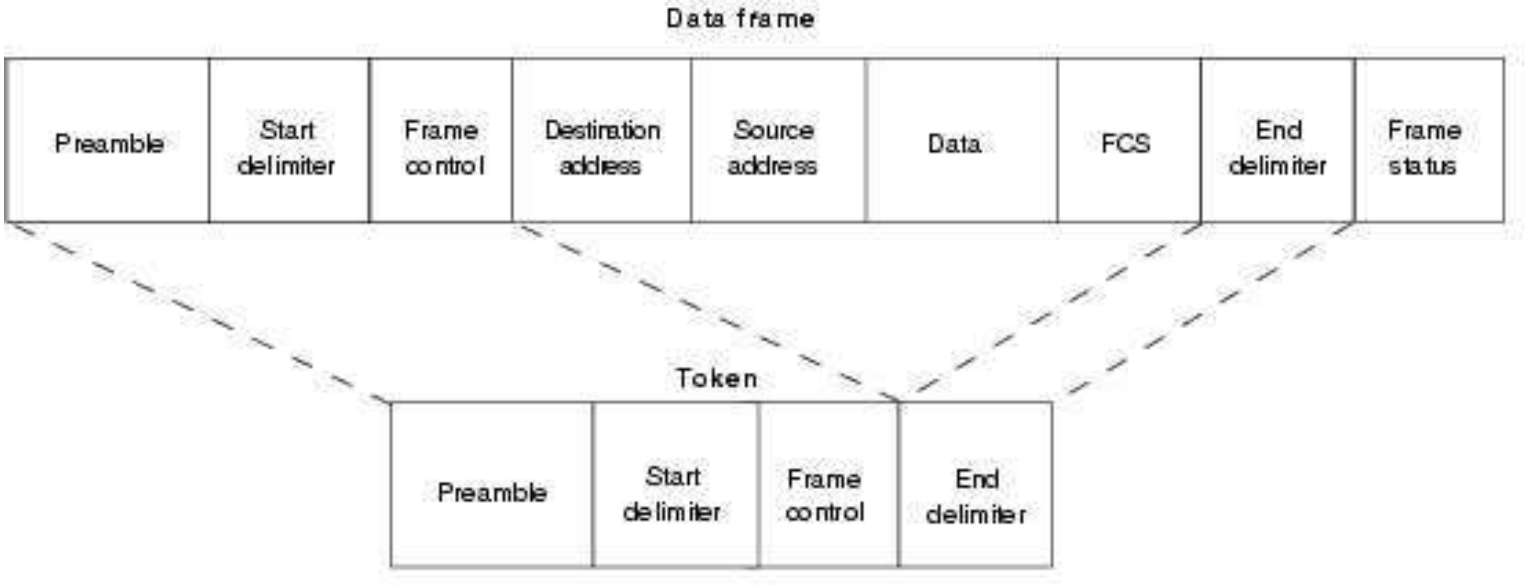


# Components of FDDI

- Fiber optic cable
- A concentrator (ring)
- Stations: 2 types
  - DAS (Dual Attachment Station) or Class A:
    - Connected to both the rings
  - SAS (Single Attachment Station) or Class B:
    - Connected to primary ring

# FDDI Frame Format

Similar to token ring frame

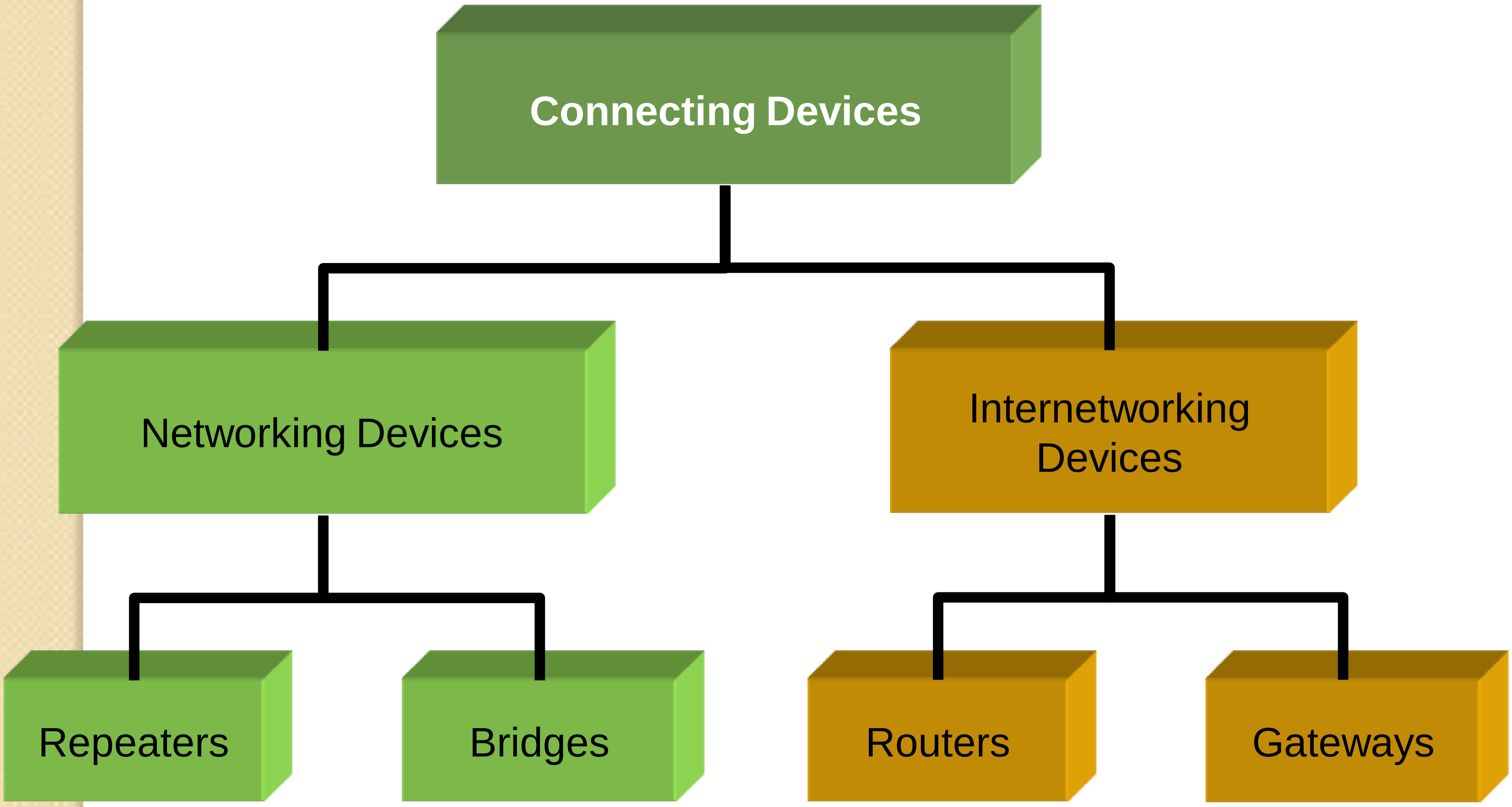


# Networking and internetworking devices:

- An internet is a interconnection of individual network. So to create a internet we need a internetworking devices. ie) Linking a number of LAN's
- Internet - WWW
- internet-Interconnection of LAN

# Why Interconnect?

- To separate / connect one corporate division with another.
- To connect two LANs with different protocols.
- To connect a LAN to the Internet.
- To break a LAN into segments to relieve traffic congestion.
- To provide a security wall between two different types of users.



Connecting Devices

Networking Devices

Internetworking Devices

Repeaters

Bridges

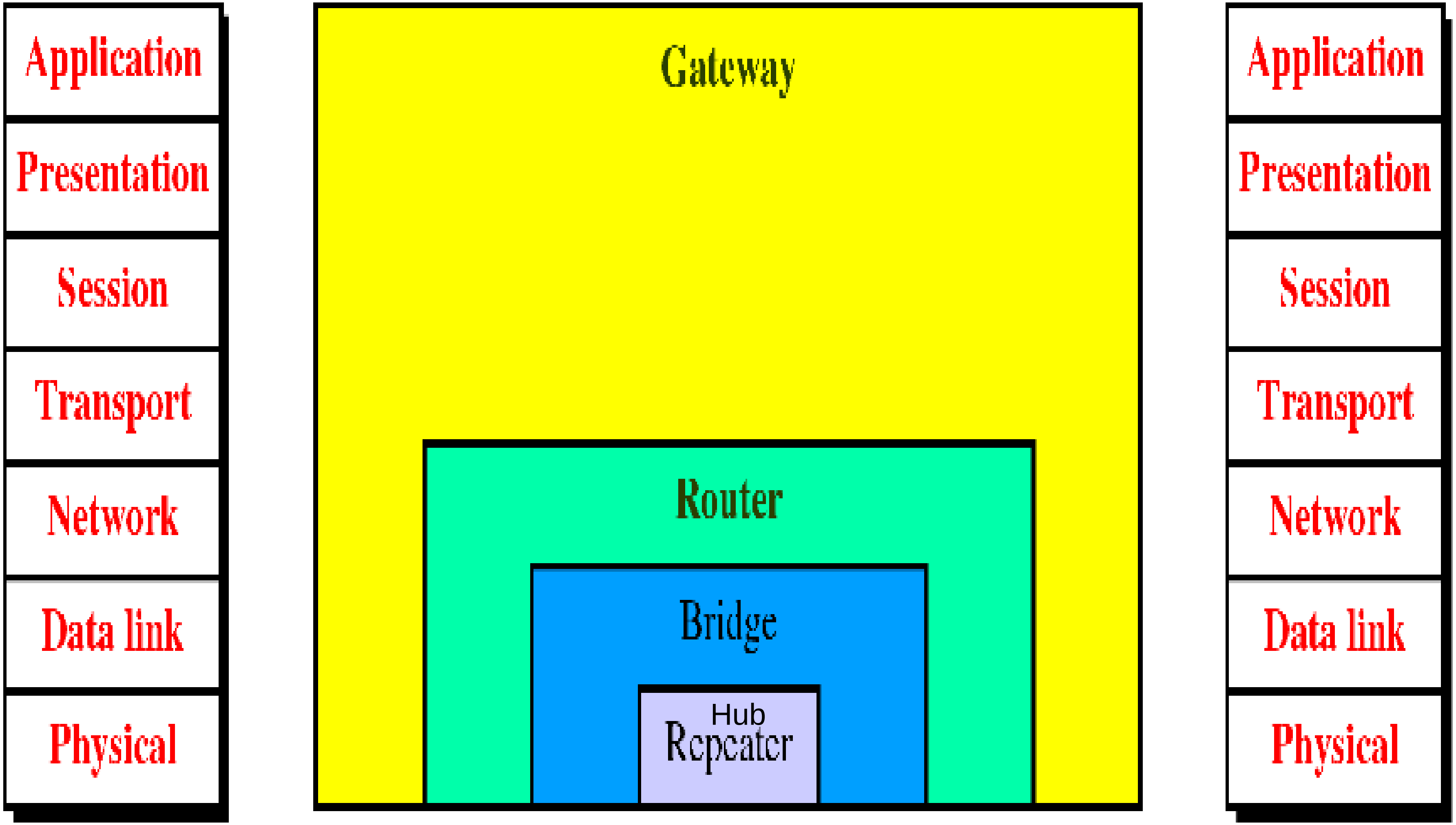
Routers

Gateways

# Introduction

- Many times it is necessary to connect a local area network to another local area network or to a wide area network.
- Local area network to local area network connections are usually performed with a **bridge.**
- Local area network to wide area network connections are usually performed with a **router.**
- A third device, the **switch**, can be used to interconnect segments of a local area network.

# Connecting Devices



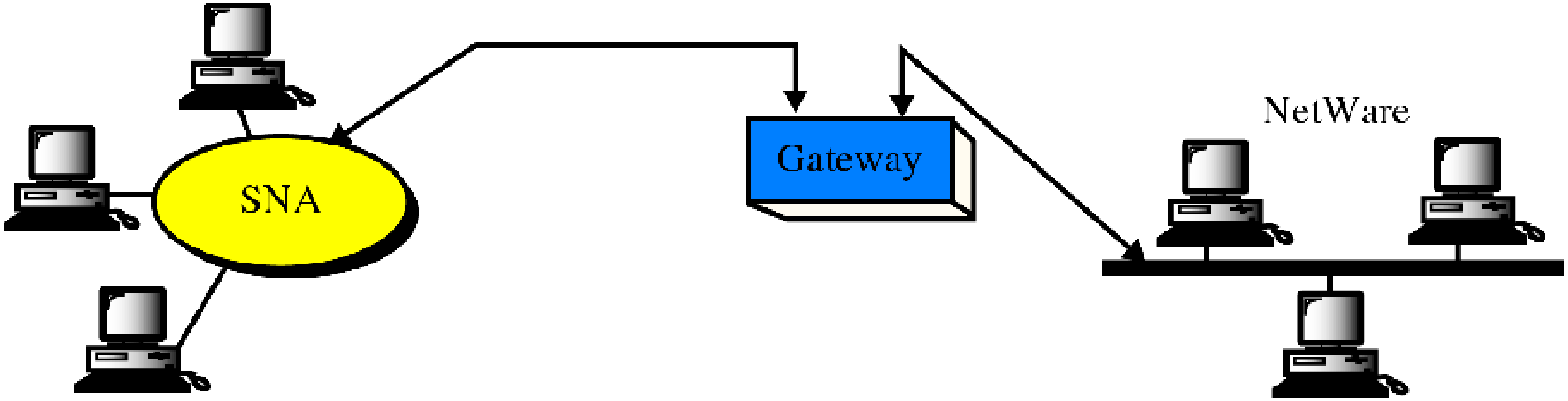
# Repeater:

- A repeater is a regenerator, not an amplifier
- A repeater installed on a link receives the signal before it becomes too weak or corrupted ,regenerates the original bit pattern, and put the refreshed copy back onto the link.

# Gateways:

- A gateway is a protocol convertor.
- It accepts a packet format for one protocol(e.g., Apple Talk) and converts it into a packet format for another protocol(e.g.,TCP/IP).

# A gateway



SNA network (IBM)
Netware network (Novell)

# Bridges

- □ Divide a large network into smaller segment
- □ It filters the traffic . It contains logic(Bridge table) that allows them to keep the traffic for each segment separate.
- □ Ie) Isolating and controlling the link problems (e.g. congestion)
- □ Bridges have look-up table that contains physical address of every station connected to it.

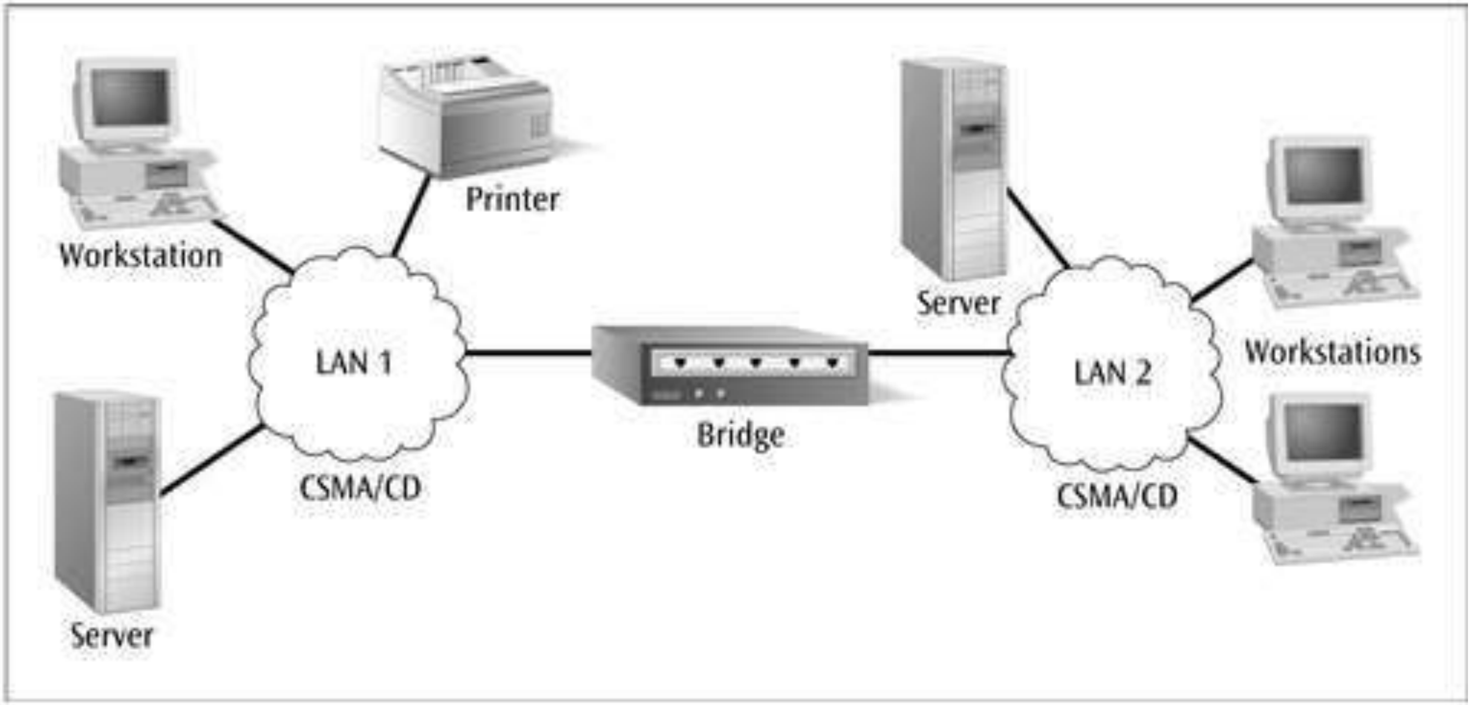
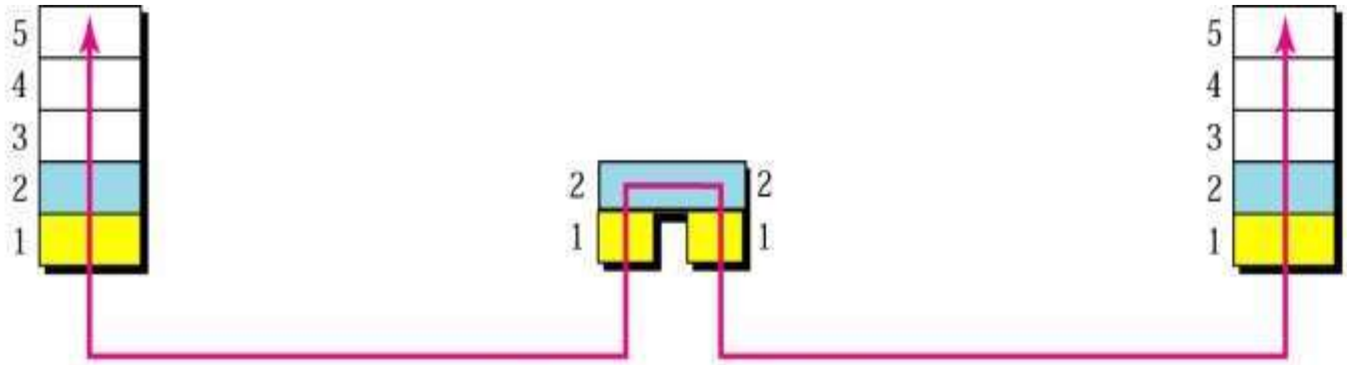


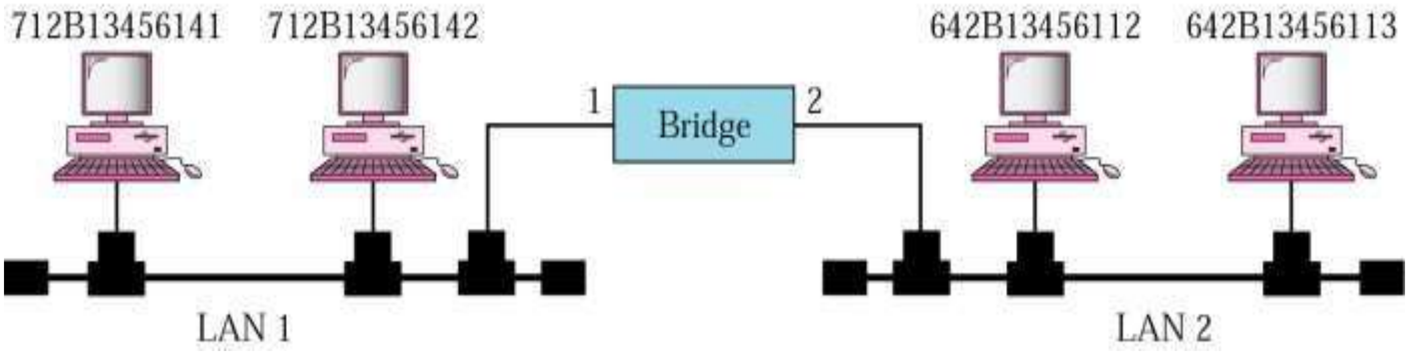
**Figure 8-2**
*A bridge interconnecting two identical local area networks*

# Bridge



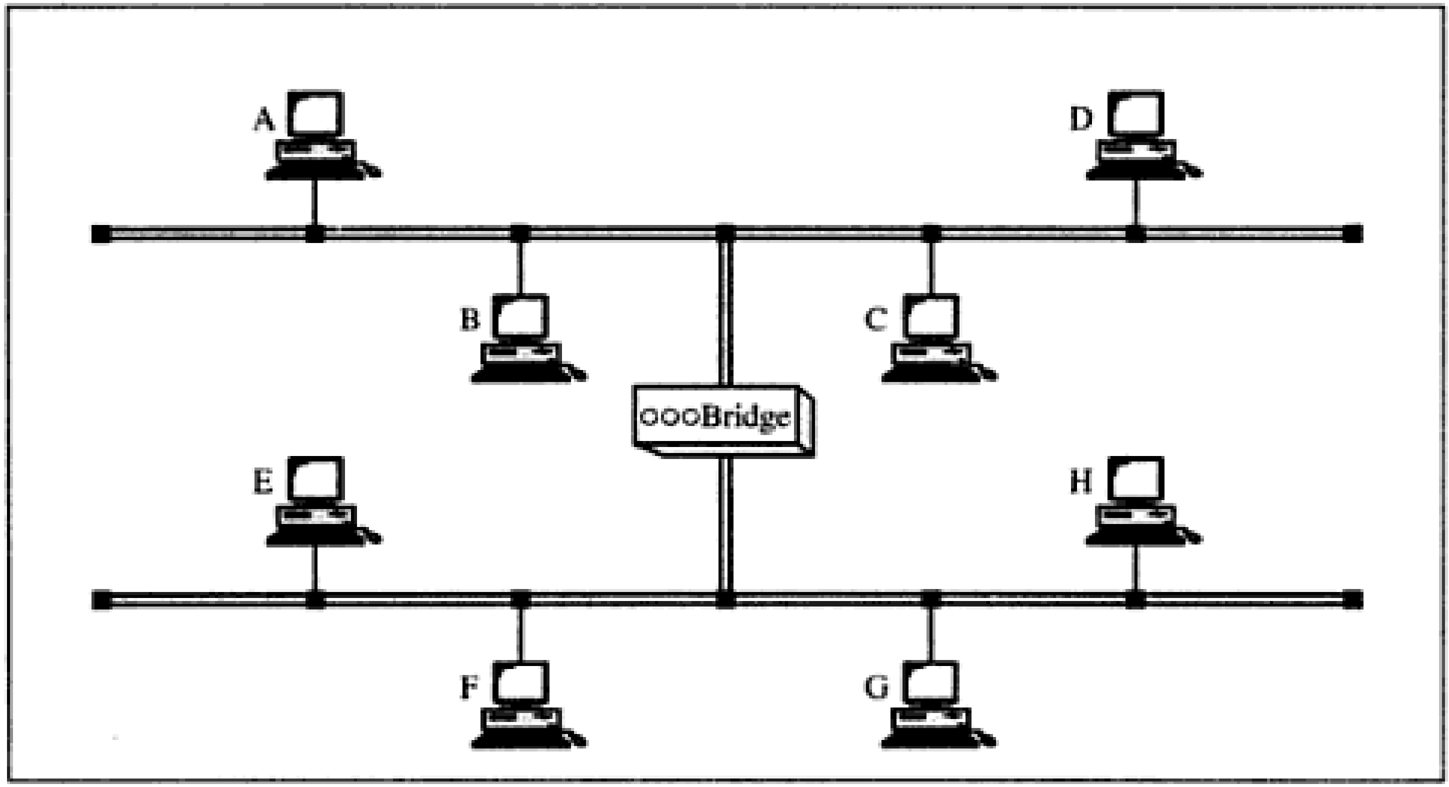
| Address | Port |
|---|---|
| 712B13456141 | 1 |
| 712B13456142 | 1 |
| 642B13456112 | 2 |
| 642B13456113 | 2 |

Bridge Table



- When a frame enters a bridge ,it checks the address of the destination and forward the new copy only to the segment to which the address which belongs

**Figure 21.7** *A bridge*



# Types

- Simple
- Multiport
- Transparent
- Remote
- Source routing

# Simple Bridge

- It is a less expensive type of bridge
- It links **2 segments** (LANS) and lists the address of all the stations in table included in each of them.
- Here address must be entered **manually**.
- The table is modified when stations are added and removed.

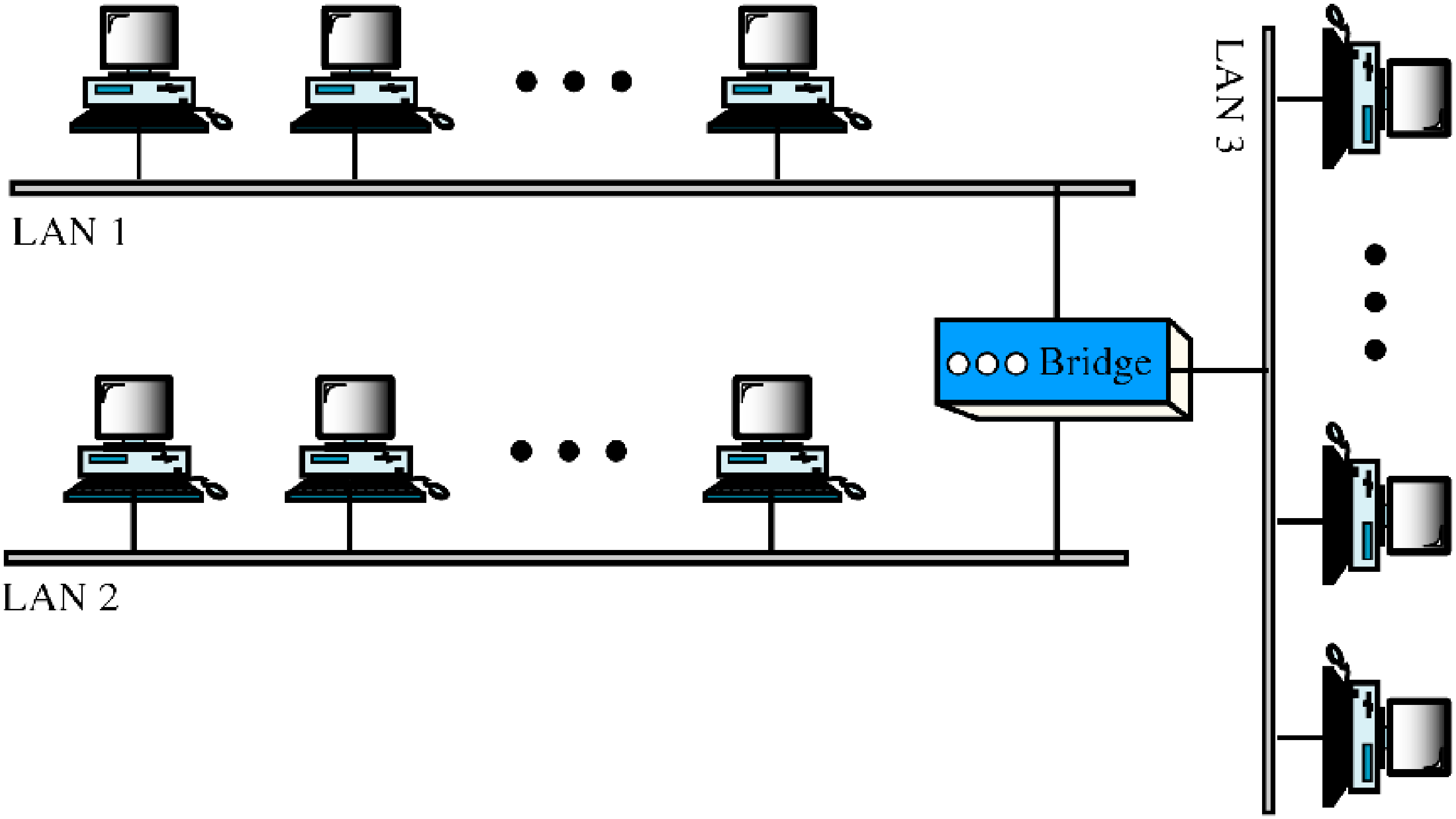
# Multiport Bridge

- It is used to connect more than two LANS.
- So the bridge has 3 tables.
- Here address must be entered **manually**

# Transparent Bridge:

- A transparent or learning bridge builds its table of station on its own (automatically).
- The table is empty when it is installed, it builds its table when it encounters the packet for transmission. It uses the source address for building table.
- It identifies the changes and update the table when system moved from one station to another

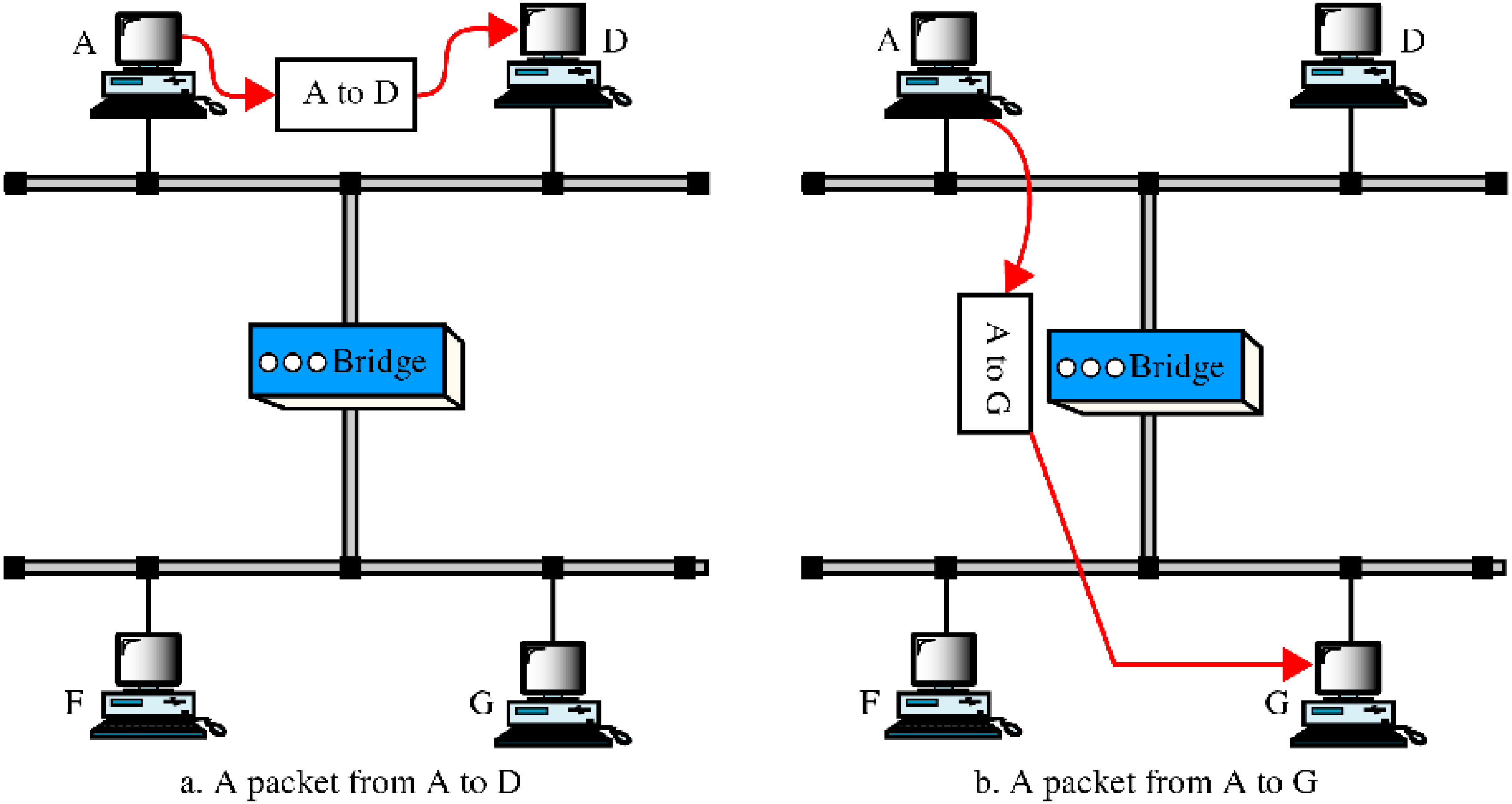
# Multiport bridge



# Cont,

- Bridges are normally installed redundantly,that is two LANS may be connected by more than one bridge.in this cases they may create a loop.
- So packet may go round and round,It can be avoided by algorithms like
  - Spannig tree algorithm
  - Source routing

# Function of a bridge



a. A packet from A to D

b. A packet from A to G

# Remote Bridges

•A remote bridge is capable of passing a data frame from one local area network to another when the two LANs are separated by a **long distance** and there is a wide area network connecting the two LANs.

•A remote bridge takes the frame before it leaves the first LAN and encapsulates the WAN headers and trailers.

•When the packet arrives at the destination remote bridge, that bridge removes the WAN headers and trailers leaving the original frame.

# Switches

- A switch is a **combination of a hub and a bridge** (multi-port bridge).
- It can interconnect two or more workstations, **but like a bridge, it observes traffic flow** and learns.
- When a frame arrives at a switch, the switch examines the destination address and forwards the frame out the one necessary connection.
- Workstations that connect to a hub are on a shared segment.
- Workstations that connect to a switch are on a switched segment.

# Wireless LANs

# LAN/WLAN World

- LANs provide connectivity for interconnecting computing resources at the local levels of an organization
- Wired LANs
  - Limitations because of physical, hard-wired infrastructure

- Wireless LANs provide
  - Flexibility
  - Portability
  - Mobility
  - Ease of Installation

# Wireless LAN Applications

- Medical Professionals
- Education
- Temporary Situations
- Airlines
- Security Staff
- Emergency Centers

# IEEE 802.11 Wireless LAN Standard

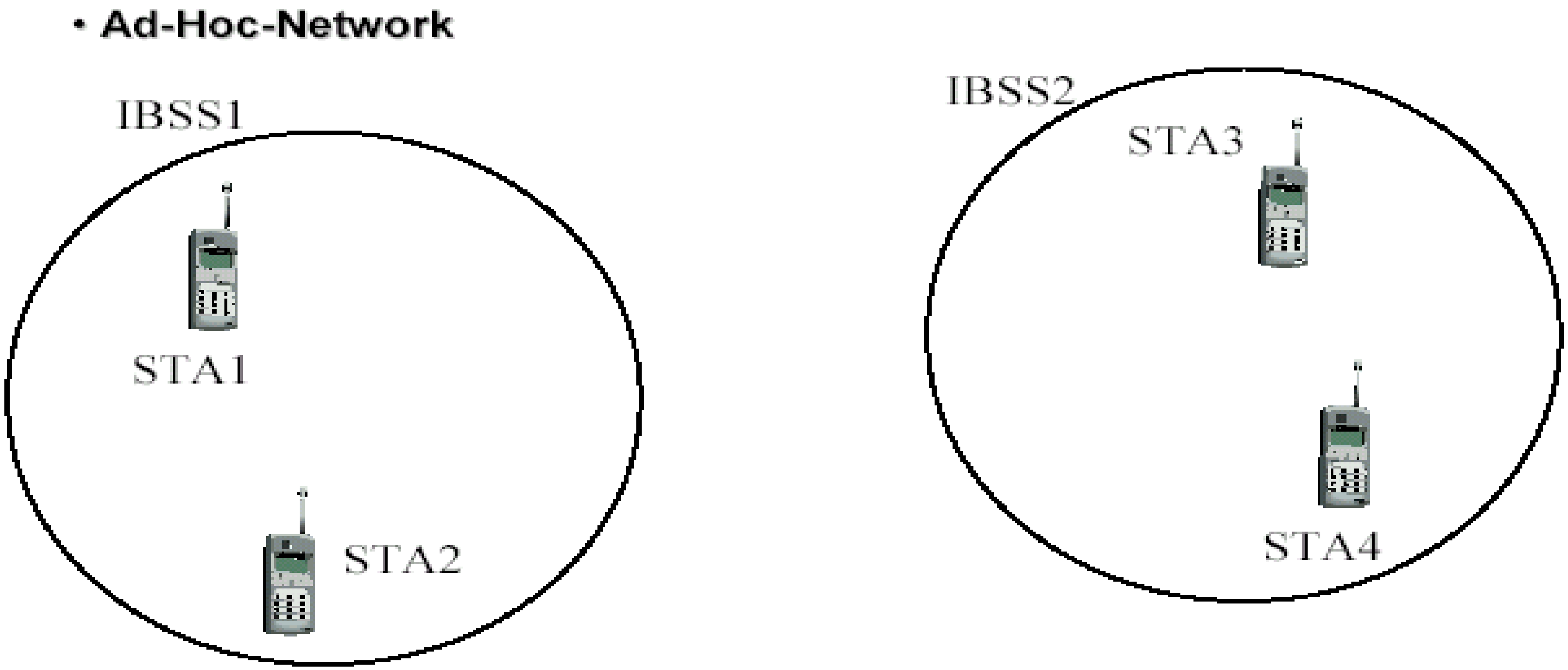
- In response to lacking standards, IEEE developed the first internationally recognized wireless LAN standard – IEEE 802.11
- IEEE published 802.11 in 1997, after seven years of work
- Scope of IEEE 802.11 is limited to Physical and Data Link Layers.

# Benefits of 802.11 Standard

- Appliance Interoperability
- Fast Product Development
- Stable Future Migration
- Price Reductions
- The 802.11 standard takes into account the following significant differences between wireless and wired LANs:
    - Power Management
    - Security
    - Bandwidth

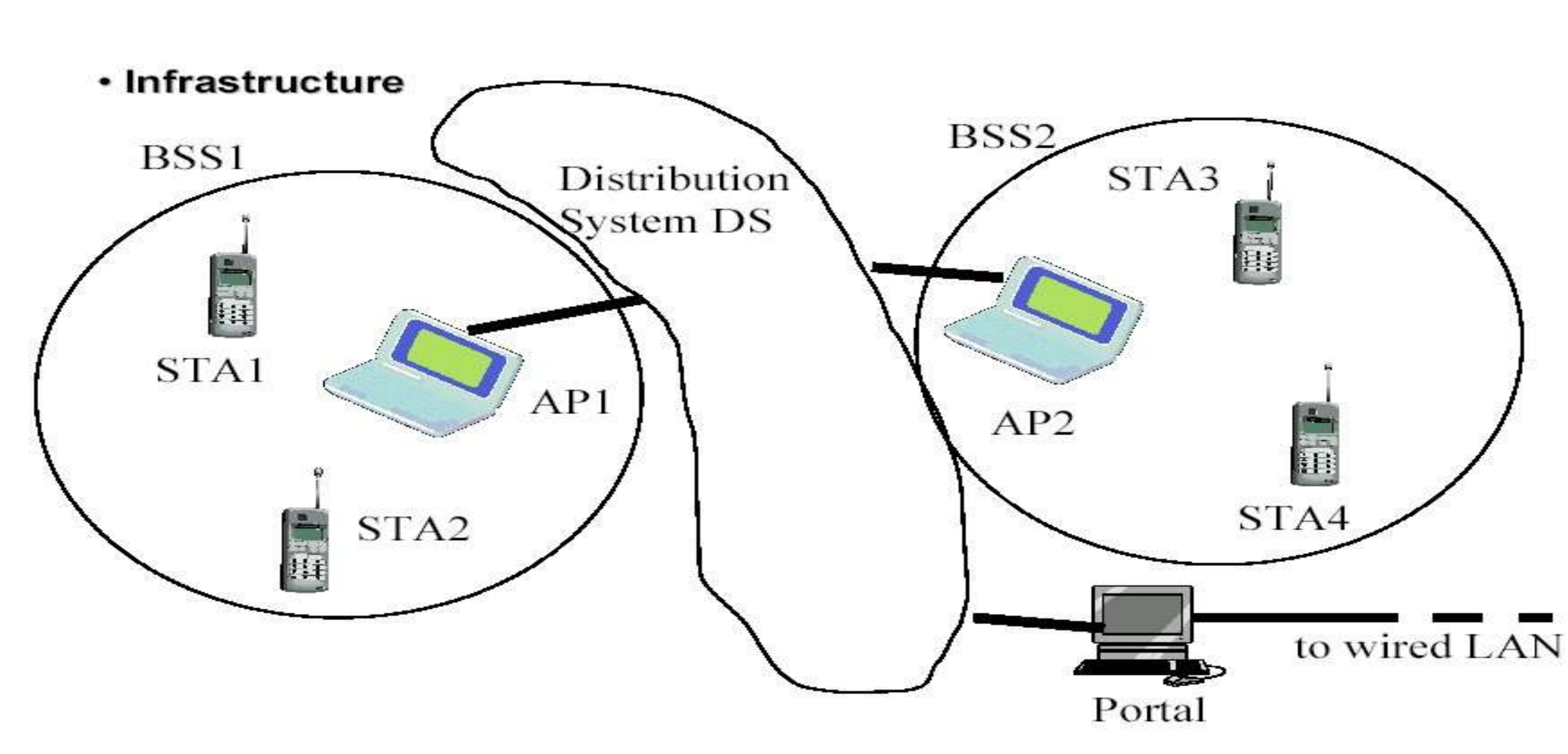
# WLAN Topology

## Ad-Hoc Network



The BSS without an AP is a stand-alone network and cannot send data to other BSSs. they can locate one another and agree to be part of a BSS.

# WLAN Topology
# Infrastructure

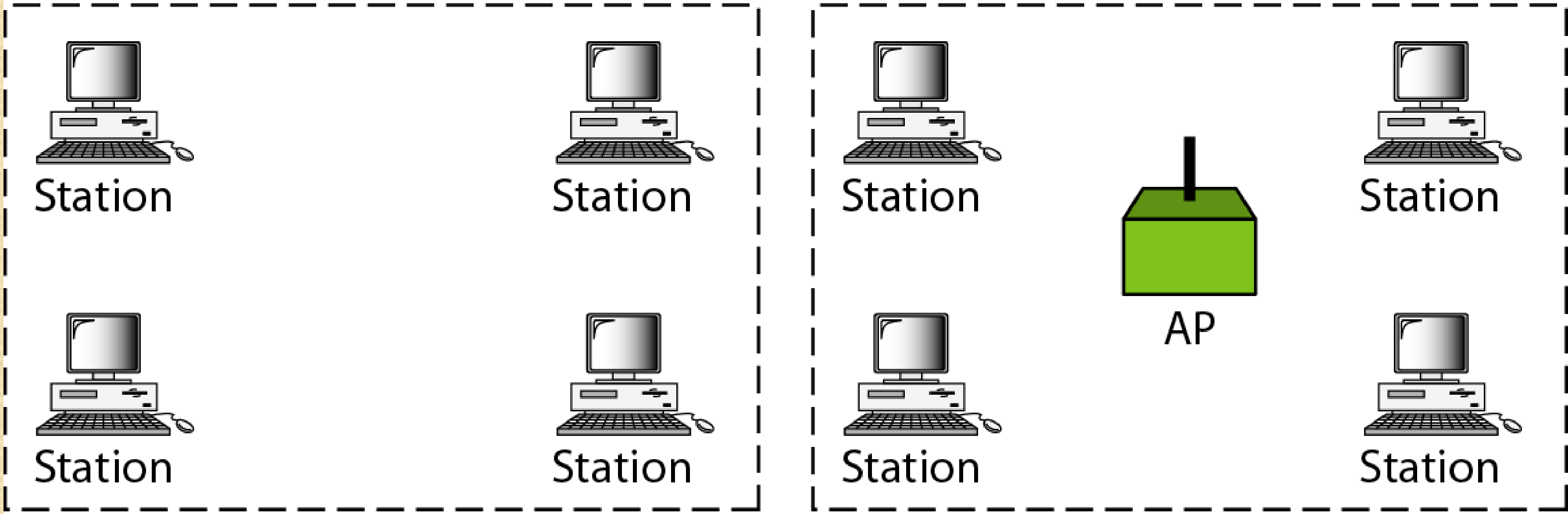


EX: cellular network if we consider each BSS to be a cell and each AP to be a base station.

*Basic service sets (BSSs)*

BSS: Basic service set

AP: Access point



Ad hoc network (BSS without an AP)

Infrastructure (BSS with an AP)

# *Station Types*

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:

- no-transition

  A station is either stationary (not moving) or moving only inside a BSS

- BSS-transition

  station can move from one BSS to another, but the movement is confined inside one ESS.

- and ESS-transition mobility.

  A station can move from one ESS to another

# collision avoidance CSMAICA

- network allocation vector (NAV) used to avoid collision.
  - RTS frame includes the duration of time that it needs to occupy the channel.
  - stations affected by this transmission create a timer called (NAV)
  - the network allocation vector (NAV) shows the time must pass before these stations allowed to check the channel for idleness.
- there is no mechanism for collision detection, if the sender has not received a CTS frame from the receiver, assumes there has been a collision ,the sender tries again.

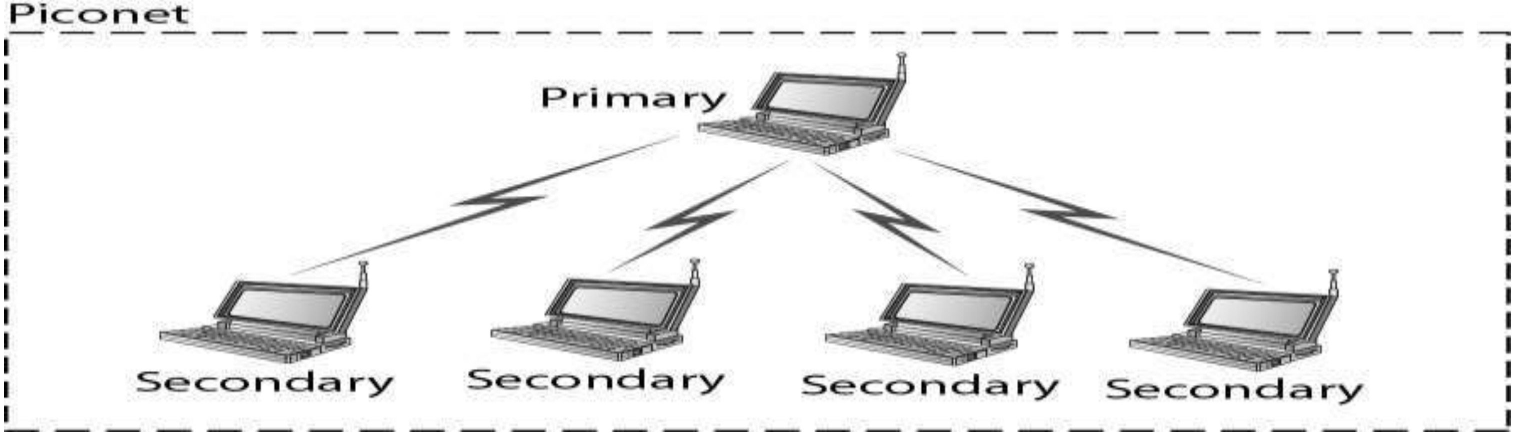
# BLUETOOTH

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.

- Bluetooth defines two types of networks: piconet and scatternet.

# Piconet

- A Bluetooth network is called a piconet, or a small net.
- It can have up to eight stations, one of which is called the master; the rest are called slaves.
- Maximum of seven slaves. Only one master.
- Slaves synchronize their clocks and hopping sequence with the master.
- But an additional eight slaves can stay in parked state, which means they can be synchronized with the master but cannot take part in communication until it is moved from the parked state.



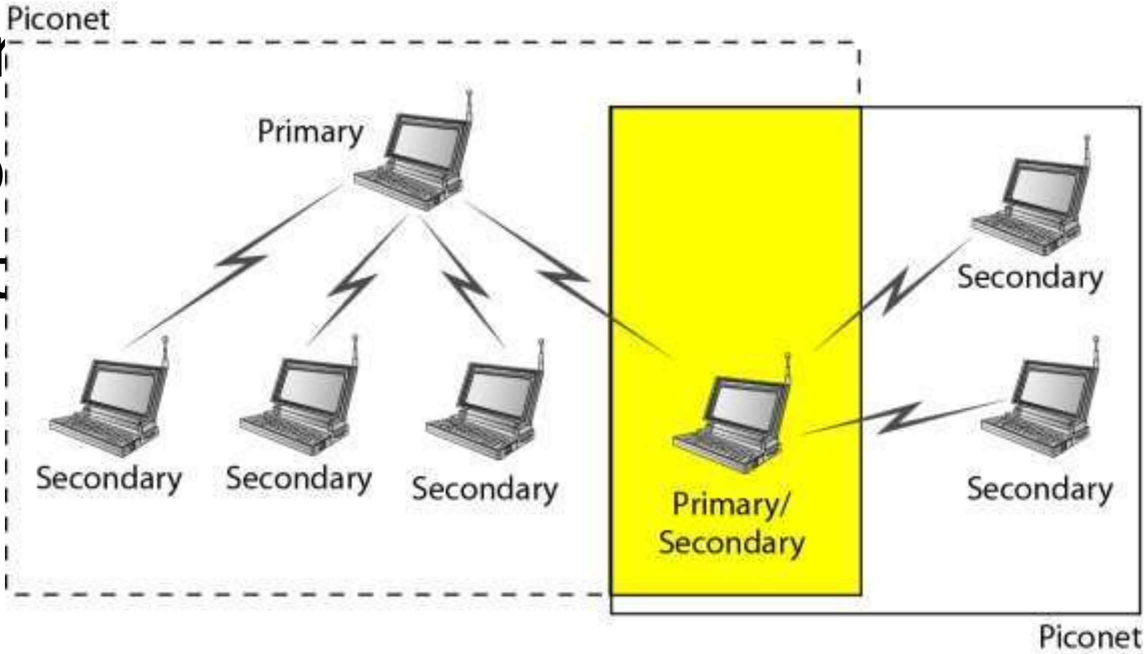
# Scatternet

□ Piconets can be combined to form what is called a scatternet.

□ A slave station in one piconet can become the master in

- another

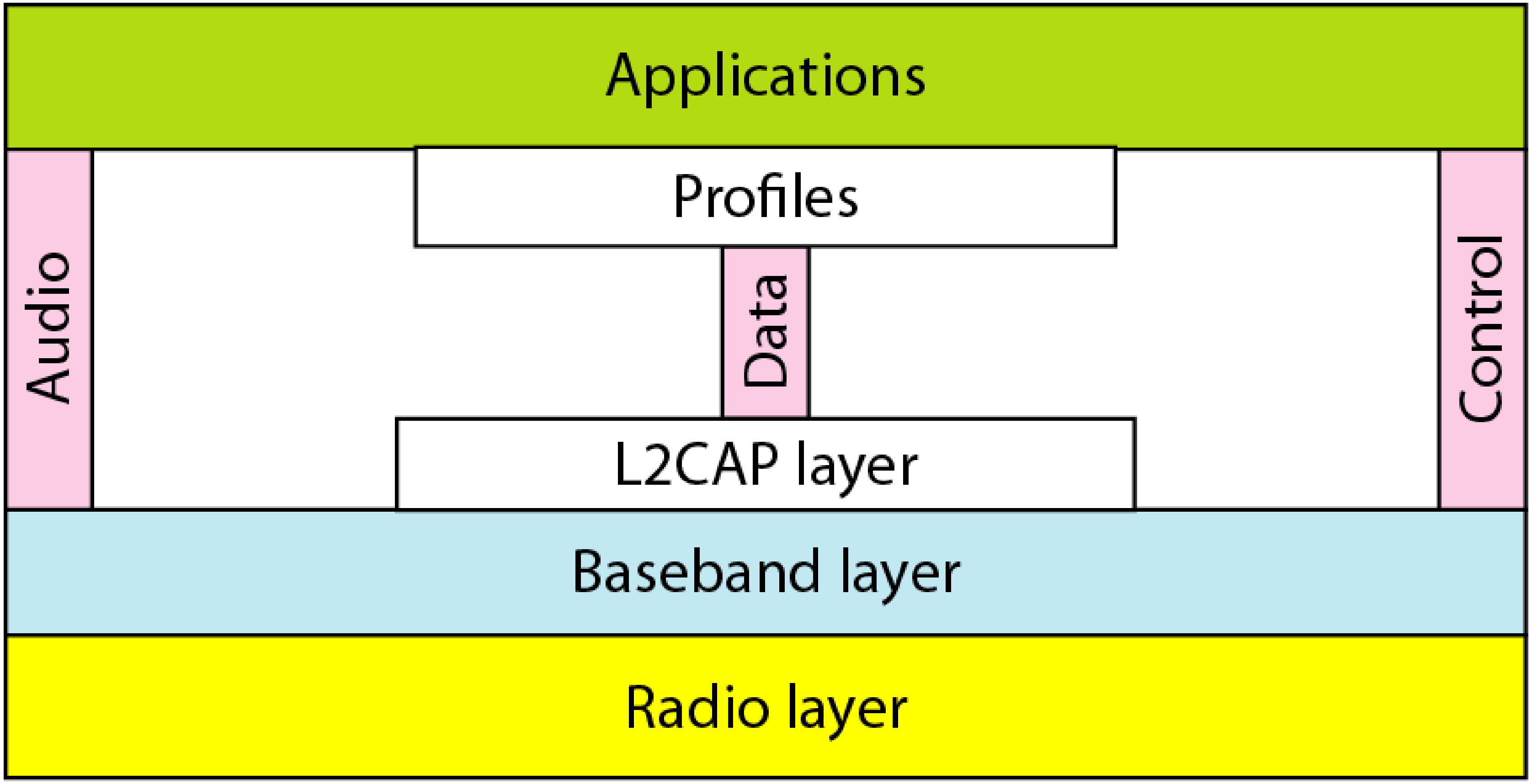
□ Bluetoo radio transmit



# Bluetooth layers

- Radio Layer: Roughly equivalent to physical layer of the Internet model. Physical links can be synchronous or asynchronous.
  - Uses Frequency-hopping spread spectrum [Changing frequency of usage]. Changes it modulation frequency 1600 times per second.
  - Uses frequency shift keying (FSK )with Gaussian bandwidth filtering to transform bits to a signal.
- Baseband layer: Roughly equivalent to MAC sublayer in LANs. Access is using Time Division (Time slots).
  - Length of time slot = dwell time = 625 microsec. So, during one frequency, a sender sends a frame to a slave, or a slave sends a frame to the master.
- Time division duplexing TDMA (TDD-TDMA) is a kind of half-duplex communication in which the slave and receiver send and receive data, but not at the same time (half-duplex). However, the communication for each direction uses different hops, like walkie-talkies.

# Bluetooth layers



# Physical Links

- Synchronous connection-oriented (SCO)
  - Latency is important than integrity.
  - Transmission using slots.
  - No retransmission.
- Asynchronous connectionless link (ACL)
  - Integrity is important than latency.
  - Does like multiple-slave communication.
  - Retransmission is done.
- L2CAP (Logical Link Control and Adaptation Protocol)
  - Equivalent to LLC sublayer in LANs.
  - Used for data exchange on ACL Link. SCO channels do not use L2CAP.
  - Frame format has 16-bit length [Size of data coming from upper layer in bytes], channel ID, data and control.
  - Can do Multiplexing, segmentation and Reassembly, QoS [with no QoS, best-effort delivery is provided] and Group mangement [Can do like multicast group, using some kind of logical addresses].

# THANK YOU

# UNIT III
# NETWORK LAYER

Network layer – Switching concepts – Circuit switching – Packet switching – IP Addressing –IPV4, IPV6 – Routing Protocols – Distance Vector – Link State.

# UNIT – III

# NETWORK LAYER

# OVERVIEW

- **Network Layer**
- **Switching Concepts**
- **Circuit Switching**
- **Packet Switching**
- **Message Switching**
- **IP Addressing**
- **IPV4**
- **IPV6**
- **Routing Protocols**
- **Distance Vector Routing**
- **Link State Routing**

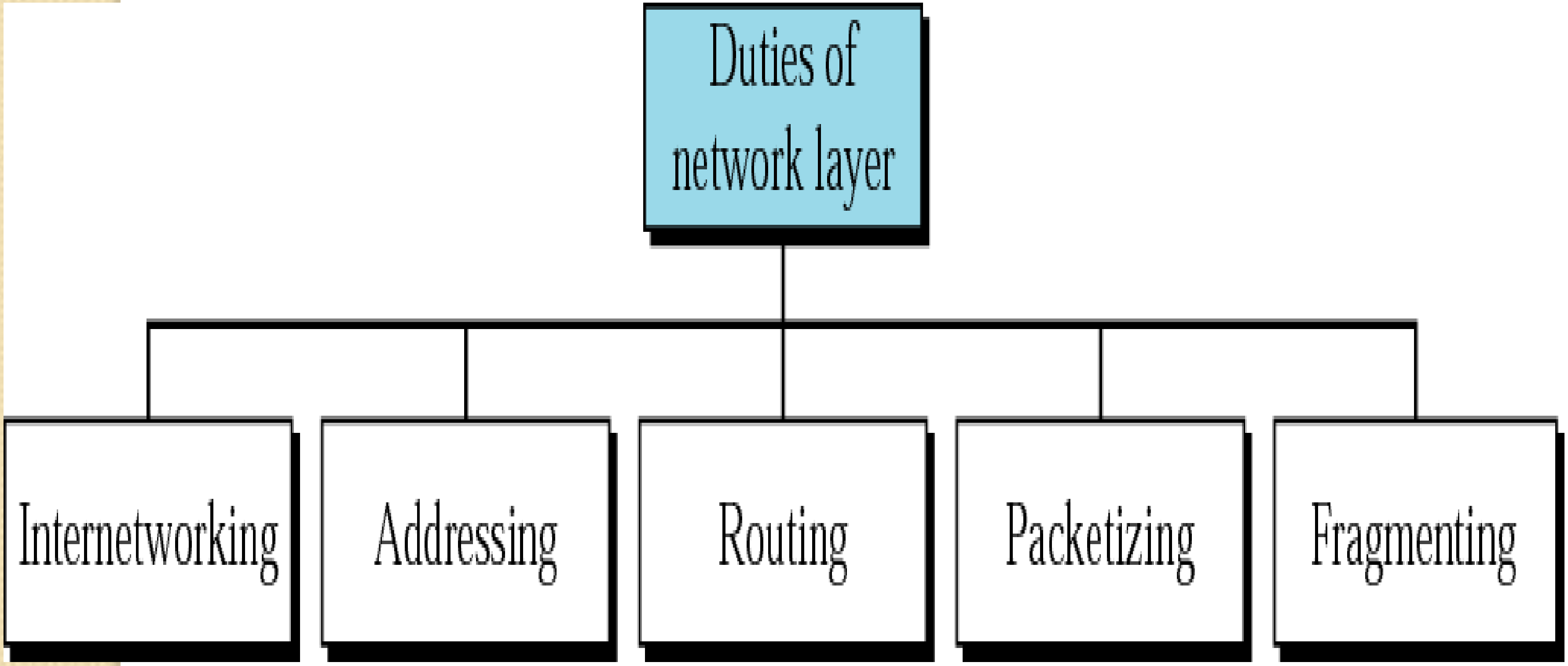
# Network Layer

- The Network layer is responsible for the **source-to-destination delivery of a packet** possible across multiple networks.
- It converts **Frames into packets.**

# Functions of Network Layer

- Source-to-Destination delivery of a packet
- Logical addressing
- Routing
- Internetworking

# Network layer Duties



# Switching Concepts

- Switches are hardware or software devices used for temporary connection b/w 2 or more devices linked to the switch in network **but not to each another**
- Switches are needed to connect multiple devices for making one-one communication

TYPES:

- Circuit Switching
- Packet Switching
- Message Switching

**Figure 14.1** *Switched network*

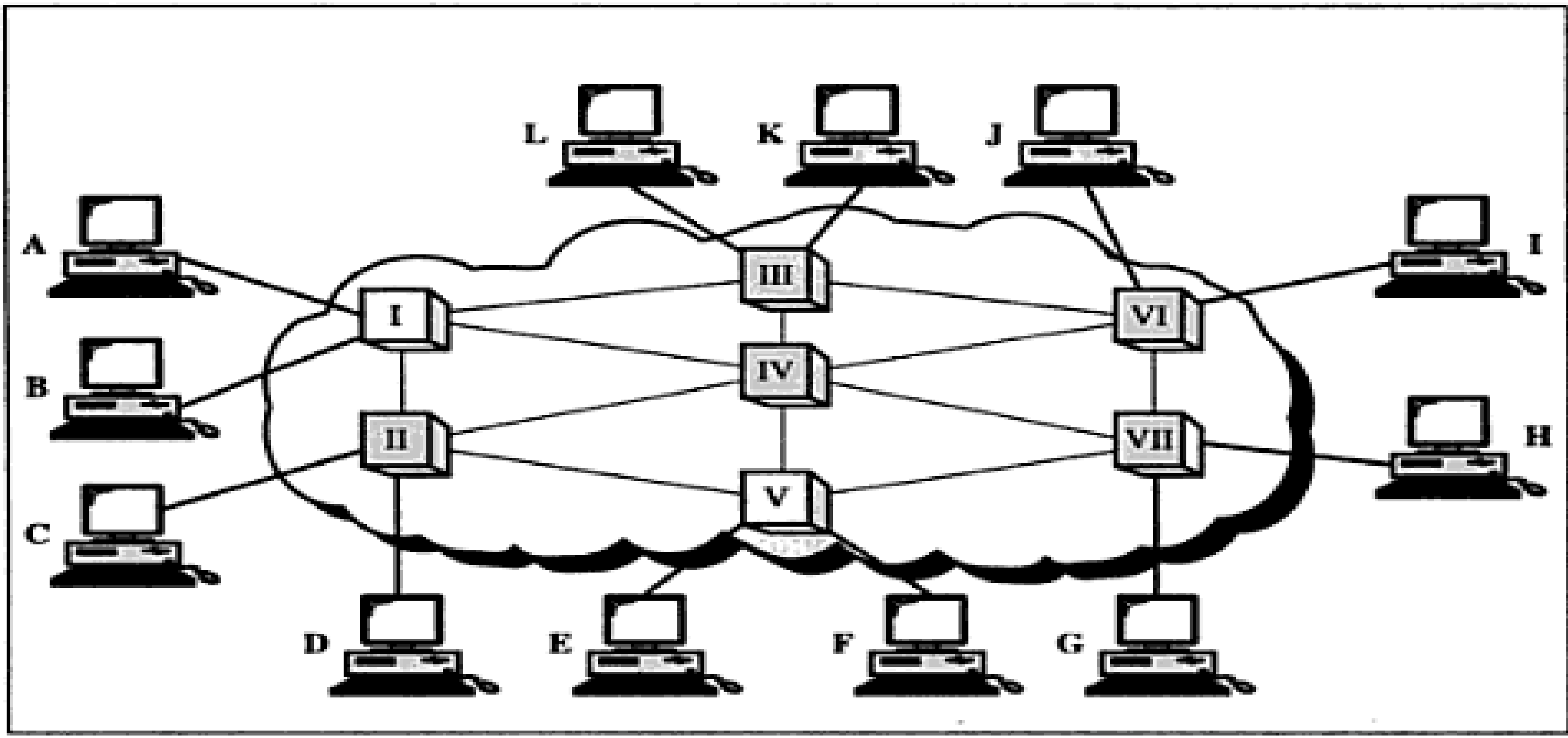
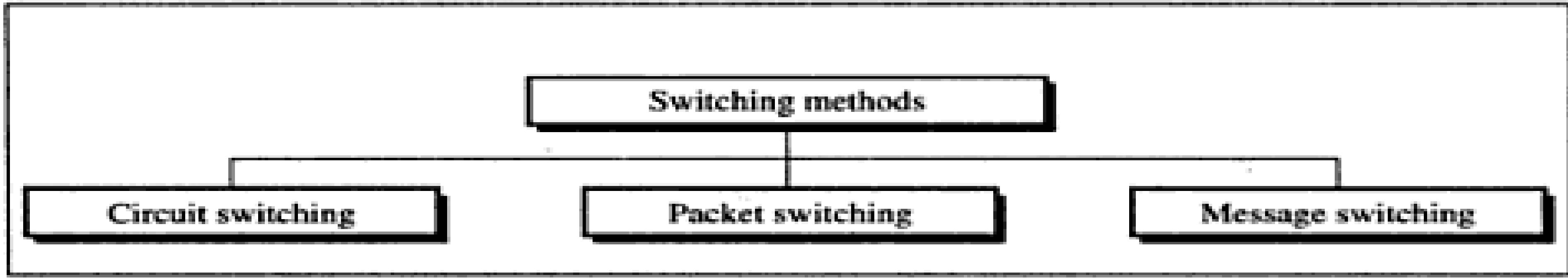


**Figure 14.2** *Switching methods*



# Circuit switching

- It creates **direct physical connection** b/w two devices such as phone or computers.
- Any computer can be connected to any other using Levers.
- N-by-N folded switches can connect n lines in full duplex mode.

2 types:

- **Space division**
- **Time division**

Figure 14.3 *Circuit-switched network*

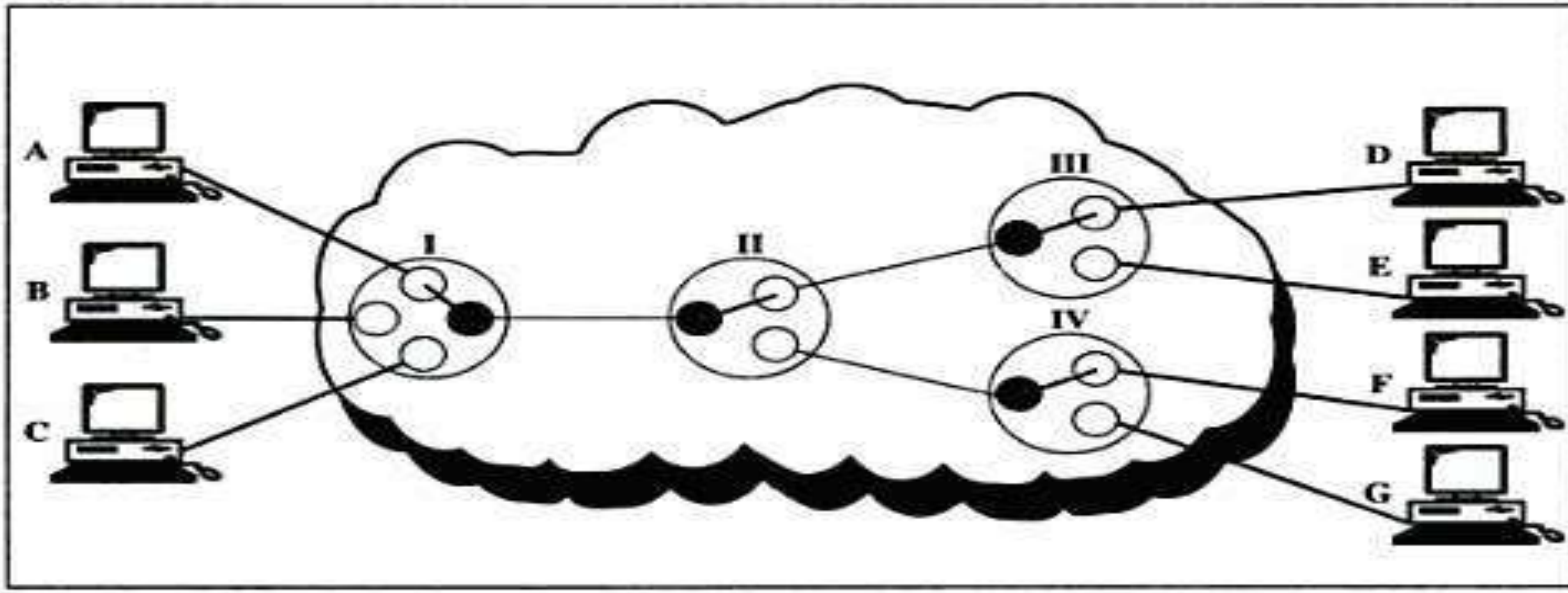


Figure 14.4 *A circuit switch*

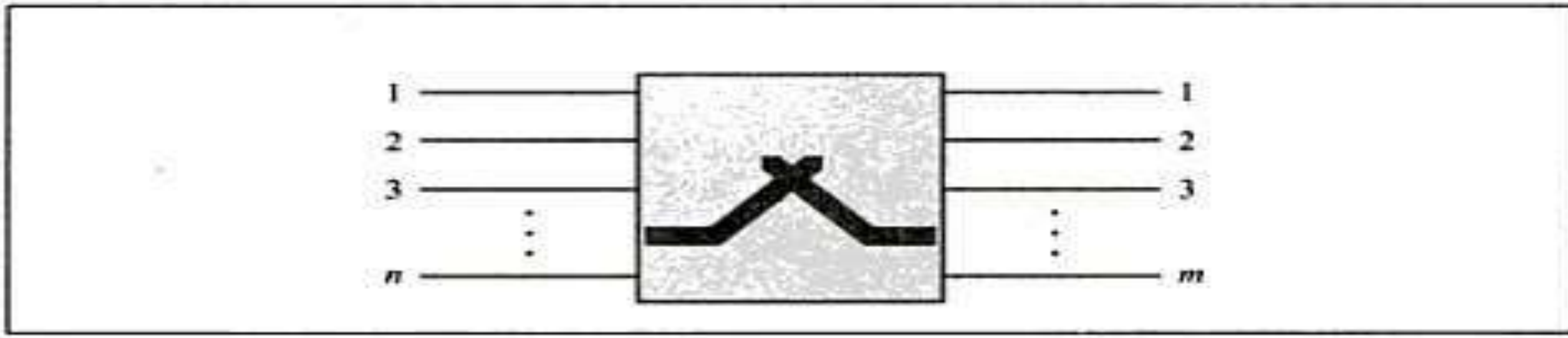
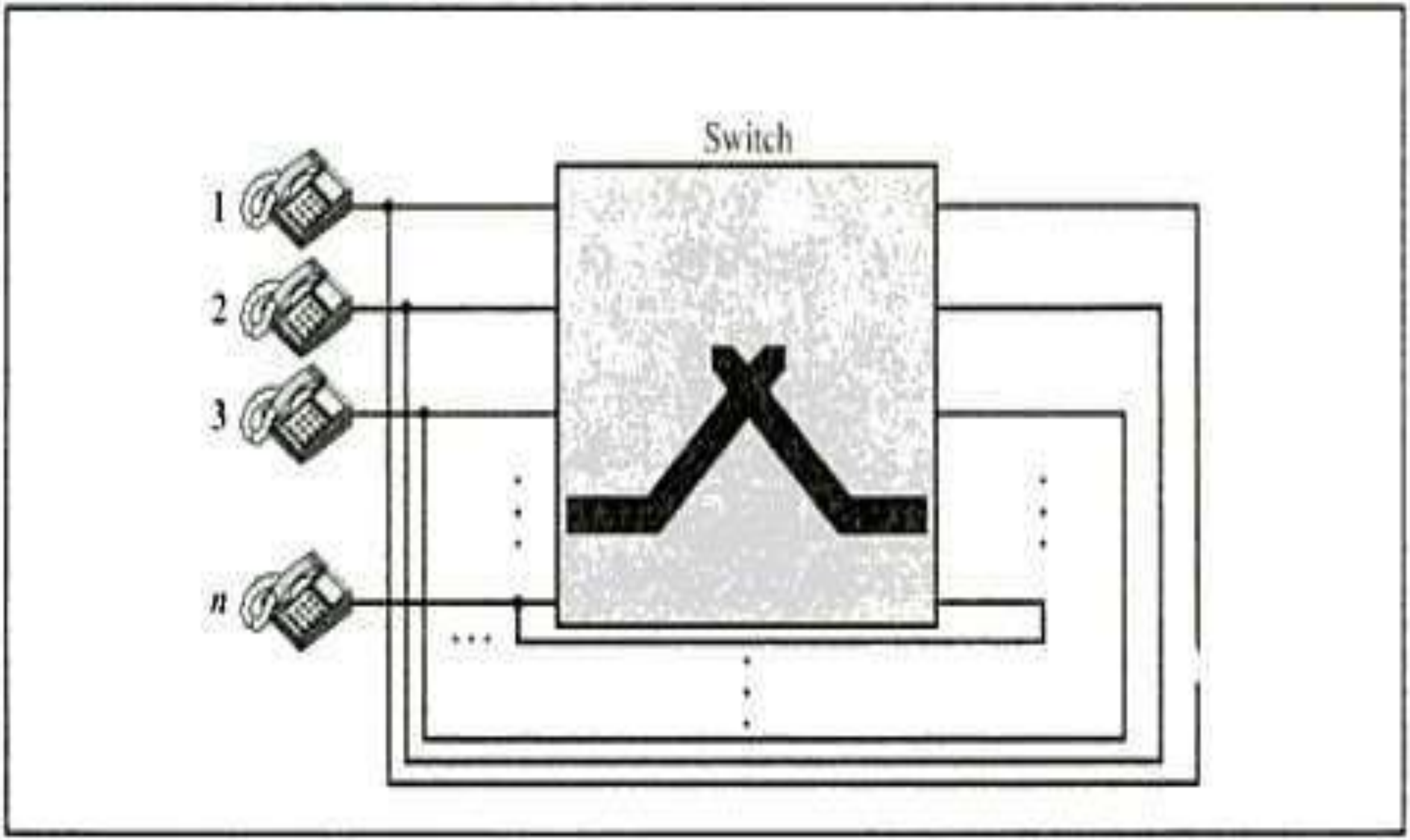


Figure 14.5 *A folded switch*



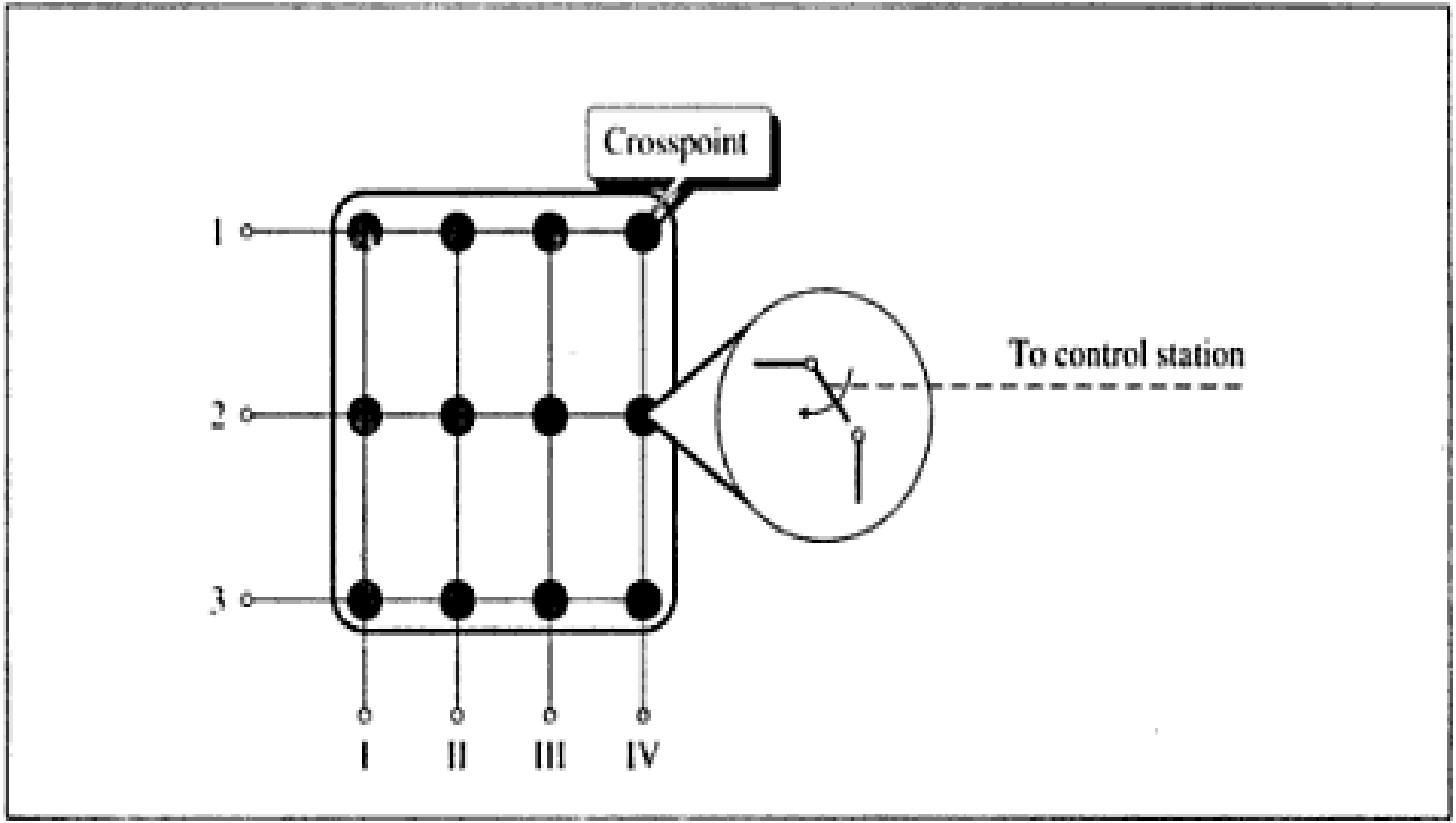
# Space Division Switch

- □ Path in the circuit are separated from each other
- □ It is used both in analog and digital communication
- □ 2 Types:
  - ○ **Crossbar switch**
  - ○ **Multistage switch**

- Crossbar Switch:
  - □ It connects n inputs to m outputs using cross points
- Limitation:
  - □ More cross points needed(1000 I/P - 1000 O/P requires 1000000 crosspoints)

# Crossbar Switch:

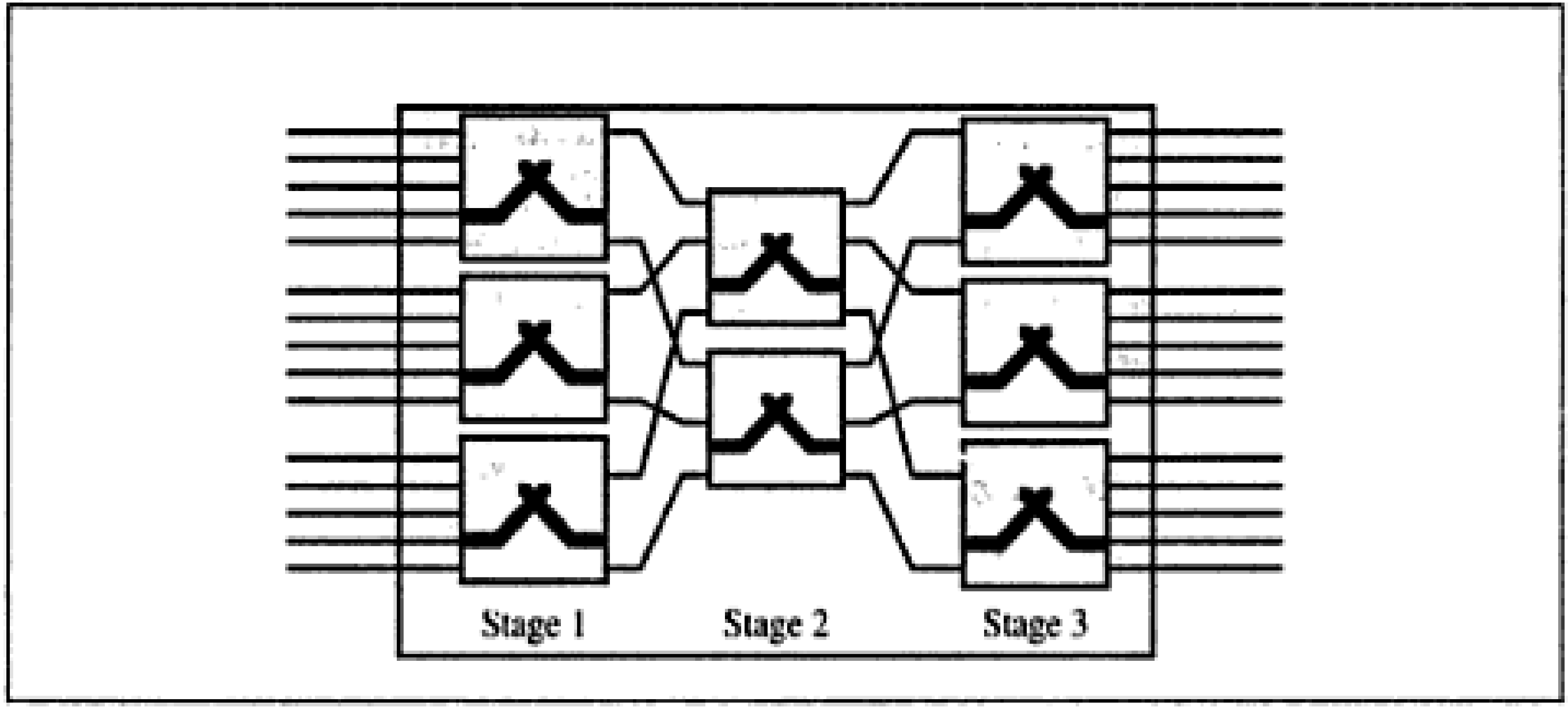
**Figure 14.7** *Crossbar switch*



# Multistage switch

- Devices are linked to switches ,that are in turn linked to another switches(Hierarchy of switches)

**Figure 14.8** *Multistage switch*



# Blocking:

□ The **reduction in a number of cross points** causes a phenomena called Blocking.

□ During heavy traffic one input cannot be connected to output because no path available

# Time Division Switches

□ It uses time division multiplexing

□ 2 methods:

□ **Time slot interchange**

□ **TDM bus**

Time slot interchange:

□ It changes the ordering of the slot based on the desired connection

□ It uses RAM to store time slot

□ Ex:

□ 1->3 2->4 3->1 4->2

□ A B C D -> C D A B

# TSI

**Figure 14.10** *Time-division multiplexing, without and with a time-slot interchange (TSI)*

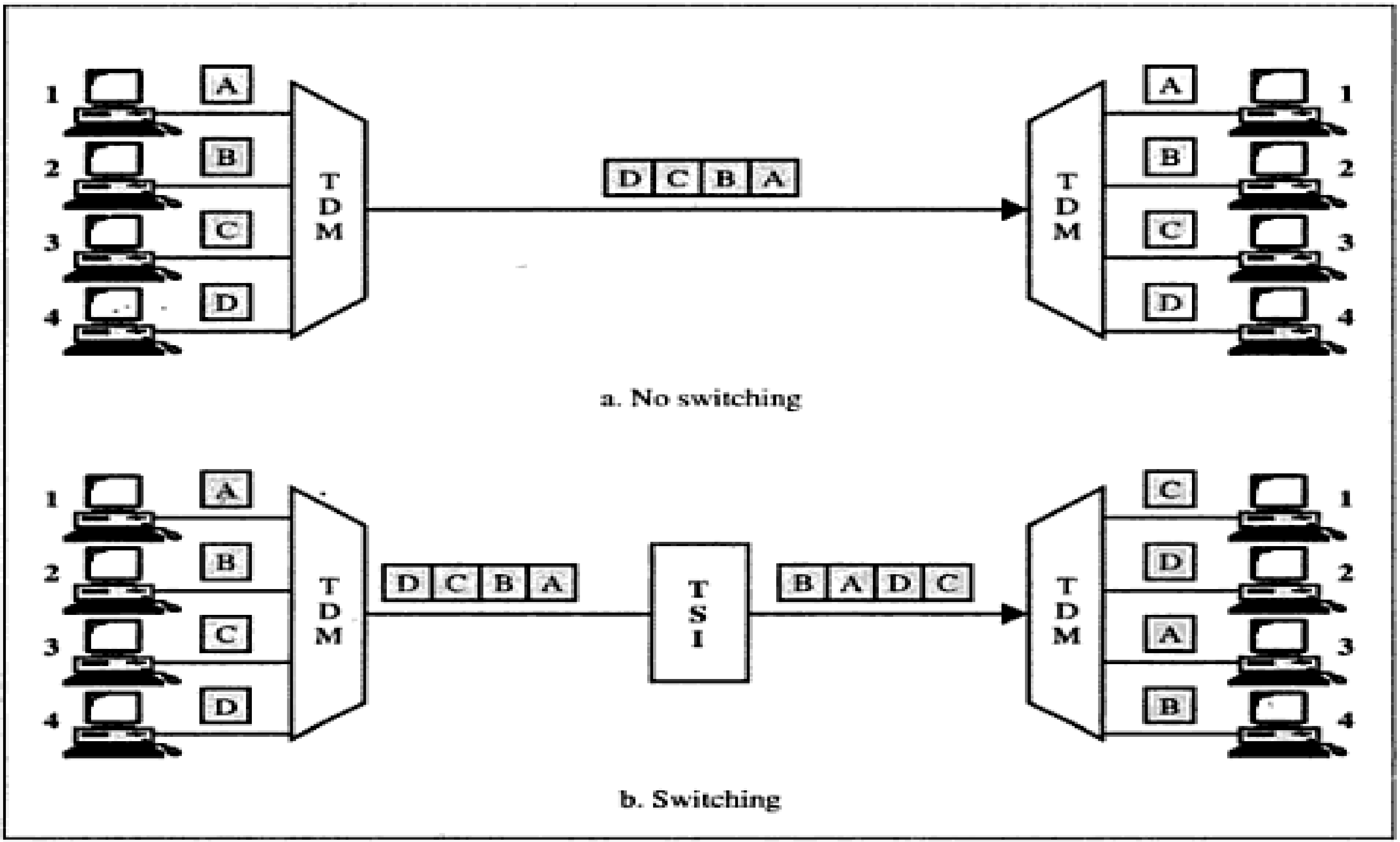
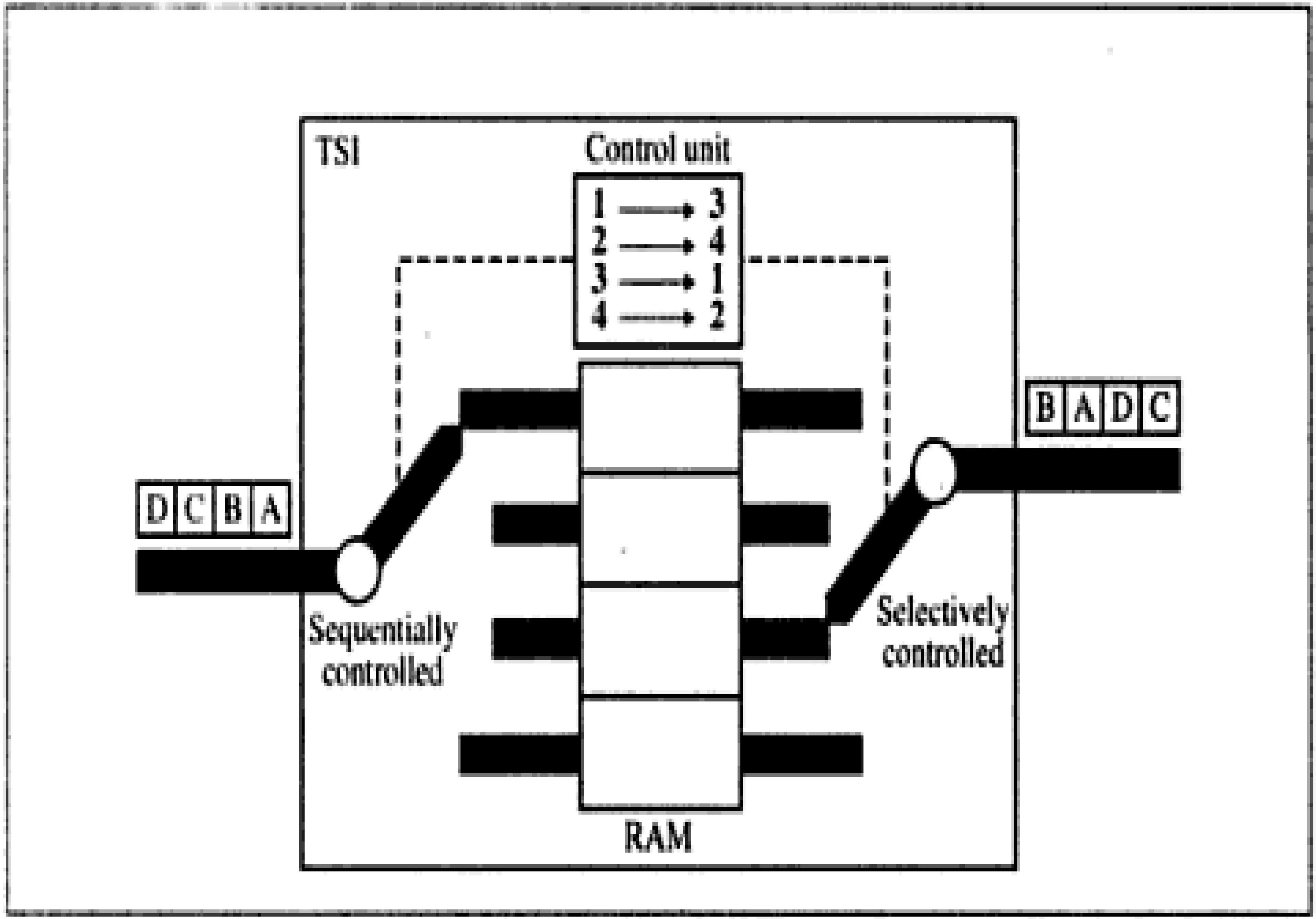


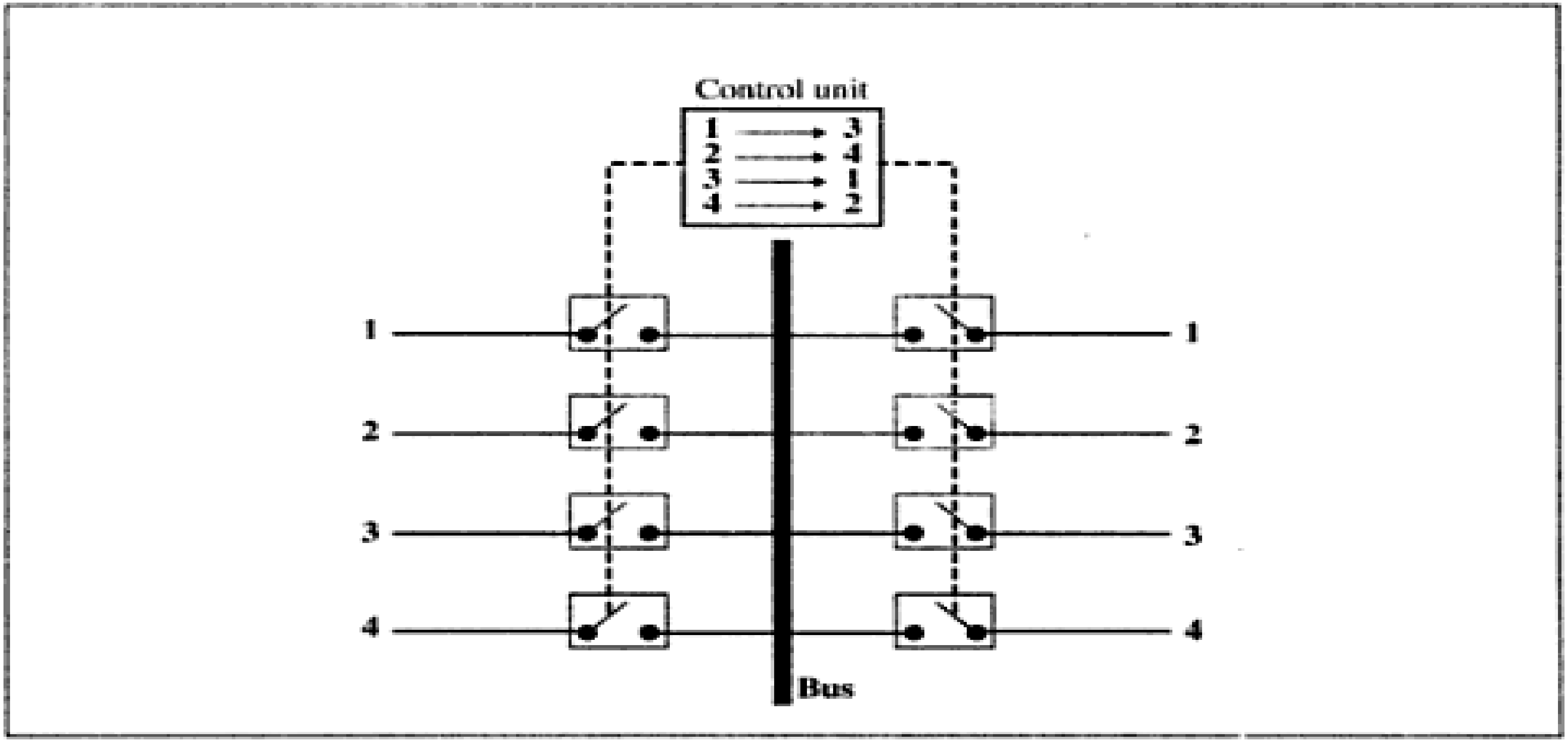
**Figure 14.11** *Time-slot interchange*



# TDM Bus- Time Division Multiplexing

- Here each input and output lines are connected to high speed bus
- Each bus is closed during one of the four time slots

**Figure 14.12** *TDM bus*



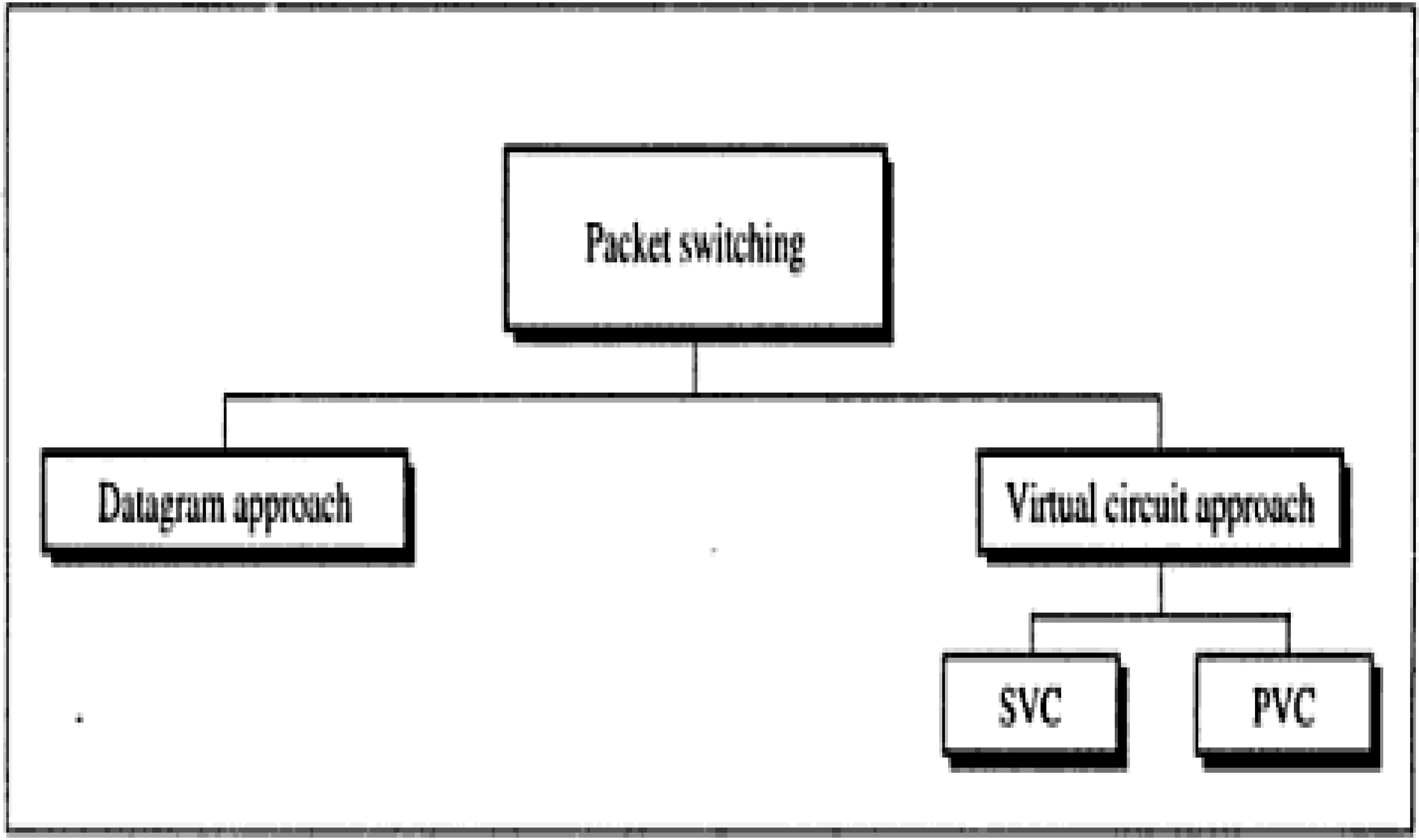
# Limitations of Circuit Switching

- It is **specially designed for voice communication**(telephone). **Not suitable for data communication.**
- Once a circuit is established, it remains for duration of the session. It creates dialed(temporary)and leased(Permanent).
- Less data rate because of point to point connection.

# Packet switching

- Packet switching is better for data transmission.
- Here data are transmitted through unit of variable length blocks called **packets**.
- Longer transmission are divided into multiple packets.
- Packet length is decided by network.

**Figure 14.16** *Packet-switching approaches*



# Datagram Approach

- In this approach a message is divided into multiple packets.
- All packets choose various routes and reaches the destination.
- Ordering of packets in destination is done by transport layer.

**Figure 14.17** *Datagram approach*

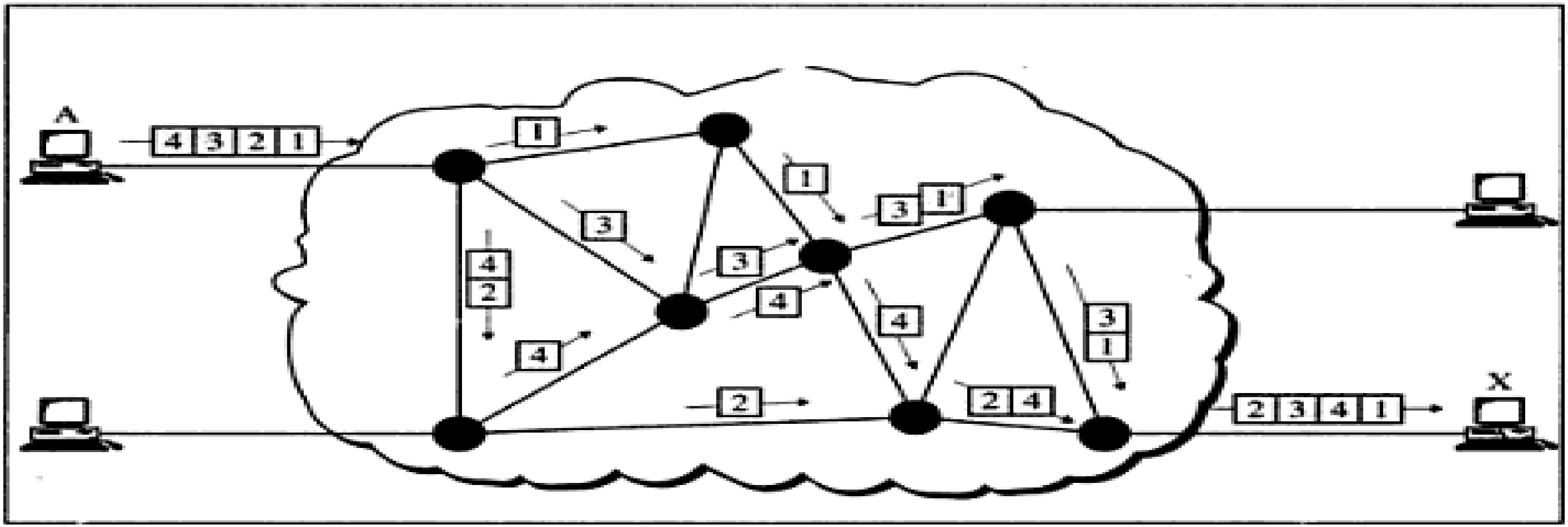
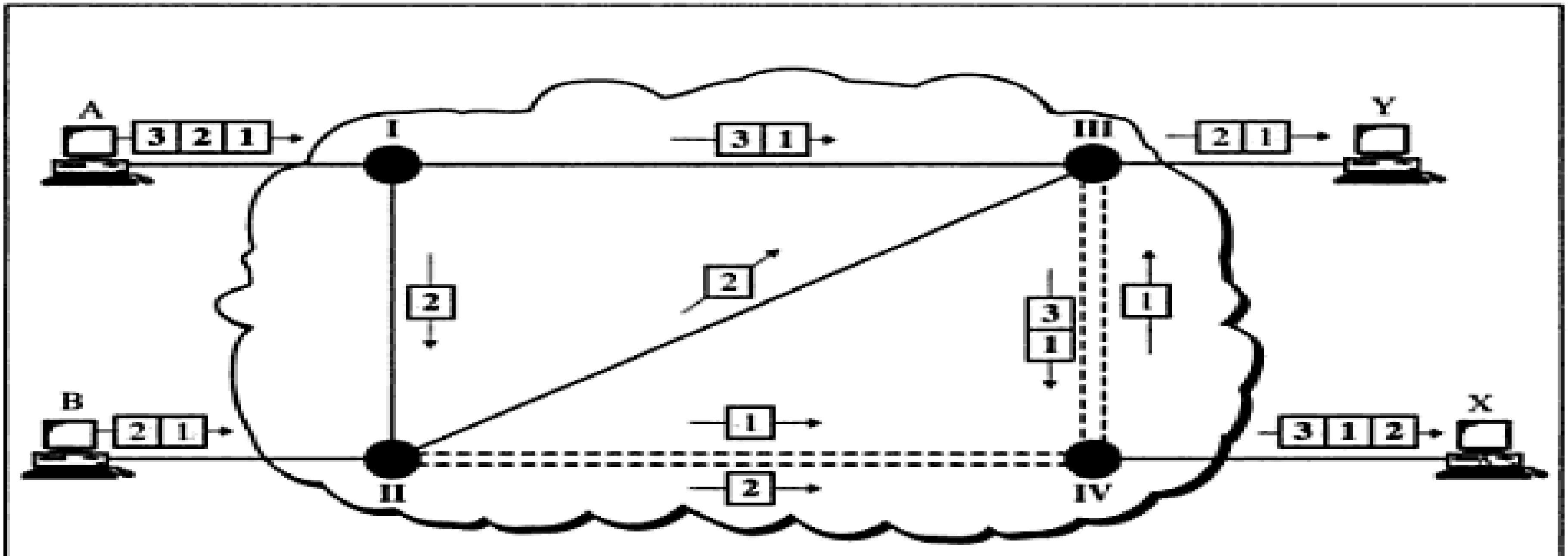


**Figure 14.18** *Multiple channels in datagram approach*



# Virtual Circuit approach

- □ It uses single route to send all packets of the message

Two formats:

- ○ Switched virtual circuit
- ○ Permanent virtual circuit

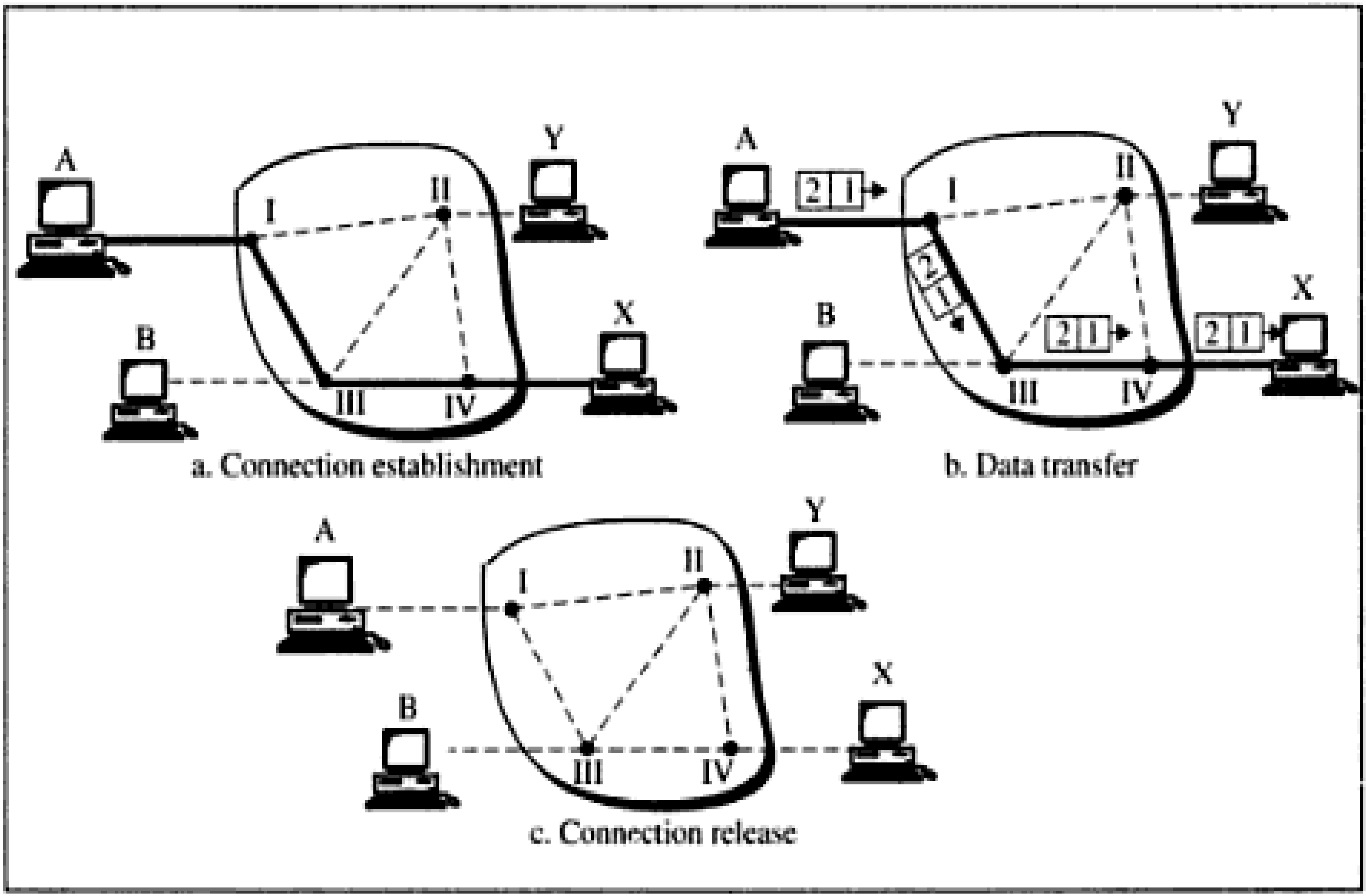
SVC

- Connection is **temporary**
- **Dial-up lines**

**During Transmission.**

- □ A connection is established-all packets are sent – proper ACK- Connection is terminated

**Figure 14.19** *Switched virtual circuit (SVC)*



# PVC

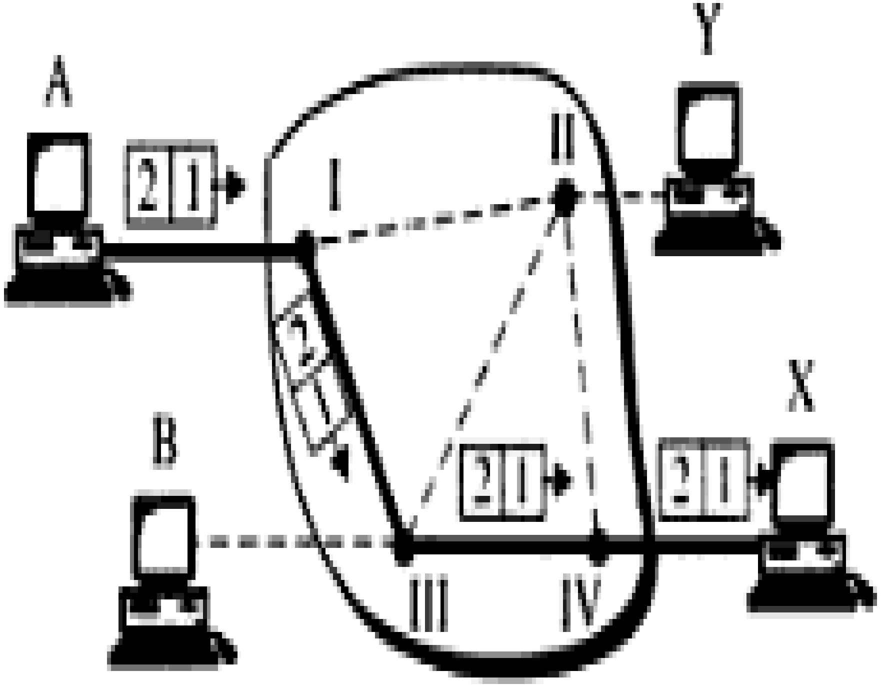
- Connection is **permanent.**
- Circuit is dedicated for two users, No one else can use the line when communication takes place.
- It always gets the same route.
- **Leased lines.**

**During Transmission.**

□ No connection establishment or termination

# PVC

**Figure 14.20** *Permanent virtual circuit (PVC)*



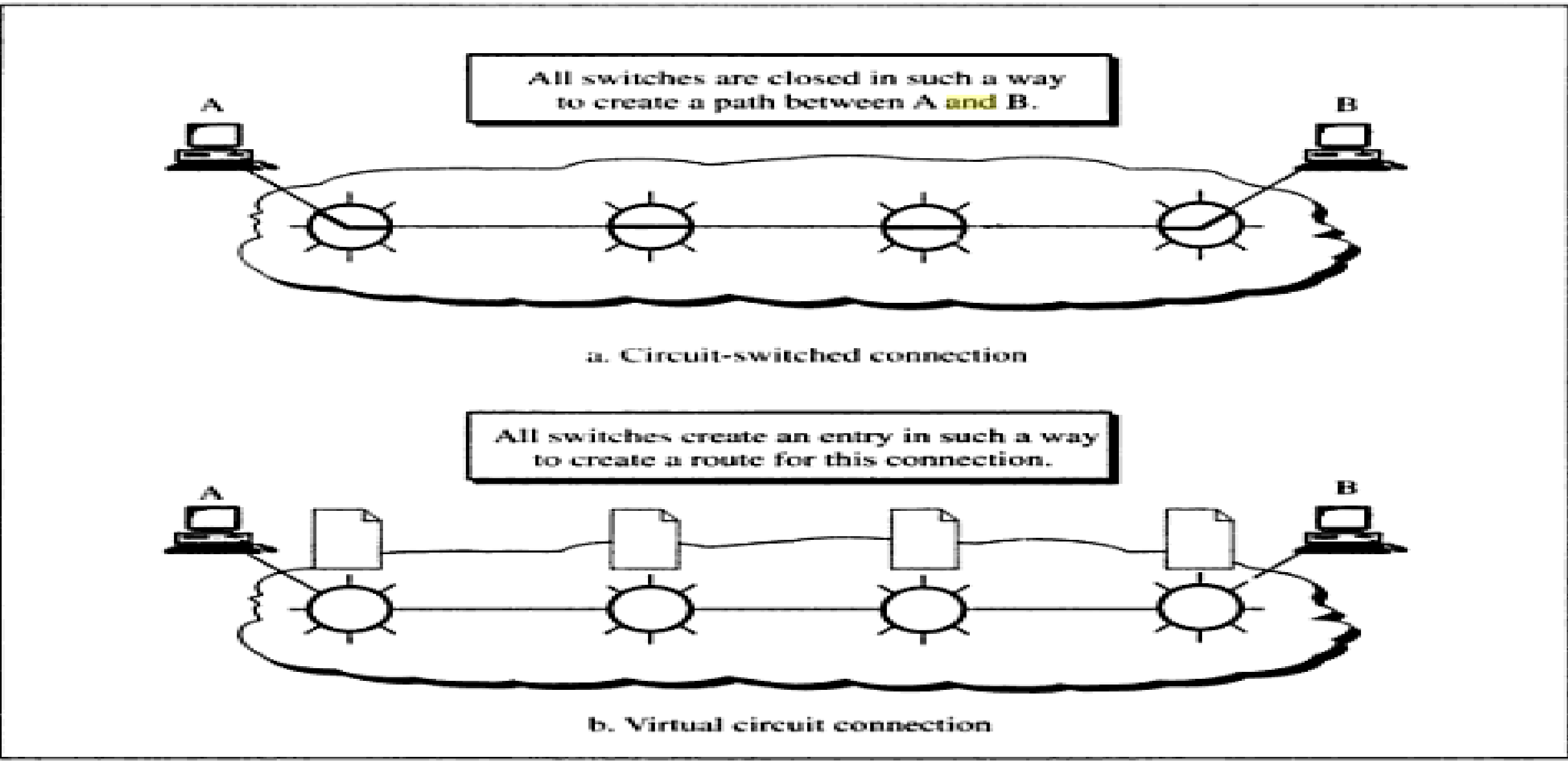
Permanent connection for the duration of the lease

# Circuit switched Vs Virtual Circuit

## Path Vs Route:

- Circuit switched->Path
- Virtual Circuit->route

**Figure 14.21** *Path versus route*



All switches are closed in such a way to create a path between A and B.
A
B
All switches create an entry in such a way to create a route for this connection.
A
B

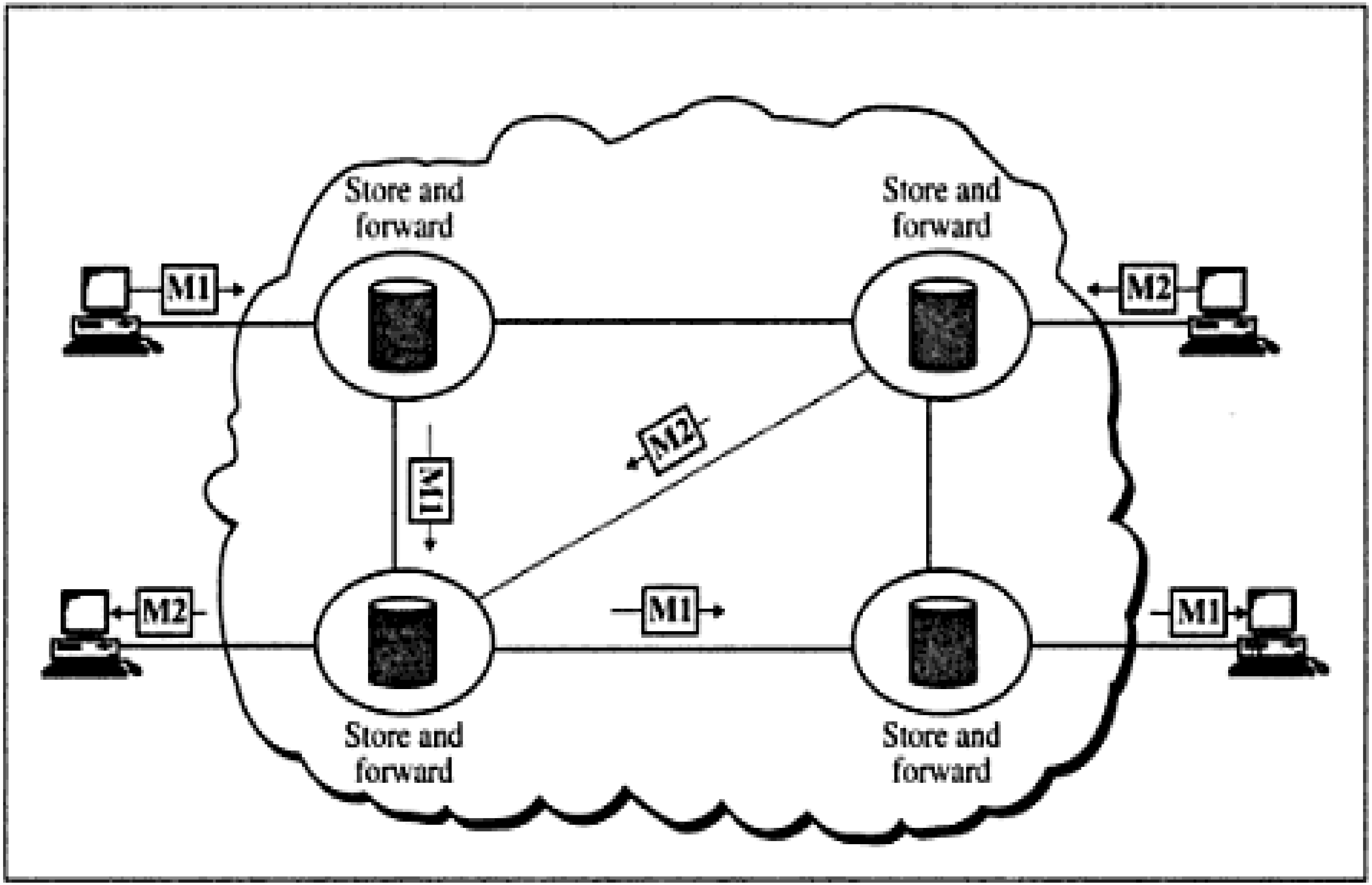
a. Circuit-switched connection

b. Virtual circuit connection

# Message Switching

- It uses a mechanism called **store and forward**
- Here a message is received and stored until a appropriate route is free, then sends along.
- Message switching- uses secondary storage(Disk)
- Packet switching – uses primary storage(RAM)

Figure 14.23 *Message switching*



# Routers

- The routers decide which route is best among many routes in a particular transmission.
- Routers are like stations on the network

Routing concepts:

□ Least cost routing:

□ Cheaper

□ Shortest path(using small number of relays or **hops**.

□ Hop-count ->Number of relays

# Non - Adaptive Routing

- In some routing protocols , once a pathway to a destination is selected ,the router sends all packets in that way.

## Adaptive Routing:

- The router may select new route for each packet.

## Packet Life Time (or)Time to Live:

The problem created by looping or bouncing is avoided by destroying the packet without looping, New packet is retransmitted

# Routing Algorithms or Routing Protocols

- To route the packet with optimal cost many routing algorithms are used to Calculating the shortest path between 2 routers

1. Distance Vector Routing
2. Link State Routing

# Distance vector Routing

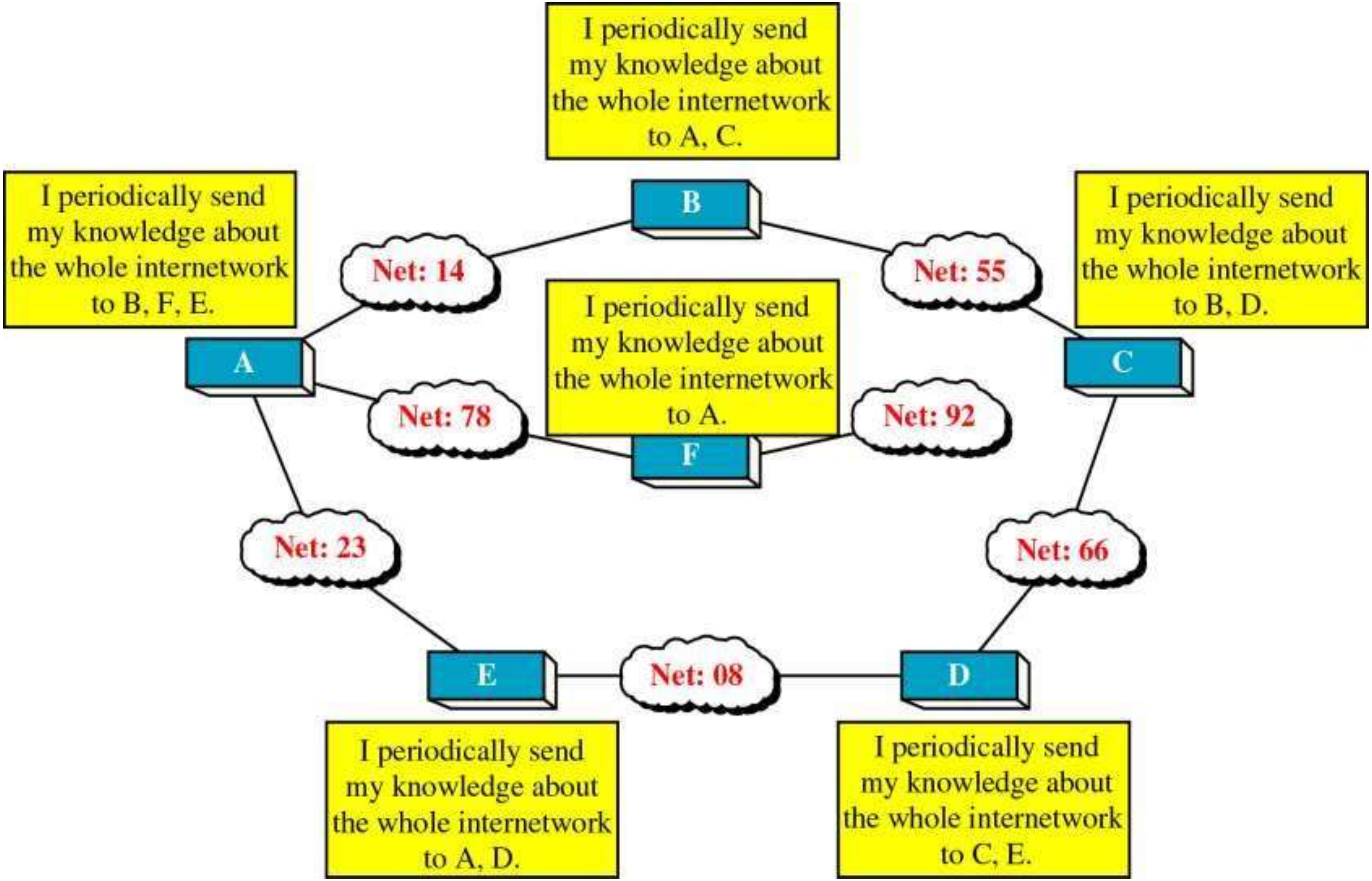
**Def:**

- Each router periodically shares its knowledge about the entire network with its neighbor.
- It is represented by graph.

□Key Works:

- Each router shares its knowledge about the entire network to neighbors.
- Routing only to the directly linked routers.
- Information sharing at regular interval(each 30 seconds).

# The Concept of Distance  Vector Routing



I periodically send my knowledge about the whole internetwork to A, C.

I periodically send my knowledge about the whole internetwork to B, F, E.

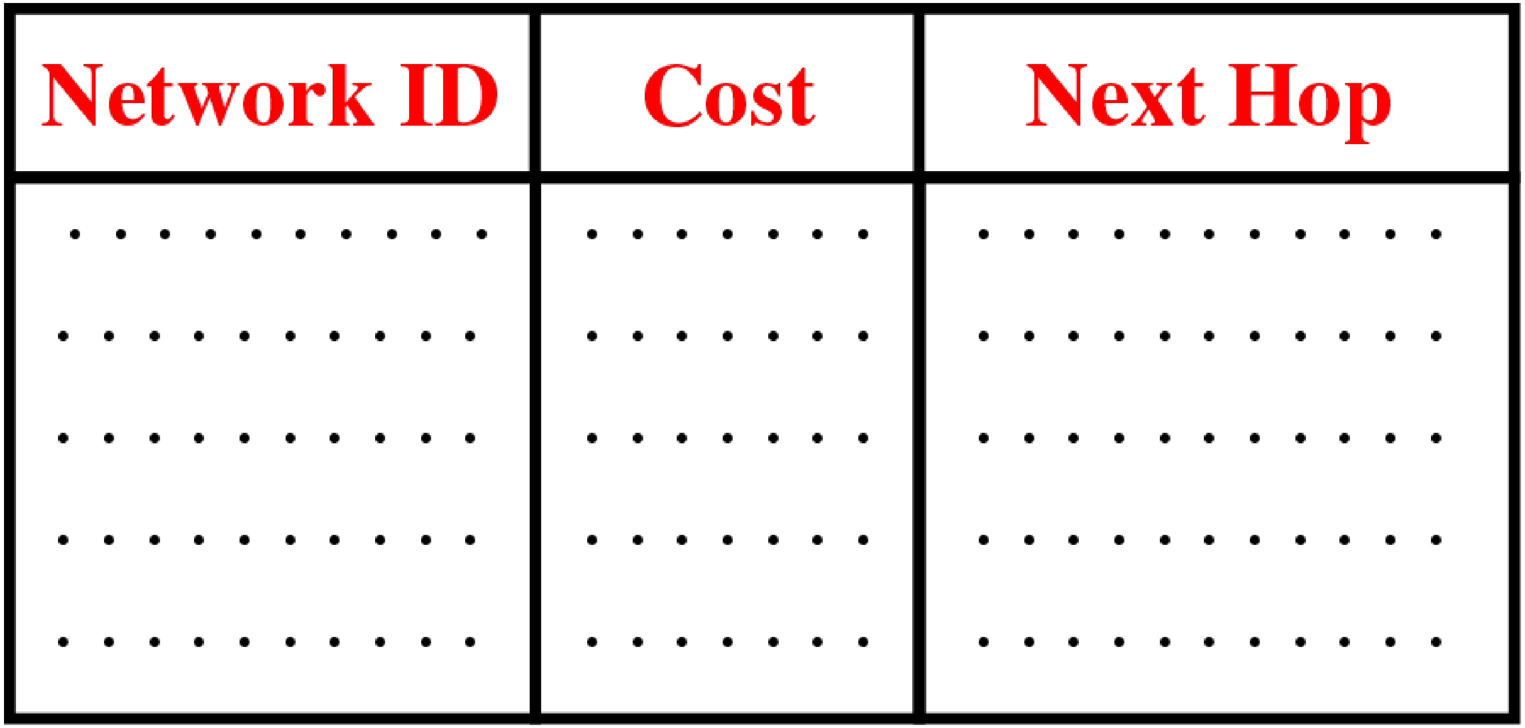
I periodically send my knowledge about the whole internetwork to B, D.

I periodically send my knowledge about the whole internetwork to A.

I periodically send my knowledge about the whole internetwork to A, D.

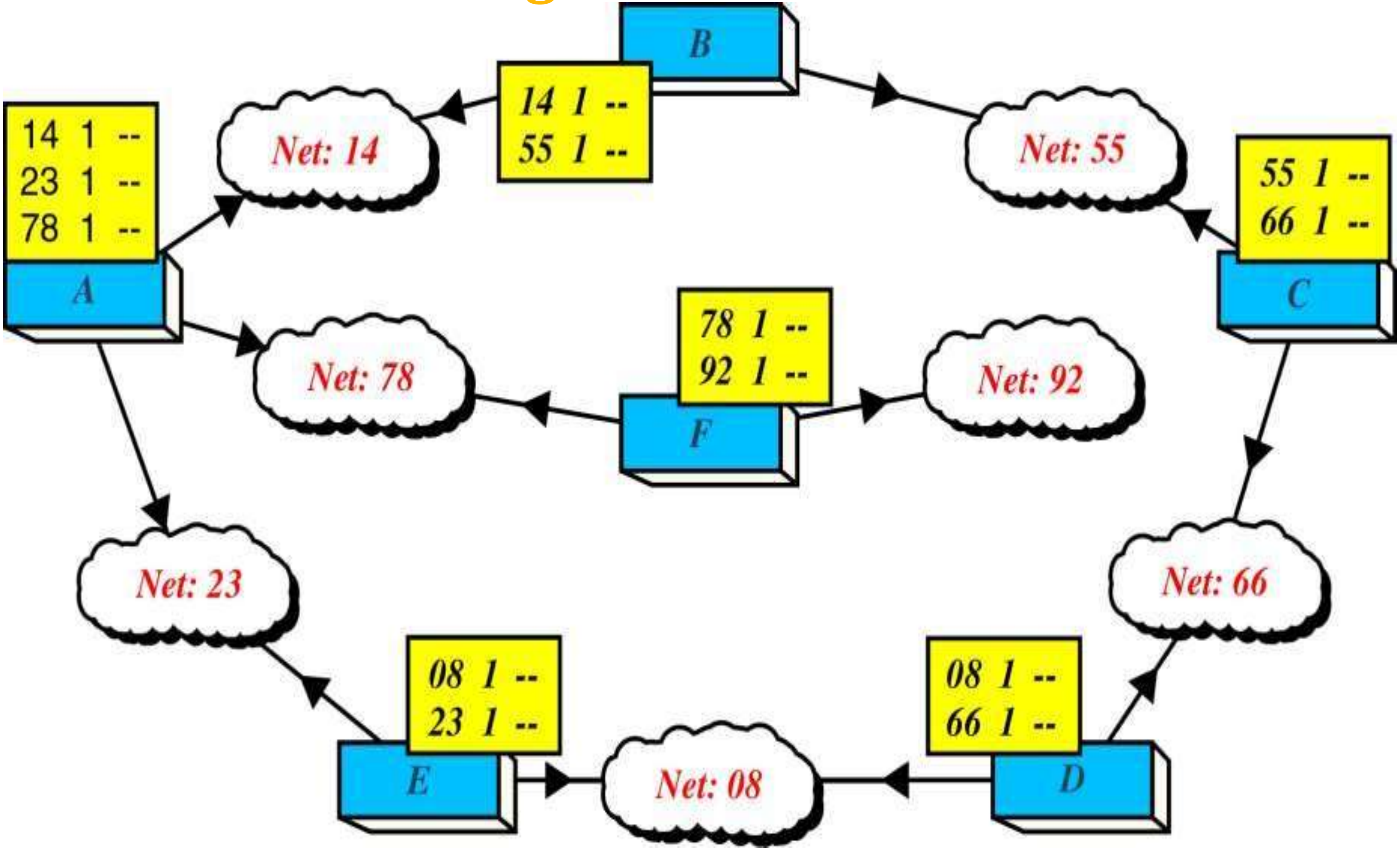
I periodically send my knowledge about the whole internetwork to C, E.

# Distance Vector Routing Table



| Network ID | Cost | Next Hop |
|---|---|---|
| • • • • • • • • • • | • • • • • • • | • • • • • • • • • • • |
| • • • • • • • • • • | • • • • • • • | • • • • • • • • • • • |
| • • • • • • • • • • | • • • • • • • | • • • • • • • • • • • |
| • • • • • • • • • • | • • • • • • • | • • • • • • • • • • • |
| • • • • • • • • • • | • • • • • • • | • • • • • • • • • • • |

# Routing Table Distribution



| | | |
|---|---|---|
| 14 | 1 | -- |
| 23 | 1 | -- |
| 78 | 1 | -- |

A

| | | |
|---|---|---|
| 14 | 1 | -- |
| 55 | 1 | -- |

B

| | | |
|---|---|---|
| 55 | 1 | -- |
| 66 | 1 | -- |

C

| | | |
|---|---|---|
| 78 | 1 | -- |
| 92 | 1 | -- |

F

| | | |
|---|---|---|
| 08 | 1 | -- |
| 23 | 1 | -- |

E

| | | |
|---|---|---|
| 08 | 1 | -- |
| 66 | 1 | -- |

D

Net: 14

Net: 55

Net: 78

Net: 92

Net: 23

Net: 66

Net: 08

# Link State Routing

Def:

□ Each router shares its knowledge of it neighborhood with all routers in the internetwork.

□It is represented by directed graph with weight.

Key work:

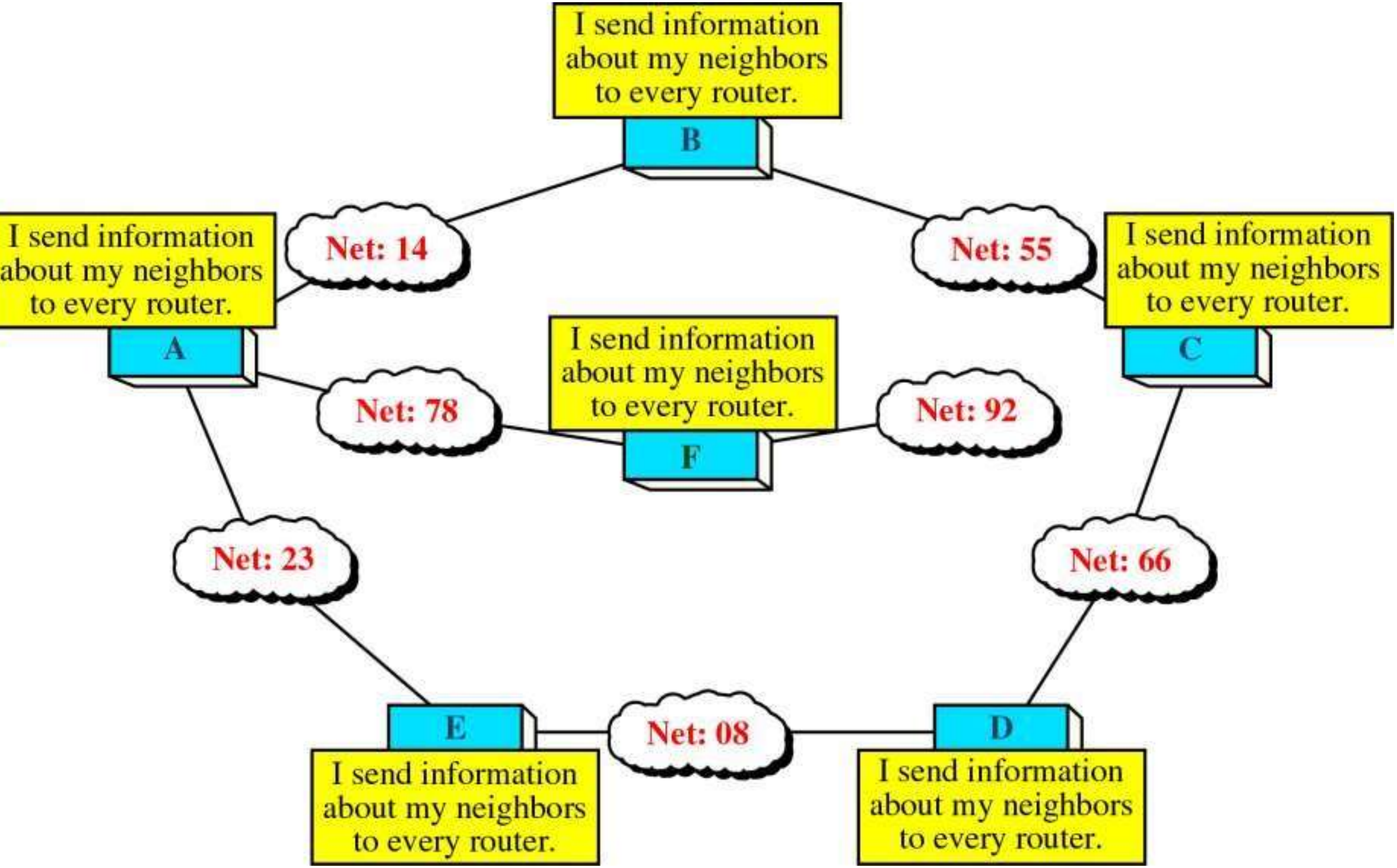
□ Each router shares its knowledge about the neighborhood

□ Each router sends its knowledge to all router.

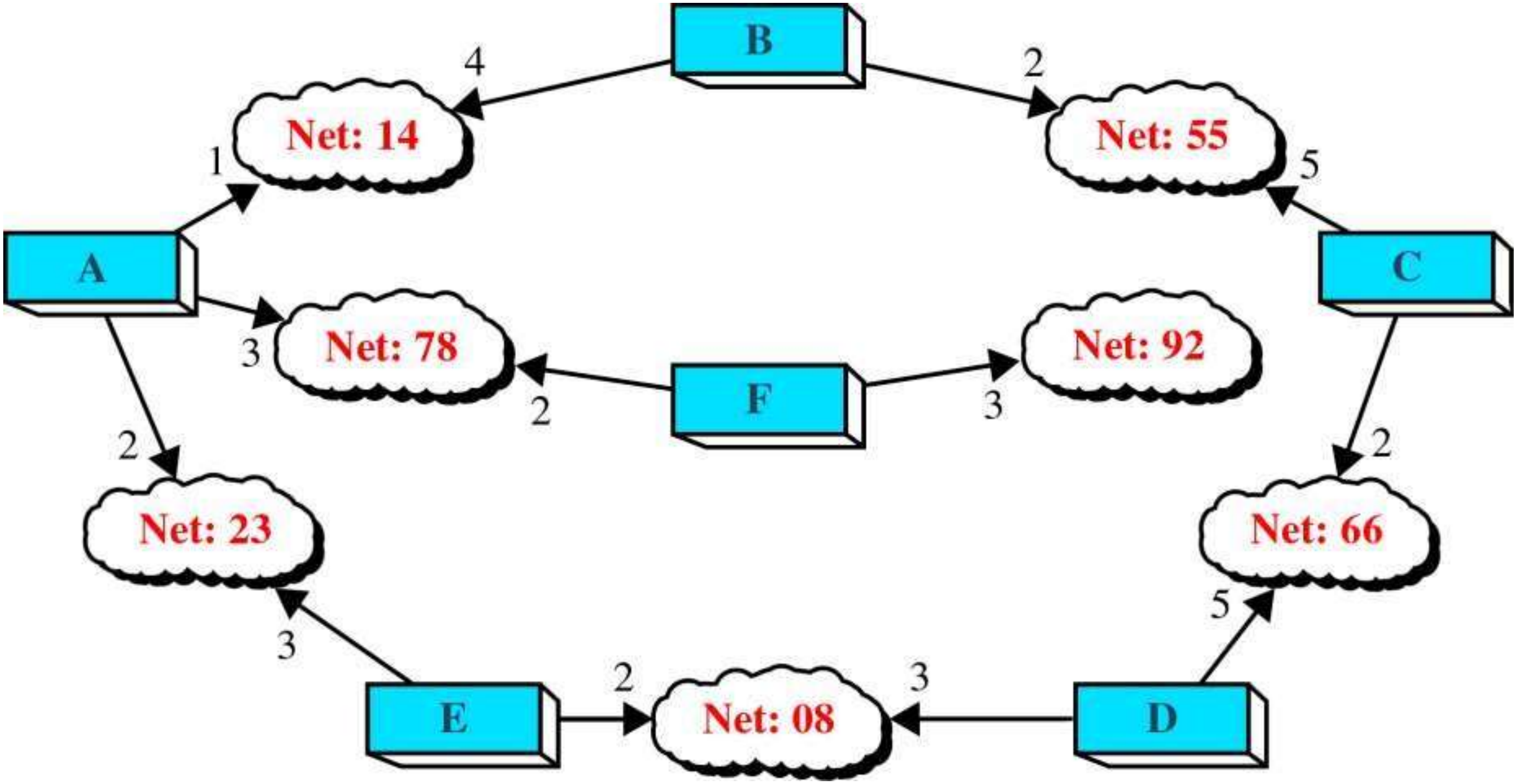
**Flooding** -> Each router share info to neighbor, The neighbor to its own neighbor and so on.,

□ Information sharing when there is a **change.**

# Concept of Link State Routing


I send information about my neighbors to every router.
B
I send information about my neighbors to every router.
A
Net: 14
Net: 55
I send information about my neighbors to every router.
C
I send information about my neighbors to every router.
F
Net: 78
Net: 92
Net: 23
Net: 66
E
Net: 08
D
I send information about my neighbors to every router.
I send information about my neighbors to every router.

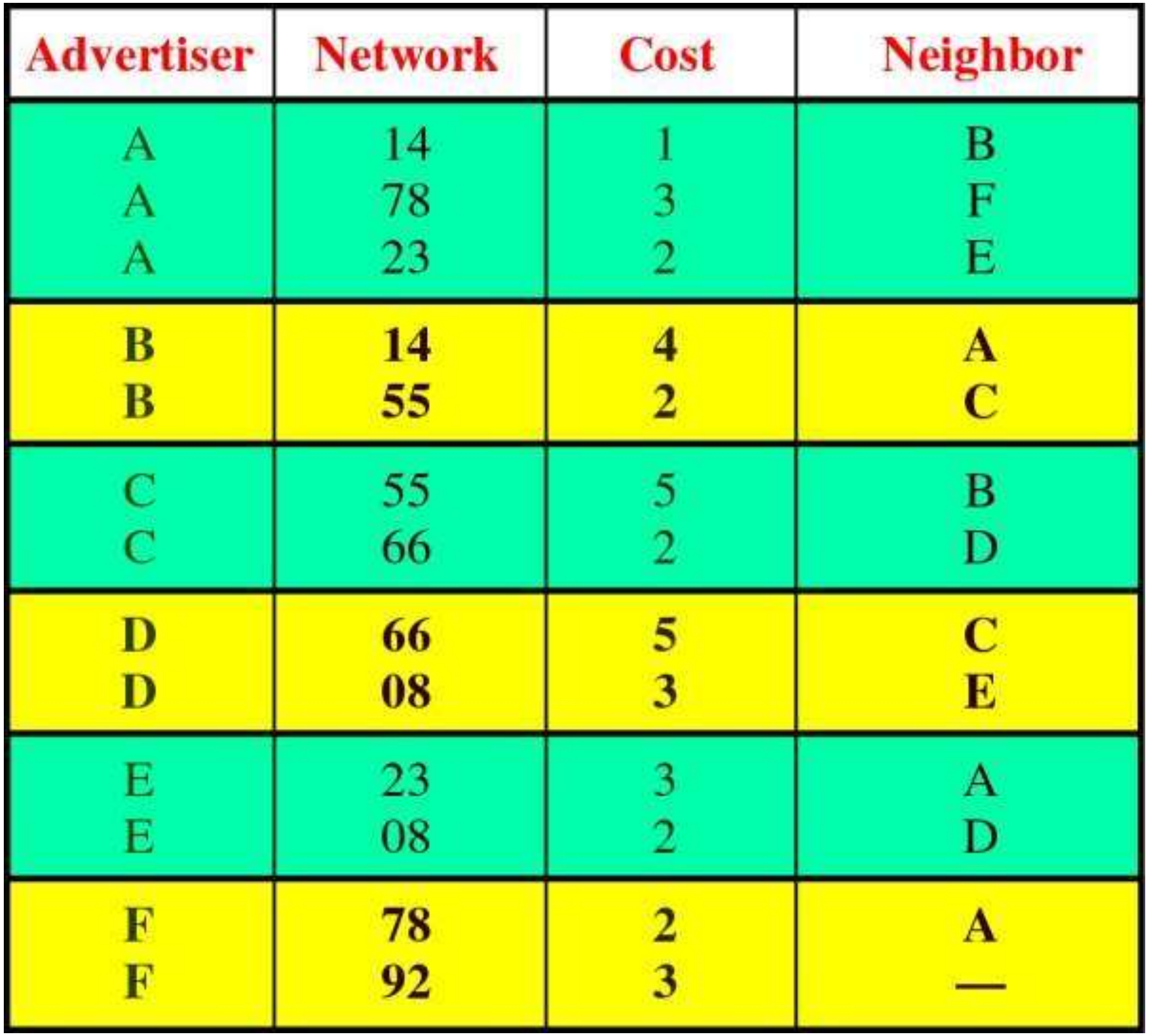
# Cost in Link State Routing



# Link State Packet

| Advertiser | Network | Cost | Neighbor |
|---|---|---|---|
| . . . . . . . | . . . . . . | . . . . . . . . . . . | . . . . . . . . . . . |
| . . . . . . . | . . . . . . | . . . . . . . . . . . | . . . . . . . . . . . |
| . . . . . . . | . . . . . . | . . . . . . . . . . . | . . . . . . . . . . . |

# Link State Database

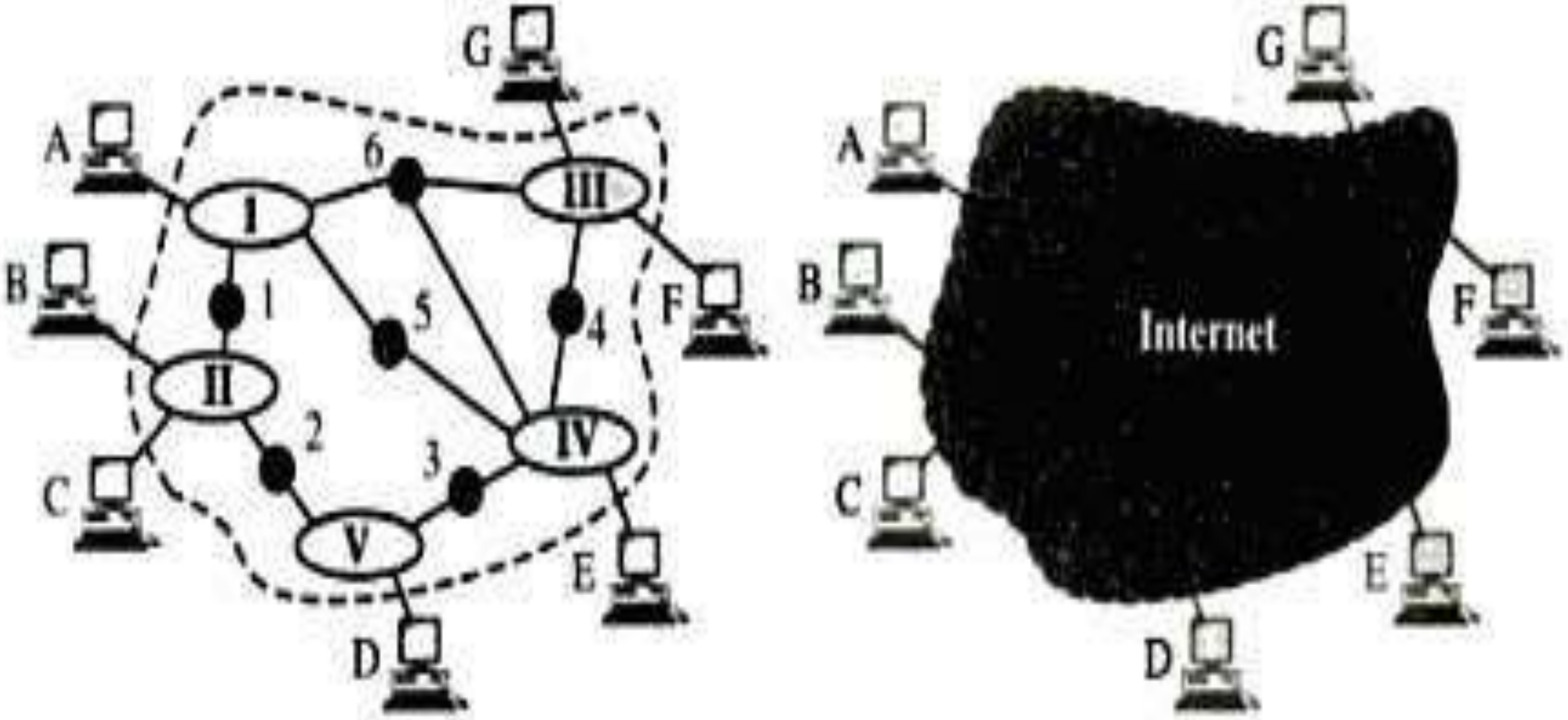


| Advertiser | Network | Cost | Neighbor |
|---|---|---|---|
| A | 14 | 1 | B |
| A | 78 | 3 | F |
| A | 23 | 2 | E |
| B | 14 | 4 | A |
| B | 55 | 2 | C |
| C | 55 | 5 | B |
| C | 66 | 2 | D |
| D | 66 | 5 | C |
| D | 08 | 3 | E |
| E | 23 | 3 | A |
| E | 08 | 2 | D |
| F | 78 | 2 | A |
| F | 92 | 3 | — |

# TCP/IP

- It was developed before OSI
- This project was funded by ARPA of U.S called ARPANET which is turned into TCP/IP
- In internet it acts like a single network connection many of any size and type.
- TCP and UDP creates a data unit called **Segment** or datagram.

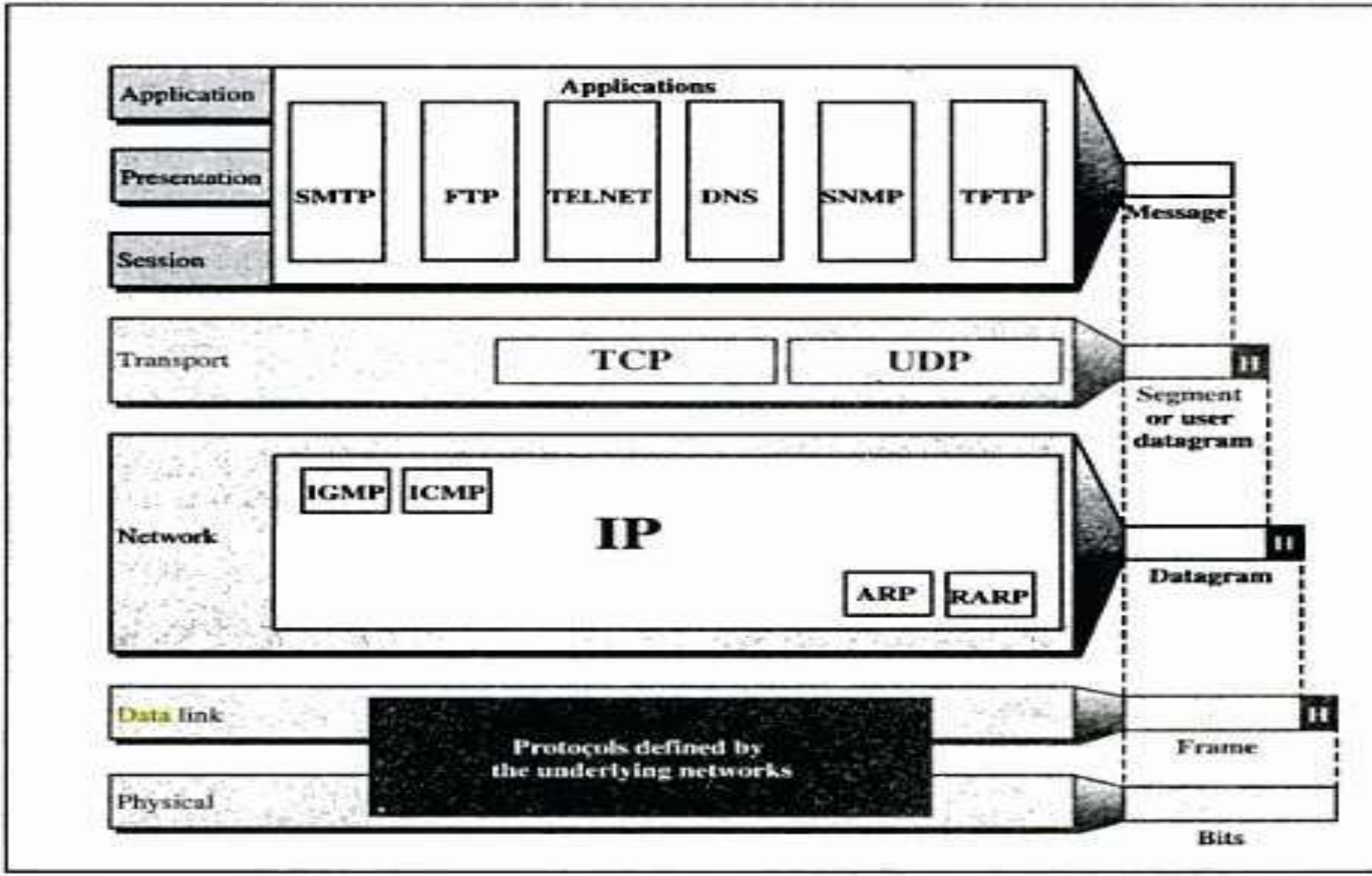
**Figure 24.1** *An internet according to TCP/IP*



a. An actual internet

b. An internet seen by TCP/IP

**Figure 24.2** *TCP/IP and OSI model*



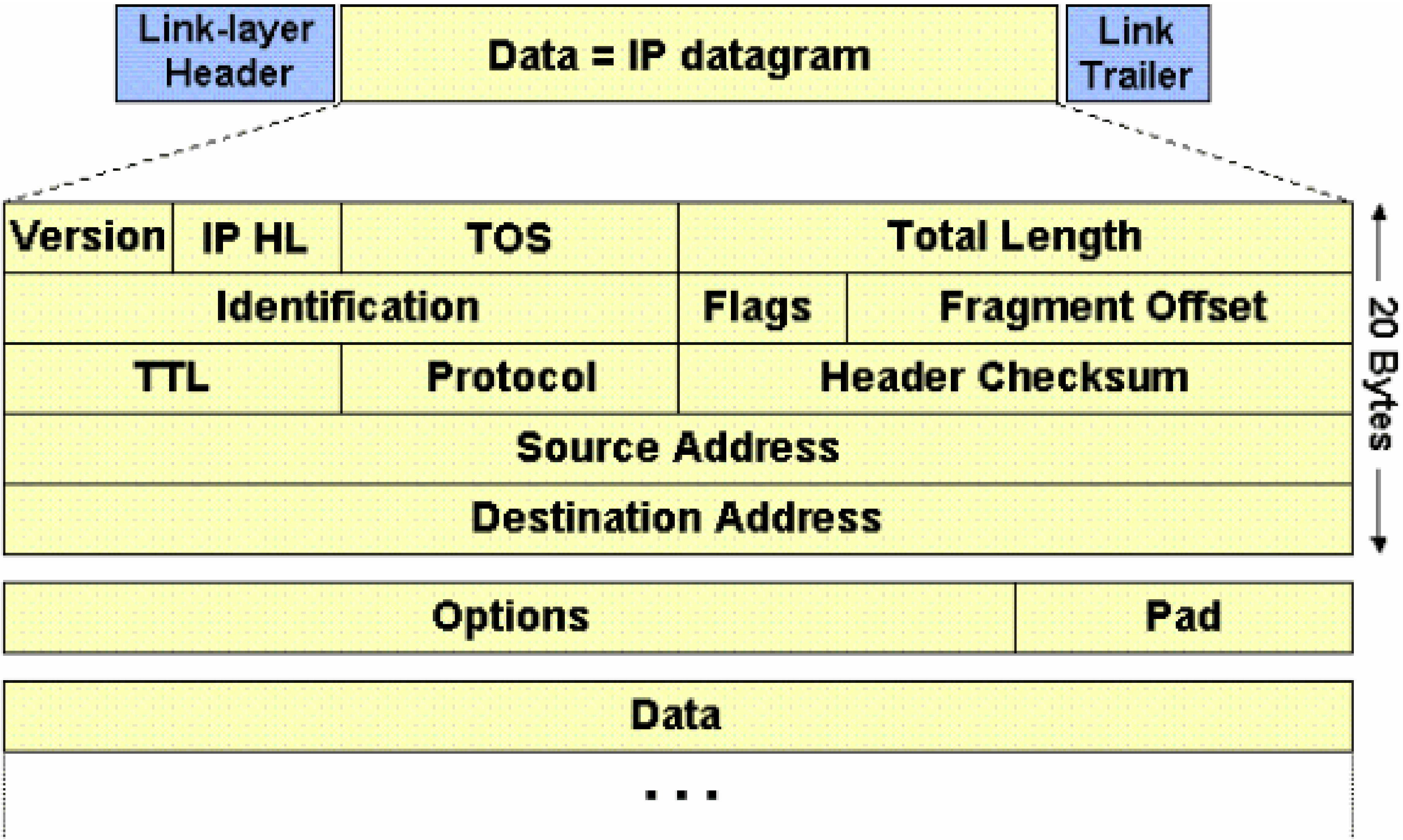
# What is an IP address?

- An **Internet Protocol address** is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
- An IP address serves two principal functions: host or network interface identification and location addressing.

# IP (Internet Proocol)

- □ Network layer of TCP/IP supports IP in turn four other supporting protocol
  - ICMP
  - IGMP
  - ARP
  - RARP
- □ It is a transmission mechanism used by TCP/IP protocols

# IP datagram



Link-layer Header

Data = IP datagram

Link Trailer

| | | | | |
|---|---|---|---|---|
| Version | IP HL | TOS | Total Length | |
| Identification | | | Flags | Fragment Offset |
| TTL | | Protocol | Header Checksum | |
| Source Address | | | | |
| Destination Address | | | | |

20 Bytes

| | |
|---|---|
| Options | Pad |

Data

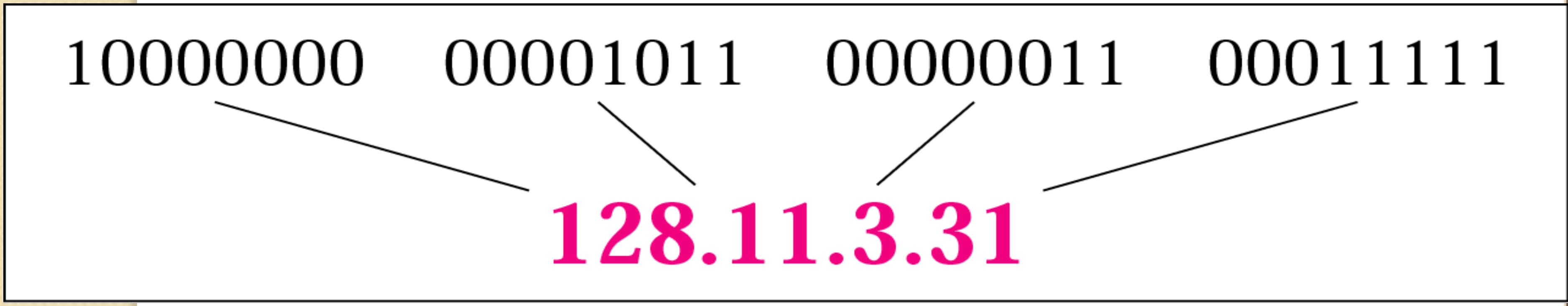
. . .

# Cont.,

- IP Is a unreliable and connection less datagram protocol.
- No error checking or tracking.
- Data transmitted to destination but no guarantees.
- IP must be paired with TCP.

# IP Addressing

- In addition to physical address (NIC) ,to identify each device in the network it requires IP address.
- Address that identify host of its network.
- ***An IP address is a 32-bit address.***
- ***The IP addresses are unique and universal.***
- **It Represented in a Dotted-decimal Notation.**



10000000 00001011 00000011 00011111

**128.11.3.31**

# Example 1

Change the following IP addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11111001 10011011 11111011 00001111

## Solution

**We replace each group of 8 bits with its equivalent decimal number and add dots for separation:**

**a. 129.11.11.239**

**b. 249.155.251.15**

## Example 2

Change the following IP addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 75.45.34.78

## Solution

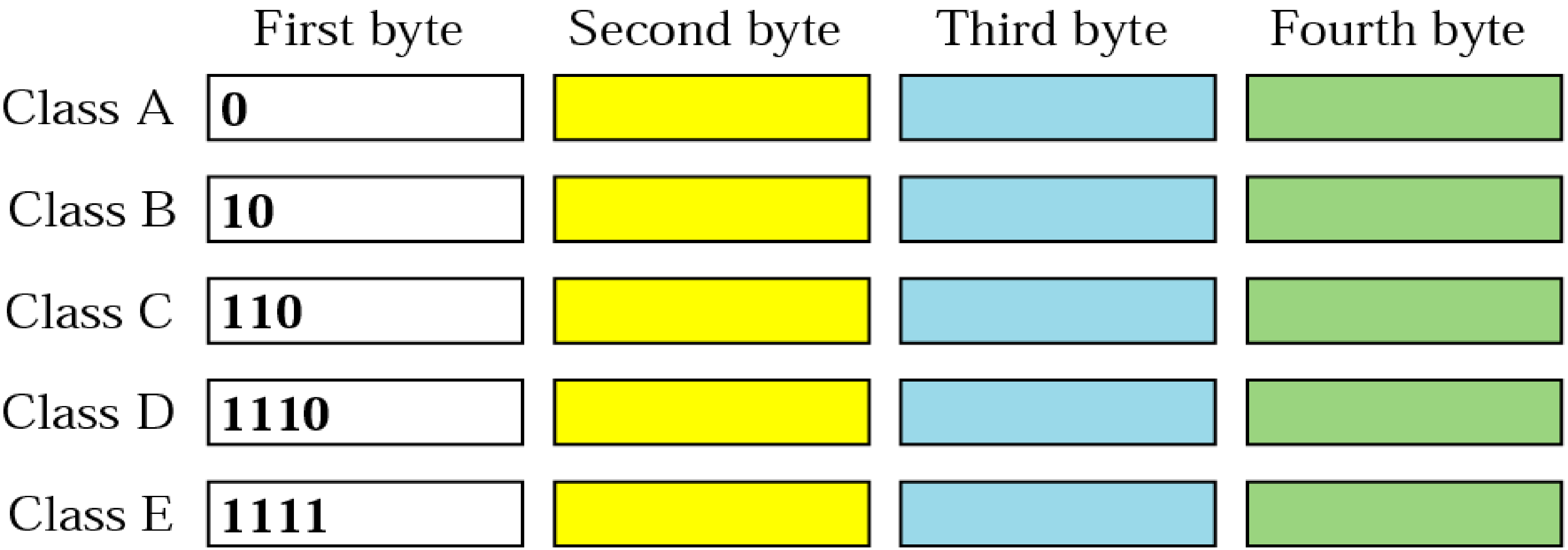
**We replace each decimal number with its binary equivalent (see Appendix B):**

**a. 01101111 00111000 00101101 01001110**
**b. 01001011 00101101 00100010 01001110**

# Classes and Blocks

- **Class A address:** designed for large organizations with a large number of attached hosts or routers. (wasted and not used)
- **Class B address:** designed for midsize organizations with ten of thousands of attached hosts or routers( too large for many organizations)
- **Class C address:** designed for small organizations with a small number of attached hosts or routers.(too small for many organizations)
- **Class D address:** designed for multicasting. (waste of addresses)
- **Class E address:** reserved for future use (waste of addresses)

## Figure 19.10 Finding the class in binary notation



| | First byte | Second byte | Third byte | Fourth byte |
|---|---|---|---|---|
| Class A | **0** | 🟨 | 🟦 | 🟩 |
| Class B | **10** | 🟨 | 🟦 | 🟩 |
| Class C | **110** | 🟨 | 🟦 | 🟩 |
| Class D | **1110** | 🟨 | 🟦 | 🟩 |
| Class E | **1111** | 🟨 | 🟦 | 🟩 |

# Finding the class in decimal notation (changes from 0 to 255)

| | First byte | Second byte | Third byte | Fourth byte |
|---|---|---|---|---|
| Class A | **0 to 127** | 🟨 | 🟦 | 🟩 |
| Class B | **128 to 191** | 🟨 | 🟦 | 🟩 |
| Class C | **192 to 223** | 🟨 | 🟦 | 🟩 |
| Class D | **224 to 239** | 🟨 | 🟦 | 🟩 |
| Class E | **240 to 255** | 🟨 | 🟦 | 🟩 |

## Private and Public IP Address

| Class | Starting IP Address | Ending IP Address | # of Hosts |
|---|---|---|---|
| A | 10.0.0.0 | 10.255.255.255 | 16,777,216 |
| B | 172.16.0.0 | 172.31.255.255 | 1,048,576 |
| C | 192.168.0.0 | 192.168.255.255 | 65,536 |

## *Example 3*

Find the class of each address:

a. **0**0000001 00001011 00001011 11101111

b. **1111**0011 10011011 11111011 00001111

## *Solution*

**See the procedure in Figure 19.11.**

**a. The first bit is 0; this is a class A address.**

**b. The first 4 bits are 1s; this is a class E address.**

## *Example 4*

Find the class of each address:

a. **227**.12.14.87

b. **252**.5.15.111

c. **134**.11.78.56

## *Solution*

**a. The first byte is 227 (between 224 and 239); the class is D.**

**b. The first byte is 252 (between 240 and 255); the class is E.**

**c. The first byte is 134 (between 128 and 191); the class is B.**

# Types of IP address

- Static address
- Dynamic address

- Static IP address
  - manually input by network administrator.
  - manageable for small networks.
  - requires careful checks to avoid duplication.

# Types of IP address

- Dynamic IP address
- examples - BOOTP, DHCP
  - Assigned by server when host boots
  - Derived automatically from a range of addresses
  - Duration of ‘lease’ negotiated, then address released back to server

# Subnetting

- Dividing the network into several smaller groups (subnets) with each group having its own **subnet IP address.**
- Site looks to rest of internet like **single network** and routers outside the organization route the packet based on the main Network address.
- Local routers route within subnetted network using subnet address.

# Subnetting

- □ Host portion of address partitioned into subnet number (most significant part) and host number (least significant part)
- □ In this case, IP address will have **3 levels** (Main network, subnet, host)
- □ **Subnet mask** is a 32-bit consists of zeros and ones that indicates which bits of the IP address are subnet number and which are host number
- □ Subnet mask when AND ed with the IP address it gives the subnetwork address

# Masking.

Masking is a process that extracts the address of the physical network from an IP address.

**Boundary level masking:** Here the mask numbers are either 255 or 0, finding the subnetwork address is very easy.

**Non-boundary level masking.**

If mask numbers are not just 255 or 0, finding the subnetwork address involves using the bitwise AND operators

# Supernetting:

- Supernetting combines several networks into one lager one (Because of Address reduction)

# IP Network Addressing

- INTERNET → world’s largest public data network, doubling in size every nine months
- IPv4, defines a 32-bit address - $2^{32}$ (4,294,967,296) IPv4 addresses available
- The first problem is concerned with the eventual depletion of the IP address space.
- Traditional model of classful addressing does not allow the address space to be used to its maximum potential.

# Classful Addressing

- When IP was first standardized in Sep 1981, each system attached to the IP based Internet had to be assigned a unique 32-bit address
- The 32-bit IP addressing scheme involves a two level addressing hierarchy

| | |
|---|---|
| Network Number/Prefix | Host Number |

# Internet Protocol (IP)

- What is Internet Protocol?
  - Internet Protocol is a set of technical rules that defines how computers communicate over a network.
  - Currently, There are two versions of IP
    - IP version 4 (IPv4)
    - IP version 6 (IPv6).

# Internet Protocol (IP)

- What is IPv4?
  - IPv4 was the first version of Internet Protocol to be widely used, and accounts for most of today’s Internet traffic.
  - There are just over 4 billion IPv4 addresses. While that is a lot of IP addresses, it is not enough to last forever.

# Internet Protocol (IP)

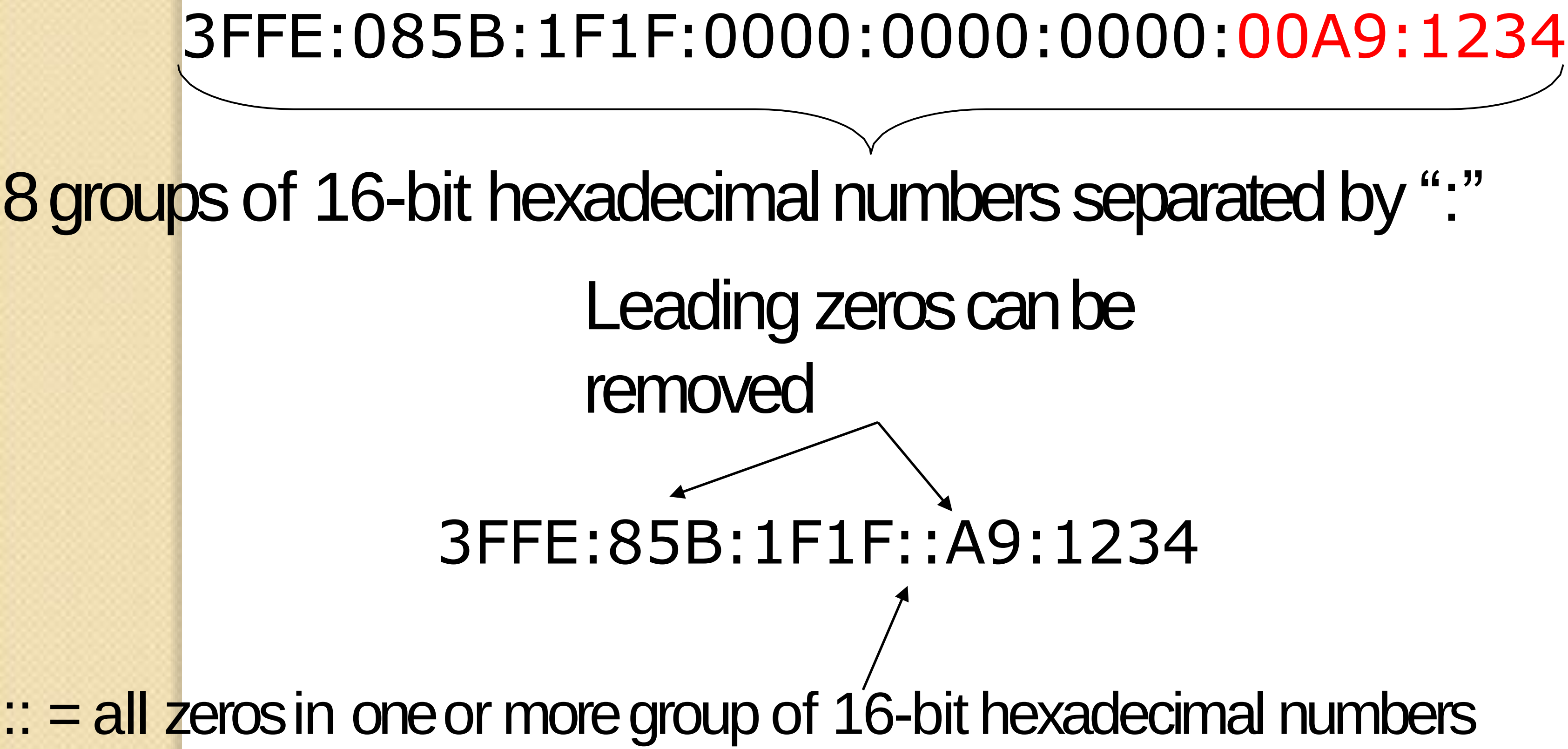
- What is IPv6?
  - IPv6 is a newer numbering system that provides a much larger address pool than IPv4. It was deployed in 1999 and should meet the world’s IP addressing needs well into the future.

# Internet Protocol (IP)

- What is the major difference?
  - The major difference between IPv4 and IPv6 is the number of IP addresses.

  - There are 4,294,967,296 IPv4 addresses.
  - while, there are 340,282,366,920,938,463,463,374,607,431,768,211,456 IPv6 addresses.

# 128-bit IPv6 Address



3FFE:085B:1F1F:0000:0000:0000:00A9:1234

8 groups of 16-bit hexadecimal numbers separated by “:”

Leading zeros can be removed

3FFE:85B:1F1F::A9:1234

:: = all zeros in one or more group of 16-bit hexadecimal numbers

# IPv4 vs. IPv6

| | IPv6 |
|---|---|
| IPv4 addresses are 32 bit length. | IPv6 addresses are 128 bit length. |
| IPv4 addresses are binary numbersrepresented in decimals. | IPv6 addresses are binary numbers represented in hexadecimals. |
| IPSec support is only optional. | Inbuilt IPSec support. |
| Fragmentation is done by sender and forwarding routers. | Fragmentation is done only by sender. |

| | |
|---|---|
| No packet flow identification. | Packet flow identification is available within the IPv6 header using the Flow Label field. |
| Checksum field is available in IPv4 header | No checksum field in IPv6 header. |
| Options fields are available in IPv4 header. | No option fields, but IPv6 Extension headers are available. |
| Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses. | Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP). |

| | |
|---|---|
| Internet Group Management Protocol (IGMP) is used to manage multicast group membership. | IGMP is replaced with Multicast Listener Discovery (MLD) messages. |
| Broadcast messages are available. | Broadcast messages are not available. Instead a link- local scope "All nodes" multicast IPv6 address(FF02::1) is used for broadcast similar functionality. |
| Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic Host configuration Protocol) | Auto-configuration of addresses is available. |

# IPv4 companion protocols (1)

- ARP: Address Resolution Protocol
  - Mapping from IP address to MAC address
- ICMP: Internet Control Message Protocol
  - Error reporting & Query
- IGMP: Internet Group Management Protocol
  - Multicast member join/leave
- Unicast Routing Protocols (Intra-AS)
  - Maintaining Unicast Routing Table
  - E.g. RIP, OSPF (Open Shortest Path First)

# IPv4 companion protocols (2)

- Multicast Routing Protocols
  - Maintaining Multicast Routing Table
  - E.g. DVMRP, MOSPF, CBT, PIM
- Exterior Routing Protocols (Inter-AS)
  - E.g. BGP (Border Gateway Protocol)
- Quality-of-Service Frameworks
  - Integrated Service (ISA, IntServ)
  - Differentiated Service (DiffServ)

# Why IPv6?

- Deficiency of IPv4
- Address space exhaustion
- New types of service → Integration
  - Multicast
  - Quality of Service
  - Security
  - Mobility (MIPv6)
- Header and format limitations

# Advantages of IPv6 over IPv4

- Larger address space
- Better header format
- New options
- Allowance for extension
- Support for resource allocation
- Support for more security
- Support for mobility

# THANK YOU

# UNIT IV

# TRANSPORT LAYER

Transport layer – service – Connection establishment – Flow control – Transmission control protocol – Congestion control and avoidance – User datagram protocol - Transport for Real Time Applications (RTP).

# UNIT – IV

## TRANSPORT LAYER

# OVERVIEW

- **Transport Layer**
- **Service**
- **Connection Establishment**
- **Flow Control**
- **Congestion Control and Avoidance**
- **Transmission Control Protocol**
- **User Datagram Protocol**
- **Transport for Real Time Applications (RTP).**

# Transport Layer

- The Transport layer is responsible for **process-to-process or end-end** delivery of the entire message.
- The transport layer ensures that the whole message arrives intact and overseeing both **Error control and flow control at the process-to-process level.**

# Transport Layer
## Functions

- Service point addressing(Process-Process delivery)
- Segmentation and reassembly
- Connection control
- Flow control(QoS) – MUX & Demux
- Error control – error checking and recovery
- Congestion control

# Transport Layer
## Services

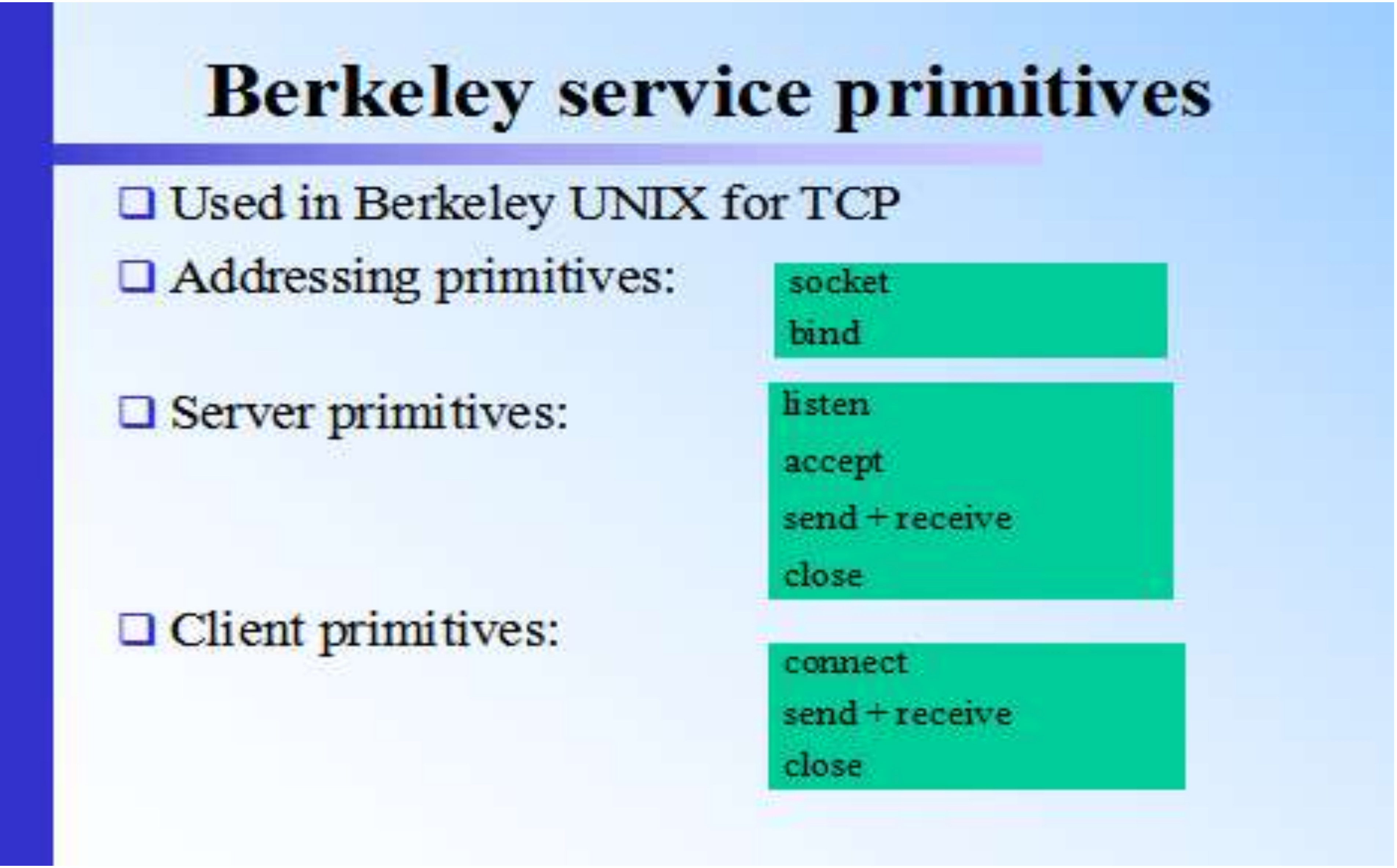
- Transport Layer Provides :
- **Efficient**
- **Reliable and**
- **Cost-effective services**
- Another TWO Kinds of Services are :
  - **Connection oriented - TCP**
  - **Connectionless - UDP**

# Simple Service: Primitives

- Simple primitives:
  - Connect
  - Send
  - Receive
  - Disconnect
- How to handle incoming connection request in server process?

  ➔Wait for connection request from client!
  - listen

# Berkeley service : Primitives



## Berkeley service primitives

□ Used in Berkeley UNIX for TCP

□ Addressing primitives:

socket
bind

□ Server primitives:

listen
accept
send + receive
close

□ Client primitives:

connect
send + receive
close

# Connection Establishment

- Once a connection is established, both client and server may exachnge data using several system calls.
- A connection is typically used for client-server interaction.
- A server advertizes a particular server at a well-known address and clients establish connections to that socket to avail of the offered service.
- Thus the connection estblishment procedure is asymmetric.

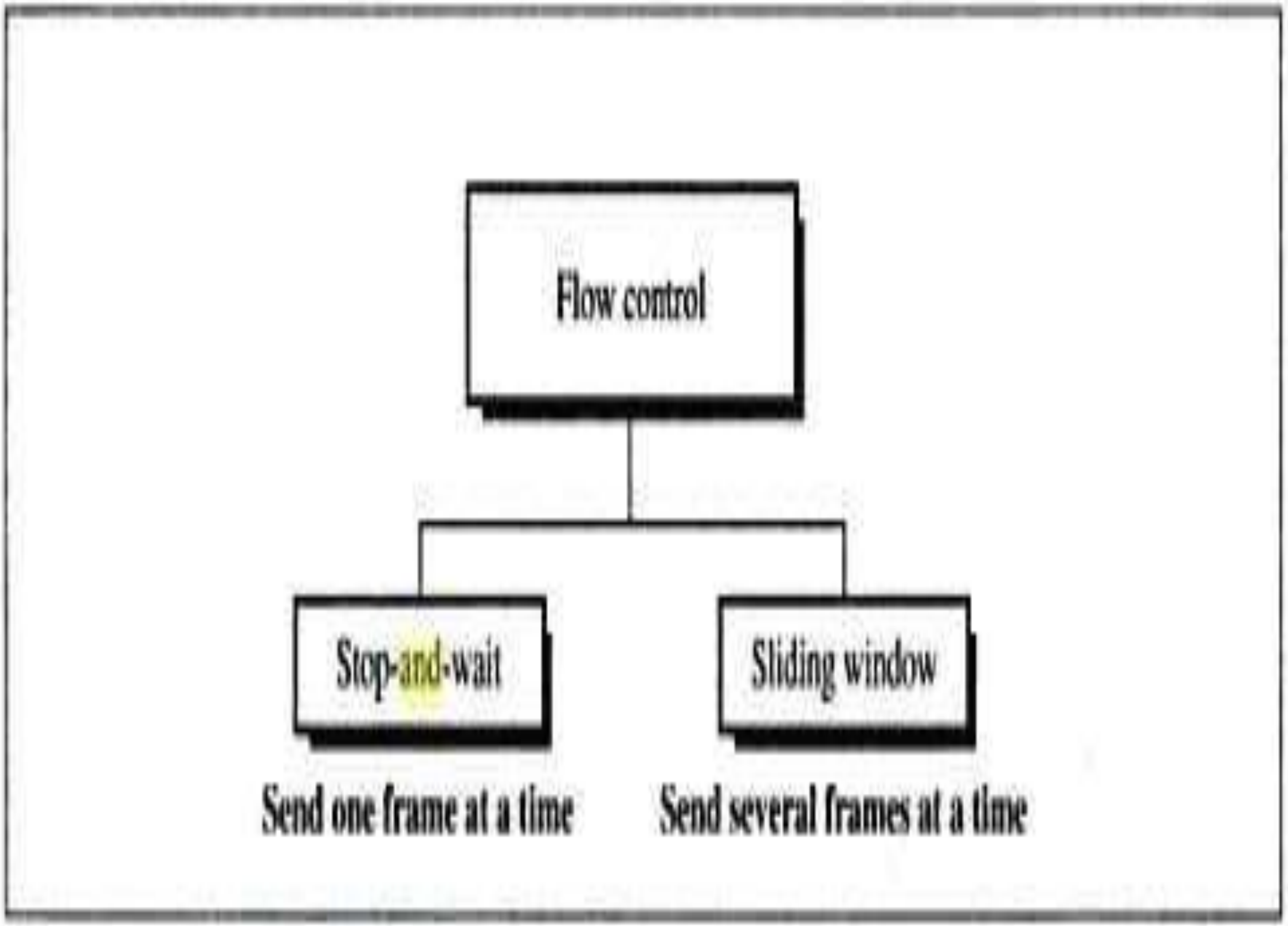
- –**Problems to solve**
  - Selection of the initial sequence number for a new connection.
  - Wrap around of sequence numbers for an active connection.
  - It Handle host crashes.

# Releasing a connection

- Asymmetric
  - Connection broken when one party hangs up
  - Abrupt! ➔ may result in data loss
- Symmetric
  - Both parties should agree to release connection
  - How to reach agreement? Two-army problem
  - Solution: three-way-handshake
- Pragmatic approach
  - Connection = 2 unidirectional connections
  - Sender can close unidirectional connection

# Flow Control

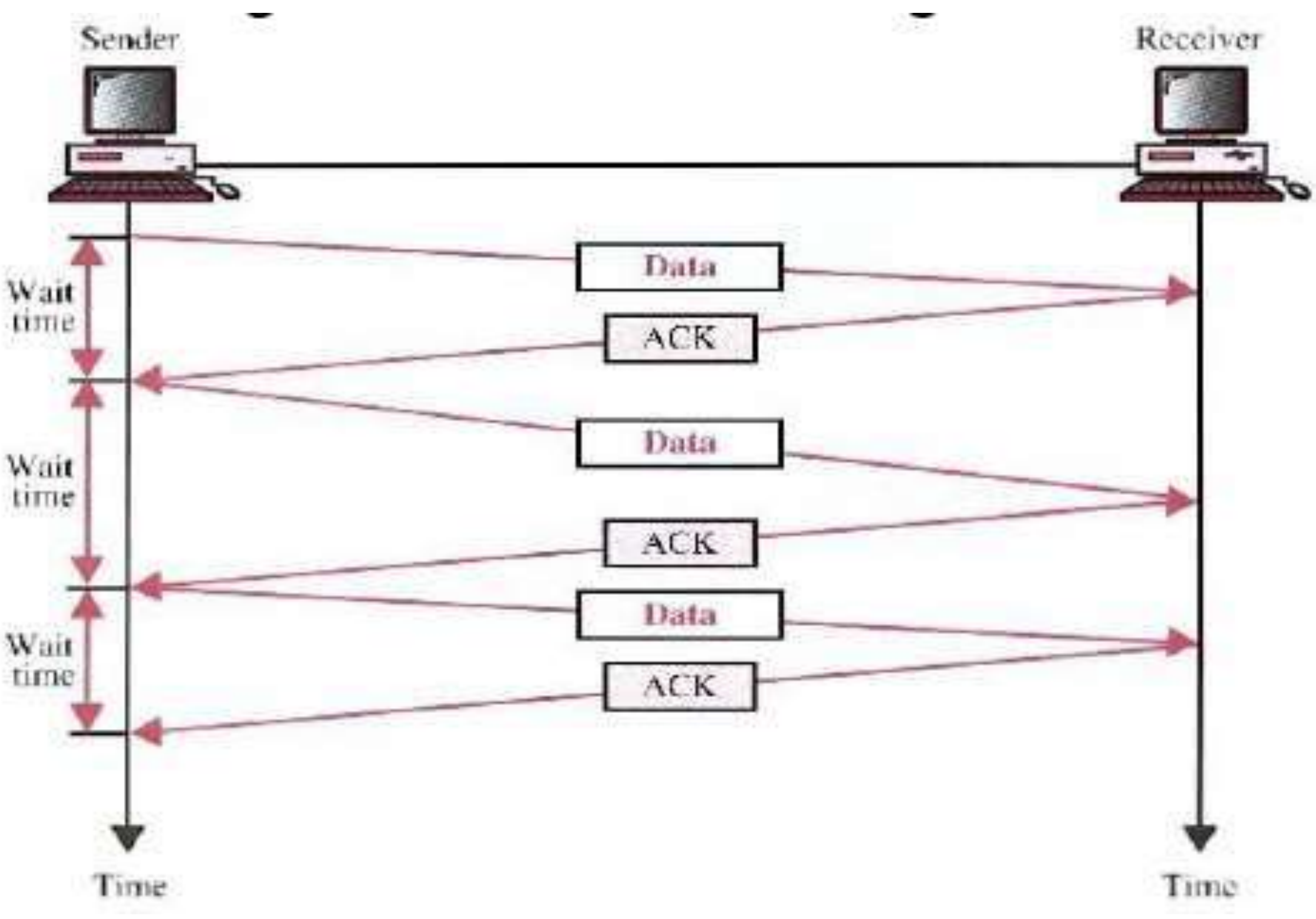
- It is a set of procedures to tell the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
- Two categories of flow control:
  - **Stop-and-wait**
    - Send one frame at a time.
  - **Sliding window**
    - Send several frames at a time.



Flow control
Stop-and-wait
Sliding window
Send one frame at a time
Send several frames at a time

# Stop-and-wait

- Sender sends one frame and waits for an acknowledgement before sending the next frame.

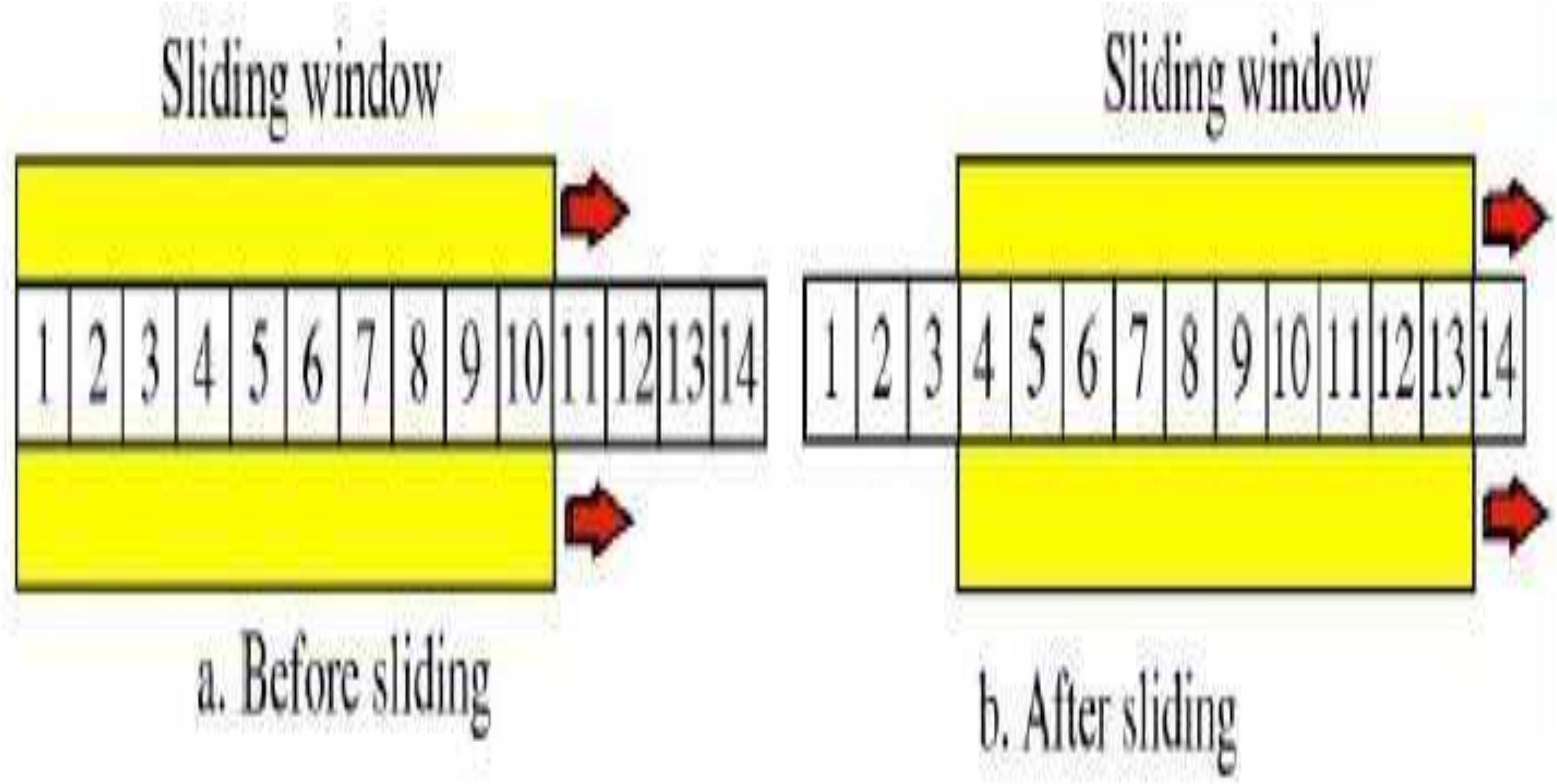


# Stop-and-wait

- Advantages:
  - Simplicity.
  - Each frame is checked and acknowledged before the next frame is sent.
- Disadvantages:
  - Slow.
    - Can add significantly to the total transmission time if the distance between devices is long.
  - Inefficiency
    - Each frame is alone on the line.

# SlidingWindow

- Sender can send several frames before needing an acknowledgement.
- Advantages:
  - The link can carry several frames at once.
  - Its capacity can be used efficiently.



a. Before sliding

b. After sliding

# Congestion Control and Avoidance

- Congestion Control is concerned with efficiently using a network at high load.
- Several techniques can be employed. These include:
- – Warning bit
  - Choke packets
  - Load shedding

Detection

  - Random Early Discard
  - Traffic shaping

Avoidance

- **The first 3 deal with congestion detection and Control. The last 2 deal with congestion avoidance.**

# Principles of Congestion Control

Congestion:

❿ informally: “too many sources sending too much data too fast for *network* to handle”

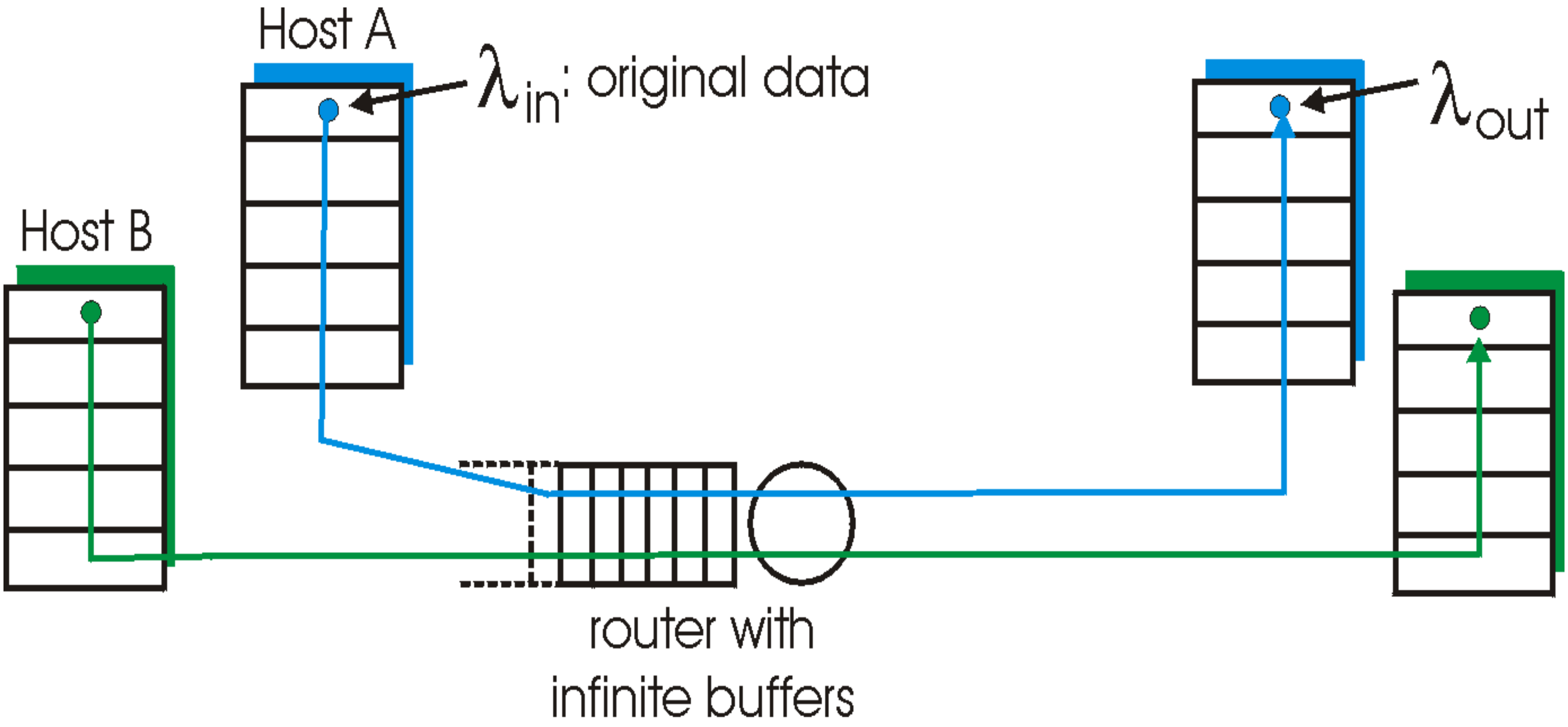
❿ different from flow control!

= end-to-end issue!

- lost packets (buffer overflow at routers)
- long delays (queue-ing in router buffers)

# Causes of Congestion

- Two senders, Two receivers
- One router, Infinite buffers
- No retransmission



# Approaches towards congestion control

Two broad approaches towards congestion control:

## End-to-End congestion control:

❿ no explicit feedback from network

❿ congestion inferred from end-system observed loss, delay

❿ approach taken by TCP

## Network-assisted congestion control:

❿ routers provide feedback to end systems

- – single bit indicating congestion (SNA, ATM)
- – explicit rate sender should send it.

# Congestion Detection and Control

**The following 3 Methods are used to Detect & Control the Congestions :**

1. **Warning bit**
2. **Choke packets**
3. **Load shedding**

# Warning Bit

- A special bit in the packet header is set by the router to **warn the source** when congestion is detected.
- The bit is copied and piggy-backed on the ACK and sent to the sender.
- The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly.

# Choke Packets

- A more direct way of telling the source to **slow down**.
- A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.
- The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.
- An example of a choke packet is the ICMP Source Quench Packet.

# Load Shedding

- When buffers become full, routers simply discard packets.
- Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer.
- For a file transfer, for, e.g. cannot discard older packets since this will cause a gap in the received data.
- For real-time voice or video it is probably better to throw away old data and keep new packets.
- Get the application to mark packets with discard priority.

# Congestion Avoidance

**The following 2 Methods are used to Avoid the Congestions :**

1. **Random Early Discard**
2. **Traffic Shaping**

# Random Early Discard (RED)

- This is a proactive approach in which the router discards one or more packets *before* the buffer becomes completely full.
- Each time a packet arrives, the RED algorithm computes the average queue length, ***avg***.
- If *avg* is lower than some lower threshold, congestion is assumed to be minimal or non-existent and the packet is queued.

# RED, cont.

- If *avg* is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded.
- If *avg* is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated.

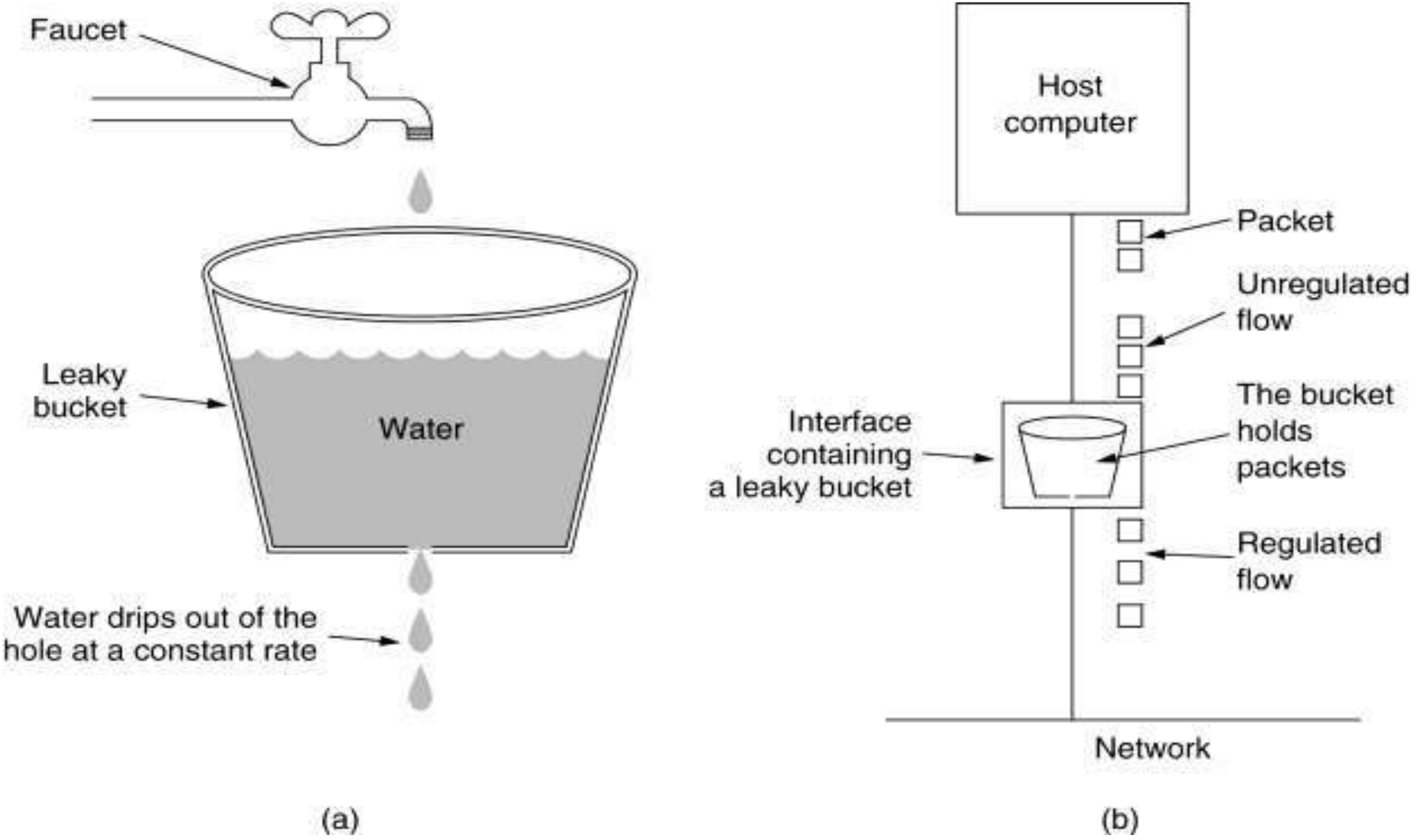
# Traffic Shaping

- Another method of congestion Avoidance is to “shape” the traffic before it enters the network.
- Traffic shaping controls the *rate* at which packets are sent (not just how many). Used in ATM and Integrated Services networks.
- At connection set-up time, the sender and carrier negotiate a traffic pattern (shape).
- Two traffic shaping algorithms are:
  - Leaky Bucket
  - Token Bucket

# The Leaky Bucket Algorithm

- The **Leaky Bucket Algorithm** used to control rate in a network. It is implemented as a single-server queue with constant service time. If the bucket (buffer) overflows then packets are discarded.

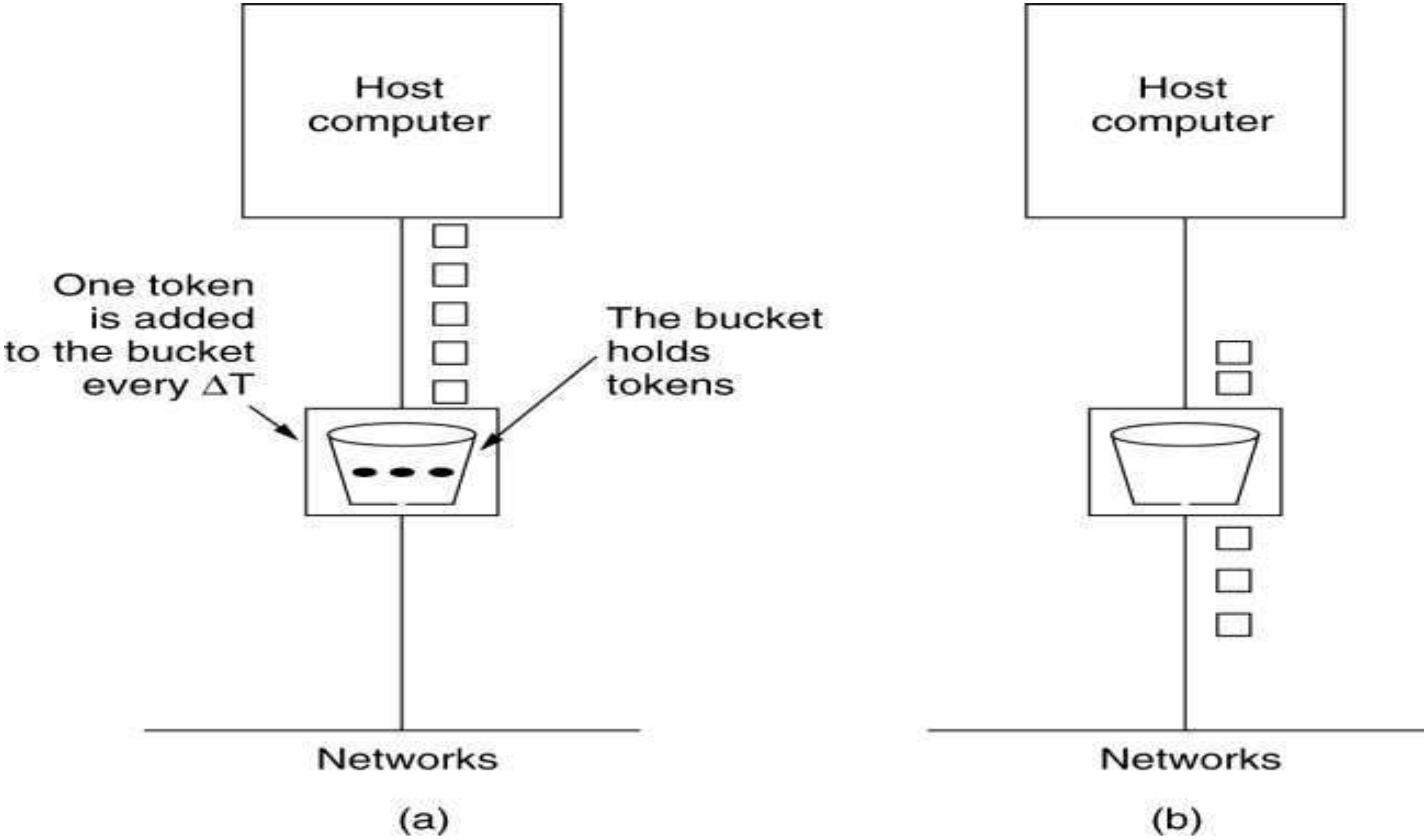
# The Leaky Bucket Algorithm



(a)A leaky bucket with water. (b) a leaky bucket with packets.

# Token Bucket Algorithm

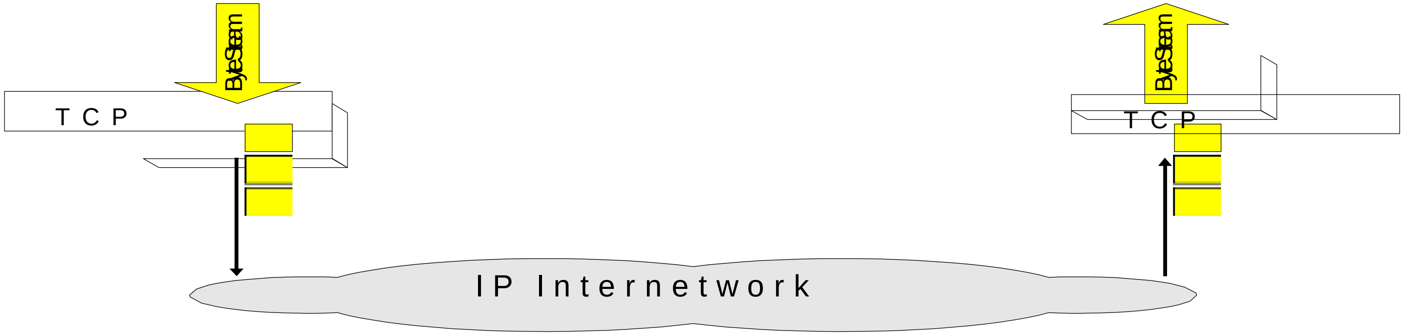
- In contrast to the LB, the Token Bucket Algorithm, allows the output rate to vary, depending on the size of the burst.
- In the TB algorithm, the bucket holds tokens. To transmit a packet, the host must capture and destroy one token.
- Tokens are generated by a clock at the rate of one token every sec.
- Idle hosts can capture and save up tokens (up to the max. size of the bucket) in order to send larger bursts later.



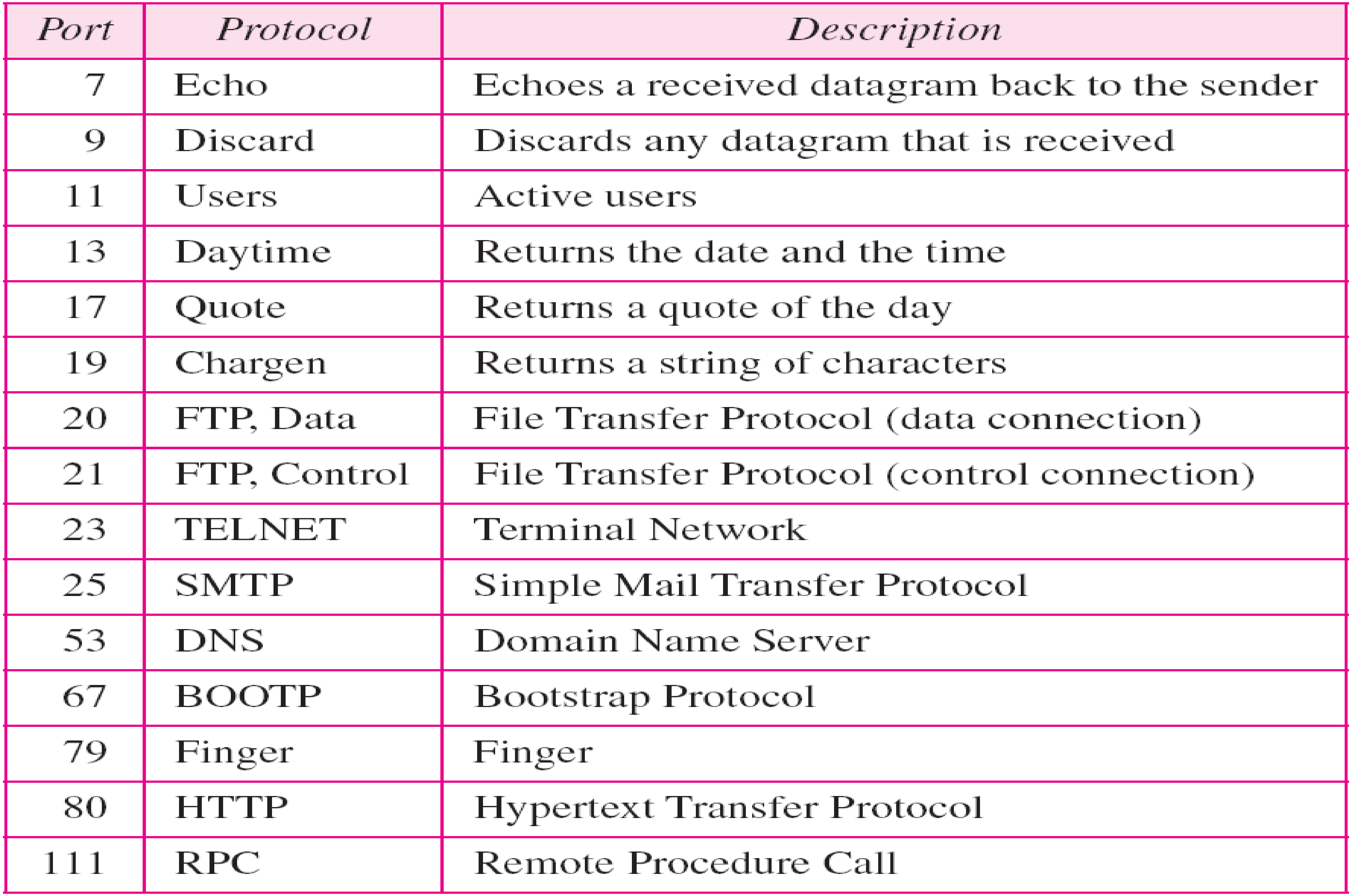
(a) Before. (b) After.

# Transmission Control Protocol

- TCP is **reliable protocol**. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender
- It ensures the data packet is reached the destination or it needs to resend it.
- TCP provides **end-to-end** communication.
- TCP provides full duplex server

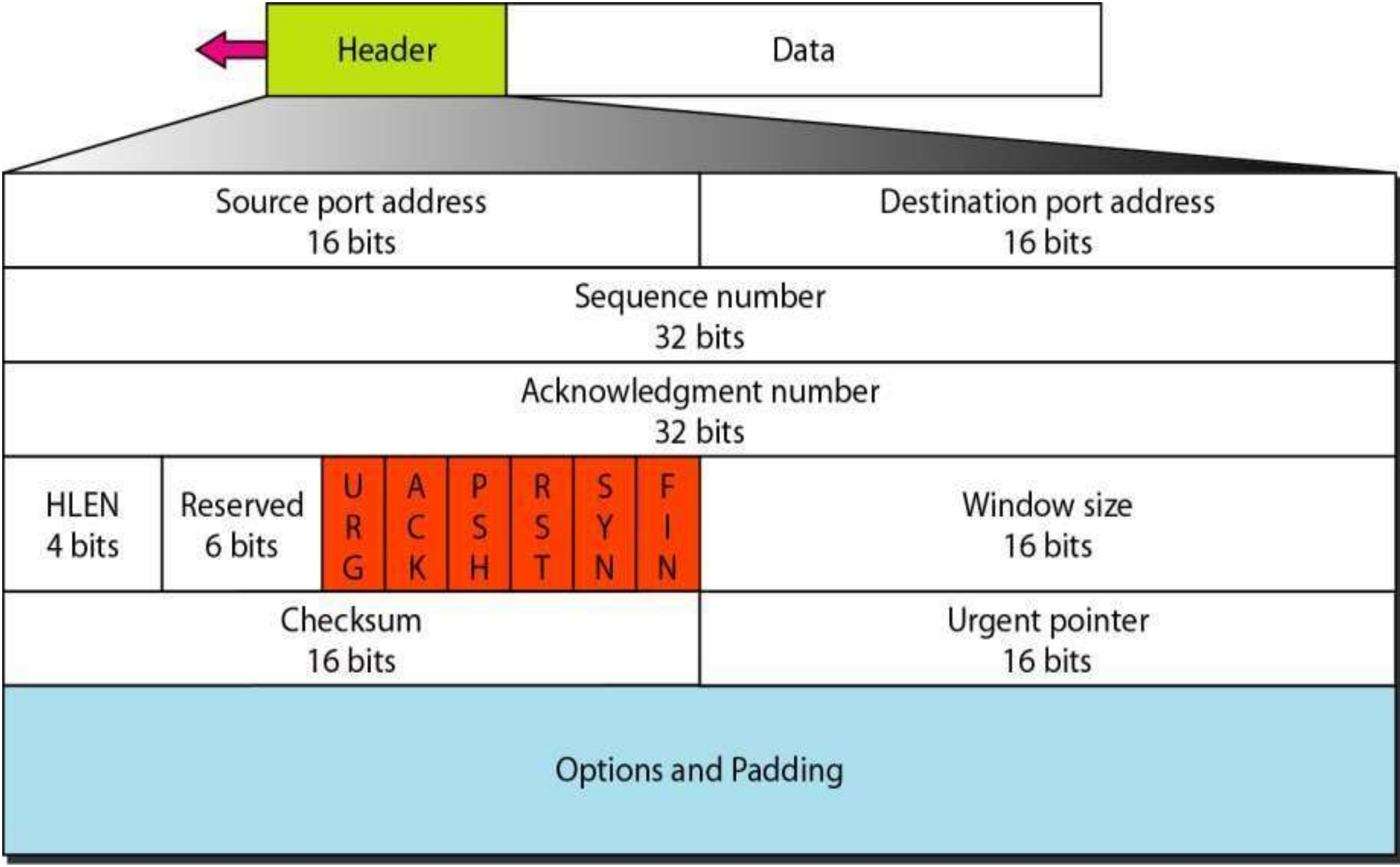


# Well-known ports used by TCP



| Port | Protocol | Description |
|---|---|---|
| 7 | Echo | Echoes a received datagram back to the sender |
| 9 | Discard | Discards any datagram that is received |
| 11 | Users | Active users |
| 13 | Daytime | Returns the date and the time |
| 17 | Quote | Returns a quote of the day |
| 19 | Chargen | Returns a string of characters |
| 20 | FTP, Data | File Transfer Protocol (data connection) |
| 21 | FTP, Control | File Transfer Protocol (control connection) |
| 23 | TELNET | Terminal Network |
| 25 | SMTP | Simple Mail Transfer Protocol |
| 53 | DNS | Domain Name Server |
| 67 | BOOTP | Bootstrap Protocol |
| 79 | Finger | Finger |
| 80 | HTTP | Hypertext Transfer Protocol |
| 111 | RPC | Remote Procedure Call |

# Figure : *TCP segment format*



Header

Data

Source port address
16 bits

Destination port address
16 bits

Sequence number
32 bits

Acknowledgment number
32 bits

HLEN
4 bits

Reserved
6 bits

URG

ACK

PSH

RST

SYN

FIN

Window size
16 bits

Checksum
16 bits

Urgent pointer
16 bits

Options and Padding

# TCP Header

- The length of TCP header is minimum 20 bytes long and maximum 60 bytes.
- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.

- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.

- **Flags (1-bit each)**
- **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
- **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
- **ECE** **-** If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.

- **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
- **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
- **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.

- **RST** - Reset flag has the following features:
  - It is used to refuse an incoming connection.
  - It is used to reject a segment.
  - It is used to restart a connection.
- **SYN** - This flag is used to set up a connection between hosts.
- **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment,
  i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.

- **Options** - It facilitates additional options which are not covered by the regular header.
- Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

# Connection Management in TCP

- **Opening a TCP Connection**
- **Closing a TCP Connection**
- **Special Scenarios**
- **State Diagram**

# TCP Connection Establishment

- TCP uses a **three-way handshake** to open a connection:

**(1)ACTIVE OPEN:** Client sends a segment with

  - SYN bit set *
  - port number of client
  - initial sequence number (ISN) of client

**(2)PASSIVE OPEN:** Server responds with a segment with

  - SYN bit set *
  - initial sequence number of server
  - ACK for ISN of client

**(3)Client acknowledges by sending a segment with:**

  - ACK ISN of server(* counts as one byte)

# Figure : *Connection establishment using three-way handshaking*

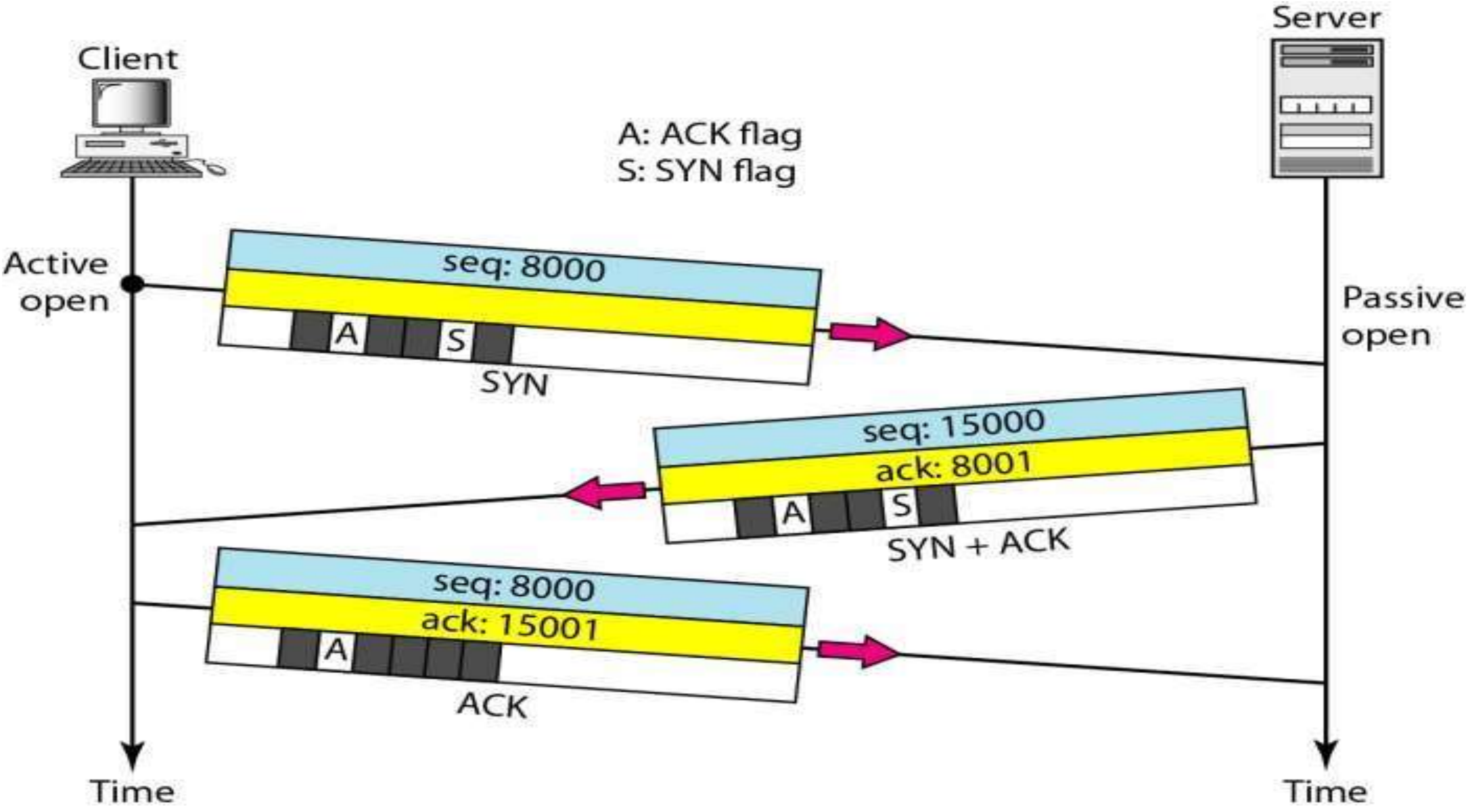
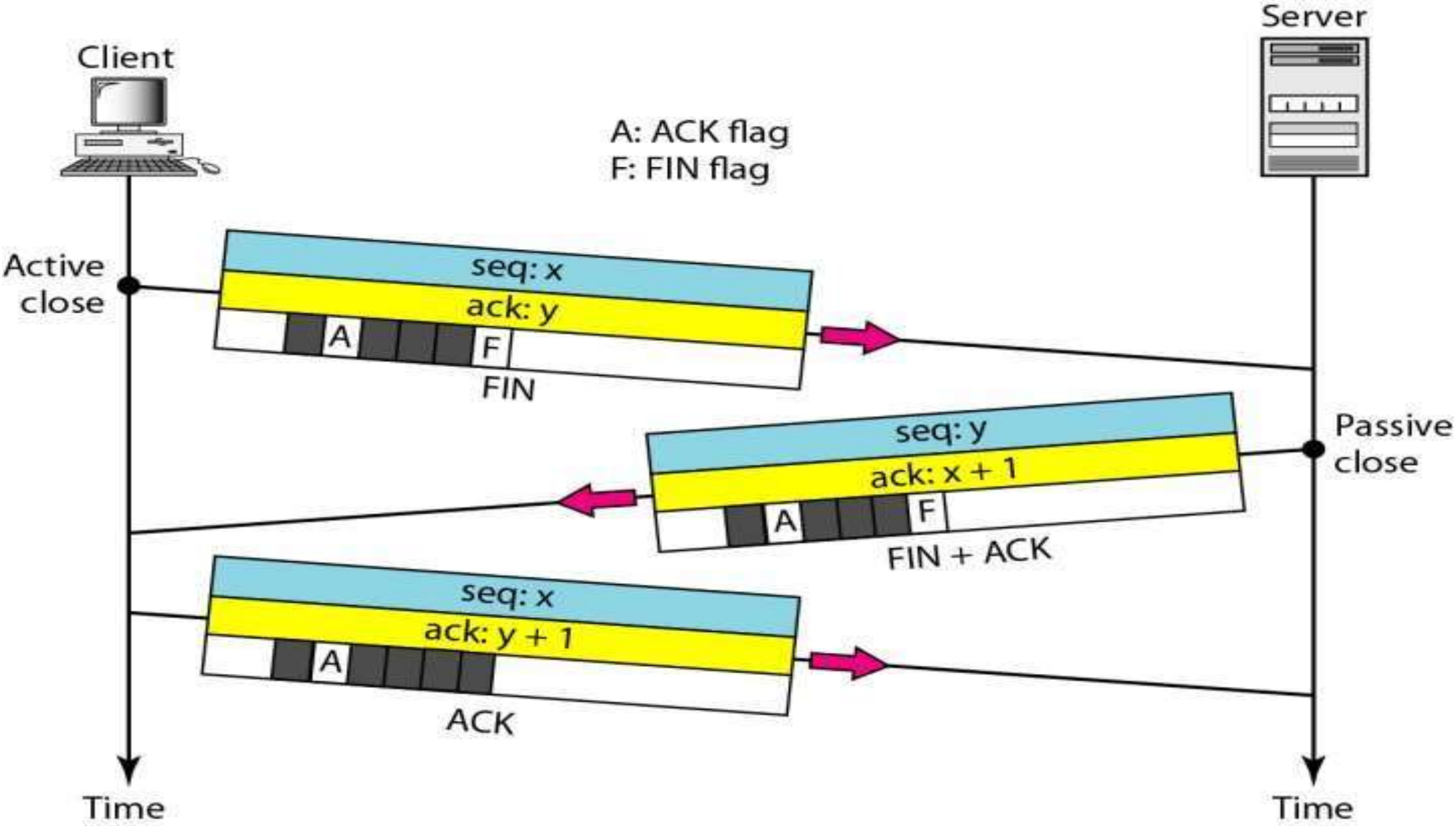


**Figure :** ***Connection termination using three-way handshaking***

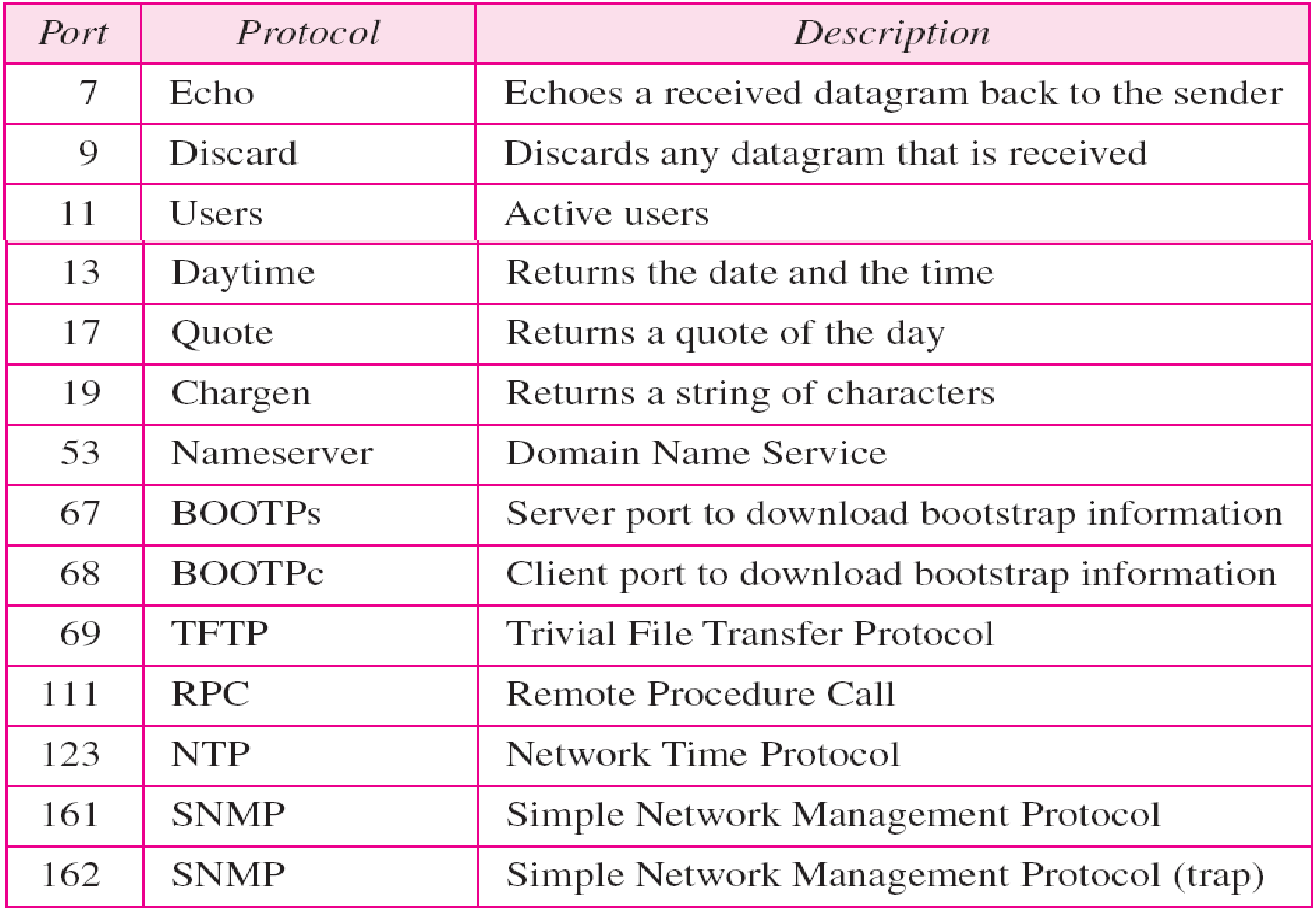


# USER DATAGRAM PROTOCOL (UDP)

***The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to- host communication.***

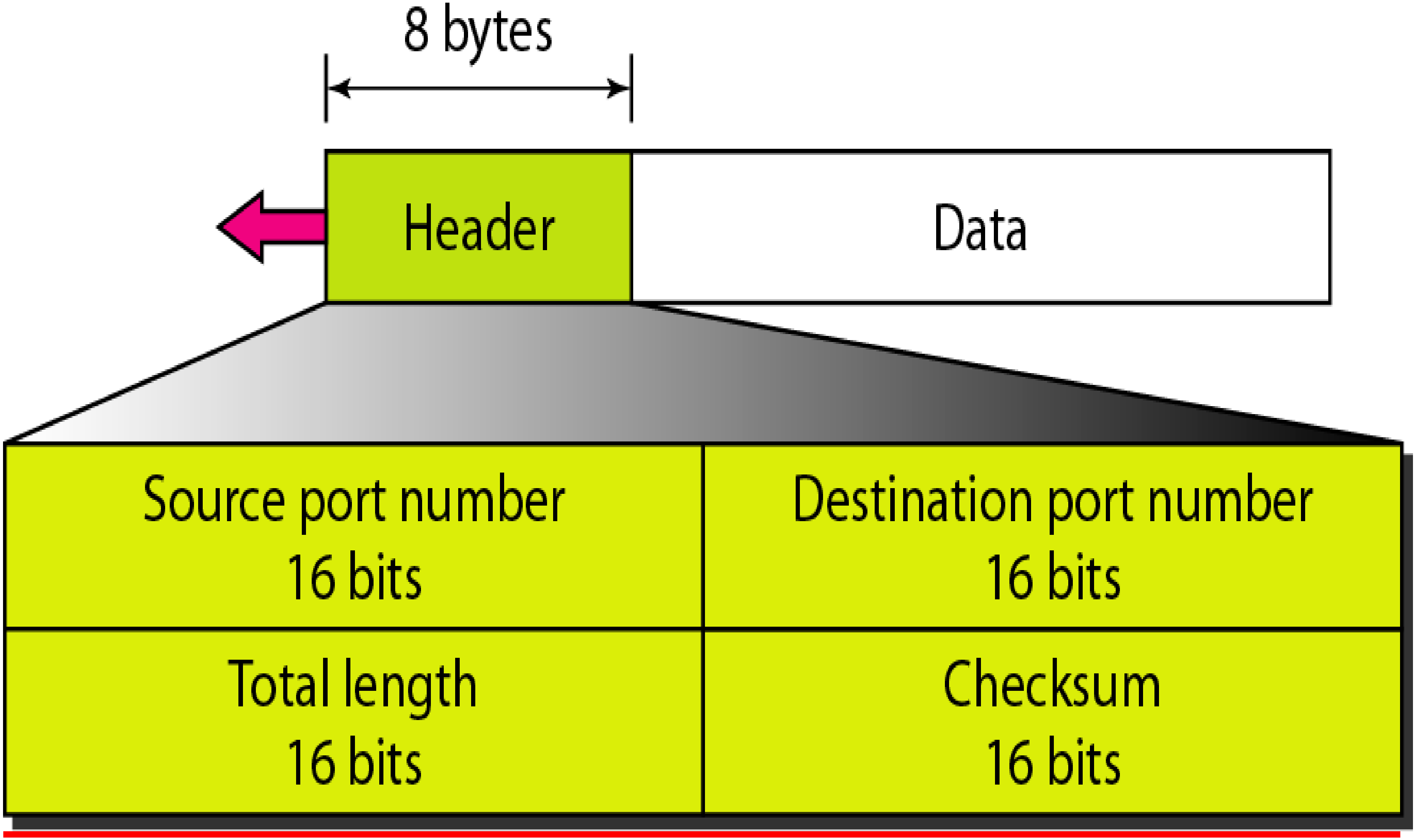
- ***provide unreliable service***

**Table : *Well-known ports used with UDP***



| *Port* | *Protocol* | *Description* |
|---|---|---|
| 7 | Echo | Echoes a received datagram back to the sender |
| 9 | Discard | Discards any datagram that is received |
| 11 | Users | Active users |
| 13 | Daytime | Returns the date and the time |
| 17 | Quote | Returns a quote of the day |
| 19 | Chargen | Returns a string of characters |
| 53 | Nameserver | Domain Name Service |
| 67 | BOOTPs | Server port to download bootstrap information |
| 68 | BOOTPc | Client port to download bootstrap information |
| 69 | TFTP | Trivial File Transfer Protocol |
| 111 | RPC | Remote Procedure Call |
| 123 | NTP | Network Time Protocol |
| 161 | SNMP | Simple Network Management Protocol |
| 162 | SNMP | Simple Network Management Protocol (trap) |

# Figure : *User Datagram Format*



8 bytes

Header

Data

| | |
|---|---|
| Source port number<br>16 bits | Destination port number<br>16 bits |
| Total length<br>16 bits | Checksum<br>16 bits |

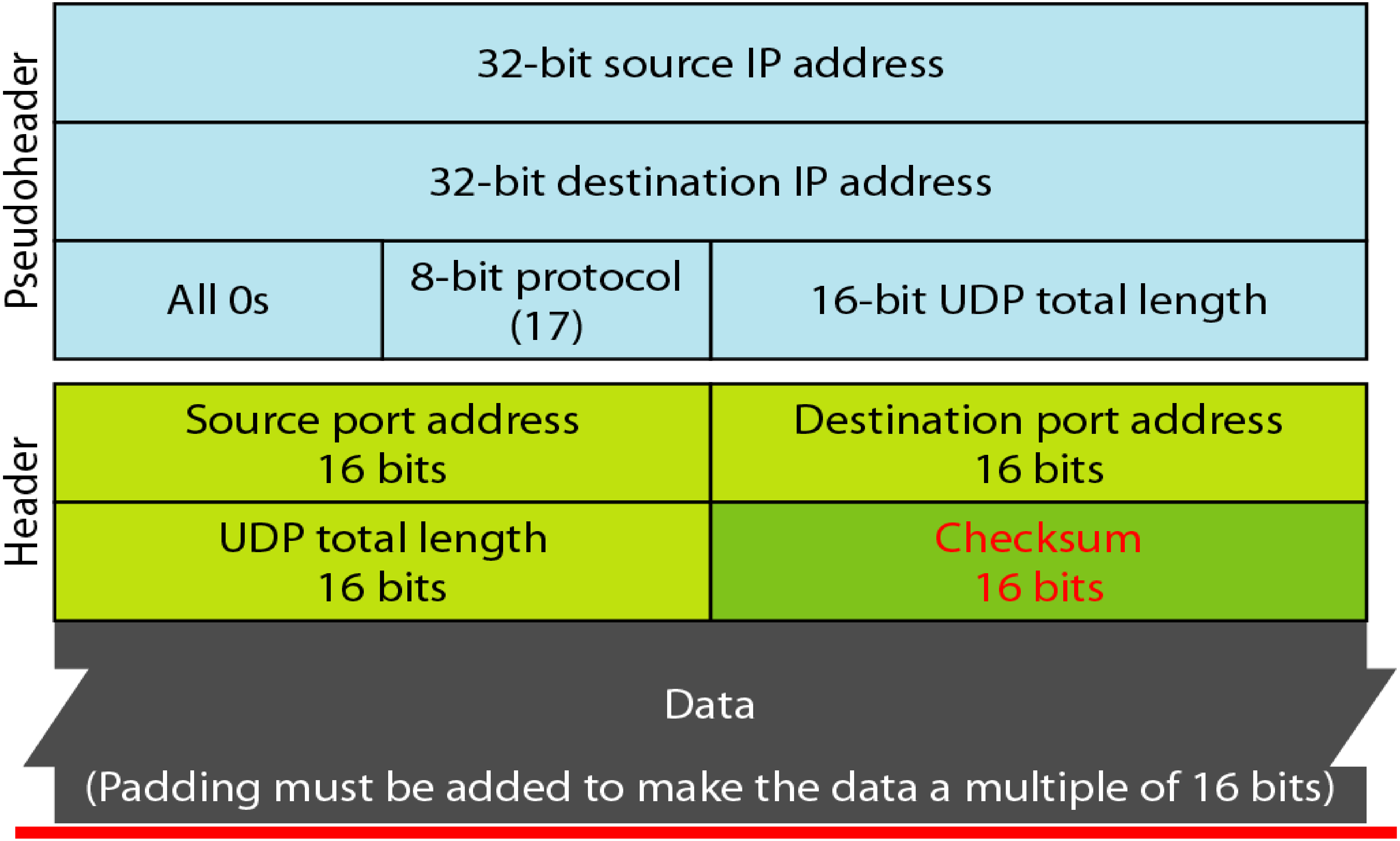
# UDP Format

- Source and destination port : 16, 16 identify applications at ends of the connection
- length: 16 - length of datagram including header and data
- checksum :16 -one’s complement of header and data including pseudo data

# UDP for Application

- TFTP
- DNS
- RPC, NFS
- SNMP

# Figure :*Pseudo header for checksum calculation*



Pseudoheader

32-bit source IP address

32-bit destination IP address

All 0s

8-bit protocol (17)

16-bit UDP total length

Header

Source port address 16 bits

Destination port address 16 bits

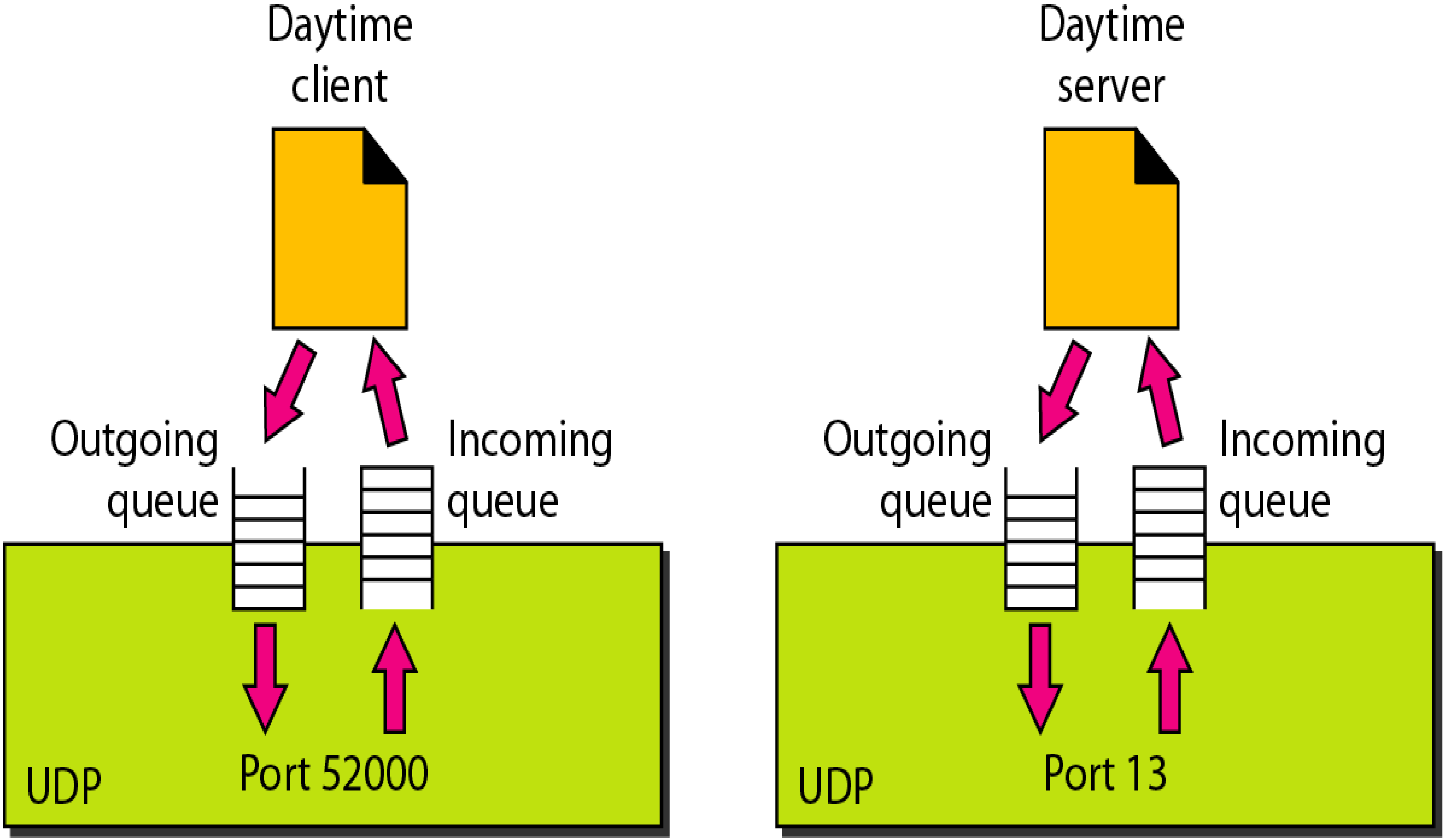
UDP total length 16 bits

Checksum 16 bits

Data

(Padding must be added to make the data a multiple of 16 bits)

# Figure : *Queues in UDP*



| TCP | UDP |
|---|---|
| Transmission Control Protocol | User Datagram Protocol |
| Connection Oriented | Connection Less |
| Slow | Fast |
| Highly Reliable | Unreliable |
| 20 Bytes | 8 Bytes |
| It takes acknowledgement of data and has the ability to retransmit if the user requests. | It neither takes acknowledgement, nor it retransmits the lost data. |
| TCP is heavy-weight. | UDP is lightweight. |

| | |
|---|---|
| Stream-based | Message-based |
| Delivery of all data is managed | Not performed |
| Flow control using sliding window protocol | None |
| TCP doesn’t supports Broadcasting. | UDP supports Broadcasting. |
| Small to moderate amounts of data | Small to enormous amounts of the data |
| Applications where reliable transmission of data matters. | Application where data delivery speed matters. |
| FTP, Telnet, SMTP, IMAP. | DNS, BOOTP, DHCP, TFTP. |

# Transport for Real Time Applications (RTP).

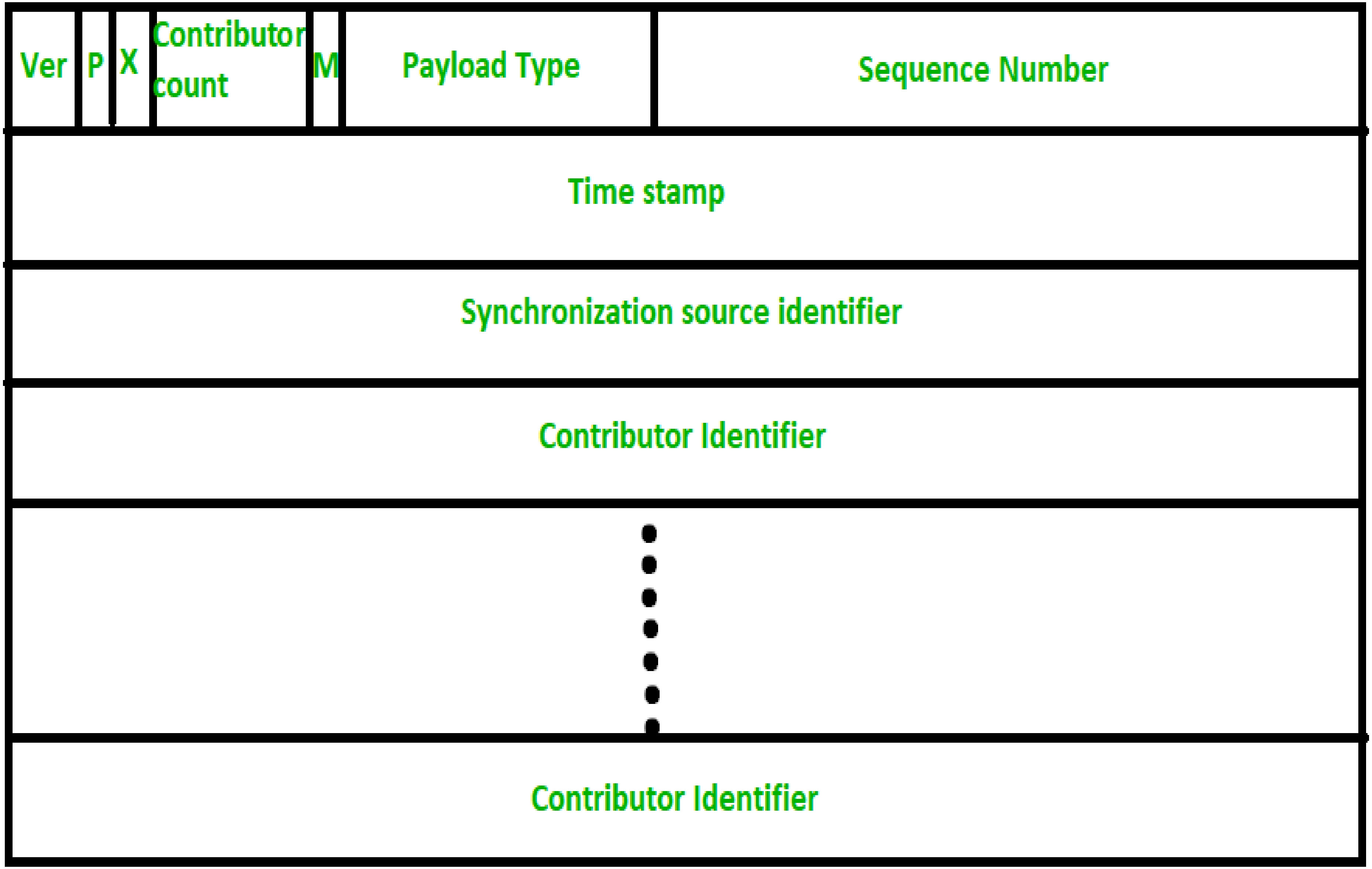
- A protocol is designed to handle **real-time traffic (like audio and video) of the Internet, is known as Real Time Transport Protocol (RTP).**
- RTP must be used with UDP.
- It does not have any delivery mechanism like multicasting or port numbers.
- RTP supports different formats of files like MPEG and MJPEG.

- It is very sensitive to packet delays and less sensitive to packet loss.
- RTP is first time published in 1996 and known as RFC 1889. And next it published in 2003 with name of RFC 3550.

# Applications of RTP

1. RTP mainly helps in media mixing, sequencing and time-stamping.
2. Voice over Internet Protocol (VoIP)
3. Video Teleconferencing over Internet.
4. Internet Audio and video streaming.

# RTP Header Format



Ver

P

X

Contributor count

M

Payload Type

Sequence Number

Time stamp

Synchronization source identifier

Contributor Identifier

Contributor Identifier

- **Version :** This 2-bit field defines version number. The current version is 2.
- **P** –The length of this field is 1-bit. If value is 1, then it denotes presence of padding at end of packet and if value is 0, then there is no padding.
- **X** –The length of this field is also 1-bit. If value of this field is set to 1, then its indicates an extra extension header between data and basic header and if value is 0 then, there is no extra extension.
- **Contributor count** –This 4-bit field indicates number of contributors. Here maximum possible number of contributor is 15 as a 4-bit field can allows number form 0 to 15.
- **M** –The length of this field is 1-bit and it is used as end marker by application to indicate end of its data.
- **Payload types** –This field is of length 7-bit to indicate type of payload. We list applications of some common types of payload.

- **Sequence Number** –The length of this field is 16 bits. It is used to give serial numbers to RTP packets.
- **Time Stamp** –The length of this field is 32-bit. It is used to find relationship between times of different RTP packets.
- **Synchronization Source Identifier** –This is a 32-bit field used to identify and define the source. The value for this source identifier is a random number that is chosen by source itself.
- **Contributor Identifier** –This is also a 32-bit field used for source identification where there is more than one source present in session.

# THANK YOU

# UNIT V APPLICATIONS

Applications - DNS – E-Mail Protocols – WWW – SNMP – SMTP - Security – Threats and Services- Cryptography -DES-RSA- Web security -SSL .

# UNIT – V

# APPLICATIONS

# OVERVIEW

- **Applications**
- **DNS**
- **E-Mail Protocol**
- **WWW**
- **SNMP**
- **SMTP**
- **Security**
- **Threats and Services**
- **Cryptography**
- **DES**
- **RSA**
- **Web security**
- **SSL**

# Applications

- An application layer is an **abstraction** layer that specifies the shared communications protocols and interface methods used by hosts in a **communications network.**
- The application layer abstraction is used in both of the **standard models of computer networking**.
- The Internet Protocol Suite **(TCP/IP) and the OSI** model.
- Although both models use the same term for their respective **highest-level layer.**

# Services of Application Layers

- File Transfer
- Addressing
- Mail Services
- Directory Services
- Authentication

# DNS

- **(Domain Name System)** The Internet's system for converting **alphabetic names into numeric IP addresses.**
- For example, when a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name.
- In this example, the DNS converts the URL **www.company.com** into the IP address **204.0.8.51.**

# A Hierarchy of Servers

- The DNS system is a hierarchy of duplicated database servers worldwide that begin with the **"root servers"** for the **top-level domains (.com, .net, .org, .gov, .edu, .mil, etc.)**. The root servers point to the "**authoritative**" servers located in ISPs,
- **Example :**

**www.yahoo.com**

**www --------> Host Name**

**Yahoo--------> Server Name**

**com ----------> Domain Name**

# Structure of DNS

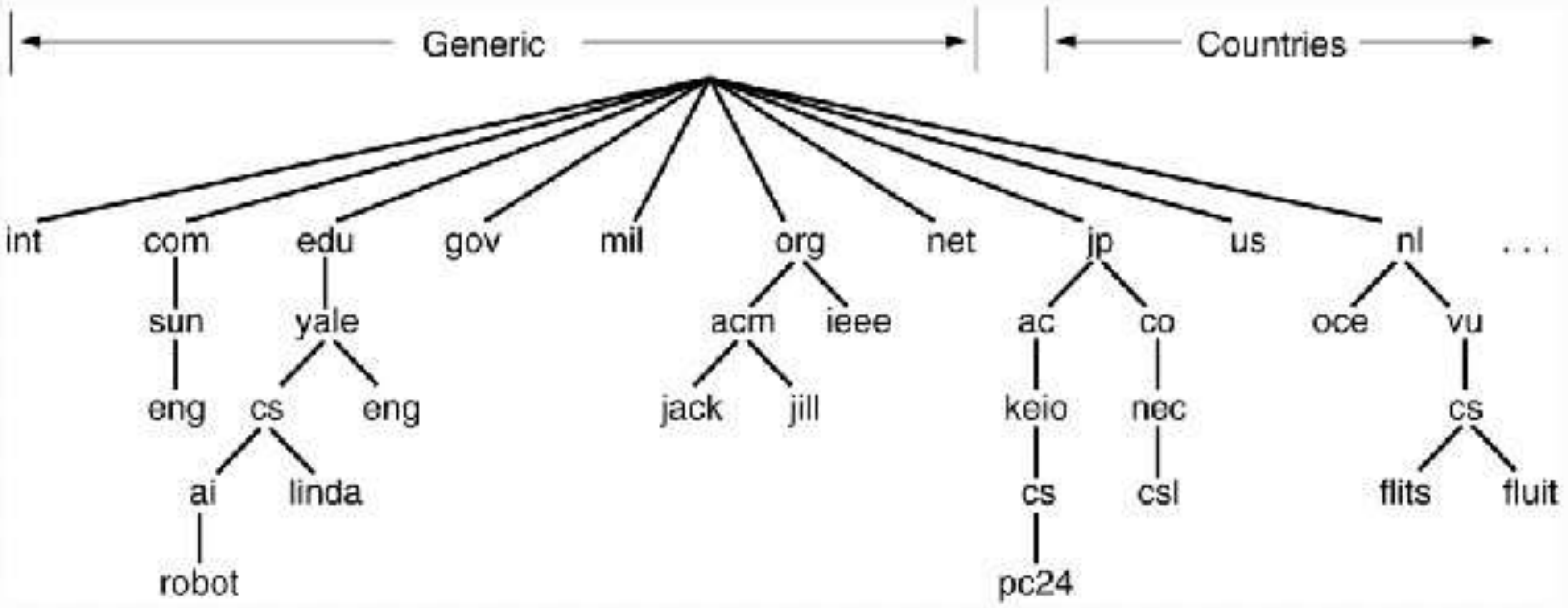
- **It Consists of Four Elements**

1. DNS Name Space
2. DNS Database
3. Name Servers
4. DNS Resolvers

# 1. DNS Name Space

- The Domain Name Space consists of a tree data structure.
- **Each node or leaf in the tree has a label and zero or more resource records (RR)**, which hold information associated with the domain name.
- The domain name itself consists of the label, parent node on the right.
- The tree sub-divides into zones beginning at the **root zone.** A DNS zone may consist of only one domain, or may consist of many domains and sub-domains, depending on the administrative choices of the **zone manager.**

# The DNS Name Space



A portion of the Internet domain name space.

# 2. DNS Database

- DNS does not only deal with IP addresses of hosts, but also exchanges information on Name Servers.
- The Key features of the Database are as Follows :

    1) Variable-Depth Hierarchy for Names.

    2) Distributed Database.

    3) Distribution Controlled by Database.

# 3. Name Servers

- The Domain Name System is maintained by a distributed database system, which uses the client–server model.
- The nodes of this database are the name servers.
- Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it.
- The top of the hierarchy is served by the root name servers.

# 4. DNS Resolvers

- The client side of the DNS is called a **DNS resolver.**
- A resolver is responsible for initiating and sequencing the queries that ultimately lead to a full resolution.
- DNS resolvers are classified by a variety of query methods, such as **recursive, non-recursive, and iterative.**

# DNS message format

- The DNS protocol uses **two types of DNS messages**, **queries and replies**; both have the same format.
- Each message consists of a **header and four sections: question, answer, authority, and an additional space**.
- A header field (flags) controls the content of these four sections.
- The header section consists of the **following fields: Identification, Flags, Number of questions, Number of answers, Number of authority resource records (RRs), and Number of additional RRs. Each field is 16 bits long.**

# Applications of DNS

- Primary website.
- Marketing campaign websites.
- Email servers.
- Customer support websites.
- Online resource libraries.
- Inside sales web portals.
- Multi-tier web applications.
- P2P resources.

# E-Mail

- Electronic Mail or E-Mail is a method of sending and receiving messages (Mail) electronically over a Computer Network.
- E-Mail is a system allows a person or a group to electronically communicate to others through Internet.
- It is method of **exchanging message** between people using electronic devices.
- Exchanging message as **Text files** and **non-text files** (images, graphics Image, files so on.,)

# Components of Email System

- **Mail Server**

  Receive, Store and Deliver the mail

- **DNS**

  Find and match the IP Address of the Mail Server

- **Mailbox**

  It is a Folder contains Emails and their information.

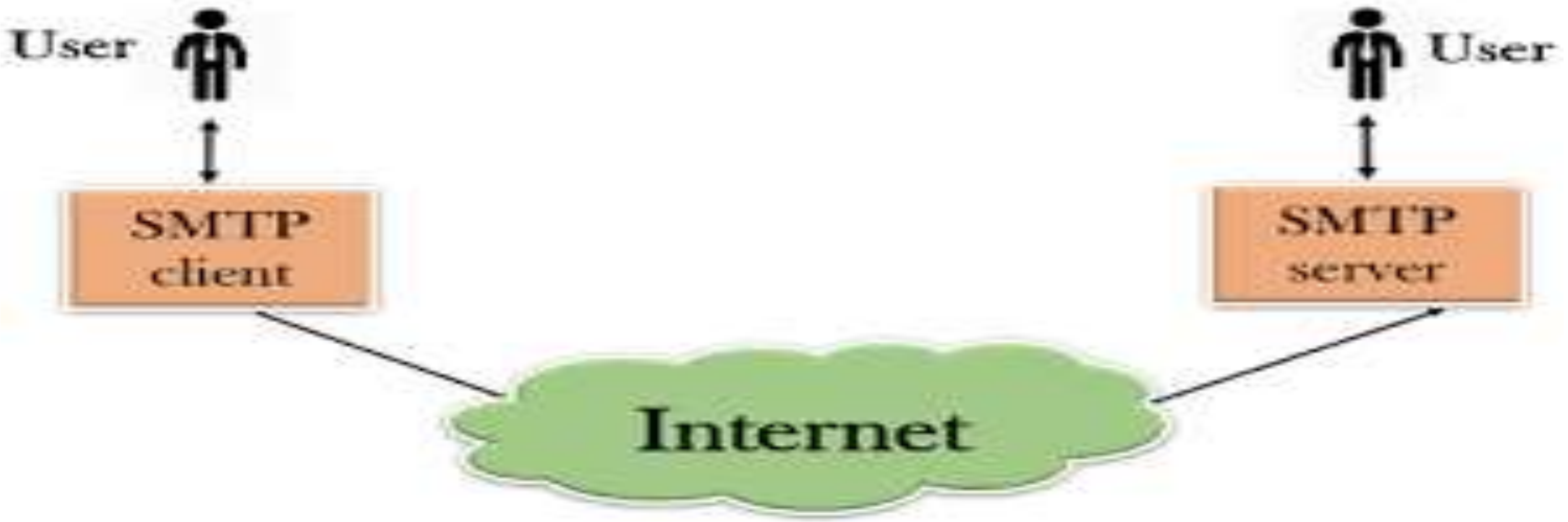
# E-Mail Protocol

The E-Mail communication is done via **three protocols** in general. They are,

1. **SMTP ( Simple Mail Transfer Protocol)**
2. **POP ( Post Office Protocol)**
3. **IMAP ( Internet Mail Access Protocol)**

# ❖ SMTP (Simple Mail Transfer Protocol)

- The SMTP stands for **Simple Mail Transfer Protocol.**
- Email is sent using this protocol.
- Is an internet standard communication protocol for **electronic mail transmission.**
- Mail servers and other message transfer agents use SMTP to send and receive mail messages.



## ✓ ADVANTAGES:

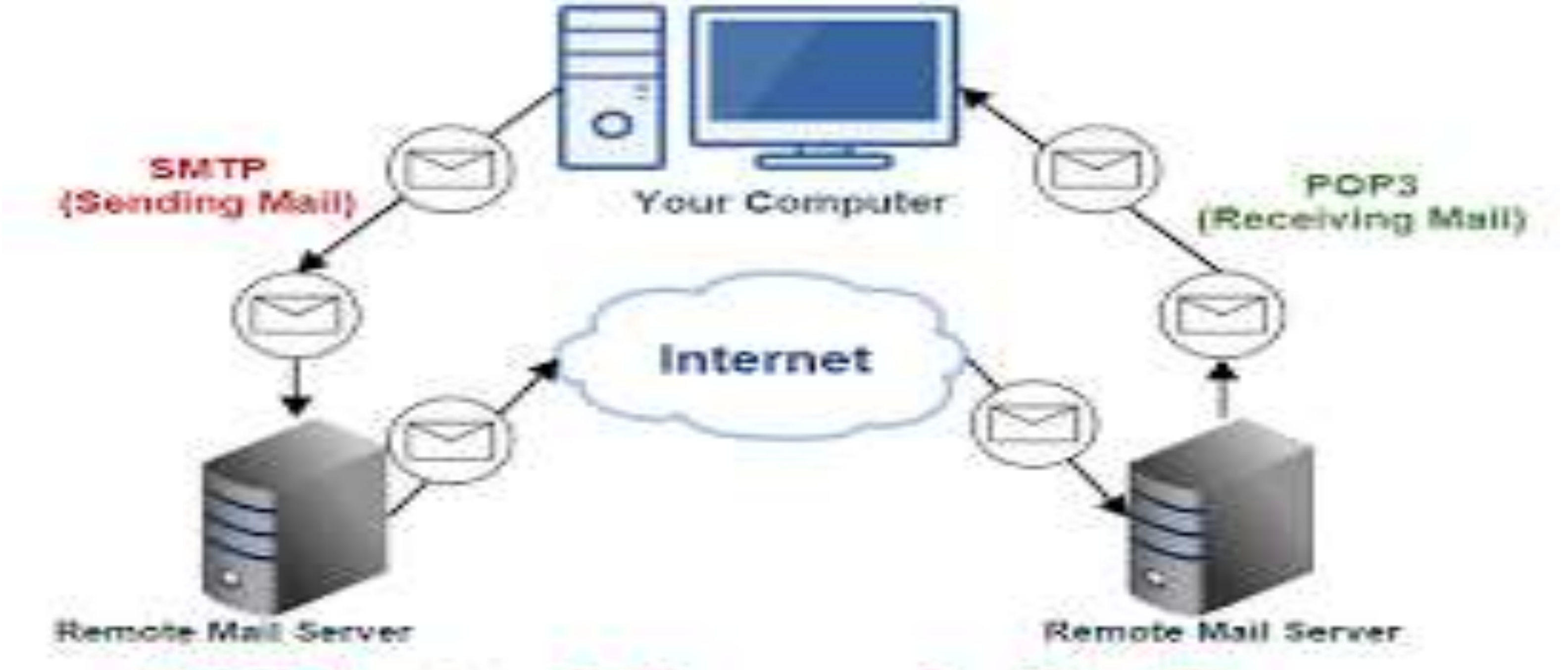
- ➢ SMTP provides the simplest form of communicating through email message between various computers in a particular network.
- ➢ Since SMTP is developed from a simple platform , email messages may be sent easily and quickly.
- ➢ SMTP also offers reliability in terms of outgoing email messages.

## ✓ DISADVANTAGES:

- ➢ The main drawback of sending through an SMTP server is that it is insecure, it can be easily hacked.
- ➢ Another disadvantage is the server limitation.

## ❖ POP (Post Office Protocol):

- This protocol is also used for **incoming emails.**
  - The main difference with the both protocols is that POP downloads the entire email into the local computer and deletes the data on the server once it is downloaded.
  - This is helpful in a server with **less free memory.**
  - Current version of POP is **POP3** .



**POP Protocol Communication Process**

✓ ADVANTAGES:

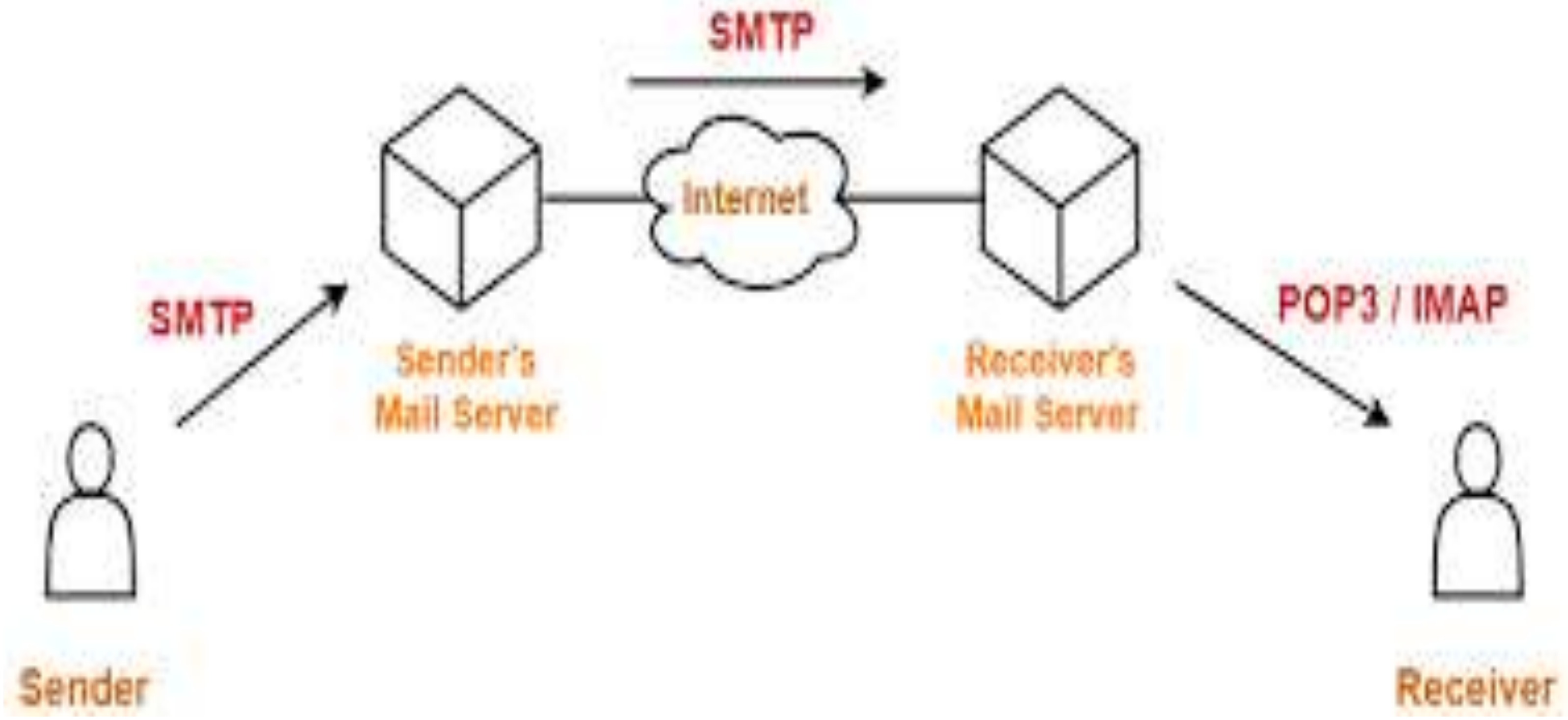
- Emails are downloaded to the user`s computer.
- opening attachments is quick and easy as they are already downloaded.
- Less server storage space required all emails are stored on local machine.
- Storage capacity of emails limited by the size of your hard disk.
- very popular, easy to configure and use.

✓DISADVANTAGES:

- Emails cannot be accessed from other machines(unless configured to do so).
- Exporting the local mail folder to another email client or physical machine can be difficult.
- Email folders can become corrupted, potentially losing the entire mailbox at once.

# ❖ IMAP(Internet Mail Access Protocol)

- This protocol is used while **receiving an email**.
- When one uses **IMAP,** the emails will be present in the server and not get downloaded to the user`s mail box and deleted from the server.
- This helps to have less memory used in the local computer and server memory is increased.



- ✓ **ADVANTAGES:**
  - ➢ Mail stored on remote server, i.e. accessible from multiple different location.
  - ➢ Internet connection needed to access mail.
  - ➢ Mail is automatically backed up if server is managed properly.

- ✓ **DISADVANTAGES:**
  - ➢ The main disadvantage of the IMAP protocols is that it is mandatory to have an internet connection on all the time to read/reply and search the message.

# WWW

- The World Wide Web is the universe of network-accessible information.
- In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet.
- The **World Wide Web is based on several different Technologies** : **Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).**

# Features of WWW

- HyperText Information System
- Cross-Platform
- Distributed
- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- “Web 2.0”

# Components of WWW

- **There are 5 Components of WWW:**

**1. Uniform Resource Locator (URL):** serves as system for resources on web.

**2. HyperText Transfer Protocol (HTTP):** specifies communication of browser and server.

**3. Hyper Text Markup Language (HTML):** It Defines structure, organisation and content of webpage.

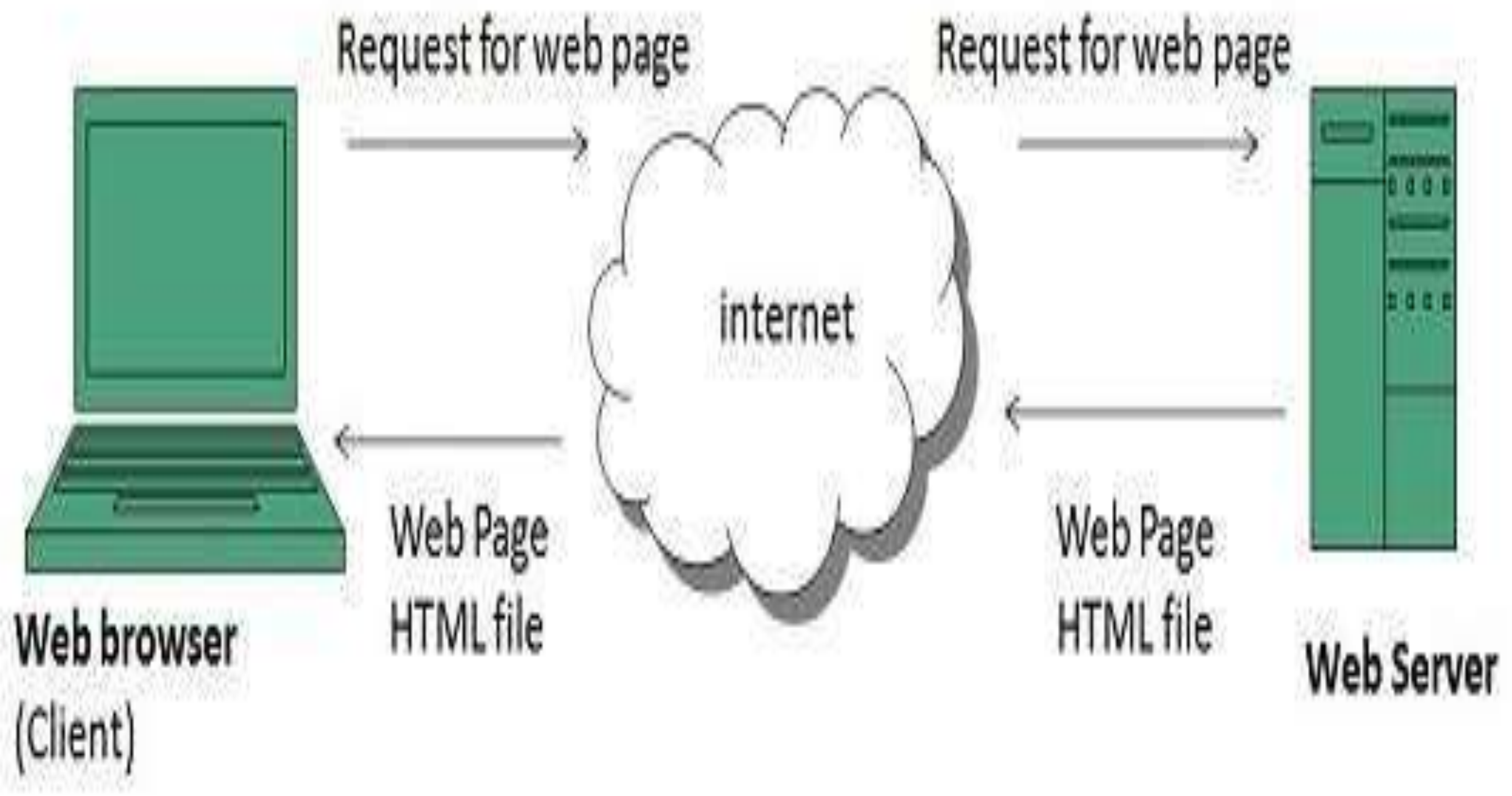
**4. Web Server :** A web server is computer software and underlying hardware that accepts requests via HTTP, the network protocol created to distribute web pages.

# Components of WWW

**5. Web Browser :** A web browser (commonly referred to as a browser or internet browser).

- It is an application software for accessing the World Wide Web.
- When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user's device.

# WWW Architecture



# Working of WWW

- **The World Wide Web** is based on several different technologies :

**1. Web browser.**

**2. Hypertext Markup Language (HTML).**

**3. Hypertext Transfer Protocol (HTTP).**

**1. Web browser :** It is used to access webpages. Web browsers can be defined as programs which display **text, data, pictures, animation and video on the Internet.**

**2. HTML :** Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers.

**3. HTTP :** It can be used for several tasks including : searches, mailing, transferring files, and much more. Some of the commonly used browsers are **Internet Explorer, Opera Mini, Google Chrome.**

# Applications of www

- Online Forms
- Shopping Carts
- Word Processors
- Spreadsheets
- Video and Photo Editing
- File Conversion
- File Scanning
- E-mail programs such as Gmail, Yahoo and AOL.
- Popular Applications include Google Apps and Microsoft 365.

# SNMP

- ***Simple Network Management Protocol (SNMP)*** *is an application–layer protocol defined by the* ***Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices.***
- *It is a part of* ***Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.***
- ***SNMP is one of the widely accepted network protocols to manage and monitor network elements.***

# Components of SNMP

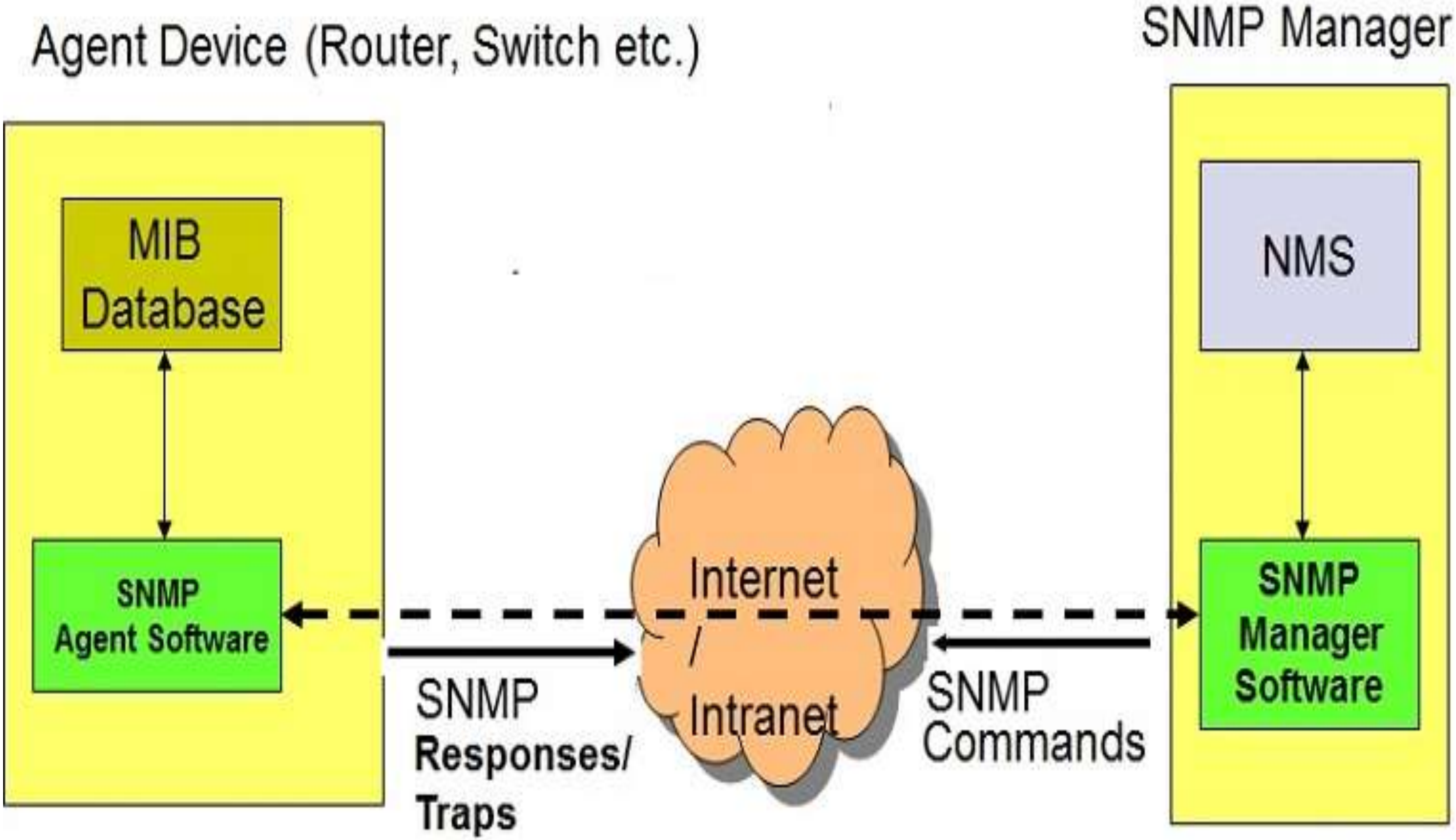
**SNMP consists of**

- **SNMP Manager**
- **Managed devices**
- **SNMP agent**
- **Management Information Base (MIB)**

# Basic Commands of SNMP

- **GET:** The GET operation is a request sent by the manager to the managed device.
- **GET NEXT:** The significant difference is that the GET NEXT operation retrieves the value of the next MIB tree.
- **GET BULK:** The GETBULK operation is used to retrieve voluminous data from large MIB table.
- **SET:** This operation is used by the managers to modify or assign the value of the Managed device.
- **TRAPS:** TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
- **INFORM:** It includes confirmation from the SNMP manager on receiving the message.
- **RESPONSE:** It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.

# SNMP Architecture



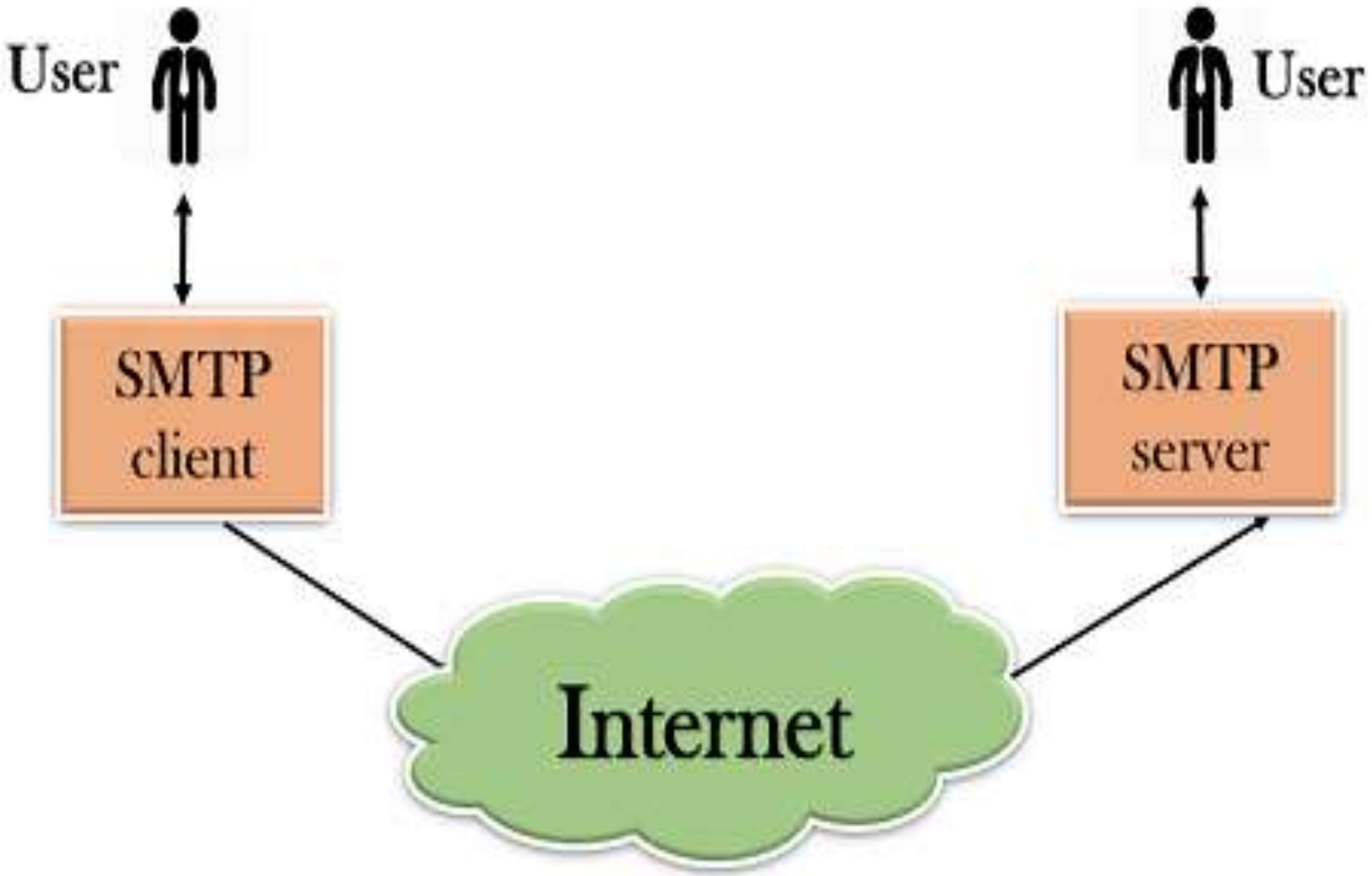
# SMTP

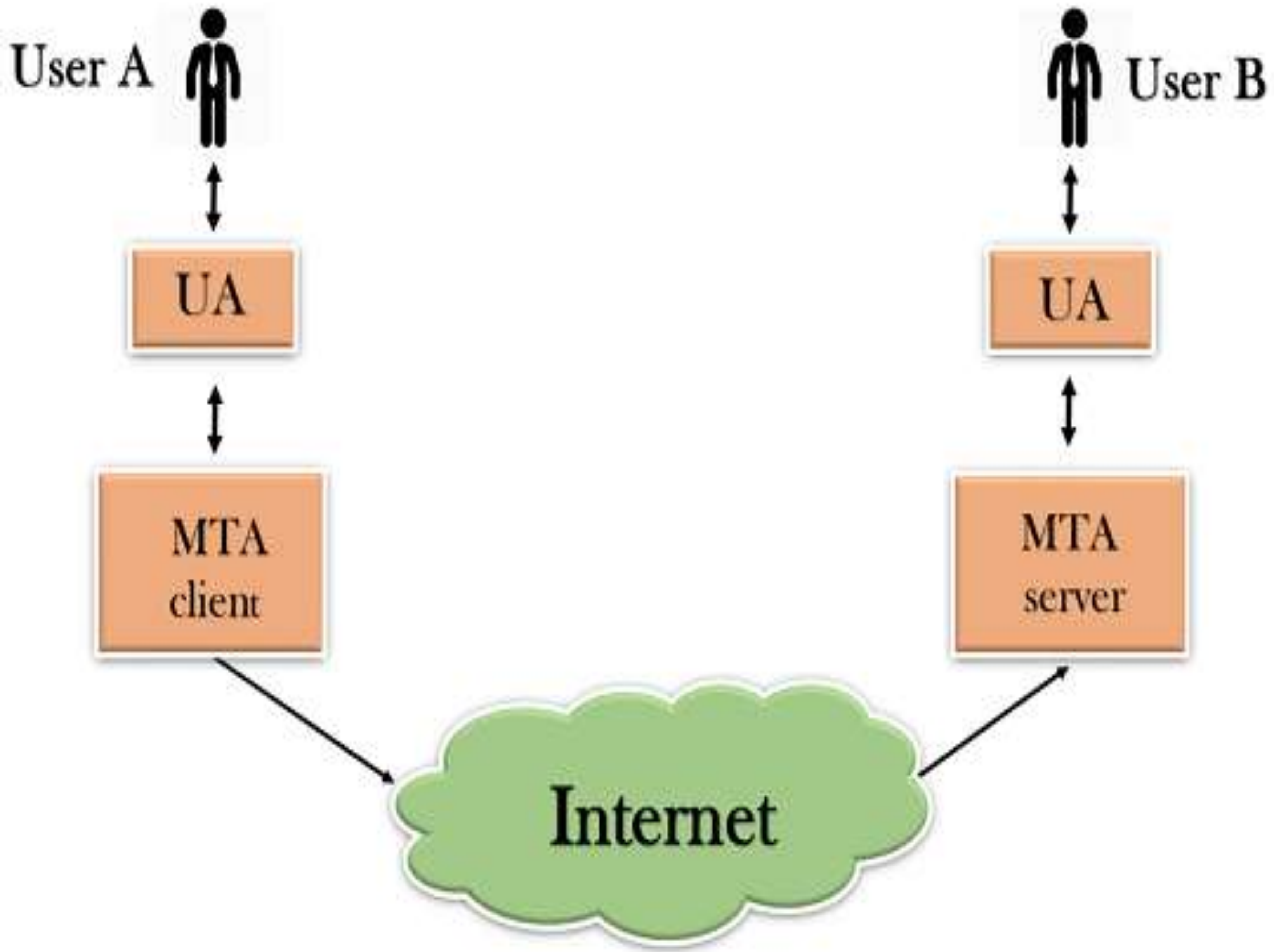
- **SMTP stands for Simple Mail Transfer Protocol.**
- SMTP is a set of communication guidelines that allow software to transmit an **electronic mail over the internet is called Simple Mail Transfer Protocol.**
- It is a program used for sending messages to other computer users based on **e-mail addresses.**

- It provides a mail exchange between users on the same or different computers, and **it also supports:**

1. **It can send a single message to one or more recipients.**
2. **Sending message can include text, voice, video or graphics.**
3. **It can also send the messages on networks outside the internet.**
4. **The main purpose of SMTP is used to set up communication rules between servers.**

# Components of SMTP




User A
User B
UA
UA
MTA client
MTA server
Internet

# Working of SMTP

- **It have the following Working Functionalities :**

1. Composition of Mail
2. Submission of Mail
3. Delivery of Mail
4. Receipt and Processing of Mail
5. Access and Retrieval of Mail

## ✓ ADVANTAGES:

- ➢ SMTP provides the simplest form of communicating through email message between various computers in a particular network.
- ➢ Since SMTP is developed from a simple platform , email messages may be sent easily and quickly.
- ➢ SMTP also offers reliability in terms of outgoing email messages.

## ✓ DISADVANTAGES:

- ➢ The main drawback of sending through an SMTP server is that it is insecure, it can be easily hacked.
- ➢ Another disadvantage is the server limitation.

# Security

- Network Security deals with all aspects related to the protection of the sensitive information assets existing on the network.
- It covers various mechanisms developed to provide fundamental security services for data communication.
- It describes the functioning of most common security protocols employed at different networking layers right from application to data link layer.

# Goals of Network Security

- The primary goal of network security are **Confidentiality, Integrity, and Availability.** These three pillars of Network Security are often **represented as CIA triangle.**

**1. Confidentiality –** The function of confidentiality is to protect precious business data from unauthorized persons.

**2. Integrity –** It means maintaining and assuring the accuracy and consistency of data.

The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

**3. Availability –** The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the users, whenever they require it.

# Security Services

**fundamental security services as the following –**

**1. Confidentiality –** E-mail message should not be read by anyone but the intended recipient.

**2. Authentication –** E-mail recipient can be sure of the identity of the sender.

**3. Integrity –** Assurance to the recipient that the e-mail message has not been altered since it was transmitted by the sender.

**4. Non-repudiation –** E-mail recipient is able to prove to a third party that the sender really did send the message.

**5. Proof of submission –** E-mail sender gets the confirmation that the message is handed to the mail delivery system.

**6. Proof of delivery –** Sender gets a confirmation that the recipient received the message.

# Threats and Services

A Computer System **Threat** is anything that leads to **loss or corruption of data or physical damage** to the hardware or infrastructure.

- **Security Threats** can be many like **Software attacks, theft of intellectual property, identity theft, theft of equipment or information.**
- Threat is any activity that can lead to data loss/corruption through to delay of normal business operations.

# Types of Threats

- **There are physical and non-physical threats.**
- **Physical Threats** : cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.
- **Non-physical Threats :** Target the software and data on the computer systems.

# Physical Threats

- A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.
- **The following list classifies the physical threats into three main categories**
- **Internal:** The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- **External:** These threats include Lightning, floods, earthquakes, etc.
- **Human:** These threats include theft, vandalism of the infrastructure and hardware, accidental or intentional errors.

# Non-Physical Threats

**The following list is the common types of non-physical threats;**

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

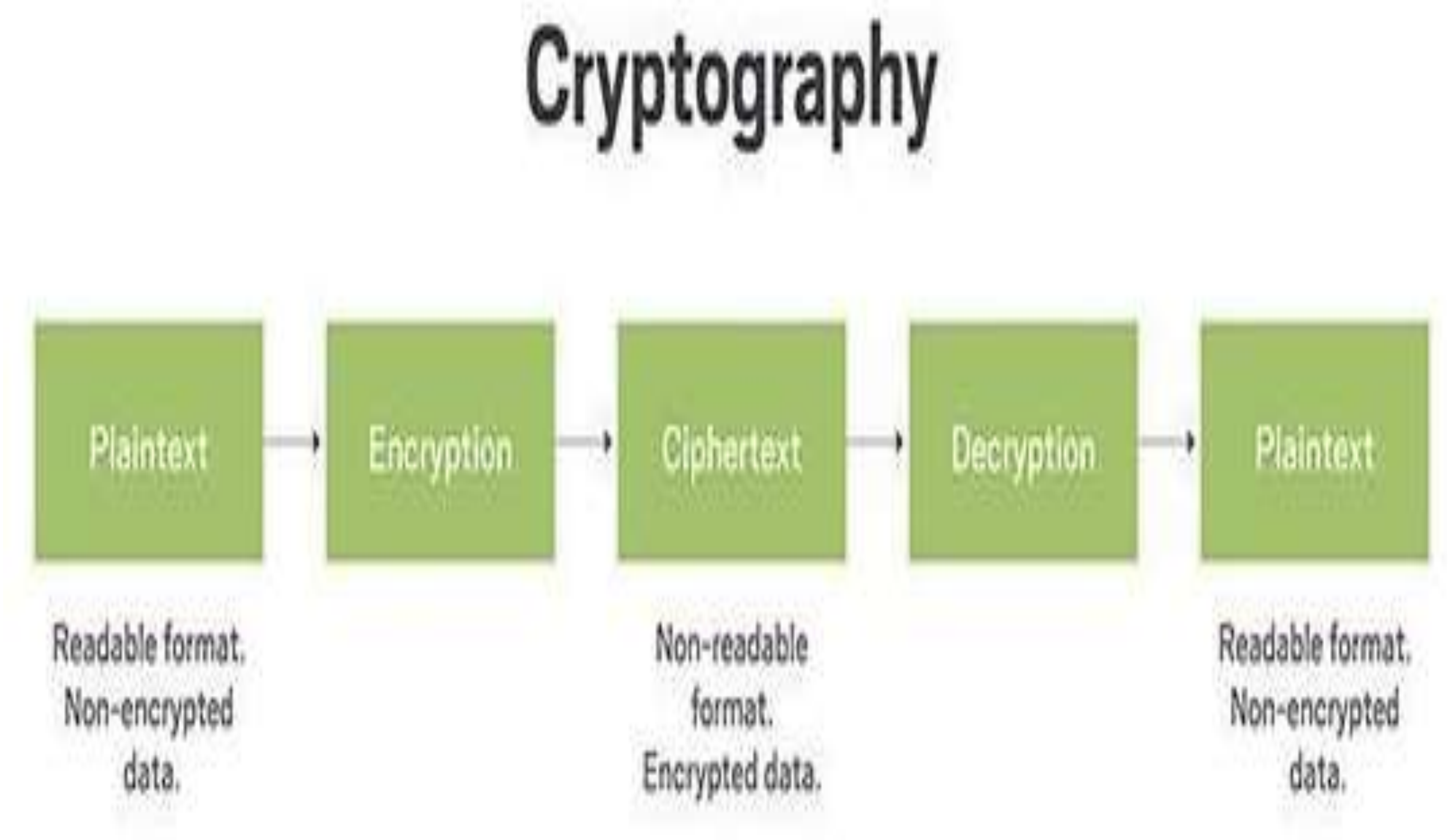
# Cryptography

- Cryptography is a method of protecting information and communications through the use of codes.
- The information is intended can read and process it.
- The **prefix "crypt-" means "hidden" or "vault"** -- and the **suffix "-graphy" stands for "writing."**
- Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms.

# Cryptography Techniques

- Cryptography is closely related to the disciplines of **cryptology and cryptanalysis.**
- It includes techniques such as **microdots, merging words with images,** and other ways to hide information in storage or transit.
- Cryptography is used to convert **Plaintext into Ciphertext is known as Encryption.** then back again **Ciphertext into Plaintext is known as Decryption.**
- **Encryption : Known to Unknown**
- **Decryption : Unknown to Known**

# Cryptography Techniques


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

# Objectives of Cryptography

- **Cryptography concerns with the following Four objectives:**
- **Confidentiality:** the information cannot be understood by anyone for whom it was unintended.
- **Integrity:** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

- **Non-repudiation:** the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
- **Authentication:** the sender and receiver can confirm each other's identity and the origin/destination of the information.

# Types of Cryptography

1. **Single-key or Symmetric-key Cryptography.**
2. **Public-key or Asymmetric-key Cryptography.**

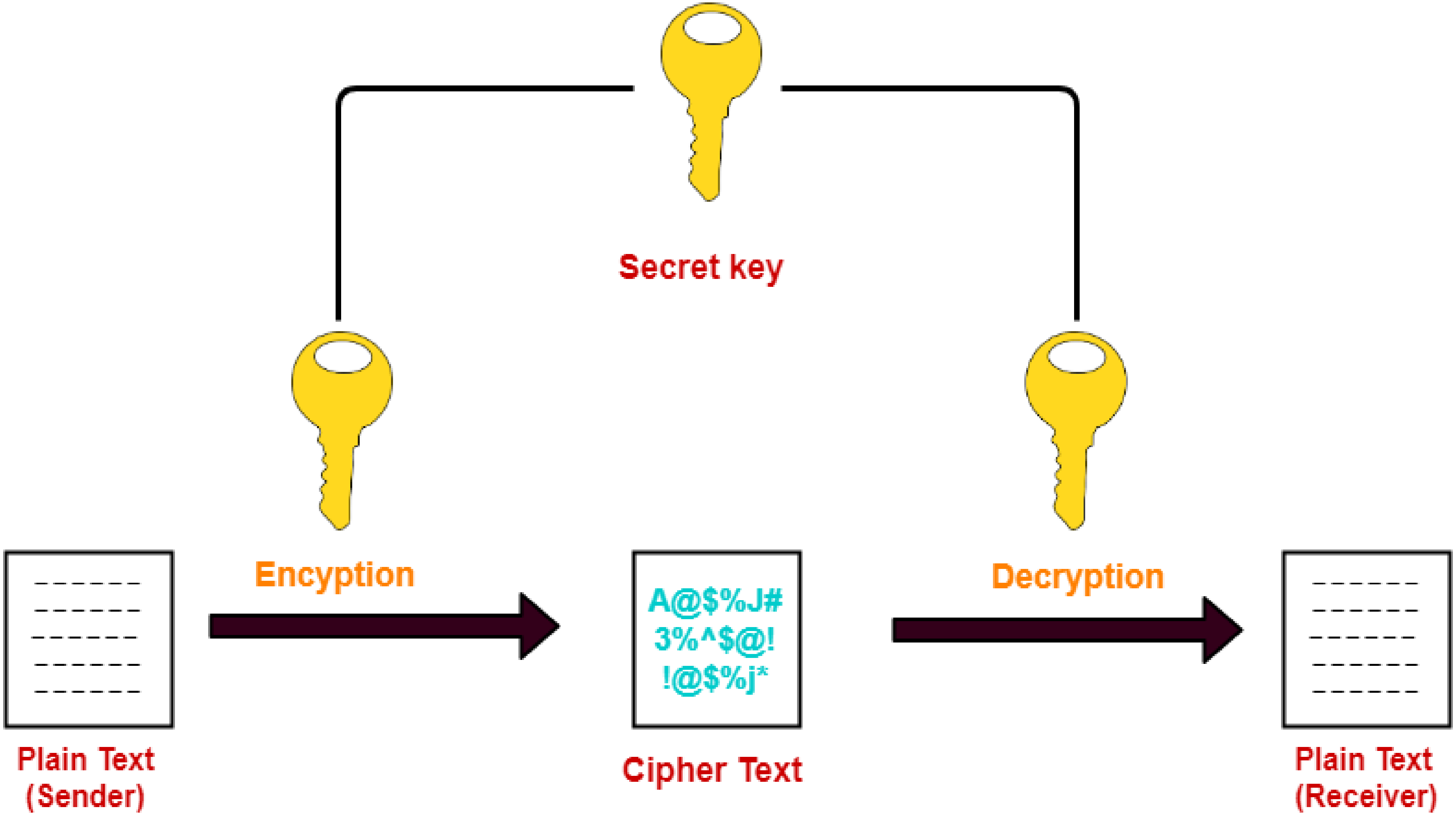
## 1. Single-key or Symmetric-key Cryptography :

Symmetric cryptography is based on the use of just **one key** is used to both Encrypt and Decrypt the messages ( **only Private Key or Secret Key** )

## 2. Public-key or Asymmetric-key Cryptography :

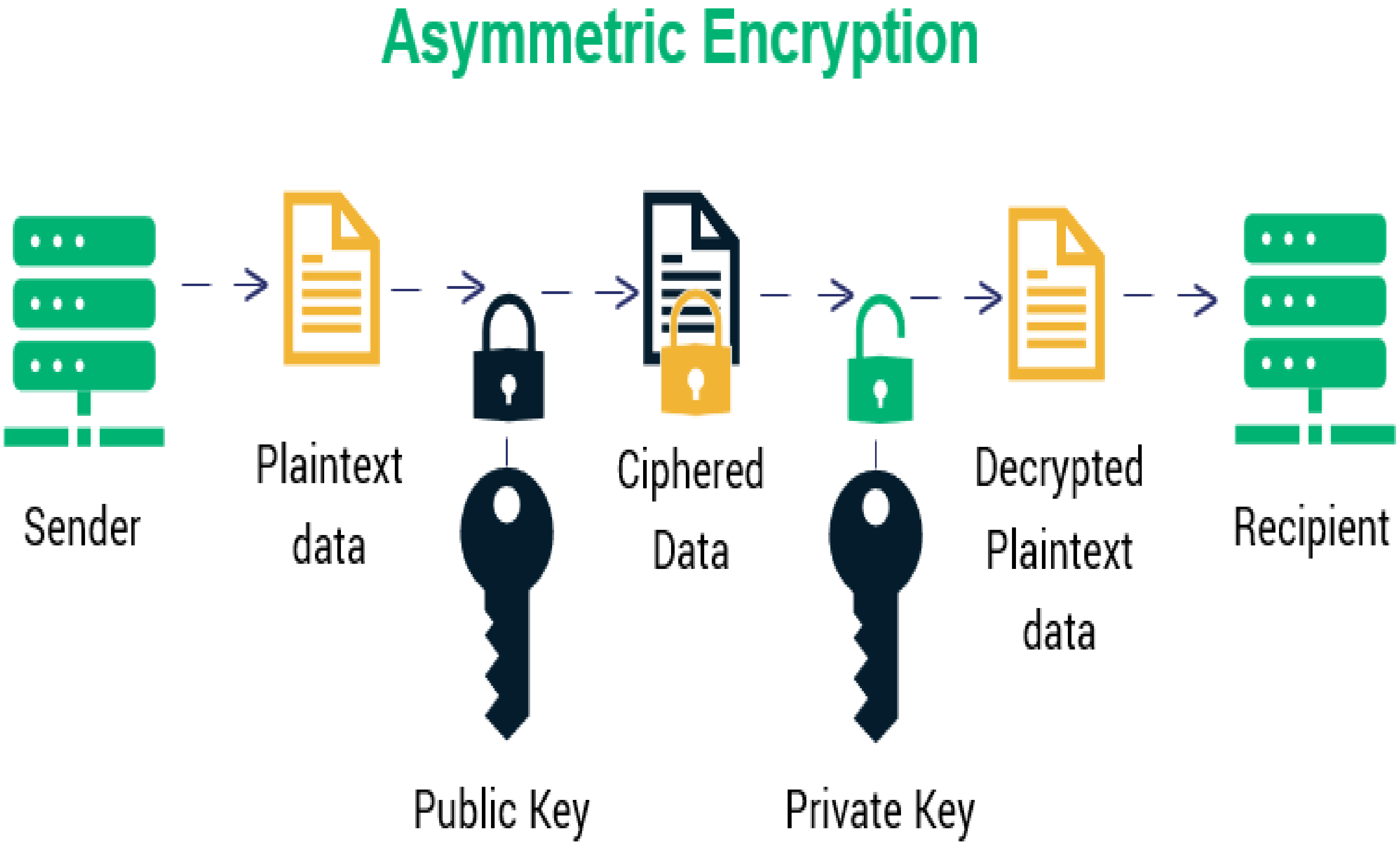
Asymmetric cryptography, also known as public-key cryptography, Here Two keys are used to Encrypt and Decrypt the messages (**Both Private and Public Key**)

# Single-key or Symmetric-key Cryptography



Symmetric Key Cryptography

# Public-key or Asymmetric-key Cryptography



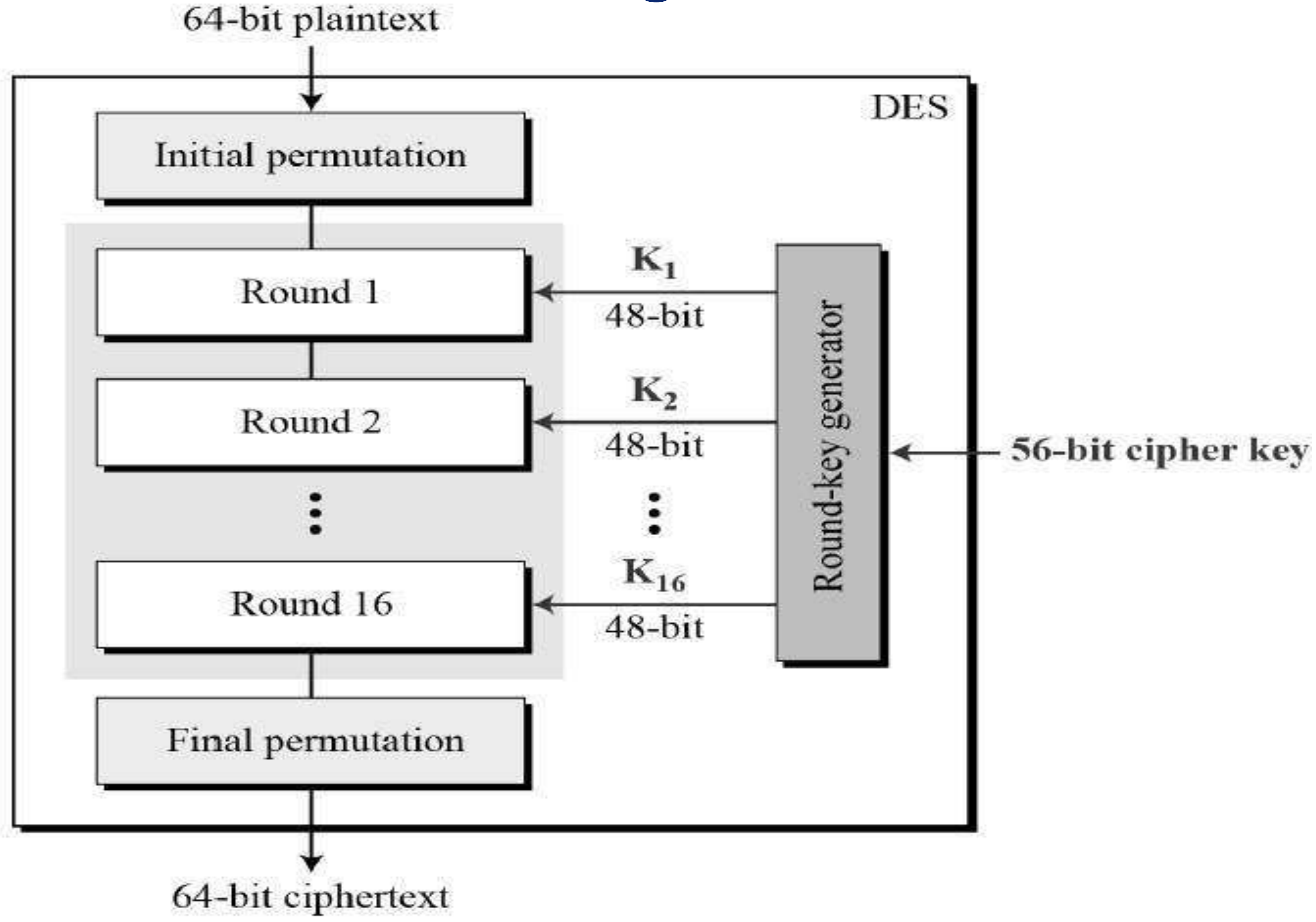
| Symmetric Encryption | Asymmetric Encryption |
|---|---|
| • Symmetric encryption consists of one key for encryption and decryption. | • Asymmetric Encryption consists of two cryptographic keys known as **Public Key** and **Private Key**. |
| • Symmetric Encryption is a lot quicker compared to the Asymmetric method. | • As Asymmetric Encryption incorporates two separate keys, the process is slowed down considerably. |
| • RC4<br>• AES<br>• DES<br>• 3DES<br>• QUAD | • RSA<br>• Diffie-Hellman<br>• ECC<br>• El Gamal<br>• DSA |

# DES

- The **Data Encryption Standard** is a **symmetric-key algorithm for the encryption of digital data.**
- The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST).
- DES is an implementation of a **Feistel Cipher.** It uses **16 round Feistel structure. The block size is 64-bit.**
- **Key length is 64-bit.**
- Since DES is based on the Feistel Cipher.

1. **Round function.**
2. **Key schedule.**
3. **Any additional processing – Initial and final permutation.**

# DES Algorithm



# DES Algorithm Steps

- The algorithm process breaks down into the following steps:

1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.

2. The initial permutation (IP) is then performed on the plain text.

3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).

4. Each LPT and RPT goes through 16 rounds of the encryption process.

5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.

6. The result of this process produces the desired 64-bit ciphertext.

# DES Analysis

- The DES satisfies both the desired properties of block cipher. T**hese two properties make cipher very strong.**

- **Avalanche effect** – A **small change in plaintext results in the very great change in the ciphertext.**

- **Completeness** – **Each bit of ciphertext depends on many bits of plaintext.**

# DES Implementation

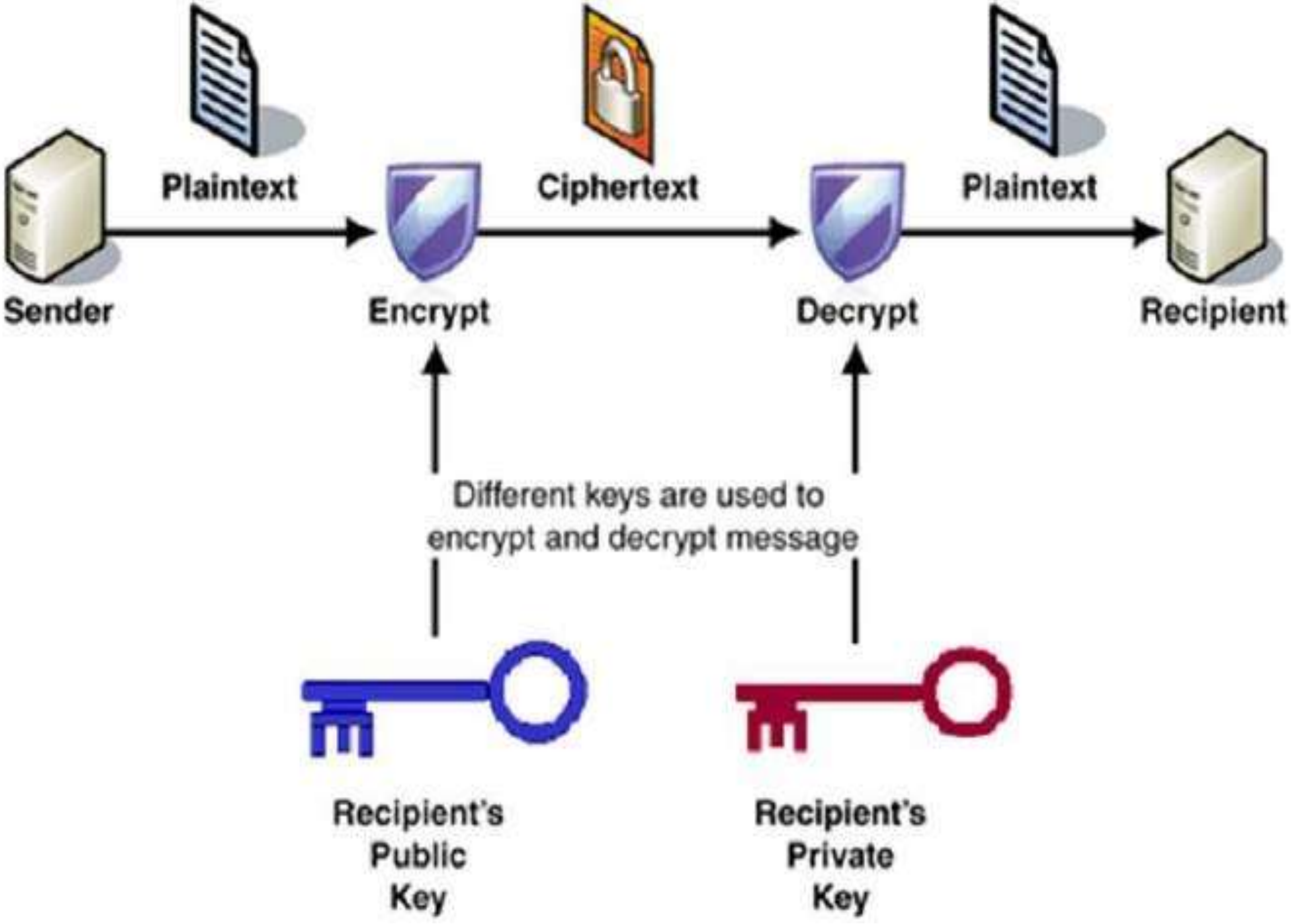
- You must choose a security provider to implement your data encryption algorithm.
- There are many available providers to choose from, but selecting one is the essential initial step in implementation.
- Your selection may depend on the language you are using, **such as Java, Python, C, or MATLAB.**

# RSA

- **RSA (Rivest–Shamir–Adleman)** is a public-key cryptosystem that is widely used for secure data transmission.
- In a public-key cryptosystem, the **encryption key is public** and **distinct from the decryption key, which is kept secret (private).**
- RSA algorithm is **asymmetric cryptography** algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that **the Public Key is given to everyone and Private key is kept private.**

## Example :

- A client (for example browser) sends its public key to the server and requests for some data.
- The server encrypts the data using client’s public key and sends the encrypted data.
- Client receives this data and decrypts it.


Plaintext
Ciphertext
Plaintext
Sender
Encrypt
Decrypt
Recipient
Different keys are used to encrypt and decrypt message
Recipient's Public Key
Recipient's Private Key

# RSA Algorithm

## The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: **private key and public key.**

- **The following steps to work on RSA algorithm :**

## Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N,

$$N=p*q$$

## Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1).

## Step 3: Public key

The specified pair of numbers n and e forms the RSA public key and it is made public.

## Step 4: Private Key

Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows :

$$ed = 1 \bmod (p-1)(q-1)$$

## Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax –

**C = Pe mod n**

## Decryption Formula

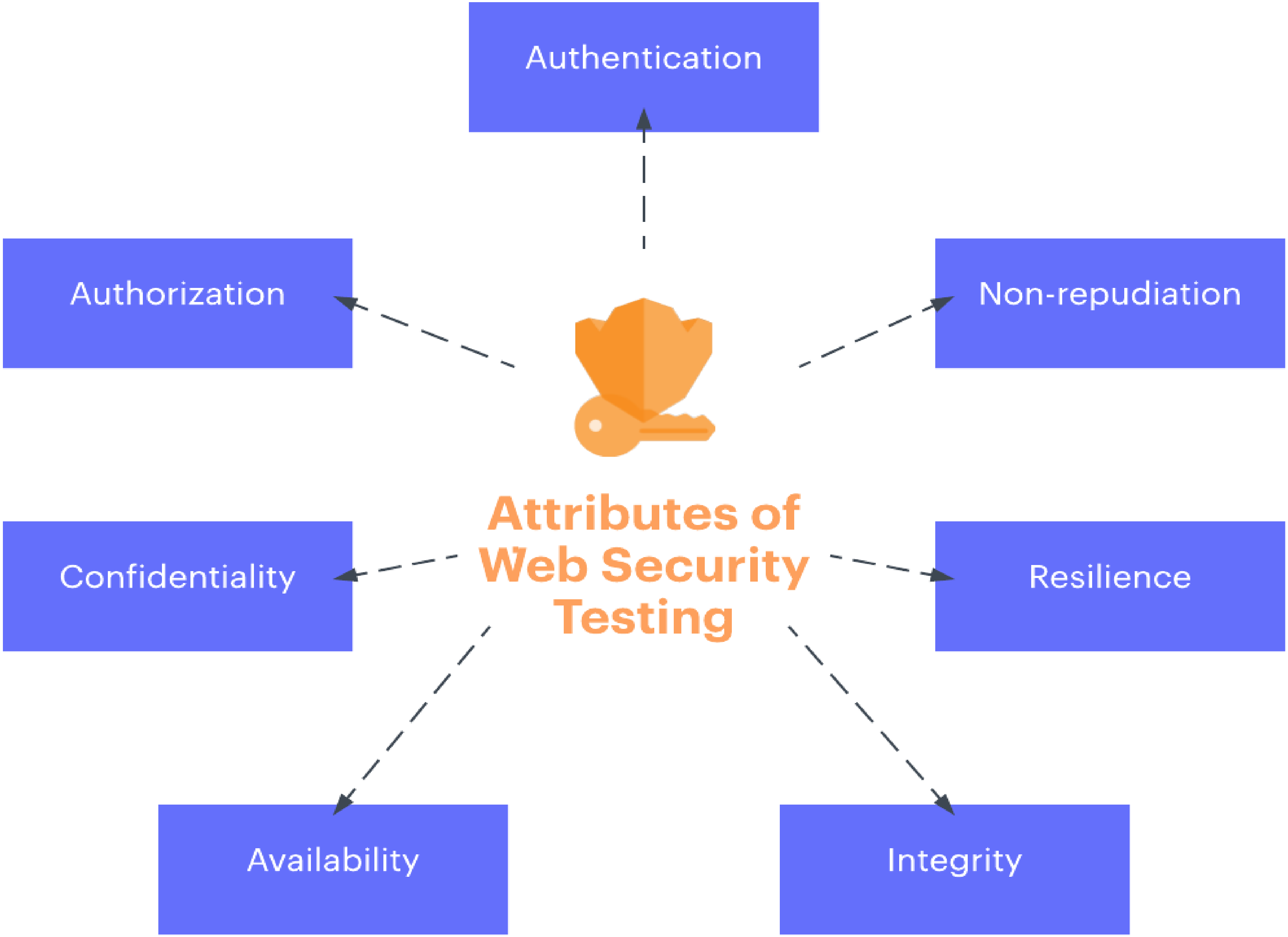
- The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as –

**Plaintext = Cd mod n**

# Web Security

- Web security is also known as **"Cybersecurity".** It basically means protecting a website or web application by **detecting, preventing and responding to cyber threats.**
- web security is easy to install and it also helps the business people to make their website safe and secure.
- A web application firewall prevents automated attacks that usually target small or lesser-known websites.

- Web is now widely used by business, government, and individuals
- But Internet and Web are vulnerable
- Have a variety of threats
    - integrity
    - confidentiality
    - denial of service
    - authentication
- Need to add security mechanisms



Attributes of Web Security Testing

Authentication

Authorization

Non-repudiation

Confidentiality

Resilience

Availability

Integrity

# SSL

- **Secure Sockets Layer (SSL)** is a security protocol that provides privacy, authentication, and integrity to Internet communications.
- SSL eventually evolved into Transport Layer Security (TLS).
- SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995.

# How Does SSL Work?

- SSL encrypts data that is transmitted across the web.
- SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide data integrity.

- **SSL supports the following information security principles:**

**1. Encryption:** protect data transmissions (e.g. browser to server, server to server, application to server, etc.)

**2. Authentication:** ensure the server you’re connected to is actually the correct server.

**3. Data integrity:** ensure that the data that is requested or submitted is what is actually delivered.

# THANK YOU