# (15A04704 ) DATA COMMUNICATIONS & NETWORKING

PREPARED
BY

P.H.CHANDRA MOULI
ASSISTANT PROFESSOR
DEPT OF ECE

# COURSE OUTCOMES

| | |
|---|---|
| **C414.1** | **Explain the fundamental of data communications and networking Layers** |
| **C414.2** | Explain data-link layer, protocols and switching techniques. |
| **C414.3** | Analyze various Multiple Access Techniques & Wired LANs |
| **C414.4** | Apply routing algorithms in network layer. |
| **C414.5** | Analyze the various types of cryptography & network security techniques |

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY ANANTAPUR

B. Tech IV-I Sem. (ECE) L T P C

3 1 0 3

## (15A04704 ) DATA COMMUNICATIONS & NETWORKING

- **UNIT-I**

  **Introduction to Networks & Data Communications**

  The Internet, Protocols & Standards, Layered Tasks, OSI Model, TCP / IP, Addressing, Line Coding Review, Transmission Media: Guided and unguided Media Review.

- **UNIT-II**

  **Switching**

  Datagram Networks, Virtual Circuit Networks, Structure of a switch ,Ethernet Physical Layer, Data Link Layer: Error detection and Correction Data Link Control: Framing, Flow and Error Control Protocols, Noiseless Channel and Noisy Channel Protocol, HDLC, Point-to-Point Protocol.

- **UNIT-III**

  **Multiple Access**

  RANDOH, CDMA, CSMA/CD, CSMA/CA, Controlled Access, Channelization, Wired LANs: IEEE Standards, Standard Ethernet, Fast Ethernet, Gigabit Ethernet, Wireless

  LAN, IEEE 802.11, Bluetooth IEEE 802.16.
- **UNIT-IV**

  **Network Layer**

  Design Issues, Routing Algorithms, Congestion control, Algorithms.IPV4 Addresses, Connecting Devices, Virtual LAN IPV6 Addresses, Internet Protocol, Hardware

  Addressing versus IP Addressing, IP Data Gram.
- **UNIT-V**

  **Transport Layer Protocol**

  UDP and TCP, ATM, Cryptography, Network Security

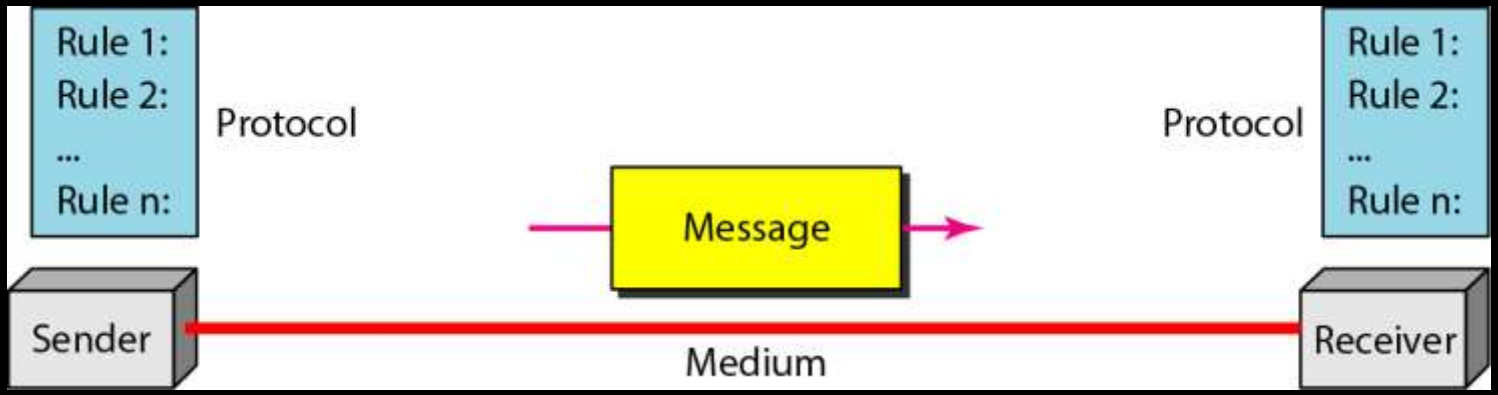
# Chapter 1

# Introduction to Networks & Data Communications

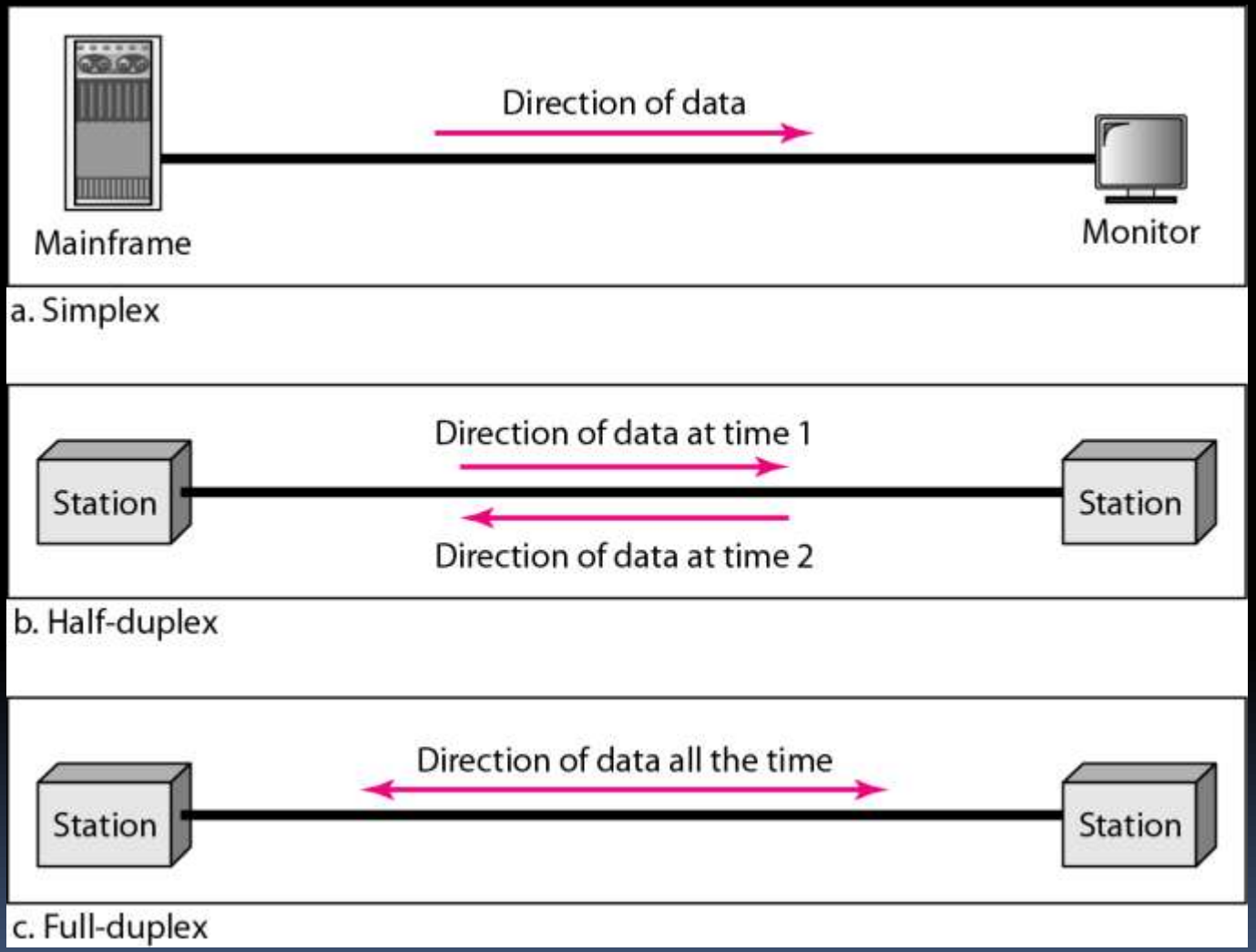
# DATA COMMUNICATIONS

The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

## Figure 1.1 *Components of a data communication system*



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



# NETWORKS

*A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.*

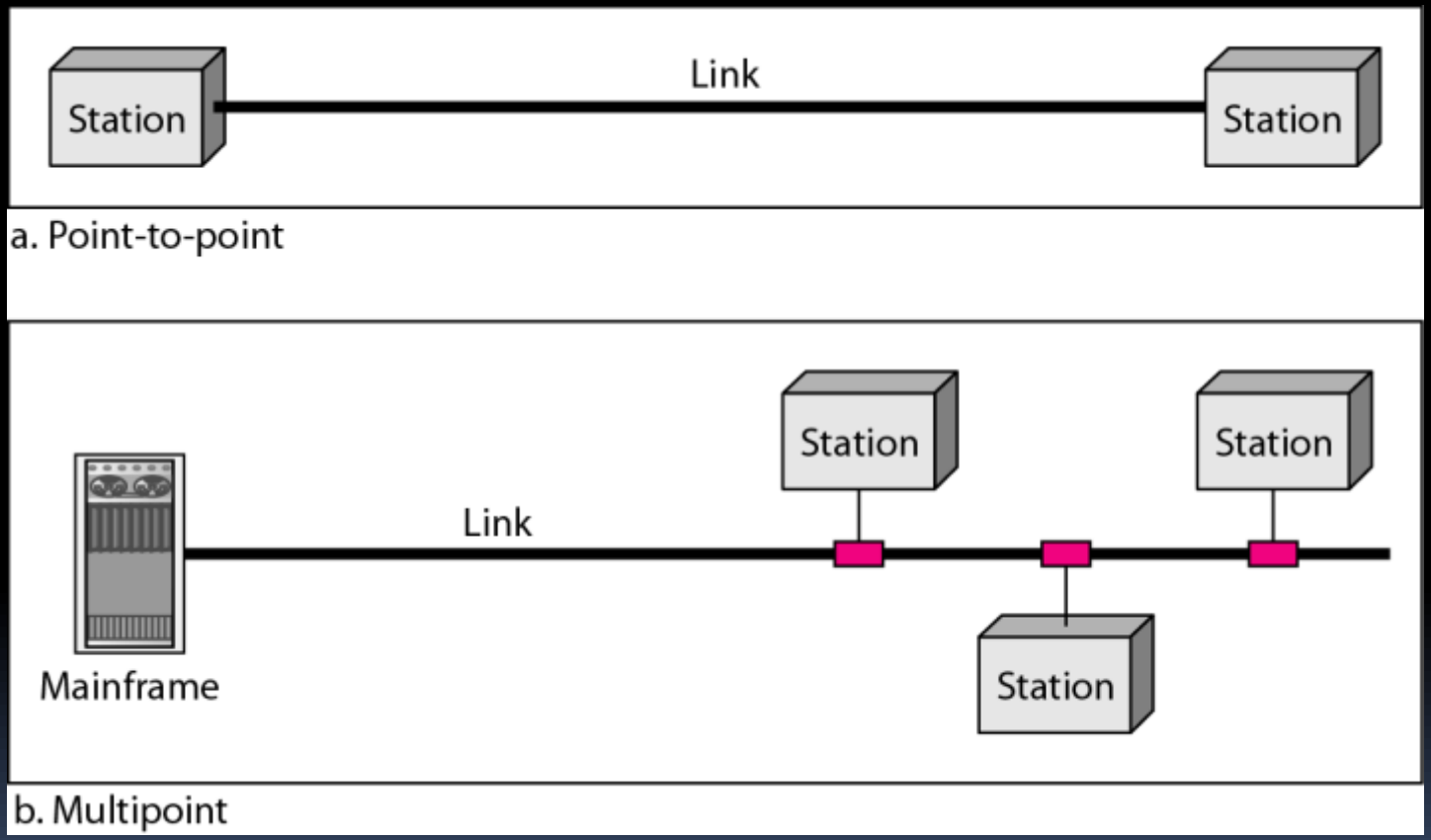
# Network Criteria

- Performance
  - Depends on Network Elements
  - Measured in terms of Delay and Throughput
- Reliability
  - Failure rate of network components
  - Measured in terms of availability/robustness
- Security
  - Data protection against corruption/loss of data due to:
    - Errors
    - Malicious users

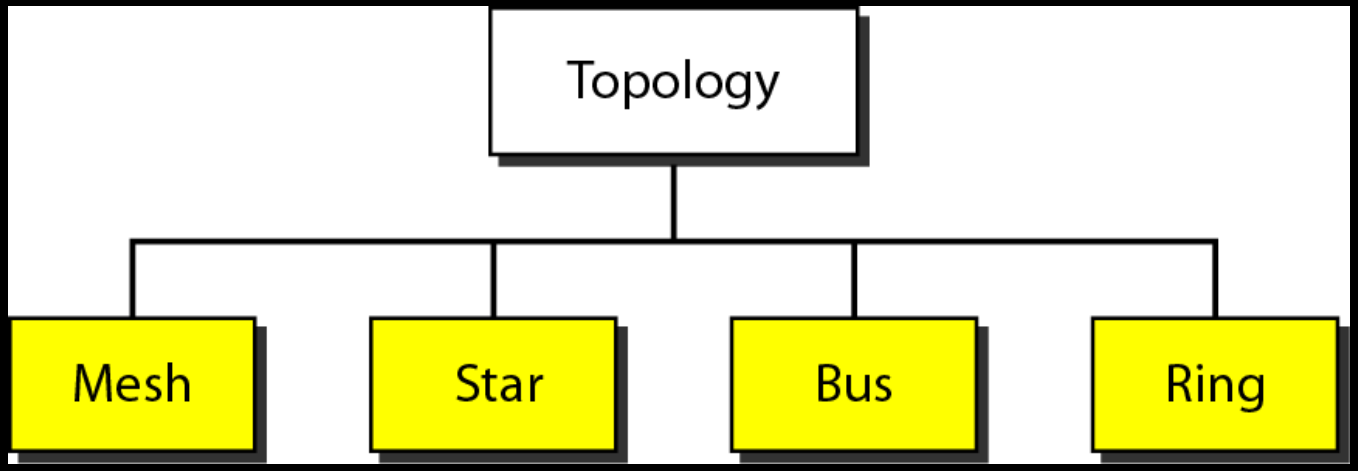
# Physical Structures

- Type of Connection
  - Point to Point - single transmitter and receiver
  - Multipoint - multiple recipients of single transmission
- Physical Topology
  - Connection of devices
  - Type of transmission - unicast, mulitcast, broadcast

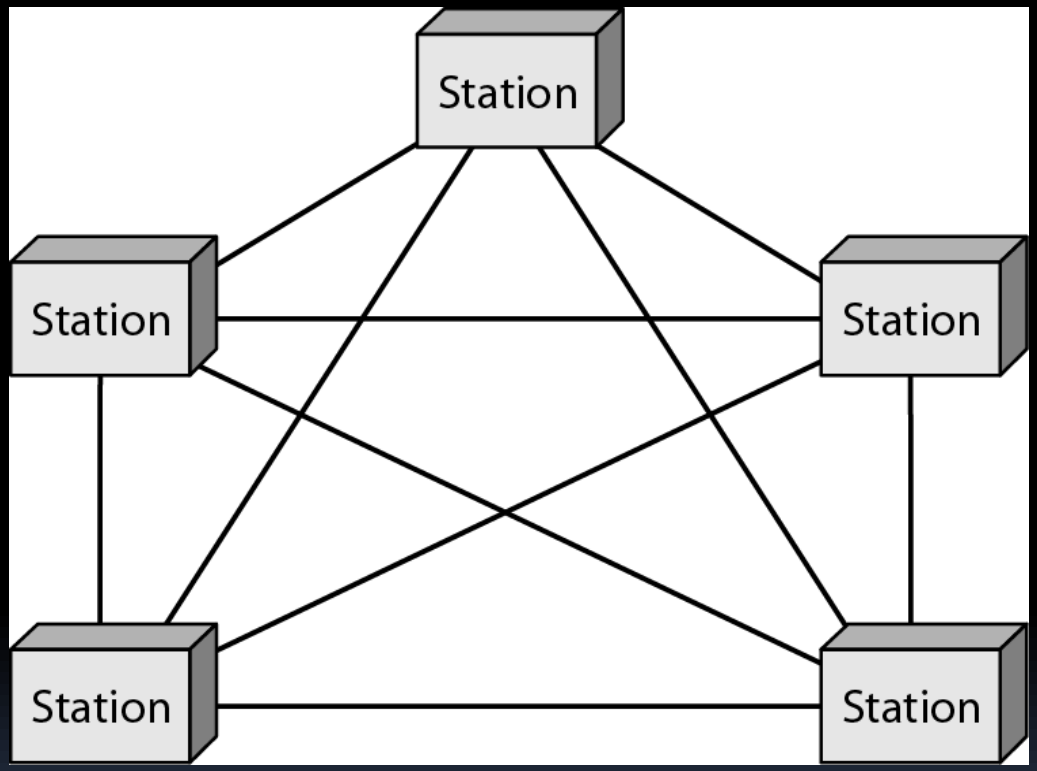
## Figure : *Types of connections: point-to-point and multipoint*



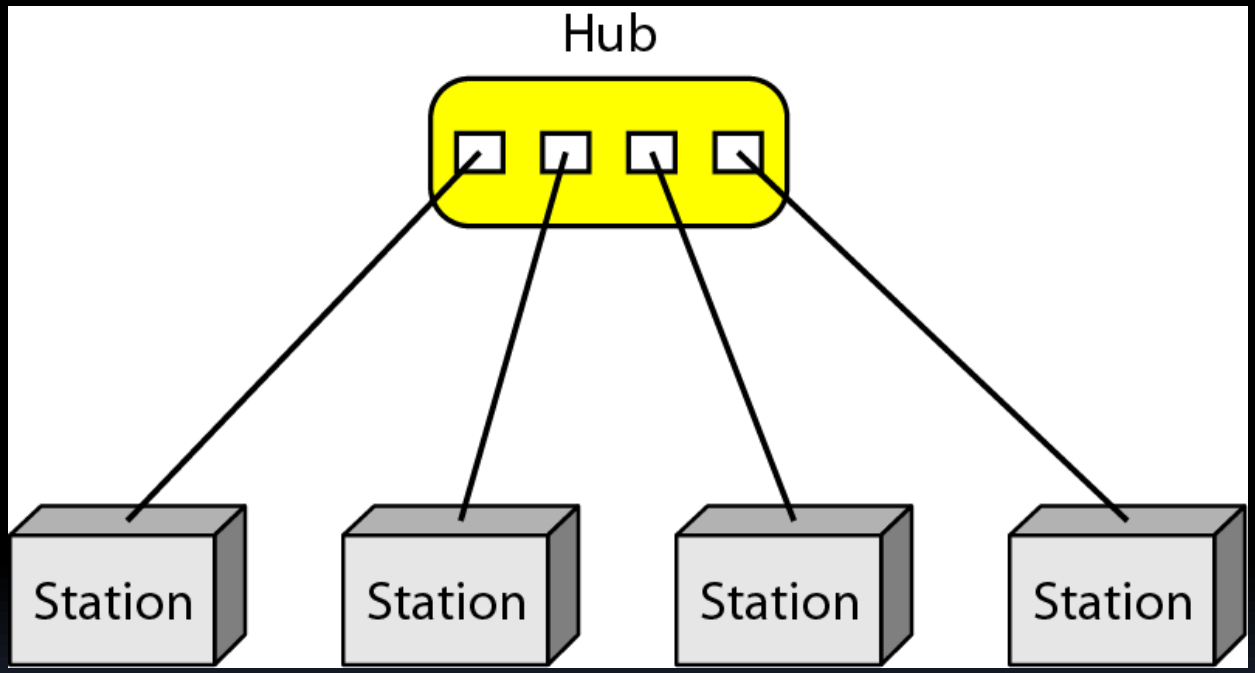
## Figure 1.4 *Categories of topology*



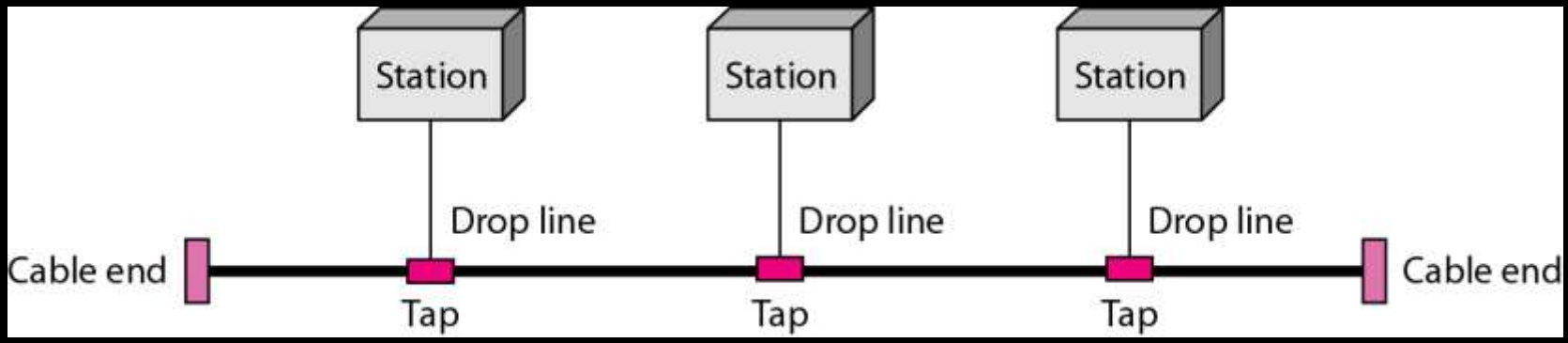
## Figure : *A fully connected mesh topology (five devices)*



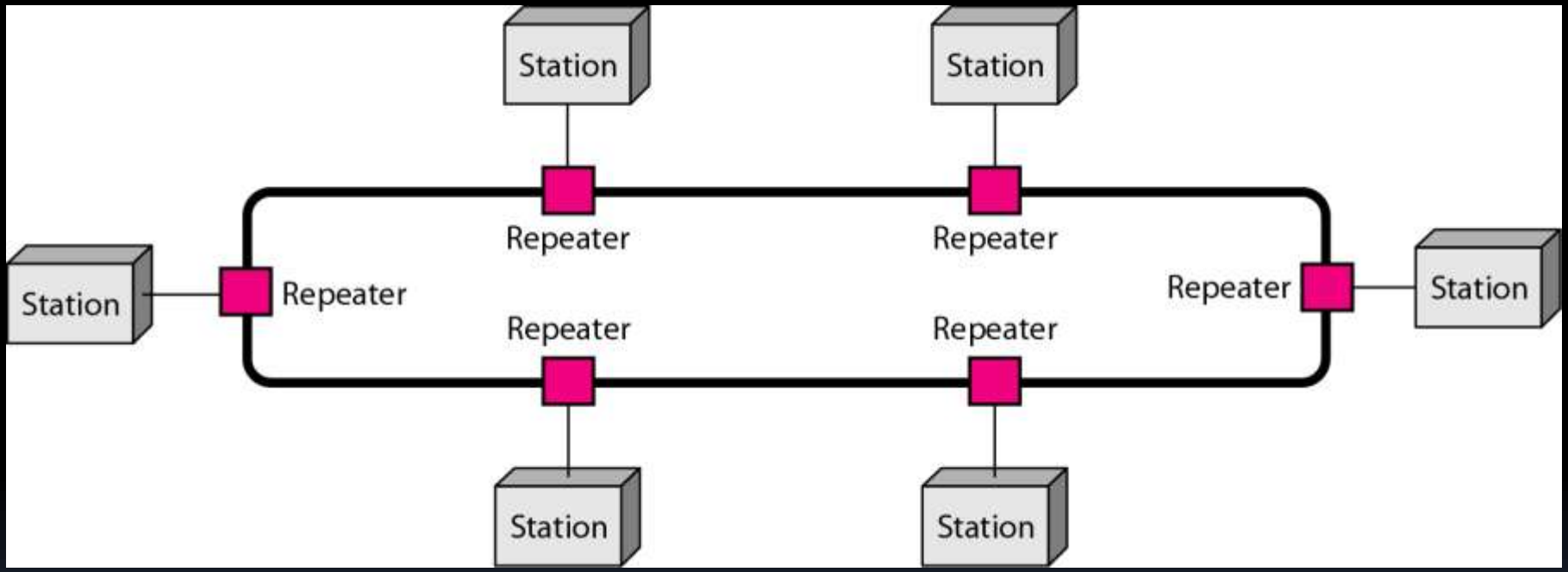
## Figure : *A star topology connecting four stations*



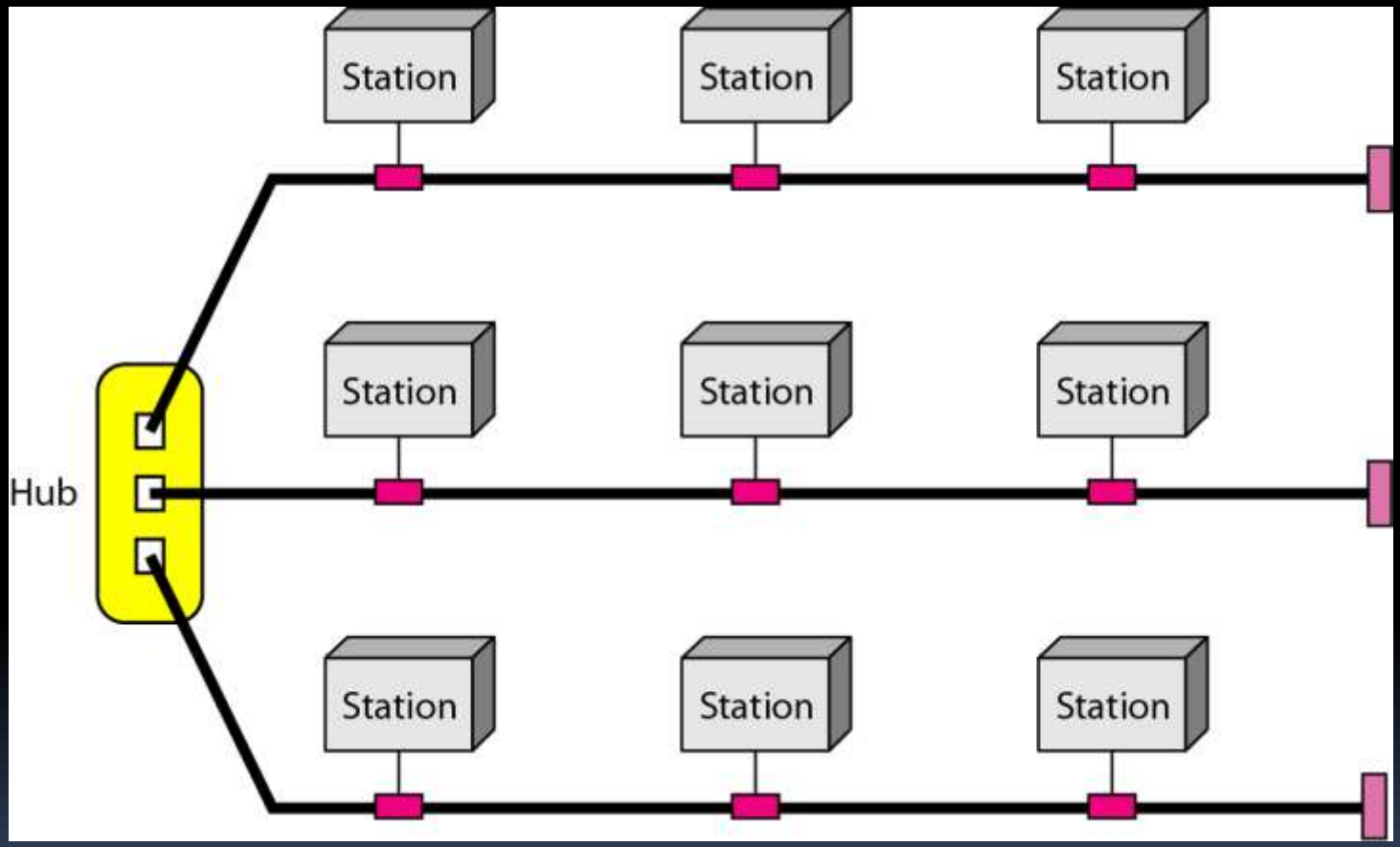
## Figure 1.7 *A bus topology connecting three stations*



## Figure 1.8 *A ring topology connecting six stations*



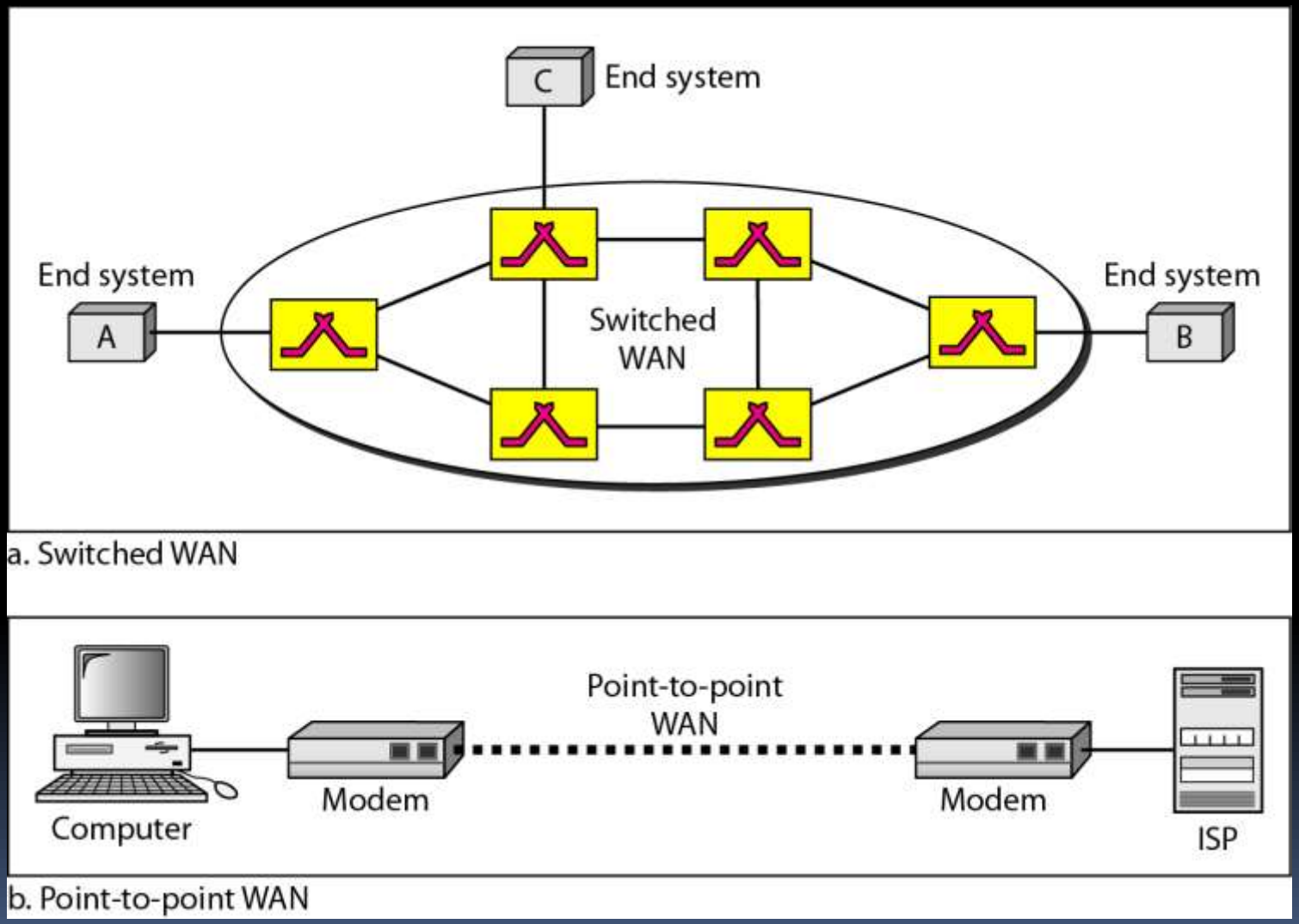
## Figure : *A hybrid topology: a star backbone with three bus networks*



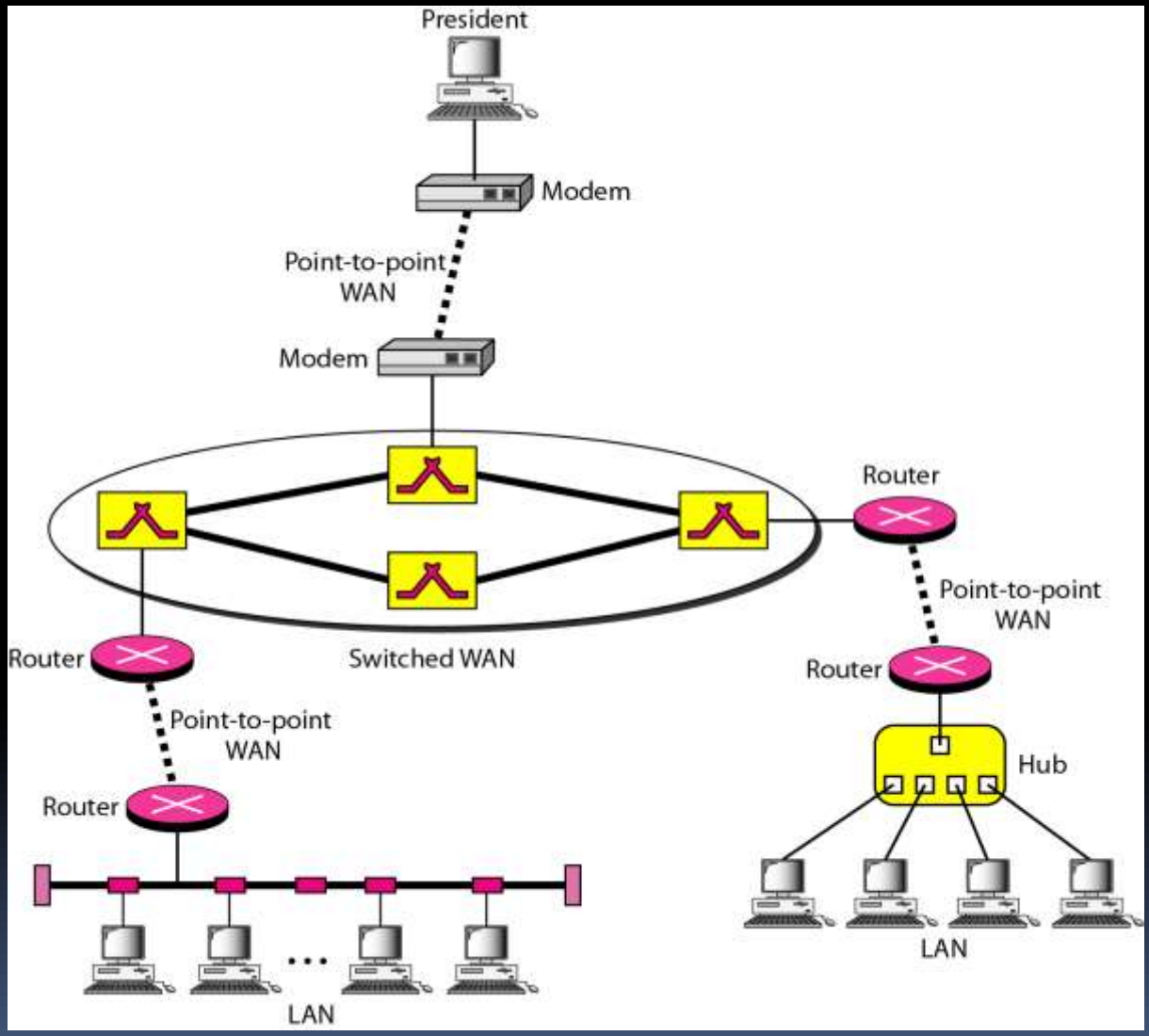
# Categories of Networks

- Local Area Networks (LANs)
  - Short distances
  - Designed to provide local interconnectivity
- Wide Area Networks (WANs)
  - Long distances
  - Provide connectivity over large areas
- Metropolitan Area Networks (MANs)
  - Provide connectivity over areas such as a city, a campus

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



# Figure : *A heterogeneous network made of four WANs and two LANs*



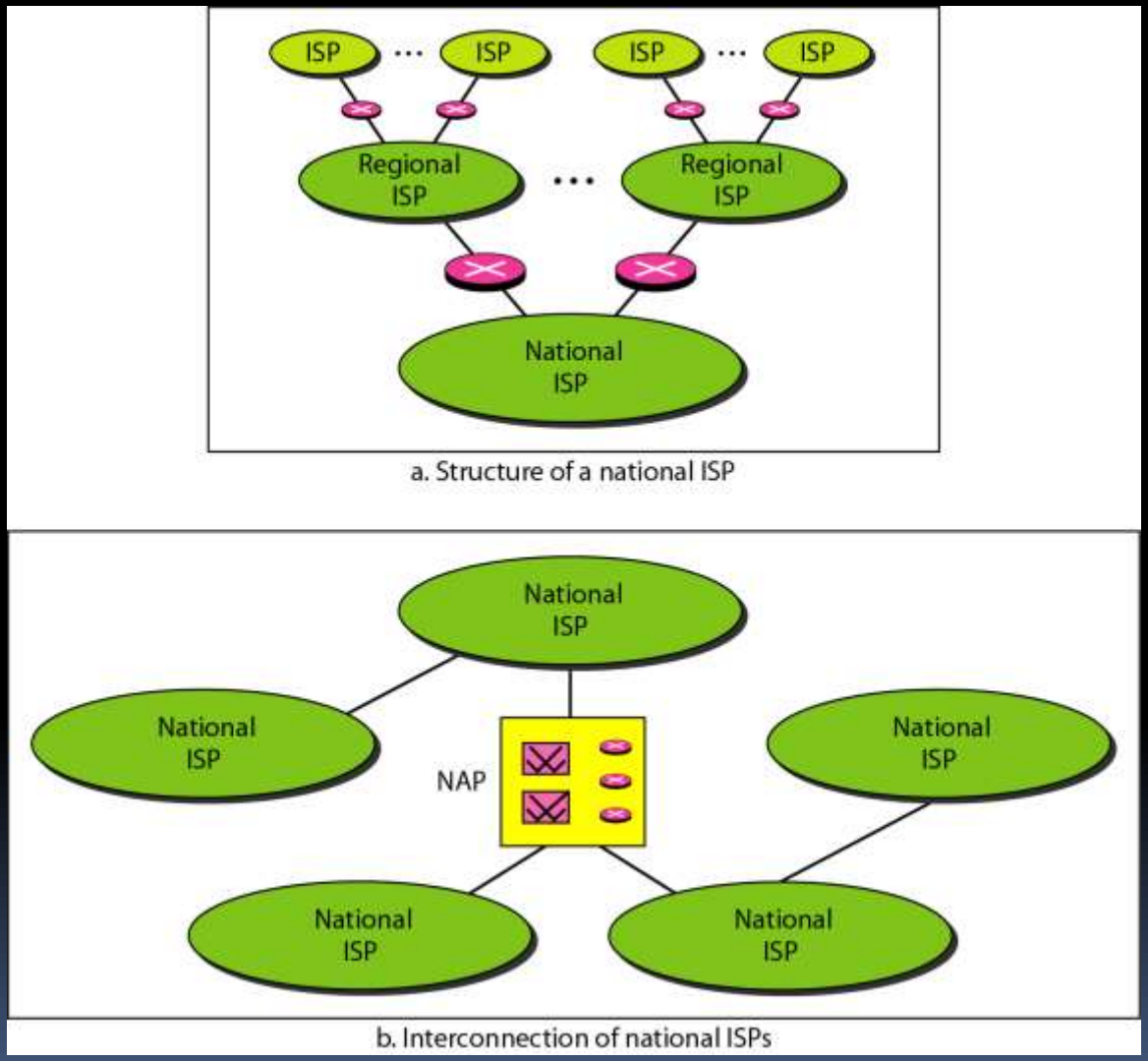
# THE INTERNET

***The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.***

***Topics discussed in this section:***

**Organization of the Internet**
**Internet Service Providers (ISPs)**

# Figure : *Hierarchical organization of the Internet*



# PROTOCOLS

***A protocol is synonymous with rule. It consists of a set of rules that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are syntax, semantics and timing***

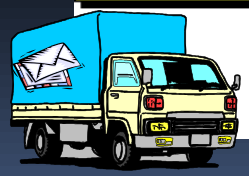
- **Syntax**
- **Semantics**
- **Timing**

# Elements of a Protocol

- Syntax
  - Structure or format of the data
  - Indicates how to read the bits - field delineation
- Semantics
  - Interprets the meaning of the bits
  - Knows which fields define what action
- Timing
  - When data should be sent and what
  - Speed at which data should be sent or speed at which it is being received.

# Layered Tasks

**An example from the everyday life**




**Hierarchy?**

**Services**

# Why layered communication?

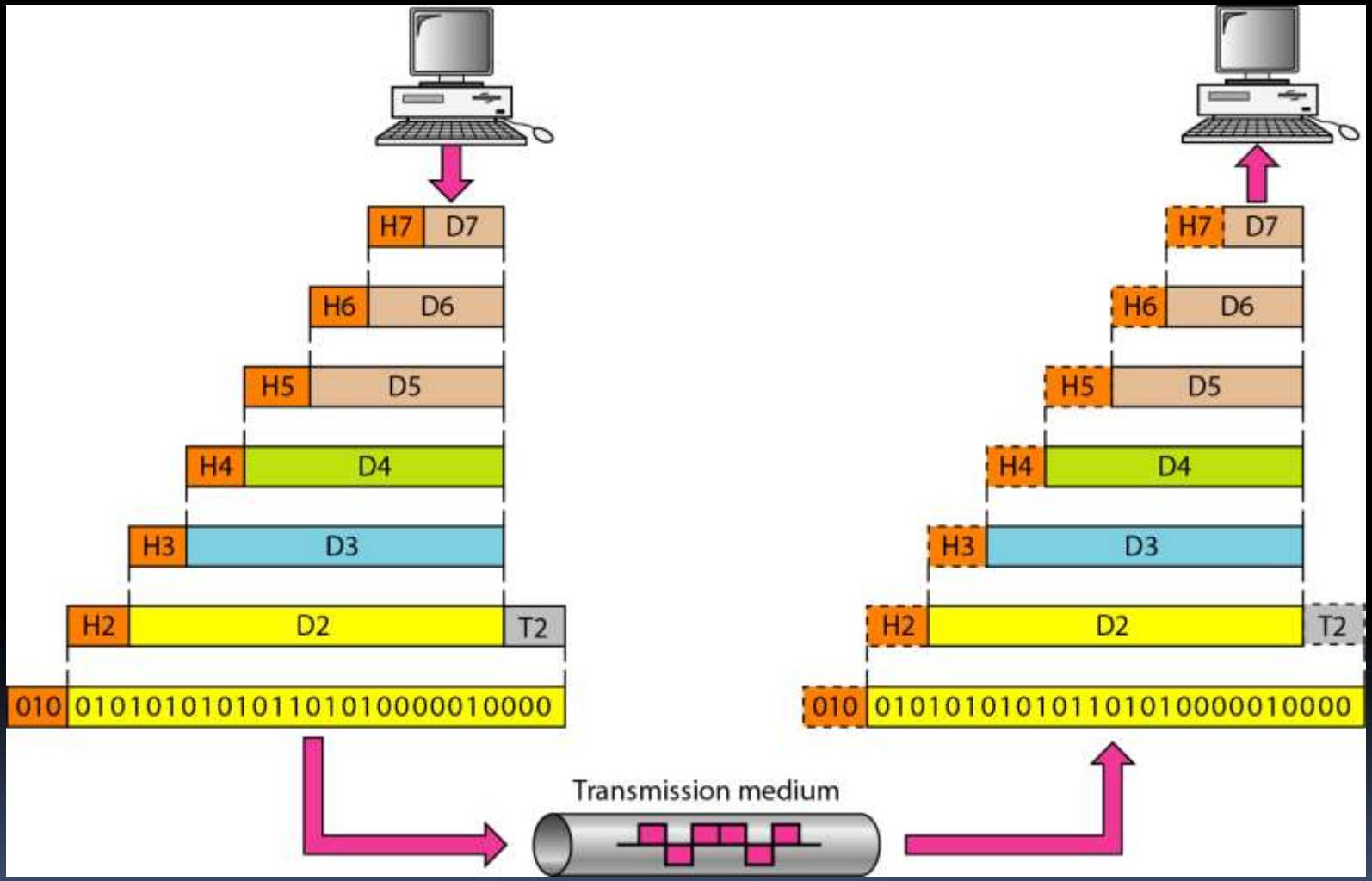
- To reduce complexity of communication task by splitting it into several layered small tasks
- Functionality of the layers can be changed as long as the service provided to the layer above stays unchanged
  - makes easier maintenance & updating
- Each layer has its own task
- Each layer has its own protocol

# OSI Reference model

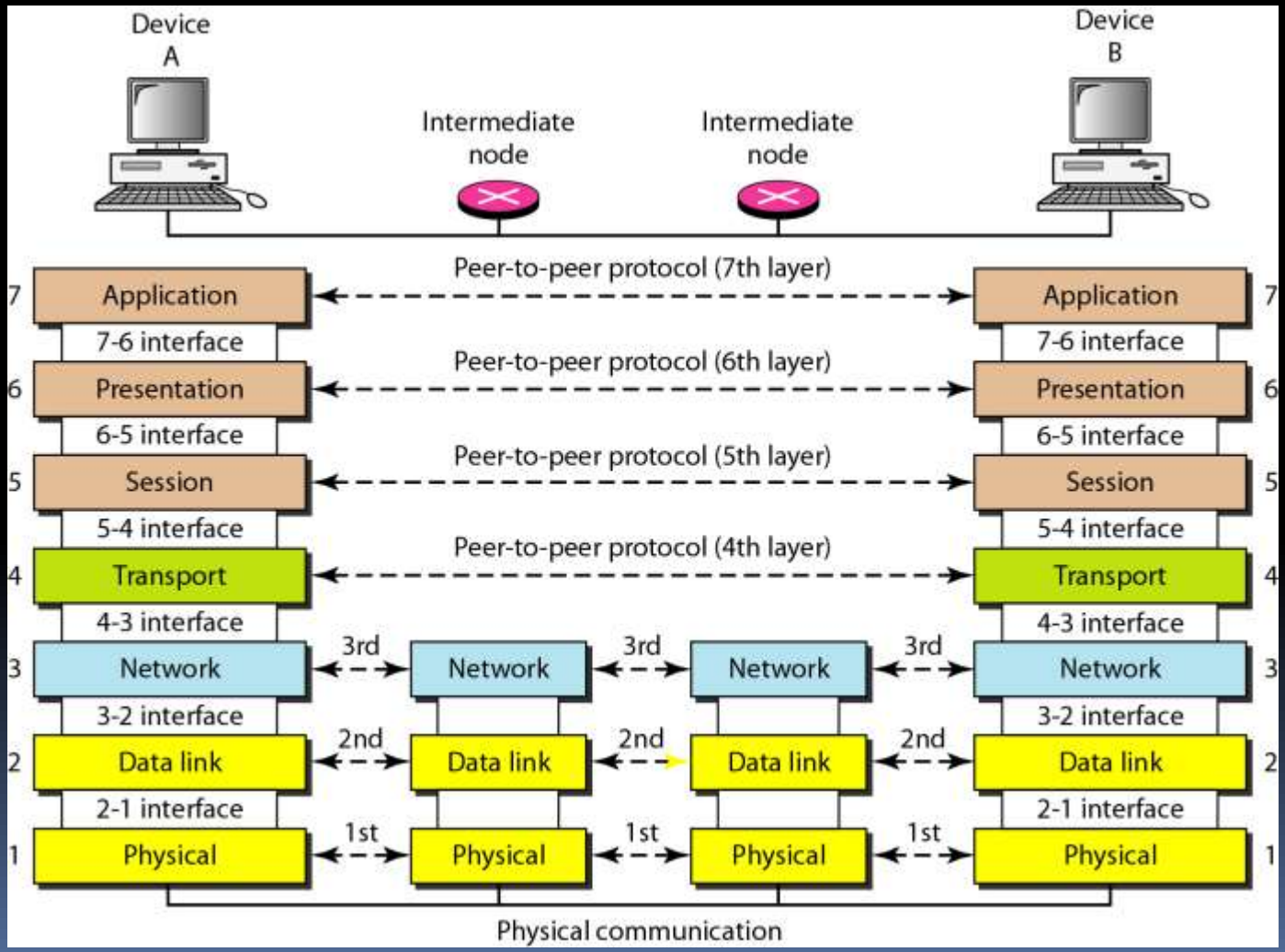
- Open System Interconnection
- 7 layers

1. Create a layer when different abstraction is needed
2. Each layer performs a well define function
3. Functions of the layers chosen taking internationally standardized protocols
4. Number of layers – large enough to avoid complexity

# Exchange using OSI Model



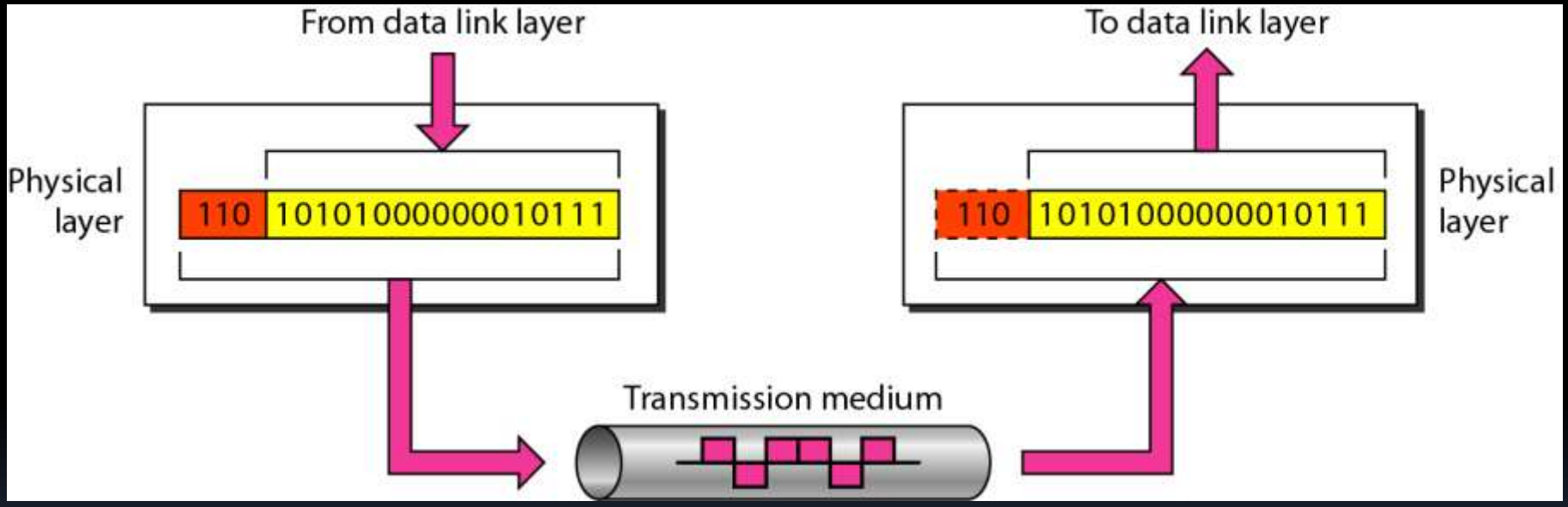
# The interaction between layers in the OSI model



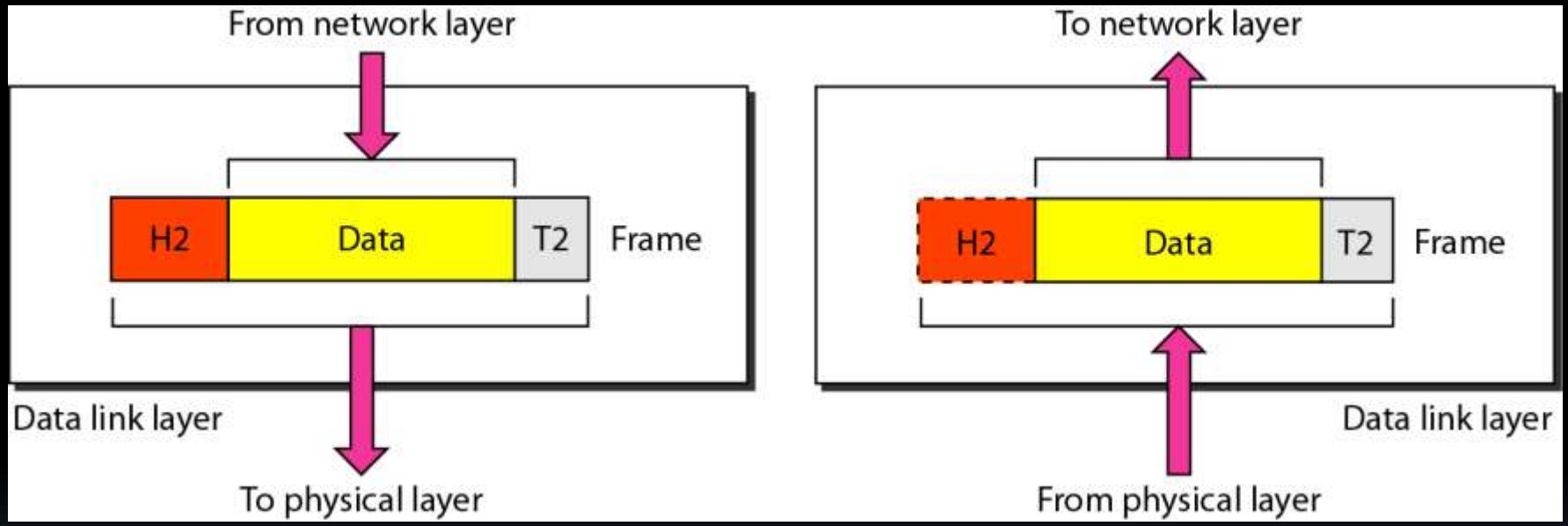
# Issues, to be resolved by the layers

- Larger bandwidth at lower cost
- Error correction
- Flow control
- Addressing
- Multiplexing
- Naming
- Congestion control
- Mobility
- Routing
- Fragmentation
- Security

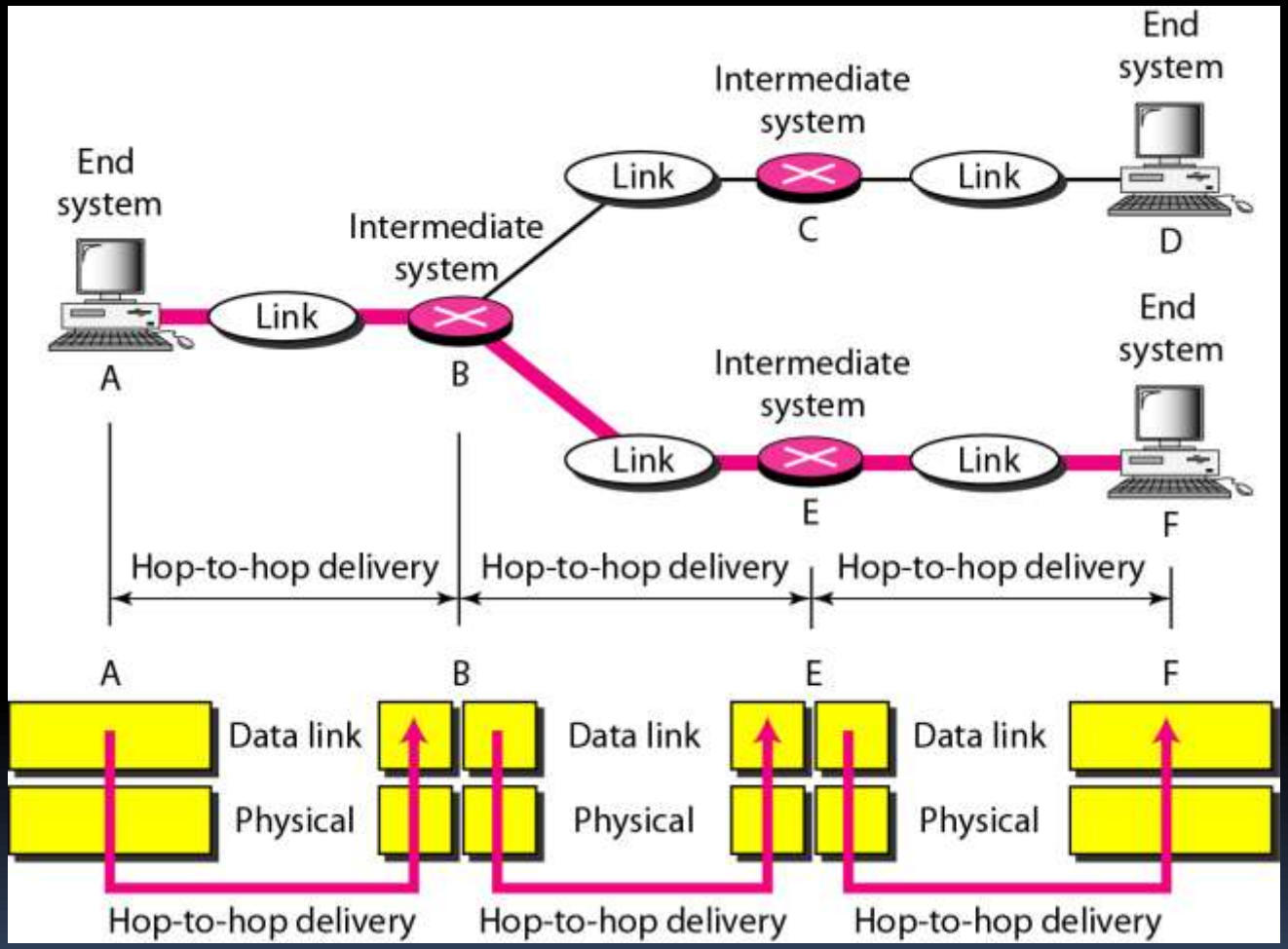
# Figure 2.5 *Physical layer*



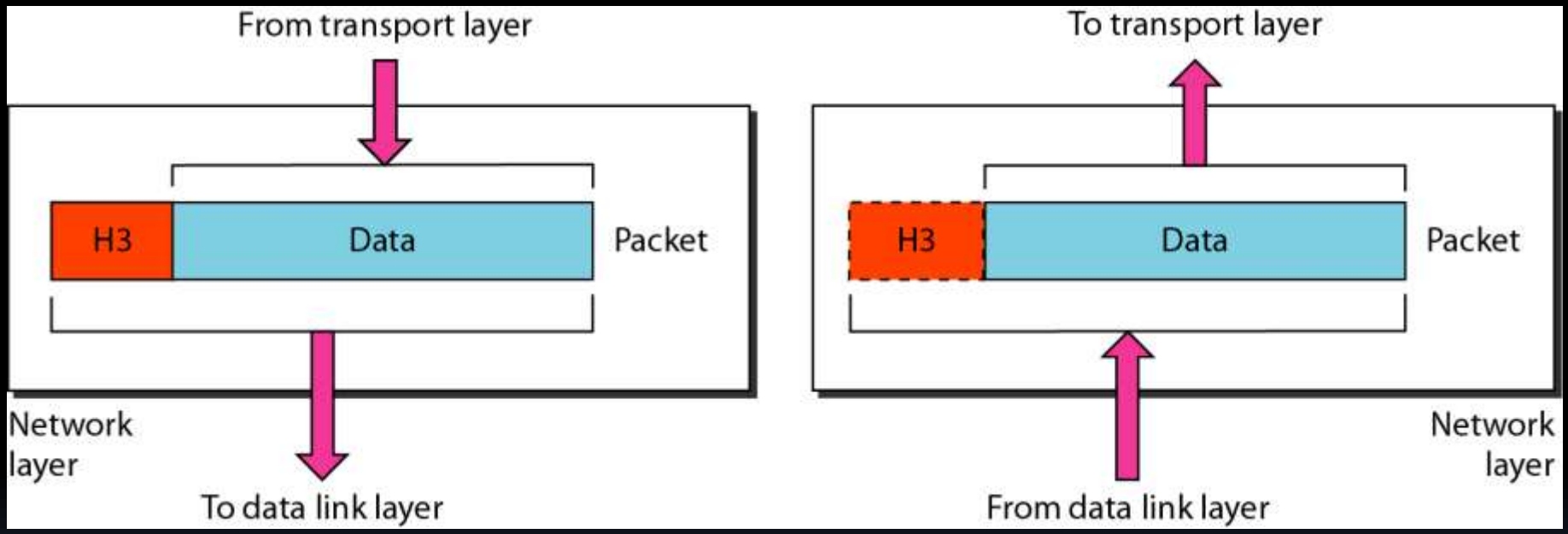
# Figure 2.6 *Data link layer*



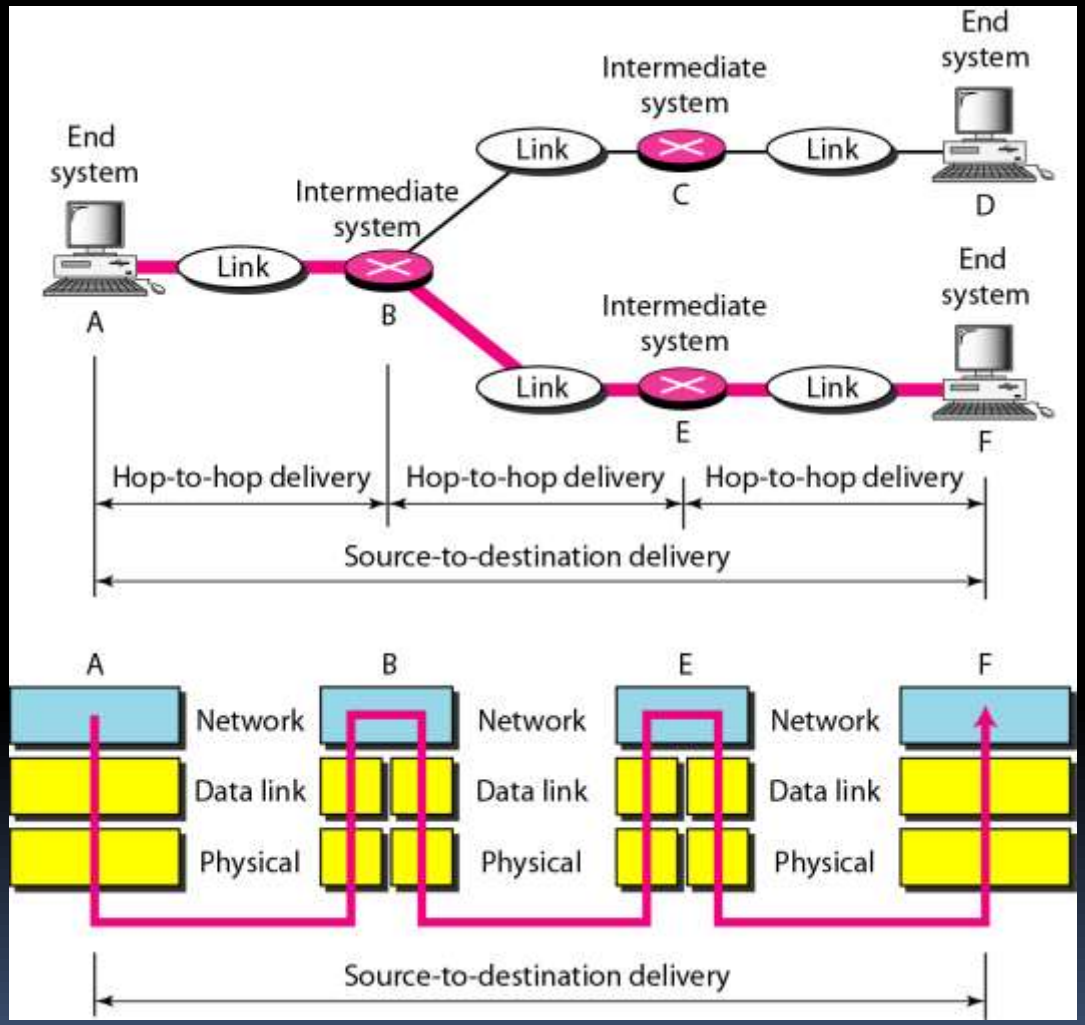
# Figure 2.7 *Hop-to-hop delivery*



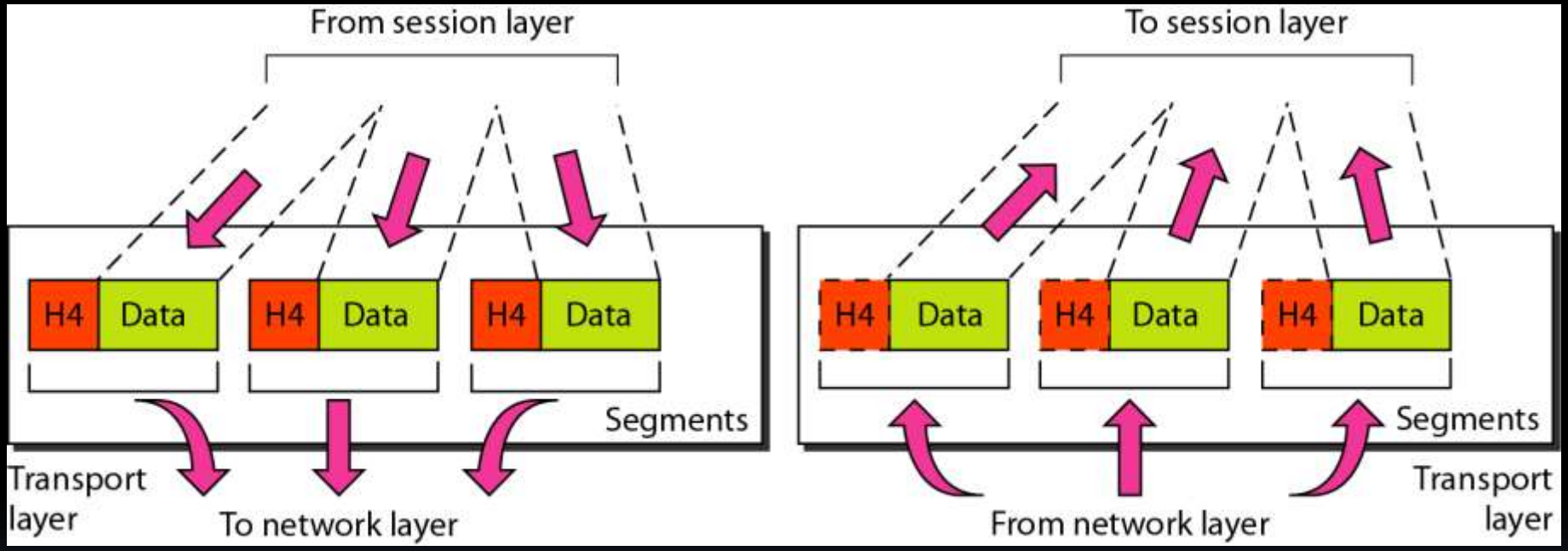
# Figure 2.8 *Network layer*



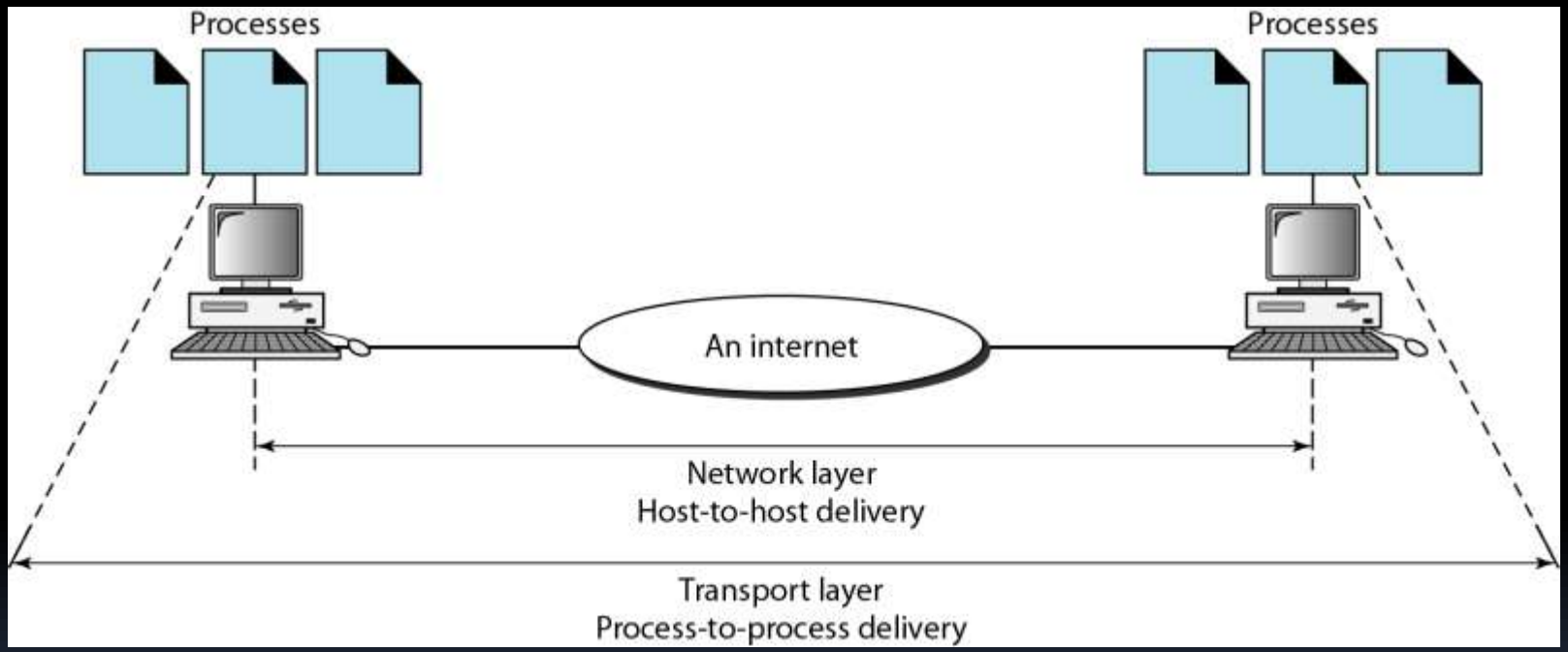
# Figure 2.9 *Source-to-destination delivery*



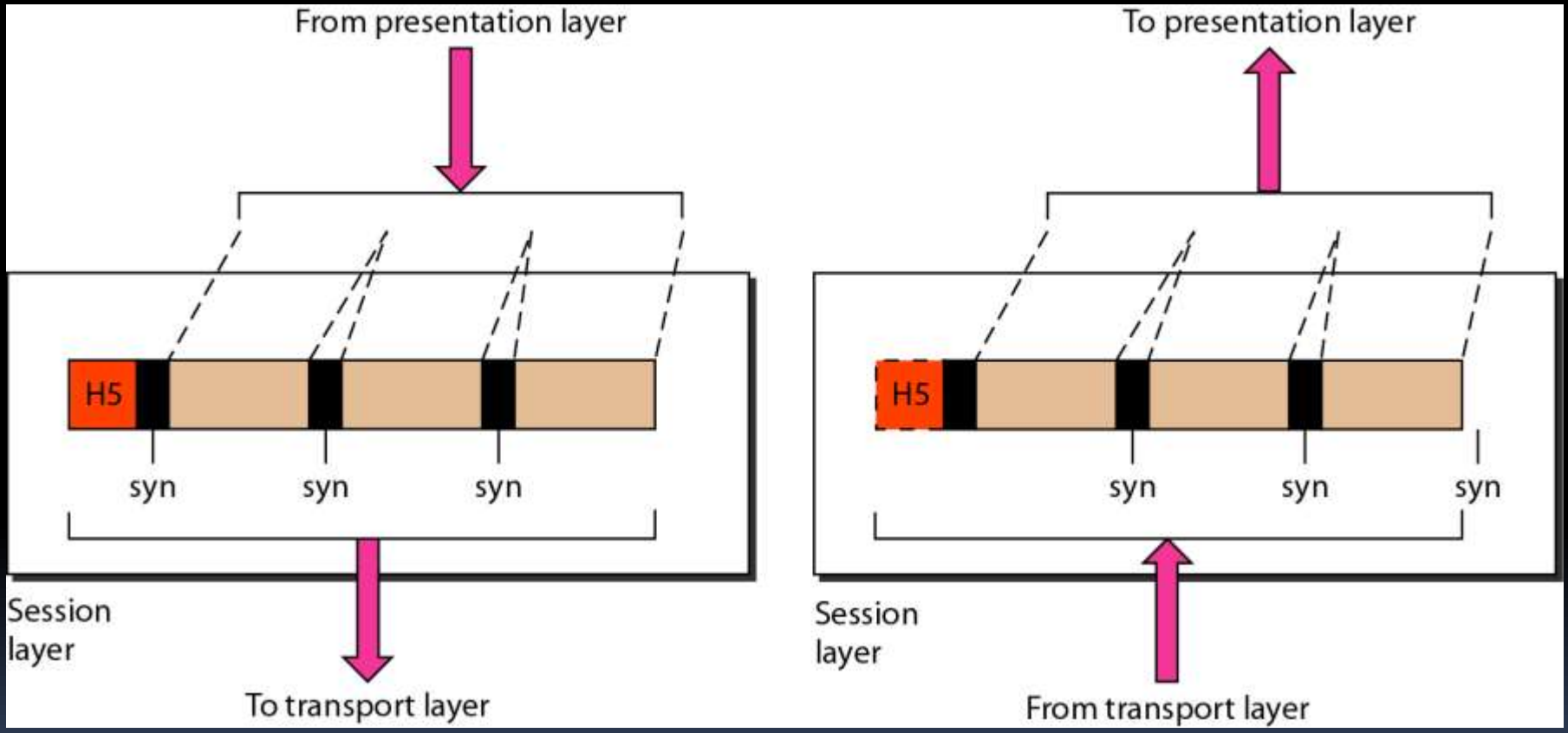
# Figure 2.10 *Transport layer*



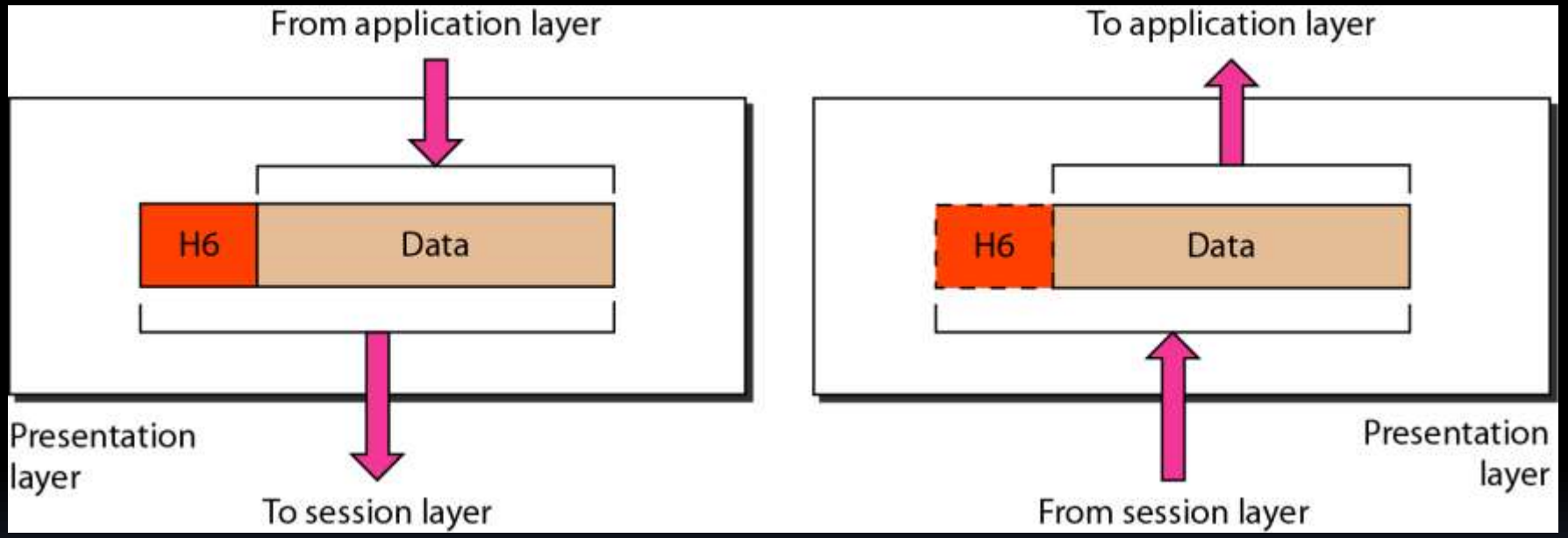
# Figure 2.11 *Reliable process-to-process delivery of a message*



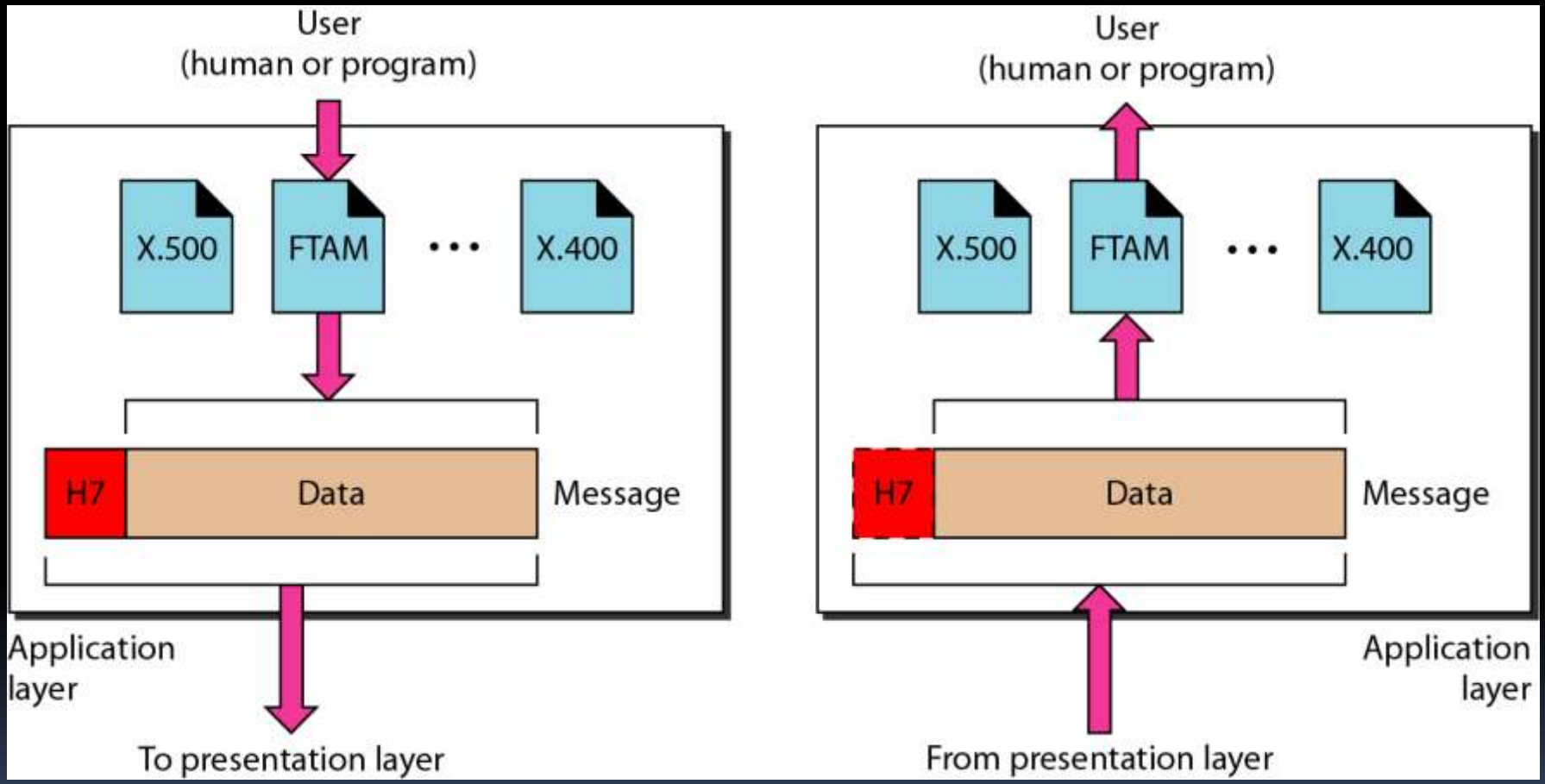
# Figure 2.12 *Session layer*



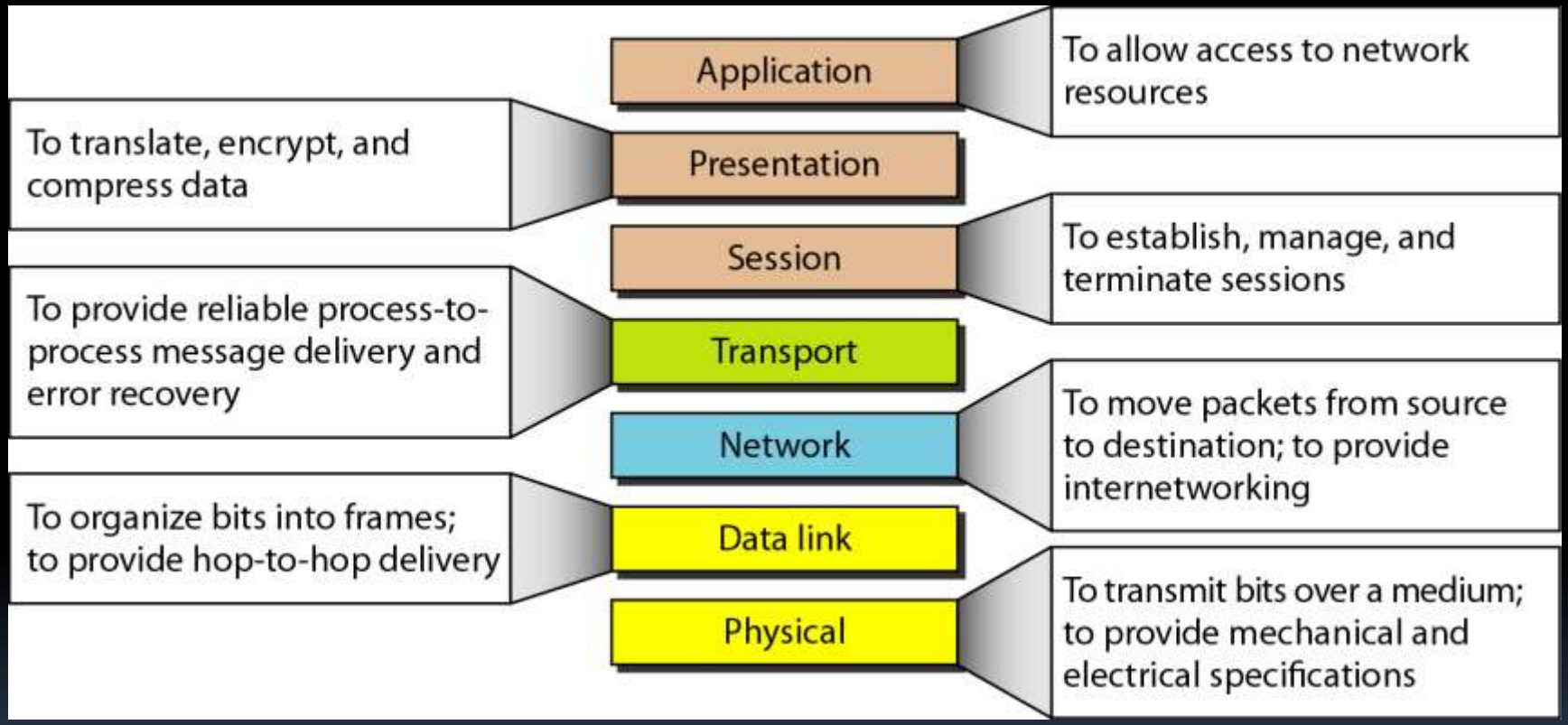
# Figure 2.13 *Presentation layer*



# Figure 2.14 *Application layer*



# Figure 2.15 *Summary of layers*

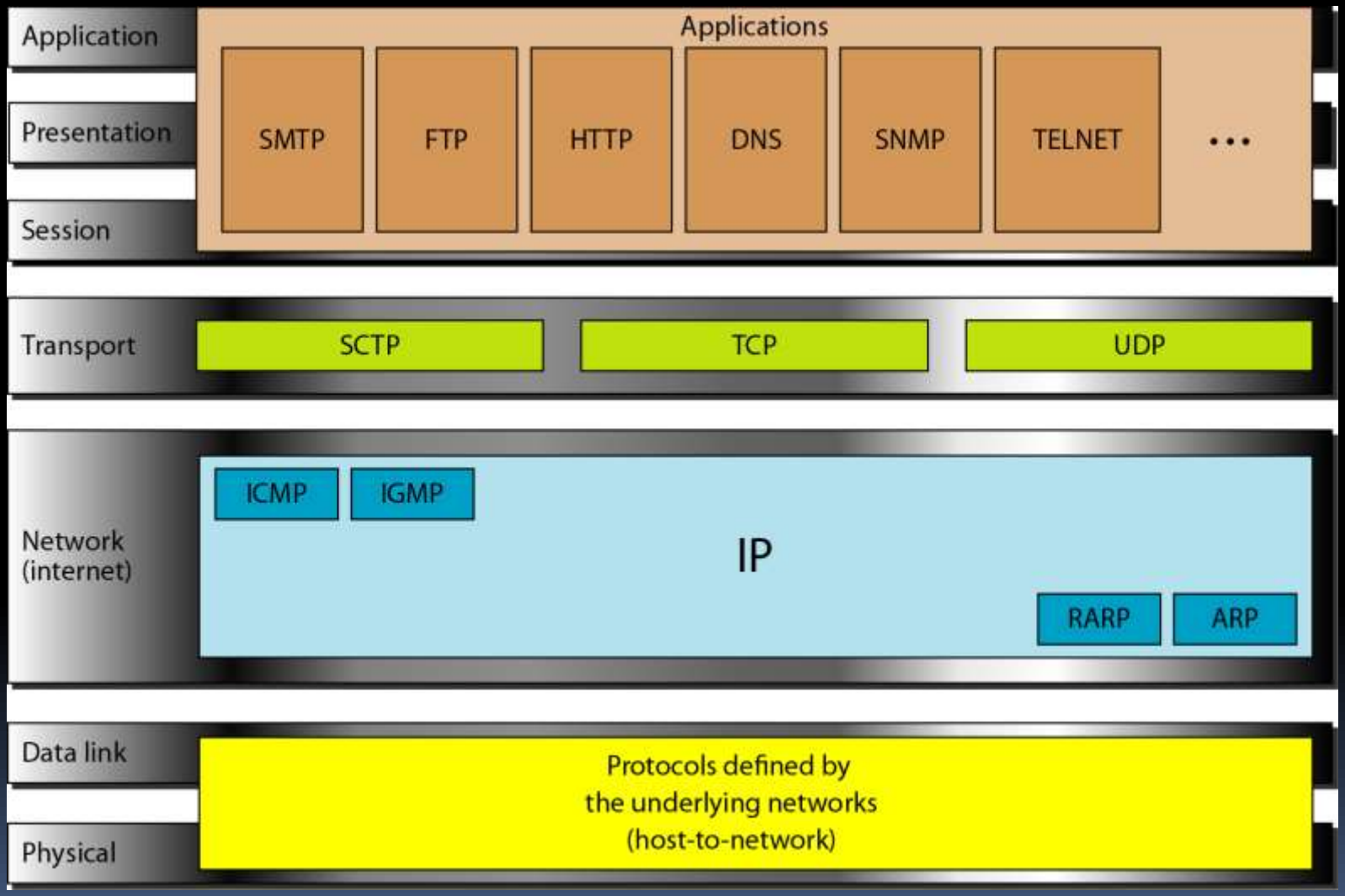


# TCP/IP PROTOCOL SUITE

***The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.***

**Physical and Data Link Layers**
**Network Layer**
**Transport Layer**
**Application Layer**

# Figure 2.16 *TCP/IP and OSI model*

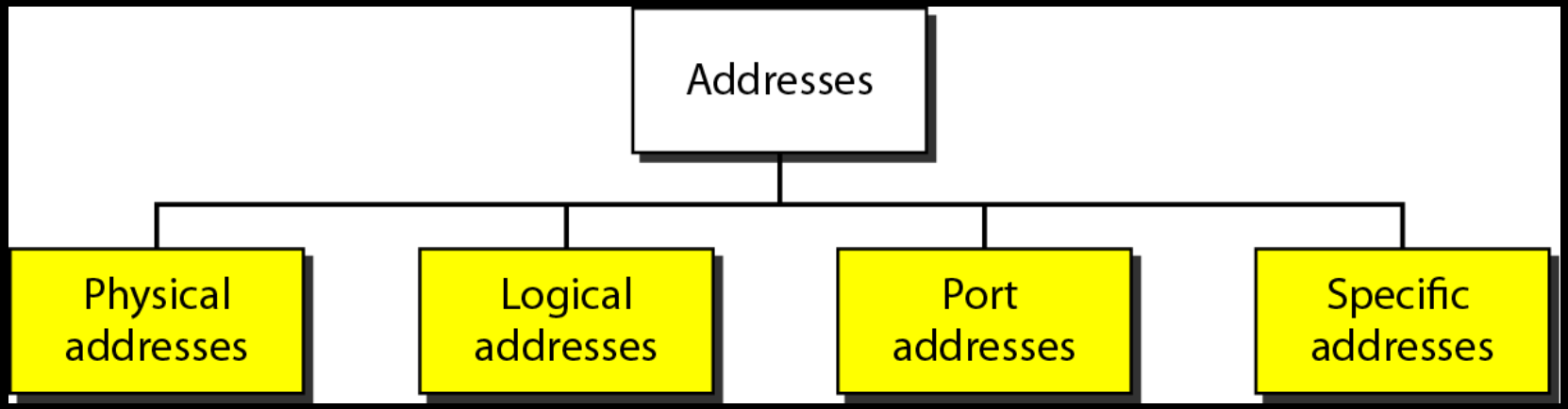


# ADDRESSING

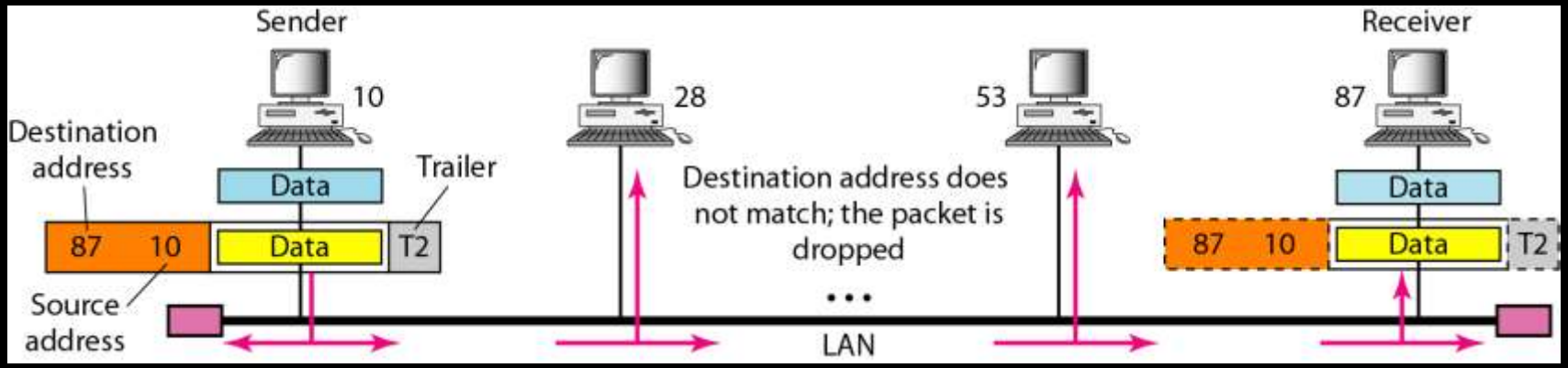
***Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.***

**Physical Addresses**
**Logical Addresses**
**Port Addresses**
**Specific Addresses**

## Figure 2.17 *Addresses in TCP/IP*



# Figure 2.19 *Physical addresses*



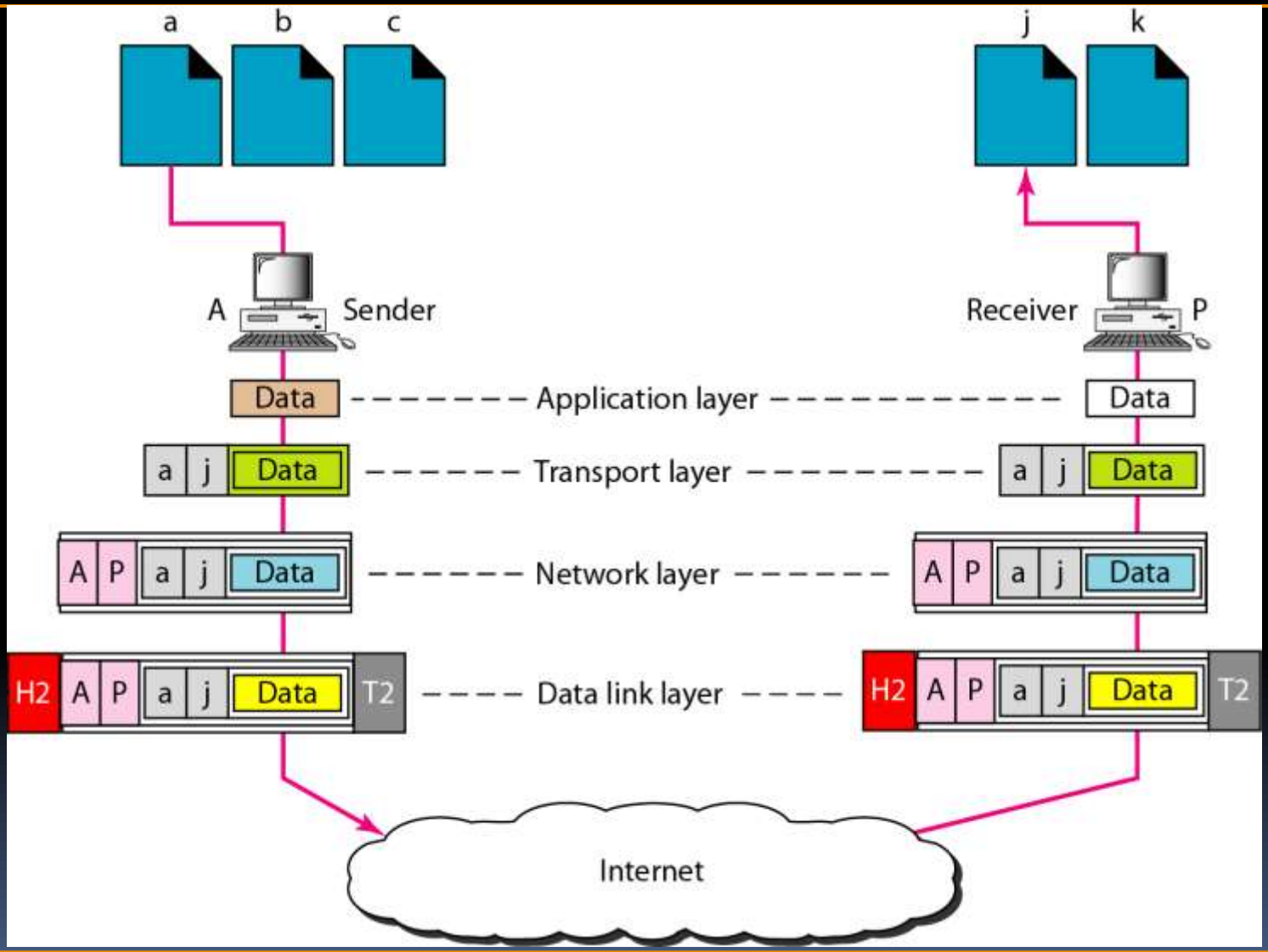
# *Example 2.2*

***Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:***

**07:01:02:01:2C:4B**

**A 6-byte (12 hexadecimal digits) physical address.**

# Figure 2.21 *Port addresses*



# Example 2.5

*A port address is a 16-bit address represented by one decimal number as shown.*

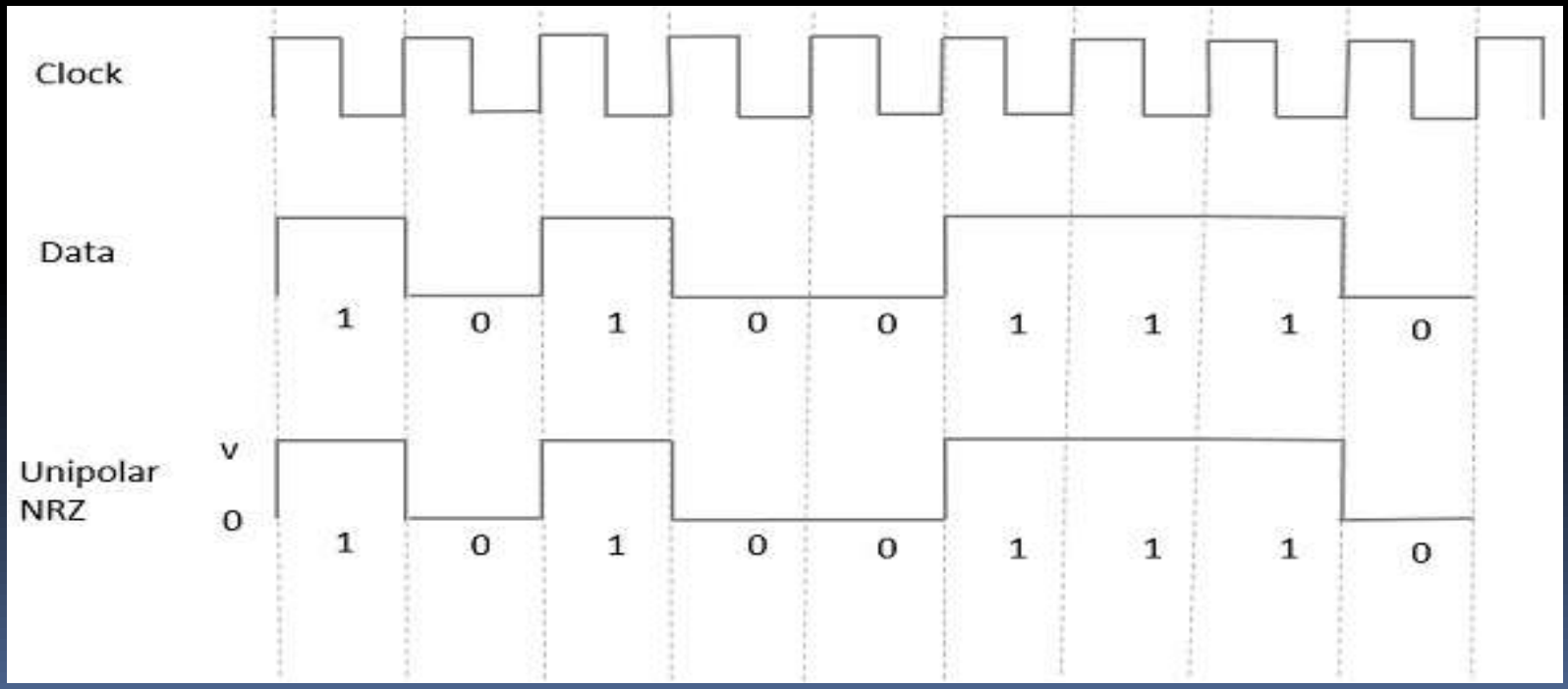
**753**

**A 16-bit port address represented as one single number.**

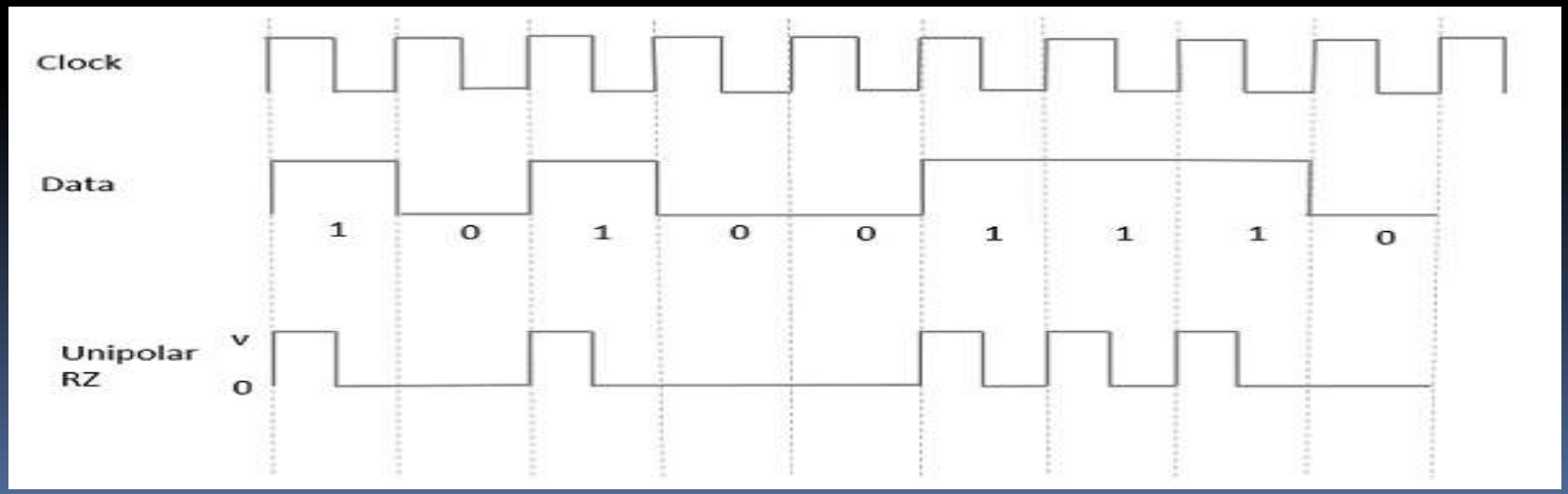
- **LINE CODING REVIEW:**
- A **line code** is the code used for data transmission of a digital signal over a transmission line. This process of coding is chosen so as to avoid overlap and distortion of signal such as inter-symbol interference.
- **Properties of Line Coding**
- Following are the properties of line coding –
- As the coding is done to make more bits transmit on a single signal, the bandwidth used is much reduced.
- For a given bandwidth, the power is efficiently used.
- The probability of error is much reduced.
- Error detection is done and the bipolar too has a correction capability.

- **Types of Line Coding**
- Unipolar
- Polar
- Bi-polar
- **Unipolar Signaling:**
- Unipolar signaling is also called as **On-Off Keying** or simply **OOK**.
- The presence of pulse represents a **1** and the absence of pulse represents a **0**.
- There are two variations in unipolar signaling
- Non Return to Zero (NRZ)
- Return to Zero (RZ)

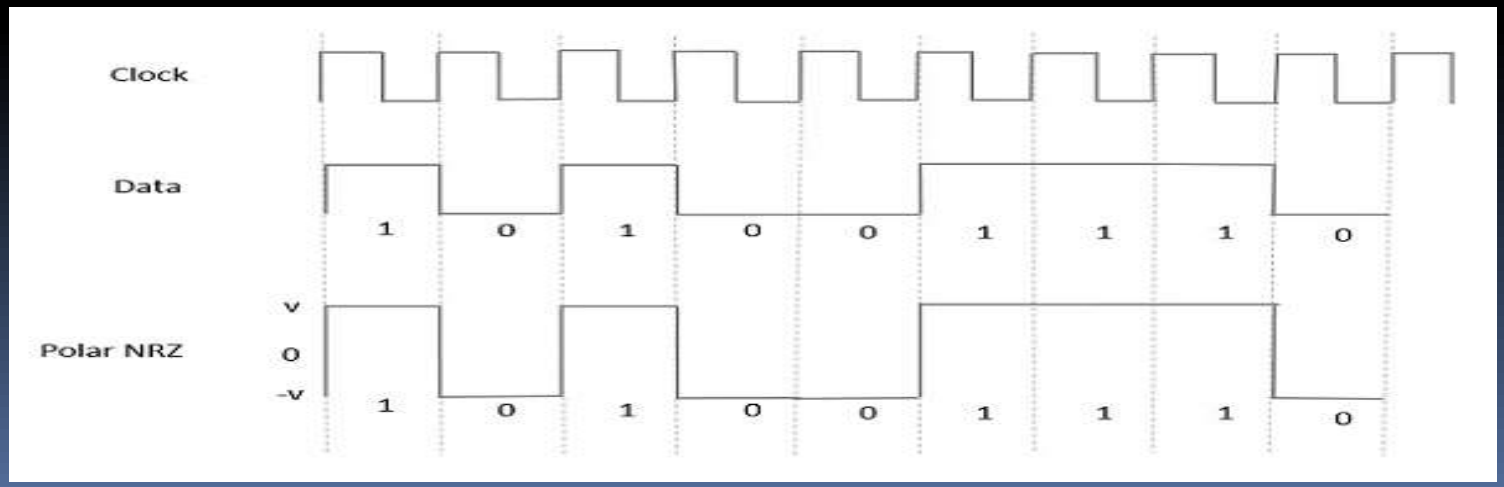
- **Unipolar Non-Return to Zero (NRZ)**
- In this type of unipolar signaling, a High in data is represented by a positive pulse called as **Mark**, which has a duration $T_o$ equal to the symbol bit duration. A Low in data input has no pulse.



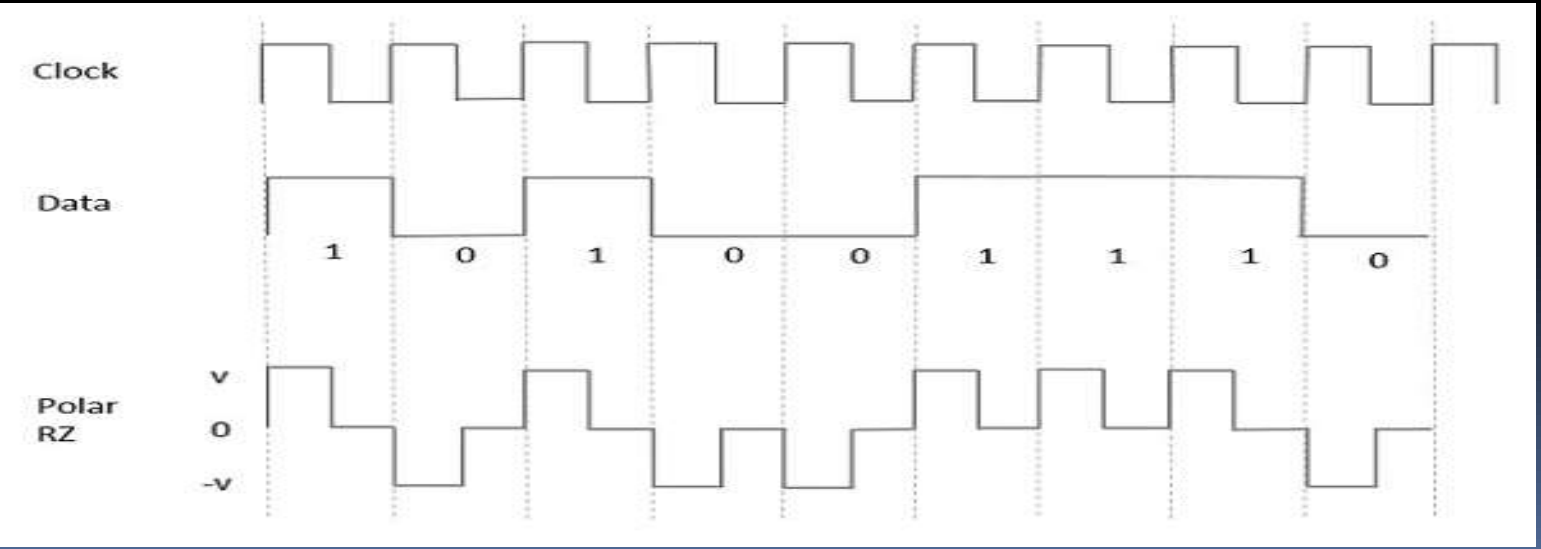
- **Unipolar Return to Zero (RZ)**
- In this type of unipolar signaling, a High in data, though represented by a **Mark pulse**, its duration $T_0$ is less than the symbol bit duration. Half of the bit duration remains high but it immediately returns to zero and shows the absence of pulse during the remaining half of the bit duration.



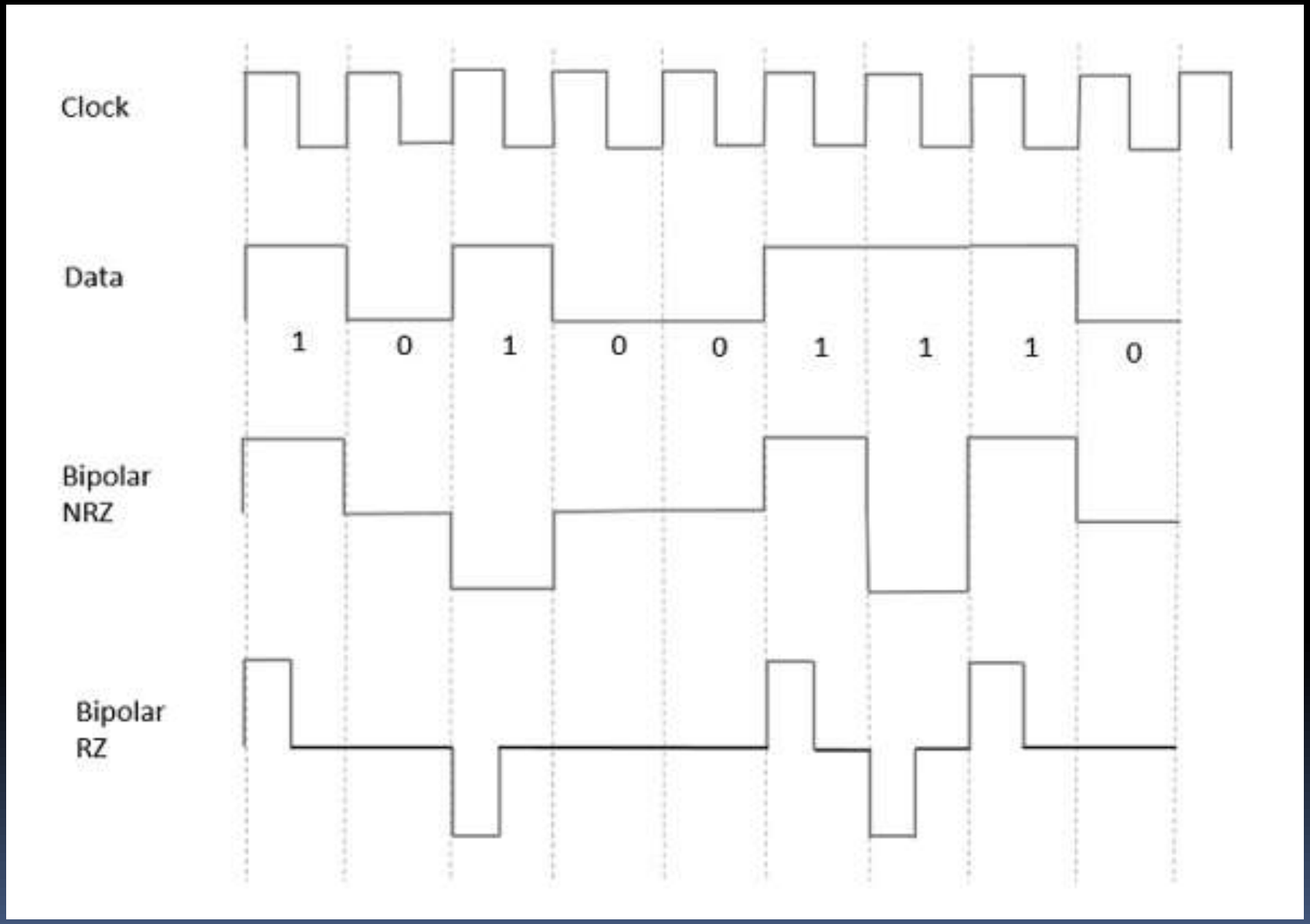
- **Polar Signaling**
- There are two methods of Polar Signaling.
- Polar NRZ
- Polar RZ
- **Polar NRZ**
- In Polar signaling, a High in data is represented by a positive pulse, while a Low in data is represented by a negative pulse.



- **Polar RZ**
- In this type of Polar signaling, a High in data, though represented by a **Mark pulse**, its duration $T_o$ is less than the symbol bit duration. Half of the bit duration remains high but it immediately returns to zero and shows the absence of pulse during the remaining half of the bit duration



- **Bipolar Signaling**
- This is an encoding technique which has three voltage levels namely **+, -** and **o**. Such a signal is called as **duo-binary signal**.
- Even in this method, we have two types.
- Bipolar NRZ
- Bipolar RZ
- From the models so far discussed, we have learnt the difference between NRZ and RZ. It just goes in the same way here too. The following figure clearly depicts this.


Clock
Data
1
0
1
0
0
1
1
1
0
Bipolar
NRZ
Bipolar
RZ

- **Advantages**
- It is simple.
- No low-frequency components are present.
- Occupies low bandwidth than unipolar and polar NRZ schemes.
- This technique is suitable for transmission over AC coupled lines, as signal drooping doesn't occur here.
- A single error detection capability is present in this.
- **Disadvantages**
- Following are the disadvantages –
- No clock is present.
- Long strings of data cause loss of synchronization.

# Classes of Transmission Media

- Conducted or guided media
  - use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver
- Wireless or unguided media
  - use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals

# Guided Transmission Media

- Transmission capacity depends on the distance and on whether the medium is point-to-point or multipoint
- Examples
  - twisted pair wires
  - coaxial cables
  - optical fiber

# Twisted Pair Wires

- Consists of two insulated copper wires arranged in a regular spiral pattern to minimize the electromagnetic interference between adjacent pairs
- Often used at customer facilities and also over distances to carry voice as well as data communications
- Low frequency transmission medium

# Types of Twisted Pair

- STP (shielded twisted pair)
  - the pair is wrapped with metallic foil or braid to insulate the pair from electromagnetic interference
- UTP (unshielded twisted pair)
  - each wire is insulated with plastic wrap, but the pair is encased in an outer covering

# Ratings of Twisted Pair

- Category 3 UTP
  - data rates of up to 16mbps are achievable
- Category 5 UTP
  - data rates of up to 100mbps are achievable
  - more tightly twisted than Category 3 cables
  - more expensive, but better performance
- STP
  - More expensive, harder to work with

# Twisted Pair Advantages

- Inexpensive and readily available
- Flexible and light weight
- Easy to work with and install

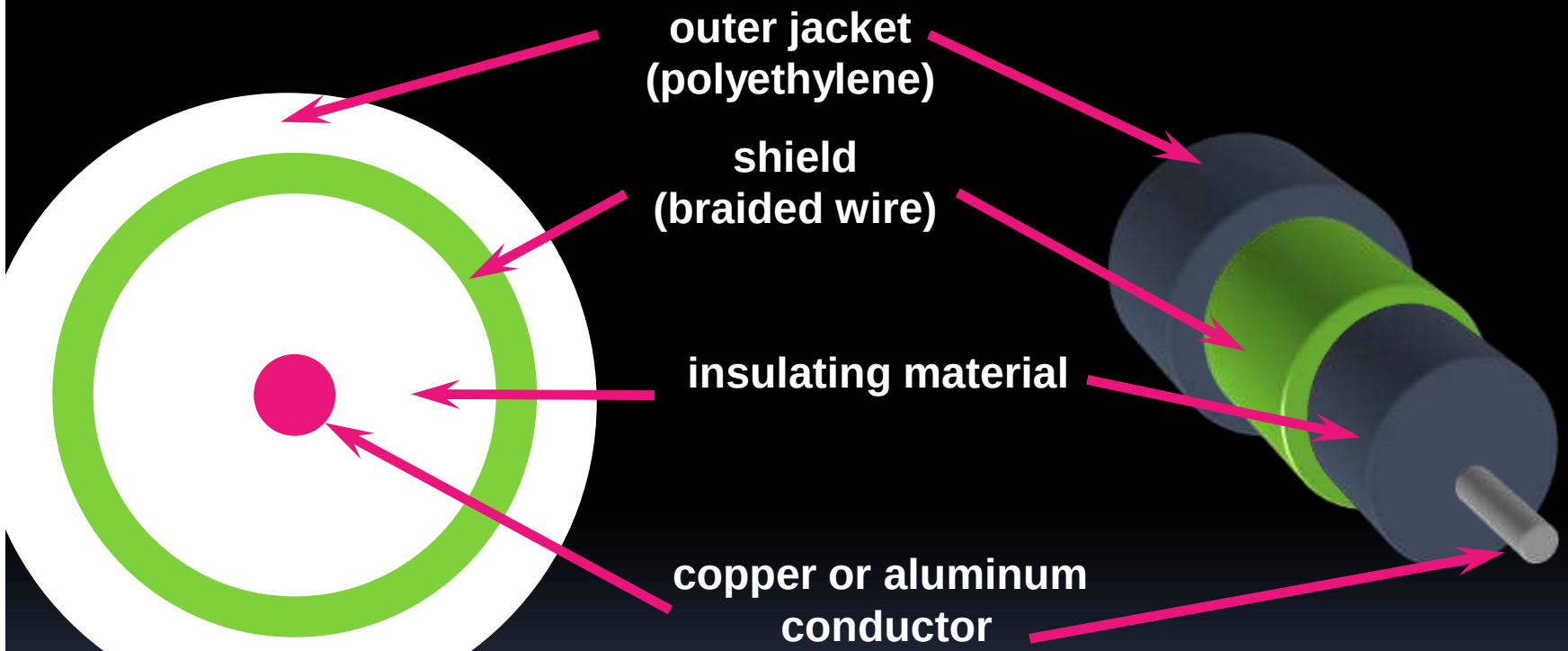
# Twisted Pair Disadvantages

- Susceptibility to interference and noise
- Attenuation problem
  - For analog, repeaters needed every 5-6km
  - For digital, repeaters needed every 2-3km
- Relatively low bandwidth (3000Hz)

# Coaxial Cable (or Coax)

- Used for cable television, LANs, telephony
- Has an inner conductor surrounded by a braided mesh
- Both conductors share a common center axial, hence the term “co-axial”

# Coax Layers


outer jacket
(polyethylene)
shield
(braided wire)
insulating material
copper or aluminum
conductor

# Coax Advantages

- Higher bandwidth
  - 400 to 600Mhz
  - up to 10,800 voice conversations
- Can be tapped easily (pros and cons)
- Much less susceptible to interference than twisted pair

## Coax Disadvantages:

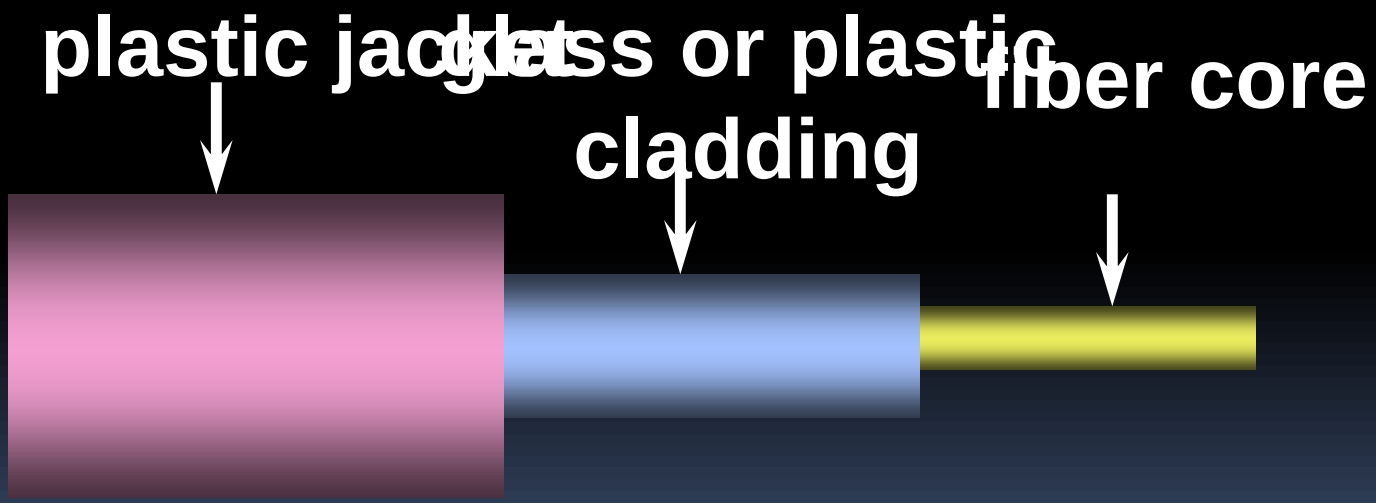
- High attenuation rate makes it expensive over long distance
- Bulky

# Fiber Optic Cable

- Relatively new transmission medium used by telephone companies in place of long-distance trunk lines
- Also used by private companies in implementing local data communications networks
- Require a light source with injection laser diode (ILD) or light-emitting diodes (LED)

# Fiber Optic Layers

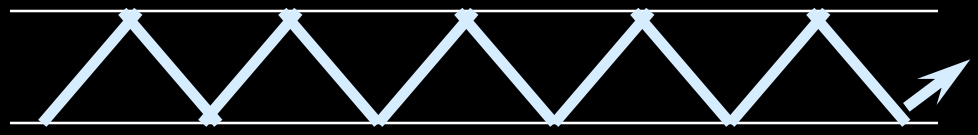
- consists of three concentric sections



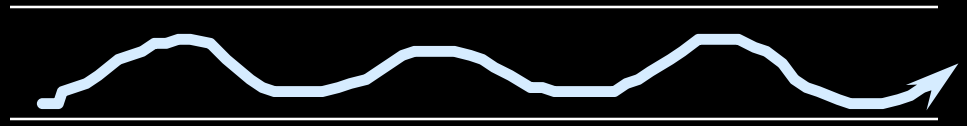
# Fiber Optic Types

- multimode step-index fiber
  - the reflective walls of the fiber move the light pulses to the receiver
- multimode graded-index fiber
  - acts to refract the light toward the center of the fiber by variations in the density
- single mode fiber
  - the light is guided down the center of an extremely narrow core

# Fiber Optic Signals



**fiber optic multimode step-index**



**fiber optic multimode graded-index**

**fiber optic single mode**

# Fiber Optic Advantages

- greater capacity (bandwidth of up to 2 Gbps)
- smaller size and lighter weight
- lower attenuation
- immunity to environmental interference
- highly secure due to tap difficulty and lack of signal radiation

# Fiber Optic Disadvantages

- expensive over short distance
- requires highly skilled installers
- adding additional nodes is difficult

# Wireless (Unguided Media) Transmission

- transmission and reception are achieved by means of an antenna
- directional
  - transmitting antenna puts out focused beam
  - transmitter and receiver must be aligned
- omnidirectional
  - signal spreads out in all directions
  - can be received by many antennas

# Wireless Examples

- terrestrial microwave
- satellite microwave
- broadcast radio
- infrared

# Terrestrial Microwave

- used for long-distance telephone service
- uses radio frequency spectrum, from 2 to 40 Ghz
- parabolic dish transmitter, mounted high
- used by common carriers as well as private networks
- requires unobstructed line of sight between source and receiver
- curvature of the earth requires stations (repeaters) ~30 miles apart

# Terrestrial Microwave Applications

- Television distribution
- Long-distance telephone transmission
- Private business networks

# Microwave Transmission Disadvantages

- line of sight requirement
- expensive towers and repeaters
- subject to interference such as passing airplanes and rain

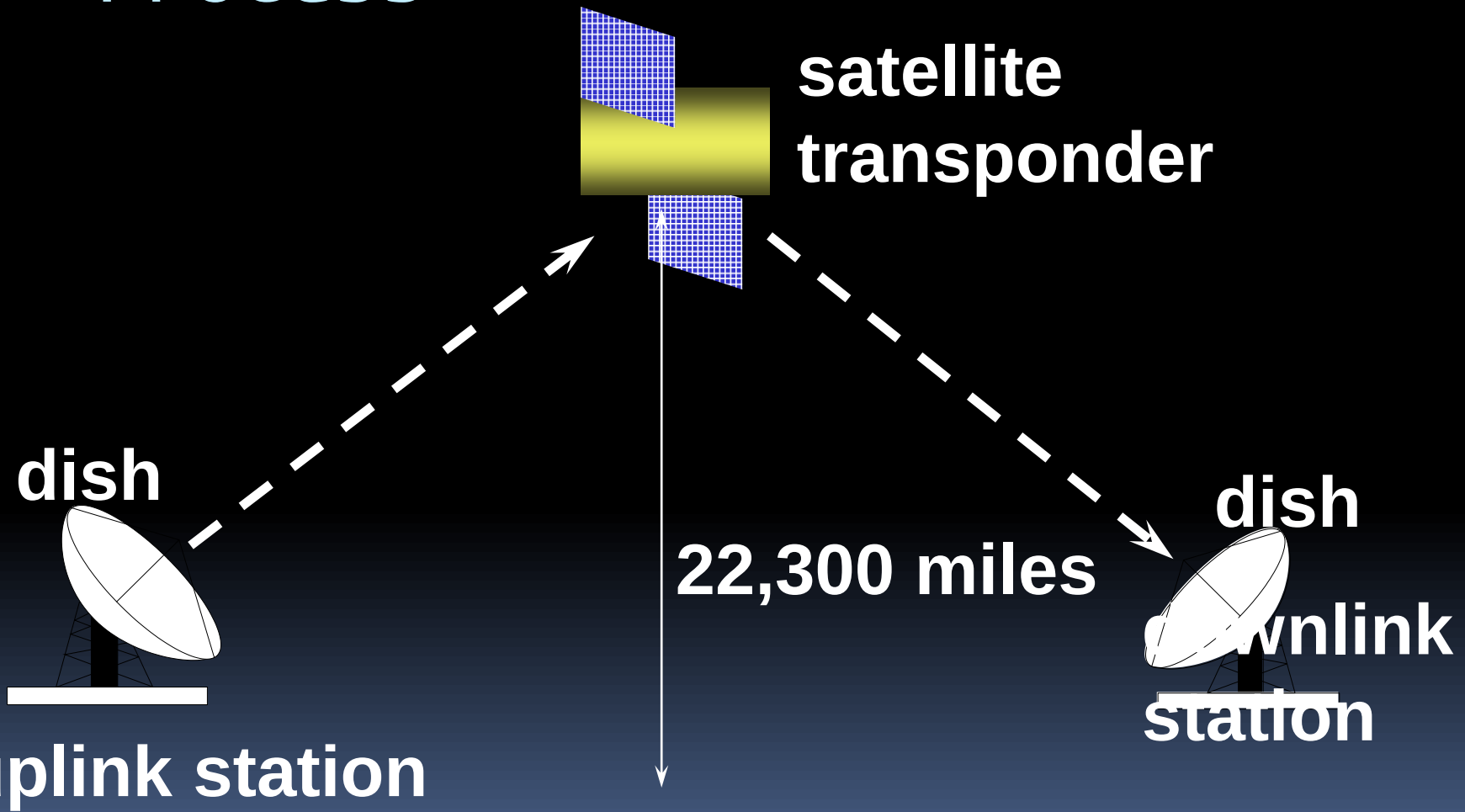
# Satellite Microwave Transmission

- a microwave relay station in space
- can relay signals over long distances
- geostationary satellites
  - remain above the equator at a height of 22,300 miles (geosynchronous orbit)
  - travel around the earth in exactly the time the earth takes to rotate

# Satellite Transmission Links

- earth stations communicate by sending signals to the satellite on an uplink
- the satellite then repeats those signals on a downlink
- the broadcast nature of the downlink makes it attractive for services such as the distribution of television programming

# Satellite Transmission Process



# Satellite Transmission Applications

- television distribution
  - a network provides programming from a central location
  - direct broadcast satellite (DBS)
- long-distance telephone transmission
  - high-usage international trunks
- private business networks

# Principal Satellite Transmission Bands

- C band: 4(downlink) - 6(uplink) GHz
  - the first to be designated
- Ku band: 12(downlink) -14(uplink) GHz
  - rain interference is the major problem
- Ka band: 19(downlink) - 29(uplink) GHz
  - equipment needed to use the band is still very expensive

# Fiber vs Satellite

**Table 7.6** A Comparison of Optical Fiber and Satellite Transmission

| Characteritic | Optical Fiber | Satellite |
|---|---|---|
| Bandwidth | Theoretical limit of 1 terahertz; currently 1–10 GHz | Typical transponder has a bandwidth of 36–72 MHz |
| Immunity to interference | Immune to electromagnetic interference | Subject to interference from various sources, including microwave |
| Security | Difficult to tap without detection | Signals must be encrypted for security |
| Multipoint capability | Primarily a point-to-point medium | Point-to-multipoint communications easily implemented |
| Flexibility | Difficult to reconfigure to meet changing demand | Easy to reconfigure |
| Connectivity to customer site | Local loop required | With antenna installed on customer premises, local loop not required |

# Radio

- radio is omnidirectional and microwave  is directional
- Radio is a general term often used to encompass frequencies in the range 3 kHz to 300 GHz.
- Mobile telephony occupies several frequency bands just under 1 GHz.

# Infrared

- Uses transmitters/receivers (transceivers) that modulate noncoherent infrared light.
- Transceivers must be within line of sight of each other (directly or via reflection ).
- Unlike microwaves, infrared does not penetrate walls.

# UNIT-2

# SWITCHING

# Switching:

- Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. At broad level, switching can be divided into two major categories:
- **Connectionless:** The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- **Connection Oriented:** Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both endpoints. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

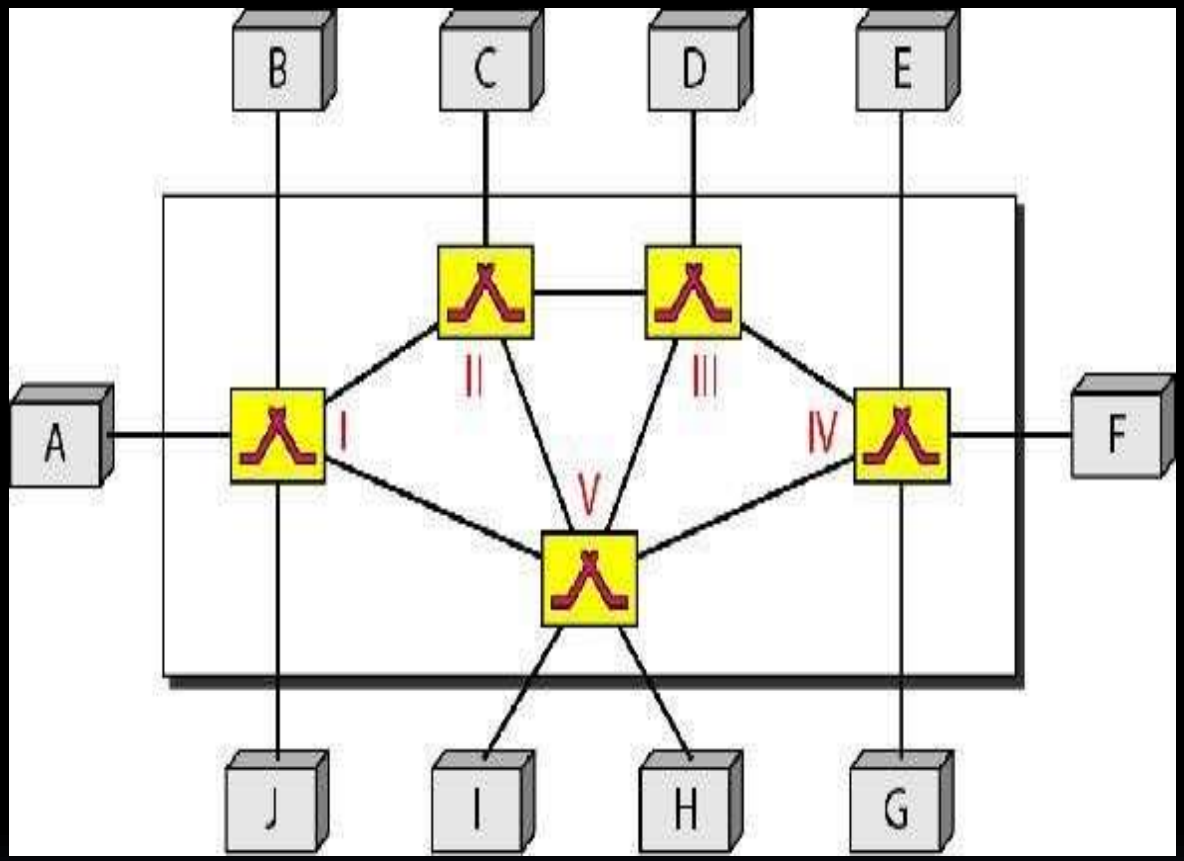
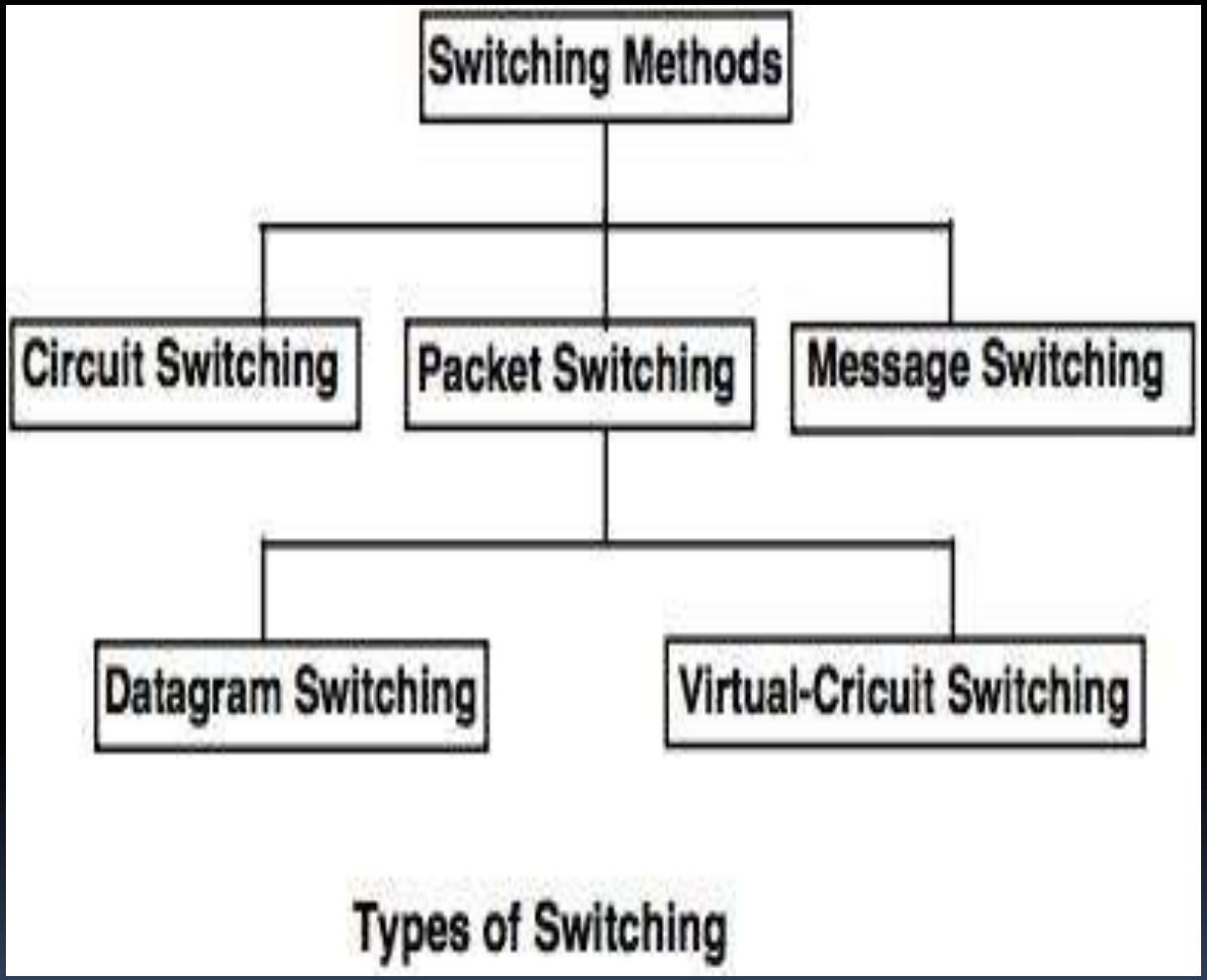



**Fig 2.1 Switching Network**




Types of Switching

## 1.CircuitSwitching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.

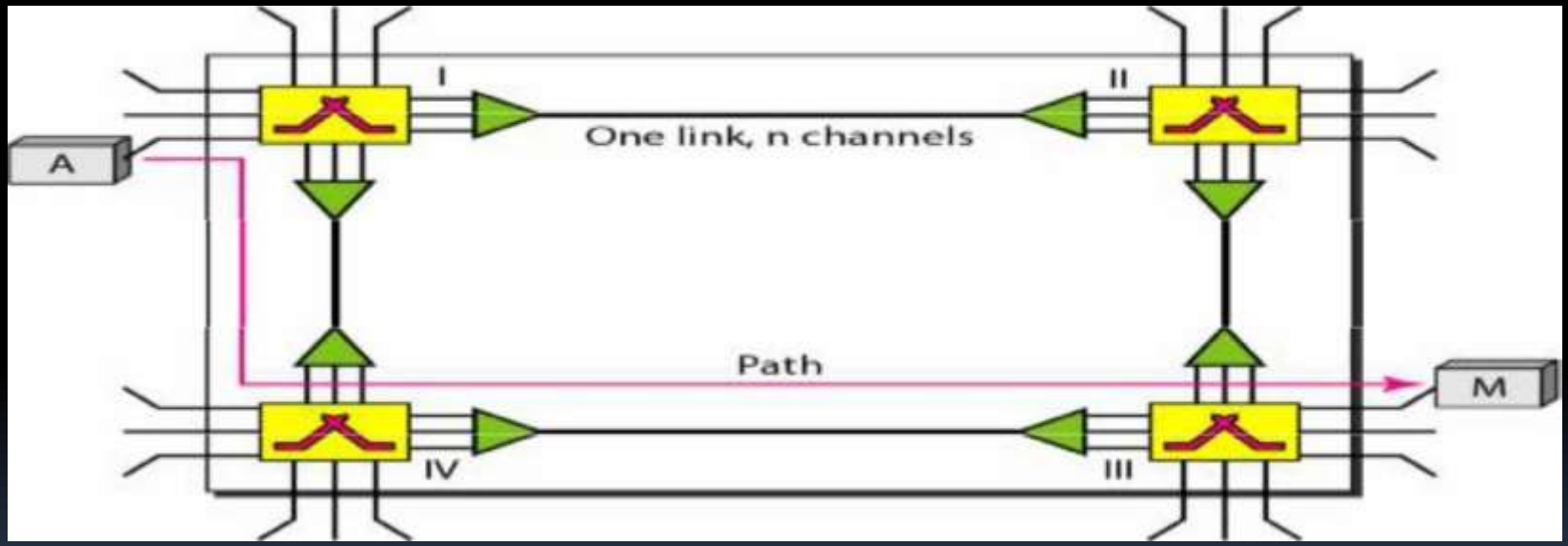



**Fig 2.2 Circuit Switching**

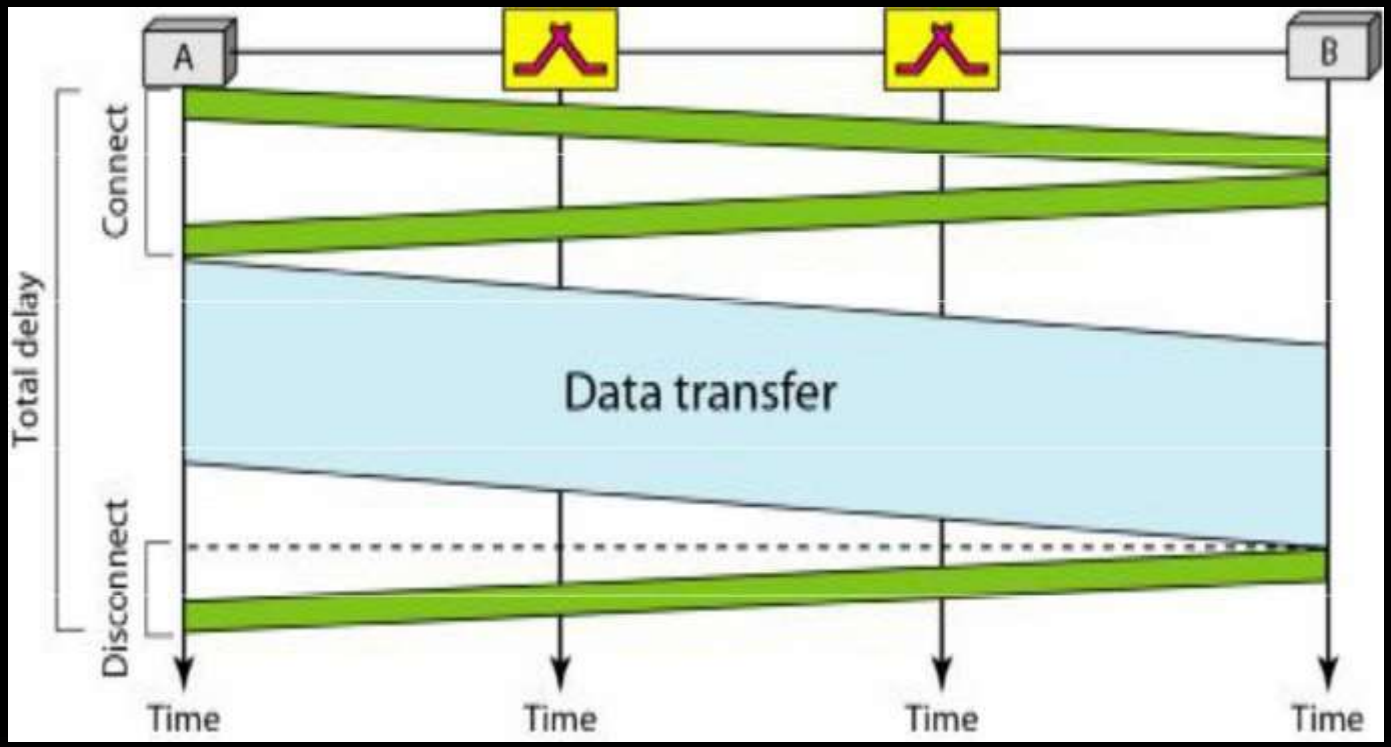



**Fig 2.3 Delay in Circuit Switching**

# PACKET SWITCHING

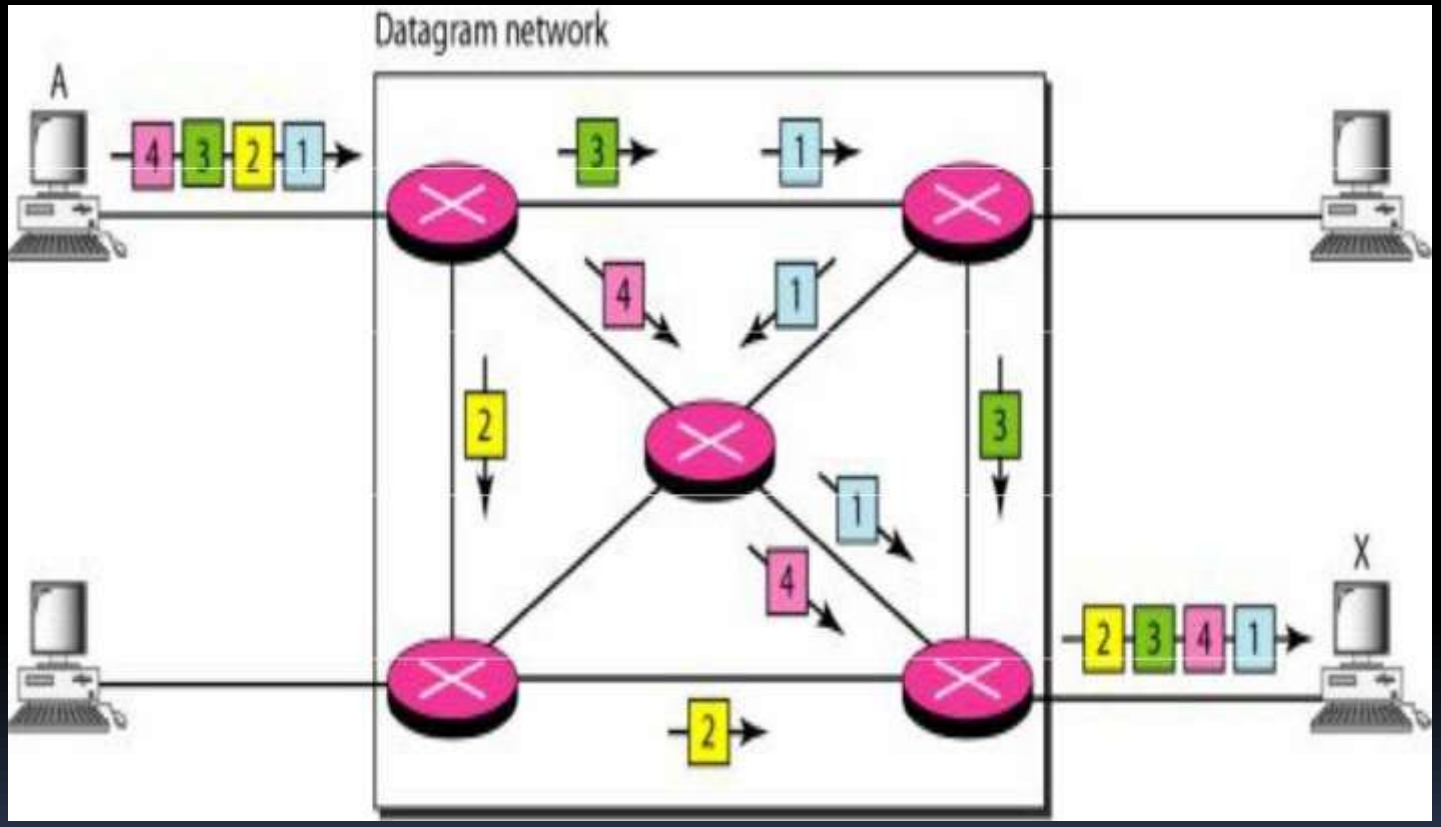
In packet Switching, flow of data is not continuous rather it flows in the form of packets. The size of the packet is determined by the network and the governing protocol. This type of switching further classify into datagram networks and virtual circuit networks.

## 1. Datagram Networks

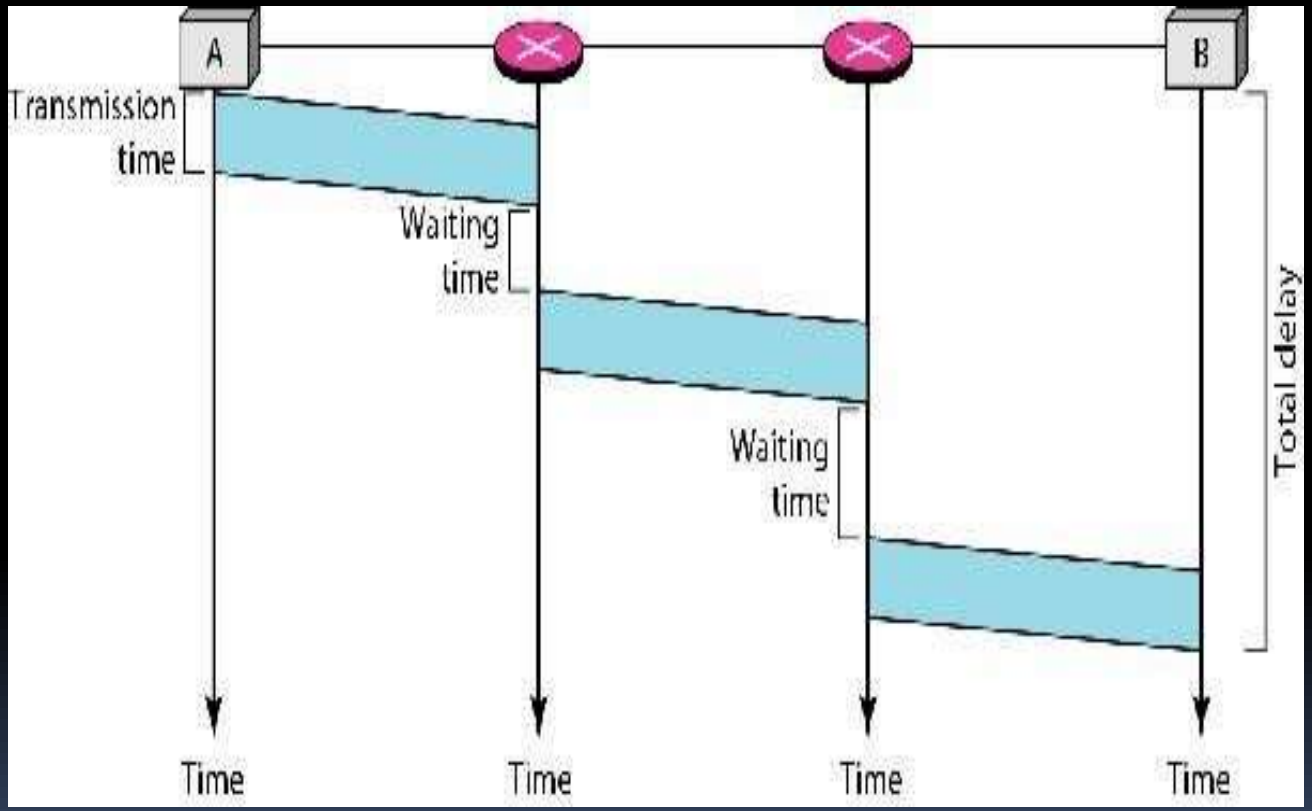
Data are transmitted in discrete units called packets. Size of the packet depends on the protocol and network. Packets switched networks are connectionless, hence no resource allocation. Connectionless means the switch does not keep information about the connection state. Datagram switching is done at network layer

A switch in a datagram network uses a routing table that is based on the destination address. The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet. The total delay is shown in Fig

# Datagram Networks



# Delay in Datagram Networks



## 2. Virtual Circuit Networks

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. The virtual -circuit shares characteristics of both. Packets form a single message travel along the same path. Following are the characteristics of virtual circuit networks:

- Three phases to transfer data
- Resources can be allocated during setup phase
- Data are packetized and each packet carries an address in the header
- All packets follow the same path
- Implemented in data link layer

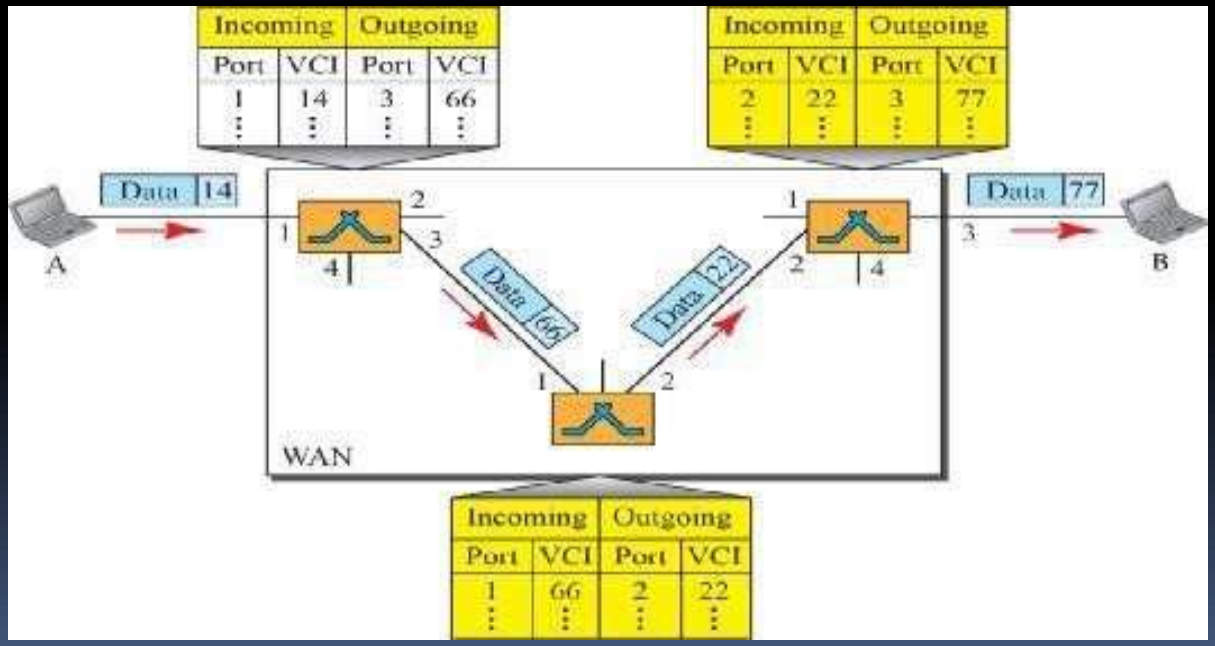



**fig :Virtual Circuit Identifier**

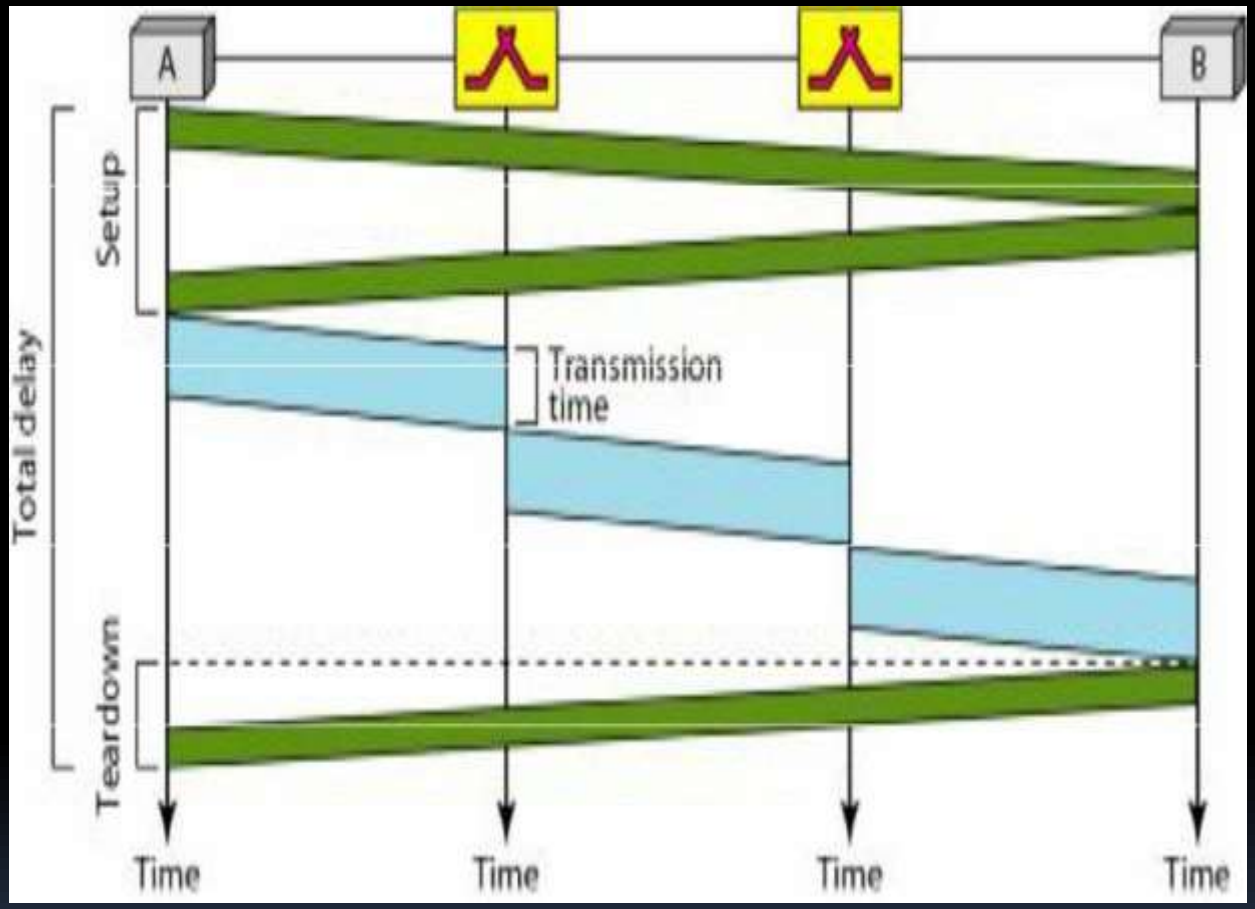



**Fig : Delay in Virtual Circuit Identifier**

# Structure of a Switch

We use switches in circuit-switched and packet-switched networks. There are two structures of a switch named as space division switch and time division switch.

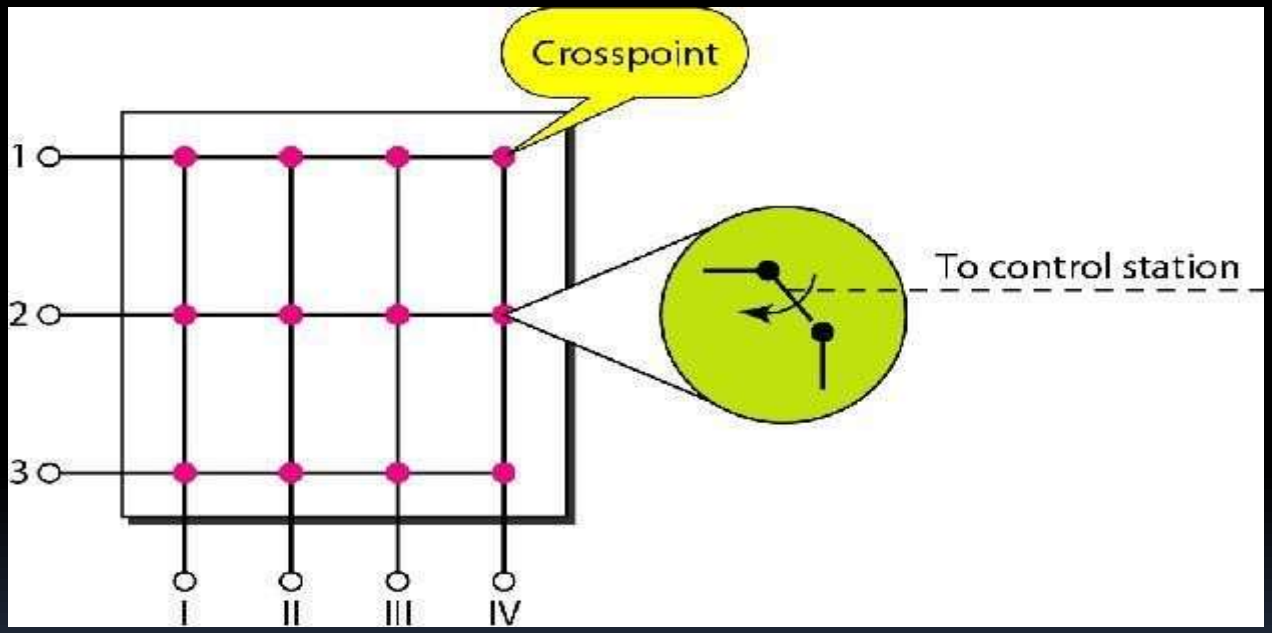



**Fig : Space Division Switching: Crossbar Switch**

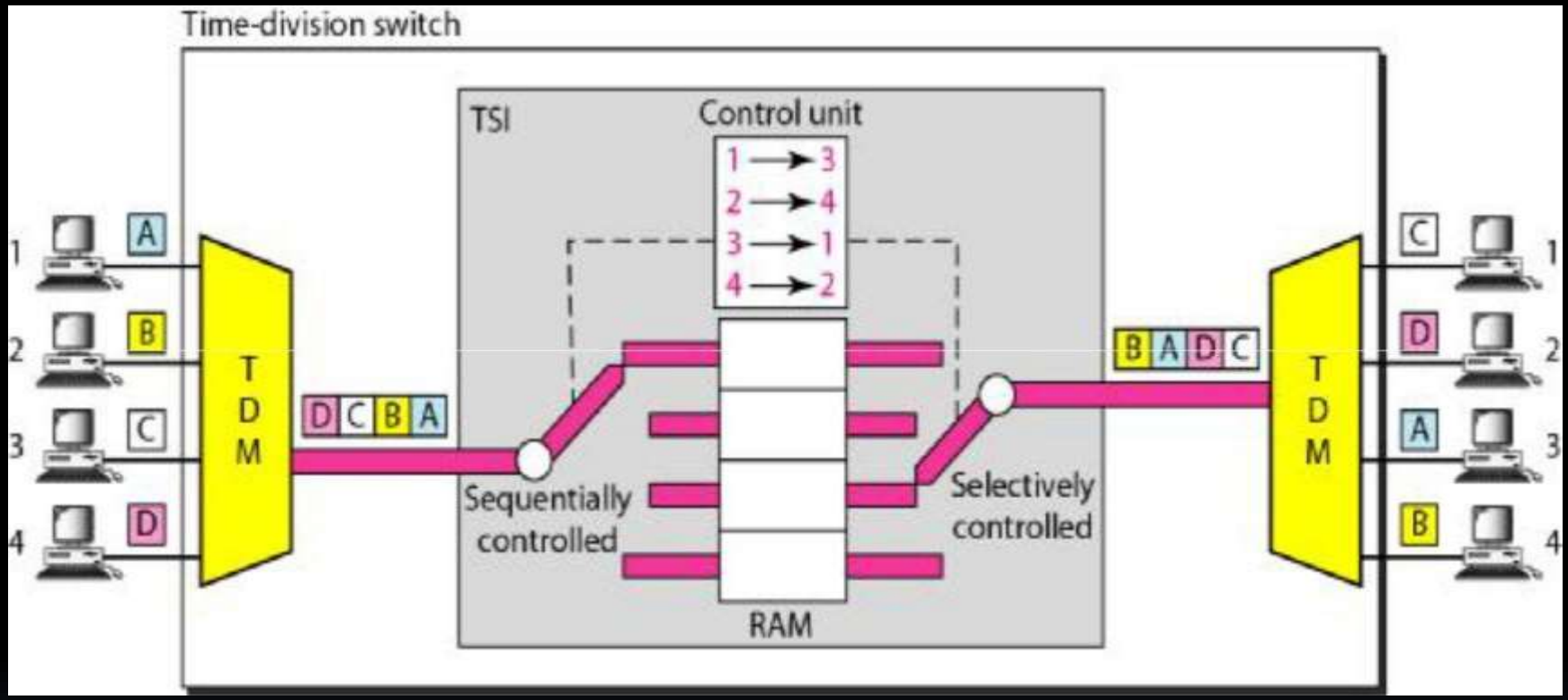
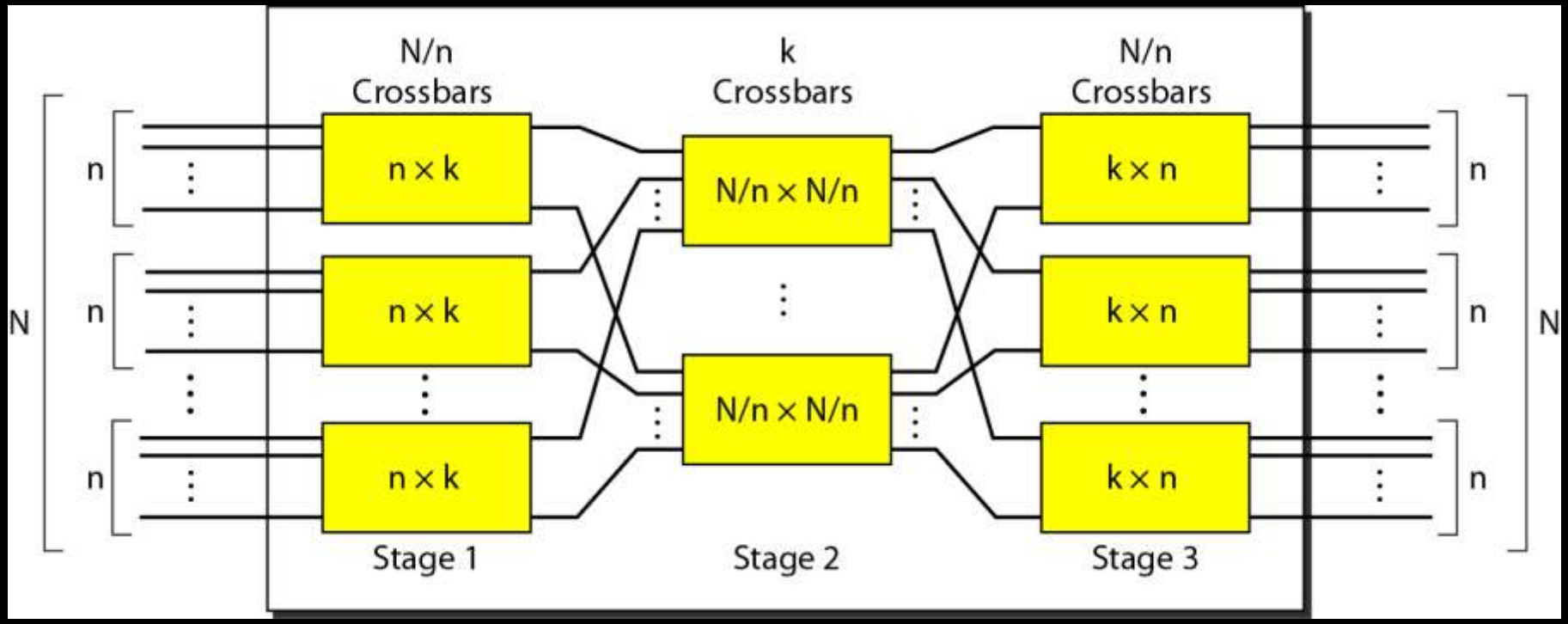



**Fig : Time Division Switching**

# Multistage switch



# Ethernet Physical Layer

Telephone networks use circuit switching. The telephone network had its beginnings in the late 1800s. The entire network, which is referred to as the plain old telephone system (POTS), was originally an analog system using analog signals to transmit voice. There are three major components of telephone system namely local loops, trunks and switching offices as shown in Fig

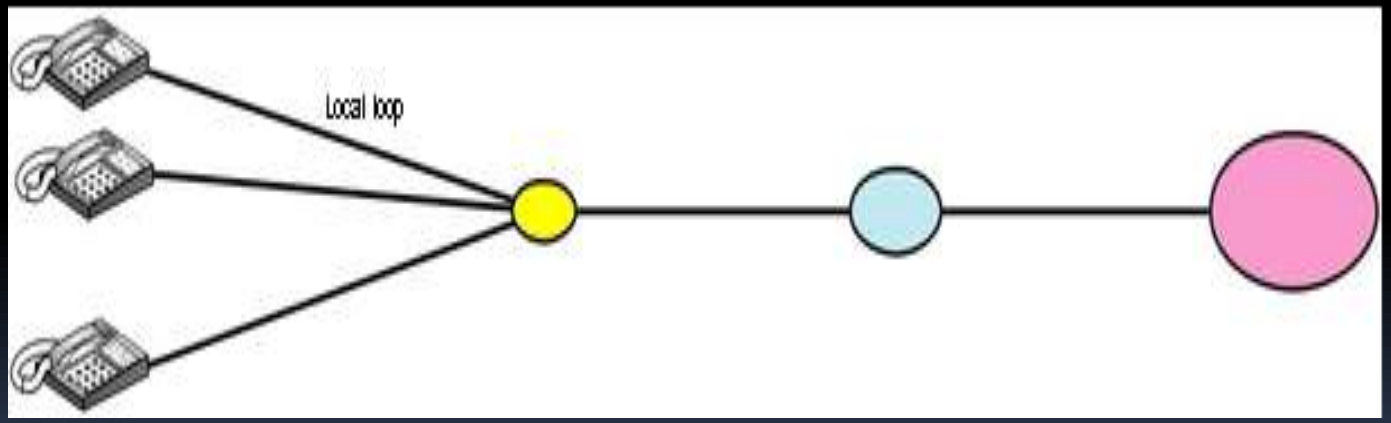



**Fig:** Telephone Network

**Signalling** can be defined as the information exchange concerning the establishment and control of a telecommunication circuit and the management of the network.

- There are two types: In- Band and Out-Band. In in-band signaling, the same circuit can be used for both signaling and voice communication.
- In out-of-band signaling, a portion of the voice channel bandwidth was used for signaling; the voice bandwidth and the signaling bandwidth were separate.
- The signaling system was required to perform other tasks such as: providing dial tone, ring tone, and busy tone, transferring telephone numbers between offices, and providing other functions such as caller ID, voice mail etc.
- These complex tasks resulted in the provision of a separate network for signaling.
- This means that a telephone network today can be thought of as two networks: a signaling network and a data transfer network.

The protocol that is used in signaling network is SS7 (Signaling System Seven) as shown in Fig

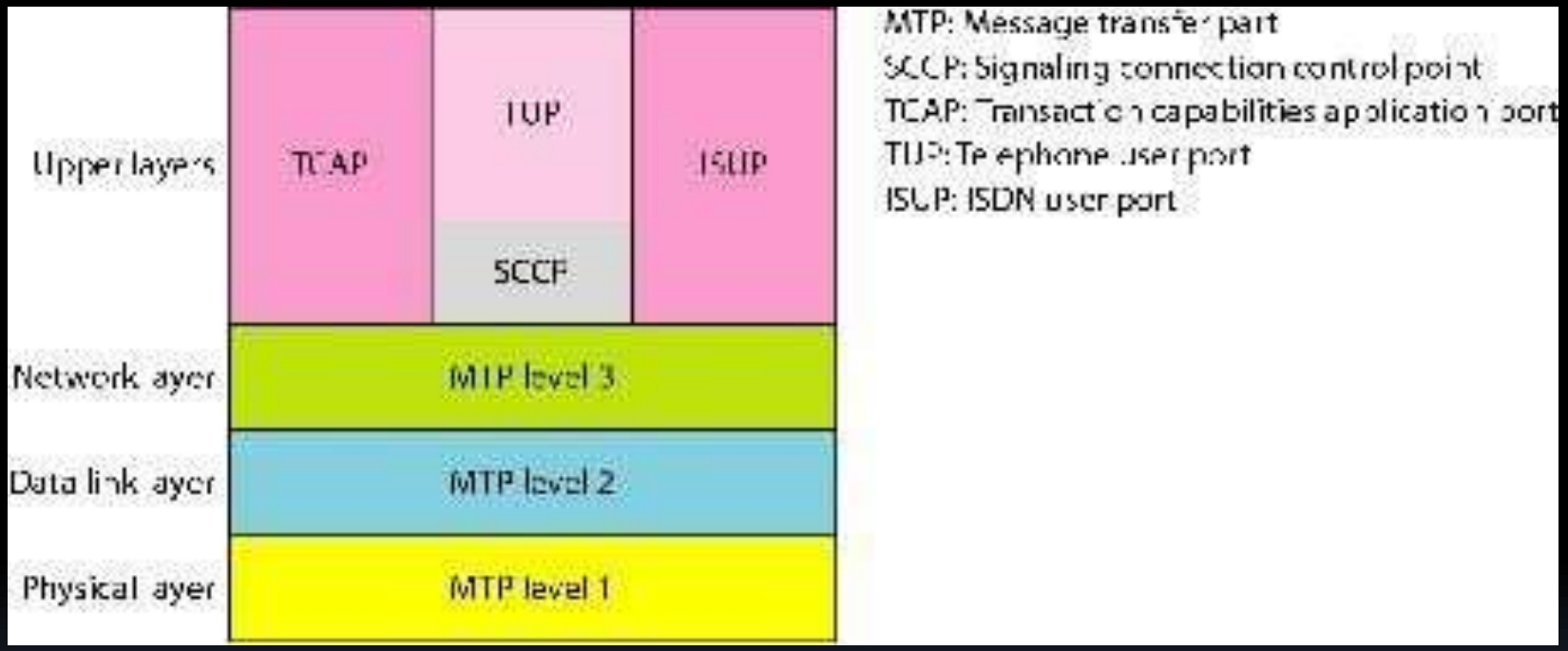



**Fig:** SS7 (Signaling System Seven)

# HDLC

High-level Data Link Control (HDLC) is a bit-oriented protocol for communication over point- to-point and multipoint links. It implements the ARQ mechanisms. HDLC provides two common transfer modes that can be used in different configurations: normal response mode (NRM) and asynchronous balanced mode (ABM).

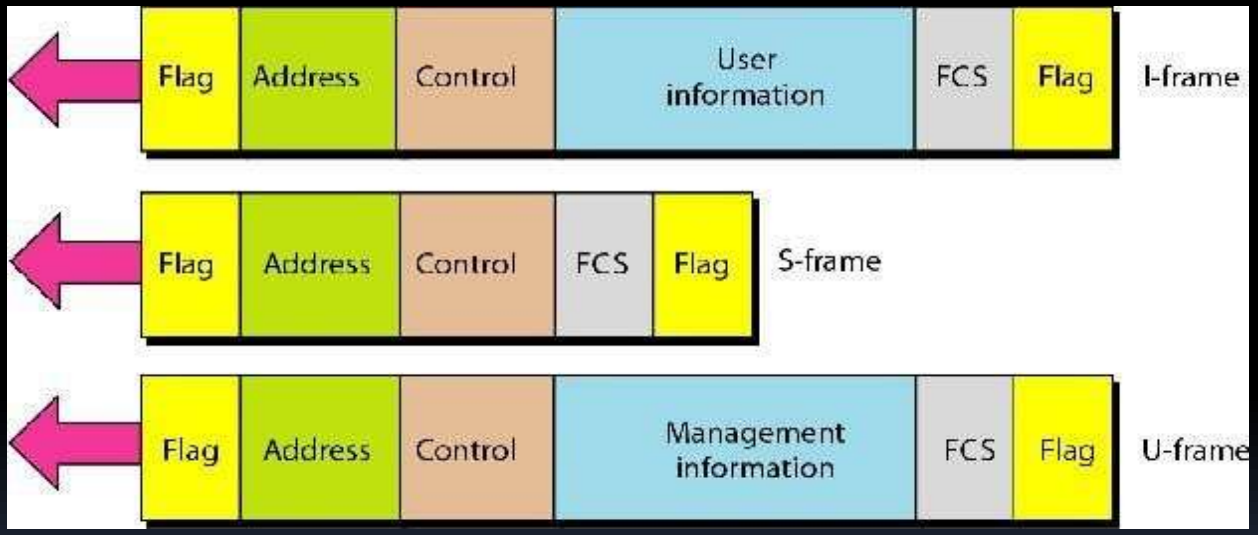



**Fig :** HDLC Frames

In normal response mode (NRM), the station configuration is unbalanced. We have one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond. The NRM is used for both point-to-point and multiple-point links as shown in Fig

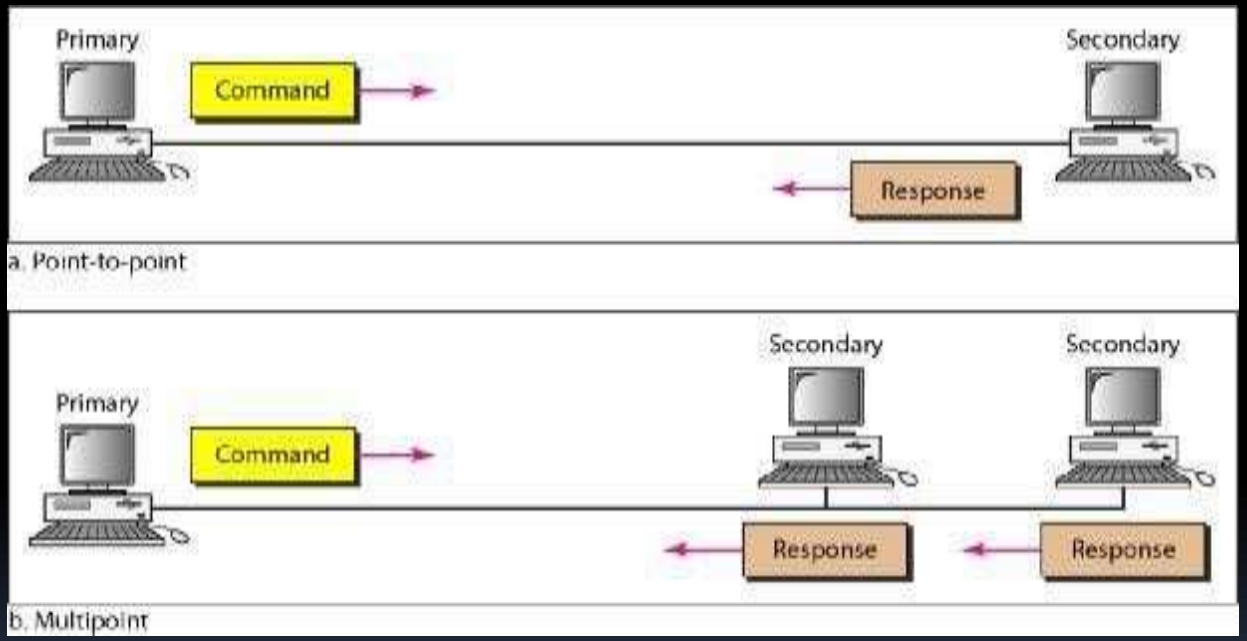



**Fig :** Normal Response Mode

In asynchronous balanced mode (ABM), the configuration is balanced. The link is point-to-point, and each station can function as a primary and a secondary as shown in Fig

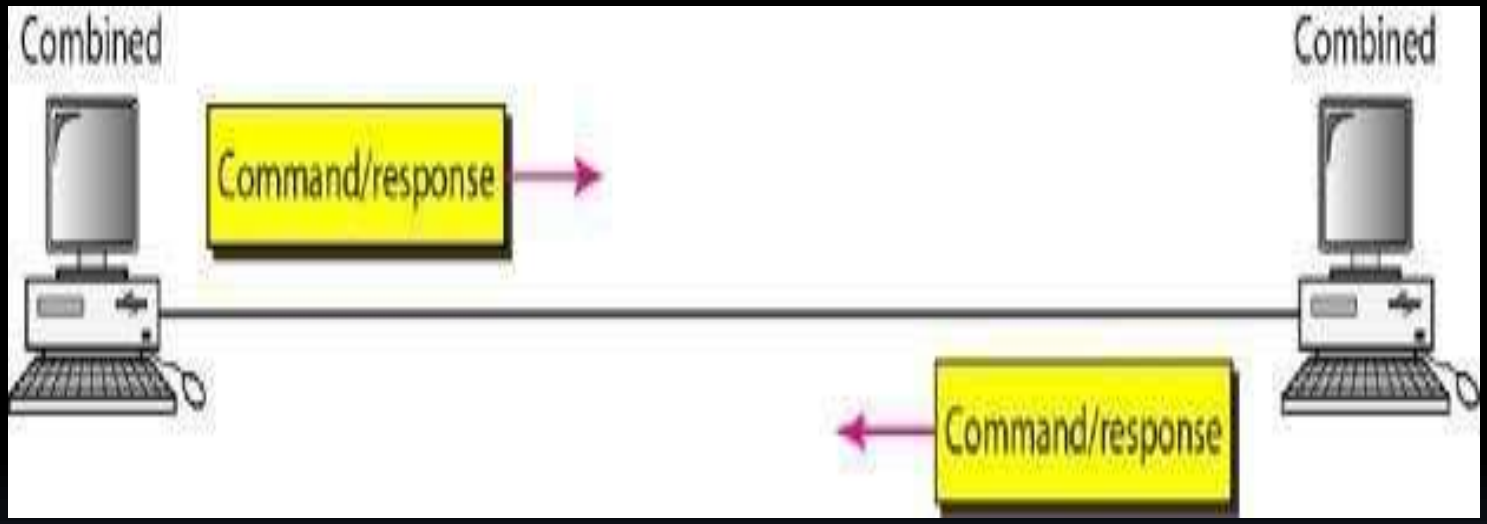



**Fig :** Asynchronous Balance Mode

# DATA LINK LAYER

Data can be corrupted during transmission. Some applications require that errors be detected and corrected. Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. Thus, we say that error had occurred. There are two types of error: single-bit error and burst error. In a single-bit error, only 1 bit in the data unit has changed whereas, in burst error means that 2 or more bits in the data unit have changed as shown in Fig

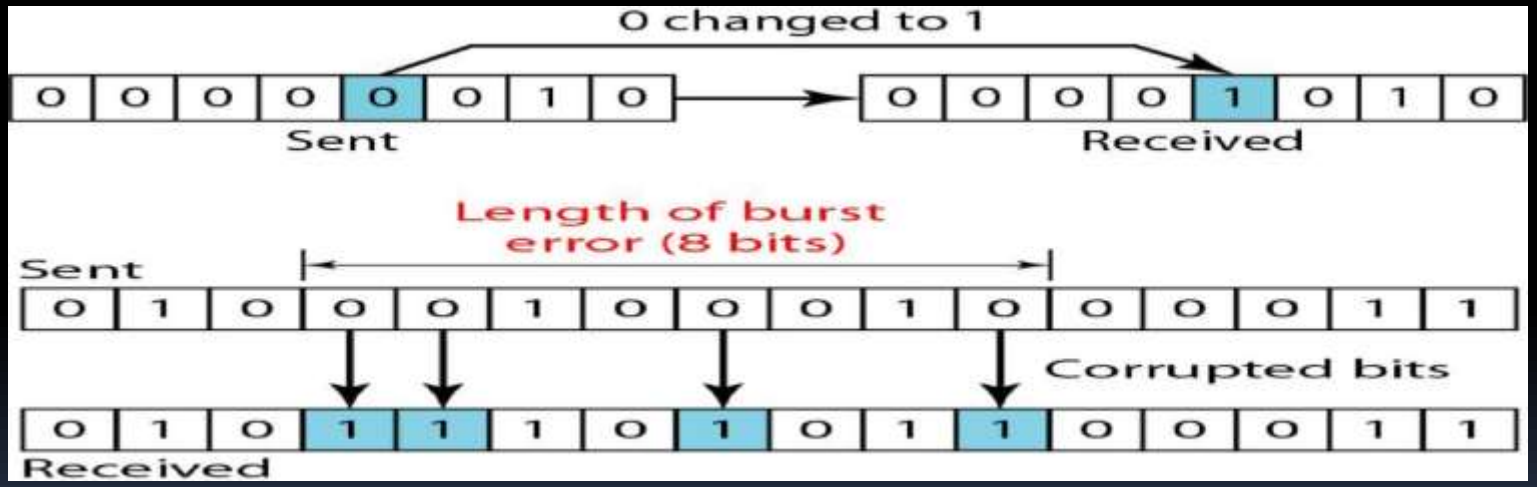



**Fig:** Single-bit and Burst Error

❖The central concept in detecting or correcting errors is redundancy.

❖ To be able to detect or correct errors, we need to send some extra bits with our data.

❖These redundant bits are added by the sender and removed by the receiver.

❖Their presence allows the receiver to detect or correct corrupted bits. Redundancy is achieved through various coding schemes.

❖The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits.

❖The receiver checks the relationships between the two sets of bits to detect or correct the errors.

❖Coding schemes into two broad categories: block coding and convolution coding.

## Block Coding:

In block coding, we divide our message into blocks, each of k bits, called datawords. We add r redundant bits to each block to make the length n = k + r. The resulting n- bit blocks are called codewords as shown in Fig

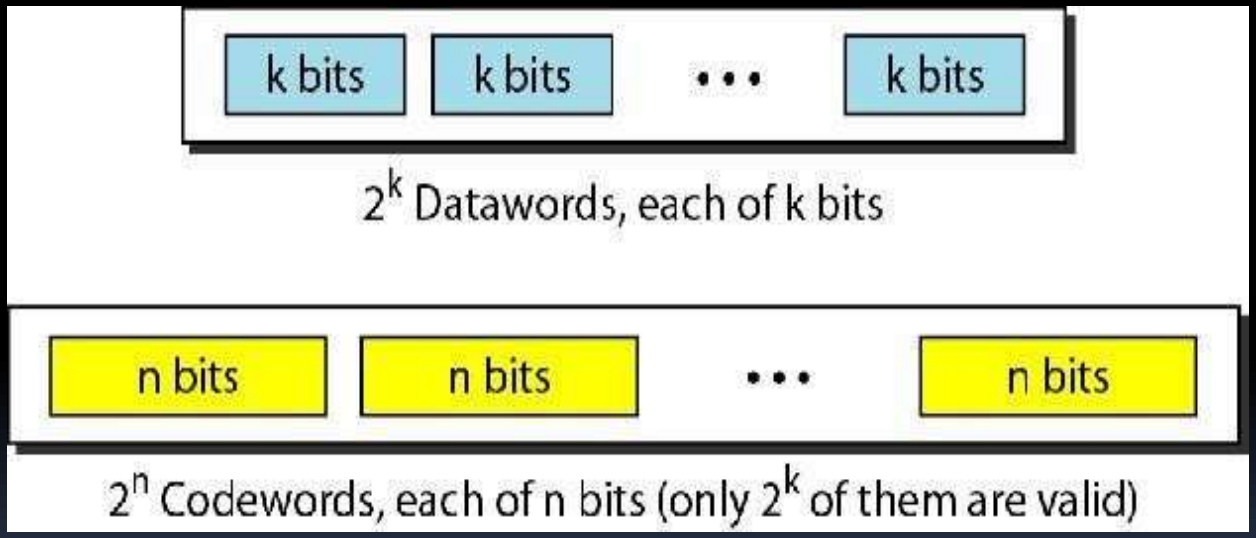



**Fig :** Datawords and Codewords

# Error Detection

An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected. Fig below shows the process of error detection in block coding.

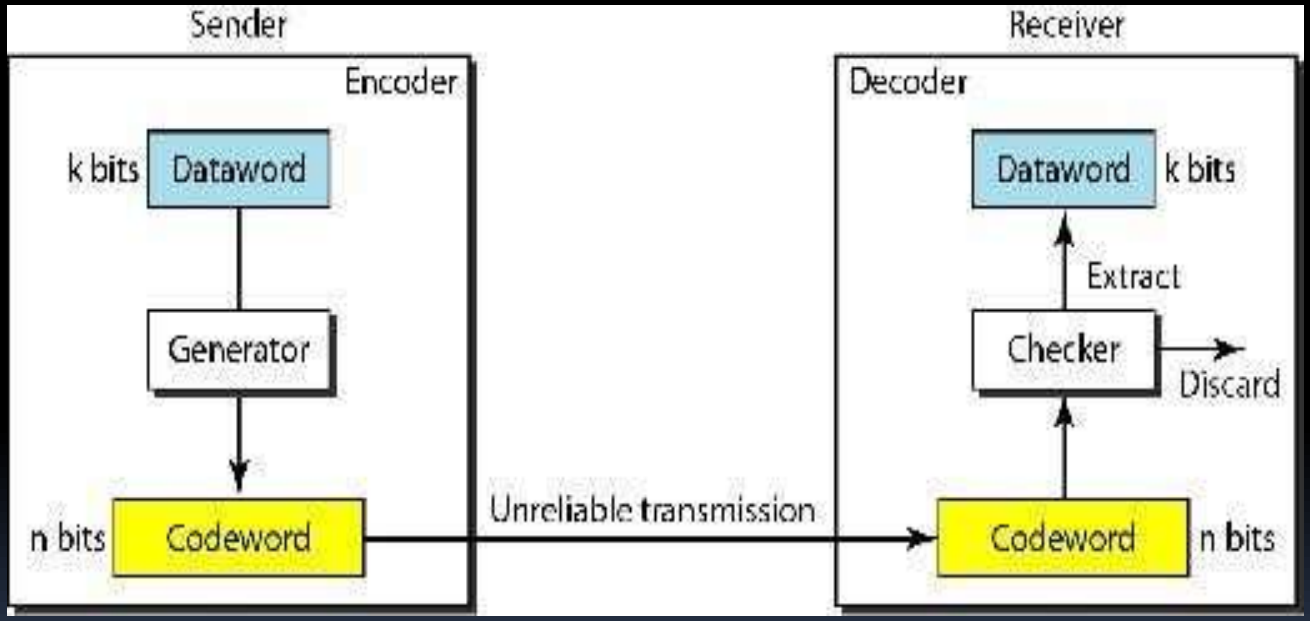



**Fig :** Process of Error Detection

# Error Correction

Once an error has been detected, it has to be corrected. Fig below shows the process of error correction.

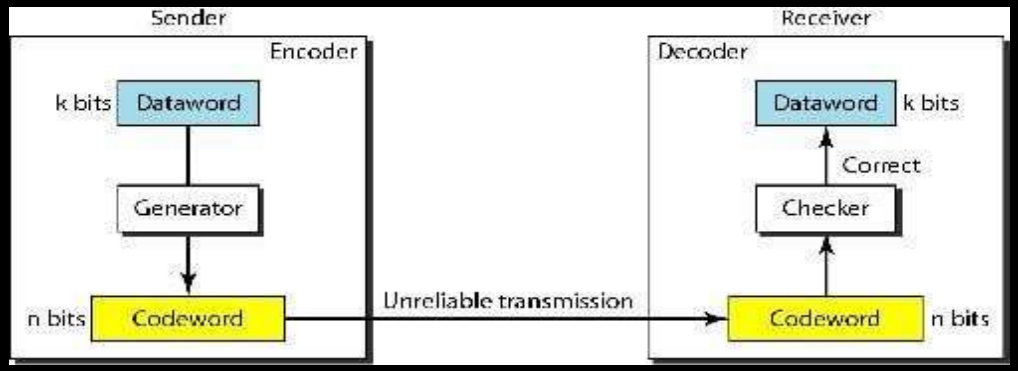



**Fig :** process of Error Correction

One of the central concepts in coding for error control is the idea of the Hamming Distance. The Hamming distance between two words is the number of differences between corresponding bits. The minimum Hamming distance is the smallest Hamming distance between all possible pairs in a set of words.

- To guarantee the detection of up to s errors in all cases, the minimum Hamming distance in a block code must be dmin = s + 1.
- To guarantee correction of up to t errors in all cases, the minimum Hamming distance in a block code must be dmin = 2t + 1.

# Linear Block Codes:

Almost all block codes used today belong to a subset called linear block codes. A linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword. A single parity-check code is of linear block code. A simple parity-check code is a single-bit error-detecting code in which n = k + 1 with dmin = 2. A simple parity-check code can detect an odd number of errors as shown in Fig

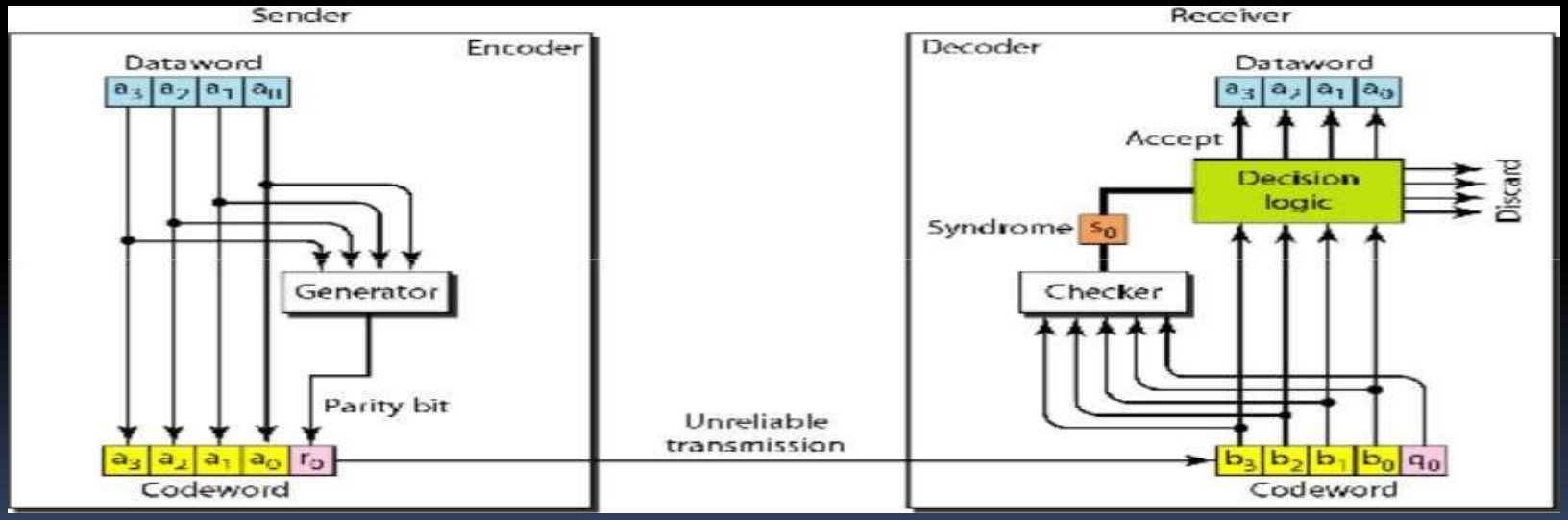



**Fig :** Single Parity Check Code

# Cyclic Codes:

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword as shown in Fig

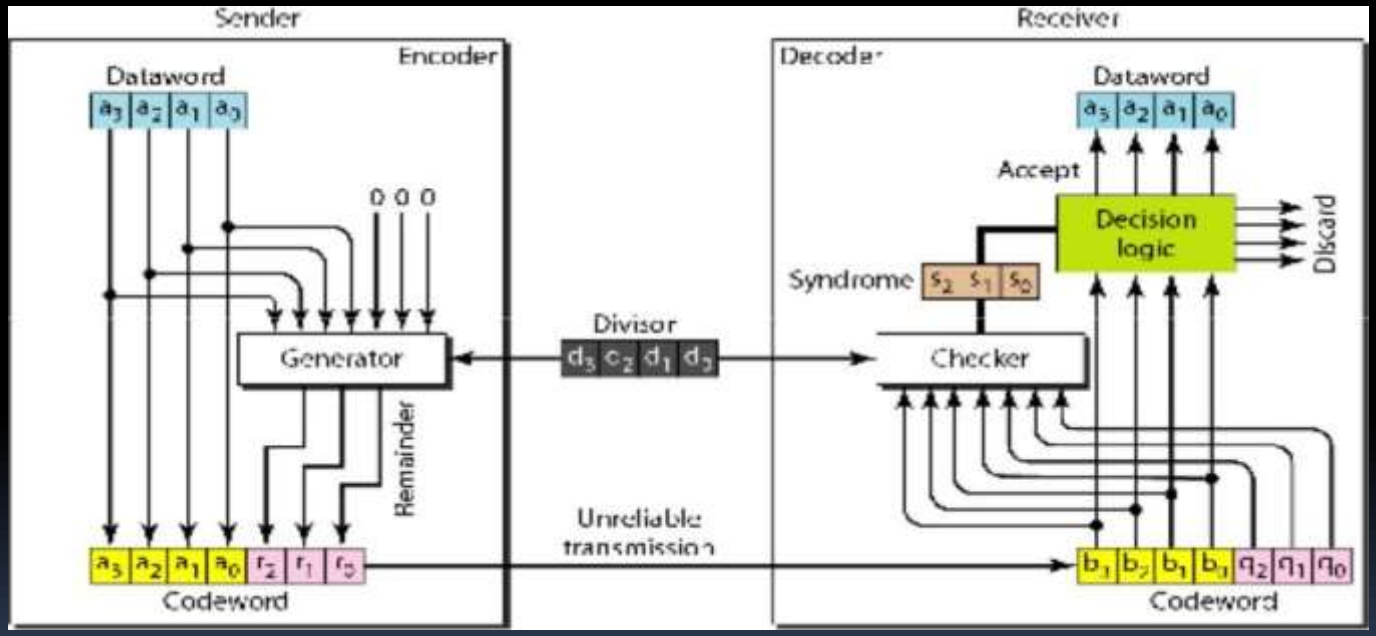



**Fig:** Cyclic Code

In cyclic code, concept of long division has been used. The divisor in a cyclic code is normally called the generator polynomial or simply the generator as shown in Fig

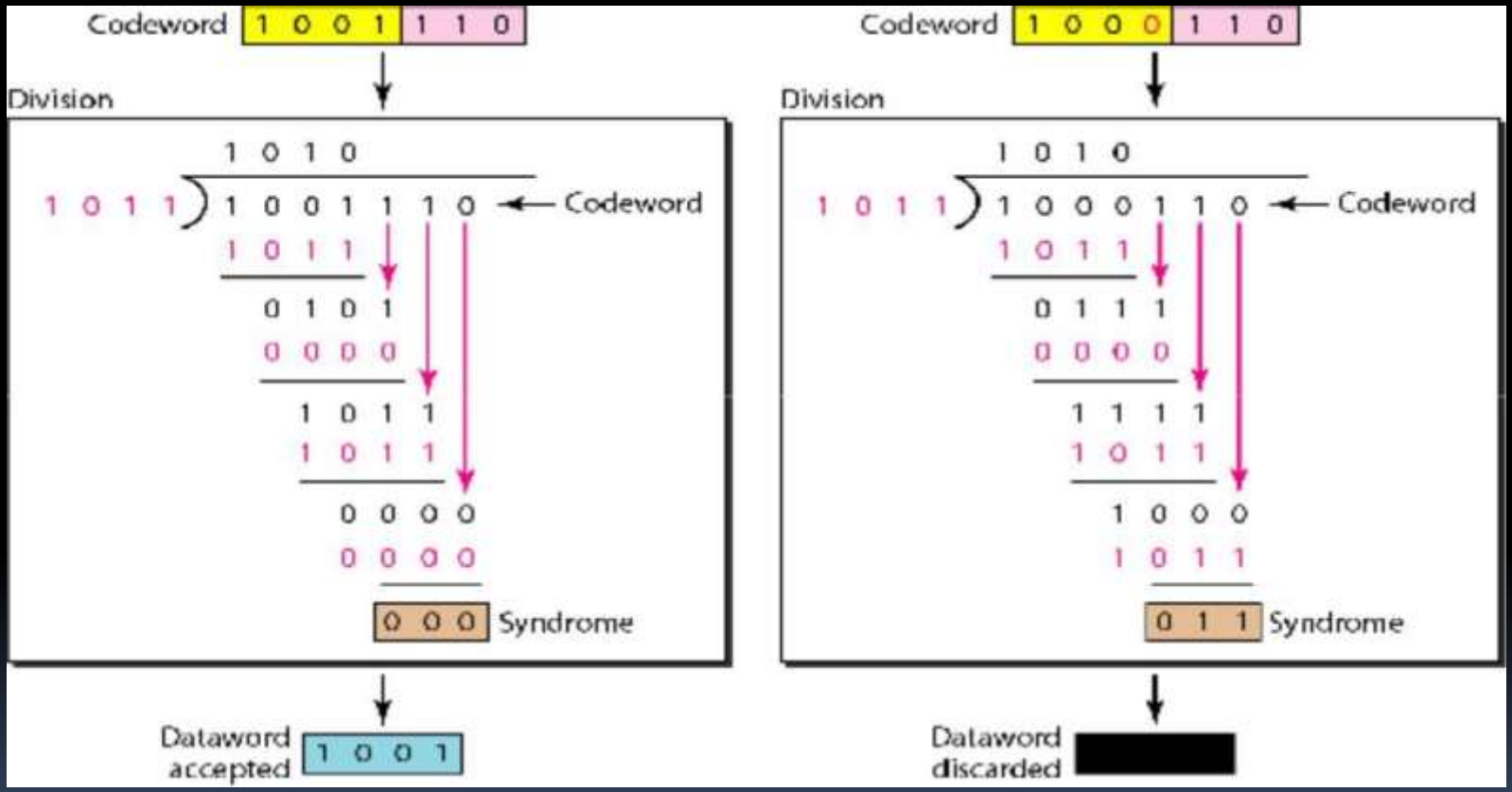



**Fig :** Division in Cyclic Code

In a cyclic code, following cases exist:

- If syndrome $s(x) \neq 0$, one or more bits is corrupted.
- If syndrome $s(x) = 0$, either
  - No bit is corrupted
  - Some bits are corrupted, but the decoder failed to detect them.

# NOISELESS CHANNEL AND NOISY CONTROL PROTOCOL

Noiseless protocols takes channel as an ideal one in which no frames are lost, duplicated, or corrupted. There are two types of protocols used for noiseless channels namely simplest and stop & wait protocol. The first is a protocol that does not use flow control; the second is the one that does. Of course, neither has error control because we have assumed that the channel is a perfect noiseless channel.

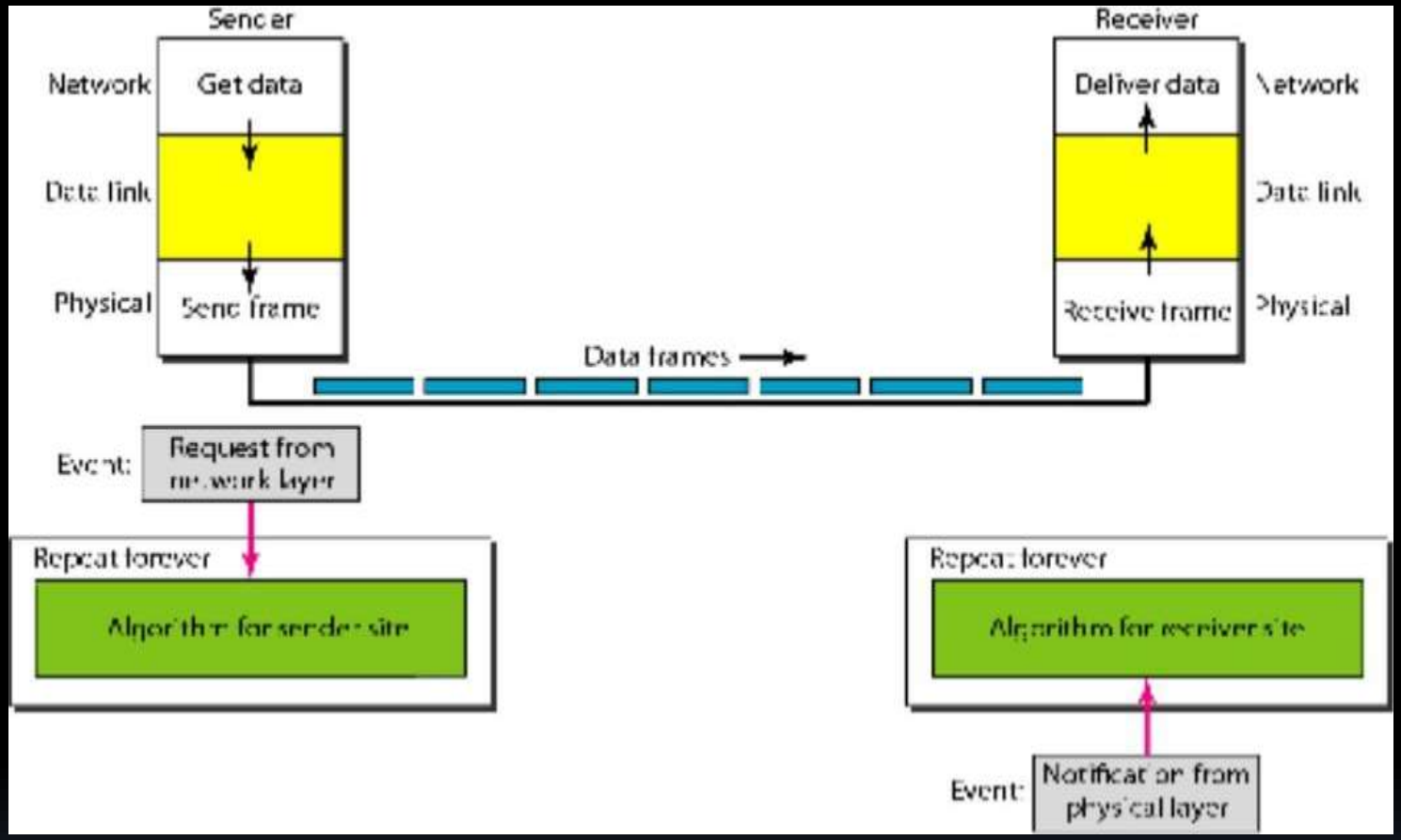



**Fig :** The design of the simplest protocol with no flow or error control

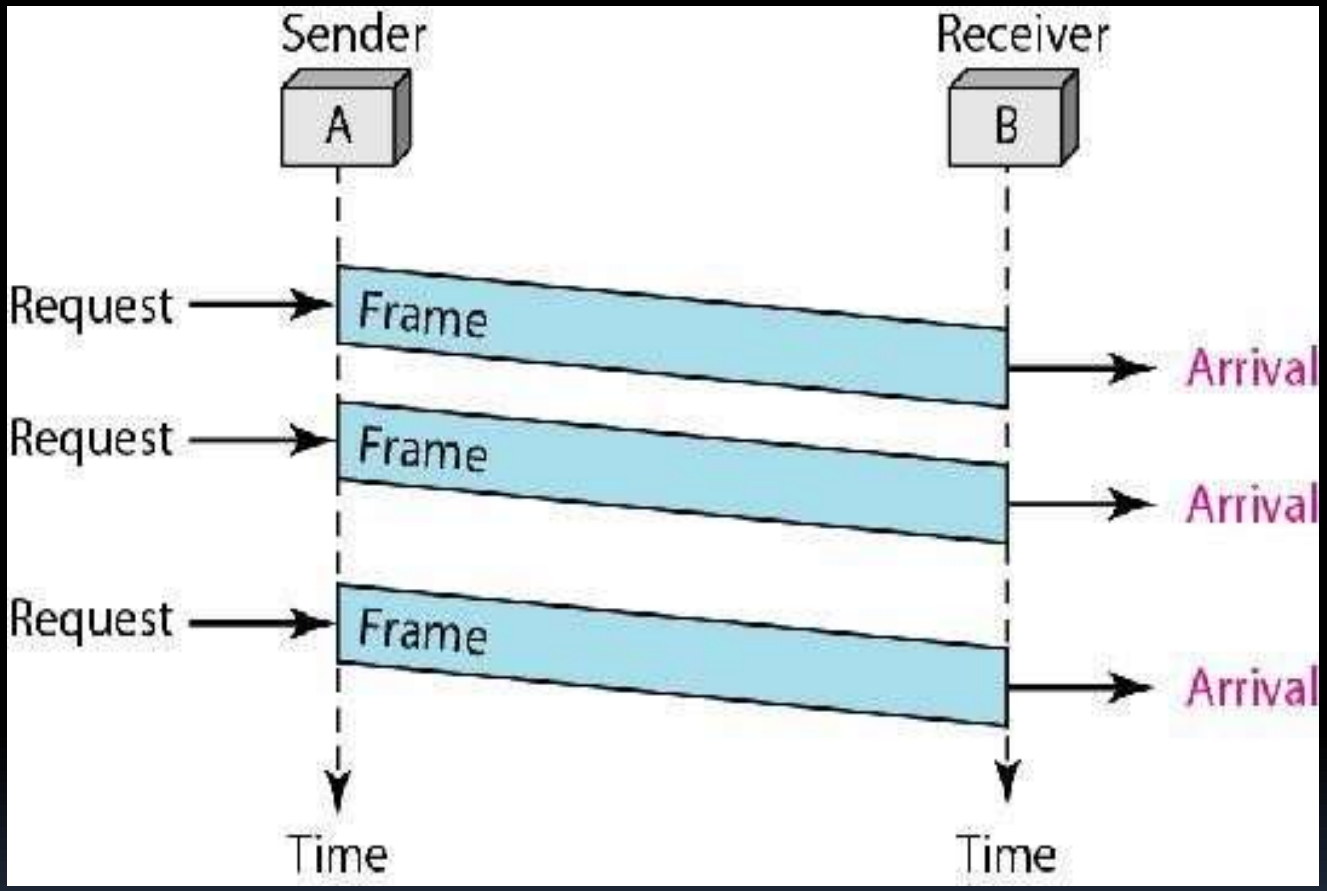



**Fig :** Flow diagram of Simplest Protocol

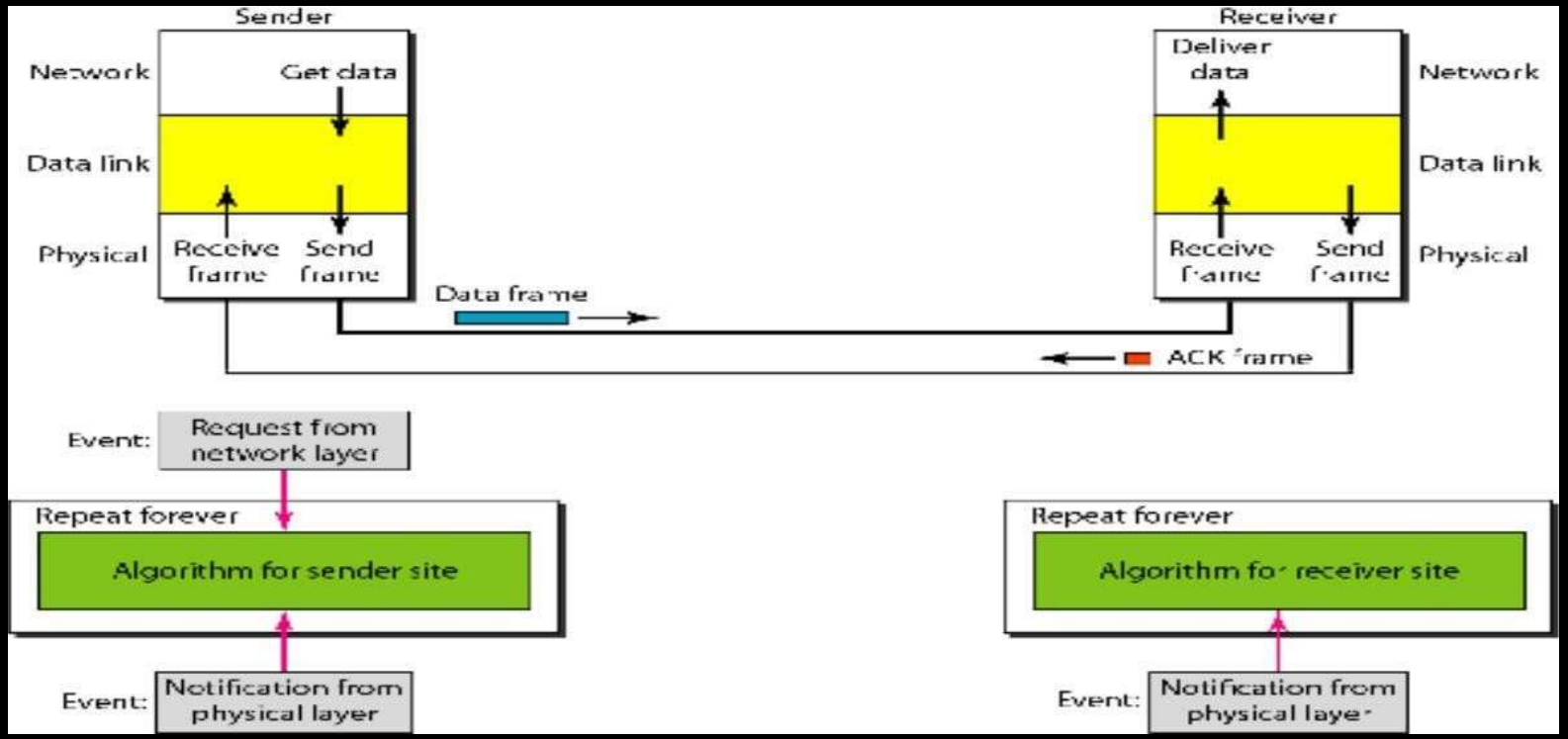



**Fig :** Design of Stop-and-Wait Protocol

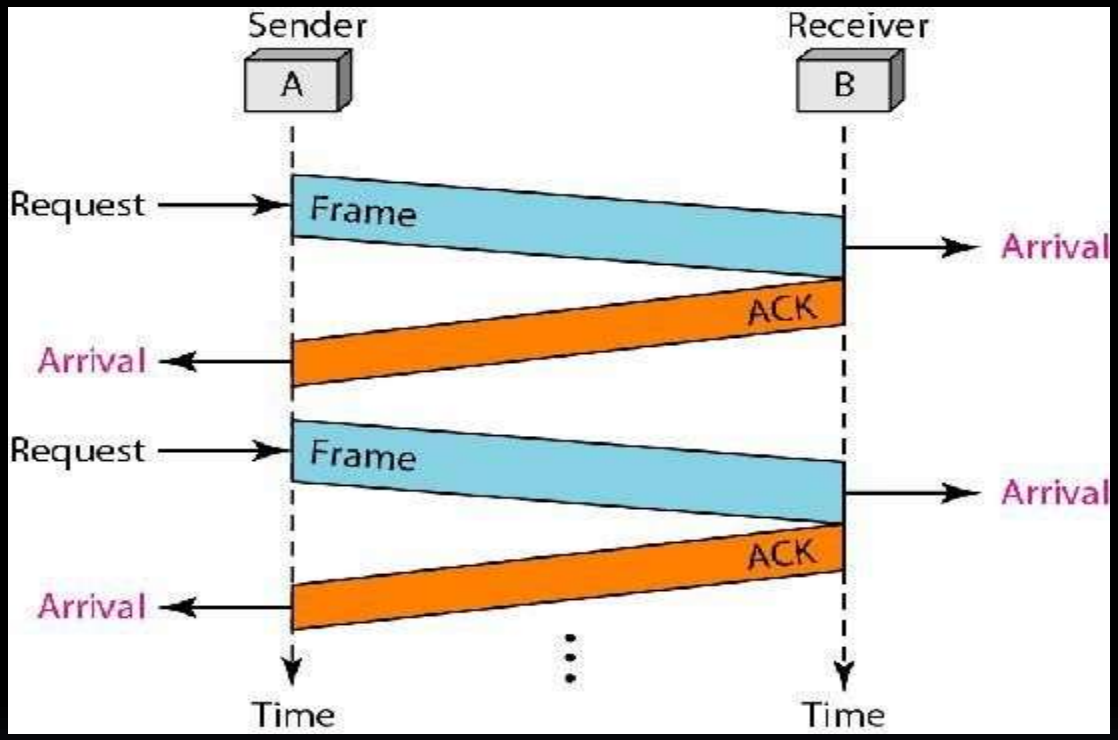



**Fig :** Flow diagram of Simplest Protocol

## Noisy Channel Protocol

Although the Stop-and-Wait Protocol gives us an idea of how to add flow control to its predecessor, noiseless channels are nonexistent. We can ignore the error or we need to add error control to our protocols. There are three protocols used in case of noisy channels namely: stop & wait automatic repeat request, go-back- n automatic repeat request and selective automatic repeat request.

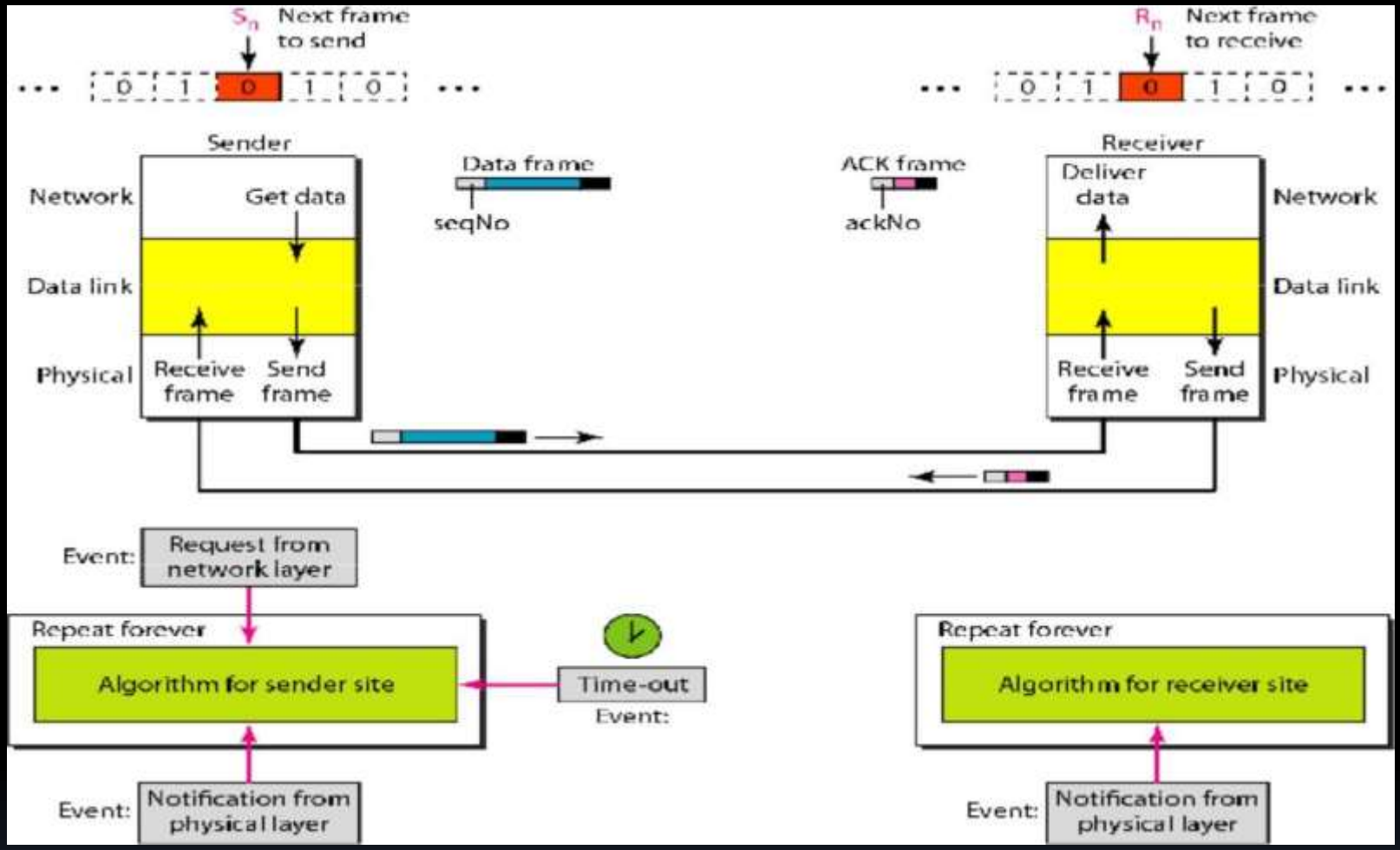



**Fig :** Stop & Wait Automatic Repeat Request

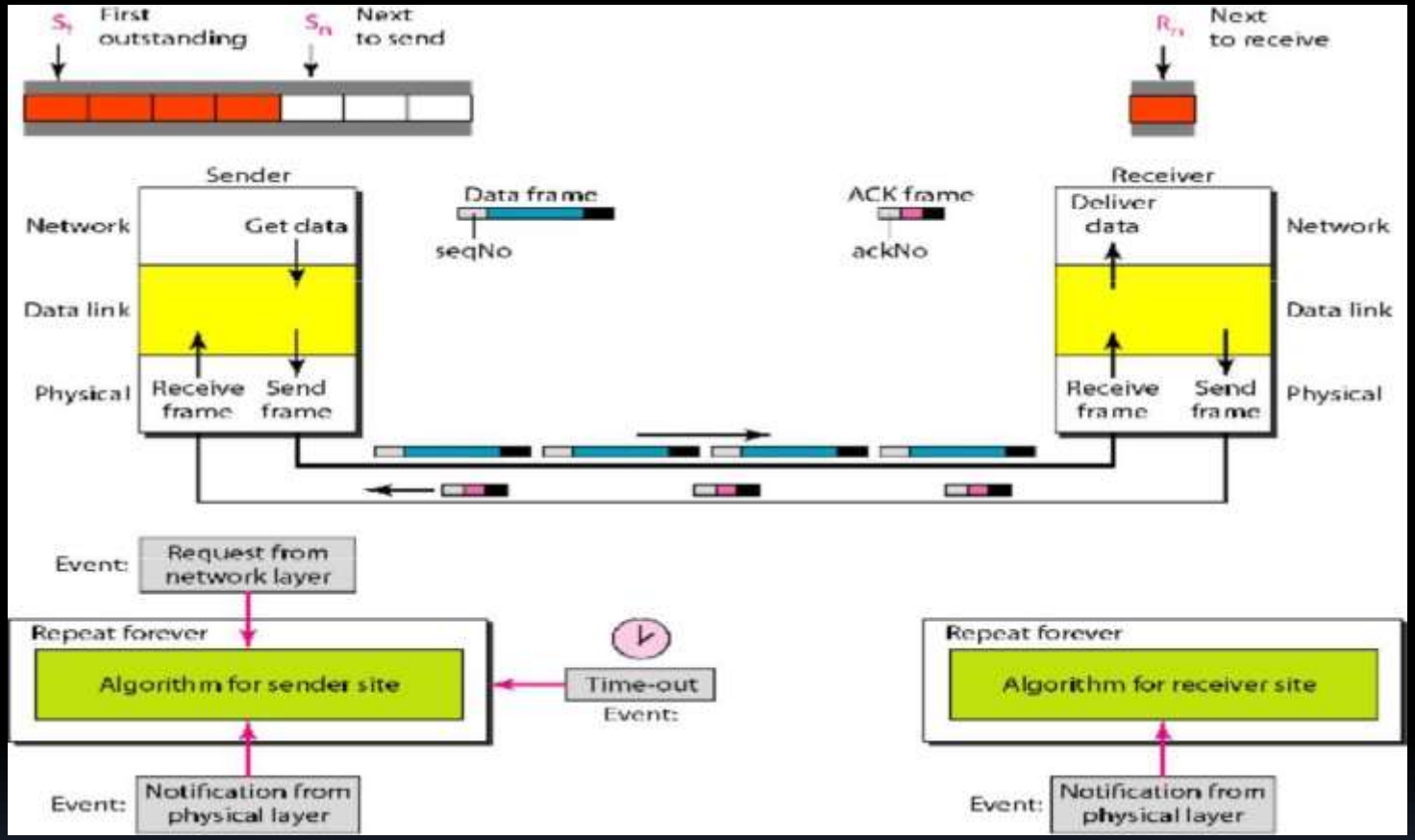



**Fig :** Go-Back-n Automatic Repeat Request

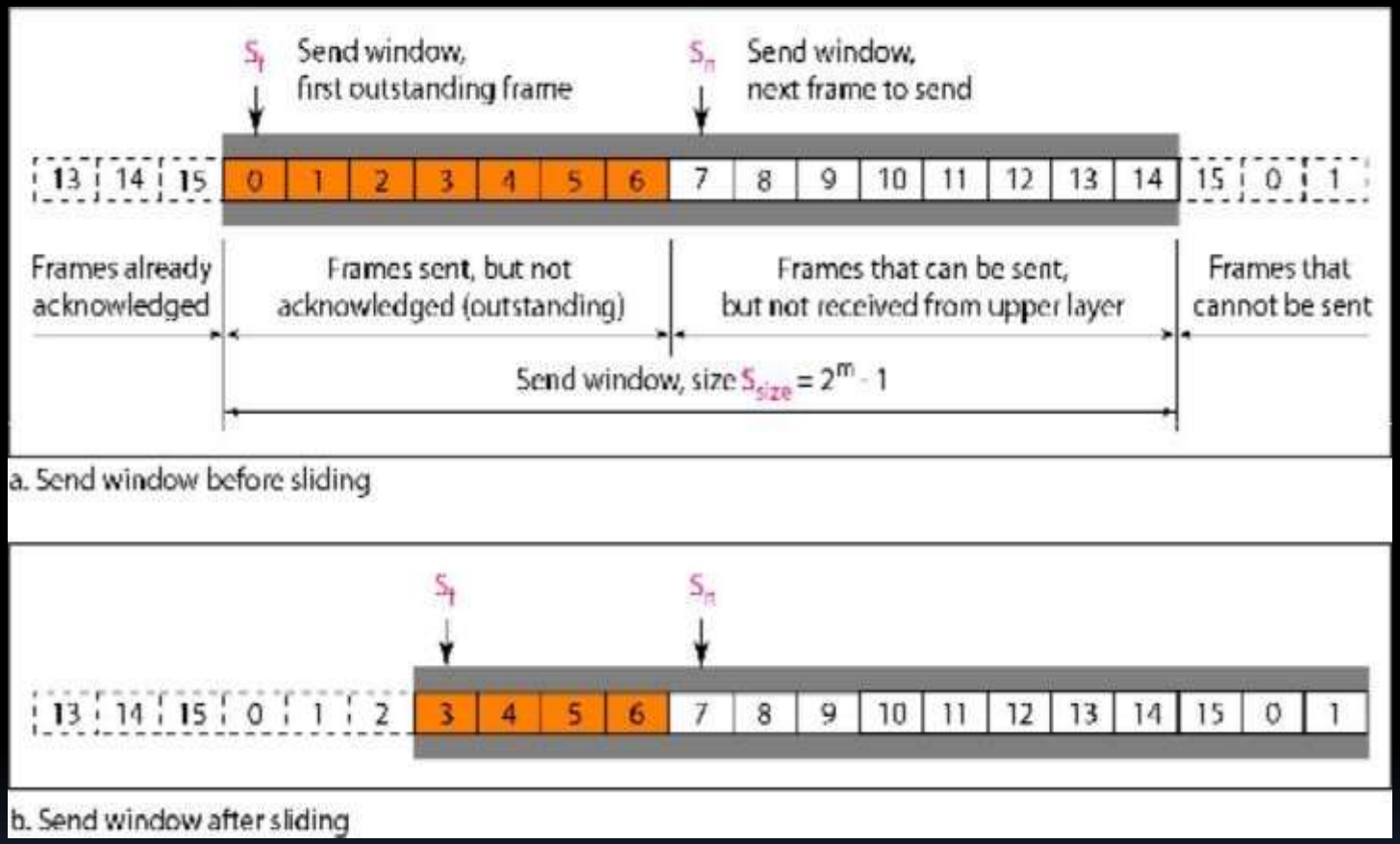



**Fig :** Send window (a) before and (b) after sliding

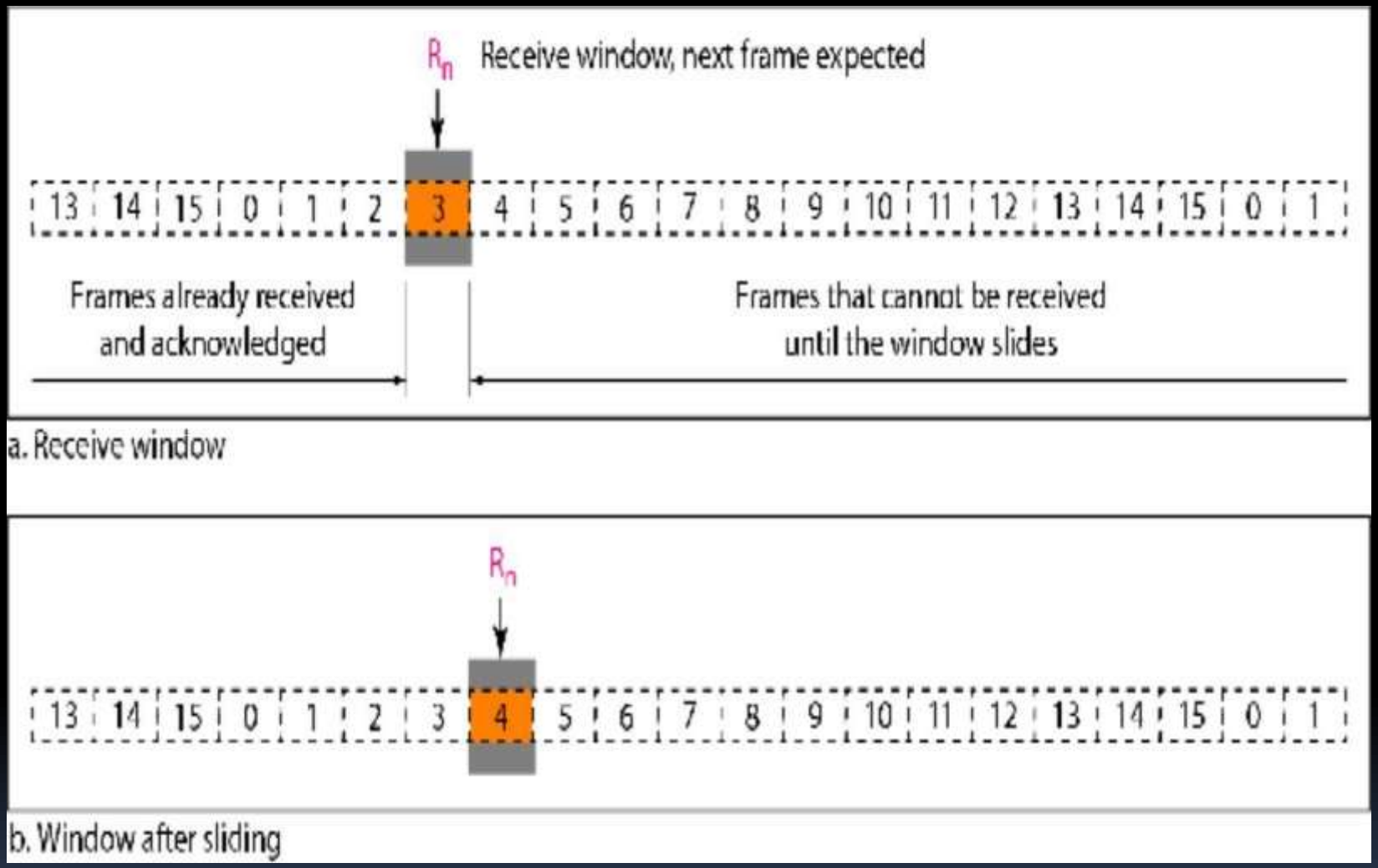



**Fig :** Receive window (a) before and (b) after sliding

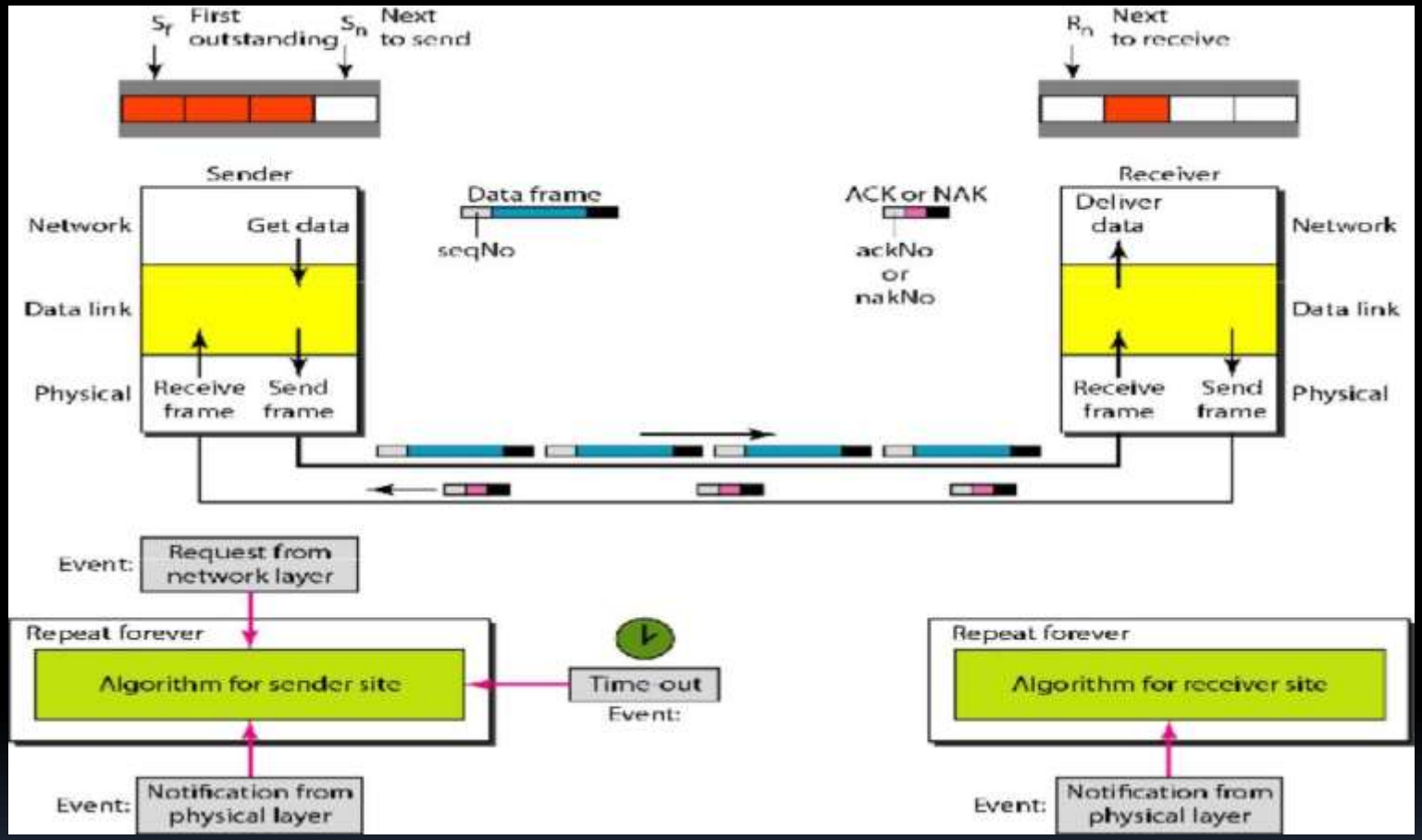



**Fig :**Selective Repeat Automatic Repeat Request

# POINT-TO-POINT PROTOCOL

Although HDLC is a general protocol that can be used for both point-to-point and multipoint configurations, one of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP. The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point- to-point protocol at the data link layer. PPP is by far the most common. PPR frame format has been shown in Fig

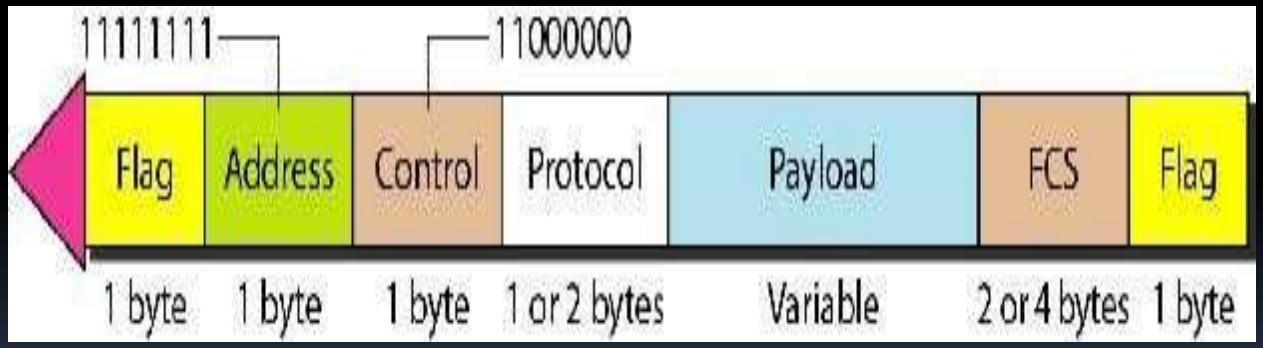



**Fig :** PPP Frame Format

**PPP provides several services:**

- PPP defines the format of the frame to be exchanged between devices.
- PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP defines how network layer data are encapsulated in the data link frame.
- PPP defines how two devices can authenticate each other.
- PPP provides multiple network layer services supporting a variety of network layer protocols.
- PPP provides connections over multiple links.
- PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

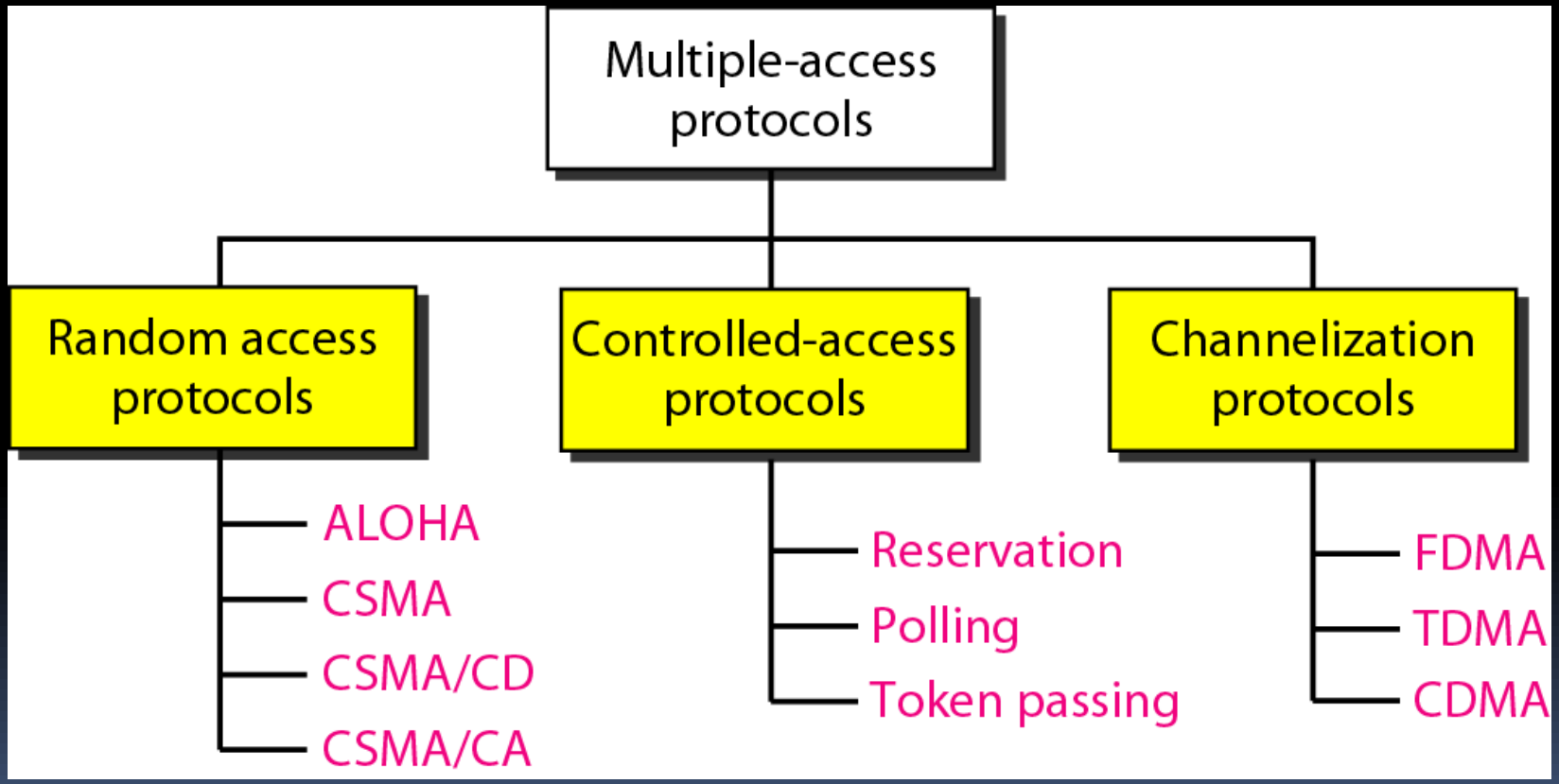
**On the other hand, to keep PPP simple, several services are missing:**

- PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver.
- PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order.

PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration

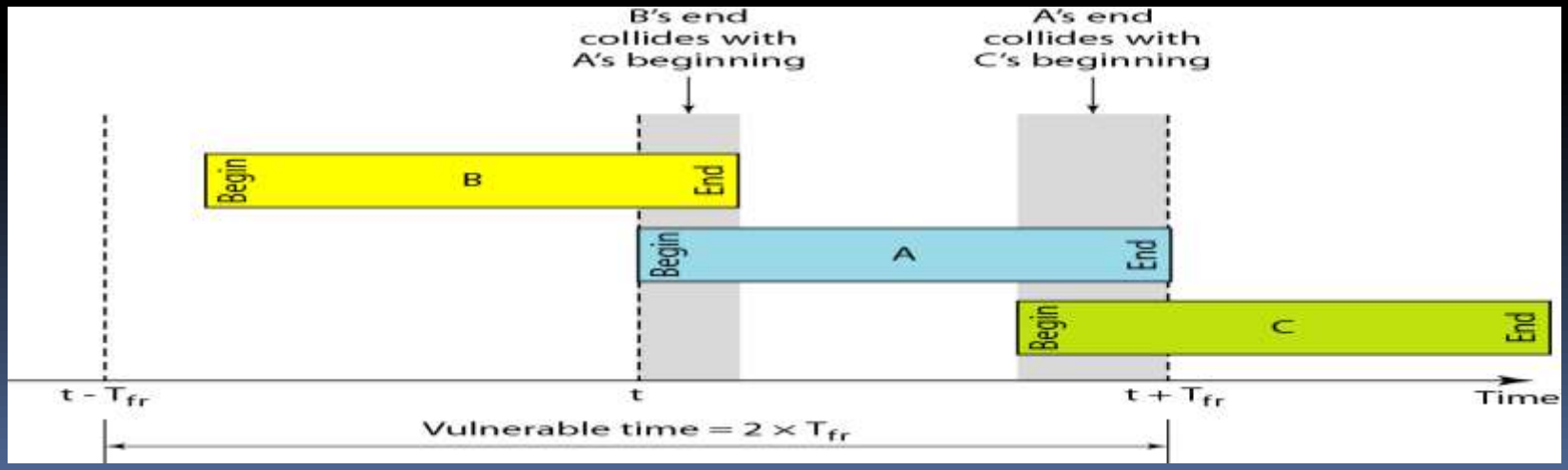
# UNIT-3
# MULTIPLE ACCESS

# RANDOH

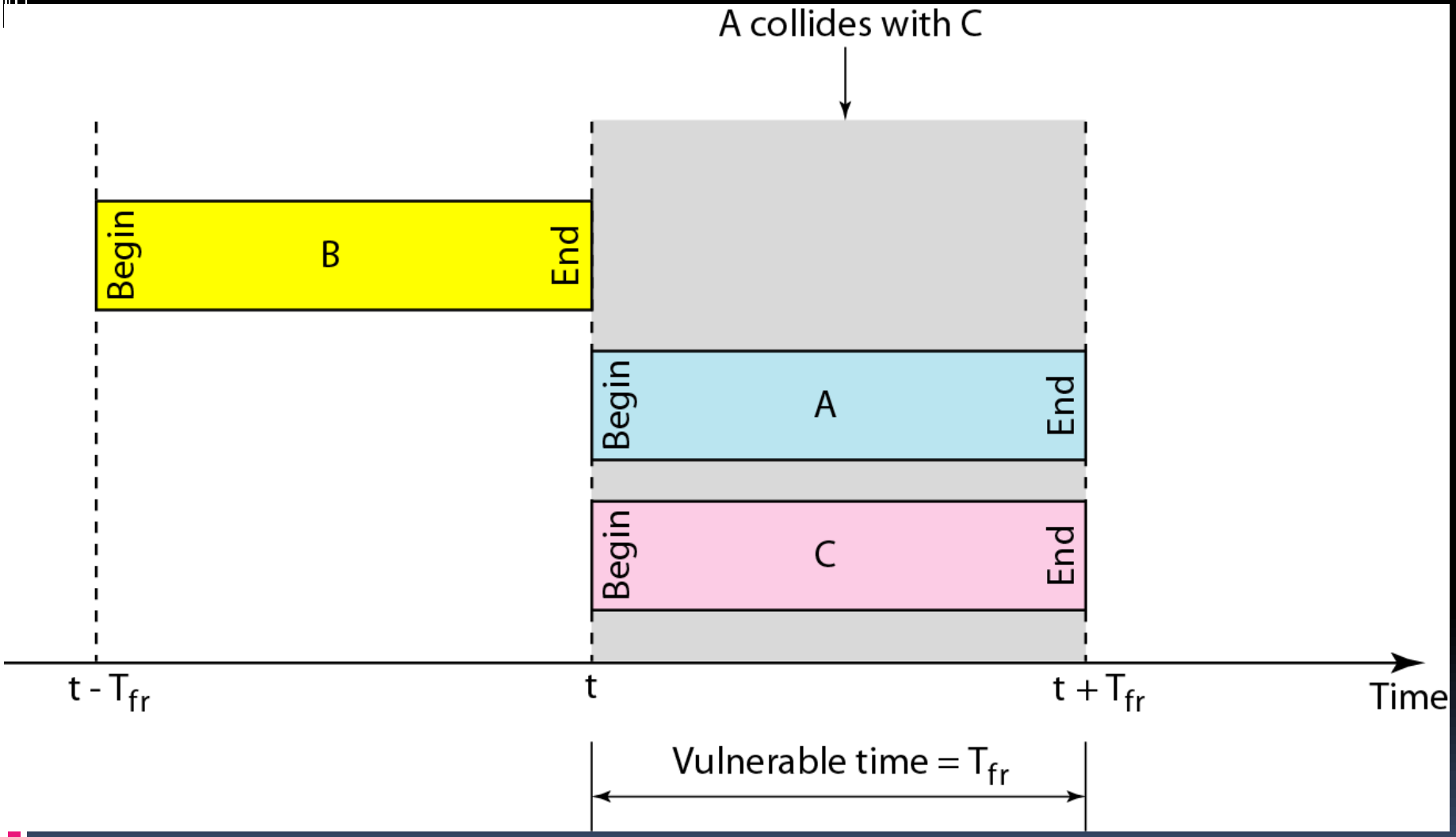

Multiple-access protocols
Random access protocols
Controlled-access protocols
Channelization protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token passing
FDMA
TDMA
CDMA

- **Random Access (or contention) Protocols:**
  - No station is superior to another station and none is assigned the control over another.
  - A station with a frame to be transmitted **can use the link directly based** on a procedure defined by the protocol to make a decision on whether or not to send.
- **ALOHA Protocols :**
- Was designed for **wireless LAN** and can be used for **any shared medium**
- **Pure ALOHA** Protocol:
- All frames from any station are of fixed length (**L bits**)
- Stations transmit at equal **transmission time** (***all stations produce frames with equal frame lengths***).

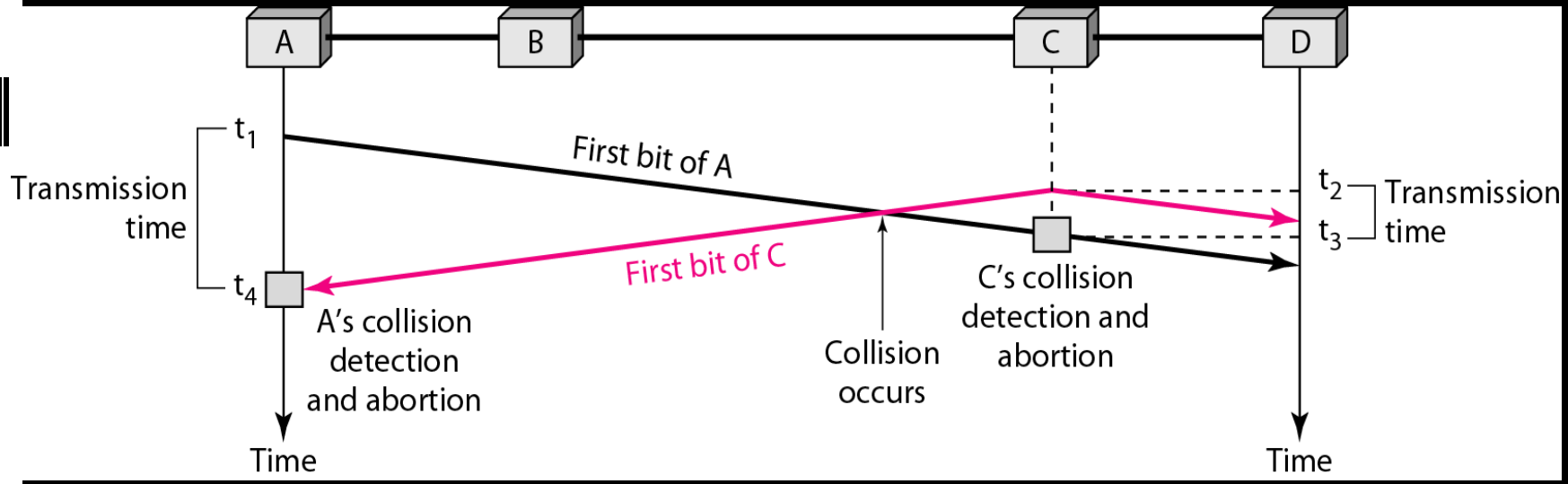
- A station that has data **can transmit at any time**
- **After transmitting a frame**, the sender **waits** for an **acknowledgment** for an amount of time (time out) equal to the **maximum round-trip propagation delay** = 2* $t_{prop}$(**see next slide**)
- If **no ACK** was received, sender assumes that the **frame or ACK** has been destroyed and **resends** that frame after it **waits for a *random* amount of time**

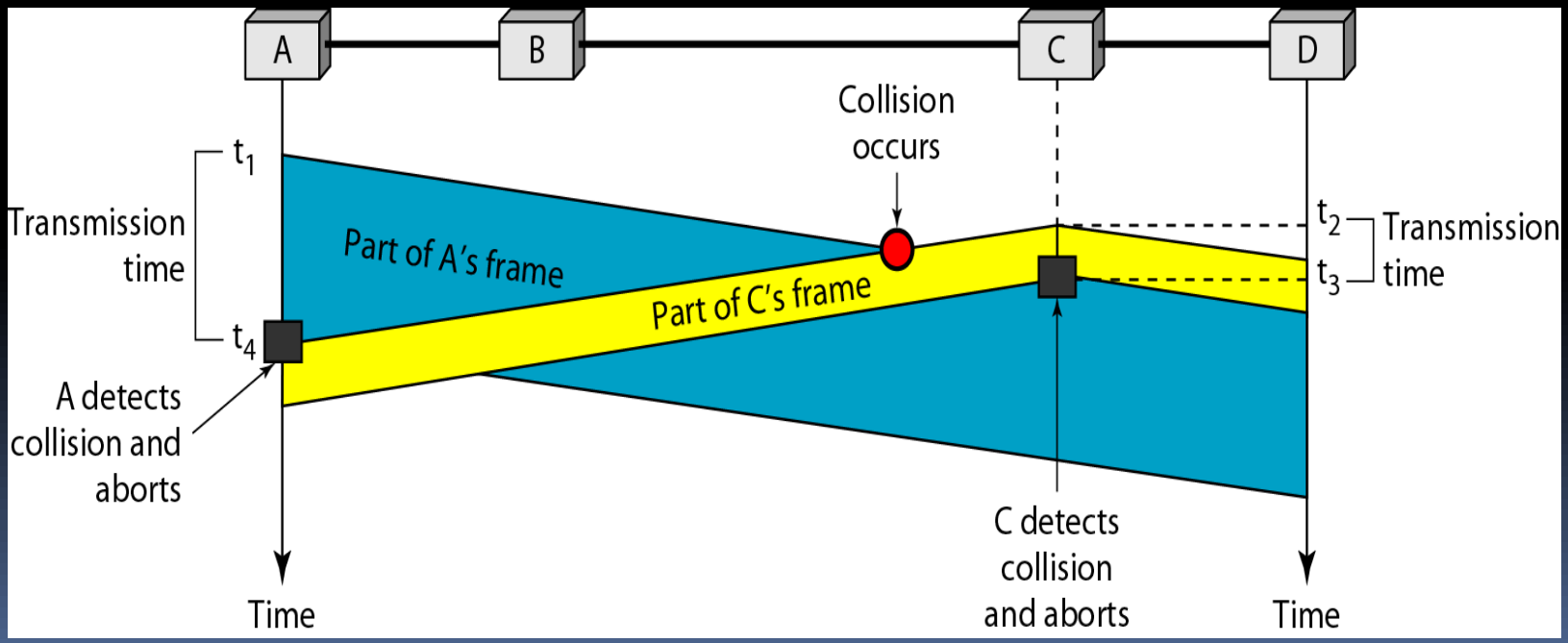


- **Slotted ALOHA:**
- Time is divided into slots equal to a **frame transmission time ($T_{fr}$)**
- A station can transmit at the beginning of a slot only
- If a station misses the beginning of a slot, it has to wait until the beginning of the next time slot.
- **A central clock** or station informs all stations about the start of a each slot
- Maximum channel utilization is **37%**

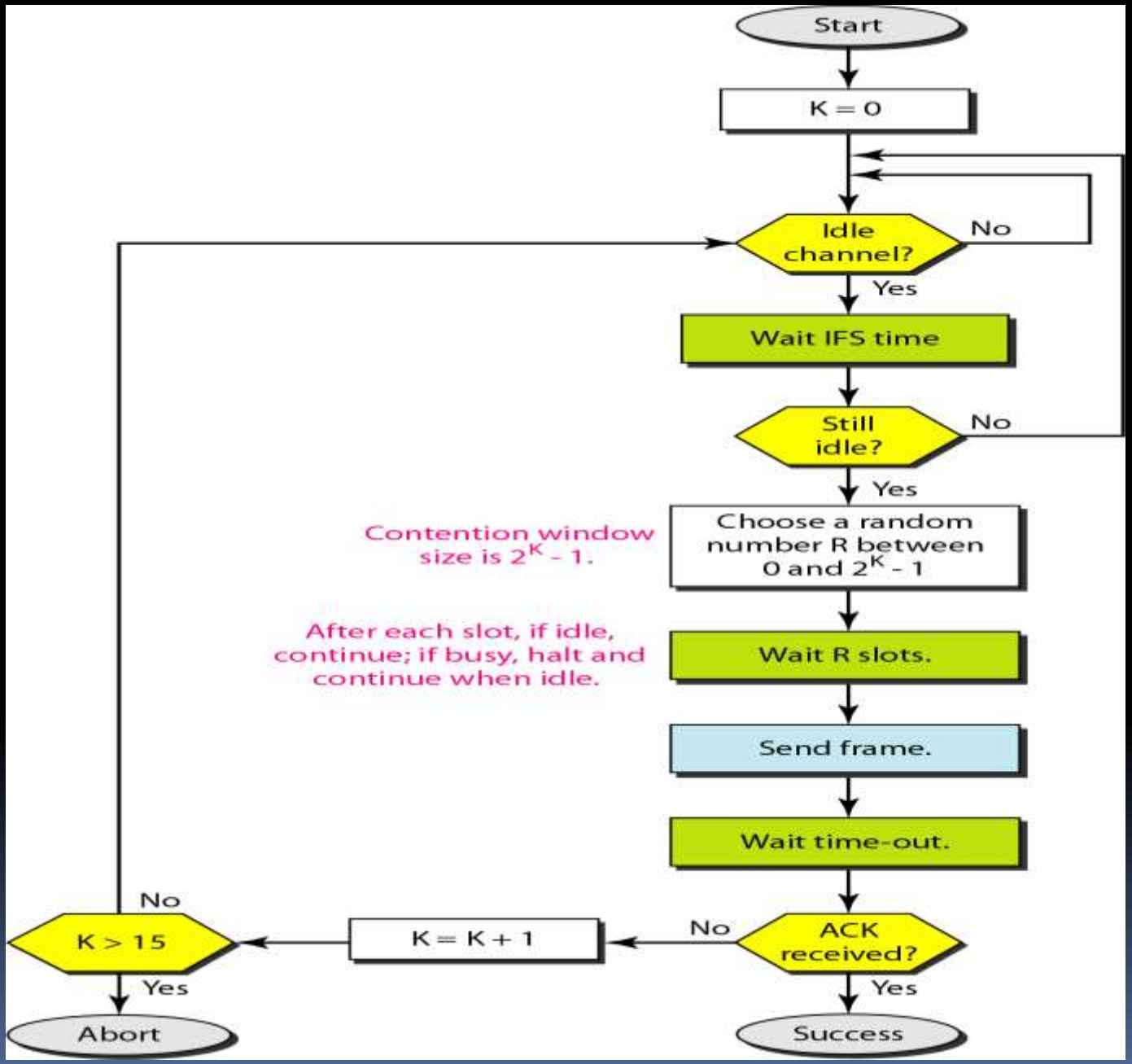

A collides with C
Begin
B
End
Begin
A
End
Begin
C
End
t - Tfr
t
t + Tfr
Time
Vulnerable time = Tfr

- Advantage of ALOHA protocols
  - A node that has frames to be transmitted can **transmit continuously** at the **full rate of channel (R bps)** if it is the only node with frames
  - Simple to be implemented
  - No master station is needed to control the medium
- **CSMA/CD:**
  - While transmitting, the sender is **listening to medium** for collisions.
  - Sender **stops transmission** if collision has occurred **reducing channel wastage**.
- CSMA/CD is widely used for **bus topology LANs** (IEEE 802.3, Ethernet).


A
B
C
D
$t_1$
Transmission time
$t_4$
First bit of A
First bit of C
A's collision detection and abortion
Collision occurs
C's collision detection and abortion
$t_2$
$t_3$
Transmission time
Time
Time


A
B
C
D
Collision occurs
$t_1$
Transmission time
$t_4$
Part of A's frame
Part of C's frame
$t_2$
$t_3$
Transmission time
A detects collision and aborts
C detects collision and aborts
Time
Time

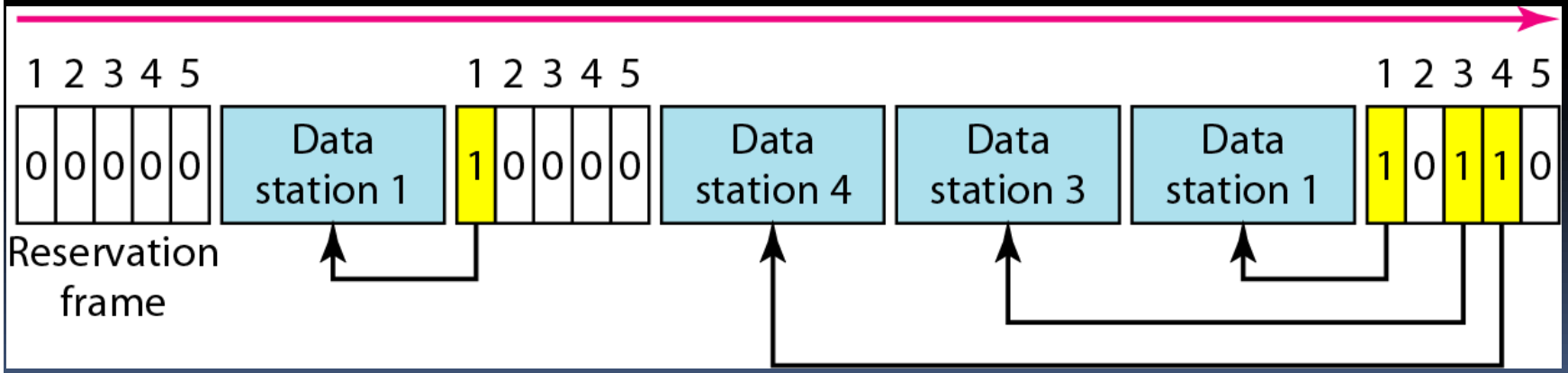
- **CSMA/CA**
- CSMA was invented for wireless networks.
- Collisions are through the use of CSMA/CA's three strategies: the inter frame space, the contention window, and acknowledgement as shown in below figure.


Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Choose a random number R between 0 and 2^K - 1
Contention window size is 2^K - 1.
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
ACK received?
No
Yes
Success
K = K + 1
K > 15
No
Yes
Abort

- **Controlled Access:**
- In controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by other stations.
- Provides **in order access** to shared medium so that every station has chance to transfer (**fair protocol**)
- ***Eliminates*** collision completely
- **Three methods** for controlled access:
  - Reservation
  - Polling
  - Token Passing

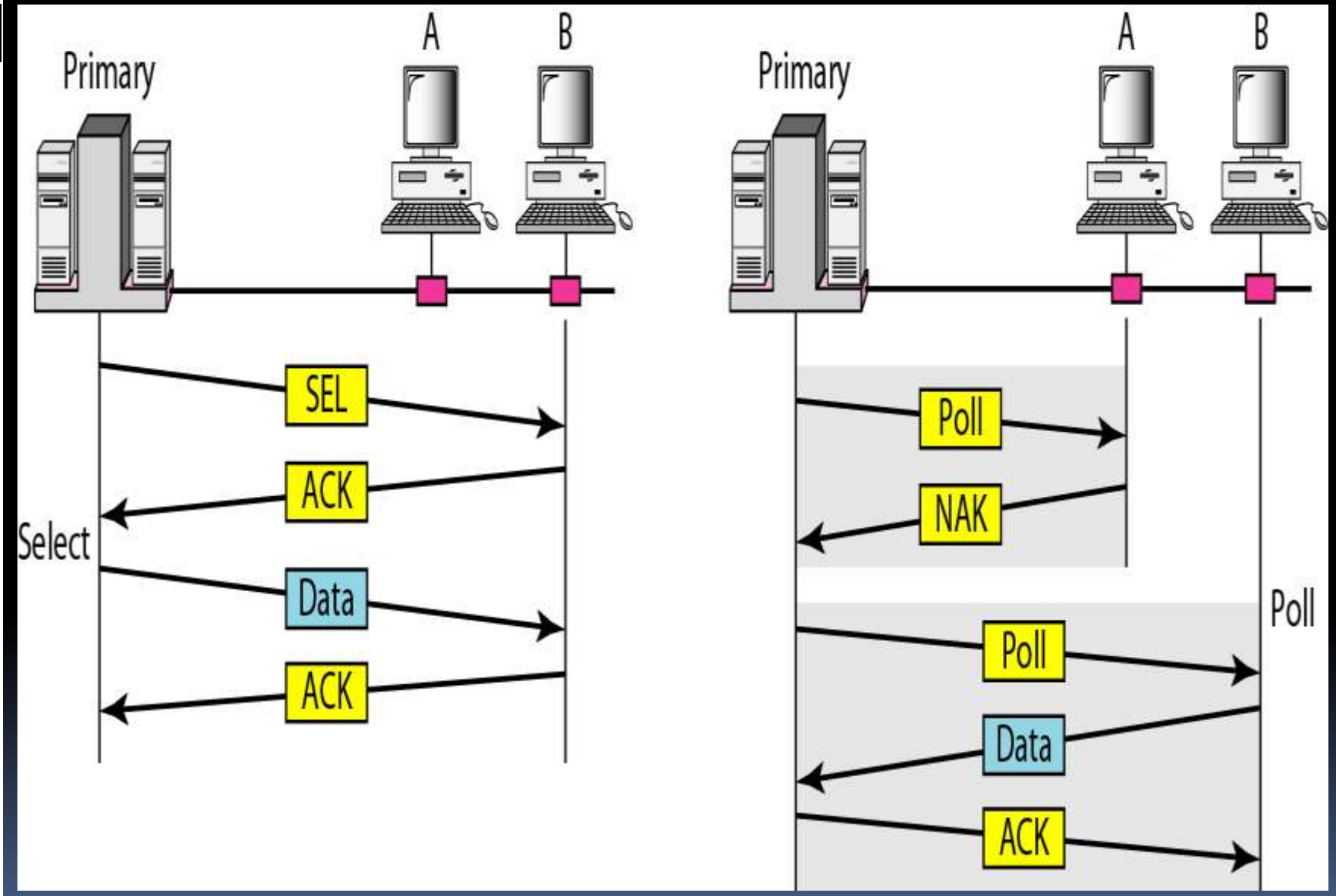
# Reservation:

- Transmissions are organized into variable length cycles
- Each cycle begins with a reservation interval that consists of (N) mini slots. One mini slot for each of the N stations
- When a station needs to send a data frame, it makes a **reservation** in its own mini slot.
- By listening to the reservation interval, every station knows which stations will transfer frames, and in which order.
- The stations that made reservations can send their data frames after the reservation frame.

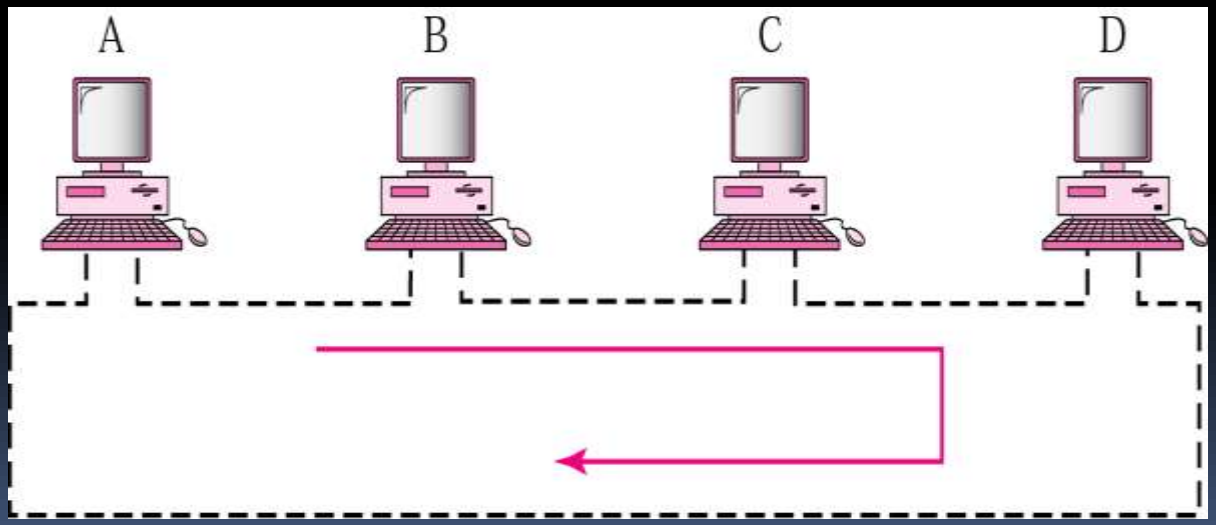


- **Polling:**
- Stations take turns accessing the medium
- Two models: **Centralized** and **distributed** polling
- **Centralized polling**
  - One device is assigned as **primary station** and the others as **secondary stations**
  - All data exchanges are done through the **primary**
  - When **the primary has a frame to send** it sends a **select** frame that includes the address of the intended secondary
  - When **the primary is ready to receive** data it send a **Poll** frame for each device to ask if it has data to send or not. If yes, **data** will be transmitted otherwise **NAK** is sent.
  - Polling can be done in order (Round-Robin) or based on predetermined order

- **Distributed polling**
  - **No primary and secondary**
  - Stations have a **known polling order** list which is made based on some protocol
  - **station with the highest priority** will have the access right first, then it passes the access right to the **next station (it will send a pulling message to the next station in the pulling list)**, which will passes the access right to the following next station, …
  - Distributed polling is shown in below figure.


Primary
A
B
SEL
ACK
Select
Data
ACK
Primary
A
B
Poll
NAK
Poll
Poll
Data
ACK

- **Token Passing:** It Implements Distributed Polling System
- In the **token-passing** method, the stations in a network are organized in a logical ring. In other words, for each station, there is a ***predecessor*** and a ***successor***.
-



- **Channelization:**
- Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.
- There are three channelization protocols: ***FDMA***, ***TDMA***, and ***CDMA***.
- **FDMA:**
- In **frequency-division multiple access (FDMA),** the available bandwidth is divided into frequency bands.

- Each station is allocated a band to send its data. In other words, each band is reserved for specific station.
- FDMA specifies a predetermined frequency band for the entire period of communication.
- FDM is a physical layer technique that combines the loads from low bandwidth channels and transmits them by using a high-bandwidth channel.
- FDMA, on the other hand, is an access method in the data-link layer.
- The data link layer in each station tells its physical layer to make a band pass signal from the data passed to it.

- **TDMA:**

- In **time-division multiple access (TDMA),** the stations share the bandwidth of the channel in time.
- Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot.
- The main problem with TDMA lies in achieving synchronization between the different stations.
- Each station needs to know the beginning of its slot and the location of its slot.
- This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area.
- To compensate for the delays, we can insert *guard times*.
- Synchronization is normally accomplished by having some synchronization bits (normally referred to as *preamble bits*) at the beginning of each slot.

## CDMA:

- **Code-division multiple access (CDMA)** was conceived (*meaning imagine/visualize*) several decades ago.
- Recent advances in electronic technology have finally made its implementation possible.
- CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link.
- It differs from TDMA in that all stations can send data simultaneously; there is no timesharing.
- In CDMA, one channel carries all transmissions simultaneously.

- **Standard Ethernet:**
- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- For Ethernet, the protocol data unit is Frame since we mainly deal with DLL.
- In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.

- Physical Media :-
  - 10 Base5 - Thick Co-axial Cable with Bus Topology
  - 10 Base2 - Thin Co-axial Cable with Bus Topology
  - 10 BaseT - UTP Cat 3/5 with Tree Topology
  - 10 BaseFL - Multimode/Single mode Fiber with Tree Topology
- **Fast Ethernet:**
- The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds.
- This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure.

- Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.
- **There are three types of Fast Ethernet**: 100BASE-TX for use with level 5 UTP cable;
- 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable.
- The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.
- Network managers who want to incorporate Fast Ethernet into an existing with existing 10BASE-T segments.

- **Gigabit Ethernet:**
- Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP).
- Also known as "gigabit-Ethernet-over-copper" or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T.
- It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone.
- Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.
- The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

- **10 Gigabit Ethernet:**
- 10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards.
- IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.
- Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections.
- This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing.

- **IEEE 802.11:**
- The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.
- **There are several specifications in the 802.11 family**
- **802.11** – this pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- **802.11a** – this is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band.

- 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- **802.11b** – The 802.11 high rate Wi-Fi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission.
- The 802.11b specification uses only DSSS.
- 802.11 standards added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- **802.11g** – this pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

## Bluetooth IEEE 802.16:

- Bluetooth radio typically hops faster and uses shorter packets as compared to other systems operating in the same frequency band.
- Use of FEC (Forward Error Correction) limits the impact of random noise.
- As the interference increases, the performance decreases.
- Bluetooth devices can interact with other Bluetooth devices.
- One of the devices acts as a master and others as slaves.
- This network is called “Piconet”.
- A single channel is shared among all devices in Piconet.
- There can be up to seven active slaves in the Piconet.
- Each of the active slaves has an assigned 3 bit Active Member address.

- A lot of other slaves can remain synchronized to the Master through remaining inactive slaves, referred to as parked nodes.
- A parked device remains synchronized to the master clock and can become active and start communicating in the Piconet anytime.
- If  Piconets are close to each other, they have overlapping areas
- The scenario where the nodes of two or more Piconets mingle is called Scatternet
- Before any connections in the Piconet are created all devices are in STDBY mode
- In this mode an unconnected unit periodically “listens” for message every 1.28 seconds.

- A cable replacement technology
- 1 Mb/s symbol rate
- Range 10+ meters
  - Single chip radio + baseband at low power & low price

# UNIT-4
# NETWORK LAYER

# DESIGN ISSUES

- Draw crude map. How to get from one host to another? If each link delivers reliably then is the whole route reliable a router may fail, limited but space (may have to throw packets on the door).Data Link Layer deals with machine-to-machine communication Network Layer lowest layer that deals with host-to-host communication, call this end-to-end communication.
- Four Issues:

1.Interface between the host and the network (the network layer is typically the boundary between the host and subnet)

2.Routing

3.Congestion and deadlock

- When more packets enter an area than can be processed, delays increase and performance decreases. If the situation continues, the subnet may have no alternative but to discard packets.
  - If the delay increases, the sender may (incorrectly) retransmit, making a bad situationeven worse.
  - Overall, performance degrades because the network is using (wasting) resources  processing packets that eventually get discarded.

4. Internetworking (A path may traverse different network technologies(e.g., Ethernet, point-to-point links, etc.) packets may travel through many different networks each network may have a different frame format some networks may be connectionless, other connection oriented

- **ROUTING ALGORITHMS:**
- **A) NON-HIERARCHICAL ROUTING**
- In this type of routing, interconnected networks are viewed as a single network, where bridges, routers and gateways are just additional nodes.
- Every node keeps information about every other node in the network
- In case of adaptive routing, the routing calculations are done and updated for all the nodes.

- **B) HIERARCHICAL ROUTING**
- This is essentially a 'Divide and conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers. Thus, the network is viewed at two levels:
- The Sub-network level, where each node in a region has information about its peers in the same region and about the region's interface with other regions.
- The Network Level, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.

- Advantages of Hierarchical Routing:
- Smaller sizes of routing tables.
- Substantially lesser calculations and updates of routing tables.
- Disadvantage:
- Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.

- **SOURCE ROUTING**
- Source routing is similar in concept to virtual circuit routing. It is implemented as under:
- Initially, a path between nodes wishing to communicate is found out, either by flooding or by any other suitable method.
- This route is then specified in the header of each packet routed between these two nodes. A route may also be specified partially, or in terms of some intermediate hops.
- Advantages:
- Bridges do not need to look up their routing tables since the path is already specified in the packet itself.

- The throughput of the bridges is higher, and this may lead to better utilization of bandwidth, once a route is established.
- Disadvantages:
- Establishing the route at first needs an expensive search method like flooding.
- To cope up with dynamic relocation of nodes in a network, frequent updates of tables are required; else all packets would be sent in wrong direction. This too is expensive.

- **POLICY BASED ROUTING**

- In this type of routing, certain restrictions are put on the type of packets accepted and sent. e.g.. The IIT - K router may decide to handle traffic pertaining to its departments only, and reject packets from other routes. This kind of routing is used for links with very low capacity or for security purposes.

- **E) SHORTEST PATH ROUTING**
- Here, the central question dealt with is 'How to determine the optimal path for routing?' Various algorithms are used to determine the optimal routes with respect to some predetermined criteria. Some of the important ways of determining the cost are:
  - **Minimum number of hops**: If each link is given a unit cost, the shortest path is the one with minimum number of hops. Such a route is easily obtained by a breadth first search method. This is easy to implement but ignores load, link capacity etc.
  - **Transmission and Propagation Delays**: If the cost is fixed as a function of transmission and propagation delays, it will reflect the link capacities and the geographical distances. However these costs are essentially static and do not consider the varying load conditions.
  - **Queuing Delays**: If the cost of a link is determined through its queuing delays, it takes care of the varying load conditions, but not of the propagation delays.

- ROUTING ALGORITHM
- **a) Bellman-Ford Algorithm**
- This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.

- Notation:

d i,j = Length of path between nodes i and j, indicating the cost of the link.

h = Number of hops

D[ i,h] = Shortest path length from node i to node 1, with upto 'h' hops.

D[ 1,h] = 0

for all h .

- **b) Dijkstra's Algorithm**
- Notation:

  Di = Length of shortest path from node 'i' to node 1.

  di,j = Length of path between nodes i and j

  **Dj = min [ Dj , Di + dj,i ]**

- Finally, after N-1 iterations, the shortest paths for all nodes are known, and the algorithm terminates.

- **c) The Floyd Warshall Algorithm**
- This algorithm iterates on the set of nodes that can be used as intermediate nodes on paths. This set grows from a single node ( say node 1 ) at start to finally all the nodes of the graph. At each iteration, we find the shortest path using given set of nodes as intermediate nodes, so that finally all the shortest paths are obtained.

- Notation

$D_{i,j}[n]$ = Length of shortest path between the nodes i and j using only the nodes 1,2,….n as intermediate nodes.

- Initial Condition

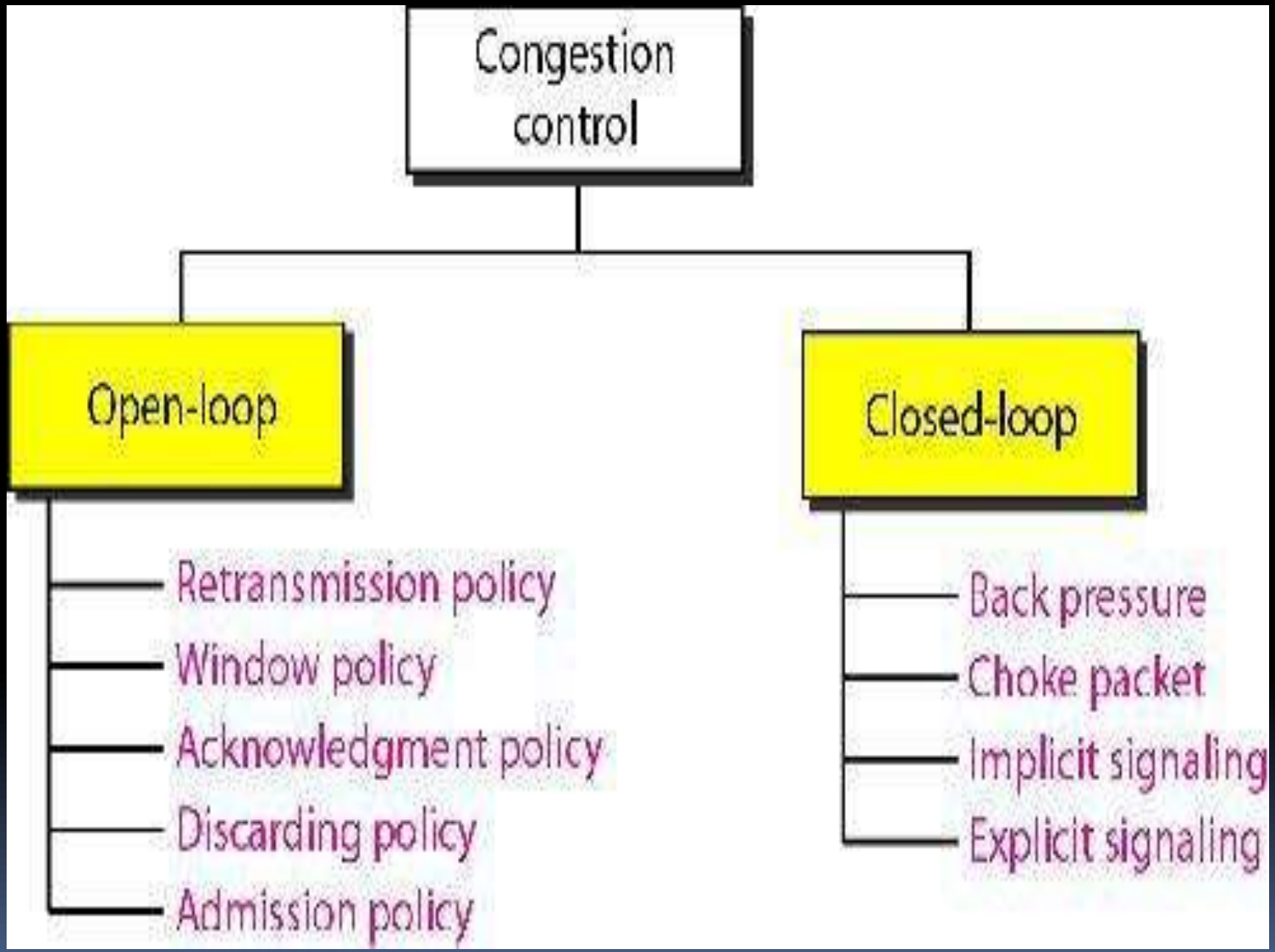
$$D_{i,j}[o] = d_{i,j}$$

- for all nodes i,j .

- **CONGESTION CONTROL ALGORITHMS:**
- An important issue in a packet-switched network is **congestion.** Congestion in a network may occur if the **load** on the network-the number of packets sent to the network-is greater than the *capacity* of the network-the number of packets a network can handle. **Congestion control** refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.
- We may ask why there is congestion on a network. Congestion happens in any system that involves waiting

# CONGESTION CONTROL

- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal) as shown in Fig.


Congestion control
Open-loop
Retransmission policy
Window policy
Acknowledgment policy
Discarding policy
Admission policy
Closed-loop
Back pressure
Choke packet
Implicit signaling
Explicit signaling

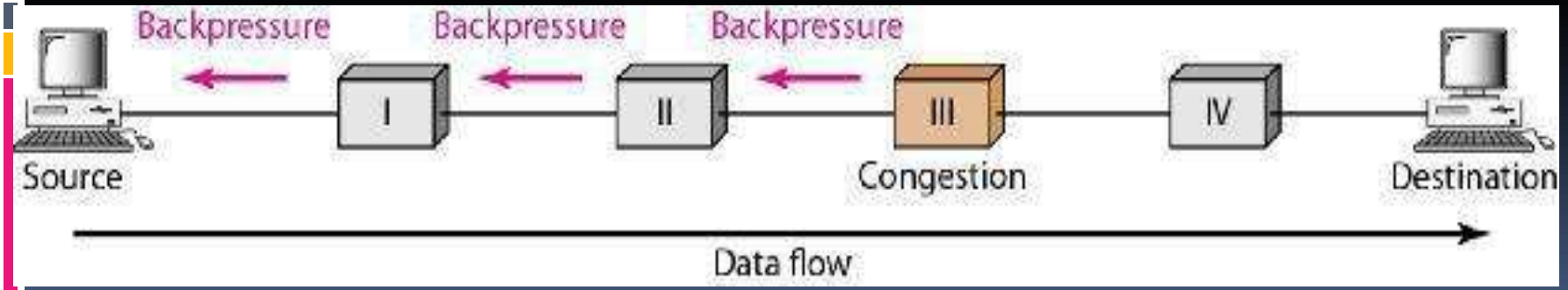
- **A) OPEN-LOOP CONGESTION CONTROL**
- In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.
- a) Retransmission Policy
- Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.

- b) Window Policy
- The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.

- c) Acknowledgment Policy
- The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.
- d) Discarding Policy
- A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.
- e) Admission Policy
- An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks..

- **CLOSED-LOOP CONGESTION CONTROL**
  Closed-loop congestion control
- Mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols.
- a) Backpressure: The technique of *backpressure* refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning.

- Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion.



- b) Choke Packet
- A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station
- c) Implicit Signaling
- In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms.

- d) Explicit Signaling
- The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke packet method.
- e) Backward Signaling
- A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.
- f) Forward Signaling
- A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion.

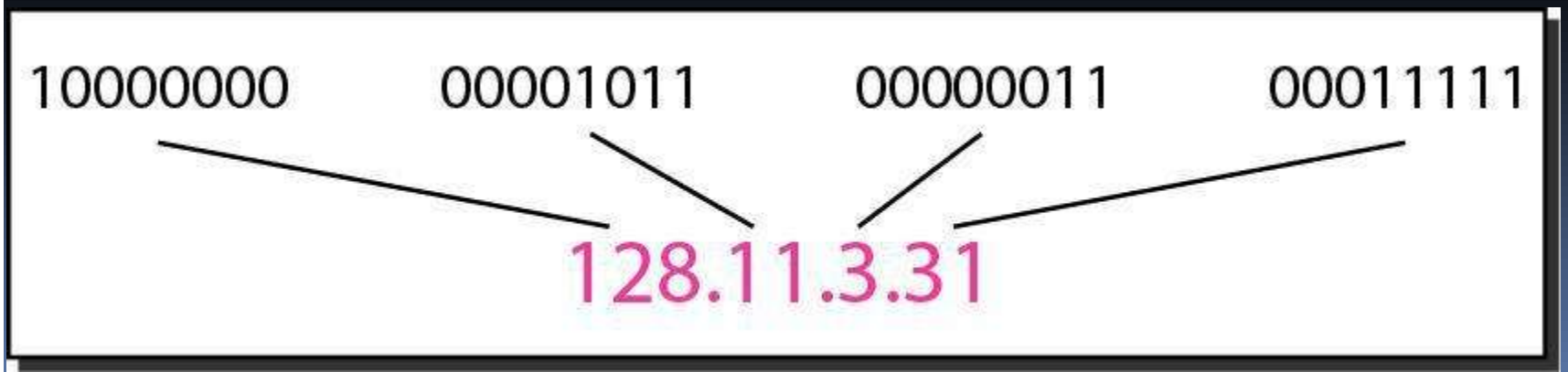
- **IPv4 ADDRESSING:**
- An IPv4 address is a 32-bit address that *uniquely* and *universally* defines the connection of a device (for example, a computer or a router) to the Internet. IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

- **ADDRESS SPACE**
- A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol.
- Notations
- There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal notation.
- Binary Notation
- In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation:
- 01110101 10010101 00011101 00000010

- Dotted-Decimal Notation
- To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation of the above address:

  117.149.29.2

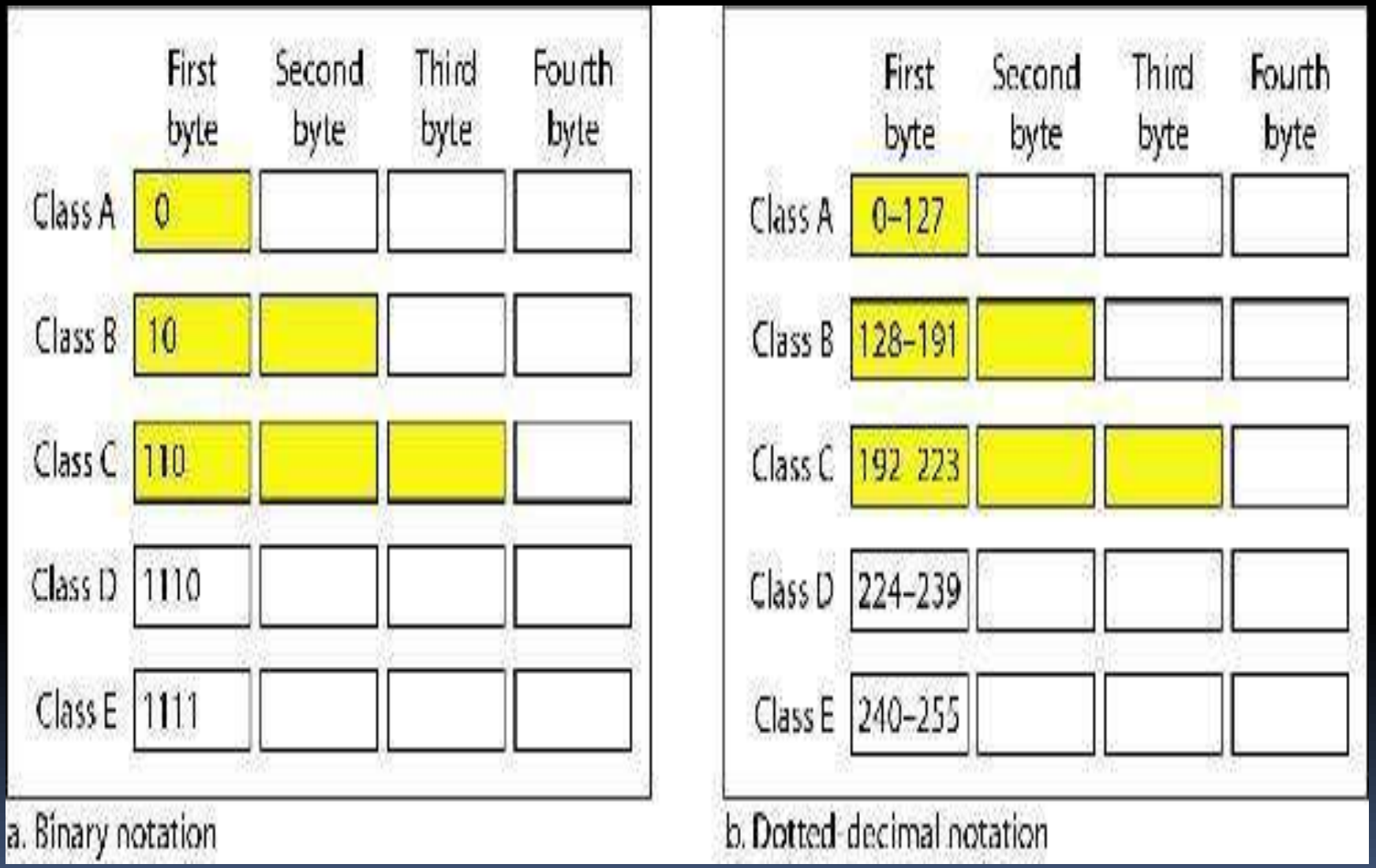
Below Fig shows an IPv4 address in both binary and dotted-decimal notation.



- **A) CLASSFUL ADDRESSING**

- IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing. Although this scheme is becoming obsolete, we briefly discuss it here to show therationale behind classless addressing. In classful addressing, the address space is divided into five classes: A, B, C, D,and E. Each class occupies some part of the address space.

- If the address is given in decimal-dotted notation, the first byte defines the class. Both methods are shown in Fig.


First byte
Second byte
Third byte
Fourth byte
Class A
0
Class B
10
Class C
110
Class D
1110
Class E
1111
a. Binary notation
First byte
Second byte
Third byte
Fourth byte
Class A
0–127
Class B
128–191
Class C
192 223
Class D
224–239
Class E
240–255
b. Dotted-decimal notation

- The notation is used in classless addressing, which we will discuss later. We introduce it here because it can also be applied to classful addressing.
- Subnetting
- During the era of classful addressing, subnetting was introduced. If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.
- Supernetting
- The time came when most of the class A and class B addresses were depleted; however, there was still a huge demand for midsize blocks.

- **B) CLASSLESS ADDRESSING**
- To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

- Address Blocks
- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses. The size of the block (the number of addresses) varies based on the nature and size of the entity. Restriction To simplify the handling of addresses, the Internet authorities impose three restrictions on classless address blocks:
- The addresses in a block must be contiguous, one after another.

- The number of addresses in a block must be a power of 2 (I, 2, 4, 8, ... ).

- The first address must be evenly divisible by the number of addresses.

## CONNECTING DEVICES:

- The communication media used to link devices to form a computer network include electrical cable (HomePNA, power line communication, G.hn), optical fiber (fiber-optic communication), and radio waves (wireless networking).
- Various devices are used to connect network of a computer The most common devices are:
- Routers
- Gateways
- Repeaters
- Bridges
- Hub
- Modem

- **A) ROUTER**
- Routers are devices which connect two are more networks that use similar protocol. A router consists of hard ware and software. Hard ware can be a computer is specific device. Software consists of special management program that controls flow of data between networks. Routers operate at a network layer of O.S.I model.
- **GATEWAYS**
- Gateways are devices which connect two are more networks that use different protocols. They are similar in function to routes but they are more powerful and intelligent devices. A gateway can actually convert data so that network with an application on a computers

- **C) REPEATERS**
- Repeaters are used within network to extend the length of communication. Data process through transmission media in the farm of waves or signals. The transmission media weaken signals that move through it.
- **BRIDGES**
- Bridges are used to connect similar network segments. A bridge does not pass or signals it receives. When a bridge receives a signal, it determines its destination by looking at its destination and it sends the signals towards it.

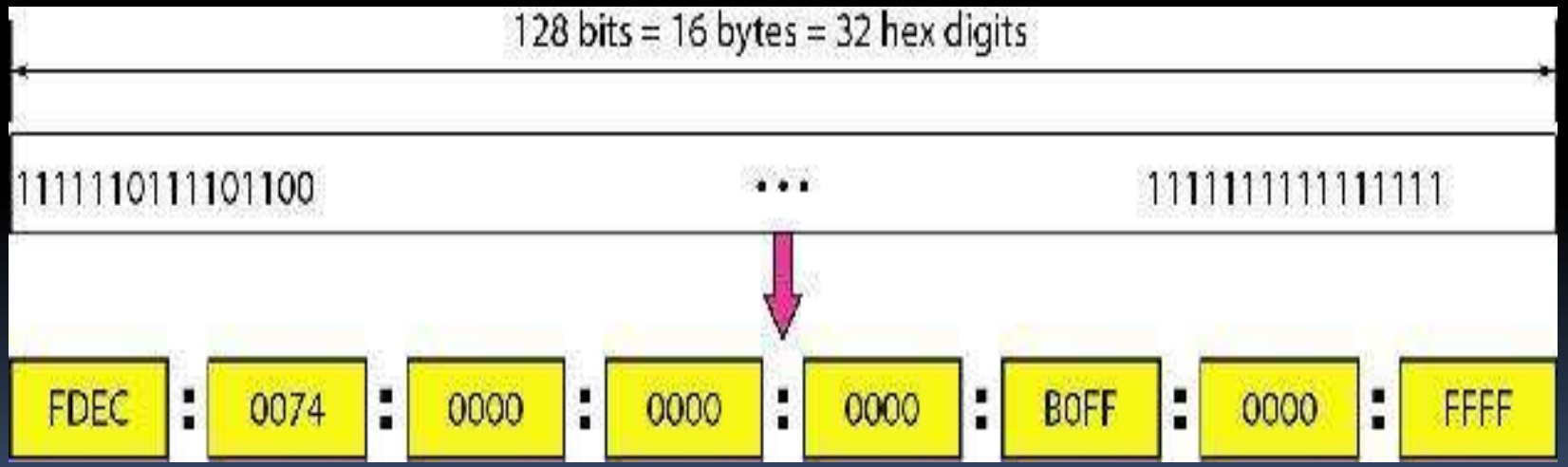
- **HUB**
- Hubs are basically multi ports repeaters for U.T.P cables. Some hubs have ports for other type of cable such as coaxial cable. Hubs range in size from four ports up to and for specific to the network types. These are some hubs which are

  I. Passive Hub
  II. Active Hub

  III. Switch/ Intelligent Hub
- **F) MODEM**
- The device that converts digital signals into analog signals and analog signals to digital signals is called Modem. The word modem stands for modulation and demodulation. The process of converting digital signals to analog signals is called modulation.

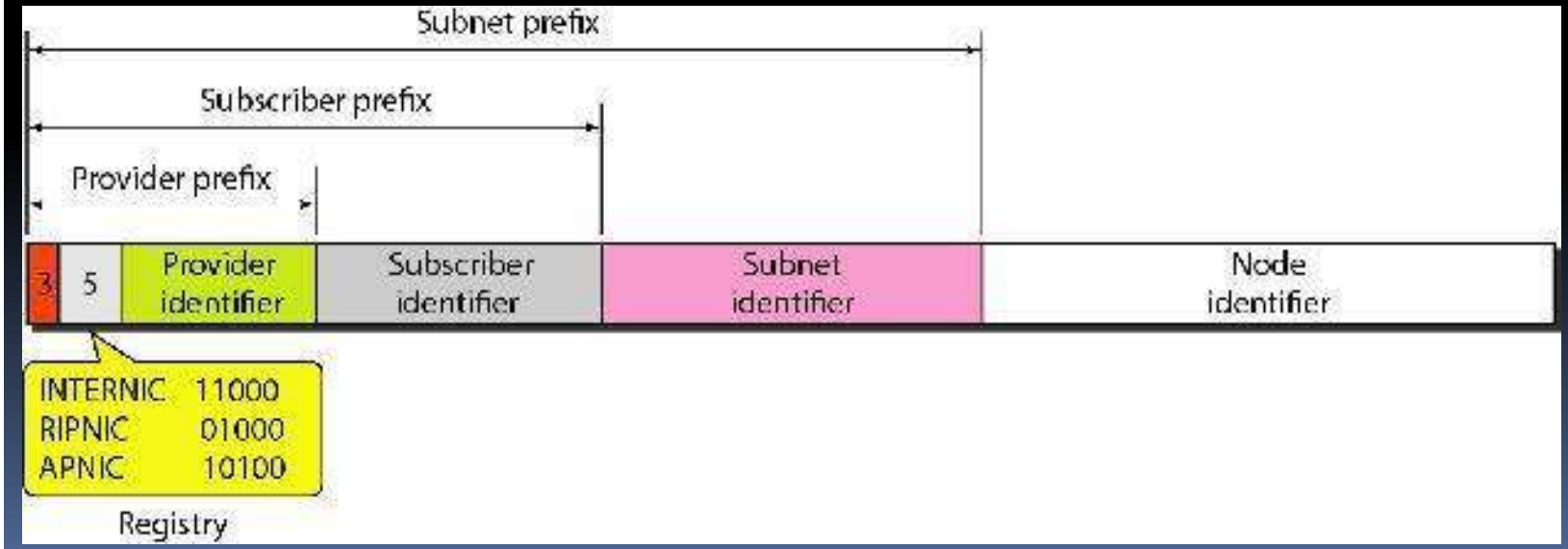
- **VIRTUAL LAN IPV6 ADDRESSES:**
- Despite all short-term solutions, such as classless addressing, Dynamic Host Configuration Protocol (DHCP), and NAT, address depletion is still a long-term problem for the Internet.
- This and other problems in the IP protocol itself such as lack of accommodation for real-time audio and video transmission, and encryption and authentication of data for some applications, have been the motivation for IPv6.
- Structure
- An IPv6 address consists of 16 bytes (octets); it is 128 bits long.

- Hexadecimal Colon Notation
- To make addresses more readable, IPv6 specifies hexadecimal colon notation. In this notation
- 128 bits is divided into eight sections, each 2 bytes in length.

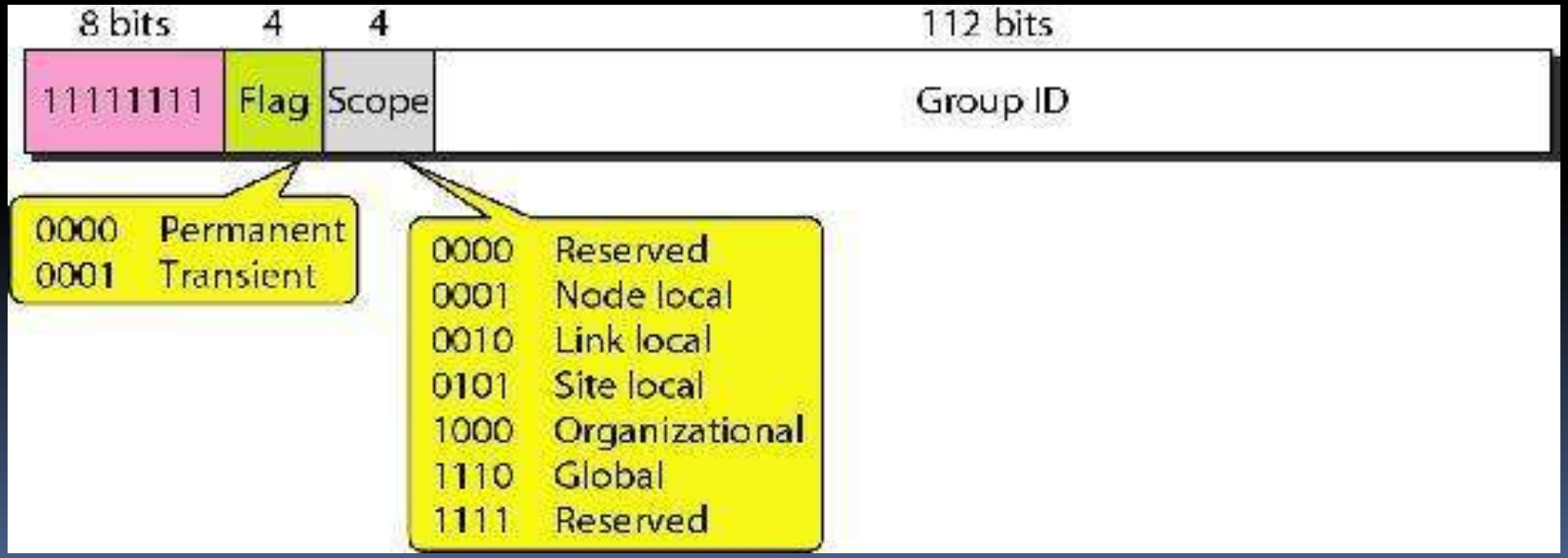


# A) UNICAST ADDRESSES

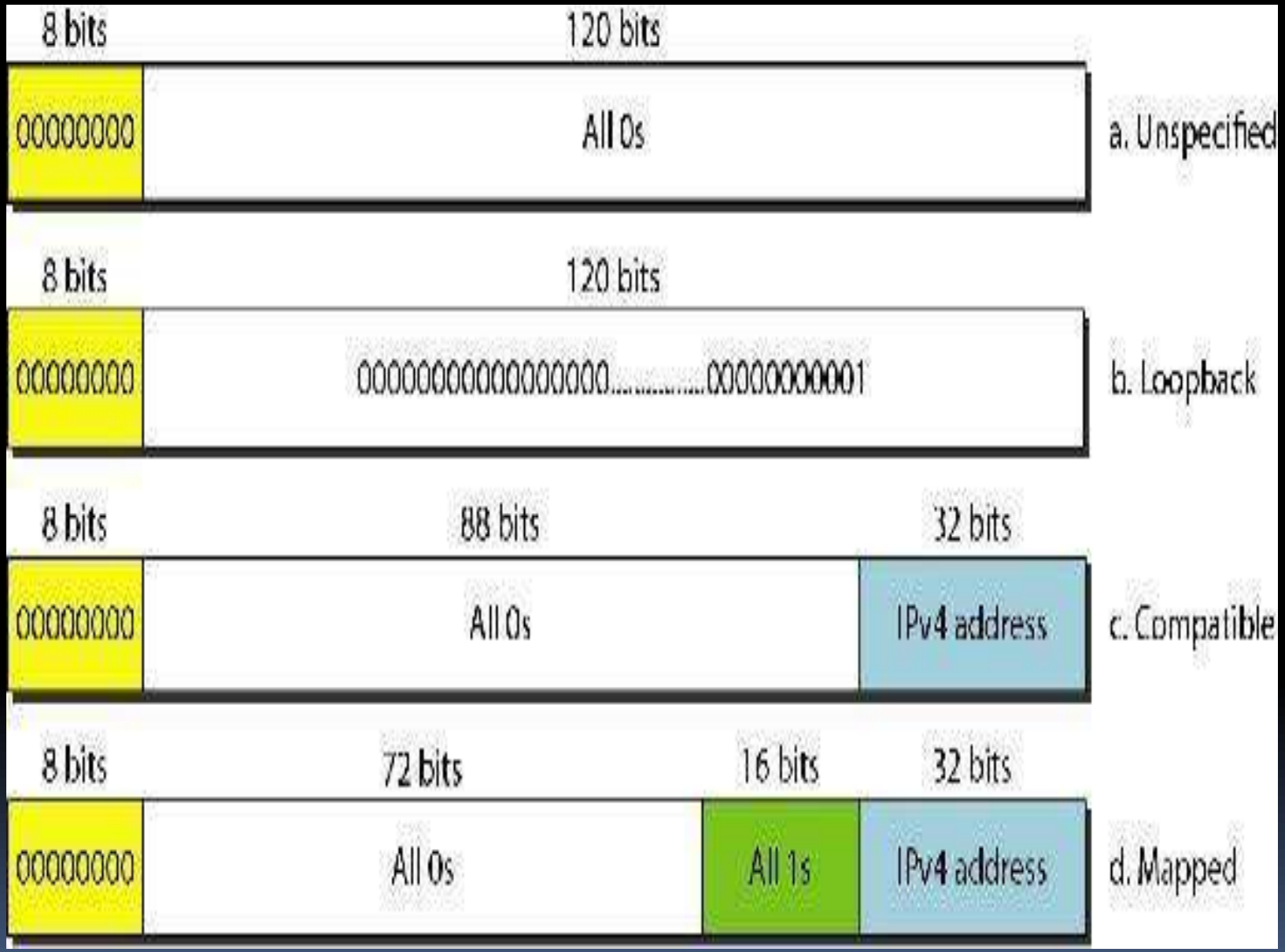
- A **unicast address** defines a single computer. The packet sent to a unicast address must be delivered to that specific computer. IPv6 defines two types of unicast addresses: geographically based and provider-based. The address format is shown in Fig.



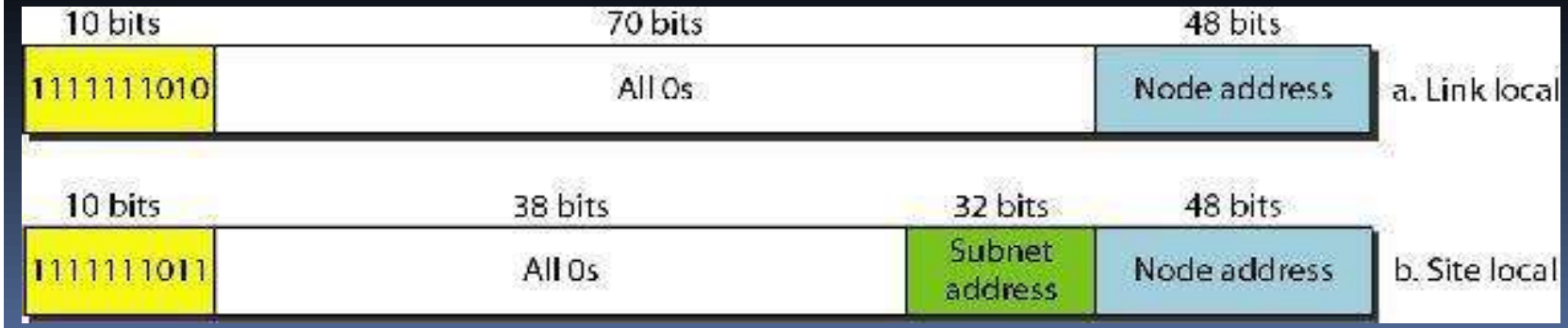
- **B) MULTICAST ADDRESSES**
- Multicast addresses are used to define a group of hosts instead of just one. A packet sent to a multicast address must be delivered to each member of the group. Fig. shows the format of a multicast address.



- **C) ANYCAST ADDRESSES**
- IPv6 also defines anycast addresses. An anycast address, like a multicast address, also defines a group of nodes. However, a packet destined for an anycast address is delivered to only one of the members of the anycast group, the nearest one (the one with the shortest route).
- **D) RESERVED ADDRESSES**
- Another category in the address space is the reserved address. These addresses start with eight Os (type prefix is oooooooo). A few subcategories are defined in this category, as shown in Fig.


8 bits
120 bits
00000000
All 0s
a. Unspecified
8 bits
120 bits
00000000
00000000000000000.....00000000001
b. Loopback
8 bits
88 bits
32 bits
00000000
All 0s
IPv4 address
c. Compatible
8 bits
72 bits
16 bits
32 bits
00000000
All 0s
All 1s
IPv4 address
d. Mapped

- **E) LOCAL ADDRESSES**
- These addresses are used when an organization wants to use IPv6 protocol without being connected to the global Internet. In other words, they provide addressing for private networks. Nobody outside the organization can send a message to the nodes using these addresses. Two types of addresses are defined for this purpose, as shown in Fig.

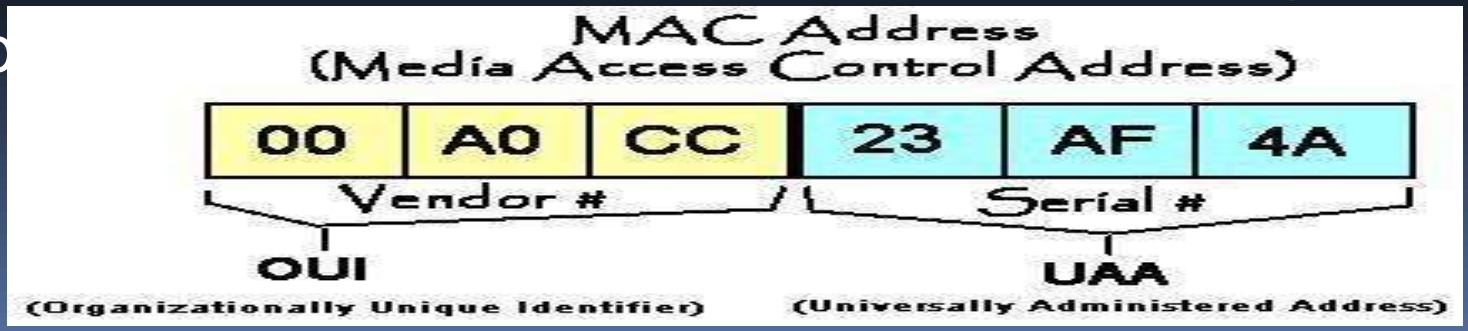


- **INTERNET PROTOCOL:**
- IP specifies the format of packets, also called *datagrams,* and the addressing scheme. Most networks combine IP with a higher-levelprotocol called *Transmission Control Protocol (TCP)*, which establishes a virtual connection between a destination and a source. IP by itself is something like the postal system.
- **A) IPv4**
- The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. Internet Protocol Version 4 (IPv4) is the fourth revision of the IP and a widely used protocol in data communication over different kinds of networks.

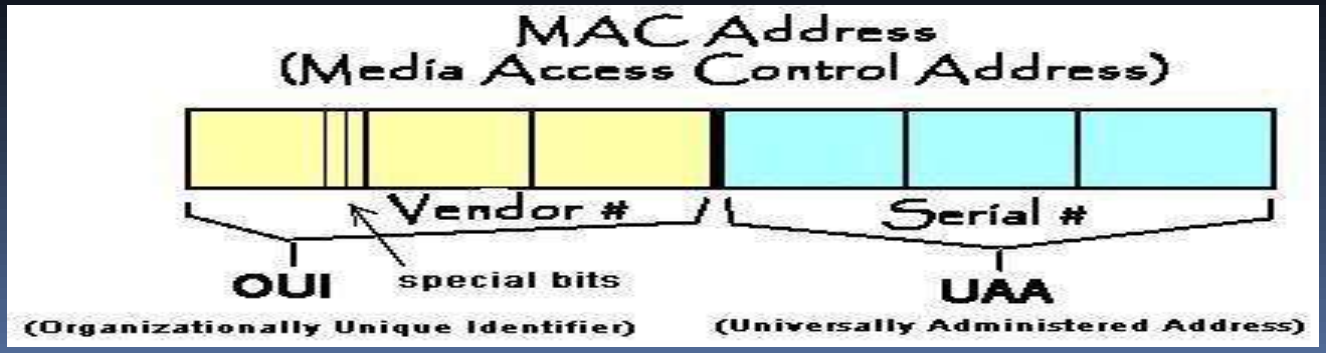
- IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices by providing identification for each device.
- IPv4 is based on the best -effort model. This model guarantees neither delivery nor avoidance of duplicate delivery; these aspects are handled by the upper layer transport. IPv4 is defined and specified in IETF publication RCF 791. It is used in the packet-switched link layer in the OSI model.
- IPv4 uses 32-bit addresses for Ethernet communication in five classes, named A, B, C, D and E.

- **IPv6**
- The network layer protocol in the TCPIIP protocol suite is currently IPv4 (Internetworking Protocol, version 4). IPv4 provides the host -to-host communication between systems in the Internet. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s.
- IPv4 has some deficiencies (listed below) that make it unsuitable for the fast-growing Internet.
  - Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.

- **HARDWARE ADDRESSING VERSUS IP ADDRESSING:**
- IP networks require two types of addresses : MAC and IP. Each station stores it's MAC address and IP address in it's own IP stack. It stores MAC and IP addresses of other stations on it's LAN or subnet in the ARP cache.
- **MAC ADDRESS (Layer2 - Data Link layer)**
- The hard coded 48-bit (6 byte) address, burned into the ROM of the NIC (Network Interface Card) - it is also called the *Hardware address*, or *Ethernet address*. They are expressed as six pairs of hexadecimal digits. The fo NIC :

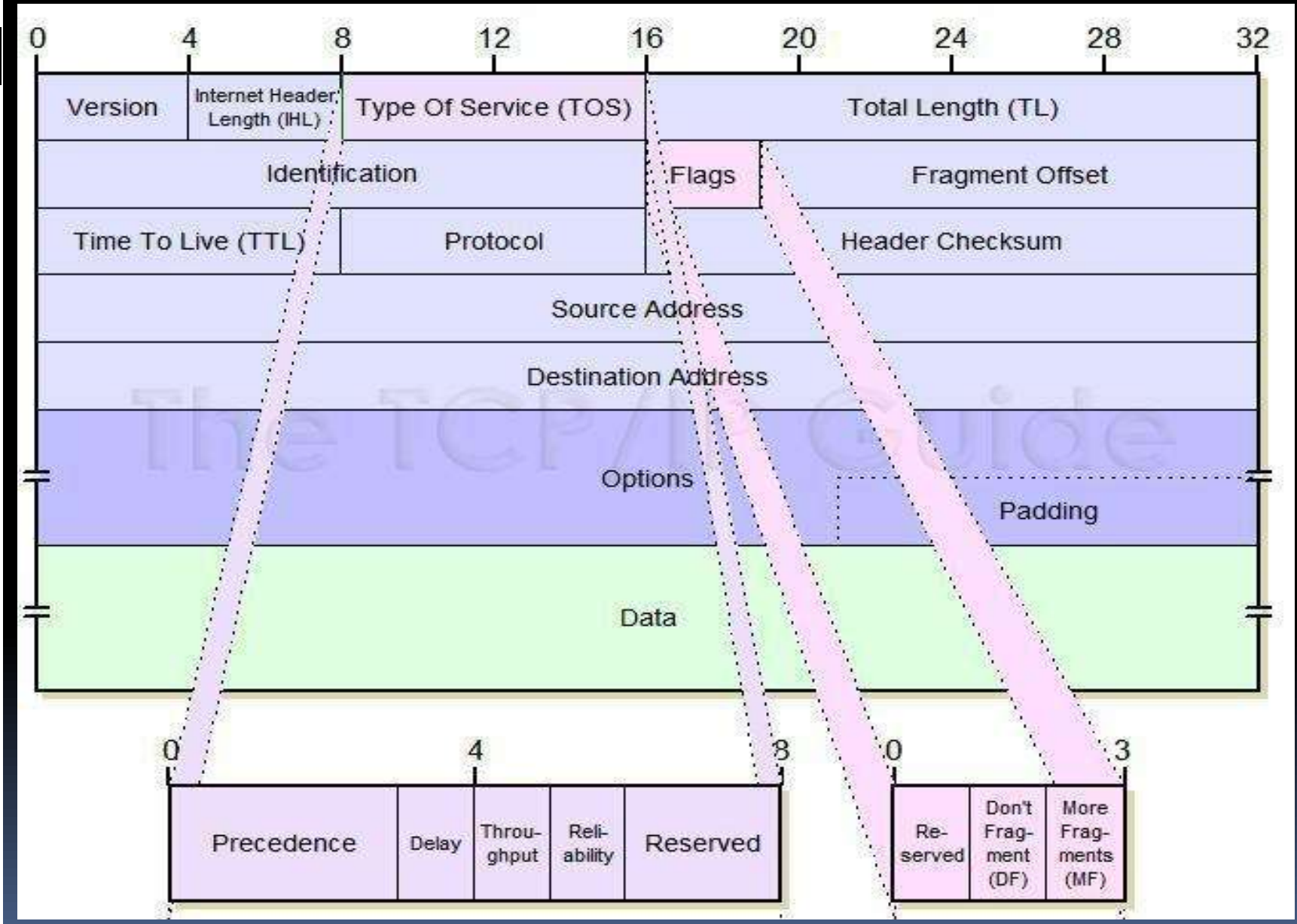


- **B) SPECIAL BITS**
- There are two special bits in a MAC address. They are the first two bits sent out on the wire in the MAC - the two least significant bits.
- They are shown as the last bits of the first byte of the MAC. Ethernet bytes are transmitted big-endian but the bits are transmitted little-endian.
- The first bit (bit 0) is used by Ethernet II. The second bit is used by IEEE 802.3.



- **The IP address (layer 3 - Network layer)**
- A 32-bit (4 byte) software stored addresses, and is assigned to represent the same NIC as MAC address represents. The 32-bit IP address is like a shorter nickname for the 48-bit MAC address.
- IP from MAC addresses is this:
- Direct-connected transmission uses Layer 2 - MAC addresses for frame delivery.
- routed transmission uses Layer 3 - IP addresses for packet delivery

- **IP DATAGRAM:**
- Data transmitted over an internet using IP is carried in messages called *IP datagrams*.
- Like all network protocol messages, IP uses a specific format for its datagrams.
- The IPv4 datagram is conceptually divided into two pieces: the *header* and the *payload*.
- The header contains addressing and control fields, while the payload carries the actual data to be sent over the internetwork.
- Even though IP is a relatively simple, connectionless, "unreliable" protocol.


0
4
8
12
16
20
24
28
32
Version
Internet Header Length (IHL)
Type Of Service (TOS)
Total Length (TL)
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding
Data
0
4
8
Precedence
Delay
Throu-ghput
Reli-ability
Reserved
0
3
Re-served
Don't Frag-ment (DF)
More Frag-ments (MF)

# UNIT-5

# TRANSPORT LAYER PROTOCOL

# TRANSPORT LAYER PROTOCOL

•The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called *node-to-node delivery.*

•The network layer is responsible for delivery of datagrams between two hosts. This is called *host-to-host delivery.*

• Communication on the Internet is not defined as the exchange of data between two nodes or between two hosts.

• Real communication takes place between two processes (application programs).

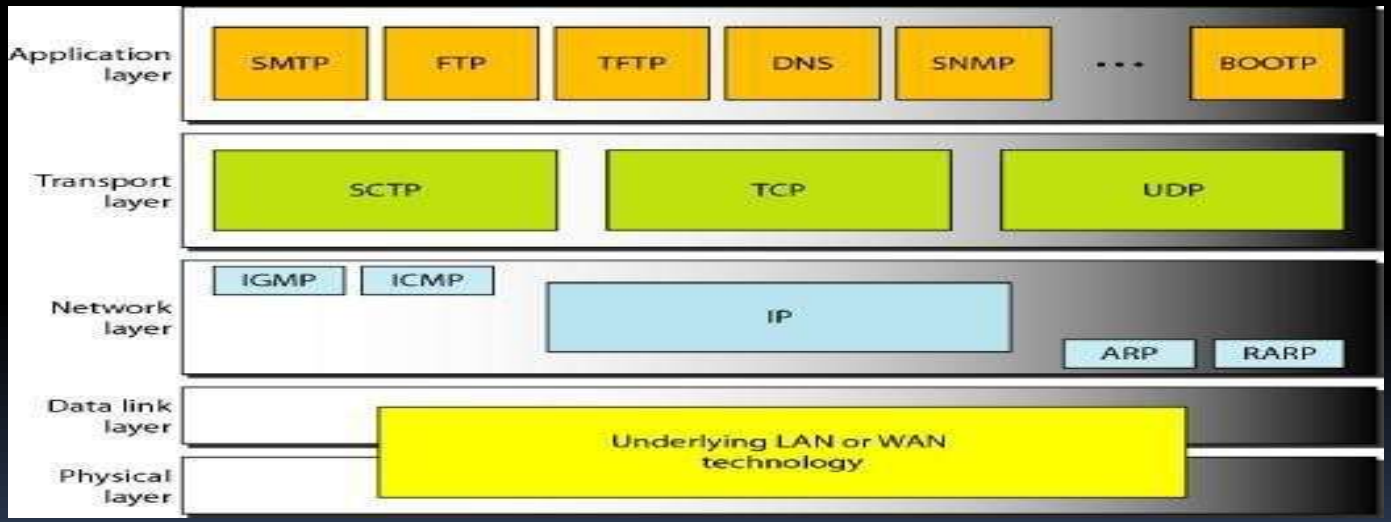



Fig.5.1 Position of UDP, TCP, and SCTP in TCP/IP suite

# 1. 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. Also, it performs very limited error checking.

| *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) |

Table 5.1 Well Known Ports used in UDP

# USER DATAGRAM

•UDP packets, called user datagrams, have a fixed-size header of 8 bytes.

- UDP is a very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP. Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or SCTP.

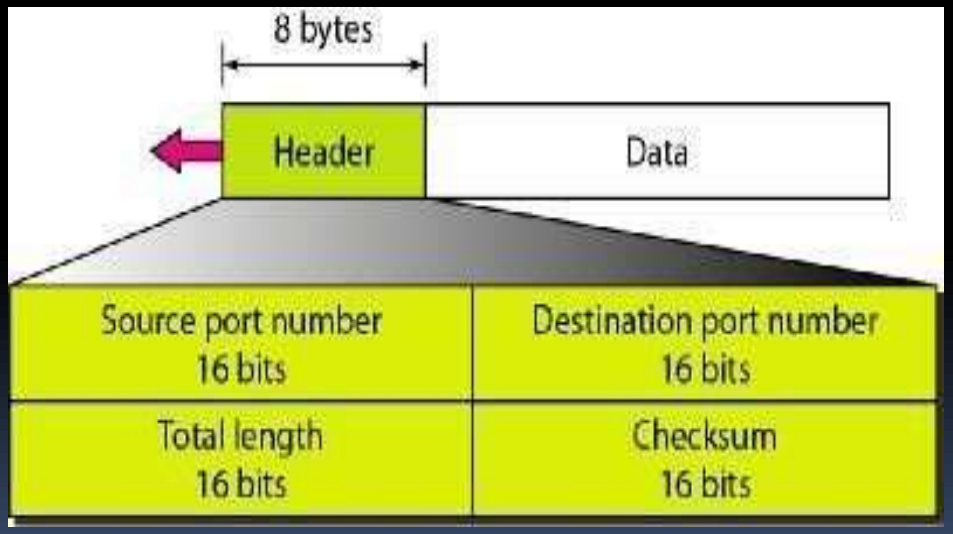



Fig. 5.2 User datagram format

**Source port number.**

This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

**destination port number**

This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.

**Length.**

This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes.

**Checksum.**

This field is used to detect errors over the entire user datagram (header plus data)

# UDP Operation

## Connectionless Services

As mentioned previously, UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program. The user datagrams are not numbered.

## Flow and Error Control

UDP is a very simple, unreliable transport protocol. There is no flow control and hence no window mechanism. The receiver may overflow with incoming messages. There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded. The lack of flow control and error control means that the process using UDP should provide these mechanisms.

## Encapsulation and Decapsulation

To send a message from one process to another, the UDP protocol encapsulates and decapsulates

messages in an IP datagram.

## Queuing

We have talked about ports without discussing the actual implementation of them. In UDP, queues are associated with ports

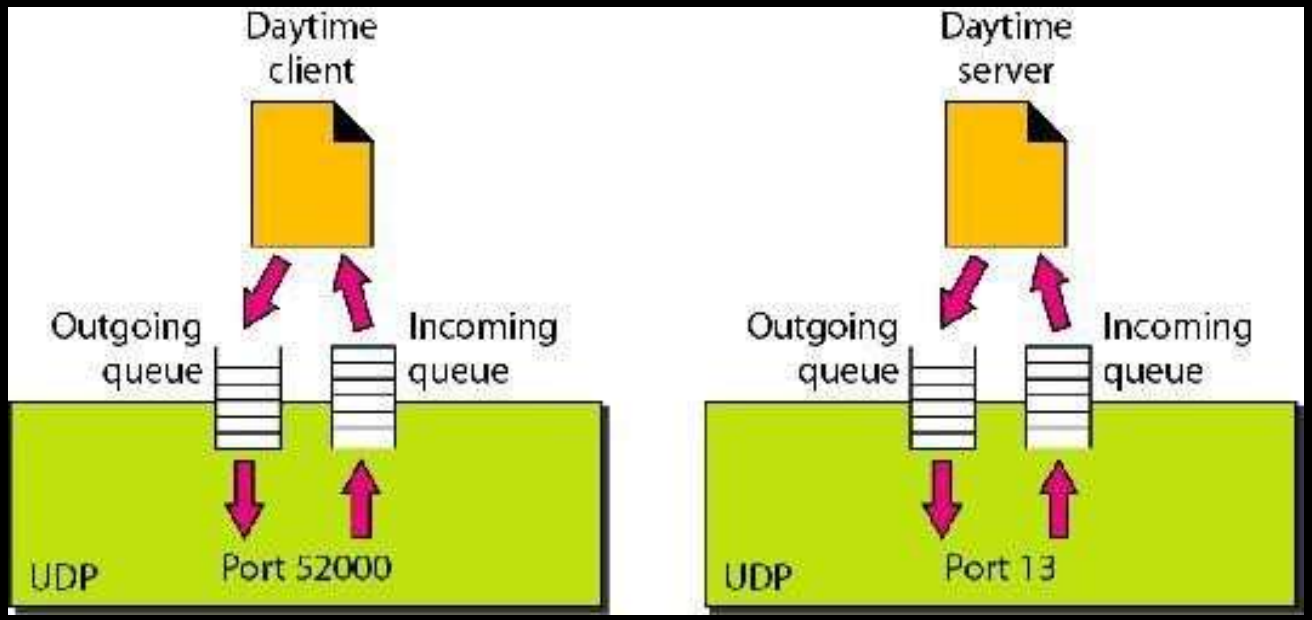



Fig. 5.3 Queue in UDP

## Use of UDP

The following lists some uses of the UDP protocol:

- UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FrP that needs to send bulk data.
- UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.
- UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- UDP is used for management processes such as SNMP .
- UDP is used for some route updating protocols such as Routing Information Protocol (RIP)

The second transport layer protocol we discuss in this chapter is called Transmission Control Protocol (TCP). TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level. In brief, TCP is called a *connection-oriented, reliable* transport protocol. It adds connection-oriented and reliability features to the services of IP.

## Connection-Oriented Service

TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

- The two TCPs establish a connection between them.
- Data are exchanged in both directions.
- The connection is terminated.

- **TCP- Transmission Control Protocol**
- The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

- **TCP Services:**
- TCP offers following services to the processes at the application layer:
- Stream Delivery Service
- Sending and Receiving Buffers
- Bytes and Segments
- Full Duplex Service
- Connection Oriented Service
- Reliable Service

# Features:

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.
- Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.
- TCP is a reliable and connection oriented protocol.

## Architecture of ATM:

ATM is a cell-switched network. The user access devices, called the endpoints, are connected through a user-to-network interface (UNI) to the switches inside the network. The switches are connected through network-to-network interfaces (NNIs). Figure 5.8 shows an example of an ATM network.

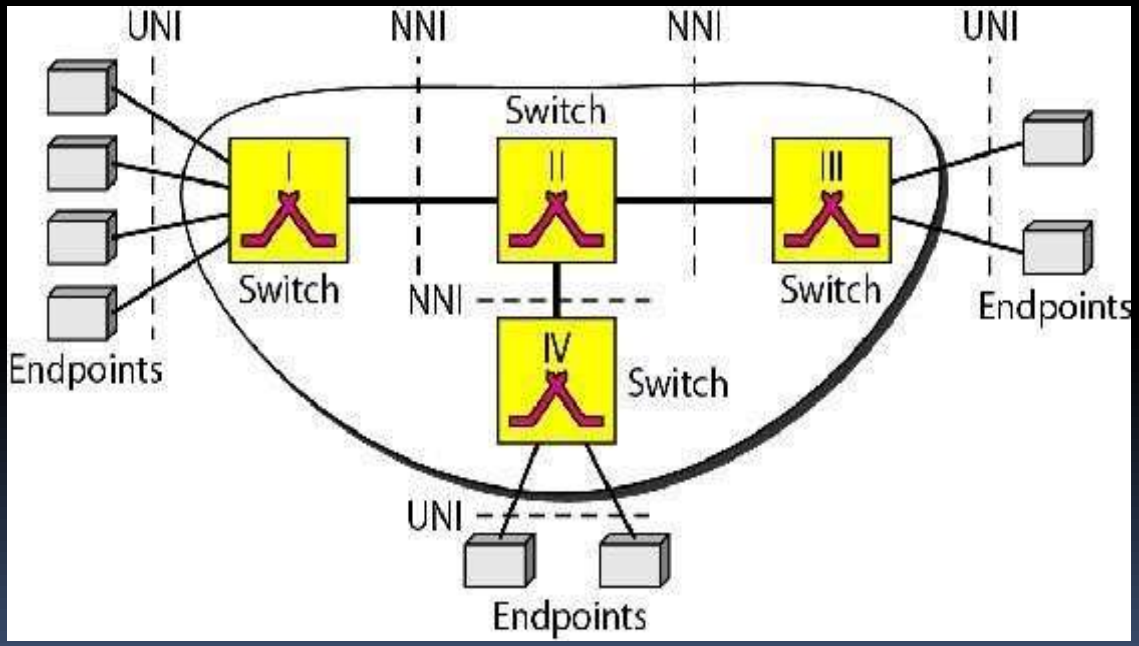



**Fig 5.8 Architecture of an ATM network**

## ATM LAYERS:

The ATM standard defines three layers. They are, from top to bottom, the application adaptation layer, the ATM layer, and the physical layer. The endpoints use all three layers while the switches use only the two bottom layers.

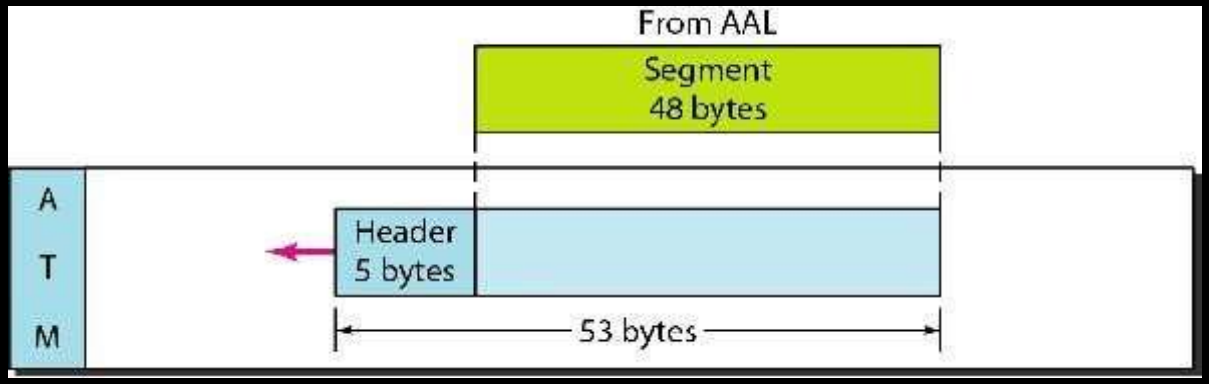



Fig. 5.10 ATM Layer

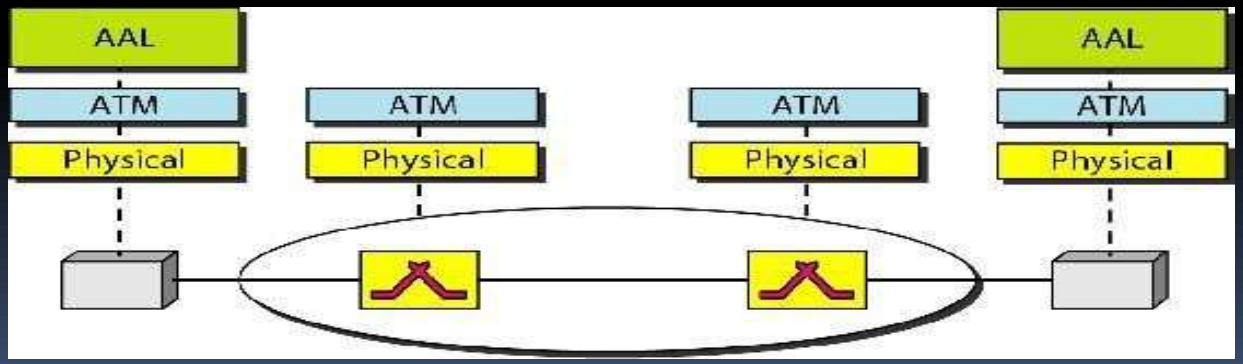



Fig. 5.11 ATM layers in endpoint devices and switches

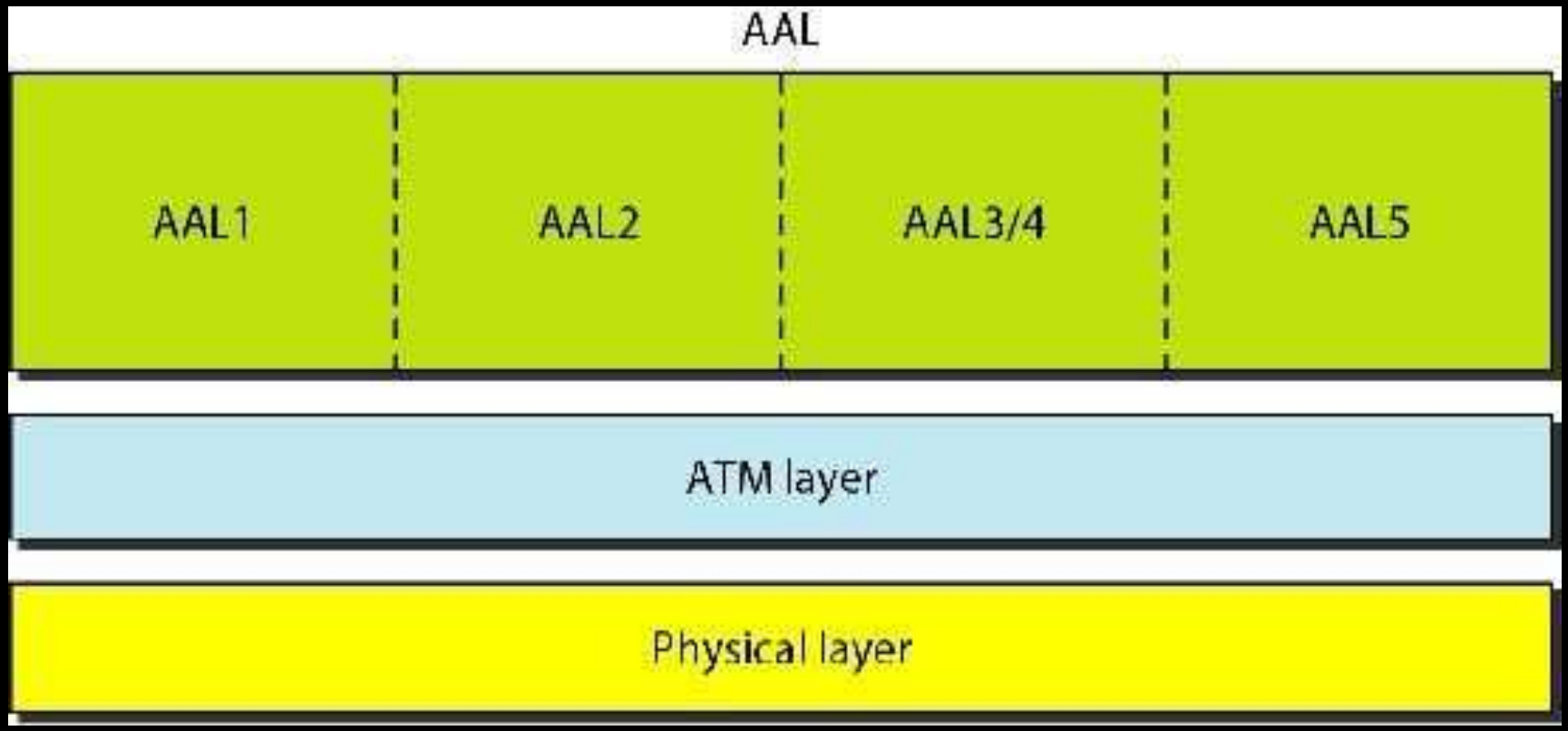



Fig. 5.12 ATM Layer in detail

## CRYPTOGRAHY

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. But it is important to note that while cryptography is *necessary* for secure communications, it is not by itself *sufficient*.

### The Purpose of Cryptography

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

## Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms are (Figure 5.13):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

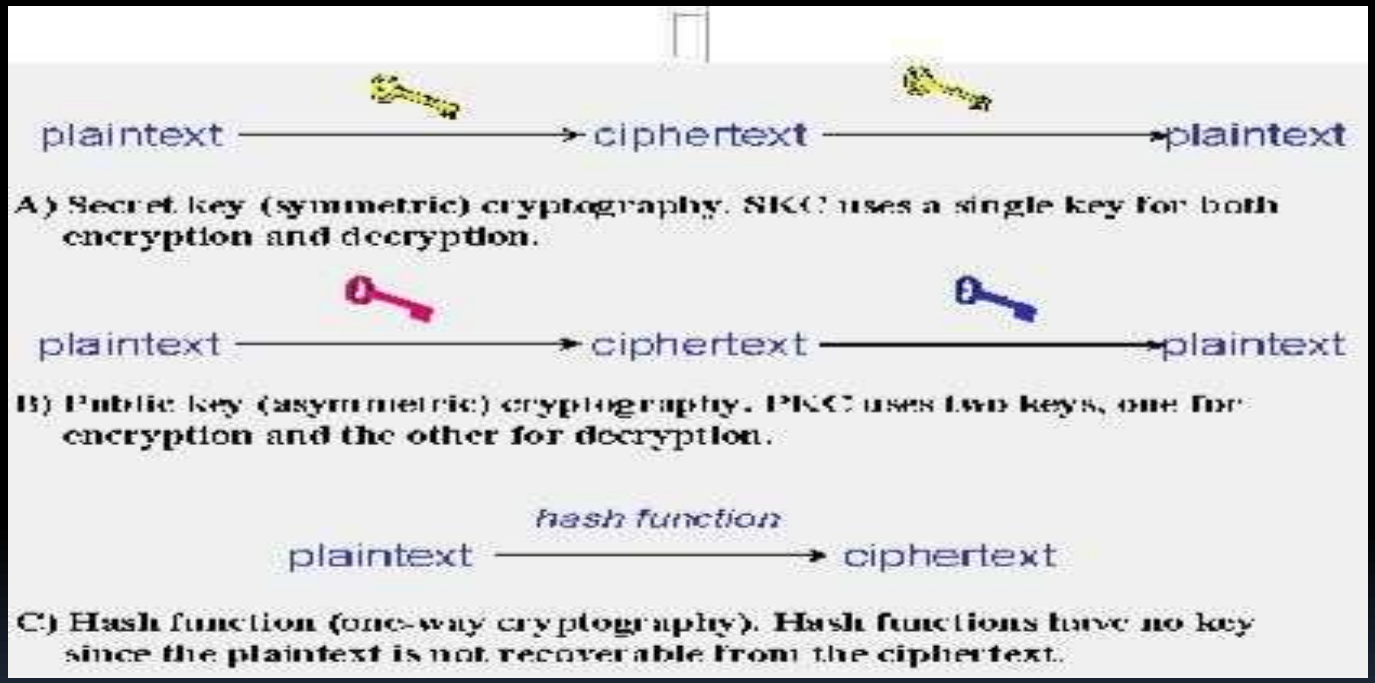



**Fig 5.13: Three types of cryptography: secret-key, public key, and hash function**

## Network security

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

## Types of Network Security Devices

**Active Devices**

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

**Passive Devices**

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

**Preventative Devices**

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

**Unified Threat Management (UTM)**

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

- # Network Security:
- SECURITY SERVICES:
- Network security can provide one of the five services.
- Four of these services are related to the message exchanged using the network: message confidentiality, integrity, authentication, and no repudiation.
- The fifth service provides entity authentication or identification.
- Message Confidentiality:
- Message confidentiality or privacy means that the sender and the receiver expect confidentiality.
- The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage.
- When a customer communicates with her bank, she expects that the communication is totally confidential.

- Message Integrity:
- Message integrity means that the data must arrive at the receiver exactly as they were sent.
- There must be no changes during the transmission, neither accidentally nor maliciously.
- As more and more monetary exchanges occur over the Internet, integrity is crucial.

- Message Authentication:
- Message authentication is a service beyond message integrity.
- In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

- Message Nonrepudiation:
- Message non repudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send.
- For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.
- Entity Authentication:
- In entity authentication (or user identification) the entity or user is verified prior to access to the system resources (files, for example).
- For example, a student who needs to access her university resources needs to be authenticated during the logging process.
- This is to protect the interests of the university and the student.