Sub.: Computer Networks (CN)
Code : BCE4405

Examination Scheme: IE1: 10 Marks, IE2: 10 Marks,
MTE: 30 Marks
ETE: 50 Marks

- Lectures : 3 Hrs./ week

- Course Objectives:

1. To understand the fundamental concepts of networking standards, protocols and technologies.
2. To learn different techniques for framing, error control, flow control and routing.
3. To learn the role of protocols at various layers in the protocol stacks.
4. To learn network programming.
5. To develop an understanding of modern network architectures from a design and performance perspective.

Course Outcomes:

After learning the course, the students should be able to:

1. Comprehend various transmission medium and networking devices.
2. Compare various networking protocols and algorithms.
3. Illustrate layered architecture from the perspective of wired and wireless networking principles.
4. Determine various error control techniques in layered architecture.
5. Determine various flow control techniques in layered architecture.
6. Distinguish various addressing mechanisms of different layers of TCP/IP model.

- **Text books:**

1. Andrew S. Tanenbaum, “Computer Networks”, Pearson Education India,6 th Edition, 2021 ISBN: 9780136764052, 0136764053.

2. Fourauzan B., "Data Communications and Networking", 5th Edition, Tata McGraw- Hill Publications, 2013 ISBN: 1259064751 · 9781259064753.

- **References Books:**

1. Kurose, Ross , “Computer Networking a Top-Down Approach Featuring the Internet”, 8/E, 2021, ISBN-10: 0136681557, ISBN-13: 9780136681557, 2021, Pearson.

2. Matthew S. G, “802.11 Wireless Networks”, O,,Reilly publications,3 rd Edition, 2017, ISBN: 81-7656-992-5.

Unit – 1

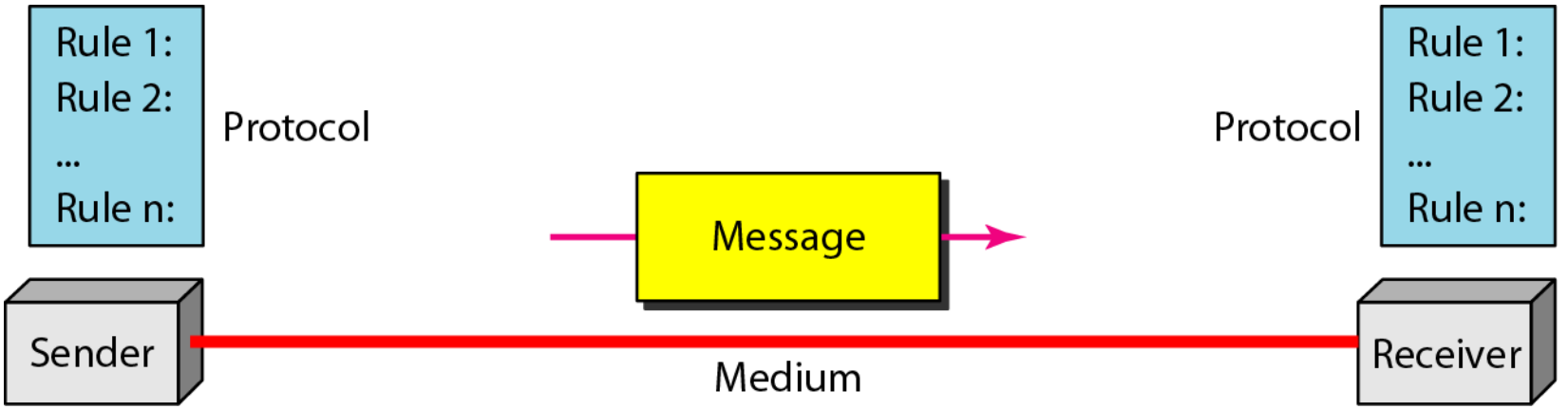
Physical Layer

Prepared By : Prof. Atul Pawar , PCCOE, Nigdi

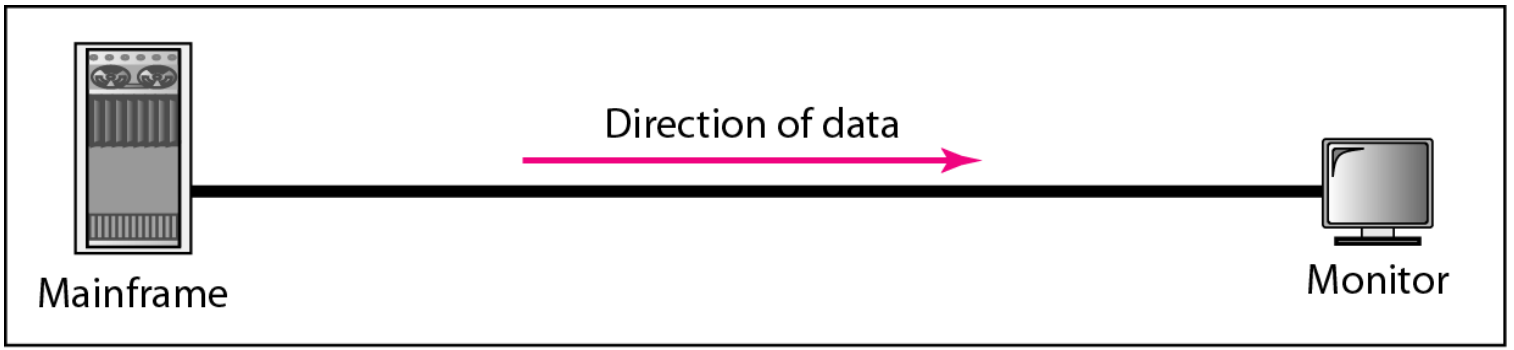
BASICS OF DATA COMMUNICATIONS

- *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.*
- *Data Representation: Text, Image, Audio, Video*

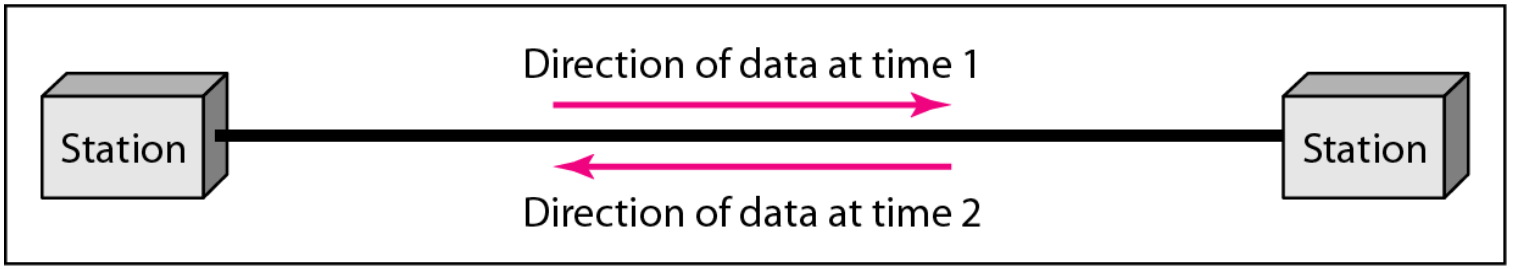
Data Components



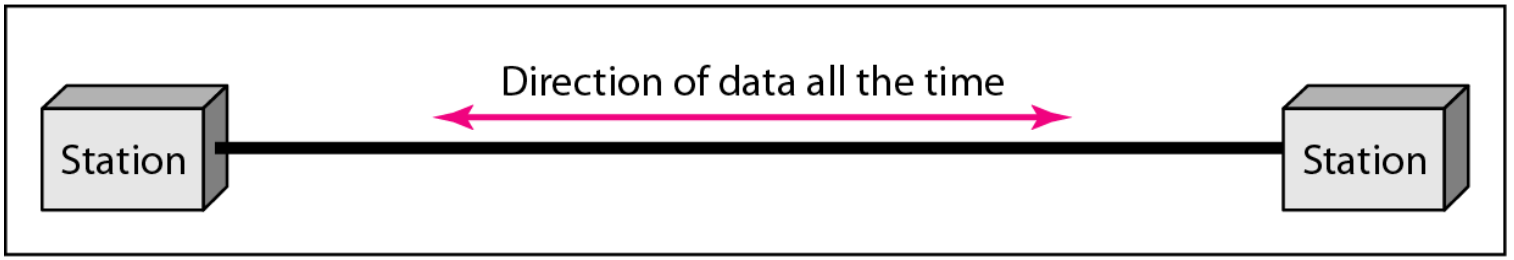
Data flow (simplex, half-duplex, and full-duplex)



a. Simplex



b. Half-duplex



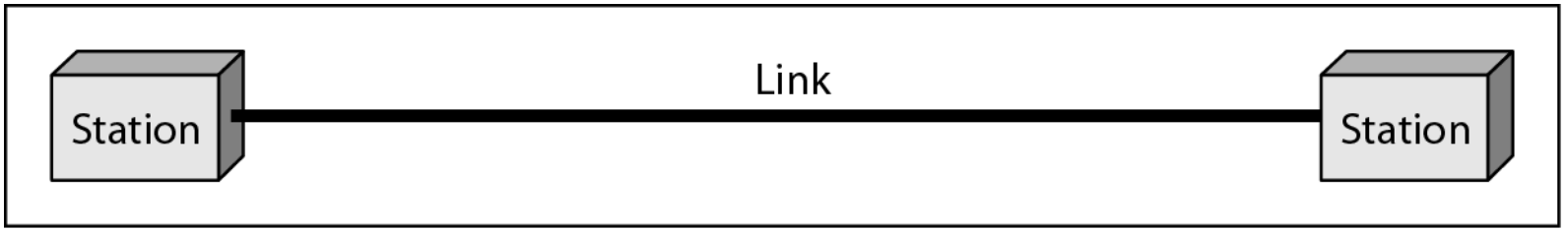
c. Full-duplex

NETWORK

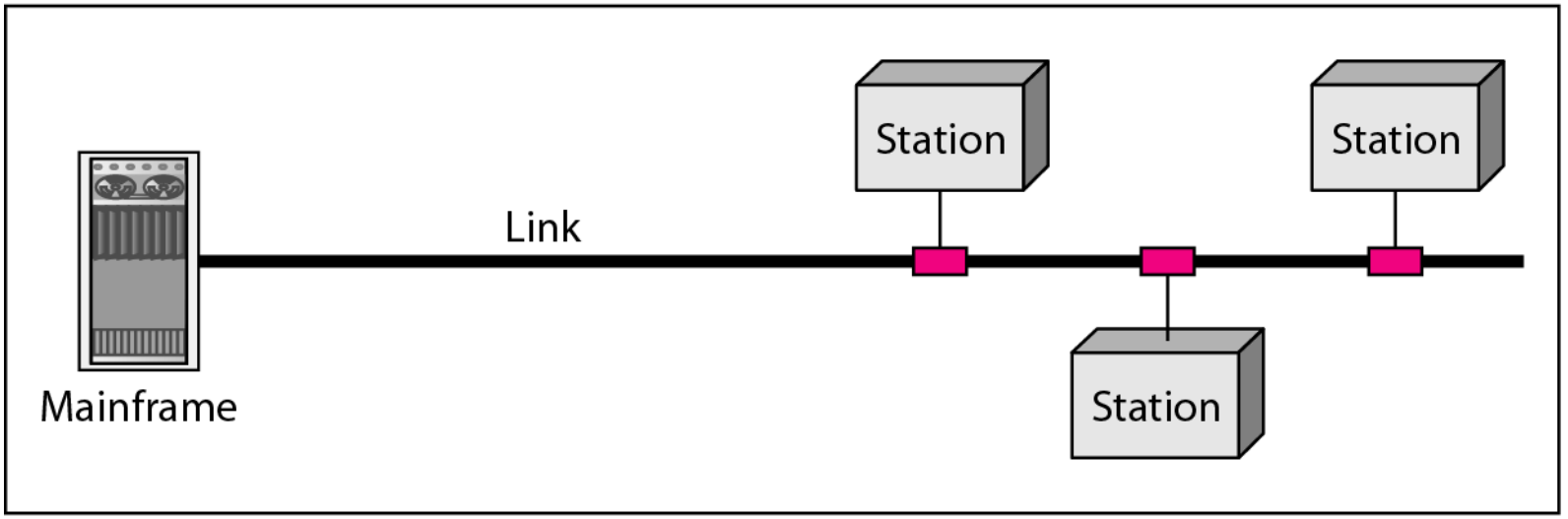
- *A network is a set of devices (nodes) connected by communication links.*

- *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.*

Types of connections: point-to-point and multipoint



a. Point-to-point



b. Multipoint

Communication System

Elements of a Communication System

- The basic elements are : Source, Transmitter, Channel, Receiver and Destination.

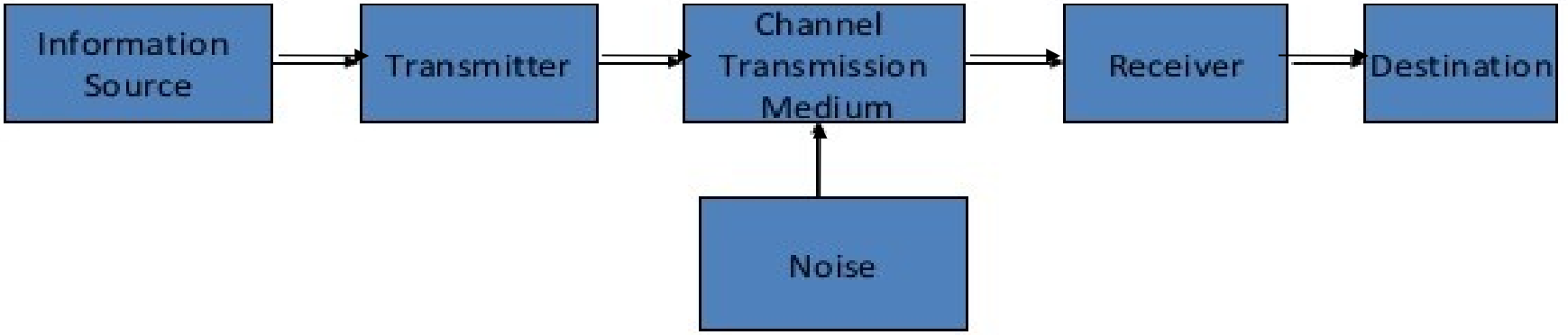


Figure : Basic Block Diagram of a Communication System

Local Area Network

- *A LAN is a network that is used for communicating among computer devices, usually within an office building or home*
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users
- Is limited in size, typically spanning a few hundred meters, and no more than a mile
- Is very fast, with speeds from 10 Mbps to 10 Gbps
- Requires very little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN's or WAN's.

LAN Basics

- LAN's can either be made wired or wireless.
- Twisted pair, coax or fiber optic cable can be used in wired LAN's
- Nodes in a LAN are linked together with a certain *topology*:Bus,Ring,Star,Mesh etc.
- A *node* is defined to be any device connected to the network: computer,printer etc.
- A *Hub/Switch* is a networking device that connects multiple segments of the network together
- A *Network Interface Card* (NIC) is the circuit board that is used to connect computers to the network. In most cases, this is an *Ethernet* card plugged in a computer's motherboard
- The *Network Operating System* (NOS) is the software that enables users to share files and hardware and communicate with other computers.
  - Eg. of NOS include: Windows XP, Windows NT, Sun Solaris, Linux, etc..
- Resource sharing in a LAN is accomplished with different *access methods*:
  - Token based access
  - CSMA/CD

Types of LAN’s

- The three most popular types of LAN’s are:
  - Token ring
  - Ethernet
  - FDDI (Fiber Distributed Data Interface)

Advantages of LAN

- Speed
- Cost
- Security
- E-mail
- Resource Sharing

Disadvantages of LAN

- Requires Administrative Time
- File Server May Fail
- Cables May Break

Metropolitan Area Network (MAN)

• A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.

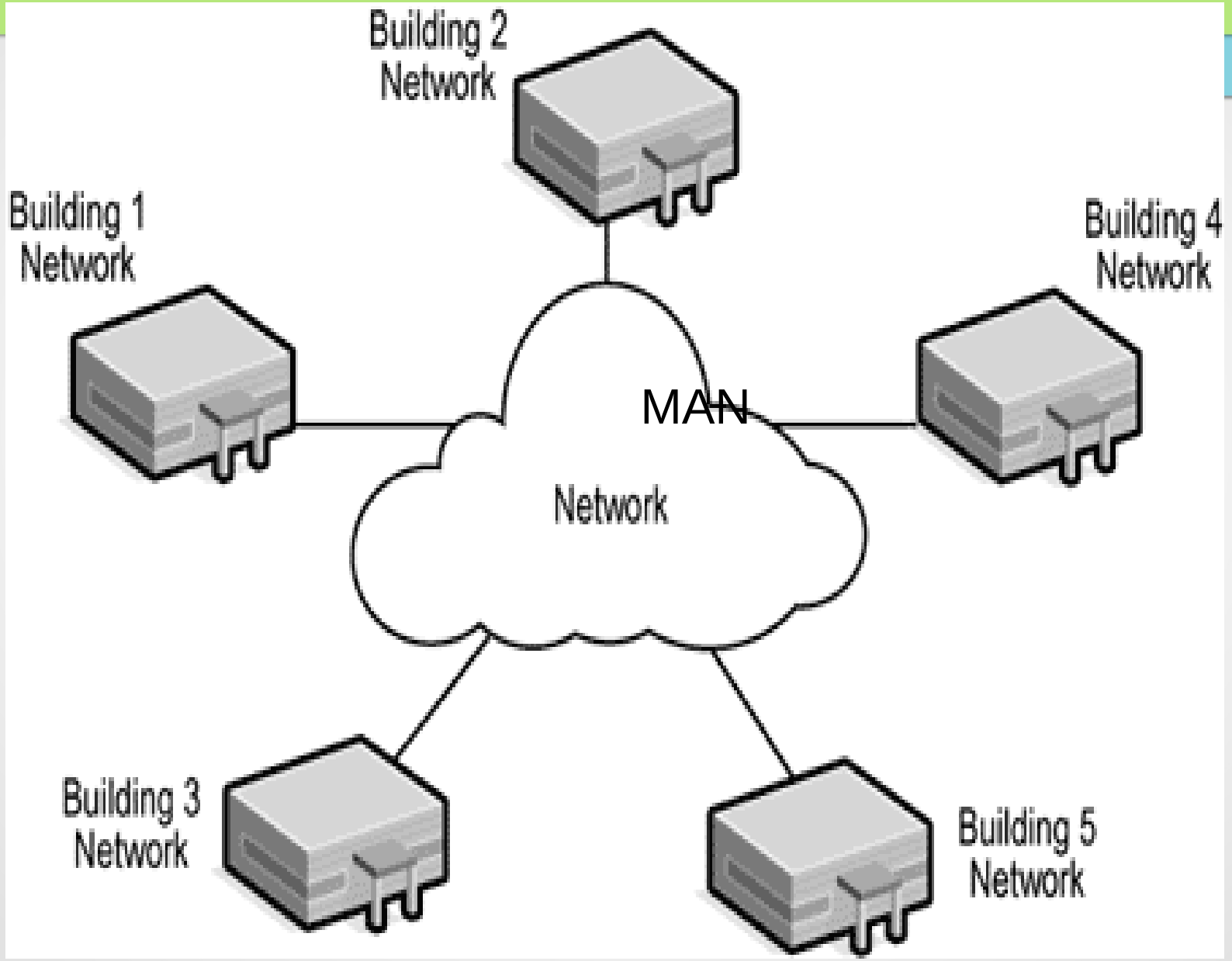
• A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.

• A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.

A MAN often acts as a high speed network to allow sharing of regional resources.

• A MAN typically covers an area of between 5 and 50 km diameter.

• Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.


Building 2
Network
Building 1
Network
Building 4
Network
MAN
Network
Building 3
Network
Building 5
Network

Types of MAN (metropolitan Area Network) Technologies

Most widely used technologies to develop a MAN network are :

- 1. FDDI (fiber distribution data interface),
- 2. ATM (Asynchronous Transfer Mode)
- 3. SMDS (switched multi megabit data service).

Advantages

Increases the efficiency of handling data.

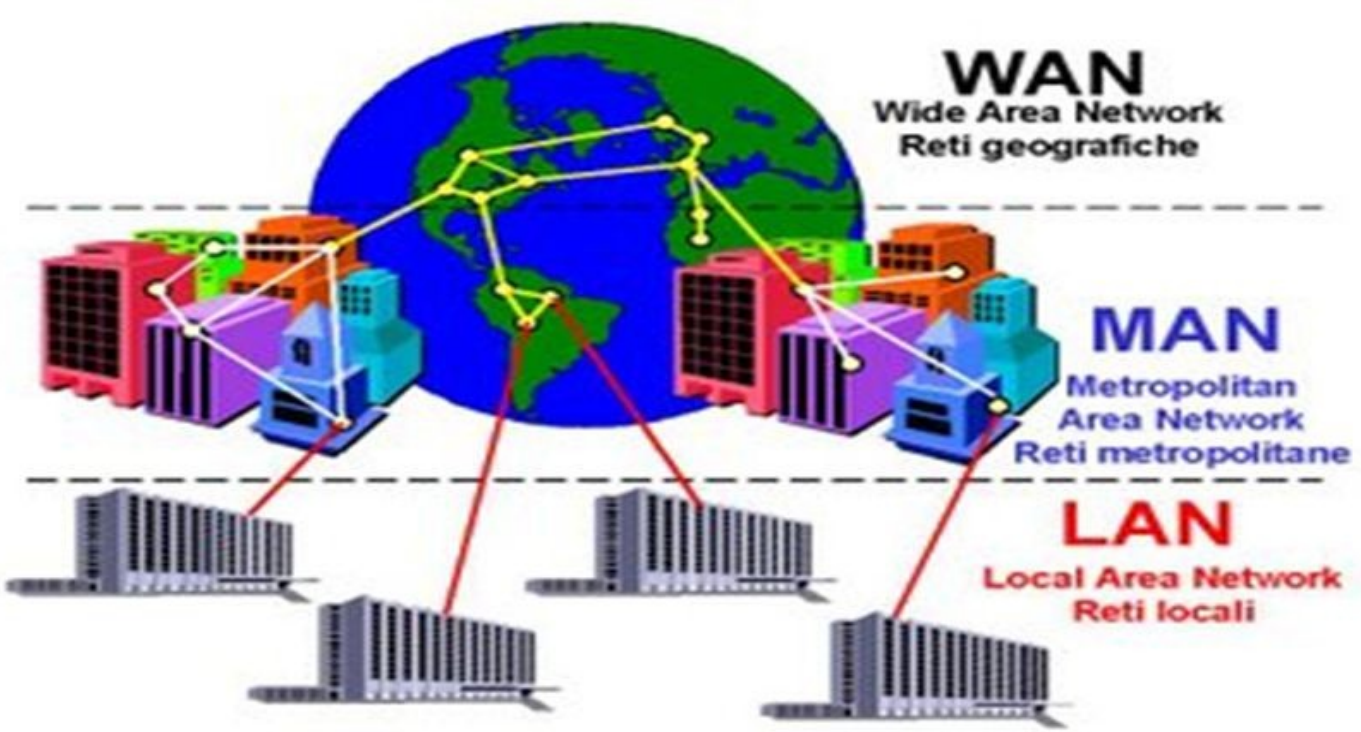
- ✓ Increase the speed of transferring data.
- ✓ Saves the cost attached to establish a wide area network.
- ✓ Cost effective by Sharing of resources such as printers.
- ✓ Offers centralized management of data.
- ✓ Enables people to connect many fast LANs together.
- ✓ Easy to implement links.
- ✓ Flexibility of the proposed service.

Disadvantages

- ✓ The large the network becomes difficult to mange.
- ✓ Difficult to make the system secure from hackers .

Wide Area Network (WAN)

- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.


WAN
Wide Area Network
Reti geografiche
MAN
Metropolitan
Area Network
Reti metropolitane
LAN
Local Area Network
Reti locali

Differences between LAN, WAN, & MAN

LAN	MAN	WAN
1. Connection in small and physical area.	1. Cover a larger geographic area than LAN .	1. Cover a largest distance.
2. Best LAN types used with Ethernet.	2. Used with in internet & Ethernet.	2. Best WAN types used with Internet.
3. Faster than WAN.	3. Higher speed.	3. Less speed than LAN.
4. Cheaper.	4. Competitive price	4. More expensive.
5. More likely need password validation as it will have specific user rights.	5. Need password validation as it will have specific user rights.	5. Less likely need password validation as it will have specific user rights.
6. More private.	6. High security.	6. Less private.
7. Hardware focus on sharing resources.	7. Hardware focus on data transmission.	7. Hardware focus on communication.
8. Operate on peer to peer	8. Operated by organizations and public utilities	8. Operate on client to server.

Personal Area Network (PAN)

- *A PAN is a network that is used for communicating among computers and computer devices (including telephones) in close proximity of around a few meters within a room*
- It can be used for communicating between the devices themselves, or for connecting to a larger network such as the internet .
- PAN's can be wired or wireless
- PAN's can be wired with a computer bus such as a universal serial bus: *USB* (a serial bus standard for connecting devices to a computer-many devices can be connected concurrently)
- PAN's can also be wireless through the use of *bluetooth* (a radio standard designed for low power consumption for interconnecting computers and devices such as telephones, printers or keyboards to the computer) or *IrDA* (infrared data association) technologies.

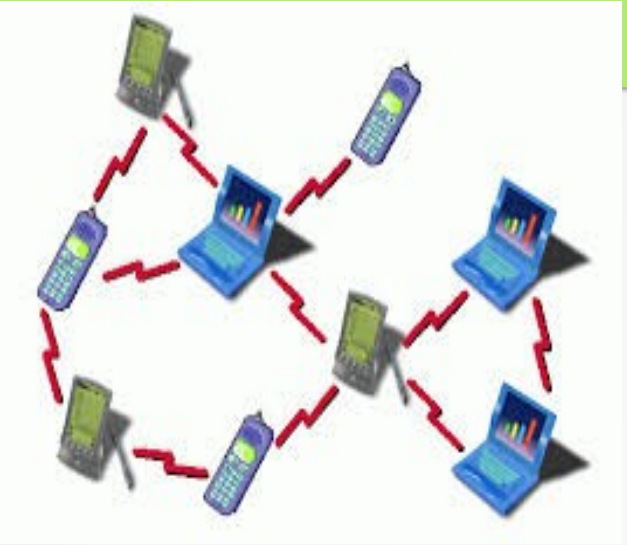
Personal Area Network (PAN)

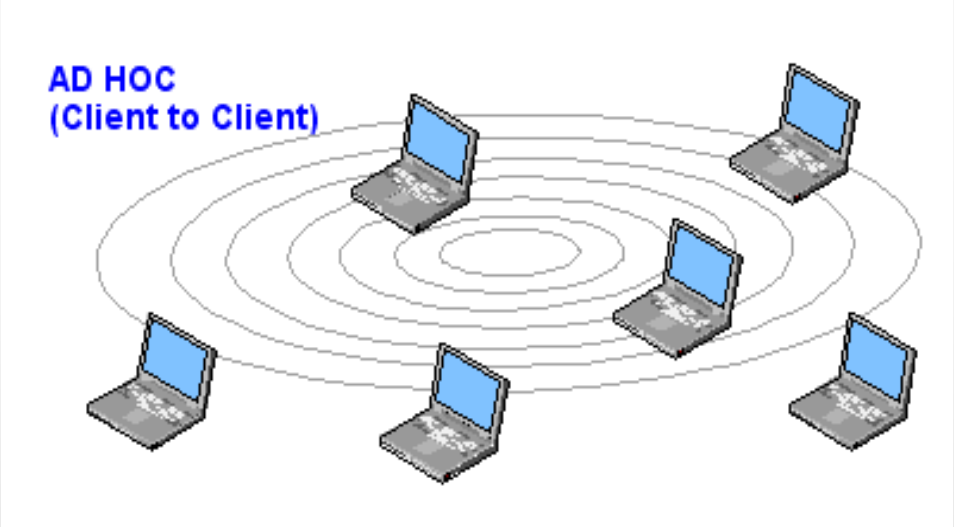
Ad hoc Network

- It is a LAN or other small network, with wireless connections.
- Devices are part of the network only for the duration of a communications session Or while in close proximity to the network.
- Collection of wireless mobile nodes (devices) dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration.
- An ubiquitous type of computing often referred to as pervasive / invisible computing

Properties

- Requires devices to cooperate autonomously
- Without user intervention
- Rapid self-organizing wireless network
- Independent of infrastructure
- Heterogeneous & adaptive

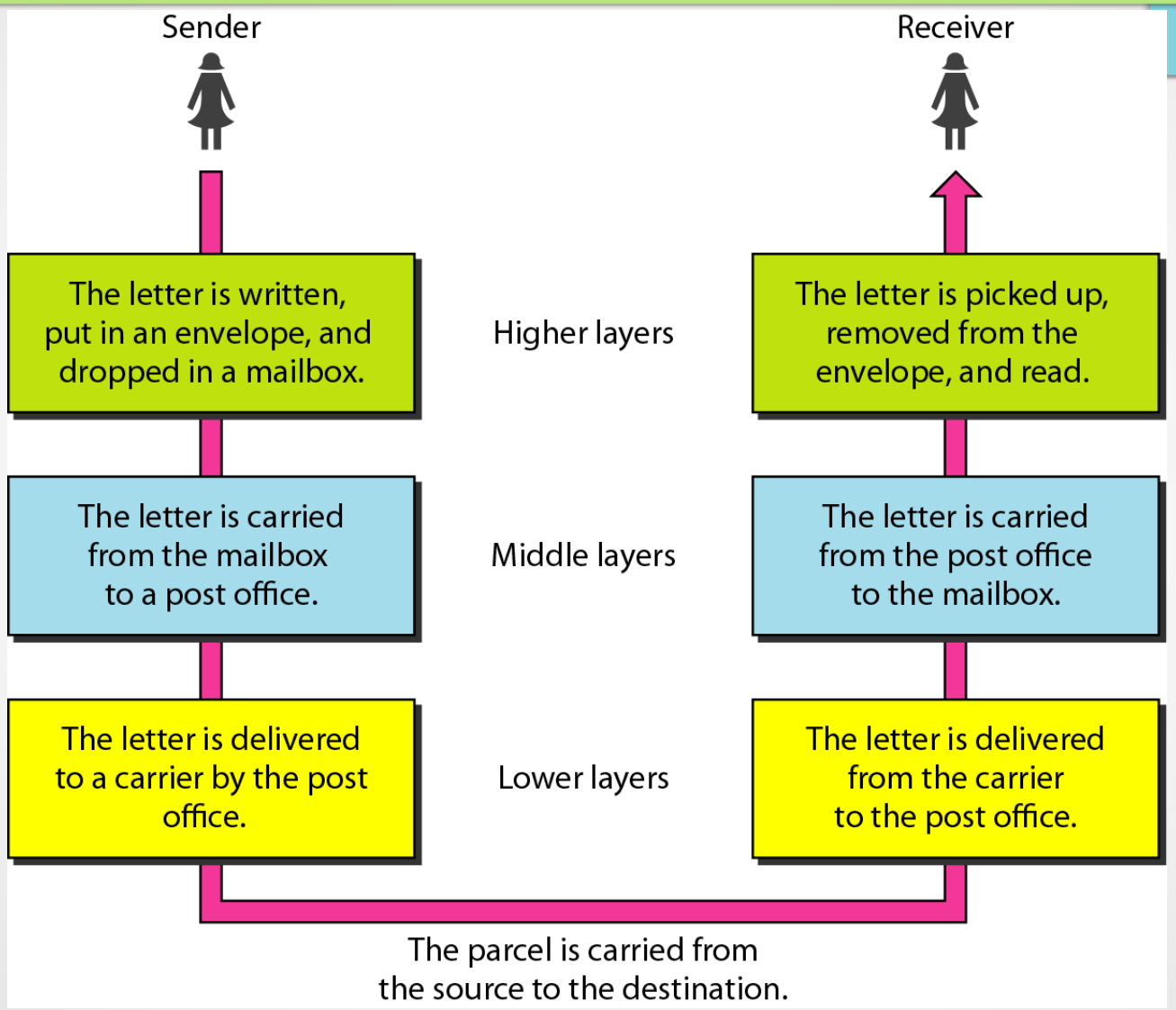



AD HOC
(Client to Client)

LAYERED TASKS

- *We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.*

Tasks involved in sending a letter

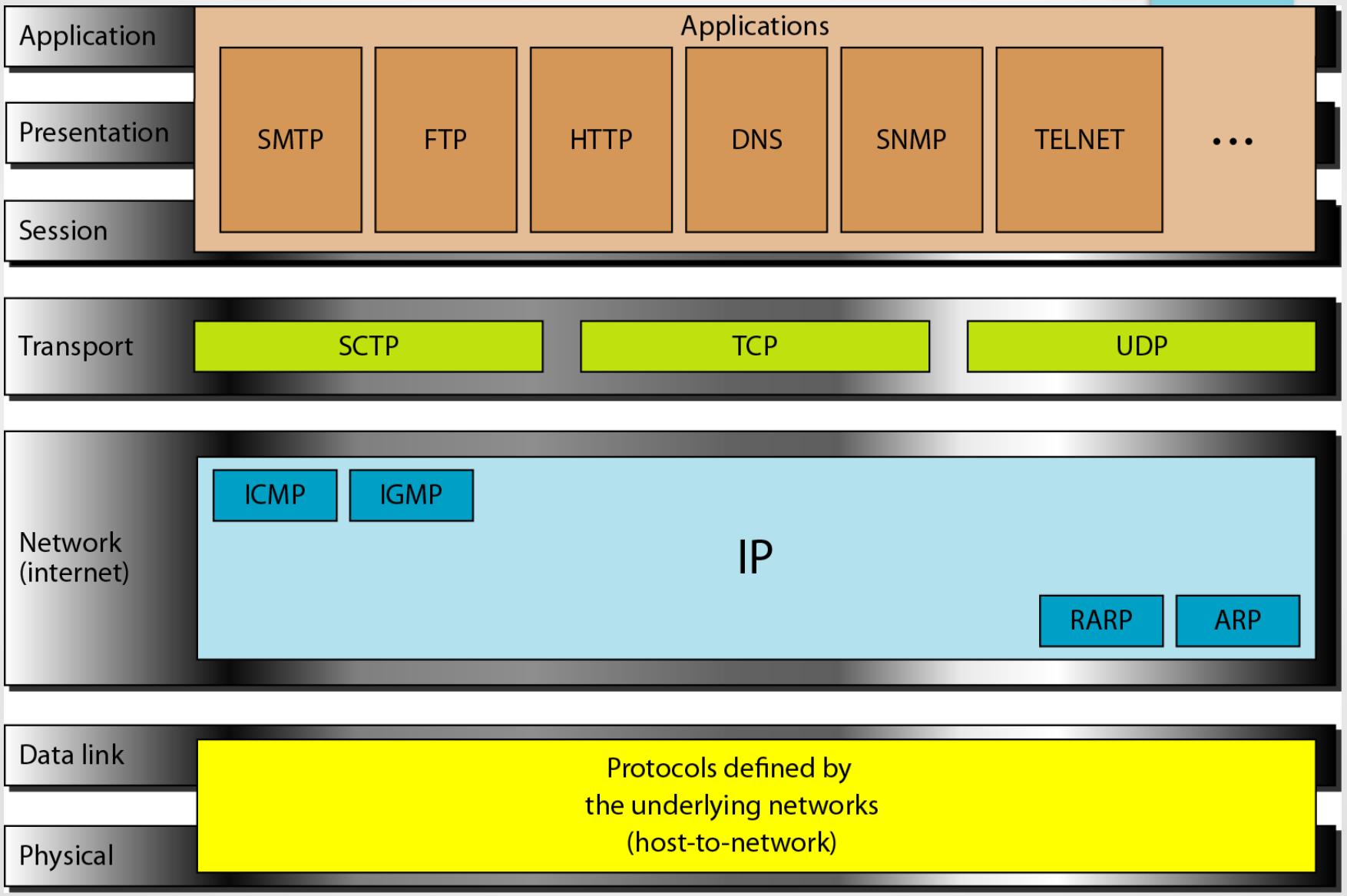


TCP/IP PROTOCOL SUITE

- *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 Layer
Data Link Layer
Network Layer
Transport Layer
Application Layer

Fig. *TCP/IP and OSI model*



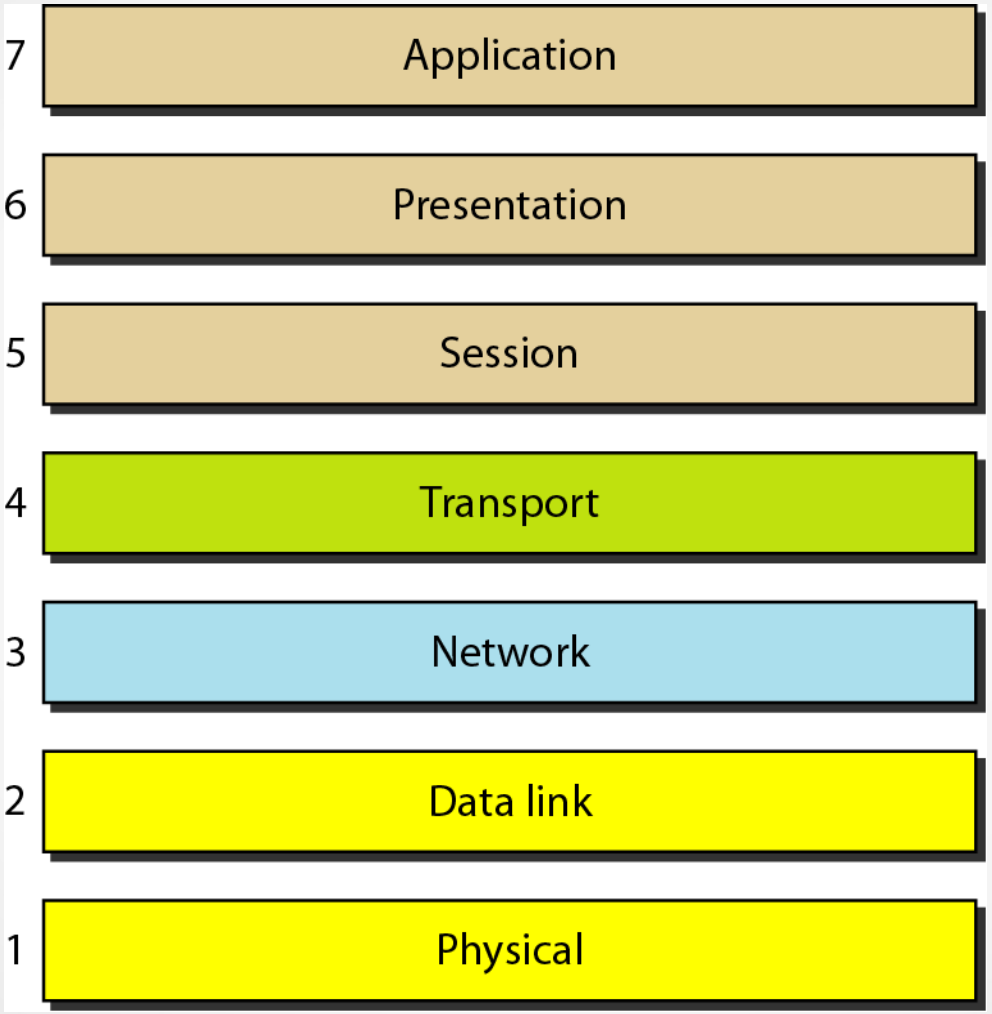
• THE OSI MODEL

- *Established in 1947, the International Organization for Standards (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1978 and TCP/IP model introduced in 1970s.*

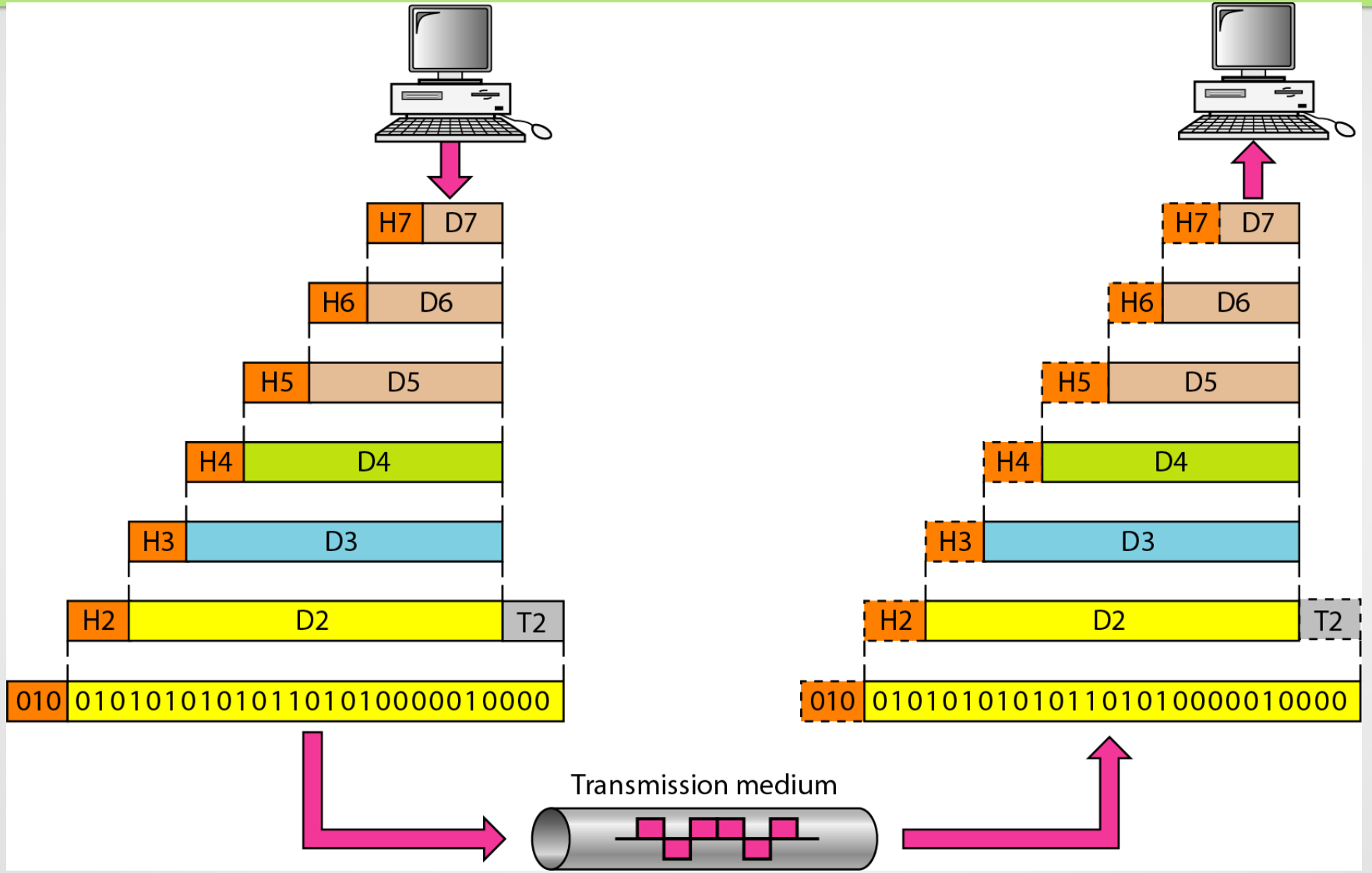
• *Note*

ISO is the organization.
• OSI is the model.

- *Seven layers of the OSI model*



- *An exchange using the OSI model*

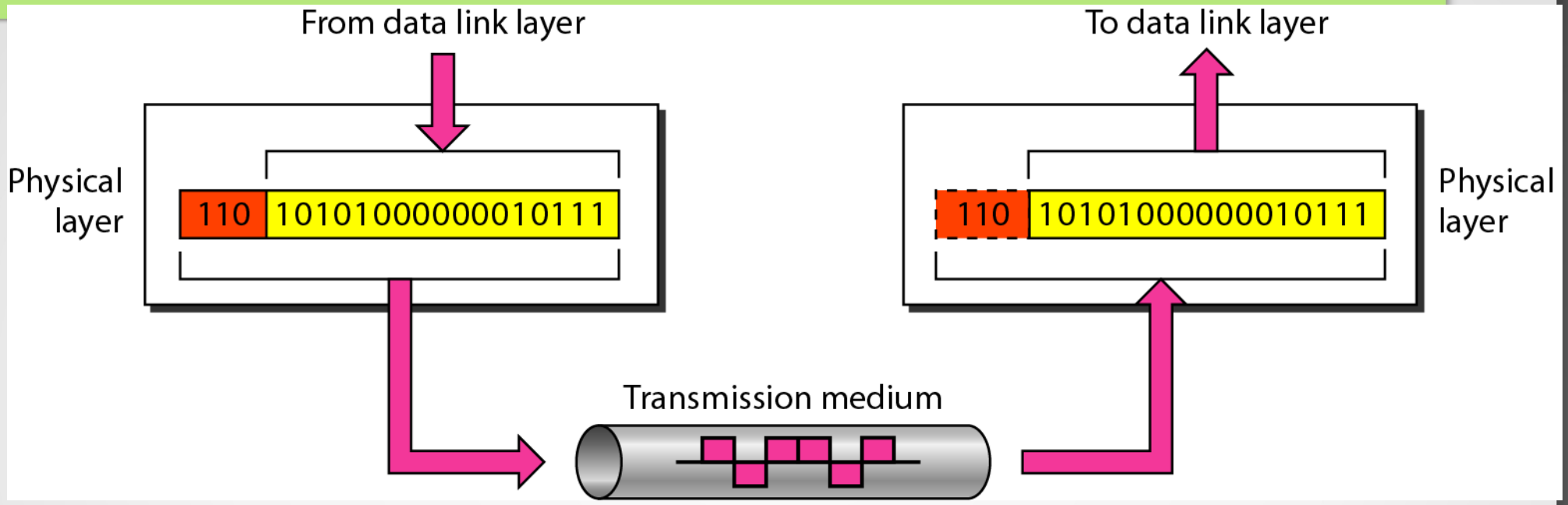


LAYERS IN THE OSI MODEL

- *In this section we briefly describe the functions of each layer in the OSI model.*

Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

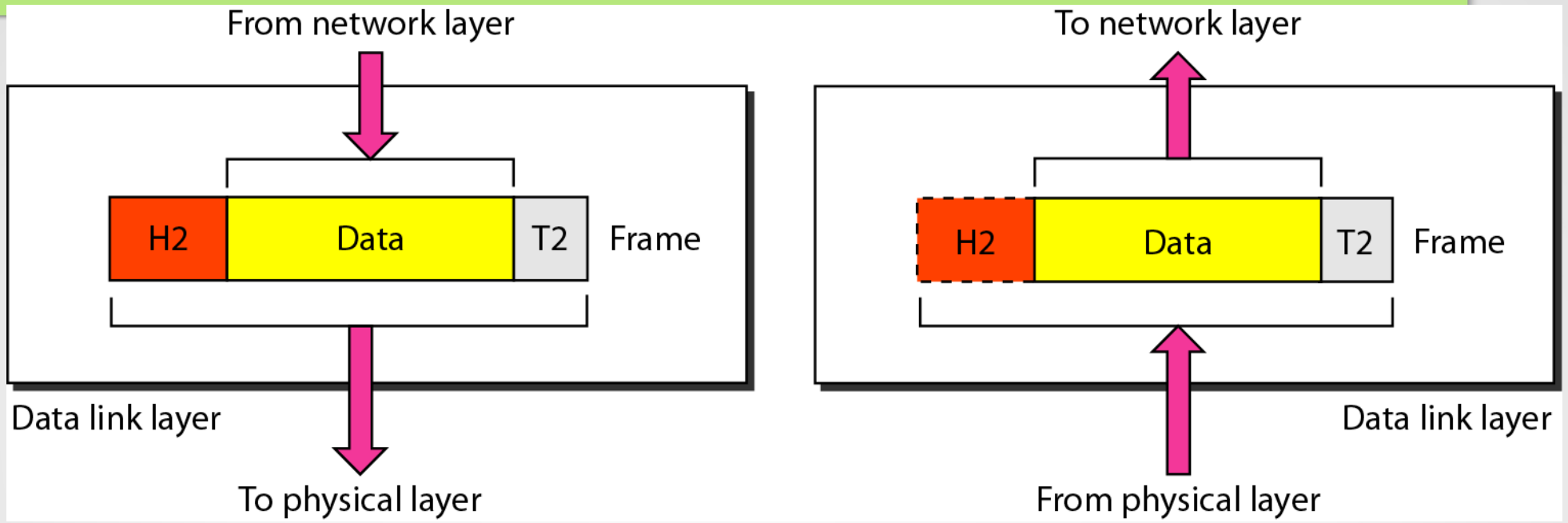
- 1. *Physical layer*



- *Note*

- The physical layer is responsible for movements of
  - individual bits from one hop (node) to the next.

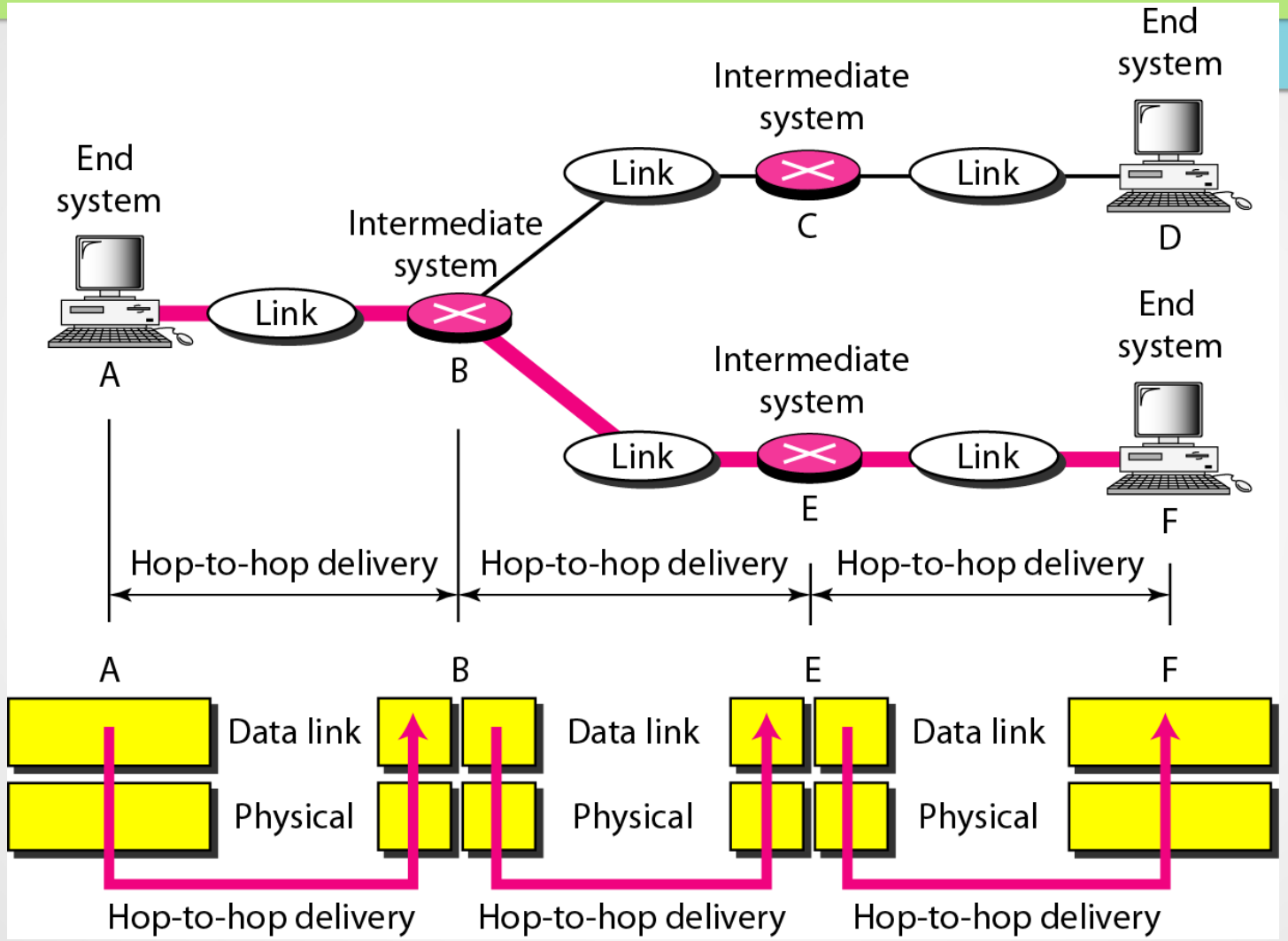
- 2. *Data link layer*



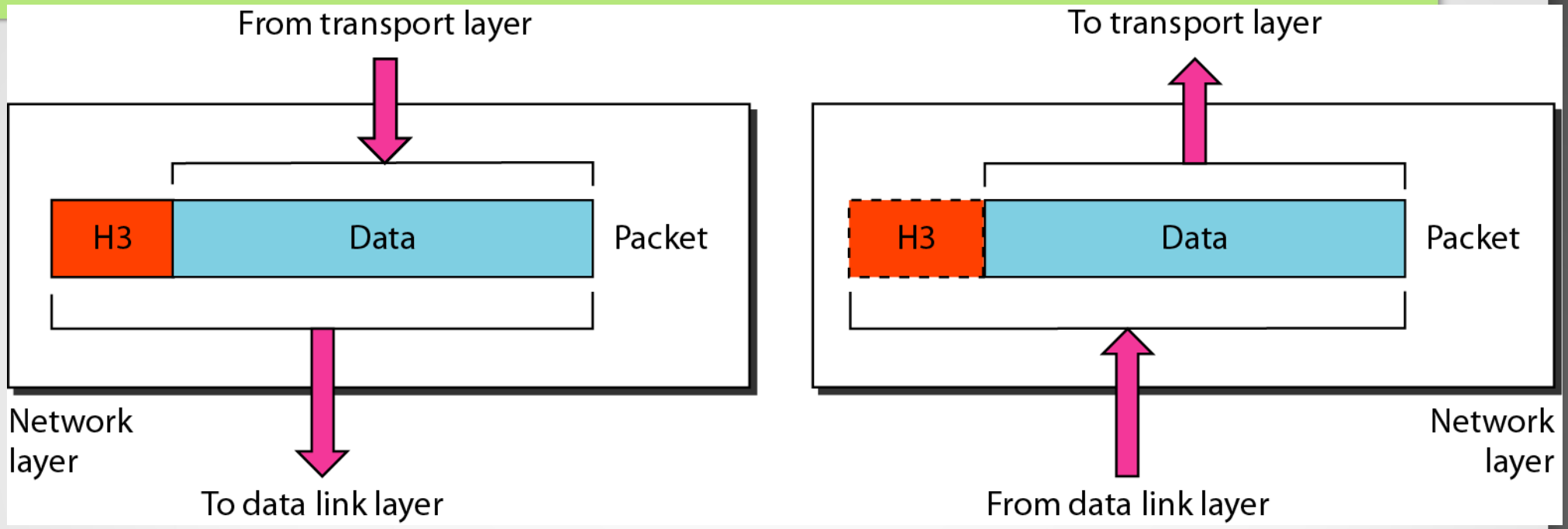
- *Note*

The data link layer is responsible for moving
- frames from one hop (node) to the next.

- Fig. *Hop-to-hop delivery*



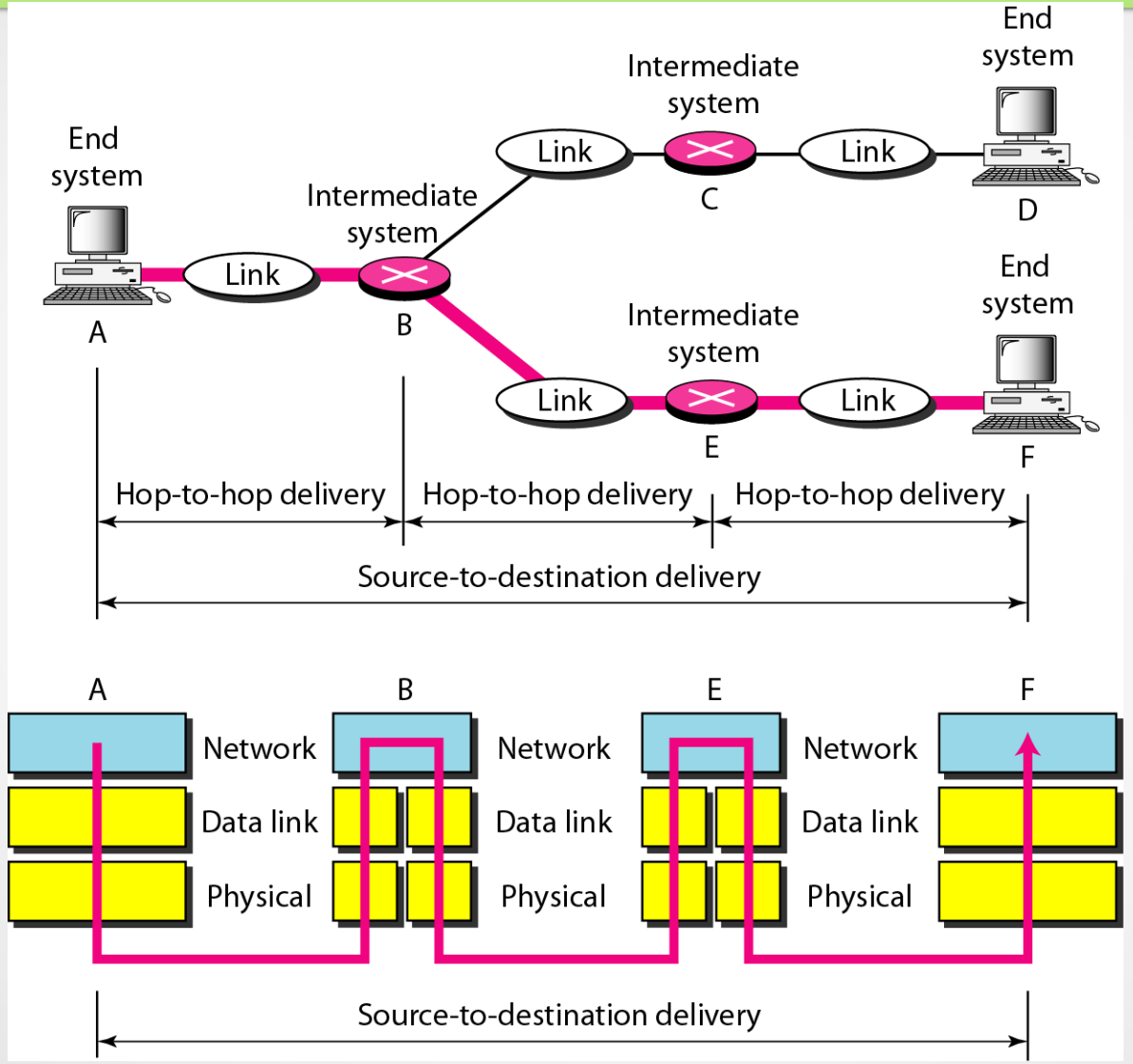
- 3. *Network layer*



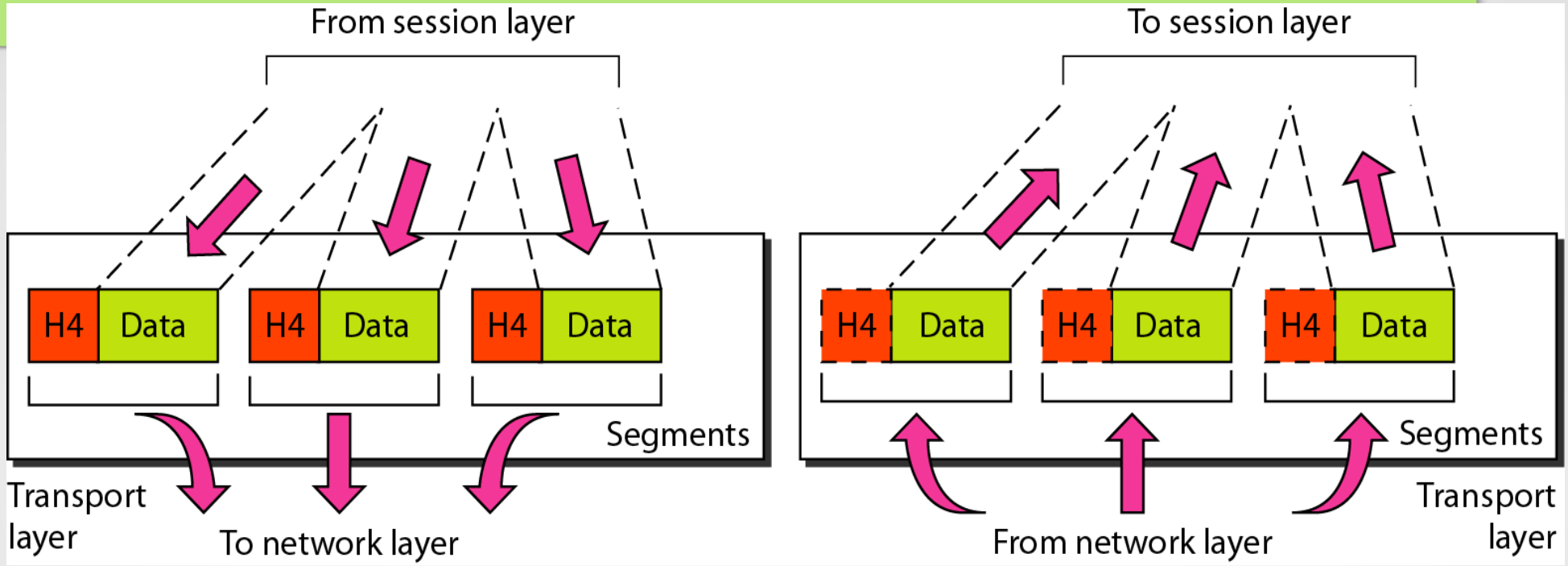
- *Note*

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

- Fig. *Source-to-destination delivery*



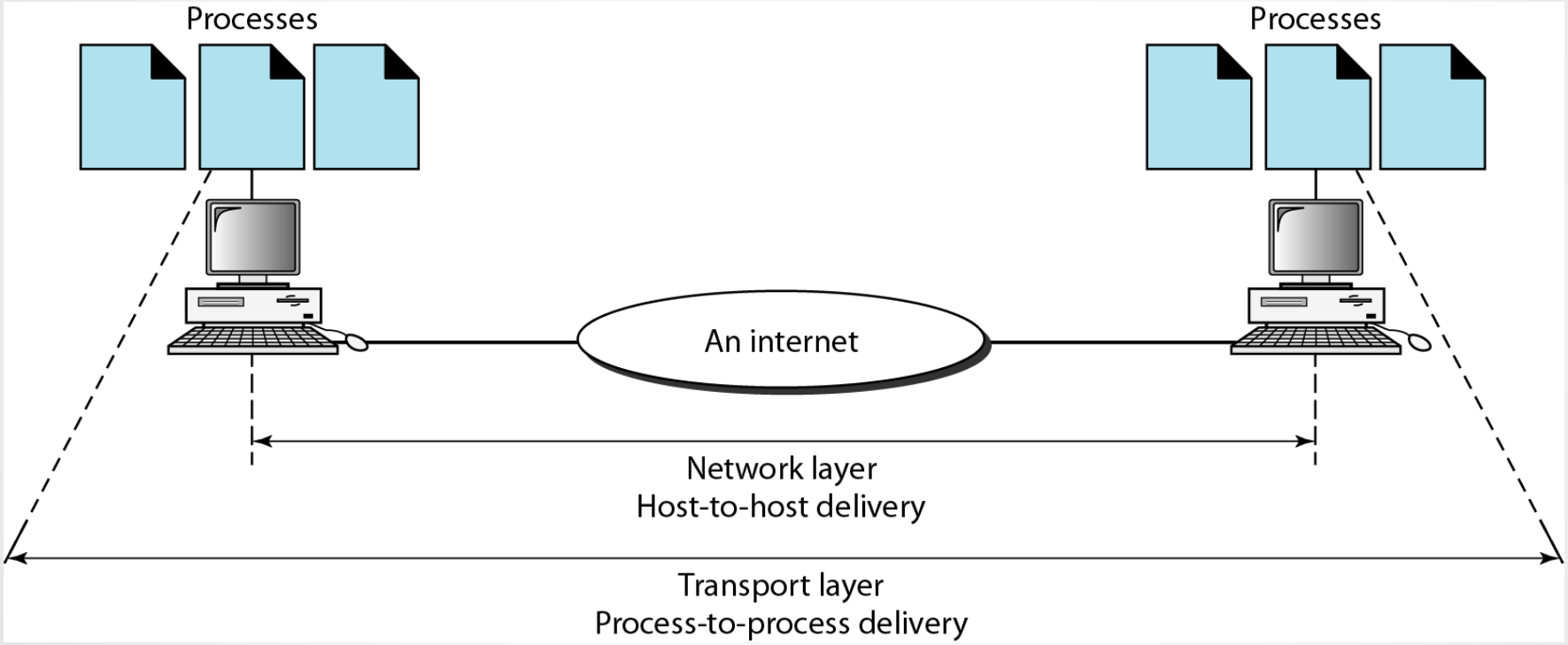
- 4. *Transport layer*



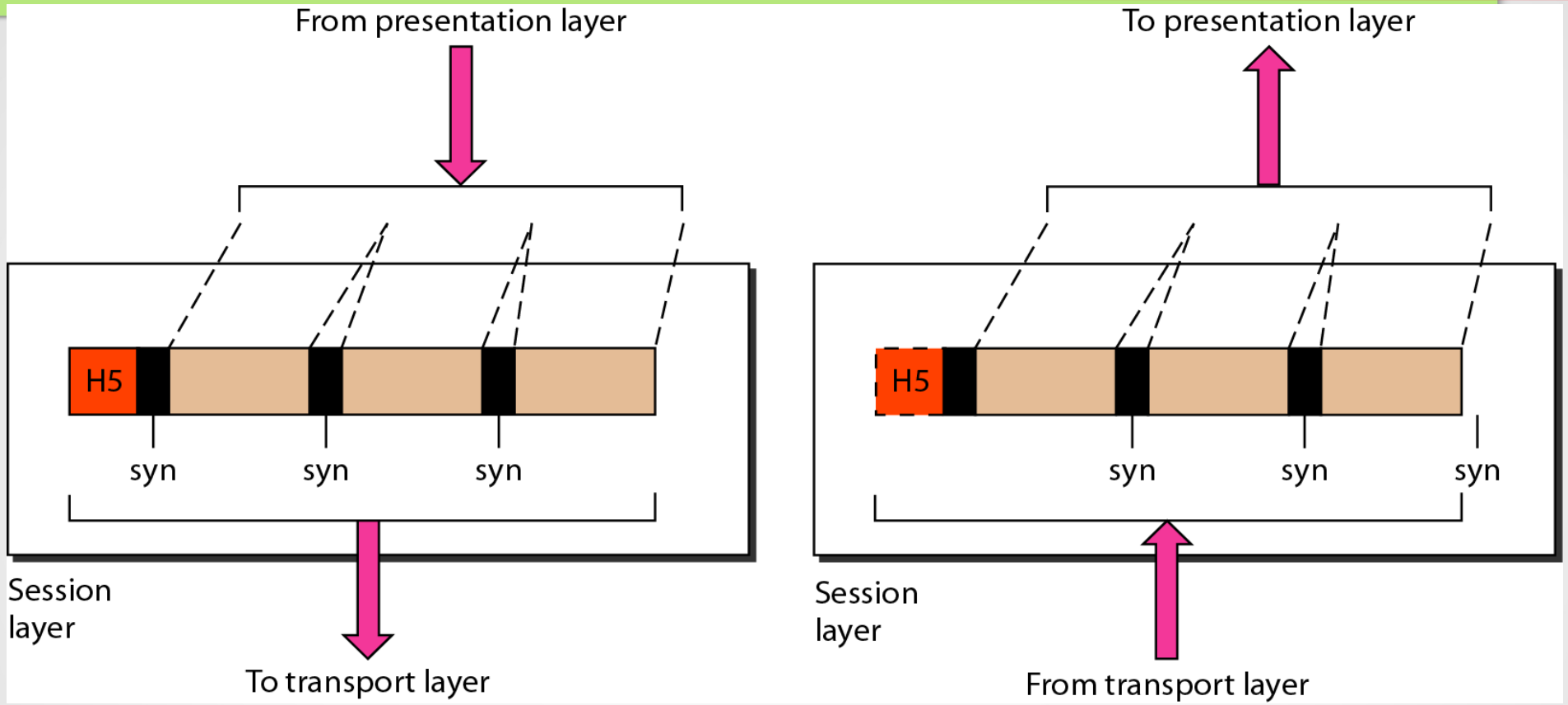
- *Note*

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

- Fig. *Reliable process-to-process delivery of a message*



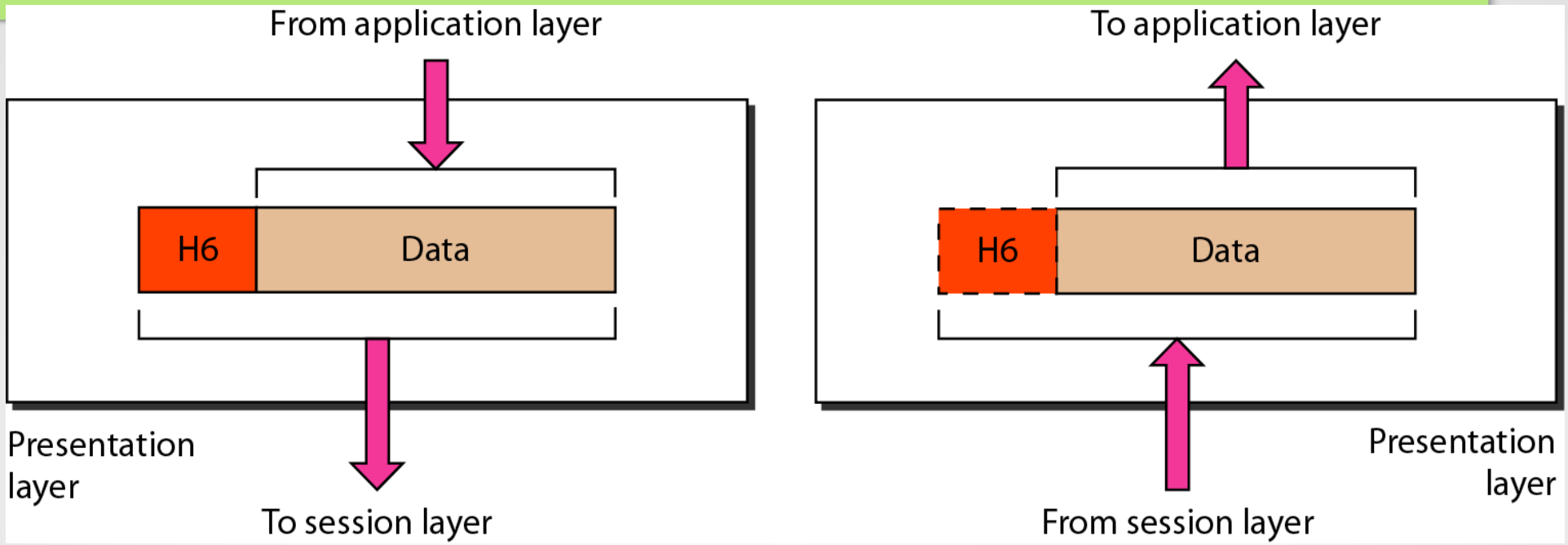
- 5. *Session layer*



- *Note*

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

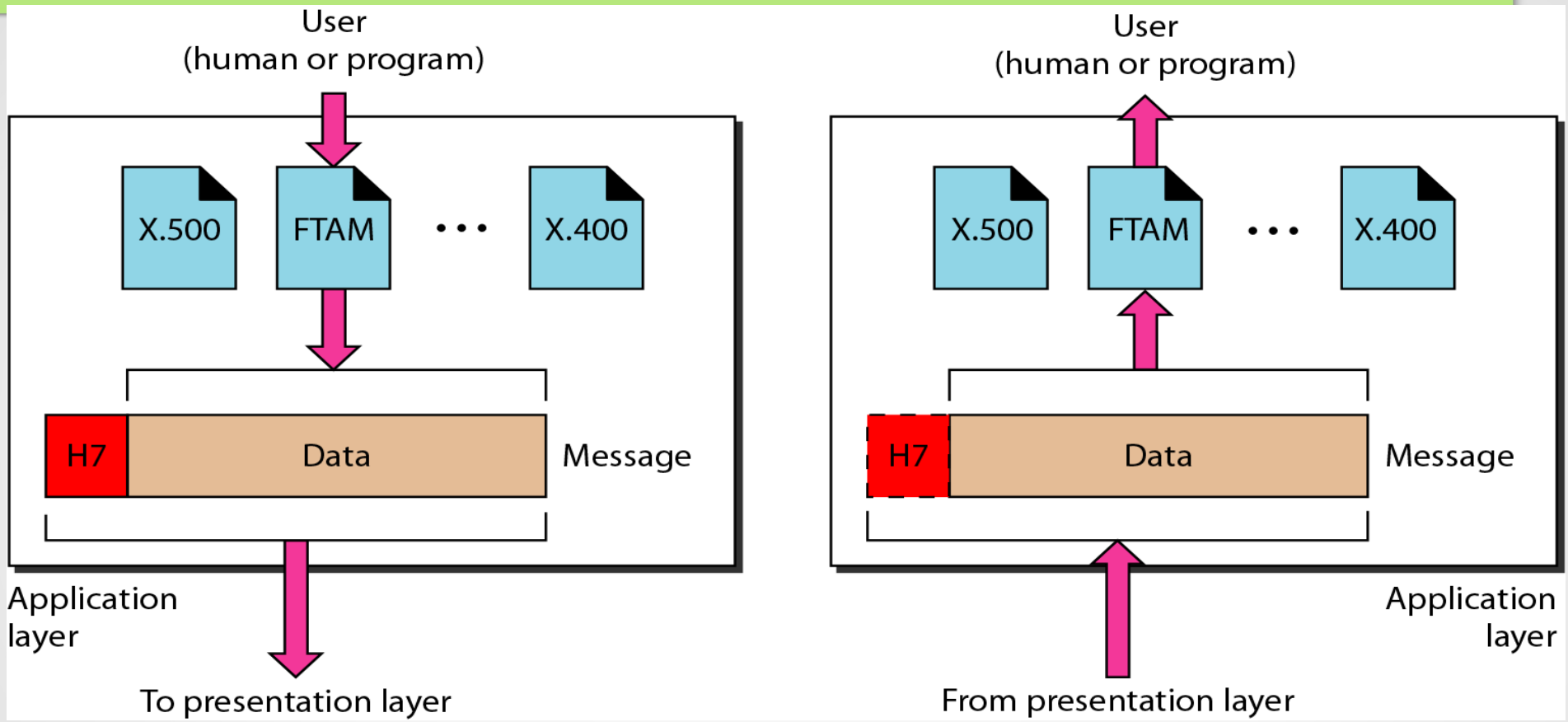
- 6. *Presentation layer*



- *Note*

- The presentation layer is responsible for translation, compression, and encryption.

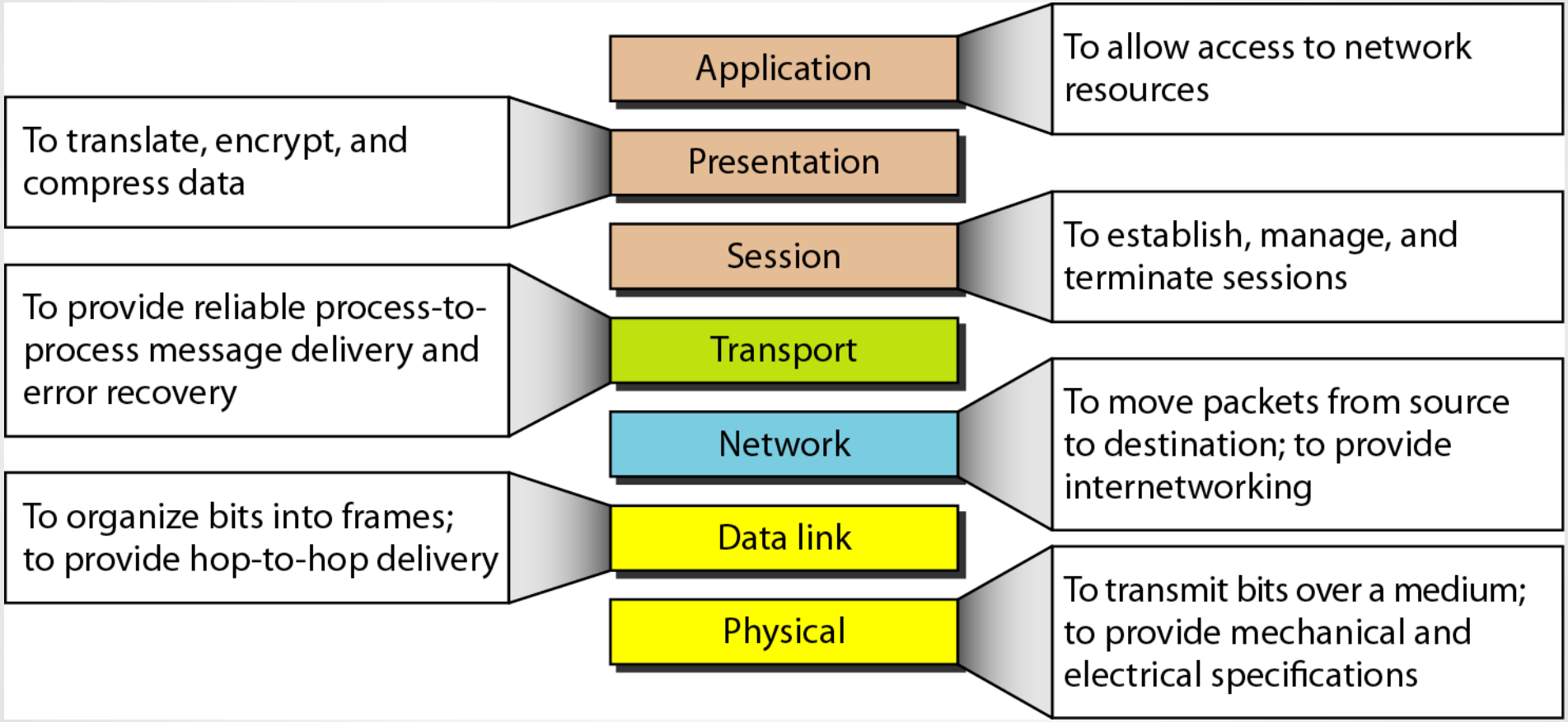
- 7. *Application layer*



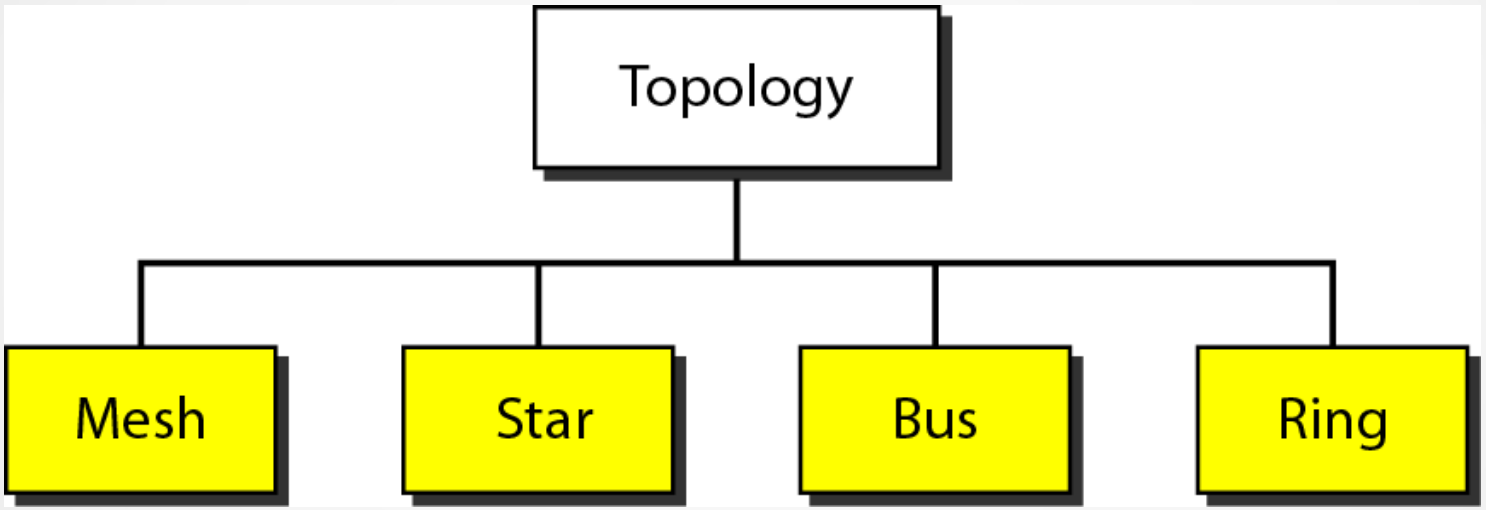
- *Note*

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

- Fig. *Summary of layers*



Categories of topology



Physical Topology

Bus topology

Star topology

Ring topology

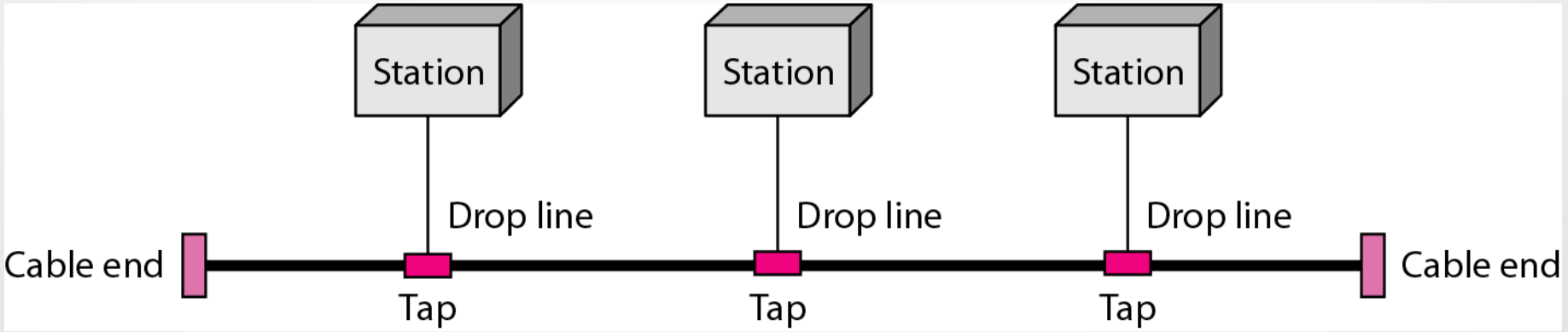
Mesh topology

Hybrid topology

Hierarchical Topology

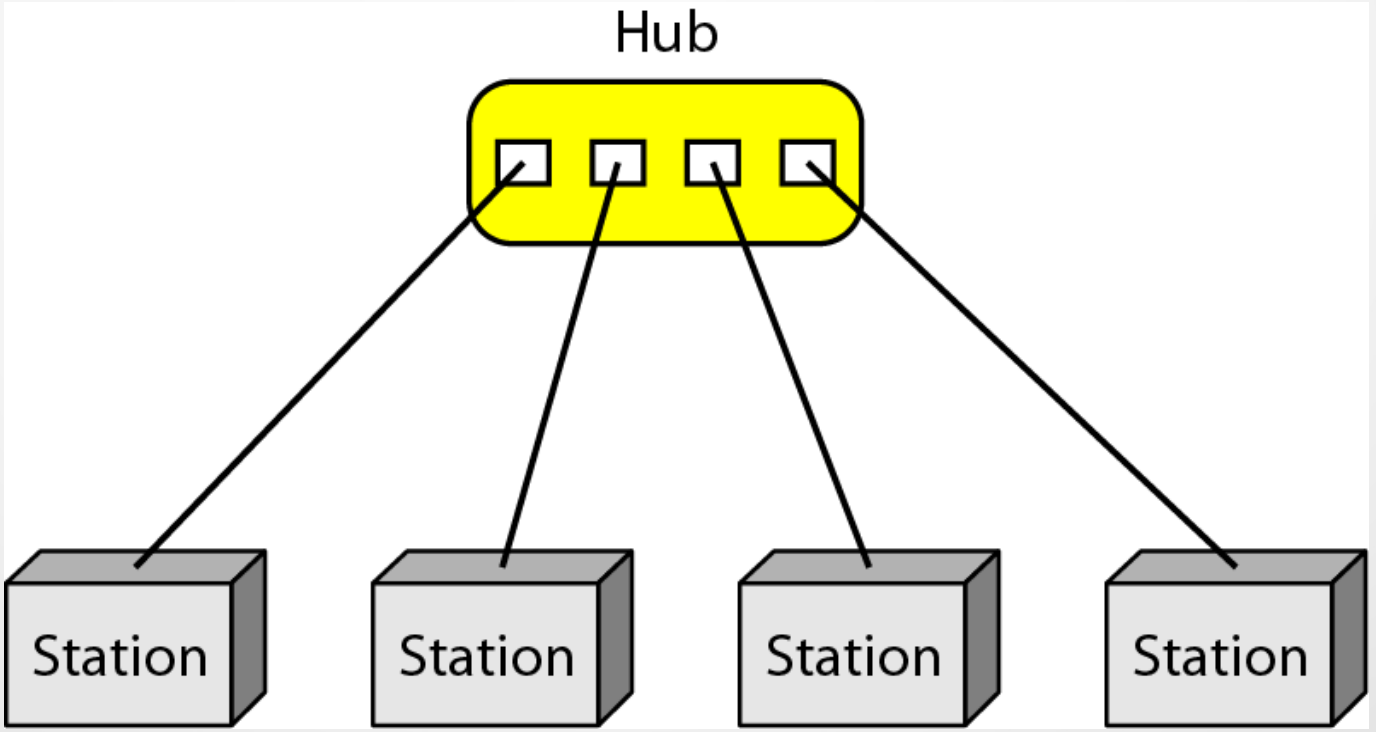
Bus Topology

- Advantage v. Disadvantage
- Early Ethernet



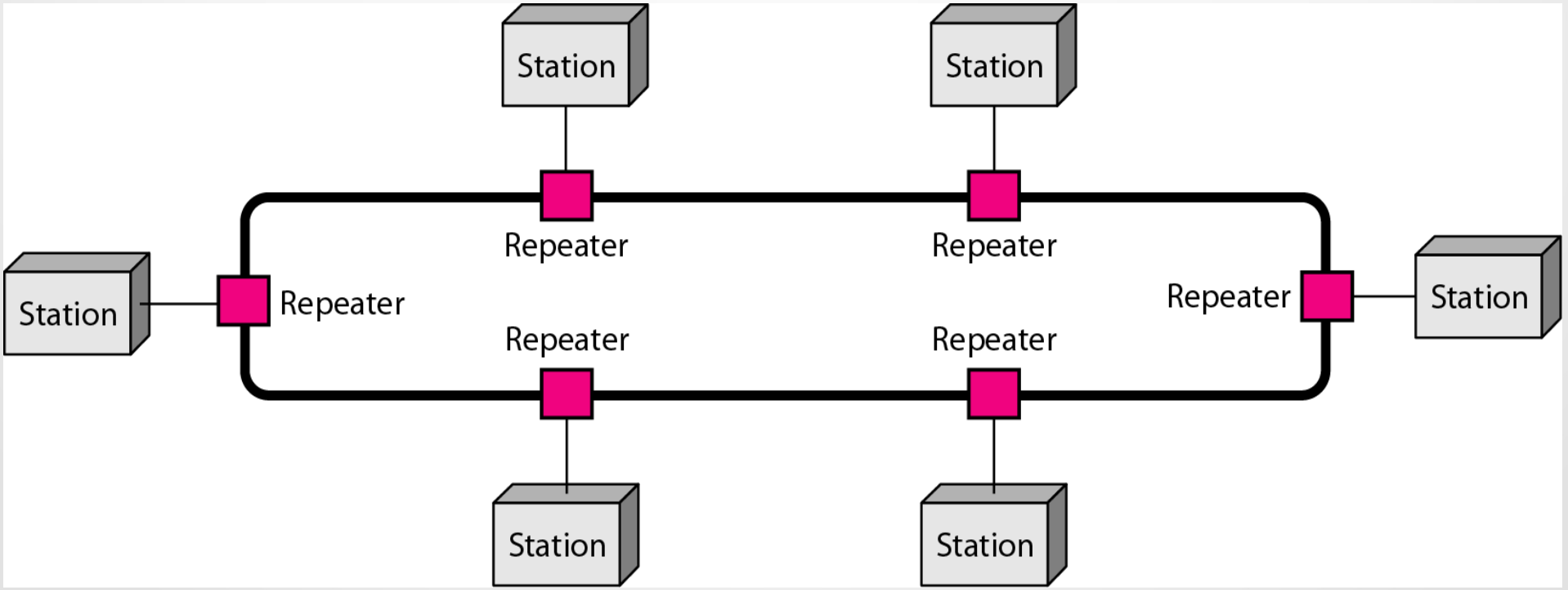
Star Topology

- Advantage v. Disadvantage
- High speed LAN



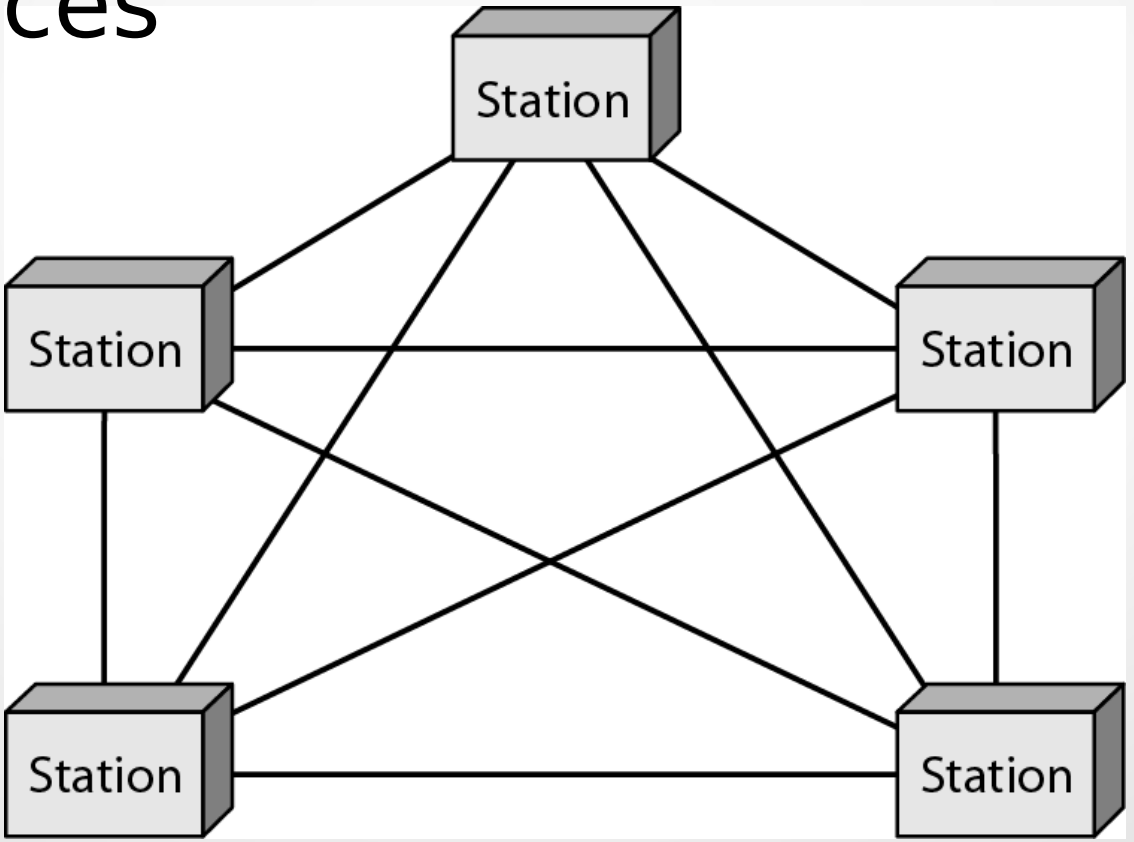
Ring Topology

- Advantage v. Disadvantage
- IEEE 802.5 Token Ring, MAN



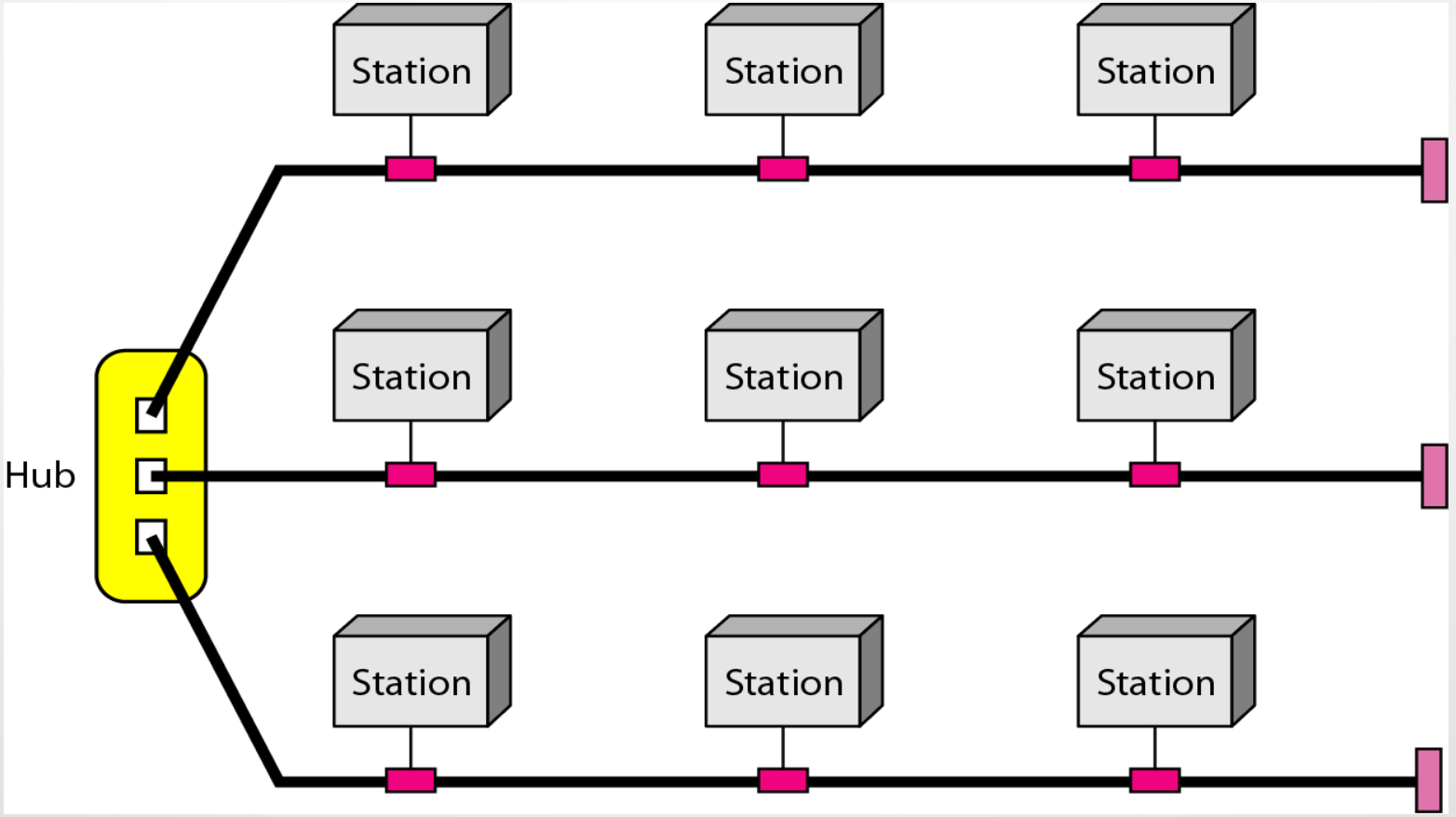
Mesh Topology

- Advantage v. Disadvantage
- Connection of telephone regional offices



Hybrid Topology

- Combination of two or more network topology



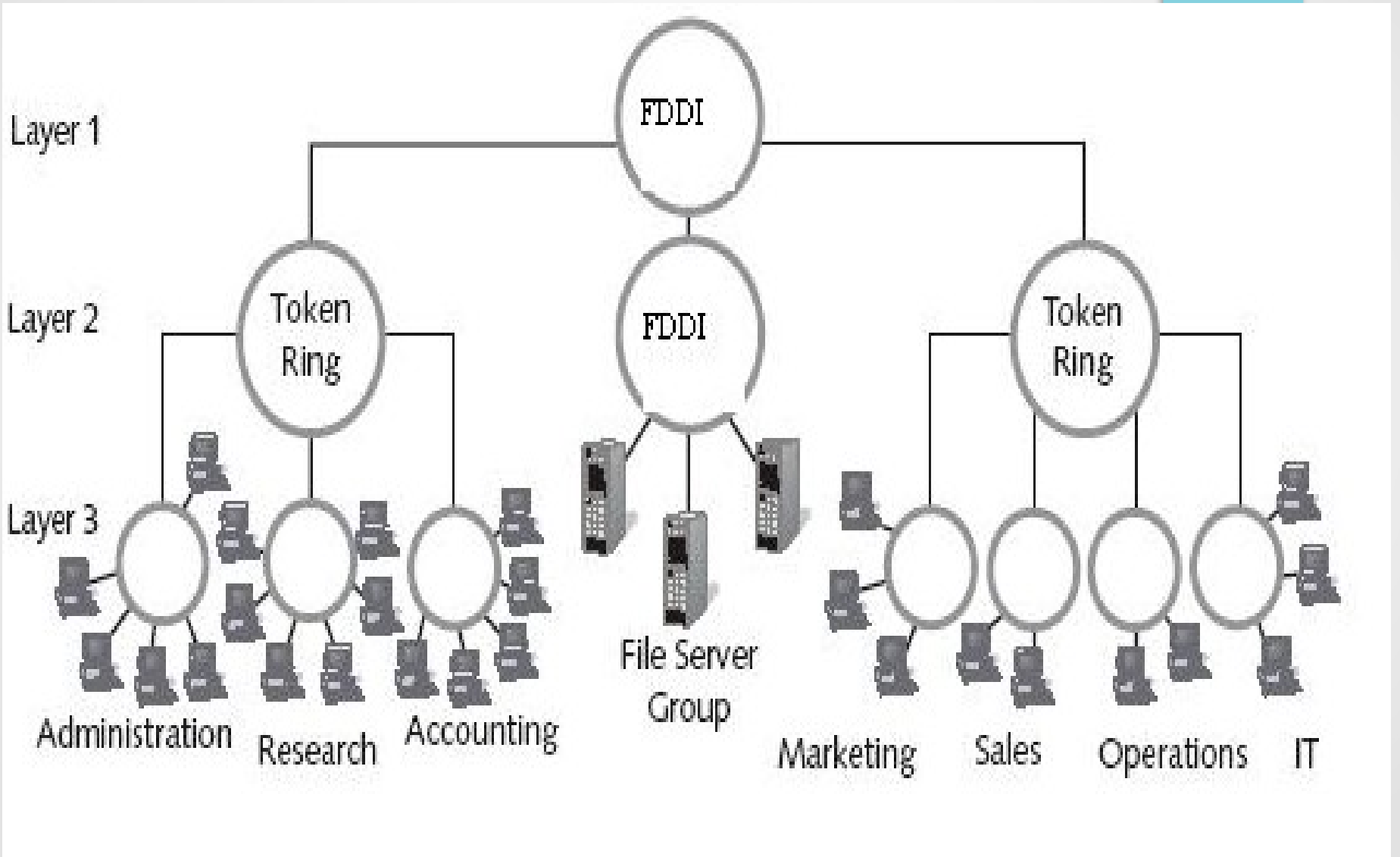
Hierarchies

- Hierarchical topologies consist of more than one layer of hubs. Each layer serves a different network function.
- The bottom tier is reserved for user station and server connectivity. Higher-level tiers provide aggregation of the user-level tier.
- A hierarchical arrangement is best suited for medium-to-large-sized LANs that must be concerned with scalability of the network and with traffic aggregation.

Hierarchical Rings

- Ring networks can be scaled up by interconnecting multiple rings in a hierarchical fashion
- User station and server connectivity can be provided by as many limited size rings as are necessary to provide the required level of performance.
- A second-tier ring, either Token Ring or FDDI, can be used to interconnect all the user level rings and to provide aggregated access to the Wide Area Network. (WAN)

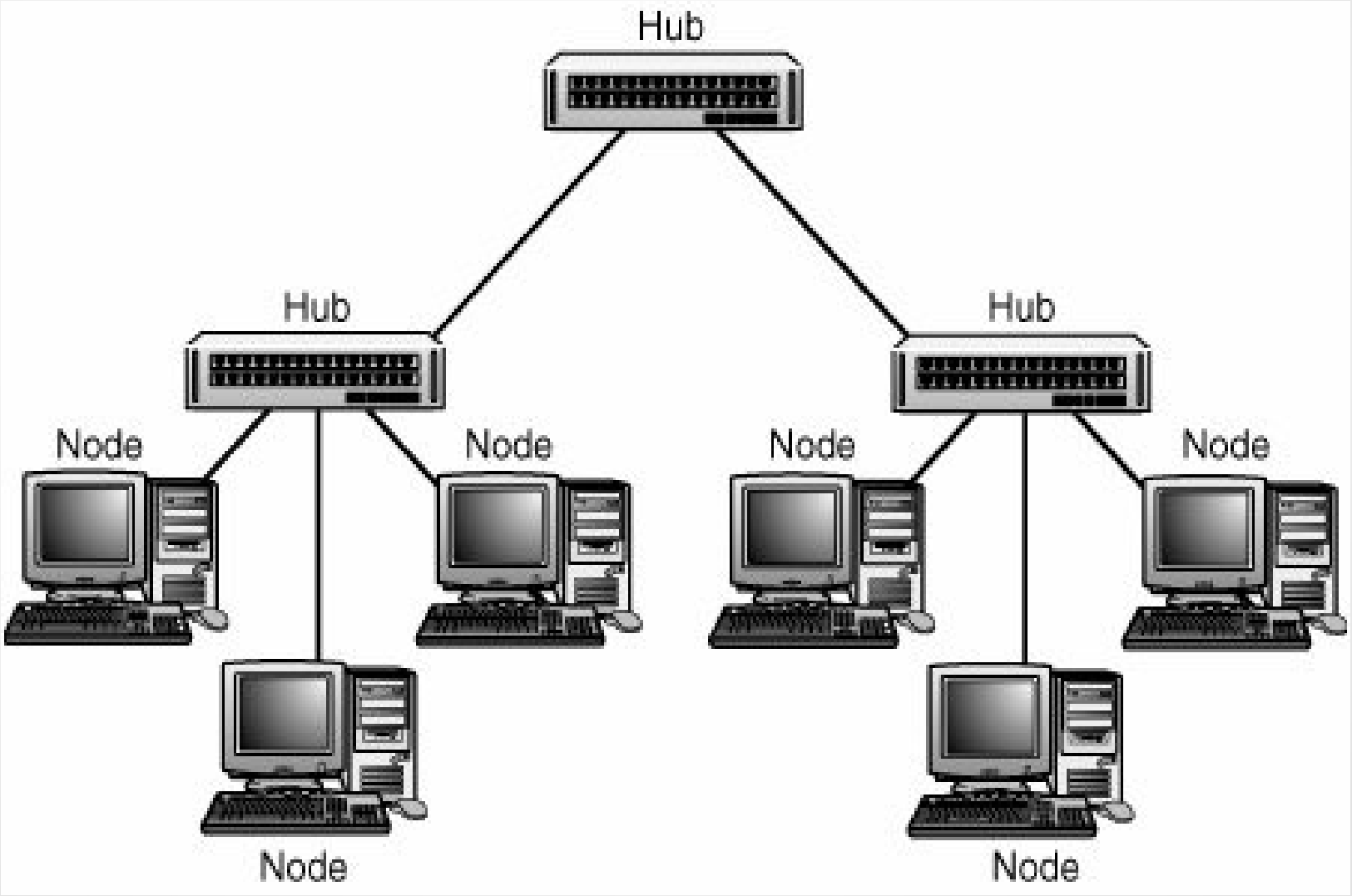
Hierarchical rings



Hierarchical stars

- Star topologies, can be implemented in hierarchical arrangements of multiple stars.
- Hierarchical stars can be implemented as a single collision domain or segmented into multiple collision domains using switches, routers or bridges.

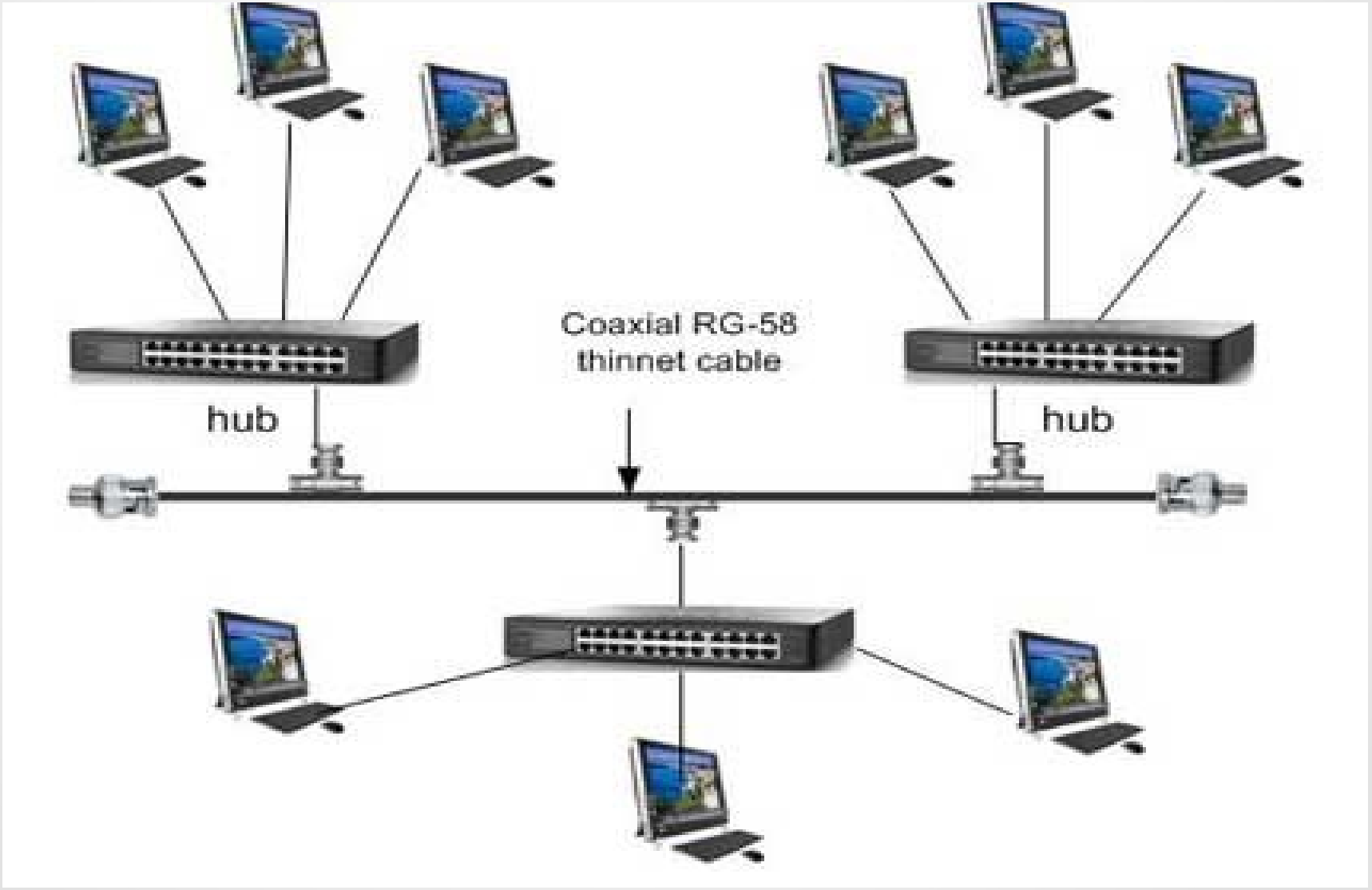
Hierarchical stars



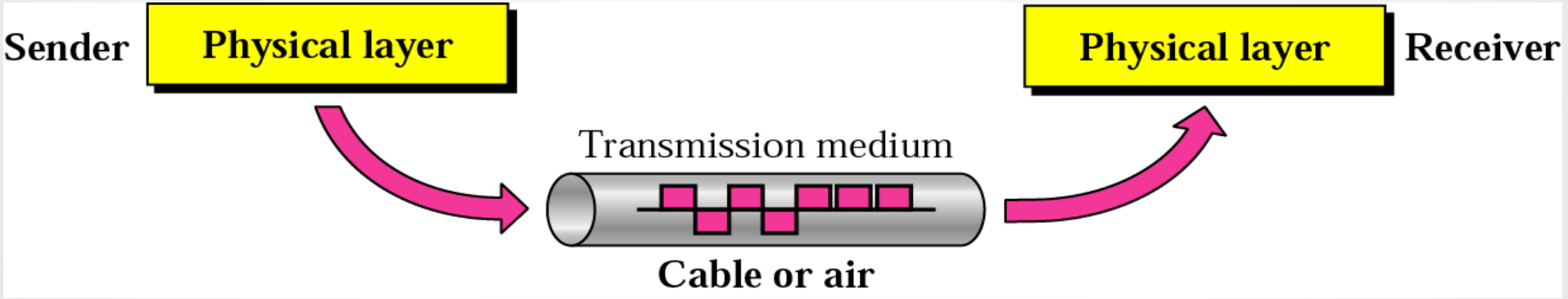
Hierarchical combinations

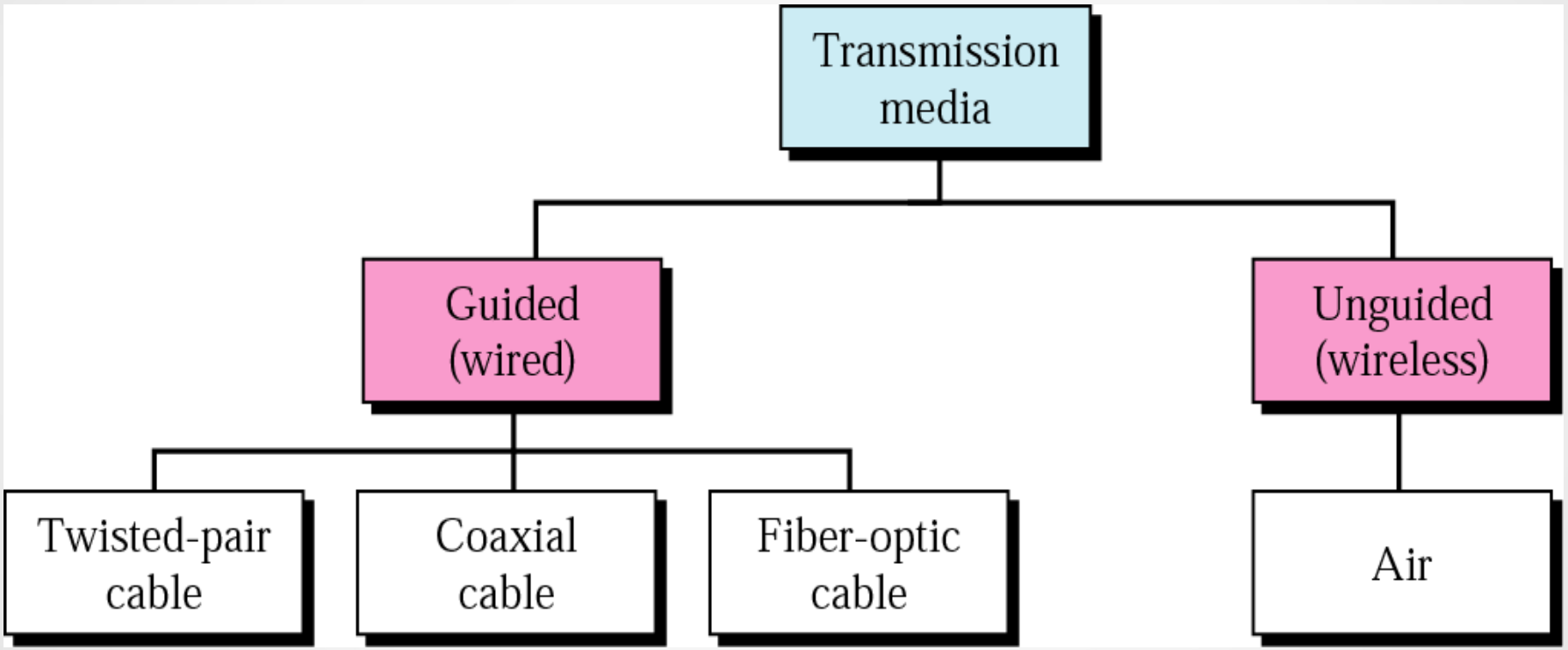
- Overall network performance can be enhanced by not force-fitting all the functional requirements of the LAN into a single solution.
- Today's high-end switching hubs enable you to mix multiple technologies.

Hierarchical combinations



Physical Media



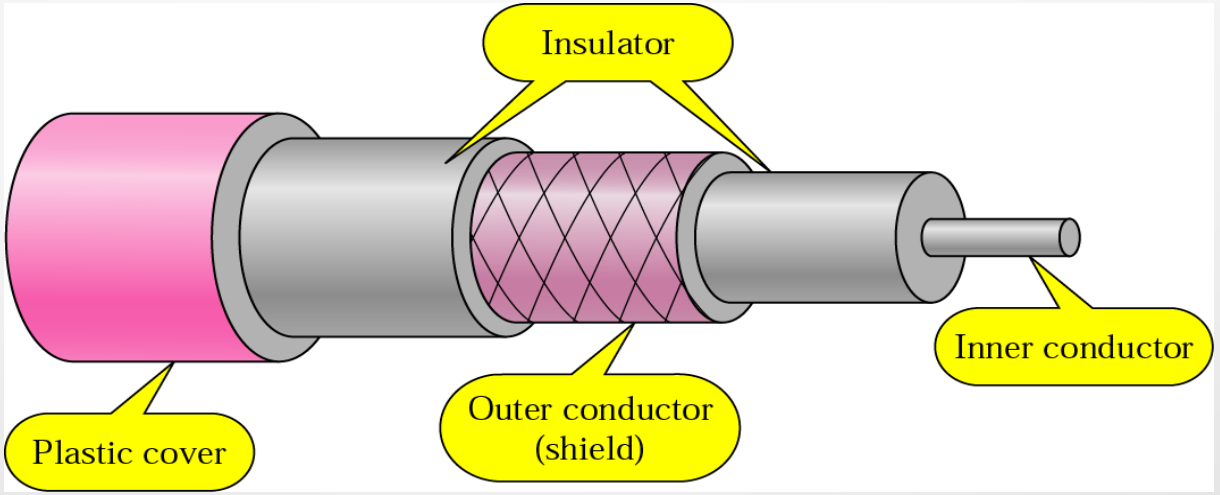

Transmission media
Guided (wired)
Unguided (wireless)
Twisted-pair cable
Coaxial cable
Fiber-optic cable
Air

Physical Media

- **Copper**
  - Coaxial Cable - Thick or Thin
  - Unshielded Twisted Pair - CAT 3,4,5,5e&6
- **Optical Fiber**
  - Multimode
  - Singlemode
- **Wireless**
  - Short Range
  - Medium Range (Line of Sight)
  - Satellite

Copper Media: Coaxial Cable

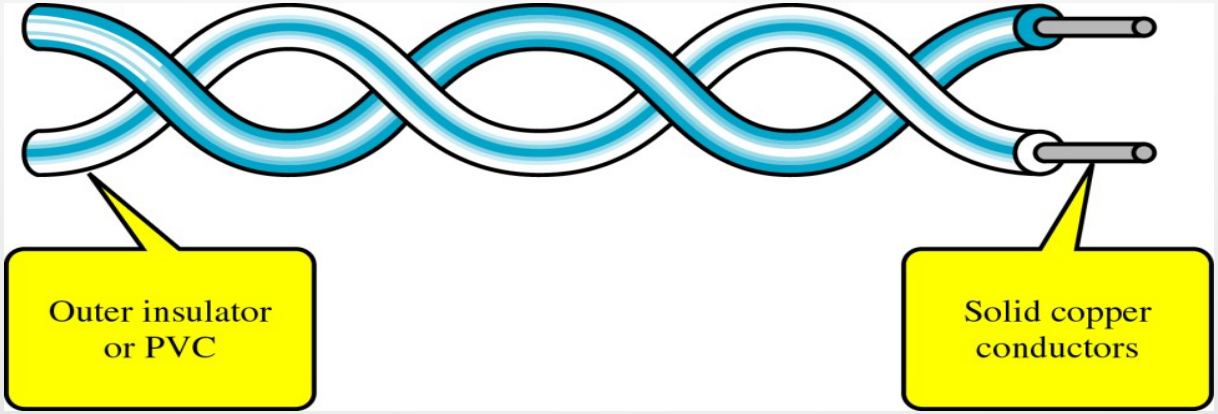
- Coaxial cable is a copper-cored cable surrounded by a heavy shielding and is used to connect computers in a network.
- High bandwidth but lossy channel.
- Repeater is used to regenerate the weakened signals.



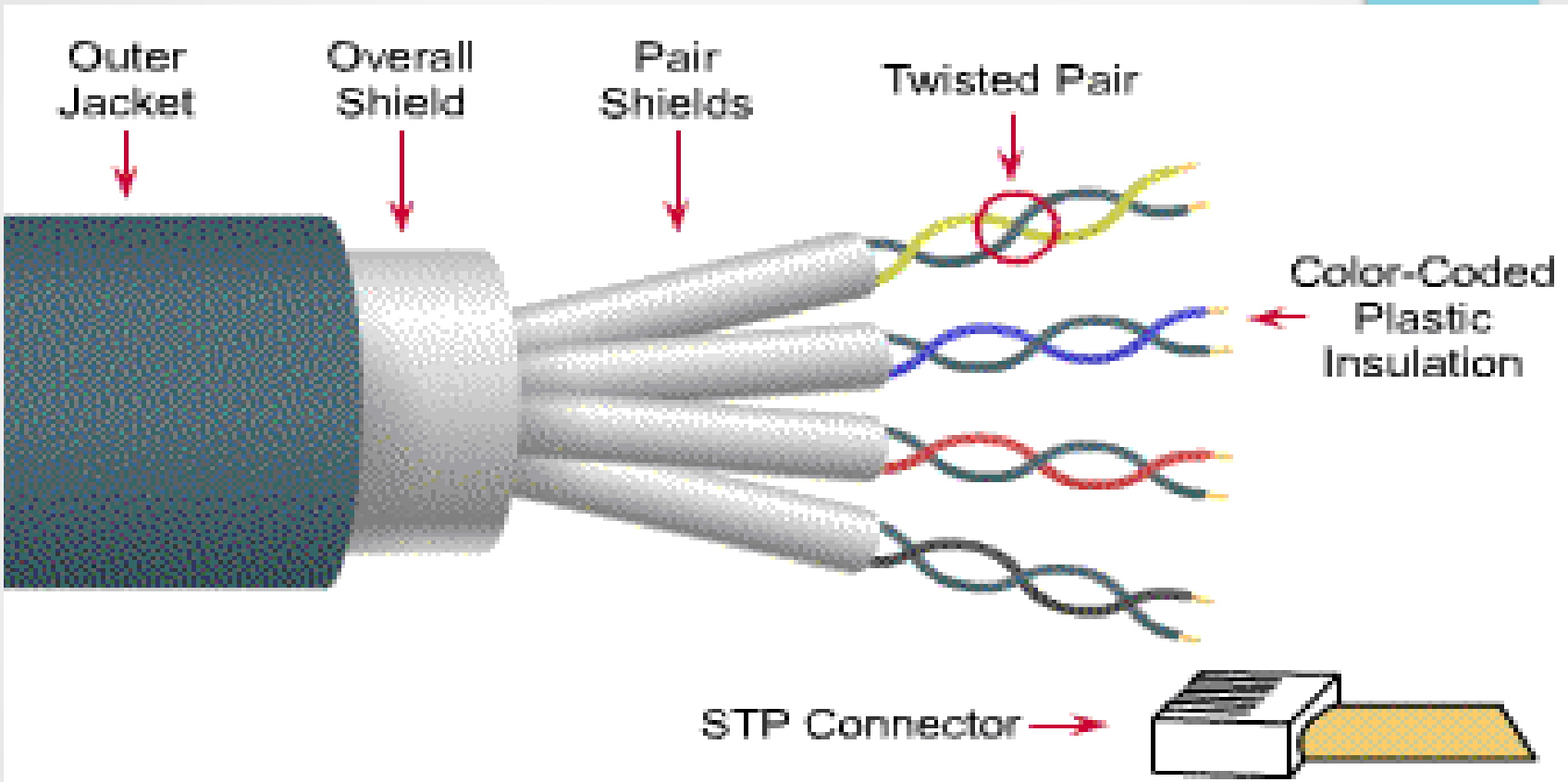
Coaxial Connectors

Copper Media: Twisted Pair

- Twisted-pair is a type of cabling that is used for telephone communications and most modern Ethernet networks.
- A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk, the noise generated by adjacent pairs.
- There are two basic types, shielded twisted-pair (STP) and unshielded twisted-pair (UTP).

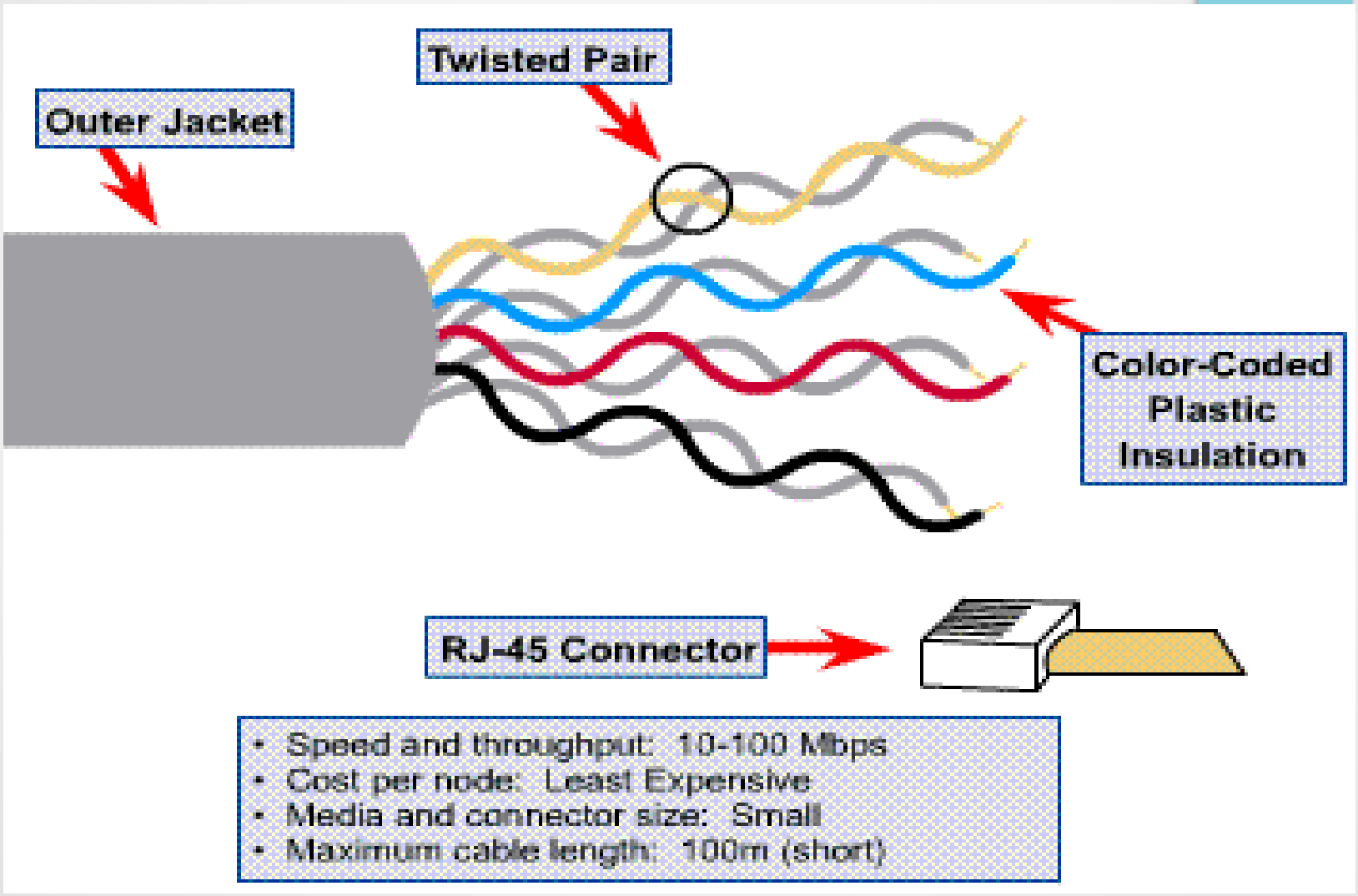


Shielded Twisted Pair (STP)



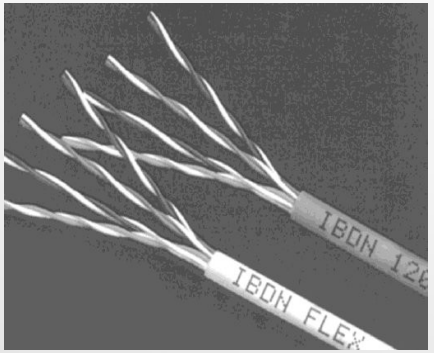
- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)

Unshielded Twisted Pair (UTP)



Unshielded Twisted Pair (UTP)

- Consists of 4 pairs (8 wires) of insulated copper wires typically about 1 mm thick.
- The wires are twisted together in a helical form.
- Twisting reduces the interference between pairs of wires.
- High bandwidth
- Flexible and cheap cable.
- Category rating based on number of twists per inch and the material used
- CAT 3, CAT 4, CAT 5, Enhanced CAT 5 and now CAT 6.



Categories of UTP

- UTP comes in several categories that are based on the number of twists in the wires, the diameter of the wires and the material used in the wires.
- Category 3 is the wiring used primarily for telephone connections.
- Category 5e and Category 6 are currently the most common Ethernet cables used.

Categories of UTP: CAT 3

- Bandwidth 16 Mhz
- 11.5 dB Attenuation
- 100 ohms Impedance
- Used in voice applications and 10baseT (10Mbps) Ethernet

Categories of UTP: CAT 4

- 20 MHz Bandwidth
- 7.5 dB Attenuation
- 100 ohms Impedance
- Used in 10baseT (10Mbps) Ethernet

Categories of UTP: CAT 5

- 100 MHz Bandwidth
- 24.0 dB Attenuation
- 100 ohms Impedance
- Used for high-speed data transmission
- Used in 10BaseT (10 Mbps) Ethernet & Fast Ethernet (100 Mbps)

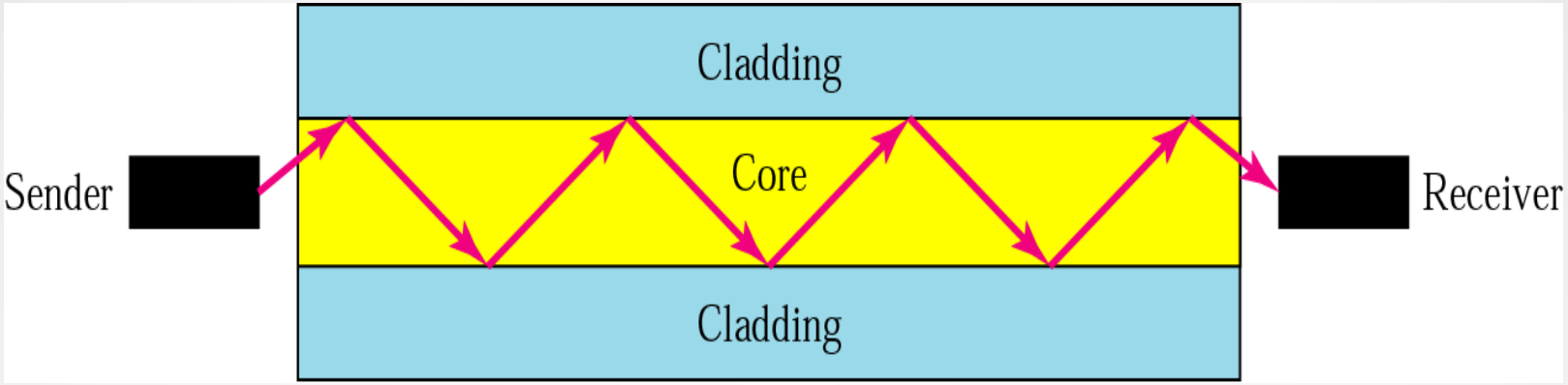
Categories of UTP: CAT 5e

- 150 MHz Bandwidth
- 24.0 dB Attenuation
- 100 ohms Impedance
- Transmits high-speed data
- Used in Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps) & 155 Mbps ATM

Categories of UTP: CAT 6

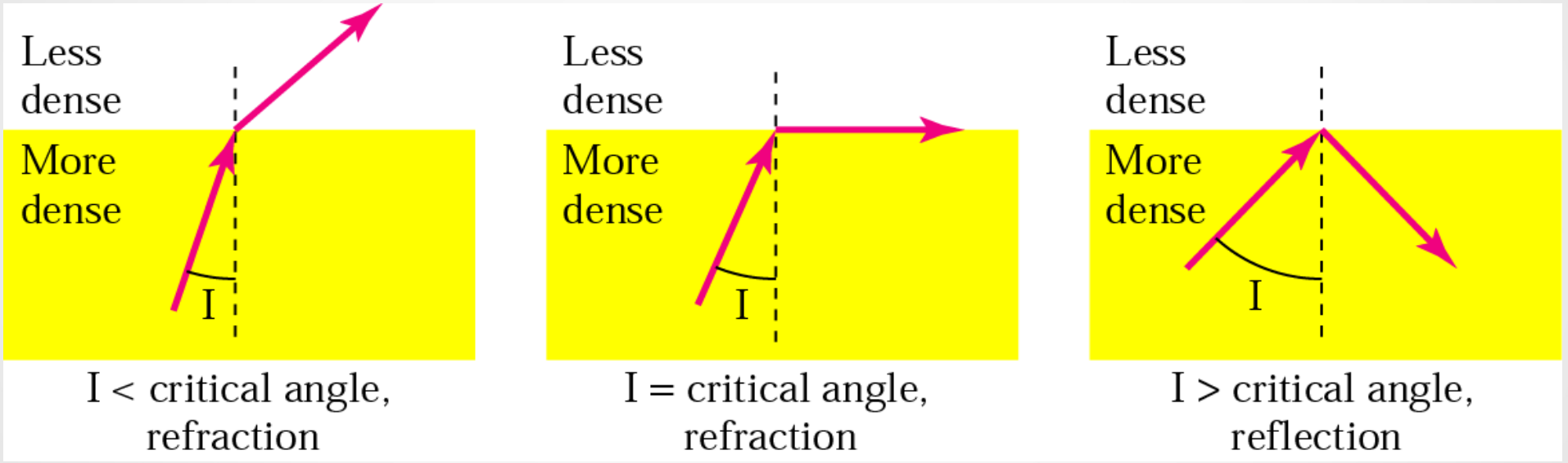
- 250 MHz Bandwidth
- 19.8 dB Attenuation
- 100 ohms Impedance
- Transmits high-speed data
- Used in Gigabit Ethernet (1000 Mbps) & 10 Gigbit Ethernet (10000 Mbps)

Optical Fiber Cable (OFC)



- Optical fibers use light to send information through the optical medium.
- It uses the principal of total internal reflection.
- Modulated light transmissions are used to transmit the signal.

Total Internal Reflection

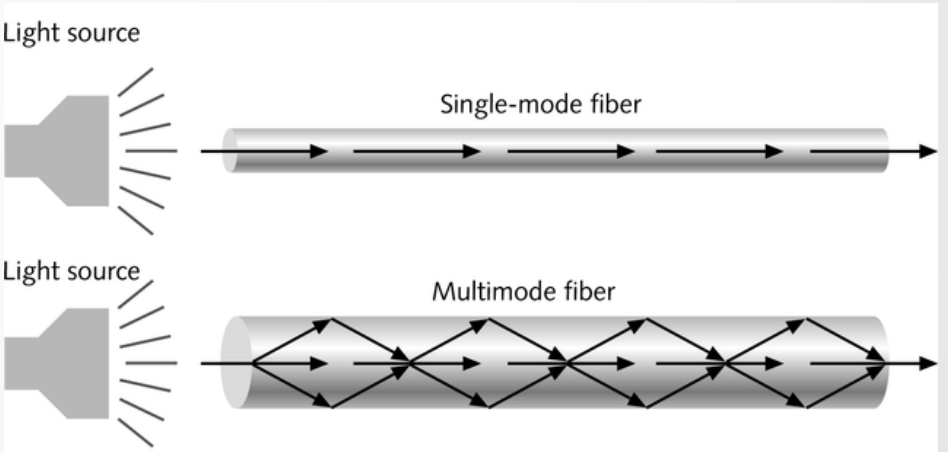


Fiber Media

- **Light travels through the optical media by the way of total internal reflection.**
- **Modulation scheme used is intensity modulation.**
- **Two types of Fiber media :**
  - Multimode
  - Singlemode
- **Multimode Fiber can support less bandwidth than Singlemode Fiber.**
- **Singlemode Fiber has a very small core and carry only one beam of light. It can support Gbps data rates over > 100 Km without using repeaters.**

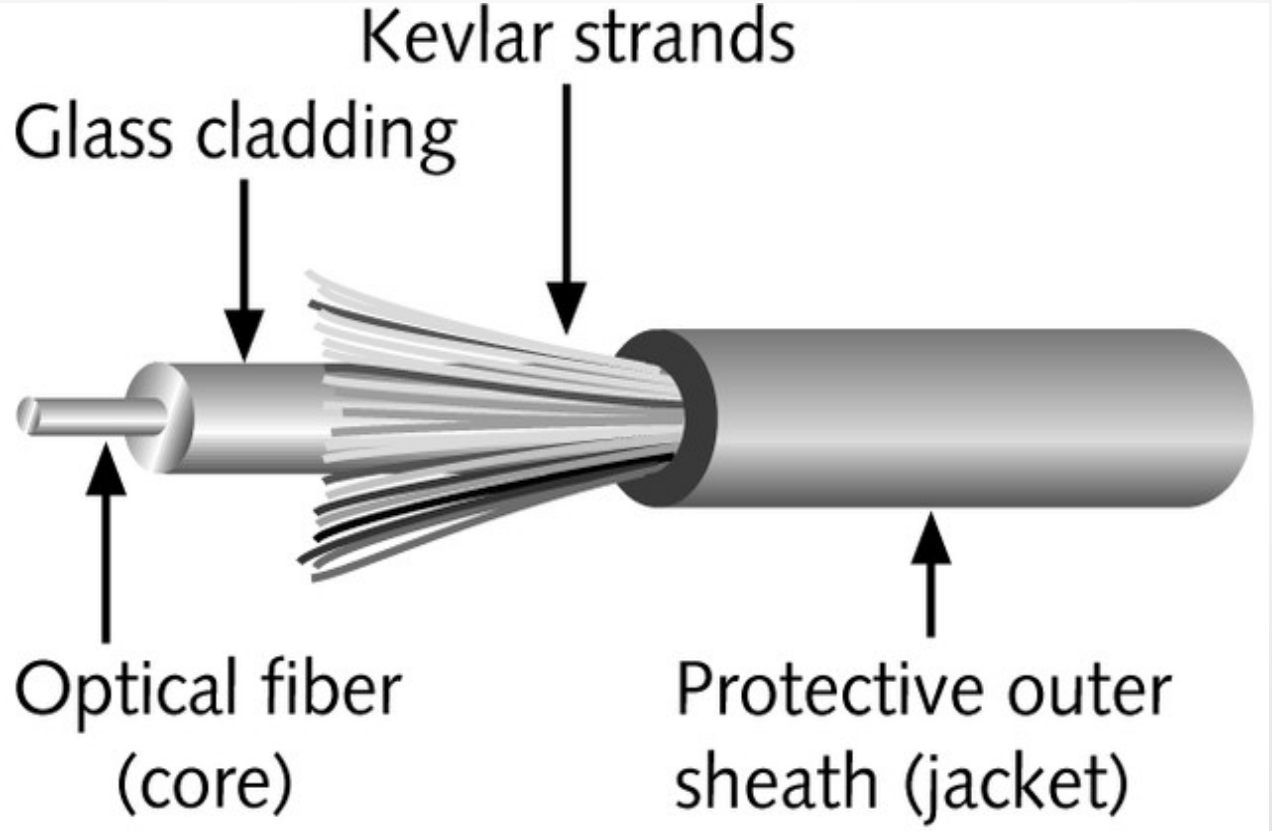
Single and Multimode Fiber

- **Single-mode fiber**
  - Carries light pulses along single path
  - Uses Laser Light Source
- **Multimode fiber**
  - Many pulses of light generated by LED travel at different angles



Fiber-Optic Cable

- Contains one or several glass fibers at its core
- Surrounding the fibers is a layer called cladding

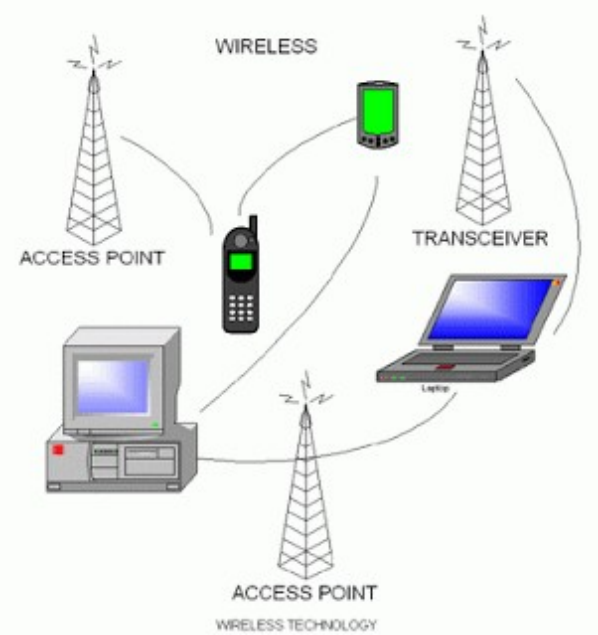


Fiber Optic Cable

- FO Cable may have 1 to over 1000 fibers

Wireless Transmission

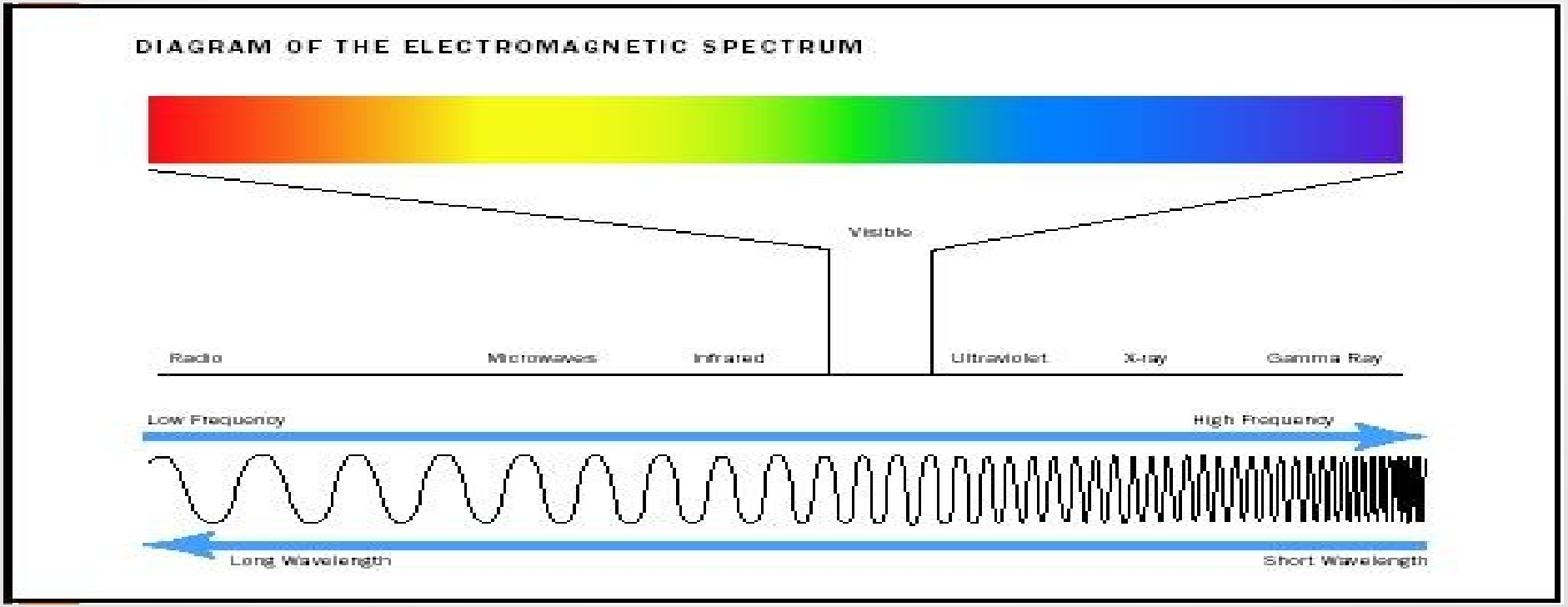
- *Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpret by appropriate antennas.*



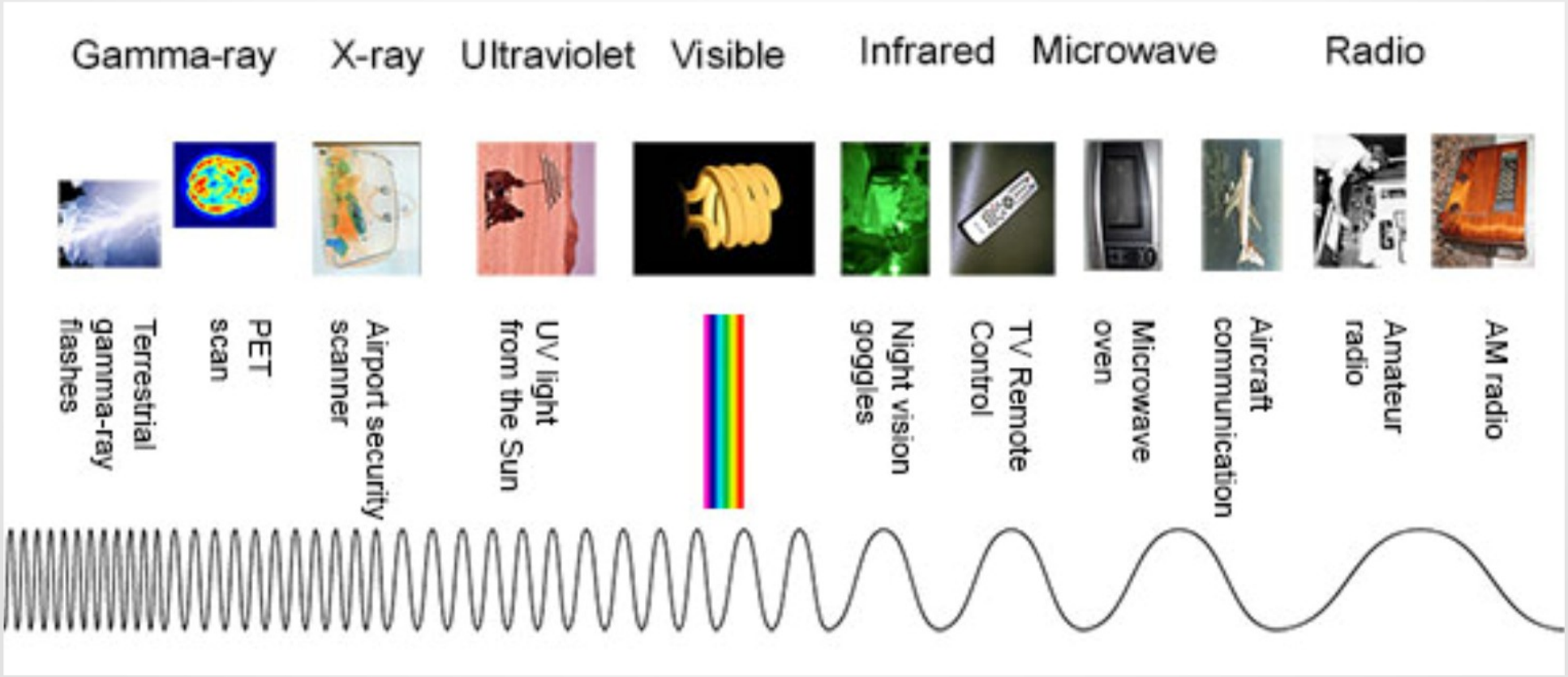
Wireless Transmission Disadvantages

1. Bit Error Rates (BER)
2. Wireless signals not confined.

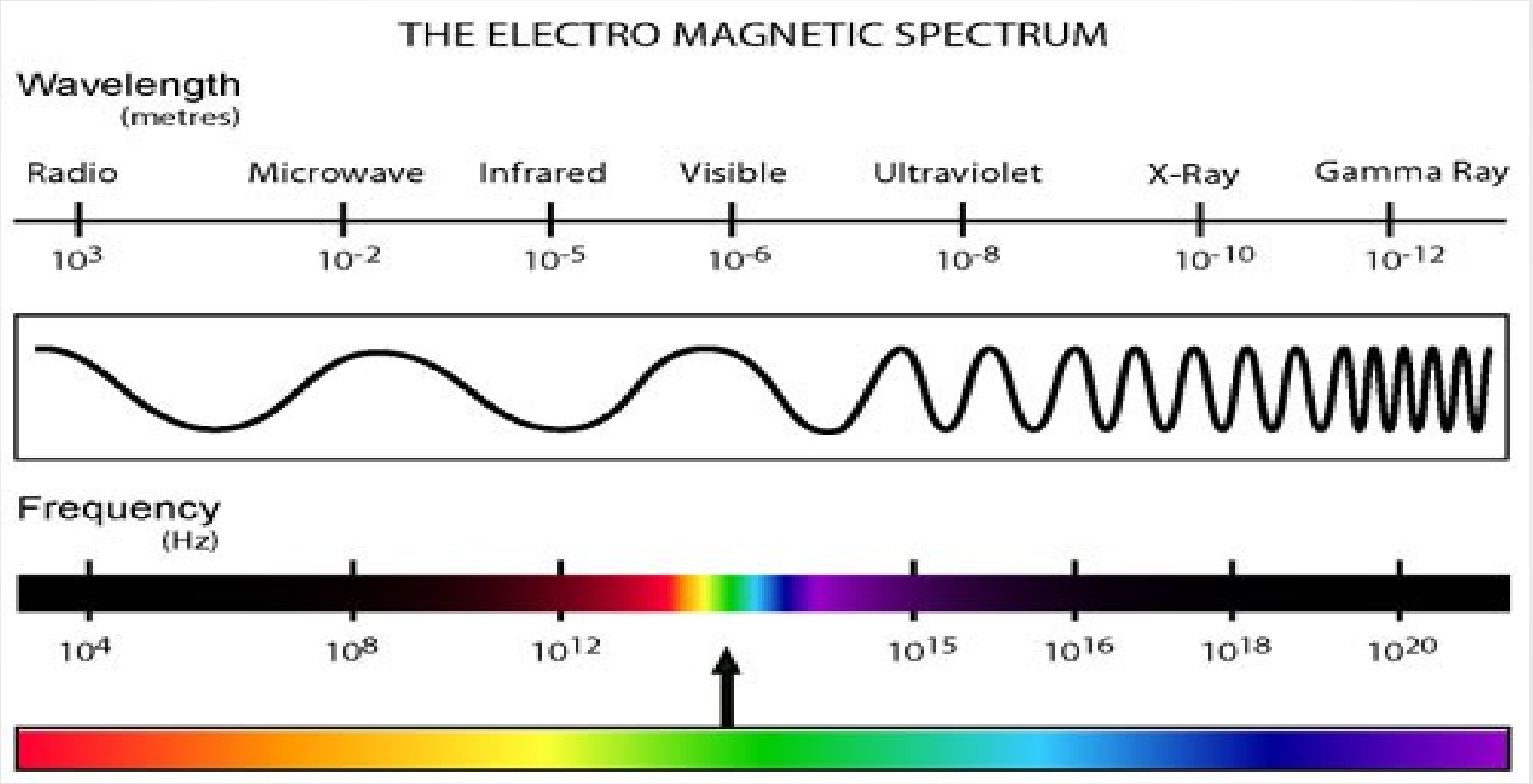
Electromagnetic Spectrum:



The image below shows where you might encounter each portion of the EM spectrum in your day-to-day life.



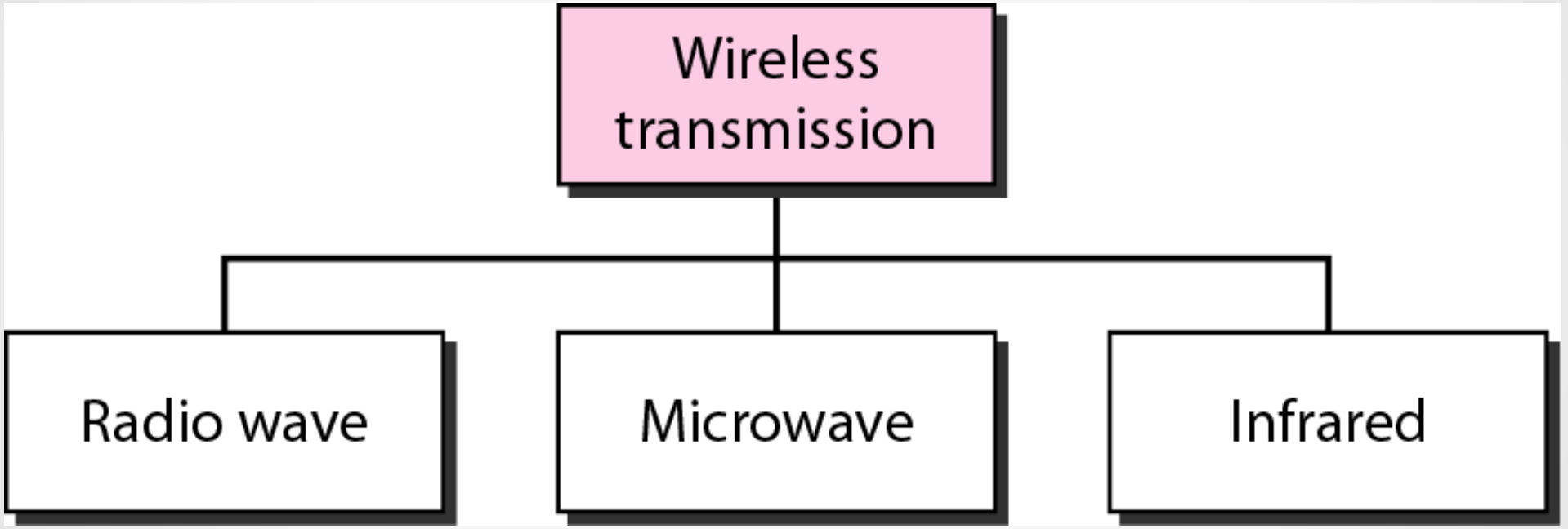
- ***Transmission Bands***



Band of Spectrum:

- Radio
- Microwave
- Infrared
- Lightwave
  - Ultraviolet Rays
  - Gamma rays
  - X - Rays

Wireless transmission waves



Note

Radio waves are used for multicast communications, such as radio and television, and paging systems.

• Radio Band

Frequency	Band Name	Applications
< 3 KHz	Extremely Low Frequency (ELF)	Submarine communications
3 KHz – 30 KHz	Very Low Frequency (VLF)	Marine communications
30 KHz – 300 KHz	Low Frequency (LF)	AM Radio
300 KHz – 3 MHz	Medium Frequency (MF)	AM Radio
3 MHz – 30 MHz	High Frequency (HF)	AM Radio
30 MHz – 300 MHz	Very High Frequency (VHF)	FM Radio - TV
300 MHz – 3 GHz	Ultra High Frequency (UHF)	TV – Cellular telephony
3 GHz – 30 GHz	Super High Frequency (SHF)	Satellites
30 GHz – 300 GHz	Extra High Frequency (EHF)	Satellites - Radars

Various Radio Bands and its Common Use

• Microwave Band

TABLE 1: MICROWAVE LETTER BAND DESIGNATIONS		
Band	Frequency range	Applications
L	1 to 2 GHz	Satellite, navigation (GPS, etc.), cellular phones
S	2 to 4 GHz	Satellite, SiriusXM radio, unlicensed (Wi-Fi, Bluetooth, etc.), cellular phones
C	4 to 8 GHz	Satellite, microwave relay
X	8 to 12 GHz	Radar
K_u	12 to 18 GHz	Satellite TV, police radar
K	18 to 26.5 GHz	Microwave backhaul
K_a	26.5 to 40 GHz	Microwave backhaul
Q	30 to 50 GHz	Microwave backhaul
U	40 to 60 GHz	Experimental, radar
V	50 to 75 GHz	New WLAN, 802.11ad/WiGig
E	60 to 90 GHz	Microwave backhaul
W	75 to 110 GHz	Automotive radar
F	90 to 140 GHz	Experimental, radar
D	110 to 170 GHz	Experimental, radar

Various Microvawe Bands and its Common Use

• Infrared (IR)

- *These radiation is located below the spectrum of red visible light.*
- *Such rays are emitted by very hot objects and the frequency depends on the temperature of the emitting body.*
- *Applications:*
  - *Night Vision Devices*
  - *Infrared light from the LED of Remote*
  - *Digital Cameras*
  - *Heating in medical field*
  - *Communications etc.*

• Lightwaves

- *The Lightwaves or visible spectrum is the portion of the electromagnetic spectrum that is visible to (can be detected by) the human eye. Electromagnetic radiation in this range of wavelengths is called visible light or simply light. A typical human eye will respond to wavelengths from about 390 to 700 nm. In terms of frequency, this corresponds to a band in the vicinity of 430–790 Thz.*

- *Ultraviolets Rays (UV)*
- *X -Rays*
- *Gamma Rays*

Network Devices

Functions of network devices

- **Separating (connecting) networks or expanding network**
  - **e.g. repeaters, hubs, bridges, routers, brouters, switches, gateways**

Hub and Repeater

- Repeaters or hubs work at the OSI physical layer to regenerate the network's signal and resend them to other segments.
- Primitive hub can be viewed as a multiport repeater.
- It regenerates data and broadcasts them to all ports.
- Hub connect networking devices physically together.
- Hubs are fundamentally used in networks that use twisted pair cabling to connect devices.
- They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received.
- They act as pathways to direct electrical signals to travel along.

Hub falls in two categories:

Active Hub:

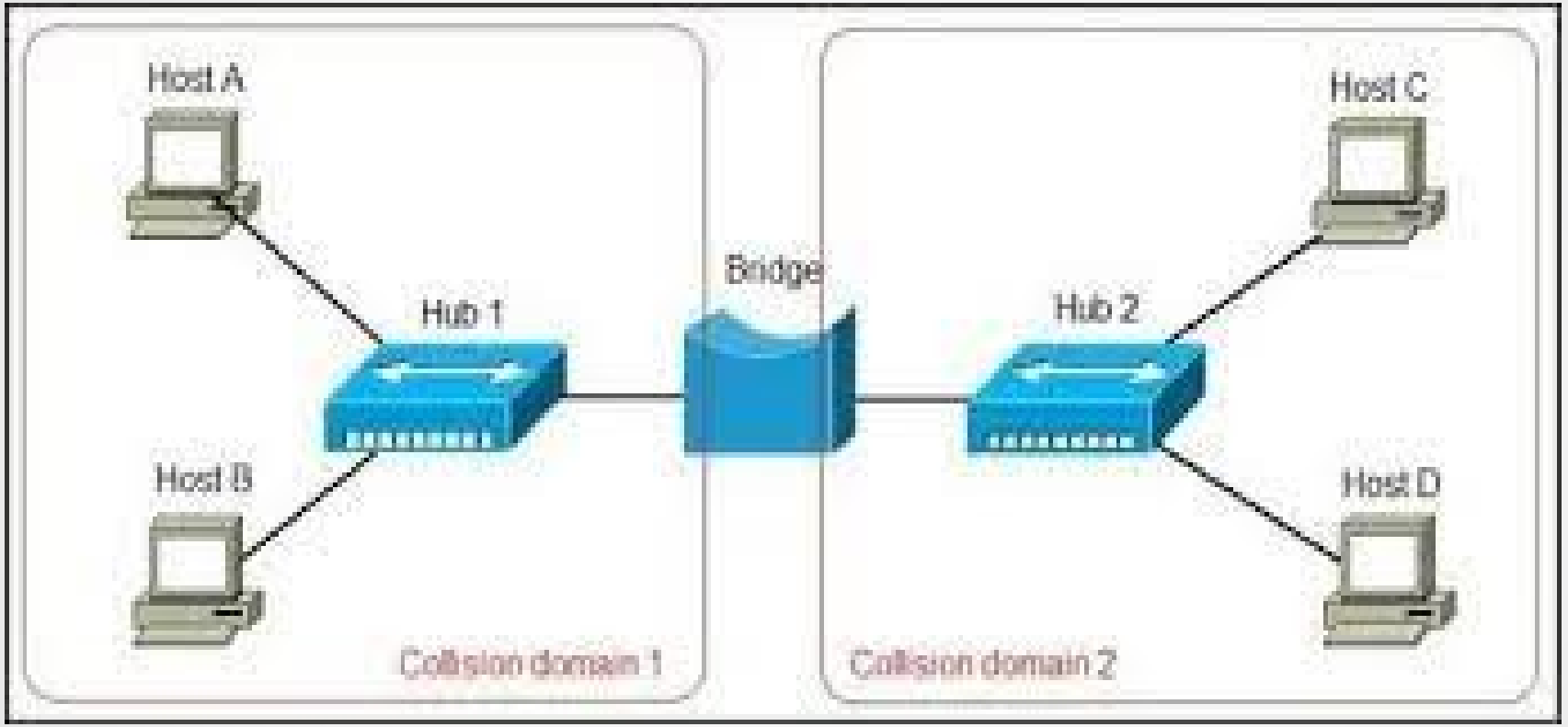
They are smarter than the passive hubs. They not only provide the path for the data signals infact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as ‘repeaters’.

Passive Hub:

They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.

Bridge

- It works at the Data Link layer and connects the different networks together and develops communication between them.
- A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.

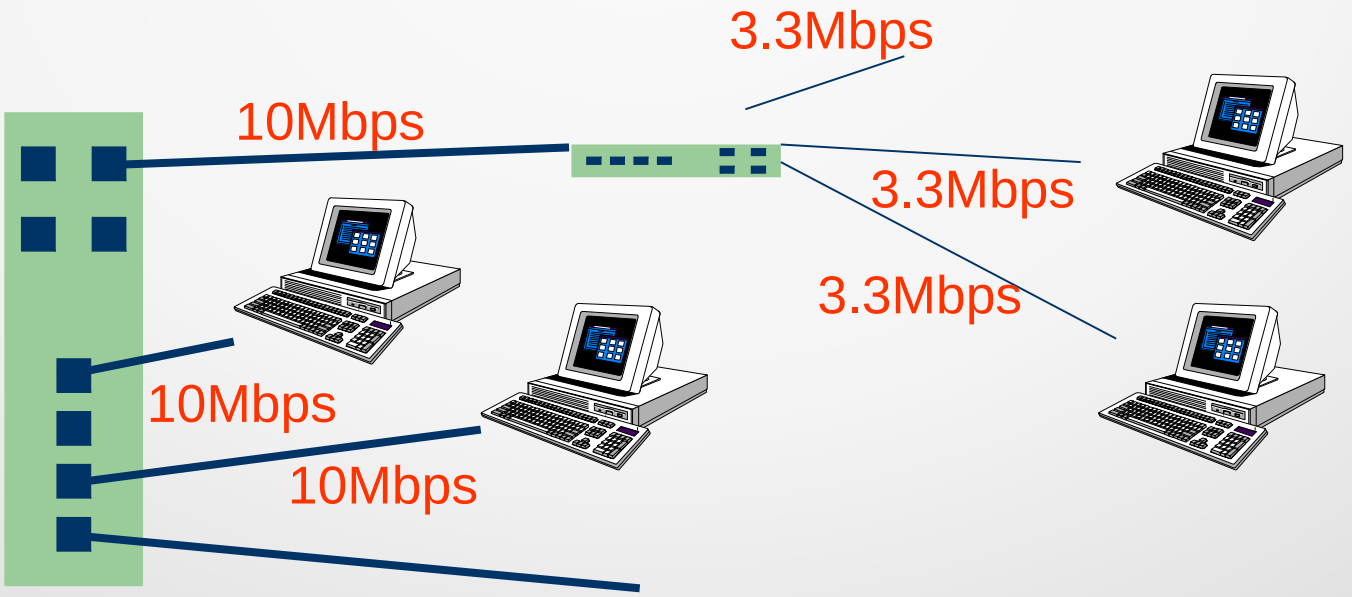

Host A
Host C
Bridge
Hub 1
Hub 2
Host B
Host D
Collision domain 1
Collision domain 2

Switches

- Switches operate at the Data Link layer (layer 2) of the OSI model.
- Switches resemble bridges and can be considered as multiport bridges.
- Can interpret address information.
- By having multiports, can better use limited bandwidth and prove more cost-effective than bridge.
- It stores MAC addresses in an internal lookup table.

Contd..

- **Switches divide a network into several isolated channels**
- **Packets sending from 1 channel will not go to another if not specify**



Advantages of Switches

- Switches divide a network into several isolated channels (or collision domains)
  - Reduce the possibility of collision
    - Collision only occurs when two devices try to get access to one channel
    - Can be solved by buffering one of them for later access
  - Each channel has its own network capacity
    - Suitable for real-time applications, e.g. video conferencing
  - Since isolated, hence secure
    - Data will only go to the destination, but not others

Routers

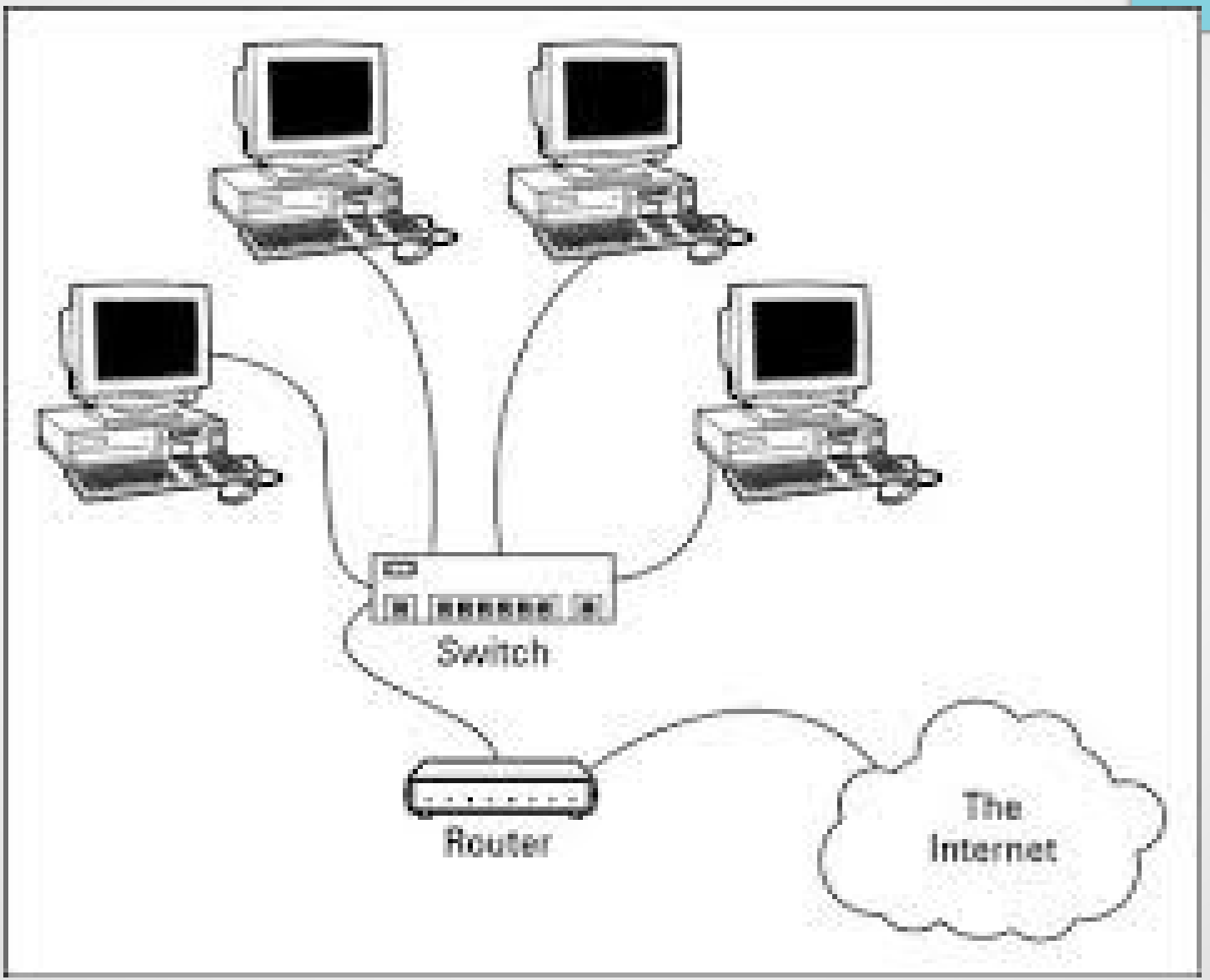
A router is a device like a switch that routes data packets based on their IP addresses.

The router is mainly a Network Layer device.

- They use the “logical address” of packets and routing tables to determine the best path for data delivery.
- These devices examine incoming packets to determine the destination address of the data. It then examines its internal routing table to choose the best path for the packet through the network, and switches them to the proper outgoing port.

Working of router

- As packets are passed from routers to routers, Data Link layer source and destination addresses are stripped off and then recreated
- Enables a router to route a packet from a TCP/IP Ethernet network to a TCP/IP token ring network
- Only packets with known network addresses will be passed - hence reduce traffic
- Routers can listen to a network and identify its busiest part
- Will select the most cost effective path for transmitting packets


Switch
Router
The
Internet

Distinguishing Between Bridges and Routers

- Routers are layer 3 devices which recognize network address
- Bridges are layer 2 devices which look at the MAC sublayer node address
- Bridges forward everything they don't recognize
- Routers select the best path

Routers

- Connect 2 or more networks.
- Combination of H/w and S/w.
- Use Logical and Physical addressing.
- Routers work at the network layer.

Wireless Router

Wired Router

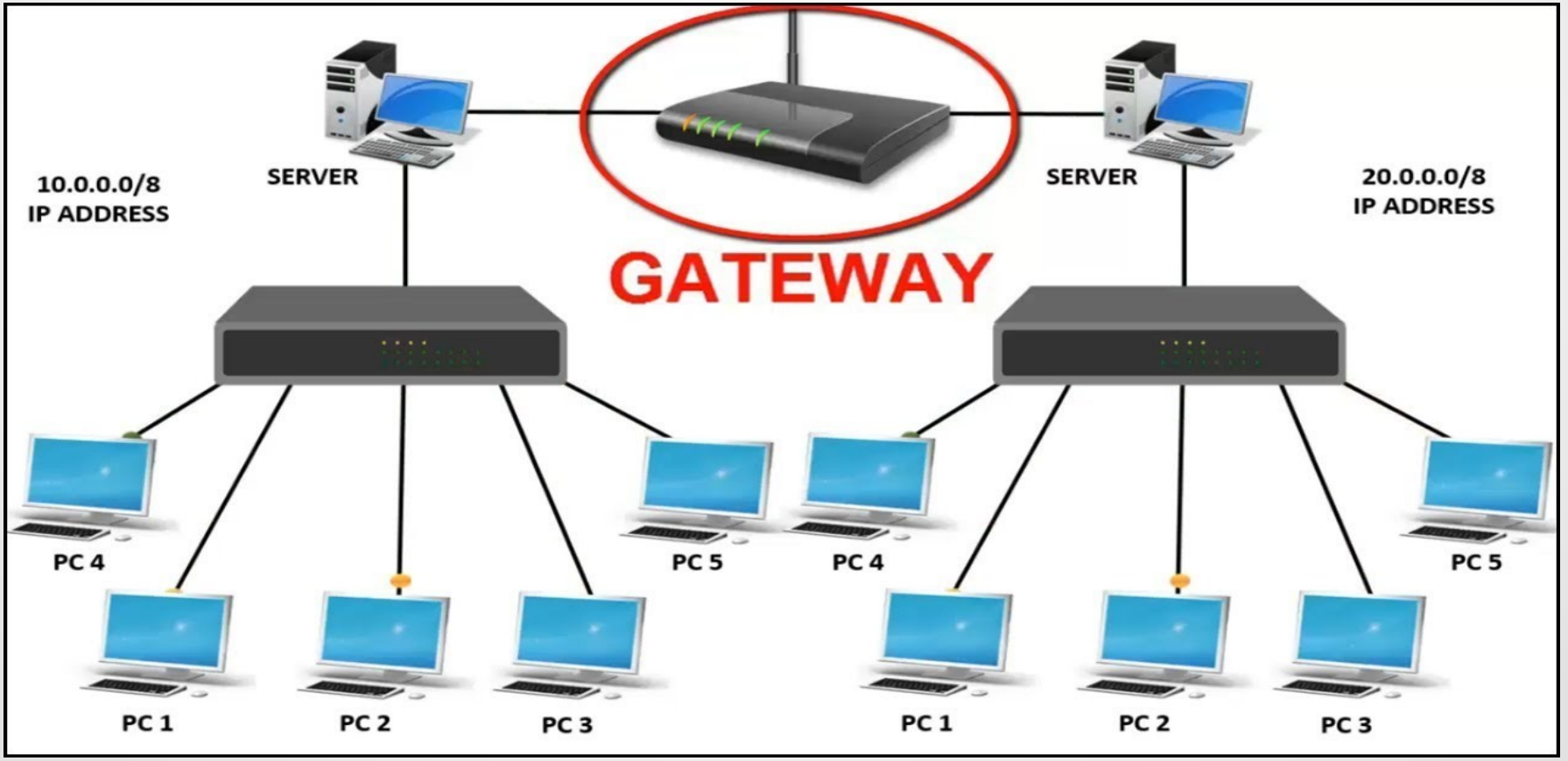
Computer

Summary

- **Repeaters** are the least expensive way to expand a network, but they are limited to connecting two segments.
- **Bridges** function similar to repeaters, but can understand the node addresses.
- **Switches** can be considered as multiport bridges, can divide a network into some logical channels.
- **Routers** interconnect networks and provide filtering functions. They can determine the best route.

Gateway

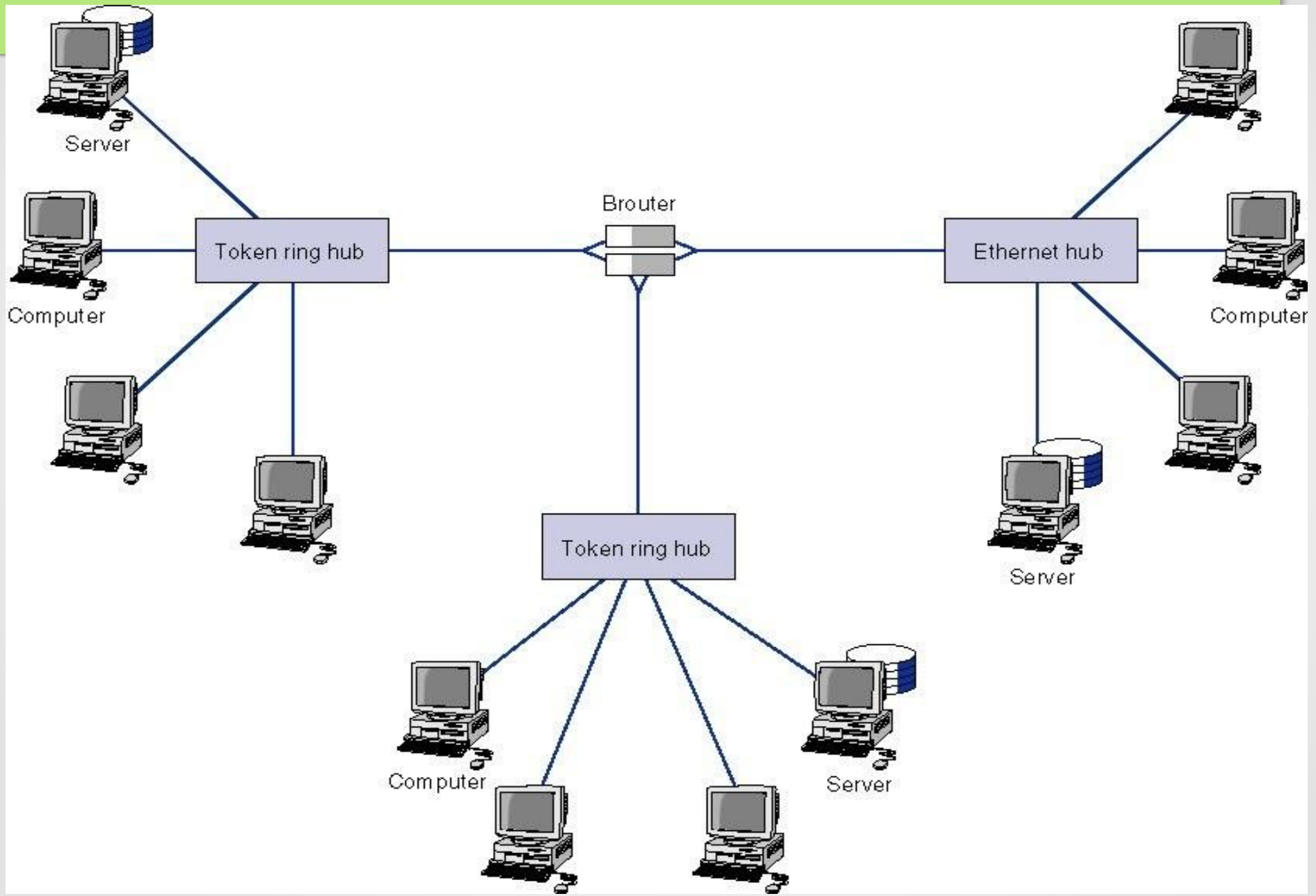
- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than switches or routers.
- A gateway is a hardware device that goes about as a “gate” between two networks.


10.0.0.0/8
IP ADDRESS
SERVER
GATEWAY
SERVER
20.0.0.0/8
IP ADDRESS
PC 4
PC 5
PC 1
PC 2
PC 3
PC 4
PC 5
PC 1
PC 2
PC 3

Brouters

- **Brouters** are devices that combine the functions of both bridges and routers.
- These operate at both the data link and network layers.
- A brouter connects both same and different data link type network LAN segments.
- It is as fast as a bridge for same data link type networks, but can also connect different data link type networks.
- They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems.
- Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.

Contd..


Server
Brouter
Token ring hub
Ethernet hub
Computer
Computer
Token ring hub
Server
Computer
Server

Access Point (AP)

- Short for ***A****ccess* ***P****oint*, a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN.

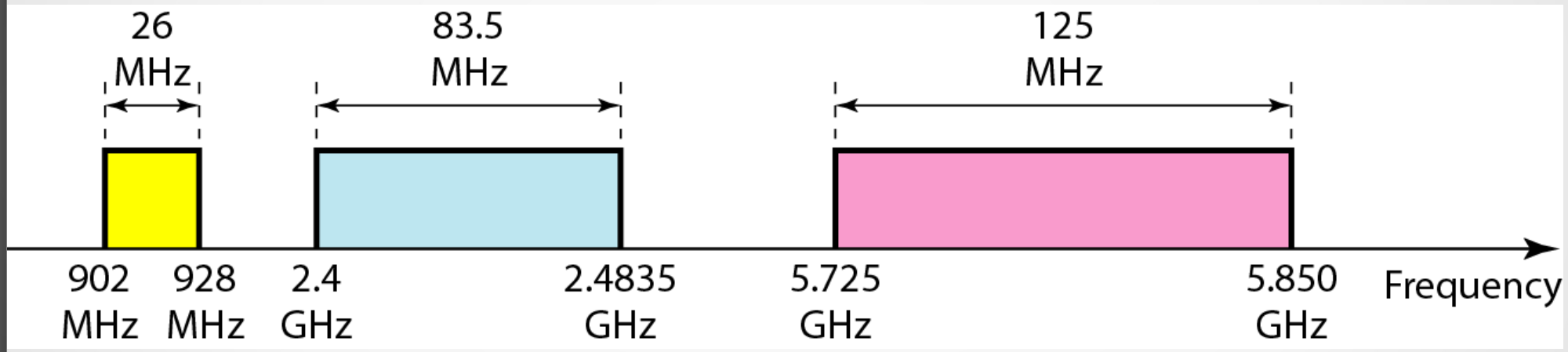
- APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to.

Physical Layer

Following all 6 implementations, except the infrared, operate in the **industrial, Scientific, and medical (ISM) band**, which defines three unlicensed bands in the three ranges 902-928 MHz, 2.400-4.835 GHz, and 5.725-5.850 Ghz.

IEEE	*Technique*	*Band*	*Modulation*	*Rate (Mbps)*
802.11	FHSS	2.4 GHz	FSK	1 and 2
	DSSS	2.4 GHz	PSK	1 and 2
		Infrared	PPM	1 and 2
802.11a	OFDM	5.725 GHz	PSK or QAM	6 to 54
802.11b	DSSS	2.4 GHz	PSK	5.5 and 11
802.11g	OFDM	2.4 GHz	Different	22 and 54

Industrial, scientific, and medical (ISM) band



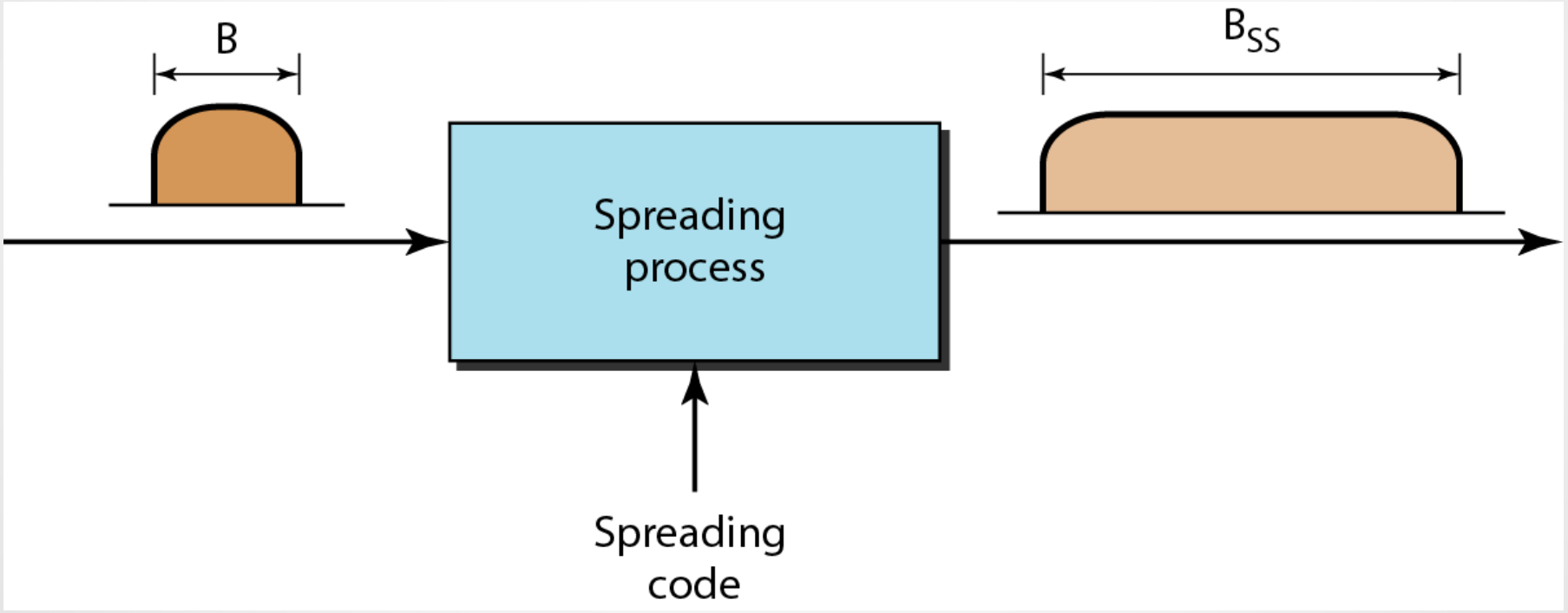
• SPREAD SPECTRUM

- ***In spread spectrum (SS), we combine signals from different sources to fit into a larger bandwidth, but our goals are to prevent eavesdropping and jamming. To achieve these goals, spread spectrum techniques add redundancy.***

SPREAD SPECTRUM

- - Important encoding method for wireless communications
- - Analog & digital data with analog signal
- - Spreads data over wide bandwidth
- - Makes jamming and interception harder
- - Two approaches, both in use:
  - 1. Frequency Hopping Spread Spectrum (FHSS)
    2. Direct Sequence Spread Spectrum (DSSS)

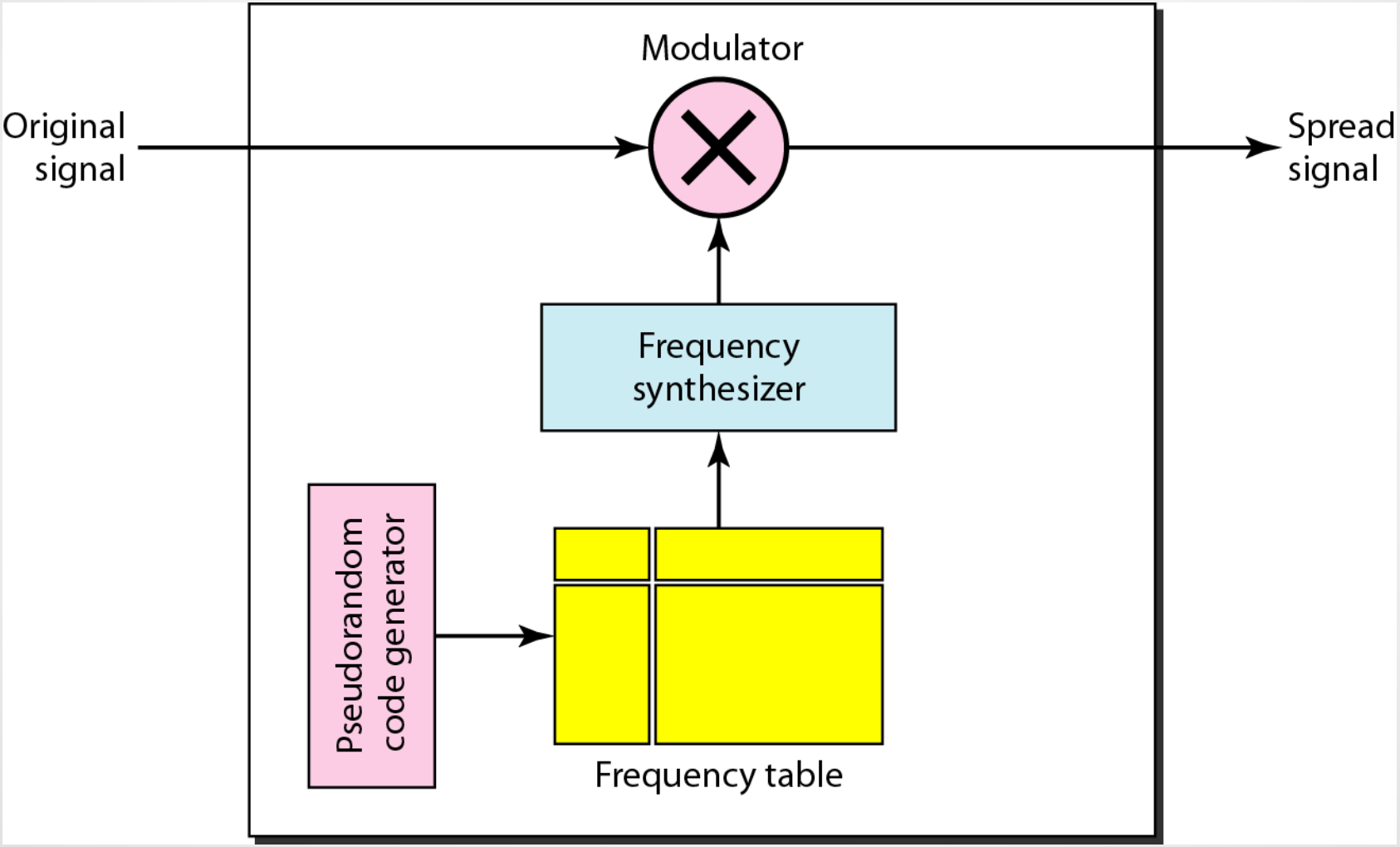
- ***Spread spectrum***



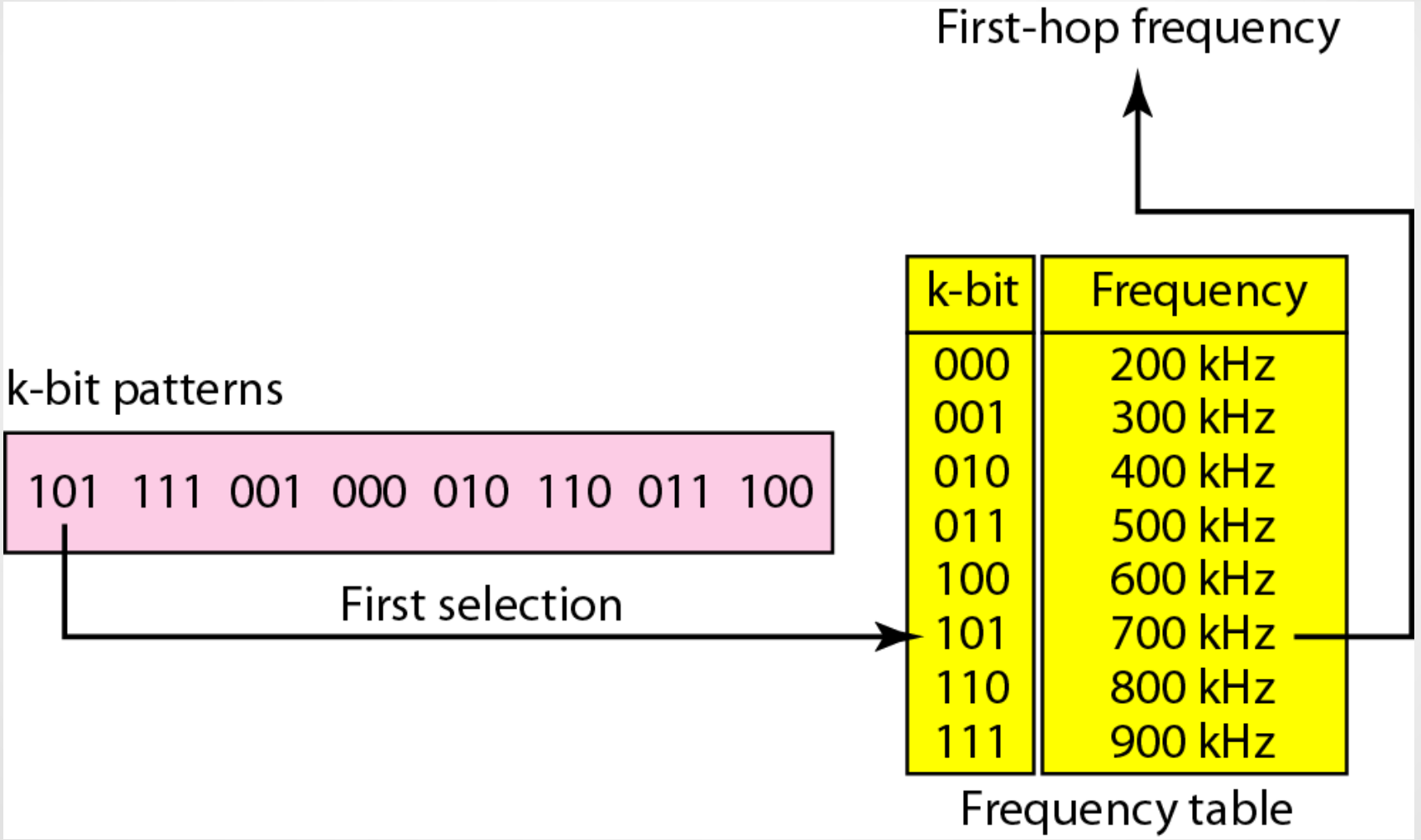
802.11 Frequency Hopping Spread Spectrum (FHSS)

- - FHSS uses M different carrier frequencies that are modulated by the source signal.
- - At one moment, the signal modulated one carrier frequency, at next moment, the signal modulates another carrier frequency.
- - $B_{FHSS} >> B$
- - Jamming on one frequency affects only a few bits.

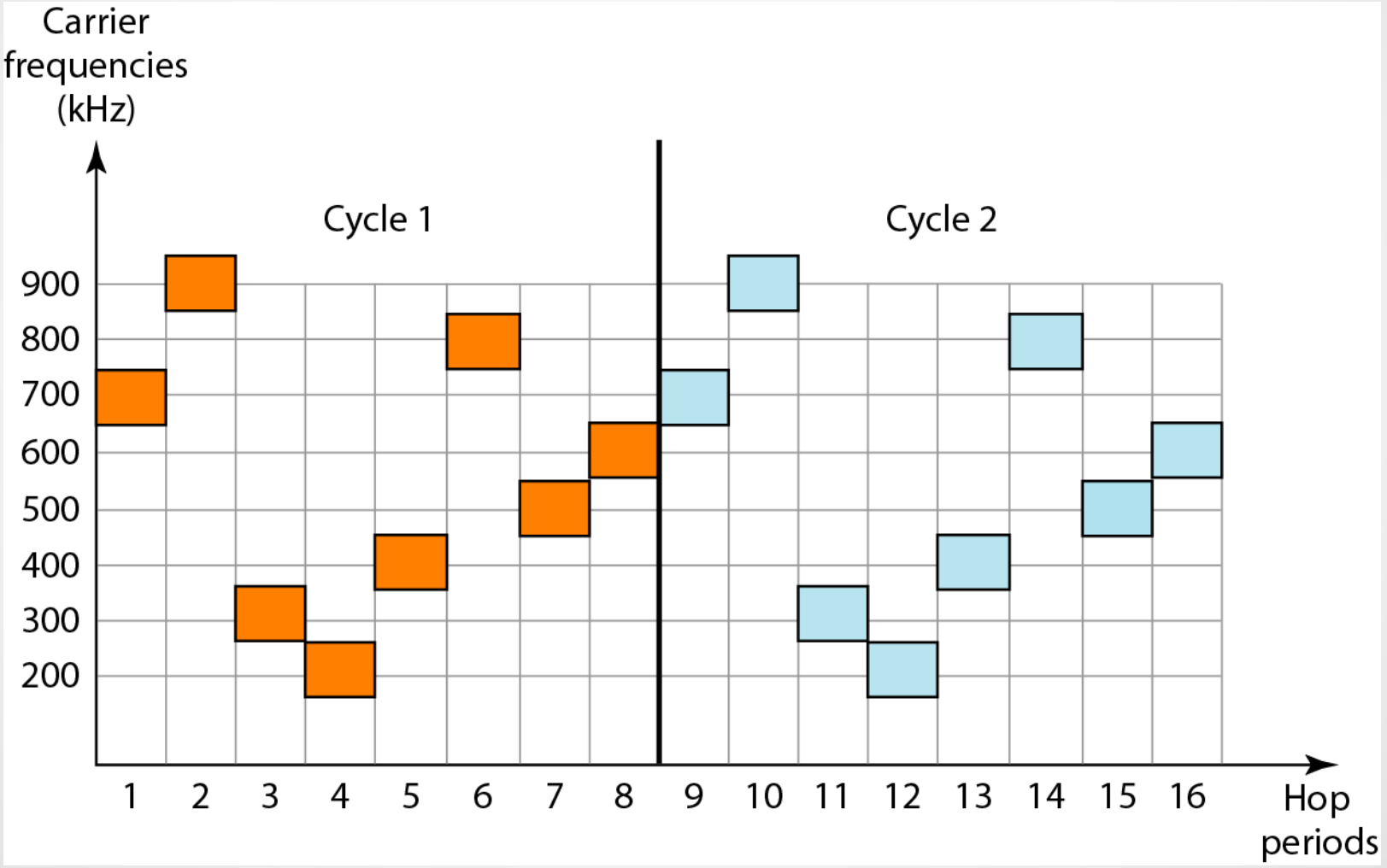
- ***Frequency hopping spread spectrum (FHSS)***



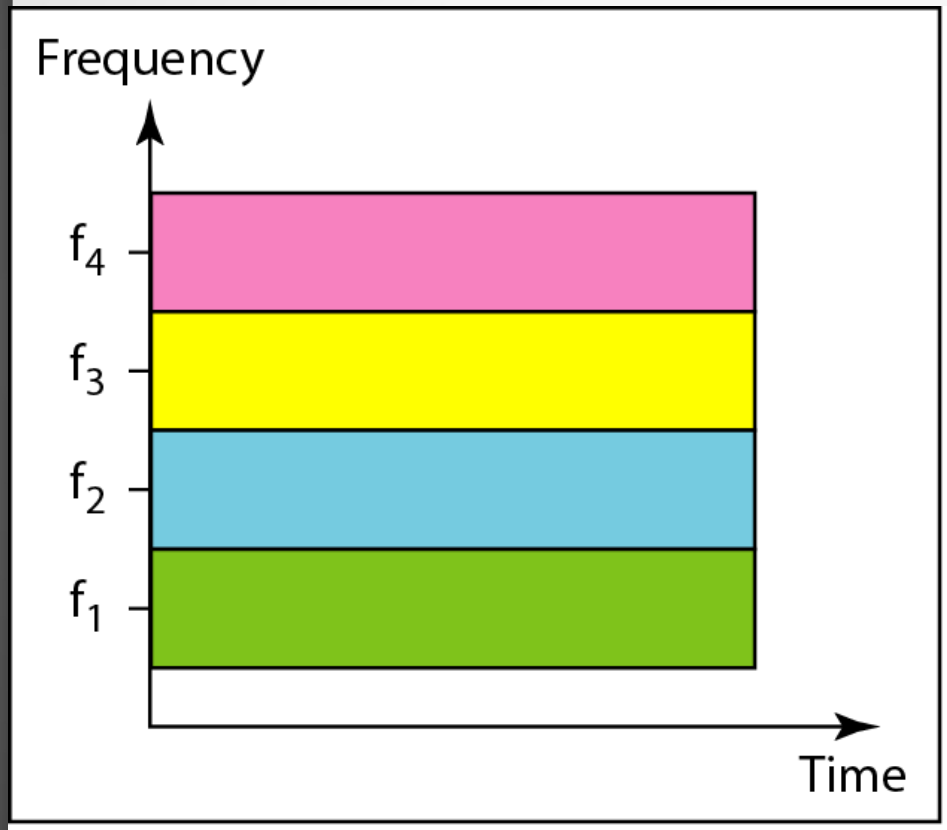
- ***Frequency selection in FHSS***



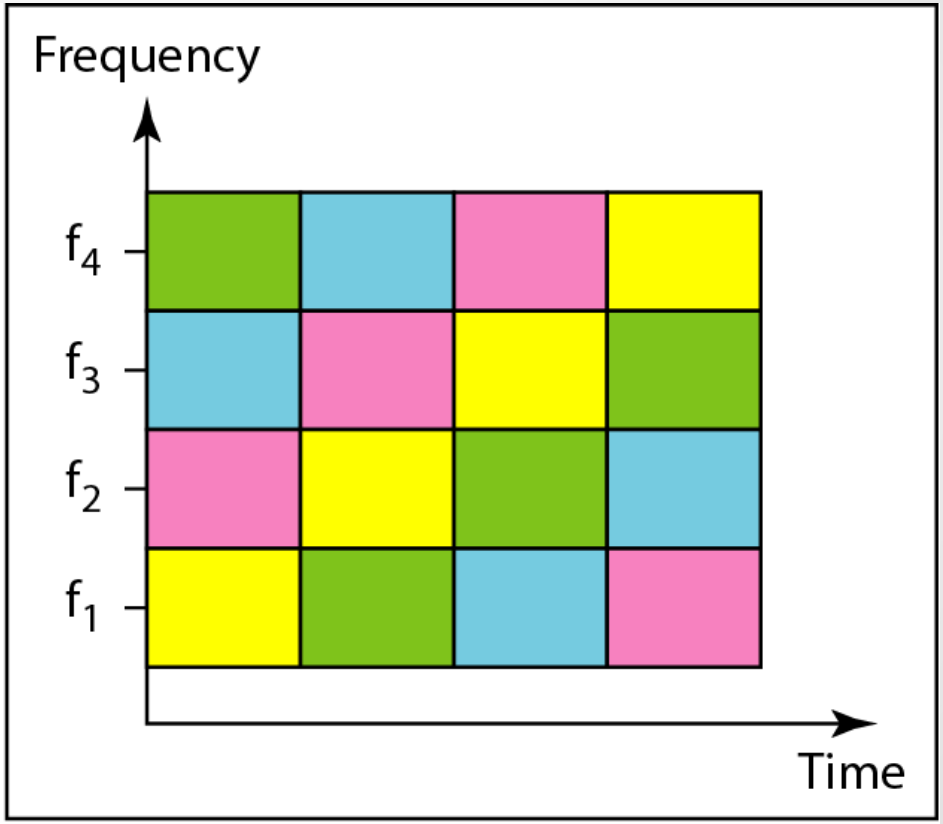
- ***FHSS cycles***


Carrier frequencies (kHz)
Cycle 1
Cycle 2
900
800
700
600
500
400
300
200
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
Hop periods

- ***Bandwidth sharing***



a. FDM

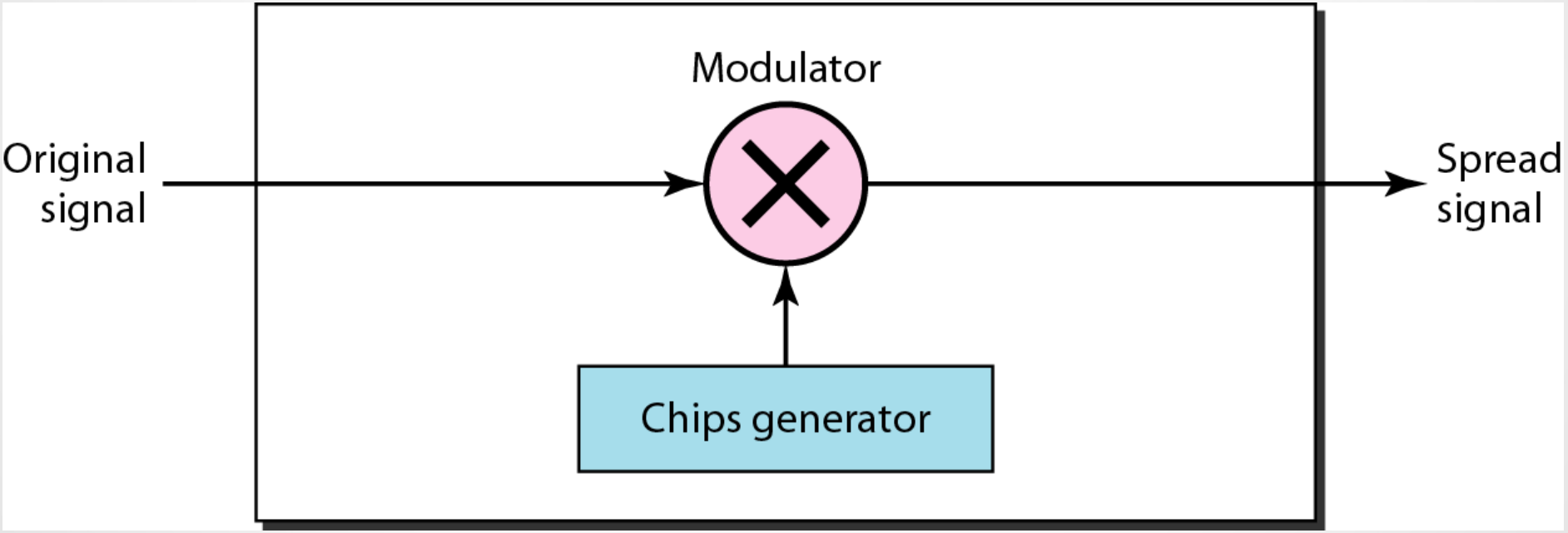


b. FHSS

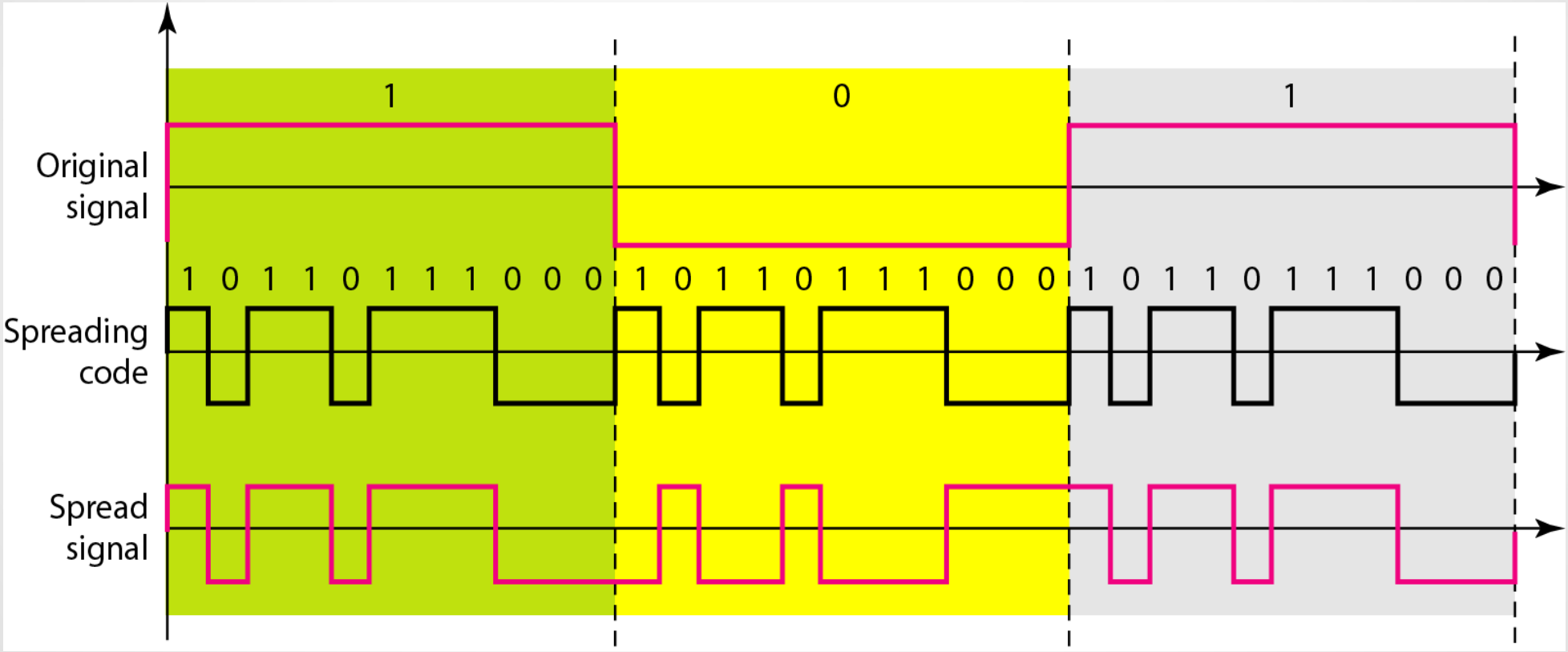
Direct Sequence Spread Spectrum (DSSS)

- - Each bit is represented by multiple bits using a spreading code.
- - In other words, each bit is assigned a code of ***n*** bits, called chips.
- - This spreads signal across a wider frequency band.
- - Has performance similar to FHSS.

- ***DSSS***



- ***DSSS example***



Spread Spectrum Advantages

- Immunity from noise and multipath distortion.
- Can hide / encrypt signals.
- Several users can share same higher bandwidth with little interference.
- Eg:
  - CDM/CDMA Mobile telephones