COMPUTER COMMUNICATION
EC 407

Syllabus

COURSE CODE	COURSE NAME	L-T-P-C	YEAR OF INTRODUCTION
EC407	COMPUTER COMMUNICATION	3-0-0-3	2016

Prerequisite: NIL

Course objectives:

- To give the basic concepts of computer network and working of layers, protocols and interfaces in a computer network.
- To introduce the fundamental techniques used in implementing secure network communications and give them an understanding of common threats and its defences.

Module	Course content (42 hrs)	Hours	End Sem. Exam Marks
I	Introduction to computer communication: Transmission modes - serial and parallel transmission, asynchronous, synchronous, simplex, half duplex, full duplex communication. Switching: circuit switching and packet switching	2	15%

Syllabus

	Networks: Network criteria, physical structures, network models, categories of networks, Interconnection of Networks: Internetwork	2	
	Network models: Layered tasks, OSI model, Layers in OSI model, TCP/IP protocol suite.	2	
II	Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP,STP, Fiber optic cable)	2	15%
	Data Link Layer: Framing, Flow control (stop and wait , sliding window flow control)	2	
	Error control, Error detection(check sum, CRC), Bit stuffing, HDLC	2	
	Media access control: Ethernet (802.3), CSMA/CD, Logical link control, Wireless LAN (802.11), CSMA/CA	2	
FIRST INTERNAL EXAM			

Syllabus

III	Network Layer Logical addressing : IPv4 & IPV6	2	15%
	Address Resolution protocols (ARP, RARP)	2	
	Subnetting, Classless Routing(CIDR), ICMP, IGMP, DHCP	3	
	Virtual LAN, Networking devices (Hubs, Bridges & Switches)	1	
IV	Routing: Routing and Forwarding, Static routing and Dynamic routing	1	15%
	Routing Algorithms: Distance vector routing algorithm, Link state routing (Dijkstra's algorithm)	2	
	Routing Protocols: Routing Information protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), MPLS	3	
SECOND INTERNAL EXAM			
V	Transport Layer –UDP, TCP	1	20%
	Congestion Control & Quality of Service – Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics	4	
	Application Layer – DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP	3	

Syllabus

VI	Introduction to information system security, common attacks	1	20%
	Security at Application Layer (E-MAIL, PGP and S/MIME). Security at Transport Layer (SSL and TLS). Security at Network Layer (IPSec).	3	
	Defence and counter measures: Firewalls and their types. DMZ, Limitations of firewalls, Intrusion Detection Systems -Host based, Network based, and Hybrid IDSs	2	
END SEMESTER EXAM			

Question Paper Pattern

The question paper shall consist of three parts. Part A covers modules I and II, Part B covers modules III and IV, and Part C covers modules V and VI. Each part has three questions uniformly covering the two modules and each question can have maximum four subdivisions. In each part, any two questions are to be answered. Mark patterns are as per the syllabus with 90% for theory and 10% for logical/numerical problems, derivation and proof.

References

Text Books:

1. Behrouz A. Forouzan, Cryptography & Network Security , , IV Edition, Tata McGraw-Hill, 2008
2. J F Kurose and K W Ross, Computer Network A Top-down Approach Featuring the Internet, 3/e, Pearson Education, 2010

References:

1. Behrouz A Forouzan, Data Communications and Networking, 4/e, Tata McGraw-Hill, 2006.
2. Larry Peterson and Bruce S Davie: Computer Network- A System Approach, 4/e, Elsevier India, 2011.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson Education, 2005.
4. Achyut S.Godbole, Data Communication and Networking, 2e, McGraw Hill Education New Delhi, 2011

UNIT 1

Social Network

- In social science, a **social relation** or **social interaction** refers to a **relationship between two , three or more individuals** (e.g. a social group).

- Normally **social network** is filled with **peoples**.

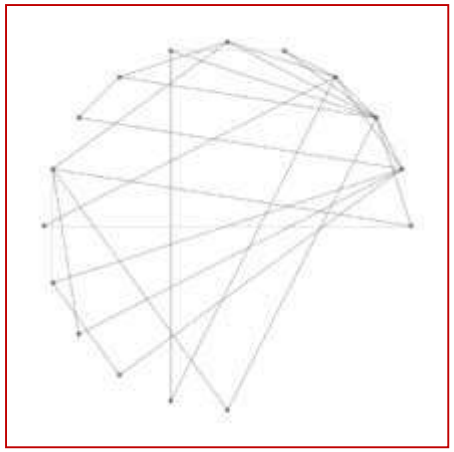
- Social networking allow users to **share ideas, activities, events,** and **interests within their individual networks**.

Social Network

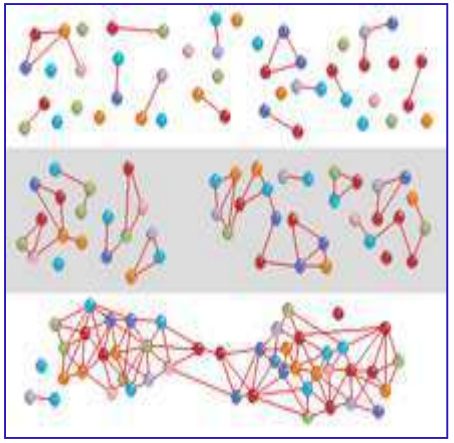
- To **protect user privacy,** social networks usually have controls that allow **users to choose who can view their profile**, **contact them, add them to their list of contacts**, and so on.

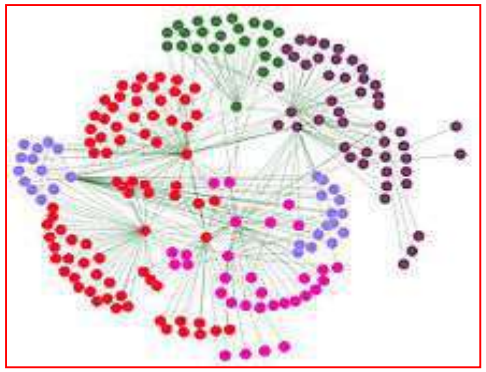
- Popular methods now combine many of these, with **Face book and Twitter** widely used worldwide.

Pictorial Representation of Social Networks

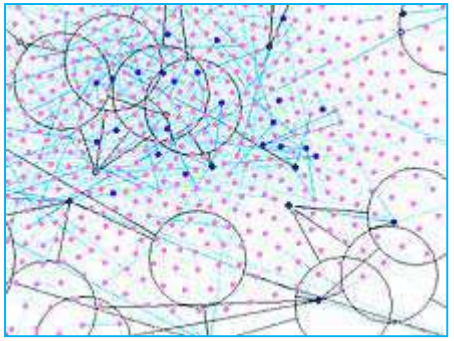


Simple





Complex



Aim for Networking

- The main **aim for networking is Communication**

- **Communication** means **sharing something**

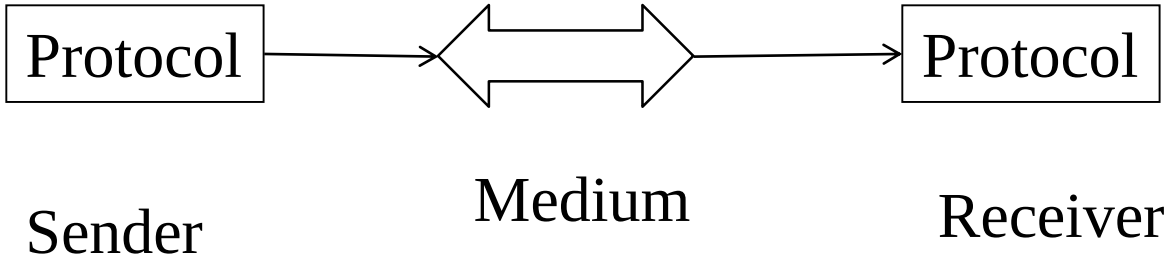
Fundamental Concepts

- **Communication**
  - **Means Sharing of information.**
- **Sharing may be**
  - **Local**
    - **Transmits information locally**
  - **Remote**
    - **Sending information to remote places.**
- **Data**
  - **Information is called data.**
- **Data communication**
  - **Sharing of information between two devices**

FUNDAMENTAL CONCEPTS

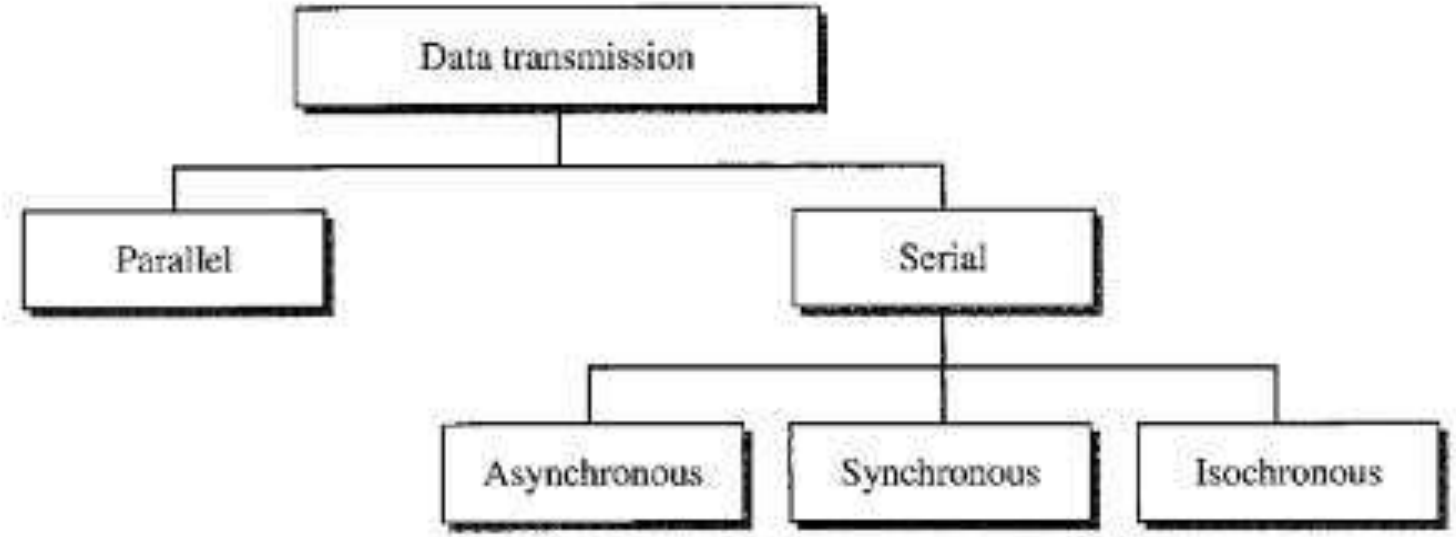
- **Effectiveness of Data Communication Depends on**
  - **Delivery**
  - **Accuracy**
  - **Timeless**

Data Communication Model

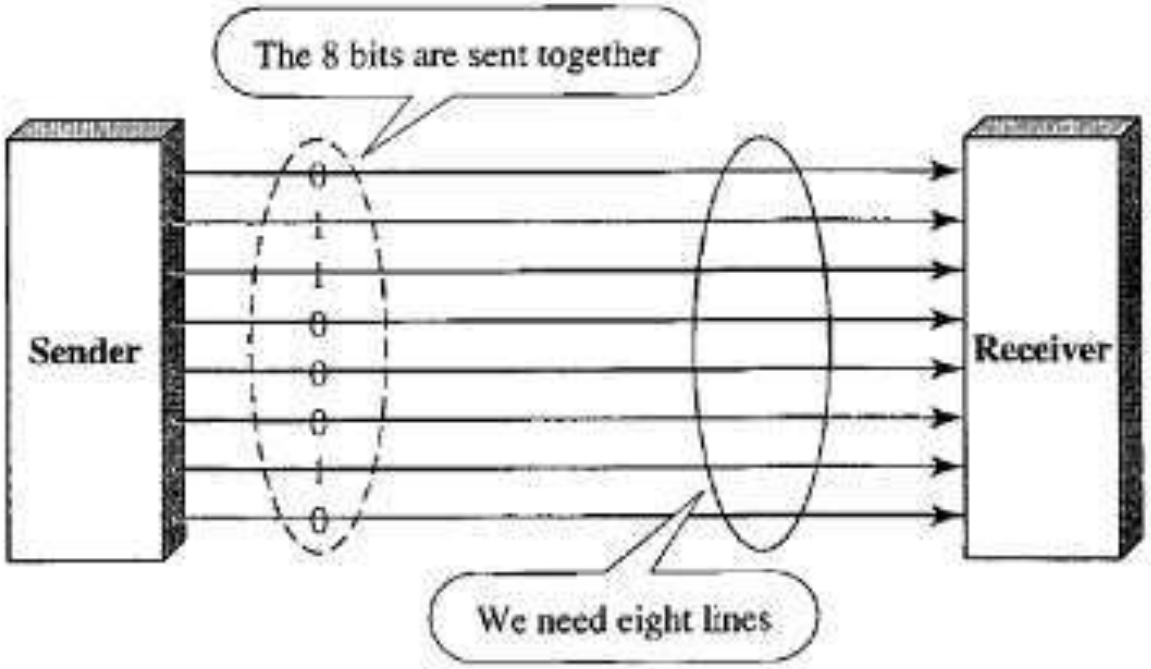


- **Protocols**
  - Specifies **common set of rules** and signals which computers on the network use to communicate.
- **Protocol suite or protocol stack**
  - The **total package of protocols.**

Transmission Modes

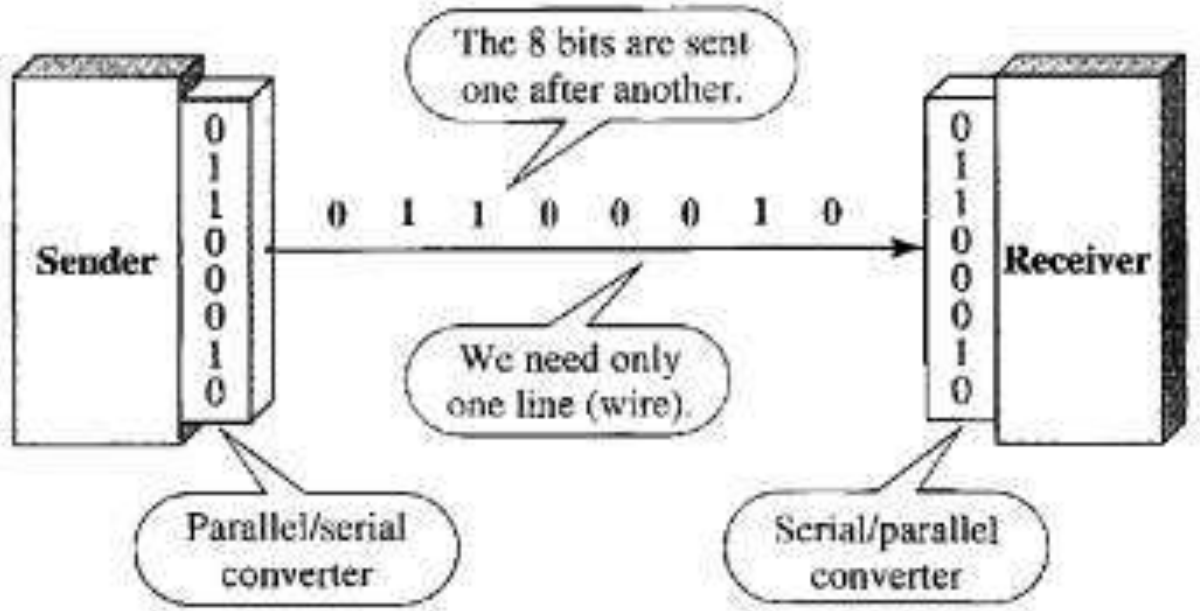

Data transmission
Parallel
Serial
Asynchronous
Synchronous
Isochronous

Parallel Transmission



- Advantage : Higher speed
- Disadvantage : Communication cost is high.

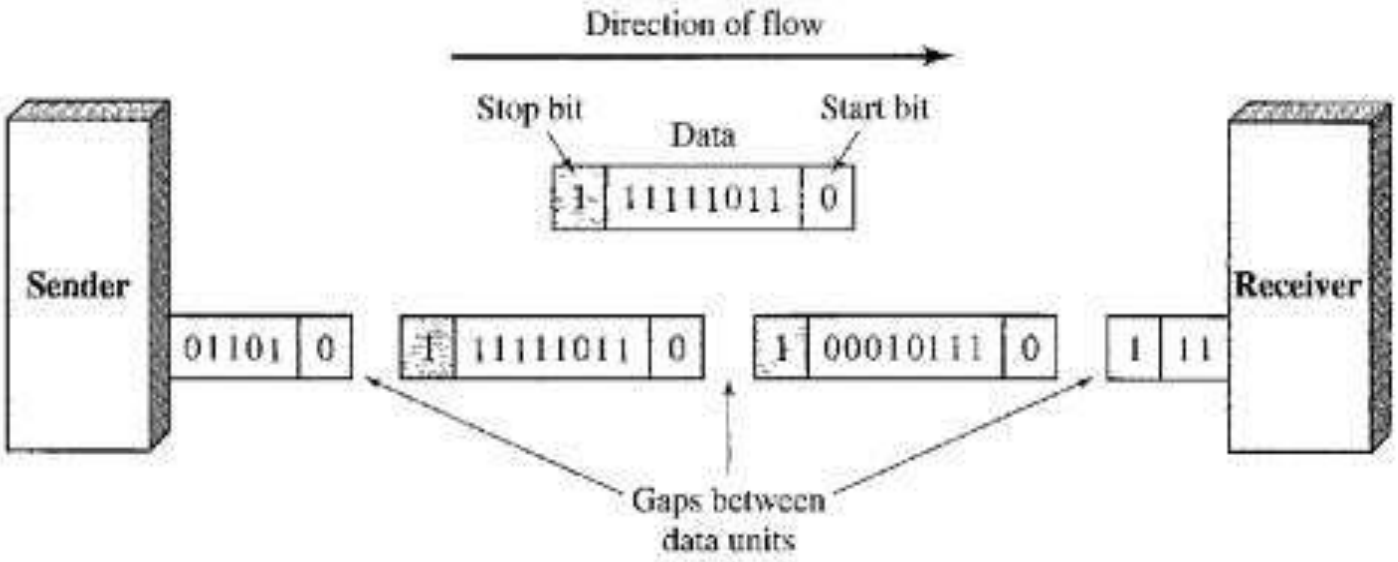
Serial Transmission



- Cost of transmission is less
- Conversion devices are required

Asynchronous Transmission

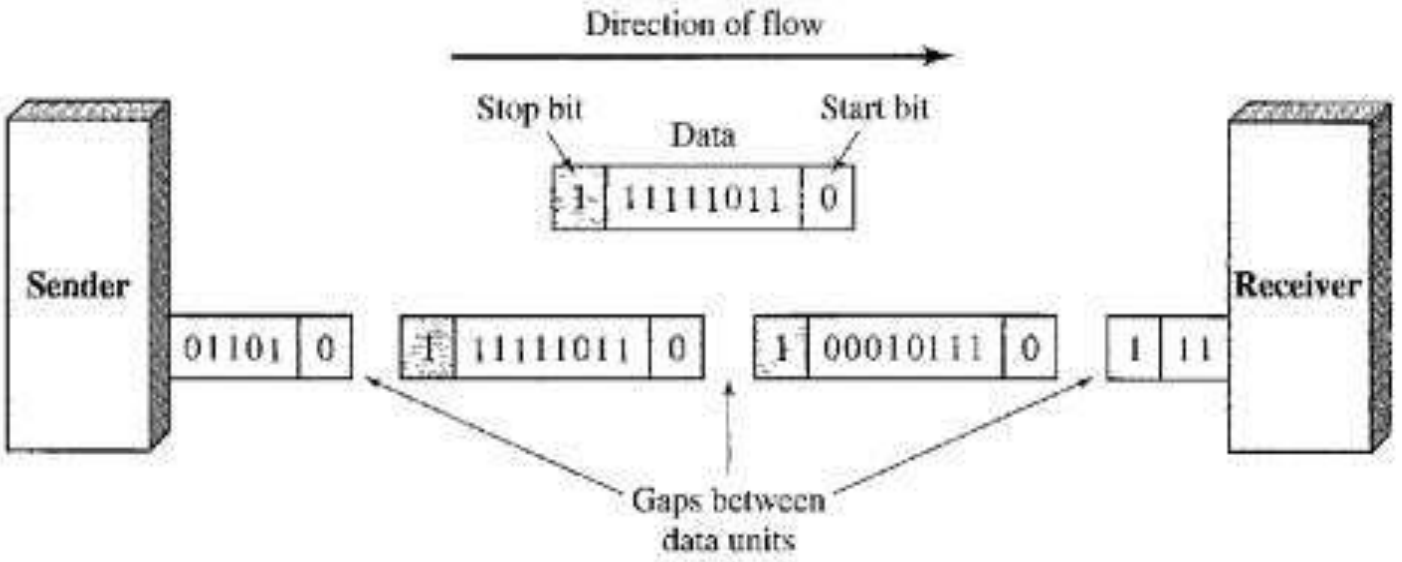
Asynchronous transmission is so named because the timing of a signal is unimportant. Instead, information is received and translated by agreed upon patterns. As long as those patterns are followed, the receiving device can retrieve the information without regard to the rhythm in which it is sent. Patterns are based on grouping the bit stream into bytes. Each group, usually 8 bits, is sent along the link as a unit. The sending system handles each group independently, relaying it to the link whenever ready, without regard to a timer.



Asynchronous Transmission

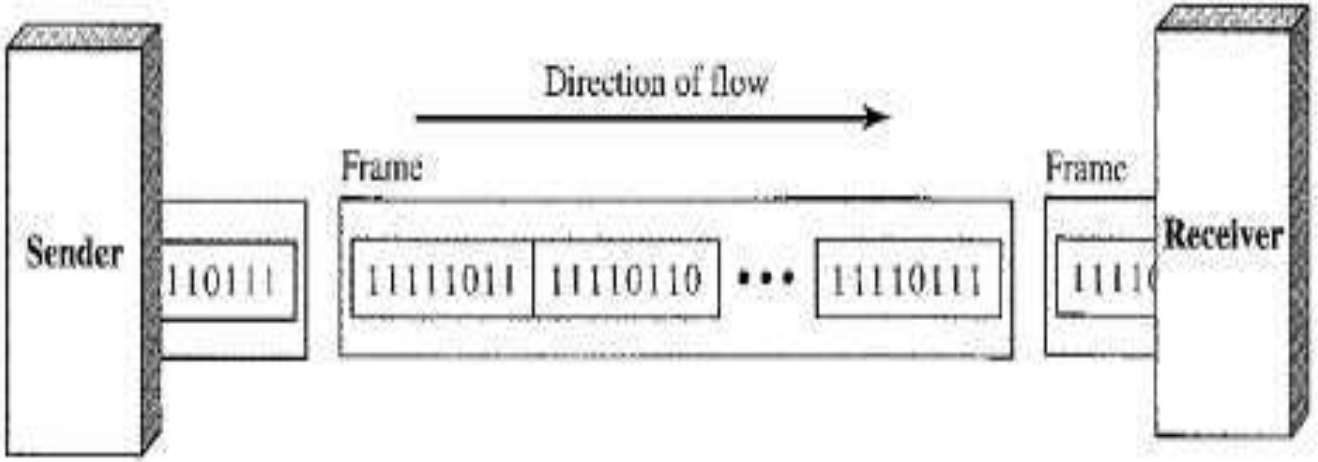
In asynchronous transmission, we send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.

Asynchronous here means "asynchronous at the byte level," but the bits are still synchronized; their durations are the same.



Synchronous Transmission

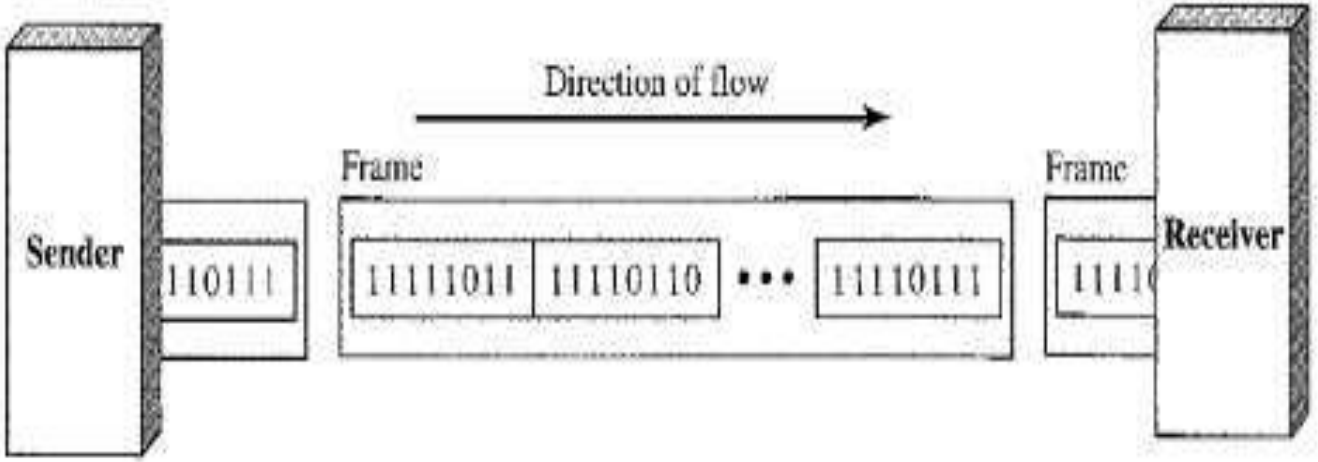
In **synchronous transmission,** the bit stream is combined into longer "frames," which may contain multiple bytes. Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is left to the receiver to separate the bit stream into bytes for decoding purposes. In other words, data are transmitted as an unbroken string of 1s and 0s, and the receiver separates that string into the bytes, or characters, it needs to reconstruct the information.



Synchronous Transmission

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits.

Speed is high since there is no addition of start or stop bits and gaps between bytes and removal of these at the receiving end



Isochronous Transmission

- In real time audio and video transmission, uneven delays between frames are not acceptable.
- Synchronization between characters is not enough, the entire stream of bits must be synchronized
- Isochronous transmission guarantees that data arrive at a fixed rate

Other modes of transmission

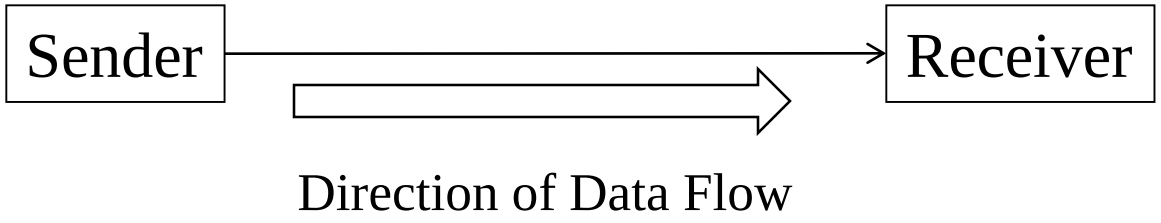
- **Unidirectional** → Simplex
- **Bidirectional** → Half Duplex
  → Full Duplex

Mode of Transmission.

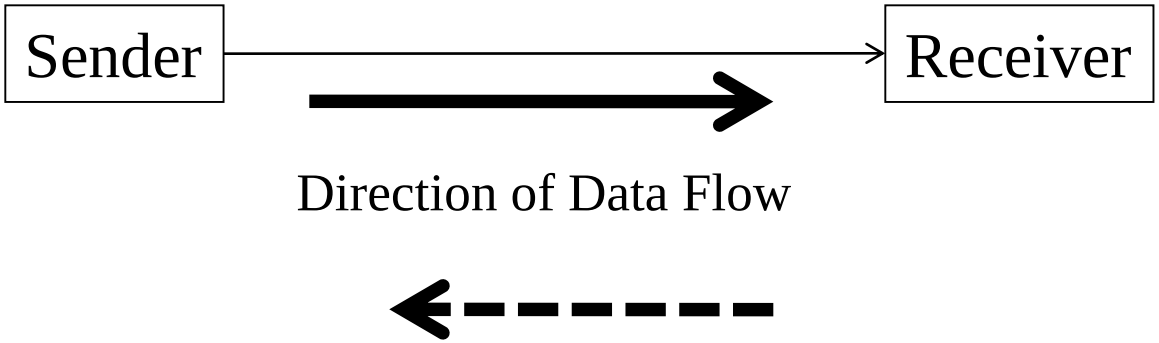
- **Unidirectional (Simplex)**
  - Information is **communicated in only one direction.**
  - It can be **implemented by single wire.**
- Examples
  - One way street
  - Communication from CPU to monitor.
  - Communication from Keyboard to CPU.
  - Communication from Computer to printer.
  - Communication from Microphone to speaker.
  - TV or radio broadcasting

Mode of Transmission

- **Simplex**



- **Half Duplex**
  - **Cannot perform two direction at a time**

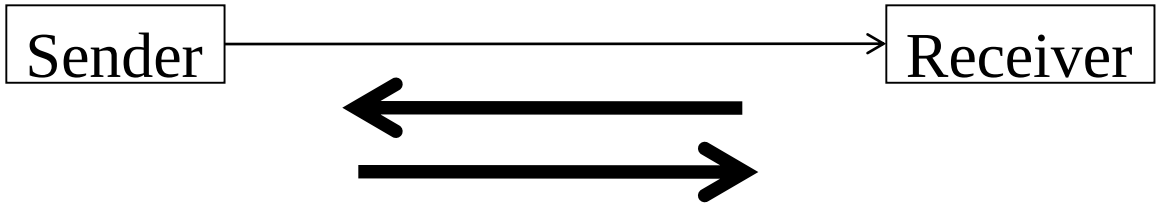


Mode of Transmission.

- **Half duplex**
  - Information is **communicated in both direction**, but **not simultaneously.**
  - It **requires** definite **turn around time** to change from transmitting mode to receiving mode.
  - Due to this delay **communication is slower** .
  - It can be **implemented by two wire**. One for Data and other is ground
- Examples
  - One line traffic in narrow bridges.
  - Walkie-talkies.
  - CB (Citizen's Band) Radio

Mode of Transmission

- **Full Duplex**
  - It **can perform in two direction at a time**



Direction of Data Flow

- **Full –Full Duplex**
- It can **perform in two direction but not between same two stations**

Direction of Data Flow

Mode of Transmission.

- **Full duplex**
  - Information is **communicated in both direction simultaneously**.
  - It can be implemented by as **two wire or four wire circuit.**
  - In two wire circuit, total channel capacity is divided in to two.
  - In four wire circuit , channel capacity can be increased.
- Examples
  - Two way traffic.
  - Telephone Conversation.

Network Components

Network Components

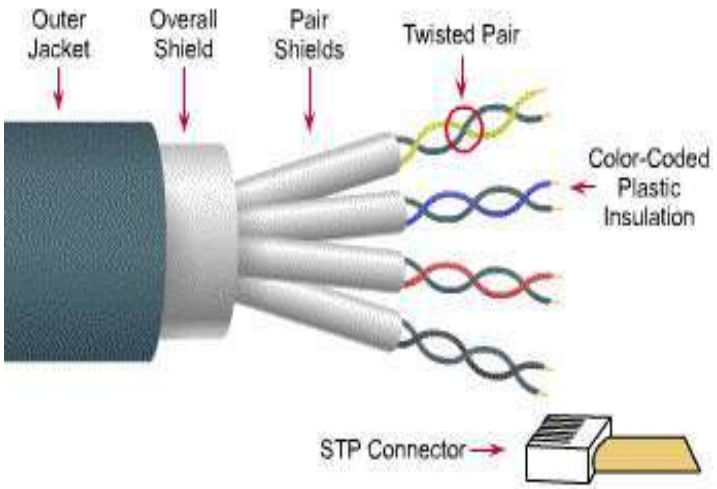
1. **Physical Media**
2. **Interconnecting Devices**
3. **Computers**
4. **Networking Software**

Network Components

- **Physical media**
  - **Cables- Telephone lines, coaxial cable, microwave, satellites, wireless, and fiber optic cables**
- **Interconnecting Devices**
  - **Routers- Devices that examine the data transmitted and send it to its destination**
  - **Switches- High speed electronic switches maintain connections between computers**
- **Protocols- Standards that specify how network components communicate with each other**

Physical Media

- Networking media can be defined simply as the means by which signals (data) are sent from one computer to another (either by cable or wireless means).

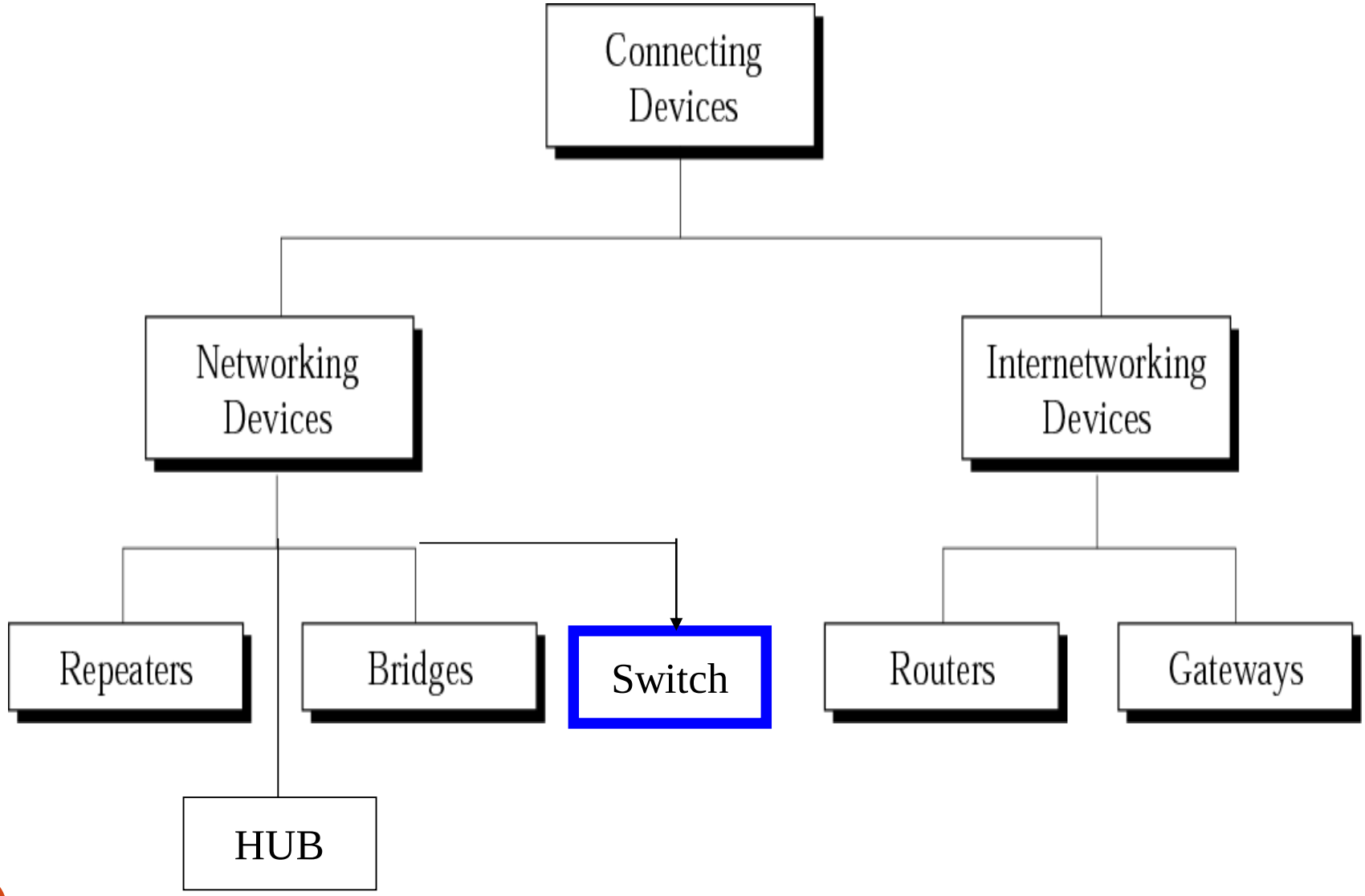


Networking Devices

- HUB, Switches, Routers, Wireless Access Points, Modems etc.

Switching

Connecting devices



Switch

- Network consists of a **set of inter connected nodes called switches**

- **From which information is transmitted from source to destination through different routers.**

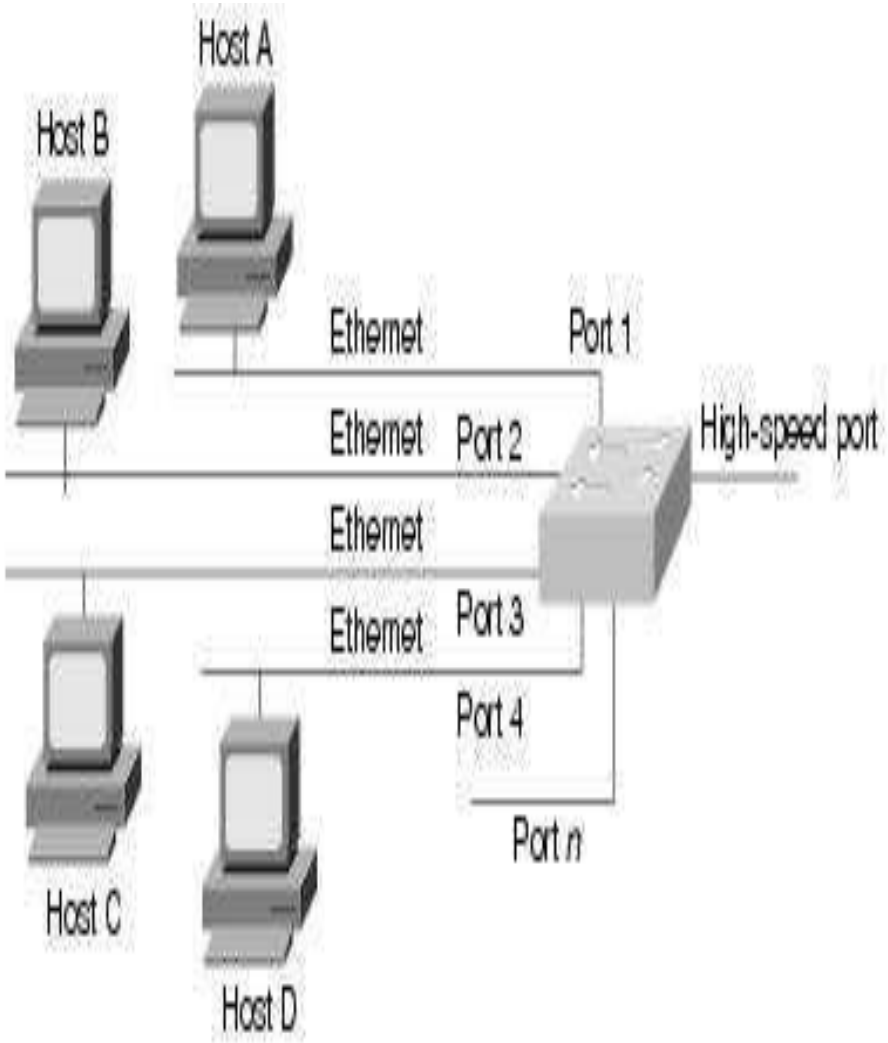
- **It operates at layer 2 of OSI model (Data Link Layer)**

Switch

- Switches can be a **valuable asset to networking**.
- Switch can **increase the capacity and speed of your network**.
- Switches **occupy the same place in the network as hubs**.
- Unlike hubs, **switches examine each packet and process it** accordingly **rather than simply repeating the signal to all ports.**

Network Switch

Network Switch



Switch

- Some **switches have additional features**, **including the ability to route packets.**

- These switches are commonly known as ***layer-3* or *multilayer switches*.**

- LAN switches come in two basic architectures,
- **Cut-through and**
- **Store-and-forward.**

Switch

- Cut-through switches **only examine the destination address before forwarding it on to its destination segment**.

- A store-and-forward switch, on the other hand, **accepts and analyzes the entire packet before forwarding it to its destination.**

Switch

Switch Benefits

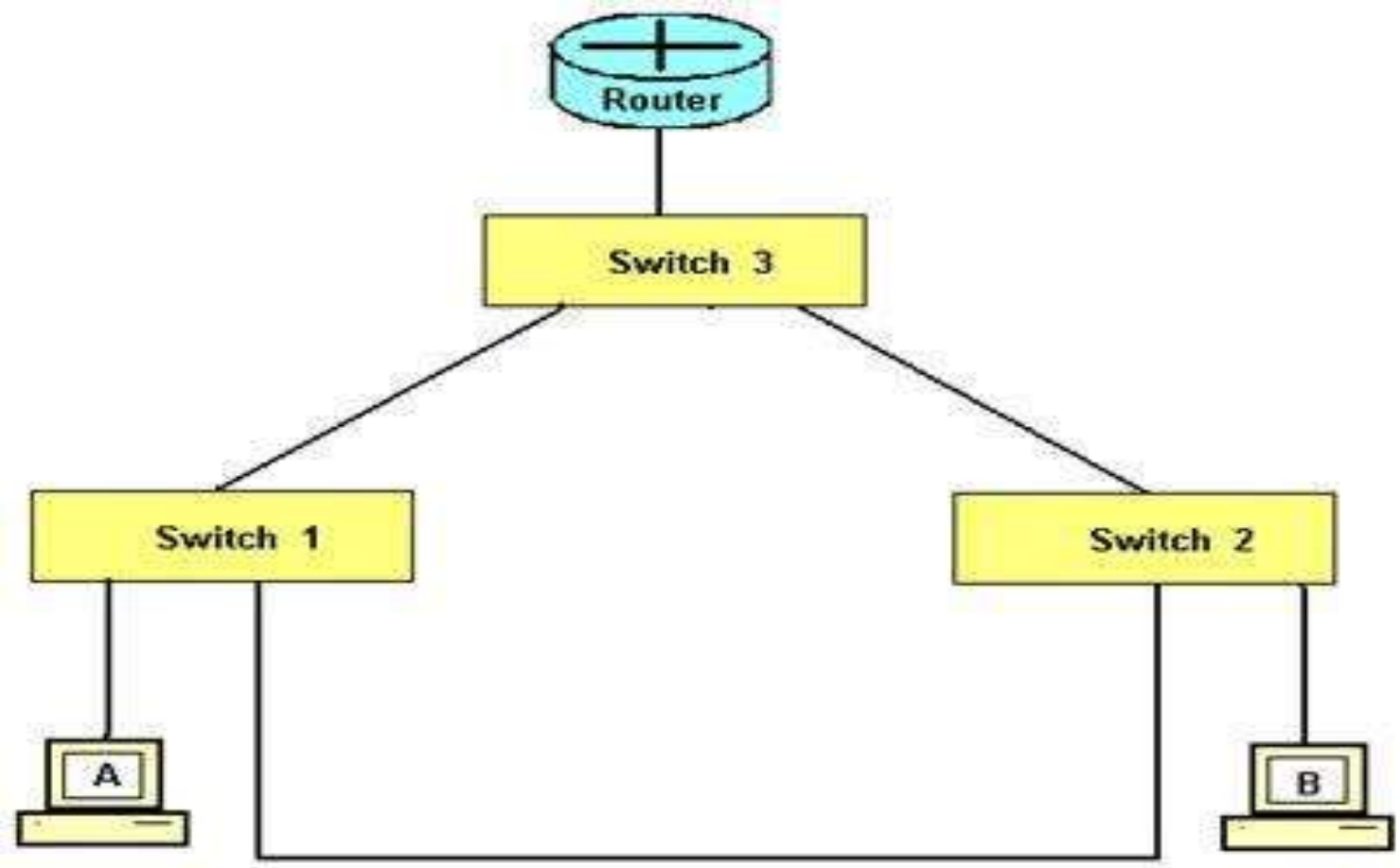
- Isolates traffic, relieving congestion
- Saparates collision domains, reducing collisions
- Segments, restarting distance and repeater rules

Switch Costs

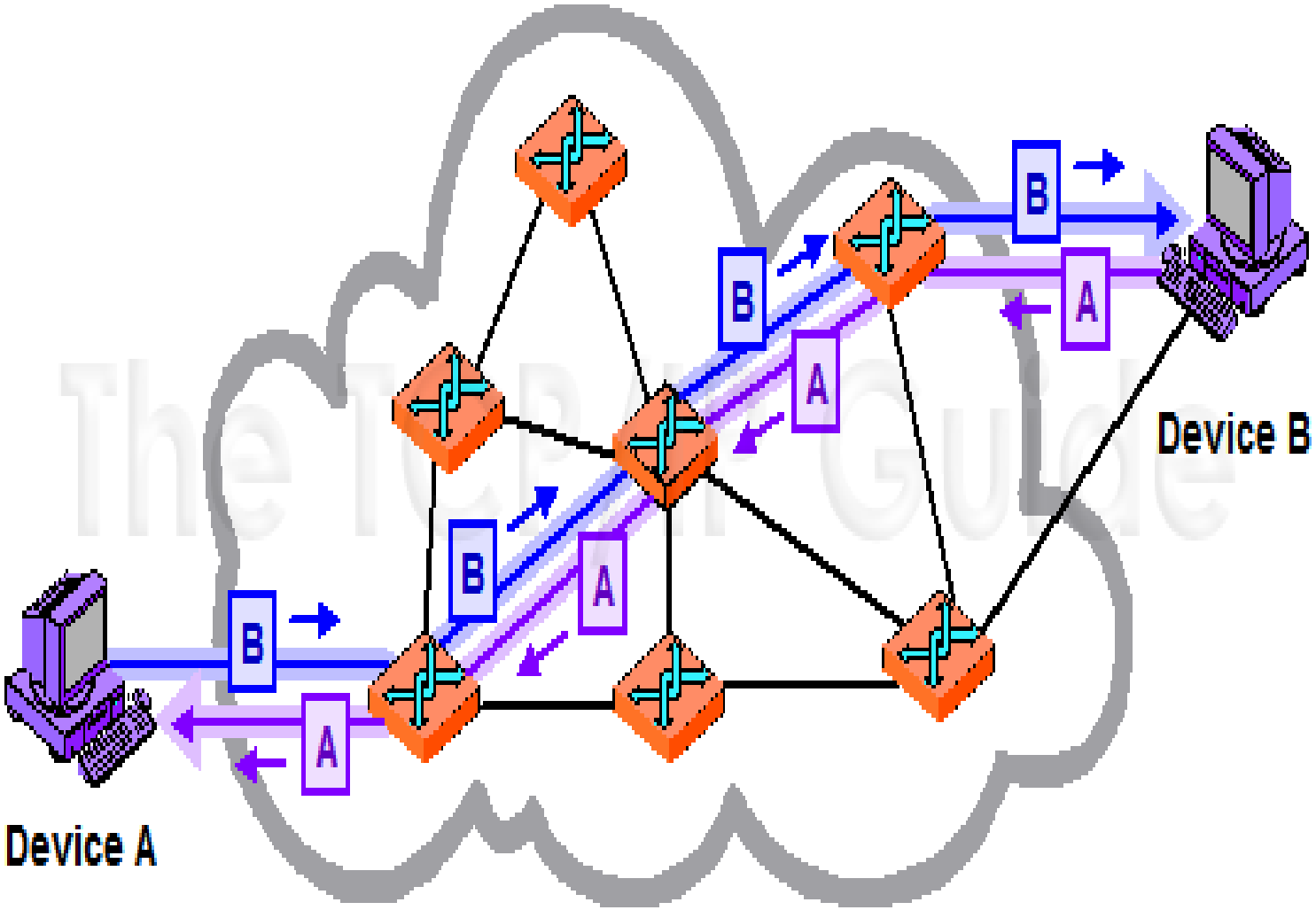
- Price: currently 3 to 5 times the price of a hub
- Packet processing time is longer than in a hub
- Monitoring the network is more complicated

Switches in a Network

Switches in Network



Switches in Network

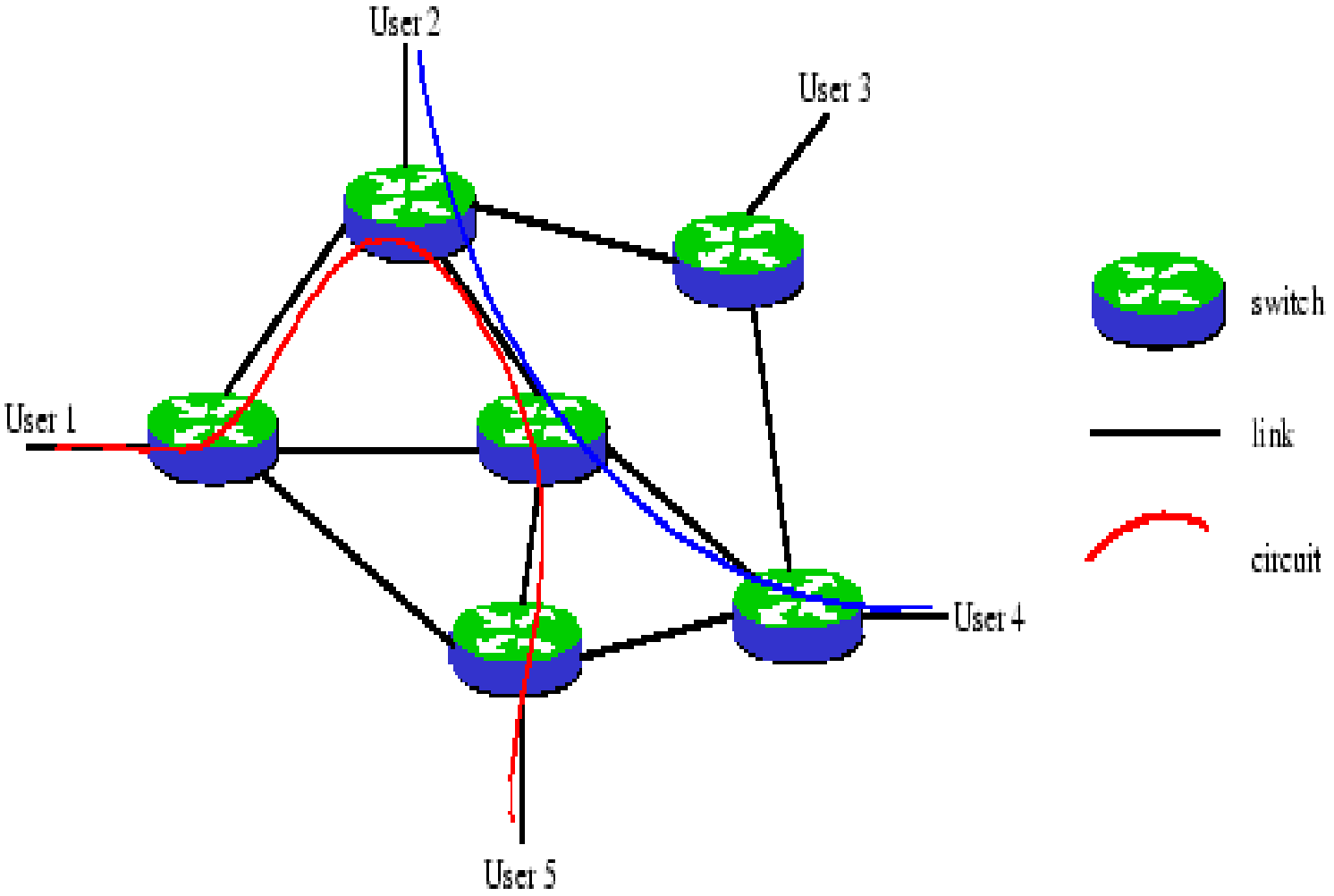


Switching

- Determines **when and how packets/messages are forwarded** through the network .

- Specifies the **granularity and timing of packet progress**

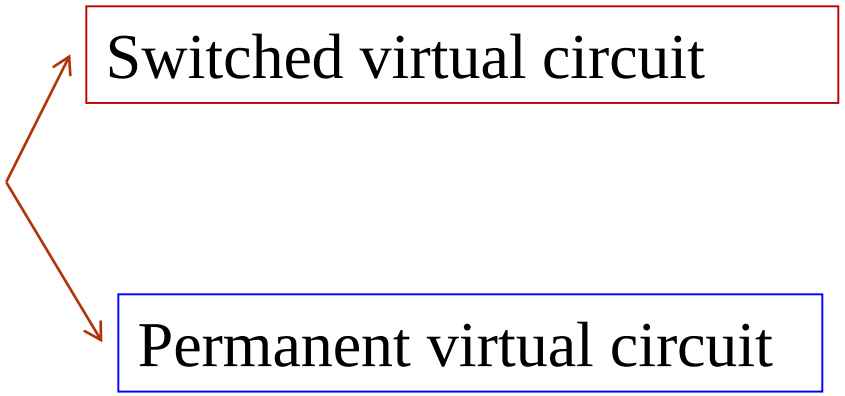
Switching



Switching

- Switching can be classified in to

1. **Circuit switched Networks**
2. **Packet switched Networks**
   - Datagram Network
   - Virtual Circuit Networks
3. **Message switched Networks**



Circuit Switching

Circuit Switching

- It is a methodology of implementing a **telecommunications network** in which two network nodes **establish a dedicated communications channel** (circuit).

- Once circuit is established , **that connection is the path for transmission.**

- **Circuit switching take place at the physical layer**

Circuit Switching

- Circuit switching is **also termed as connection oriented networks**

- It has three steps

1. Connection Establishment-Set up phase

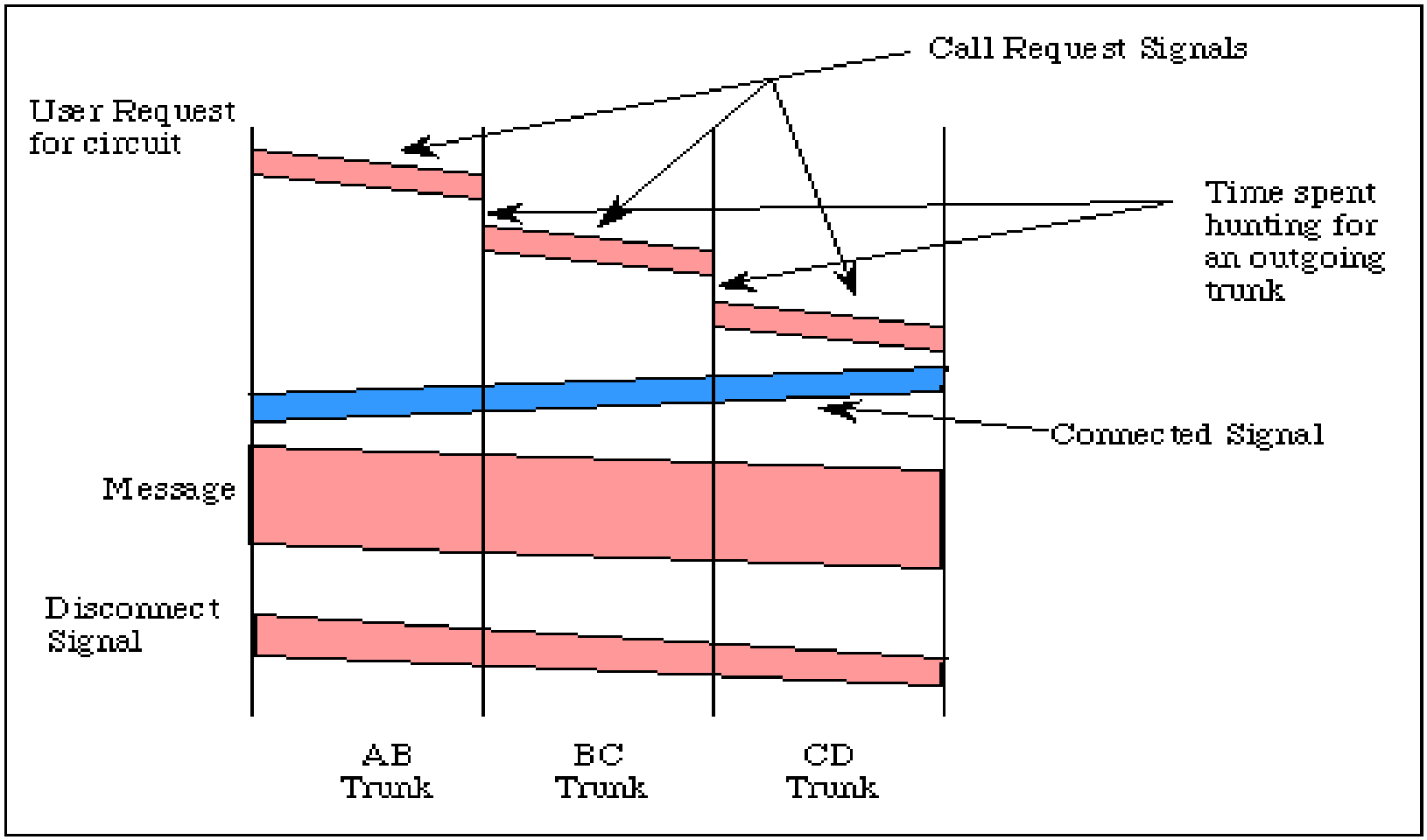
2. Data Transfer phase

3. Circuit Disconnects – Teardown phase

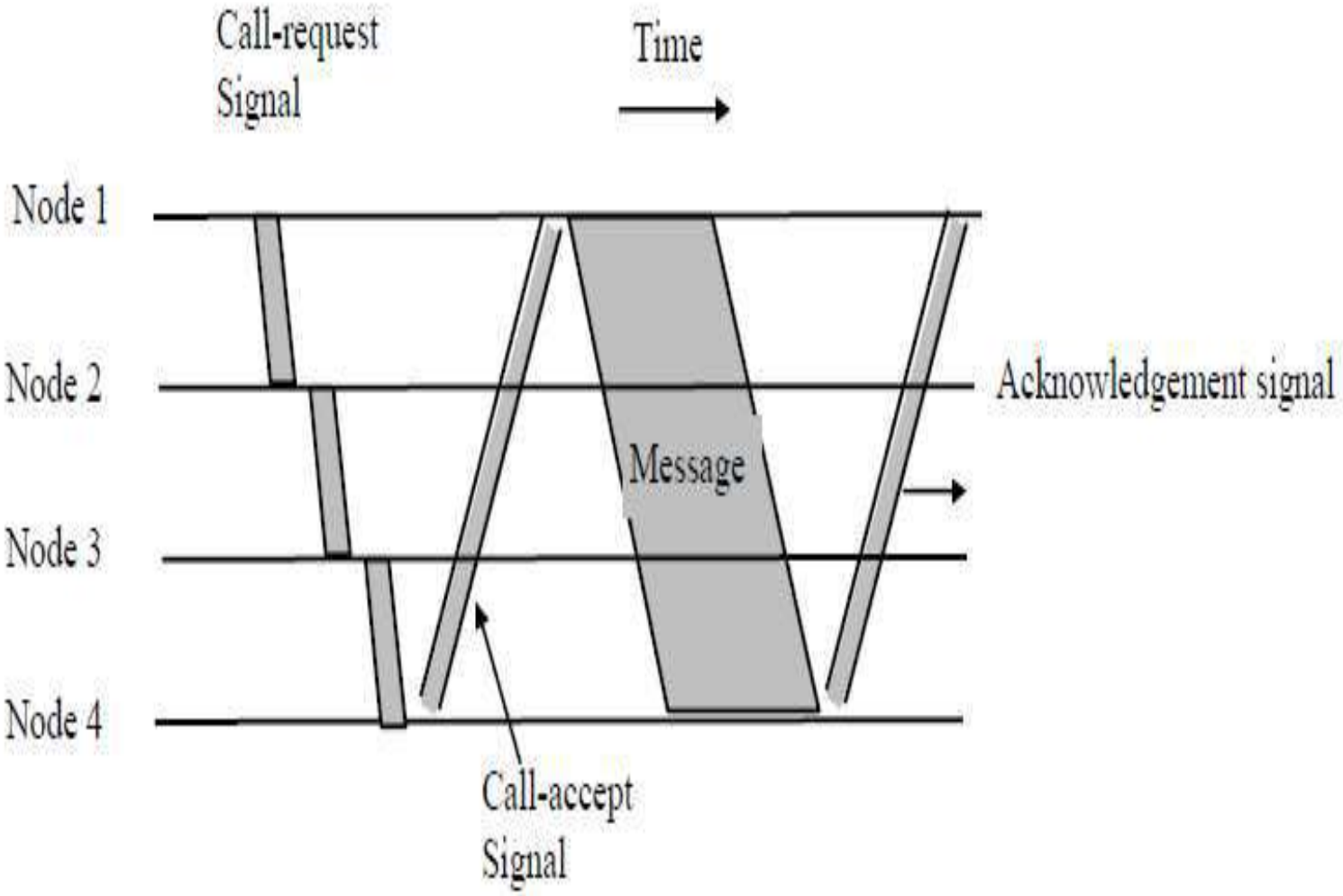
Circuit Switching

- In circuit switching, a **caller must first establish a connection to a called party before any communication** is possible.
- It **maintain the connection to transfer message**
- The circuit is ***terminated*** when the **connection is closed.**

Circuit Switching



Circuit Switching



Circuit Switching

- Set Up phase

when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time.

In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established.

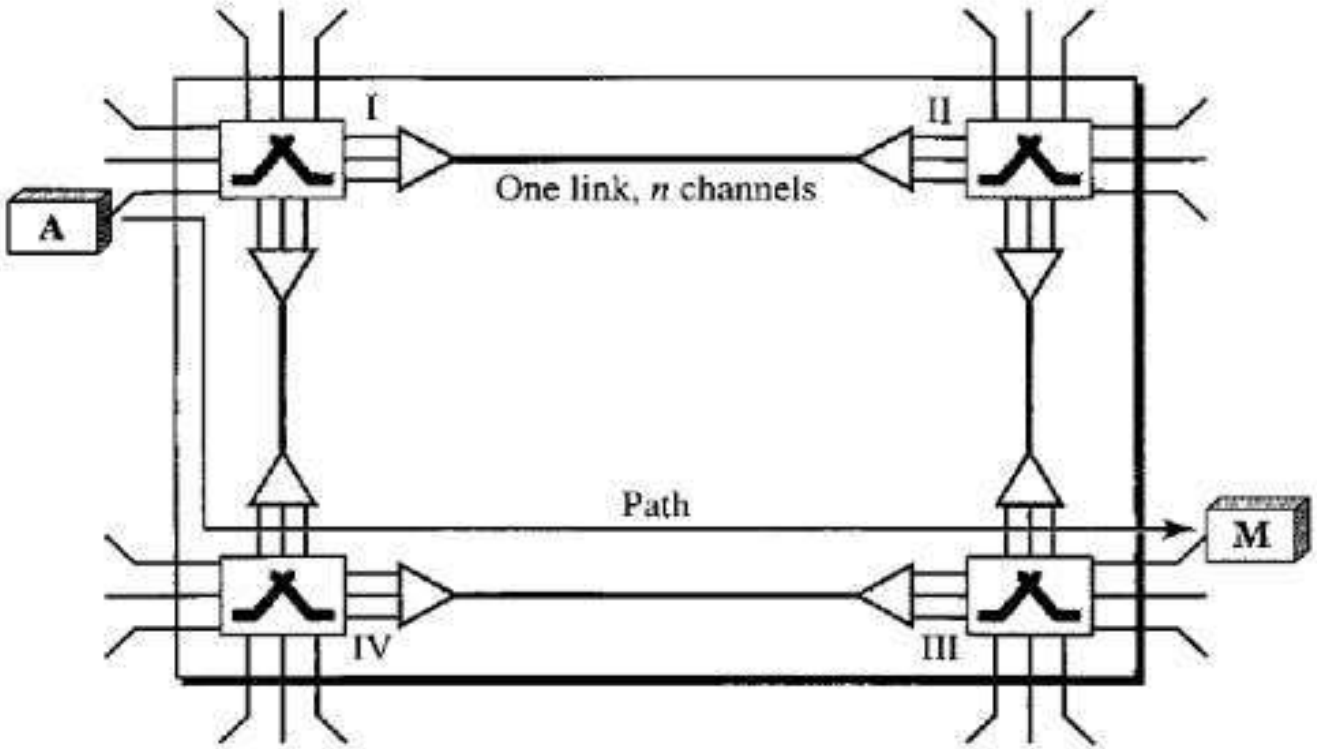
- Data Transfer phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

- Teardown phase

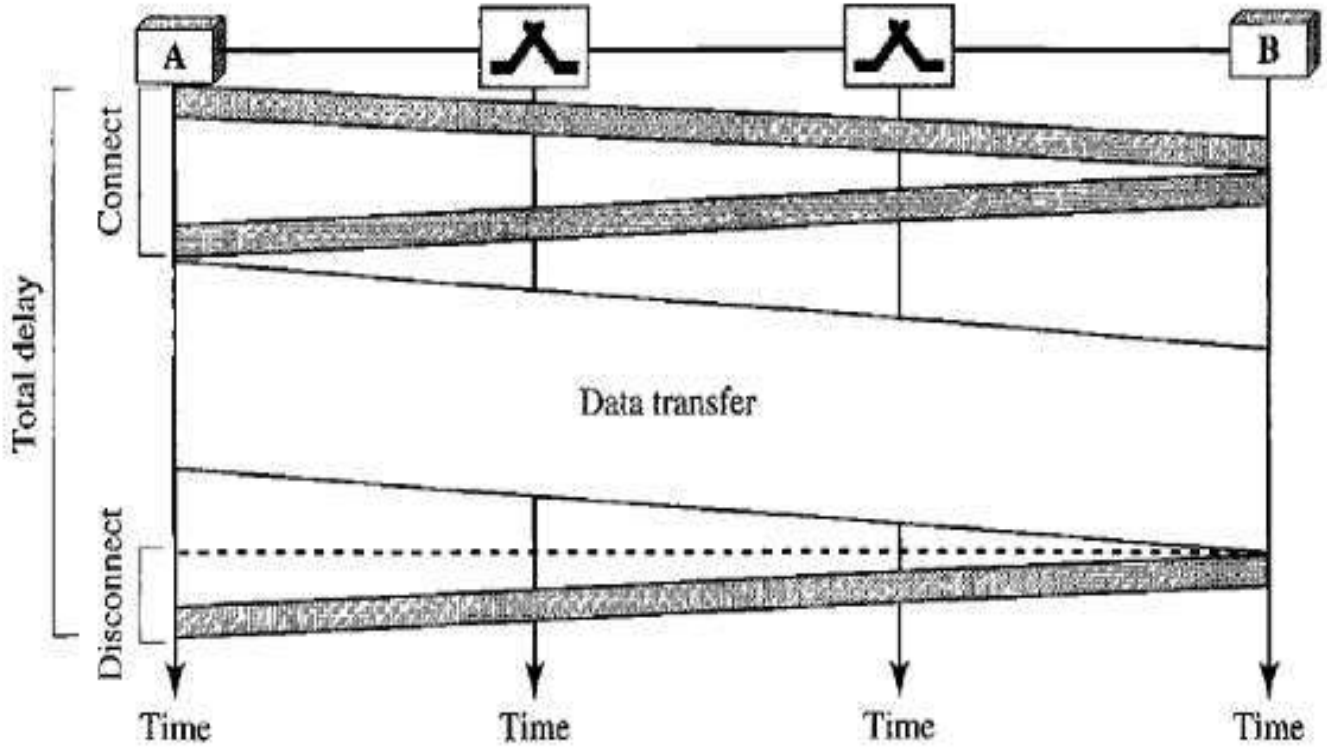
When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Circuit Switching



Circuit Switching

- **Efficiency is low**
- **Total delay = Delay for connection establishment + delay for data transfer + delay for teardown**

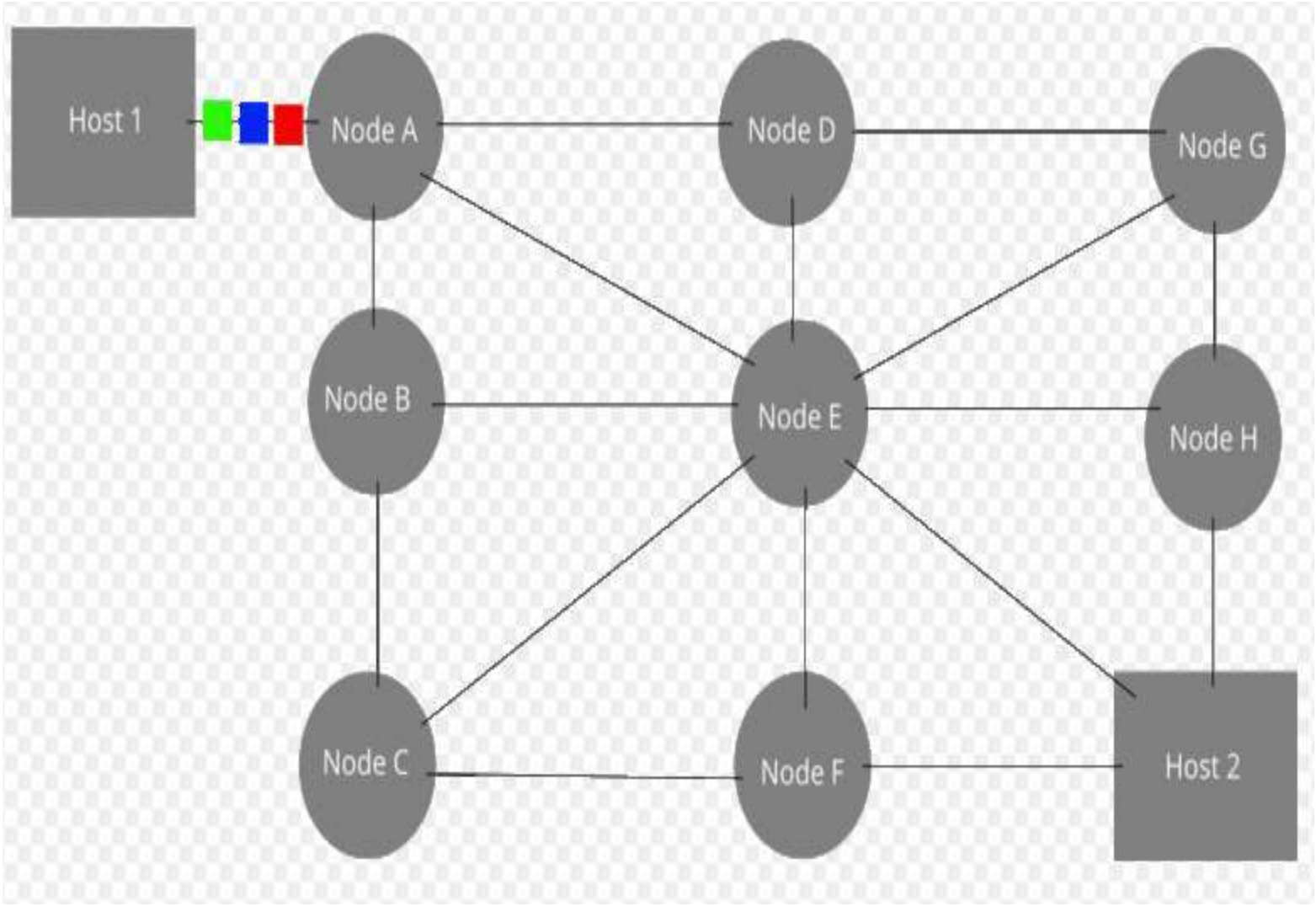


Packet Switching

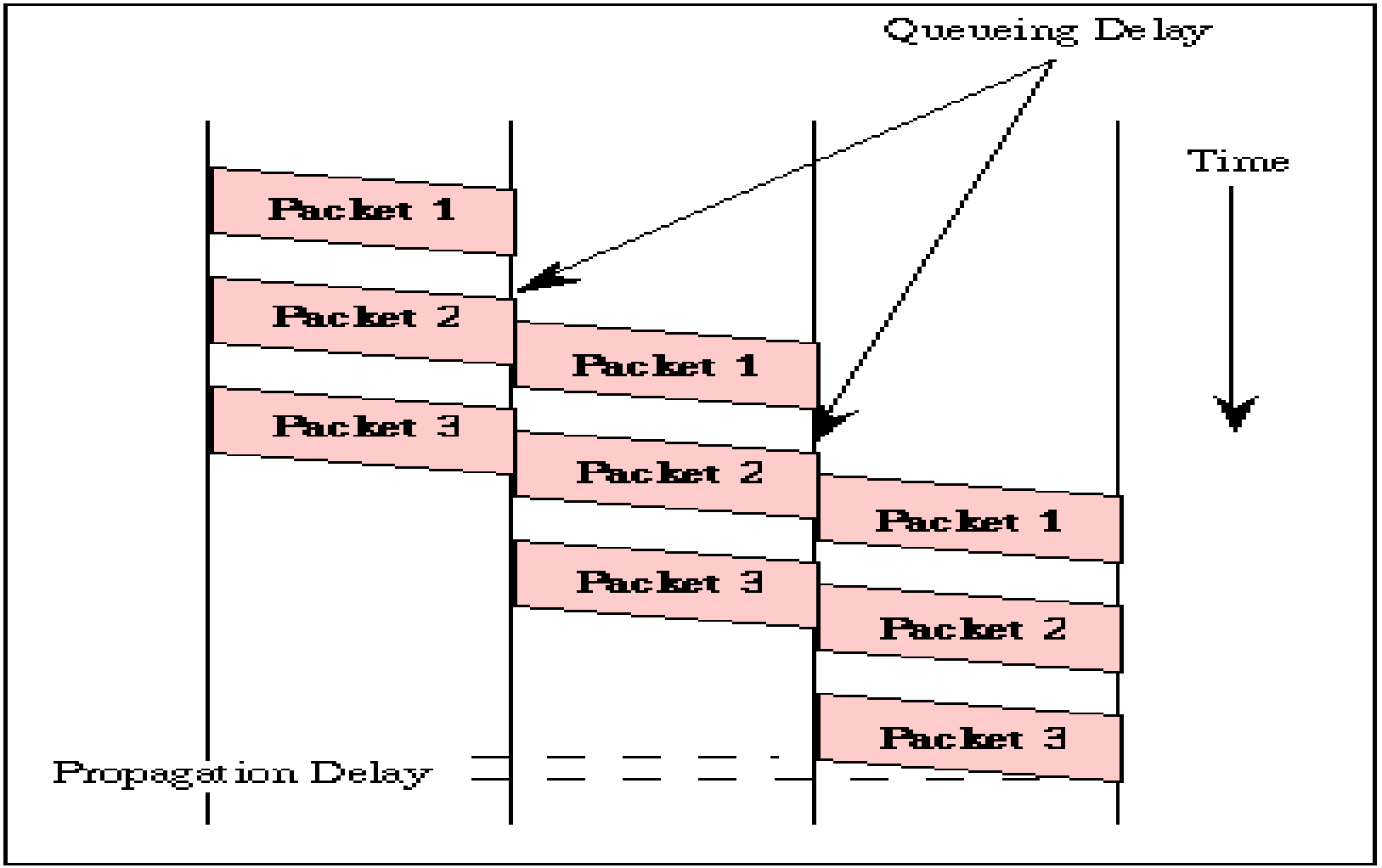
Packet Switching

- Data are send as packets
- **Packet size** can be **variable**
- Packet contains **data and header**

Switch


Host 1
Node A
Node D
Node G
Node B
Node E
Node H
Node C
Node F
Host 2

Switching


Queueing Delay
Time
Packet 1
Packet 2
Packet 3
Packet 1
Packet 2
Packet 3
Packet 1
Packet 2
Packet 3
Propagation Delay

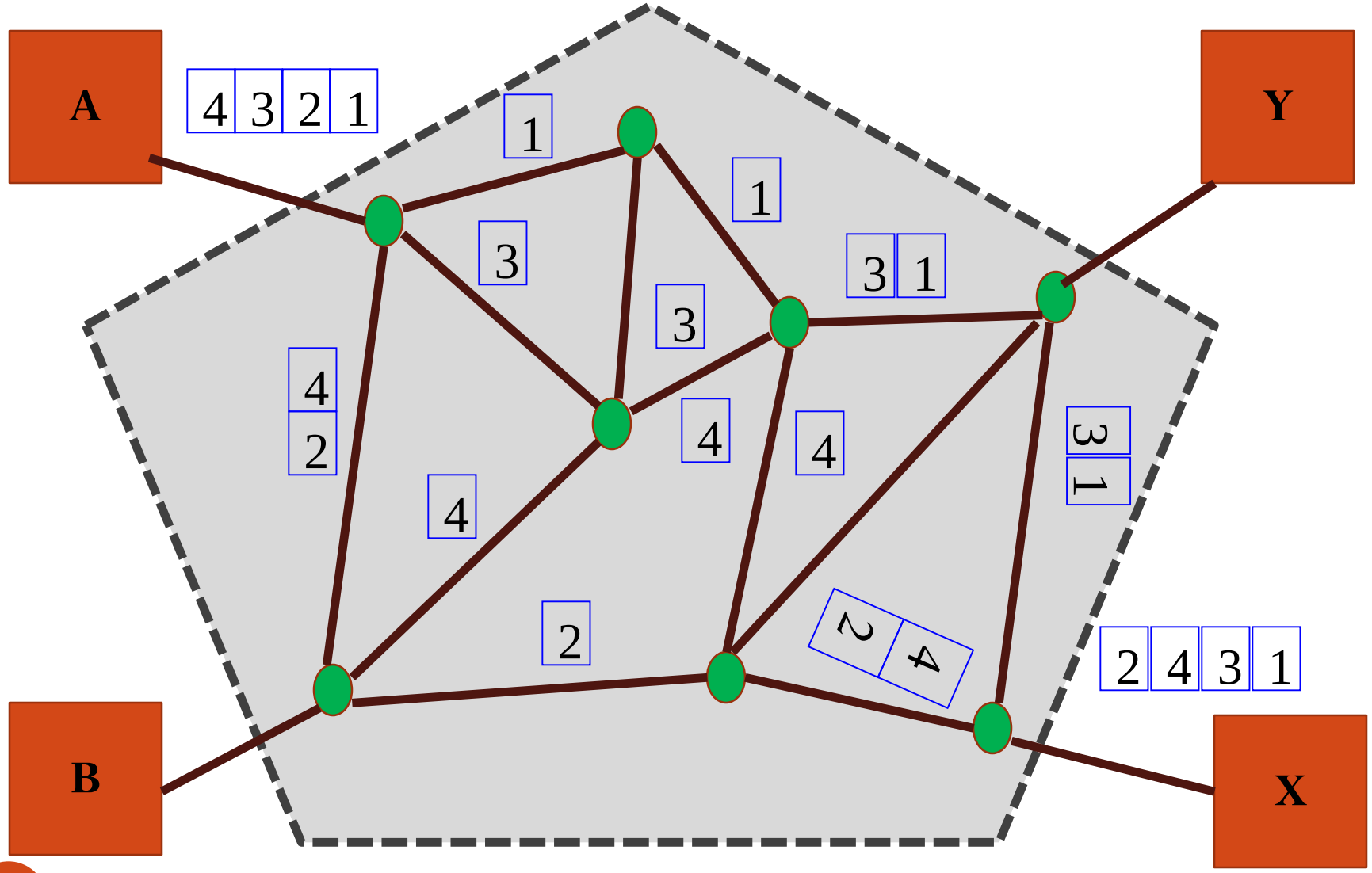
Packet Switching

- Network layer offer two services
  - **Connection oriented service**
    - A connection is called virtual circuit
  - **Connectionless service**
    - The independent packets are called Data grams

1. Data gram Network

- Routes from source to destination are not **worked out in advance.**
- Packets takes **different routes.**
- It **does not maintain a table.**
- It is the responsibility of **transport layer** to **re order the Data grams**

Data grams



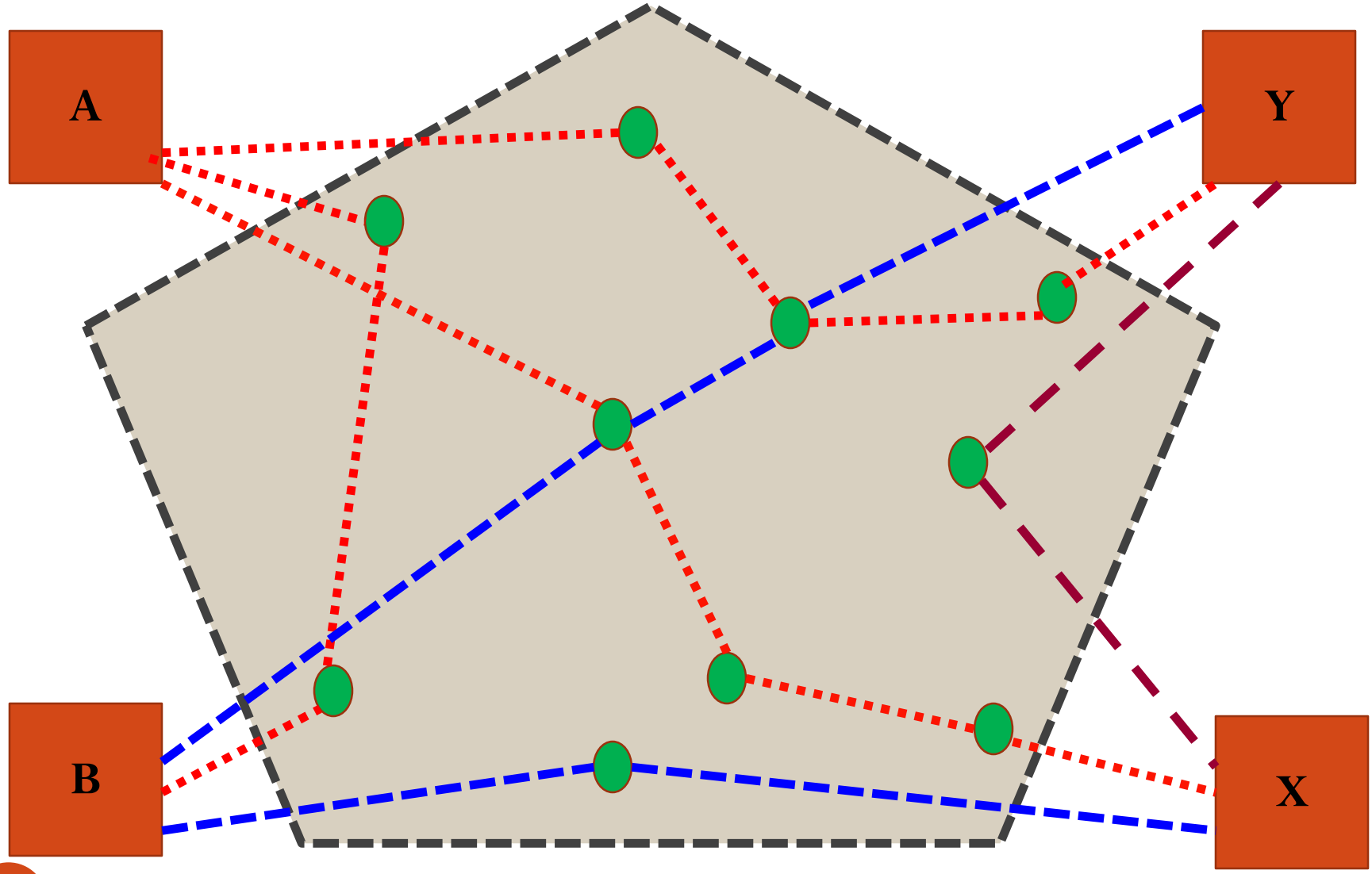
2. Virtual Circuit

- Only **one route from source to destination.**
- When **connection is established**, it is used for **all the traffic.**
- When connection is **released**, the **virtual circuit is terminated.**
- Every **router has to maintain a table.**

i. Switched Virtual Circuit (SVC)

- It is similar to **dial-up lines**
- A virtual circuit is **created whenever it is needed.**

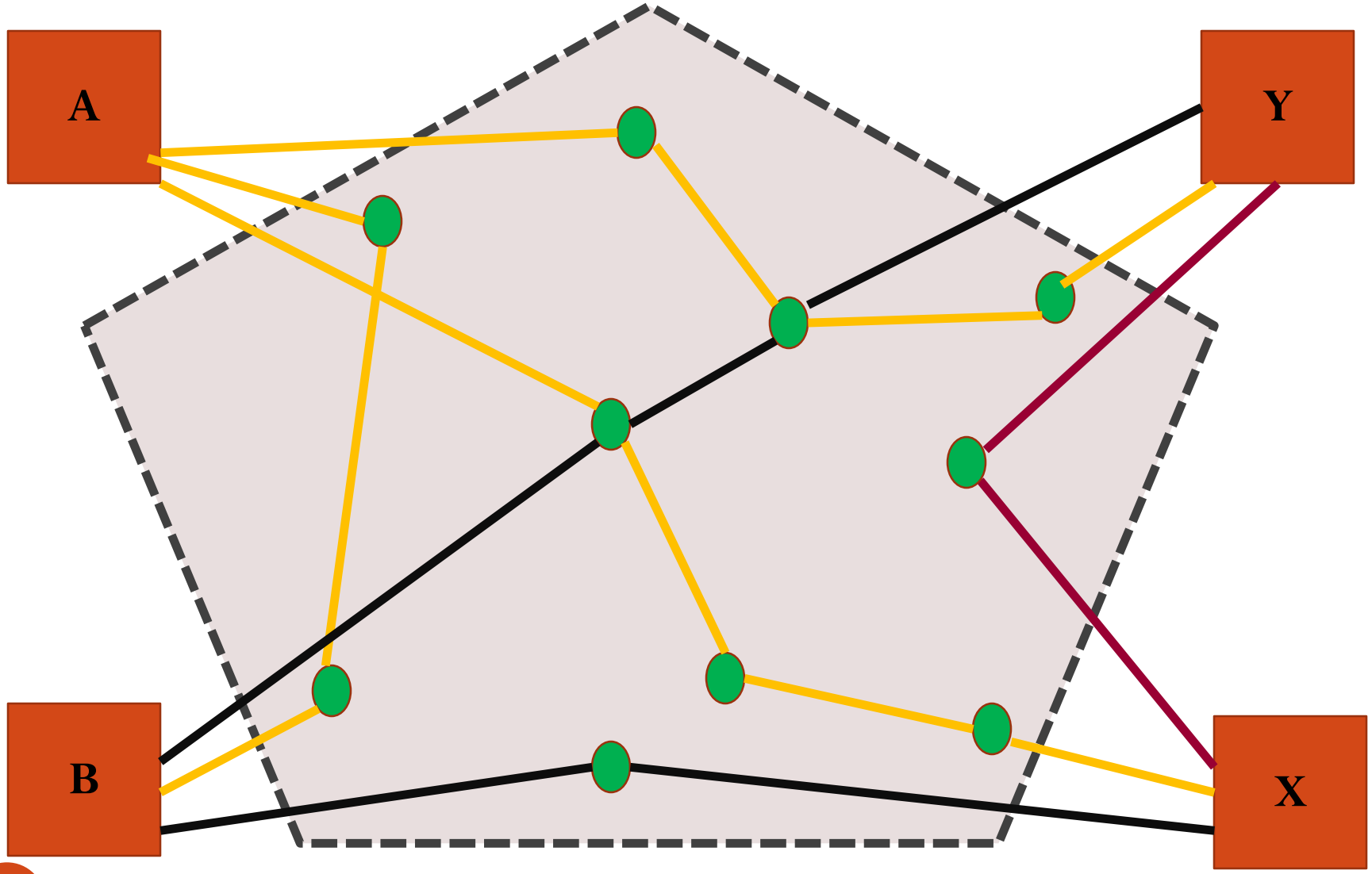
Switched Virtual Circuit (SVC)



ii. Permanent Virtual Circuit (PVC)

- Virtual circuit is provided between two user on a **continuous basis.**

Permanent Virtual Circuit



Data gram Vs Virtual circuit Network

Parameter	VC	Datagram
Circuit setup	Required	Not required
Addressing	Each packet contains a short VC number	Each packet contains a source , destination address
Repairs	Easy to repair	Harder to repair
State information	Table is required to hold state information	Table is not required to hold state information
Routing	Route is fixed. (Static routing)	Routed independently(dynamic routing)
Congestion control	Easy	Difficult

Computer Networks

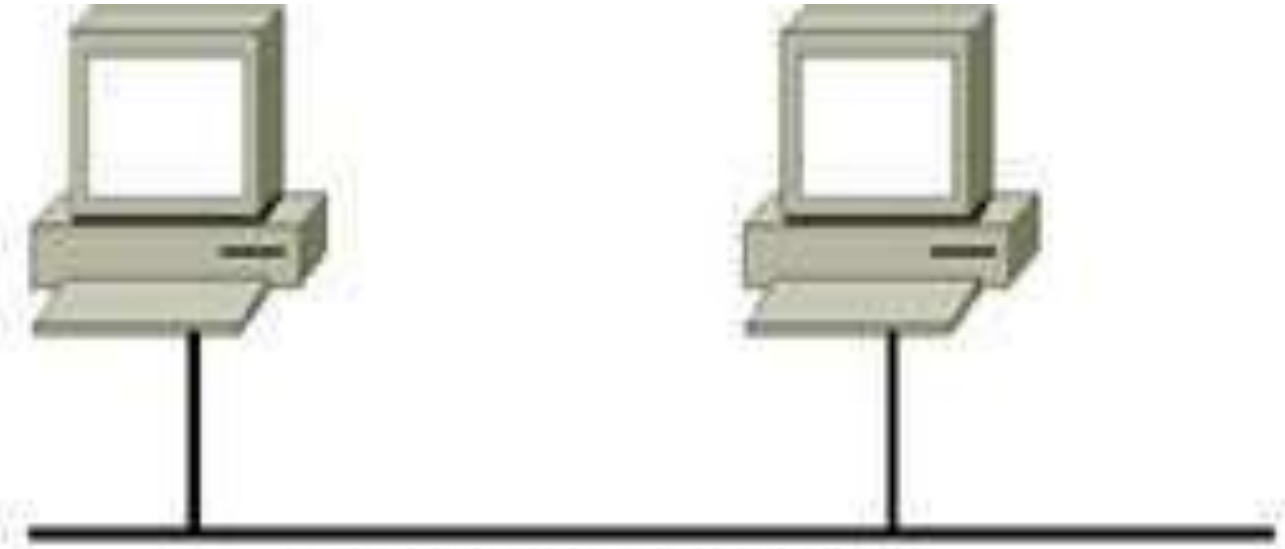
Computer network

- In its simplest form, networking is defined as **two computers being linked together**, either **physically through a cable or through a wireless device.**

- Computer network consists of two or more **computers linked together** to **exchange data and share resources**

- A computer network is a collection of **hardware components and computers interconnected** by **communication channels.** .

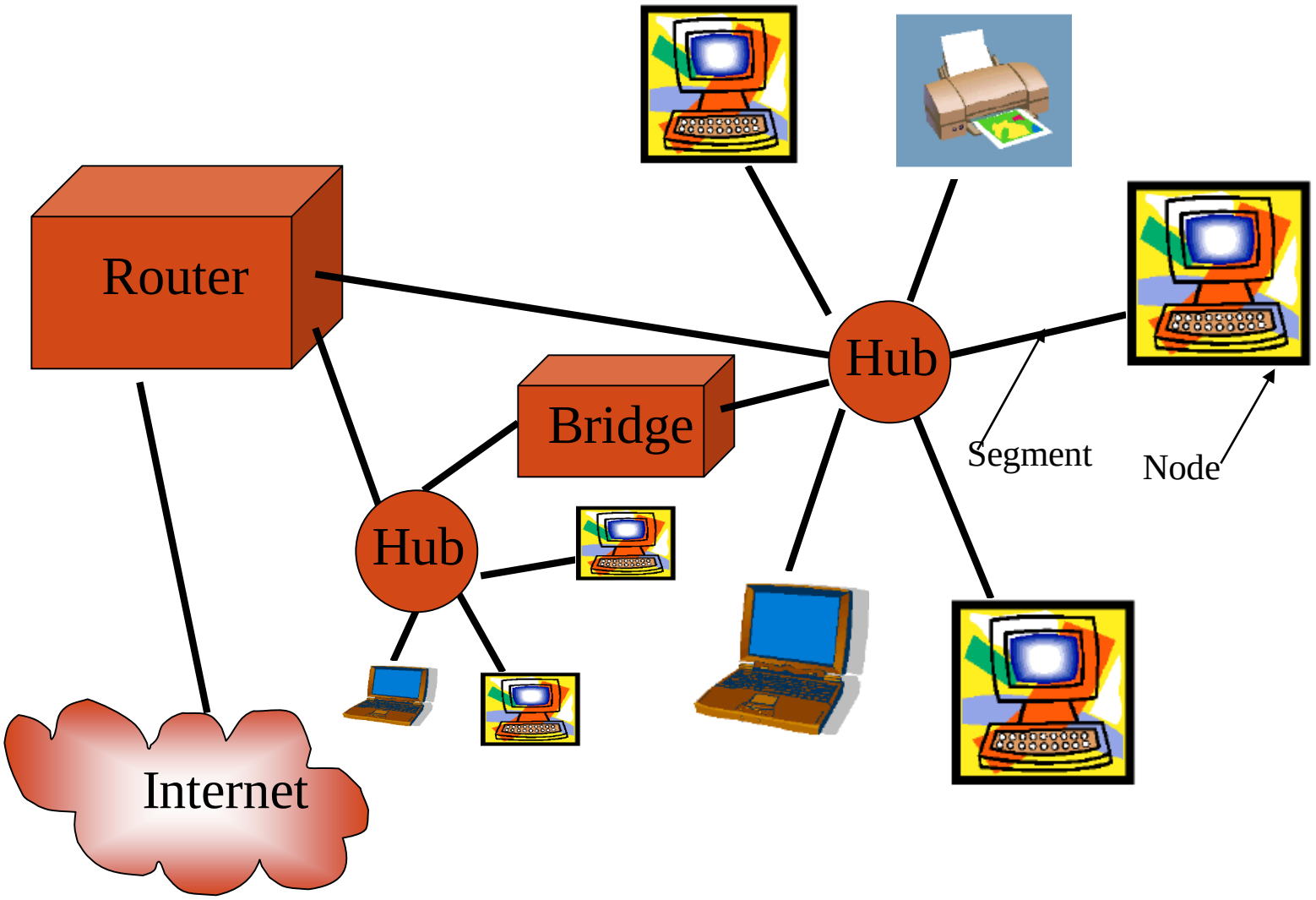
Computer network



Two host network

- A popular example of a computer network is the **Internet**, which allows millions of users to share information

An example of a network



Network Goals

Networks Fundamentals

- **Network Goals or aims**

1. Resource sharing.
2. High reliability.---Alternative Sources of data
   - **Important in banking, military, Air traffic control**
3. Data Sharing.
4. Network security
5. System performance can be improved.
6. Powerful communication medium.

Network Criteria

Networks Fundamentals

- **Network Issues/Criteria**
- To consider a **network is effective and efficient**, it must meet some criteria

I. **Performance**

II. **Reliability.**

III. **Security**

I. **Performance** can be analyzed by

- Transit time ⟶ :Time taken to Transmit
- Response Time ⟶ :Time taken to get a response

Network Issues/Criteria

- **Response Time**
- **It depends on the following factors.**

1. No of users. (Traffic Load).
2. Types of medium
3. Type of hardware included in the network.
4. Software were not updated.
5. Lack of education
6. Improper instruction

Network Issues/Criteria

II. Reliability

- It depends on the following factors.

1. Frequency of failure.
2. Recovery time after failure.

III. Security

Protecting Data from

1. Un authorized access
2. Virus

Network Issues/Criteria

Un authorized access

It has two levels

Lower level------Improper/Week password

Higher level------Encryption techniques

Network Functions

Network Functions

- **Addressing--- Identify sender and receiver**
- **Ways to transfer information on a link(Signal Format)**
- **Routing--- Find the path between sender and receiver**
- **Flow Control----Traffic flow can be controlled**
- **Congestion control**
- **Security**
- **Failure monitoring**
- **Traffic Monitoring**
- **Network Management**
- **Error detection and correction**

Network Connections

Types Of Connections

1. **POINT-TO-POINT**

Provides a direct link between two devices.

Eg. Each computer is connected directly to a printer .

2. **MULTI-POINT/MULTI DROP**

Provides a link between three or more devices on a network.

It will share the link/Channel capacity

Types Of Connections

Multi point

It is two types

- **Time sharing**
  - **Sharing the link turn by turn**
- **Spatially shared**
  - **Sharing of link simultaneously**

Two relationship is possible in multi point connection

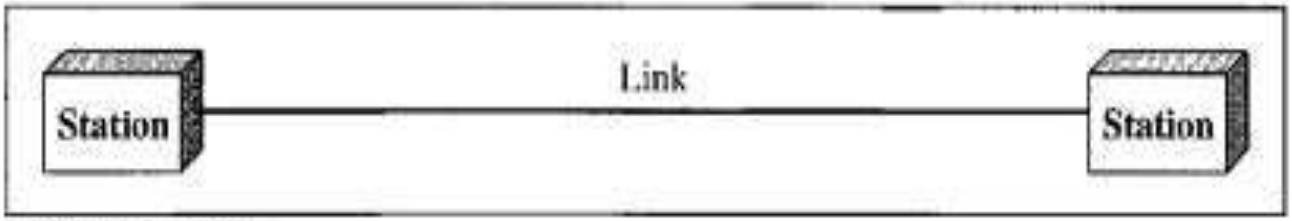
Peer- to –peer

- **All the nodes has equal right to access the link**

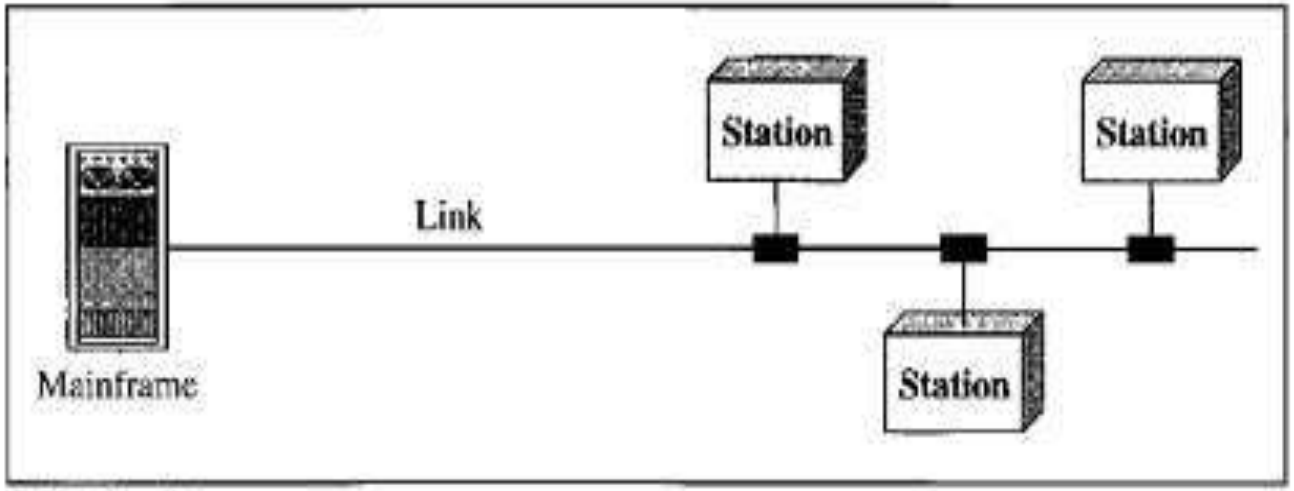
Primary-Secondary

One will be master and other will be slave

Types Of Connections



a. Point-to-point



b. Multipoint

Physical Structure-Network Topology

Topology

- A network topology is the **basic design** of a computer network.
- It details **how the network components** such **as nodes and links are interconnected.**
- Topology, in relation to networking, **describes the configuration of the network**; including the **location** of the workstations and **wiring connections.**

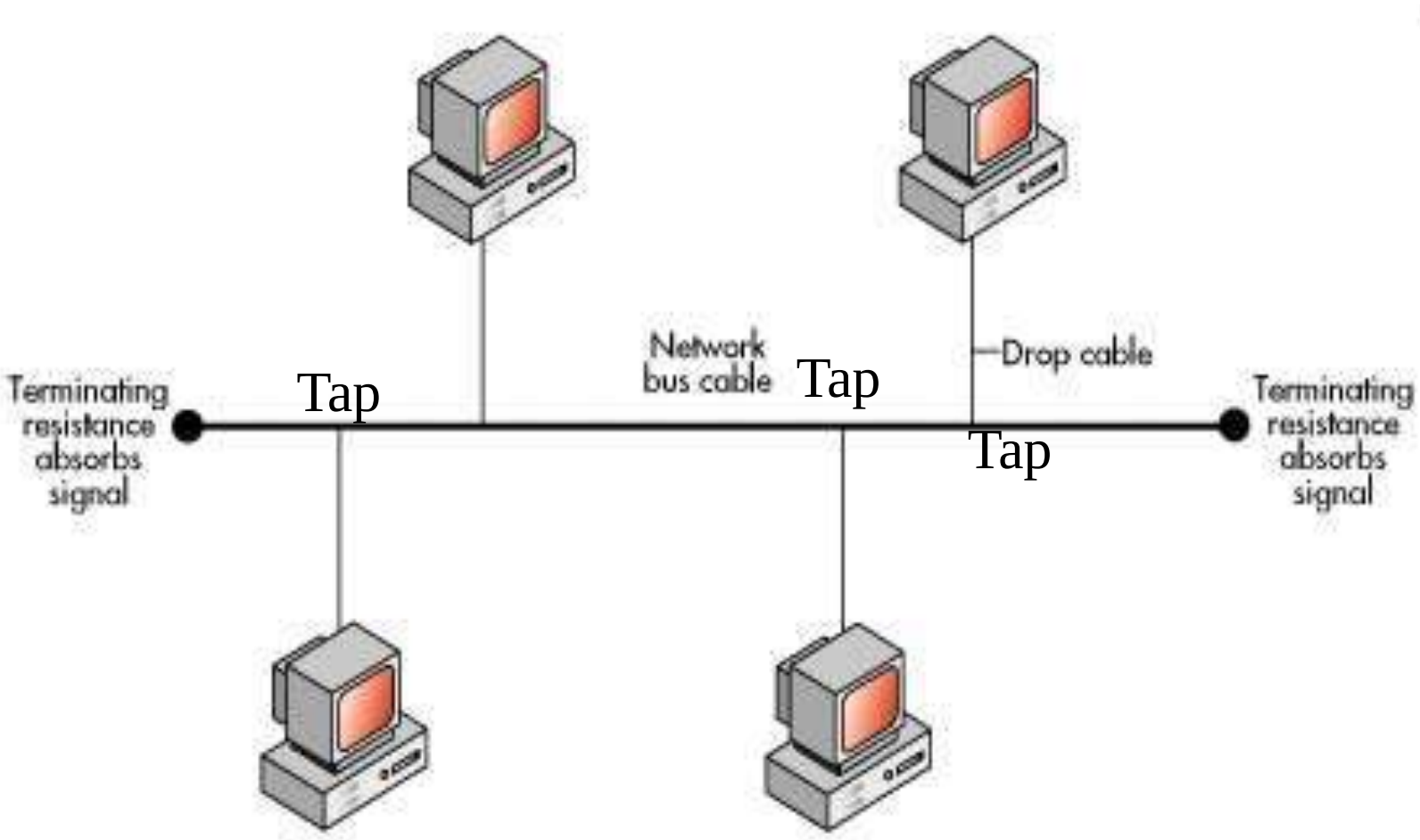
Network Topology

- *Network topology can be classified in to*

- BUS
- STAR
- MESH
- TREE
- RING
- HYBRID

Bus Topology

Bus Topology



Bus Topology

- The **simplest** and one of the most **common** of all topologies
- Bus consists of a **single cable,** called a **Backbone**, that **connects all workstations on the network using a single line.**
- Each **workstation has its own individual signal** that identifies it and allows for the requested data to be returned to the correct originator.
- In the Bus Network, **messages are sent in both directions** from a single point and are read by the node (computer or peripheral on the network) **identified by the code with the message.**

Bus Topology

- Most **Local Area Networks (LANs) are Bus Networks** because the network will **continue to function even if one computer is down.**
- **Installation is easy**
- **Less cabling is required**
- **Reconnection and fault isolation is difficult**
- **If backbone fails, it affect entire network**

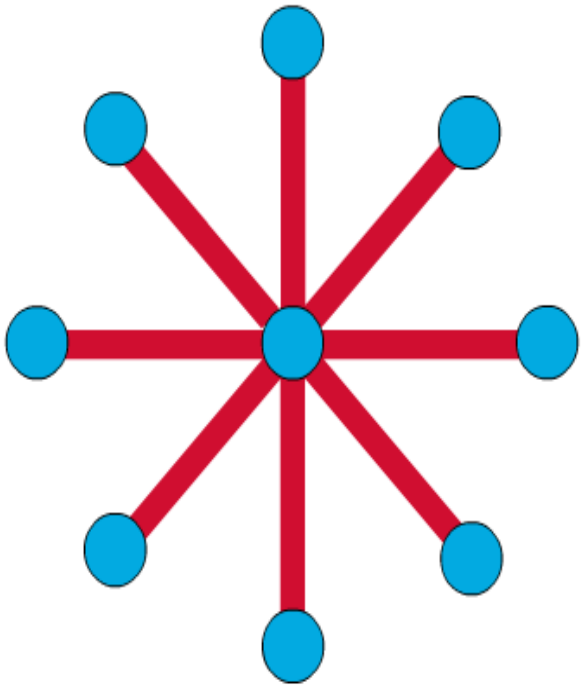
- This topology works equally well for either **peer to peer** or **client server.**

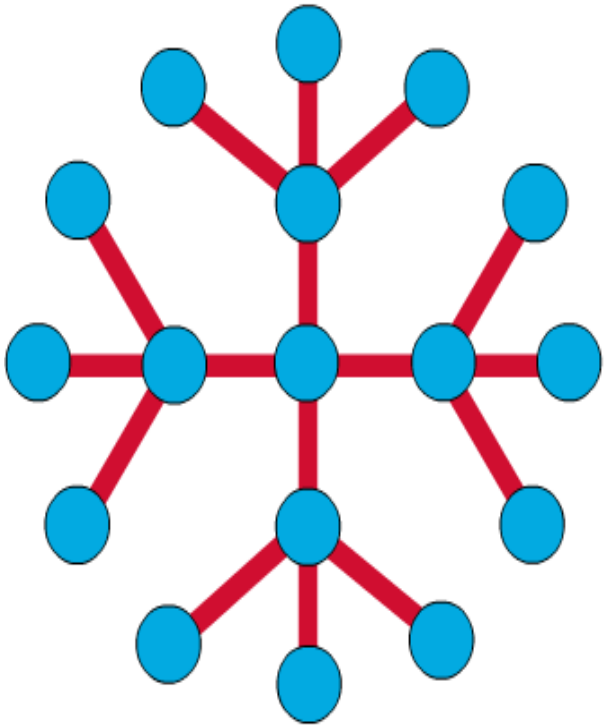
Star Topology

Star Topology

- All devices are **connected with a Star setup** communicate through a **central Hub by cable segments. Not directly connected as in mesh**
- **Each device needs only one link and one I/O port to connect it to any number of others**
- Signals are **transmitted and received** through the **Hub**.
- It is the **simplest** and the **oldest** and all the **telephone switches are based on this.**
- In a star topology, **each device has separate connection to the network.**

Star Topology





Star Topology

- Robust- If one link fails, it does not affect others
- Less expensive than mesh
- If central hub fails, it affect all hosts.
- Higher amount of cabling is required
- High speed LAN uses star topology with central hub

Mesh Topology

Mesh Topology

- The mesh topology **connects all devices (nodes) to each other** for redundancy and fault tolerance
- For 'n' nodes, there are n(n-1) links to connect each node to other nodes. There are n(n-1)/2 duplex links

- **It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.**
- **Implementing the mesh topology is expensive and difficult**

Mesh Topology

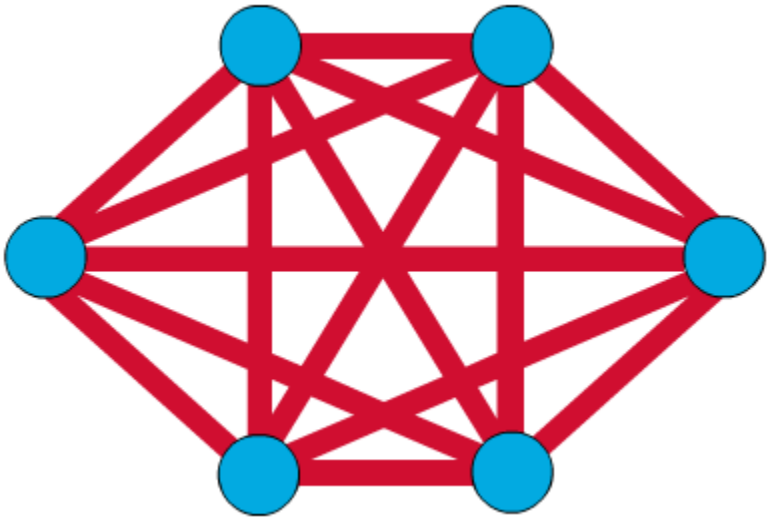
Advantages

- Traffic is less since each link carries data from two nodes
- Security or privacy is high since only the intended recipient sees the data.
- Fault identification is very easy
- Robust- If one link fails, all others are unaffected.

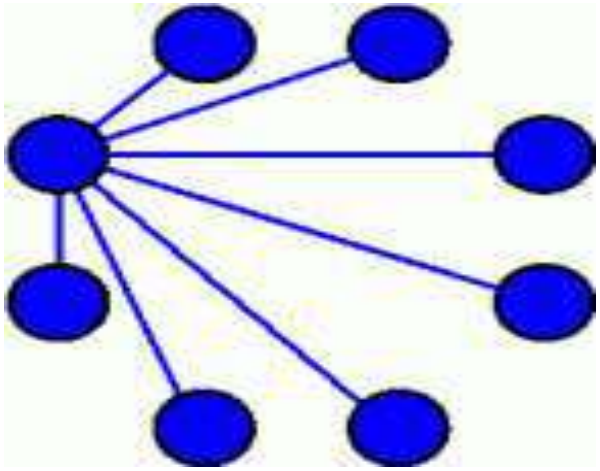
Disadvantages

- Cabling and number of I/O ports required is very high
- Wiring spans large area
- Since every device is connected to every other device, installation and reconnection are difficult
- Hardware required to connect each link(I/O ports and cable) can be expensive.

Mesh Topology



Full Mesh



Partial Mesh

Ring Topology

Ring Topology

- All the nodes in a Ring Network are **connected in a closed circle of cable.**
- **Each device is directly connected to two devices in either side**

- Messages that are transmitted **travel around the ring** until they **reach the computer that they are addressed to**, the **signal being refreshed by each node.**

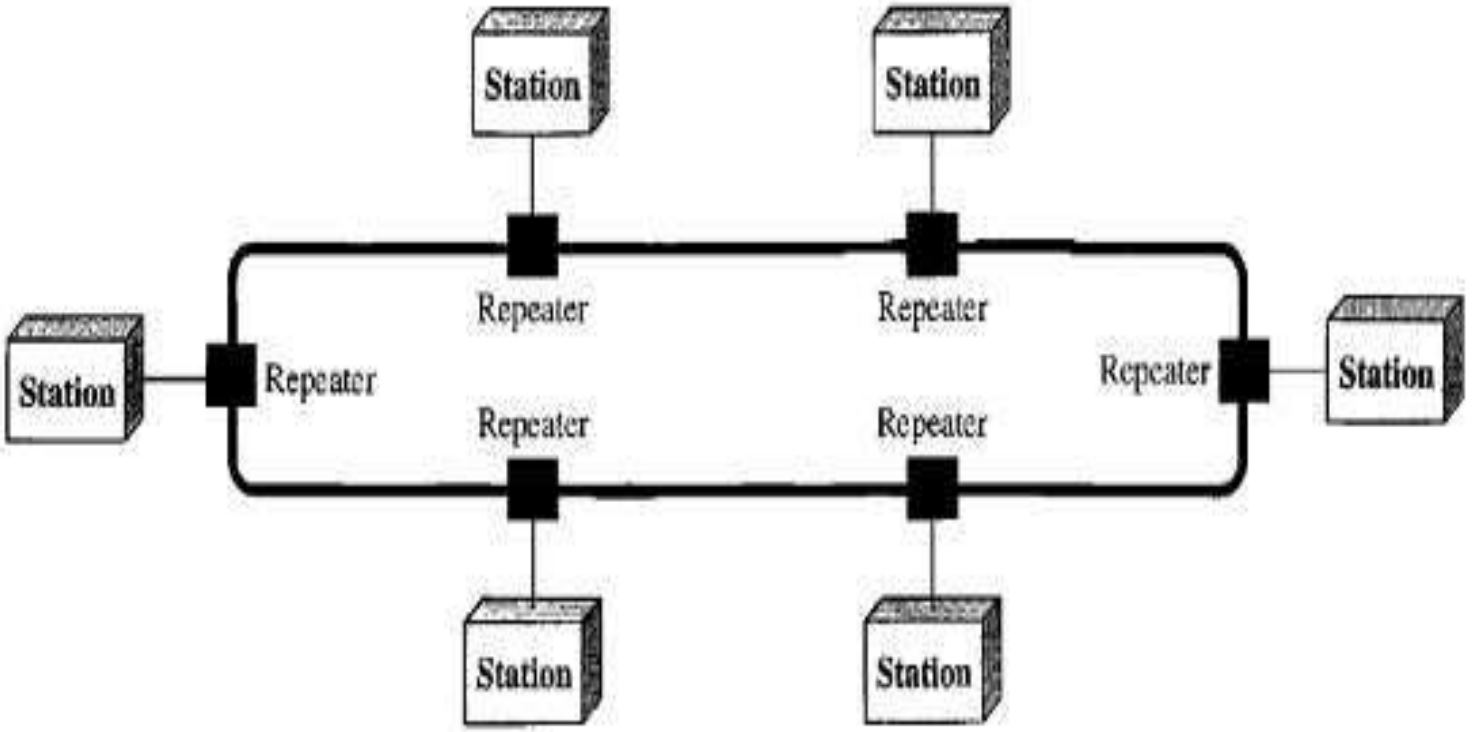
- In a ring topology, the network signal is **passed through each network card of each device** and **passed on to the next device.**

Ring Topology

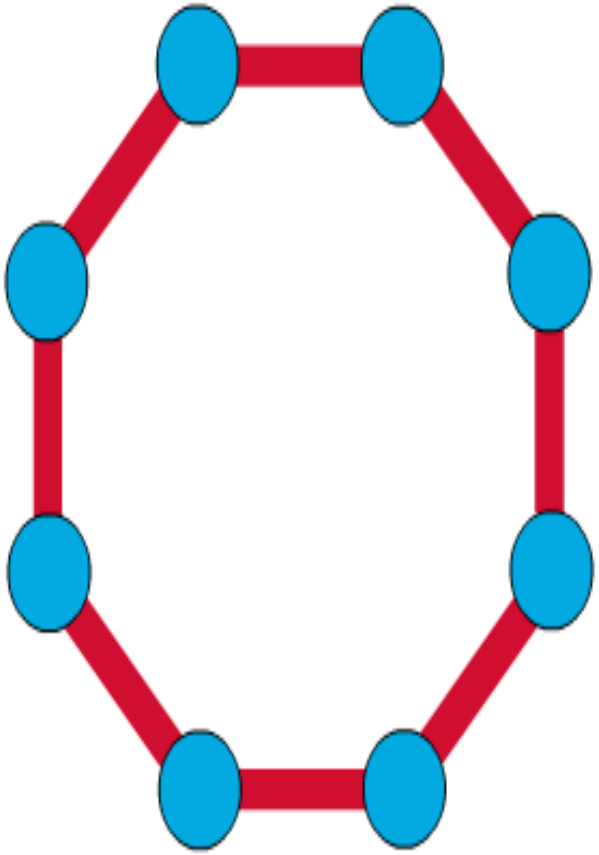
- Each device **processes and retransmits** the signal, so it is capable of supporting many devices in a somewhat slow but very orderly fashion.
- Important feature is that **everybody gets a chance to send** a packet and it is **guaranteed** that every node gets to **send a packet in a finite amount of time.**
- **To add or delete a device, requires changing only two connections**
- **Fault isolation is simplified. If one device does not receive a signal with in a specified period, it can issue an alarm. The alarm alerts the network operator , the problem and location**
- **Unidirectional traffic can be disadvantage**
- **A break in the ring disable the entire network**

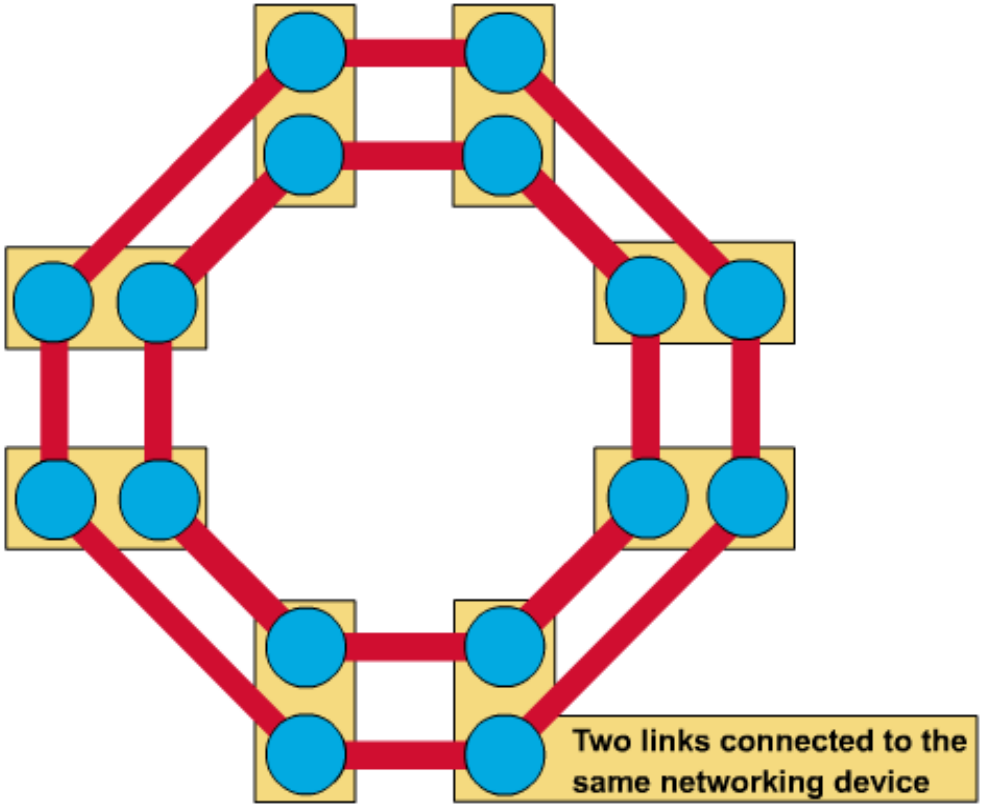
Ring Topology

Ring Topology



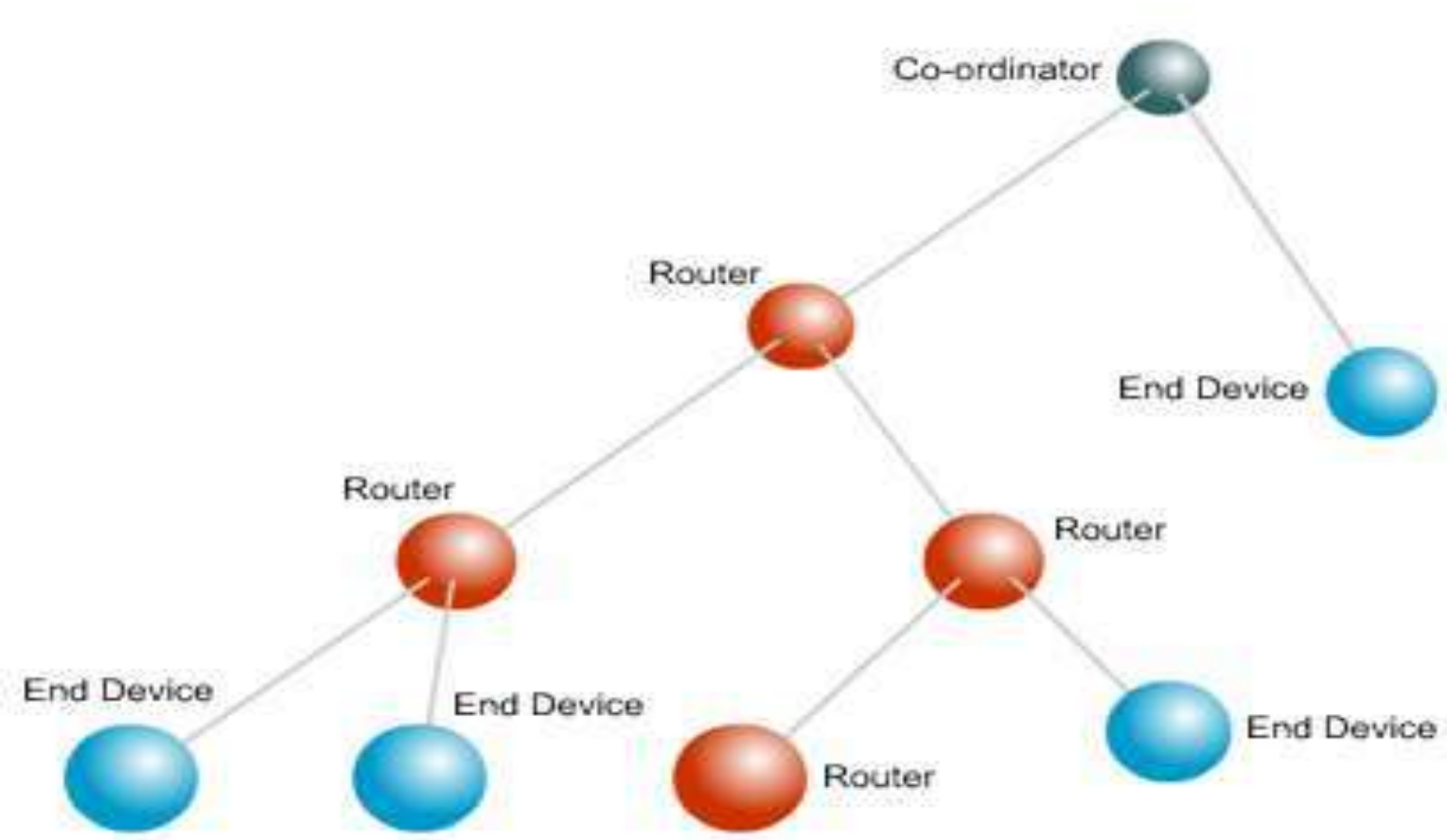
Ring Topology



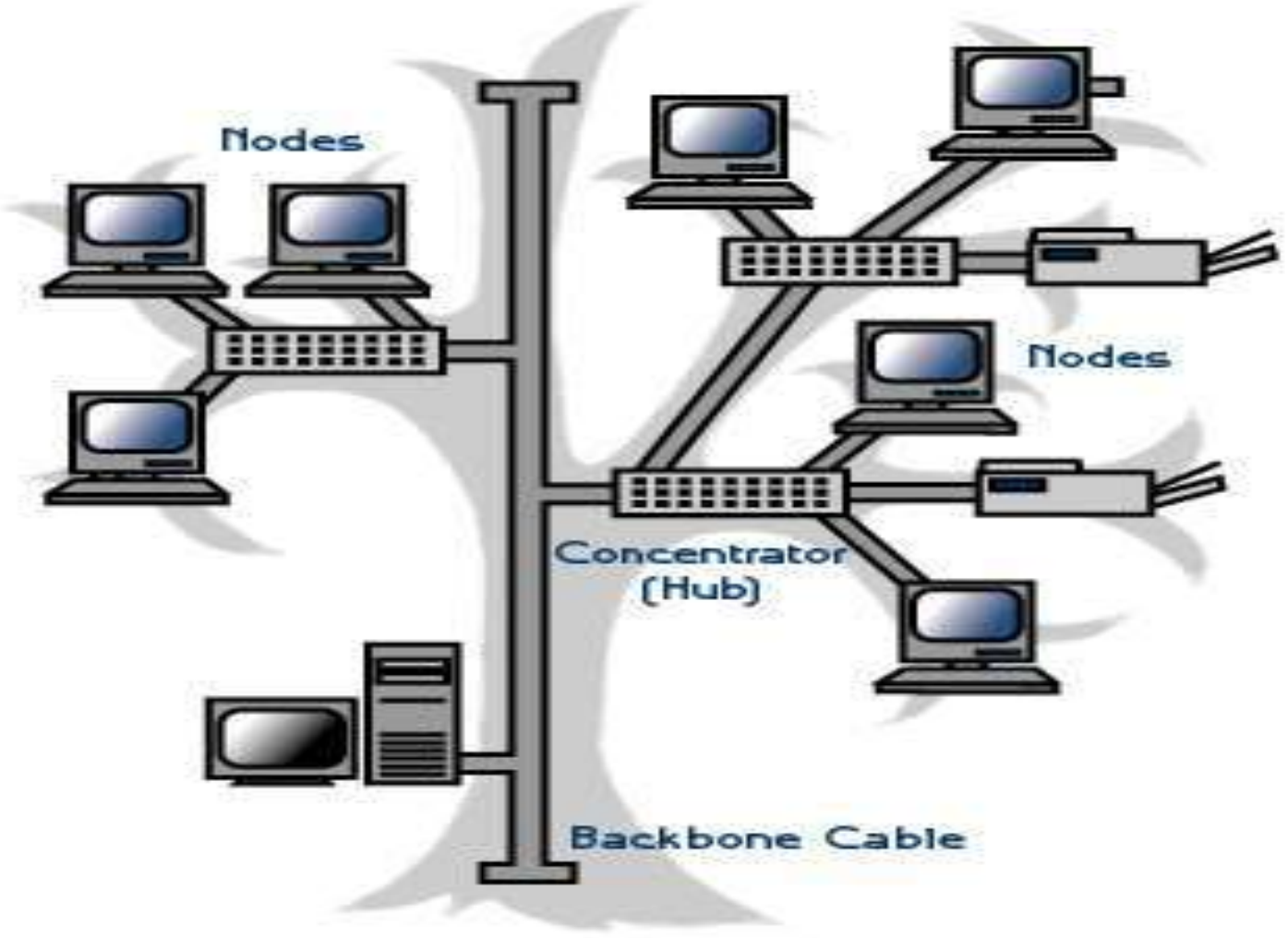


Tree Topology

Tree Topology



Tree Topology



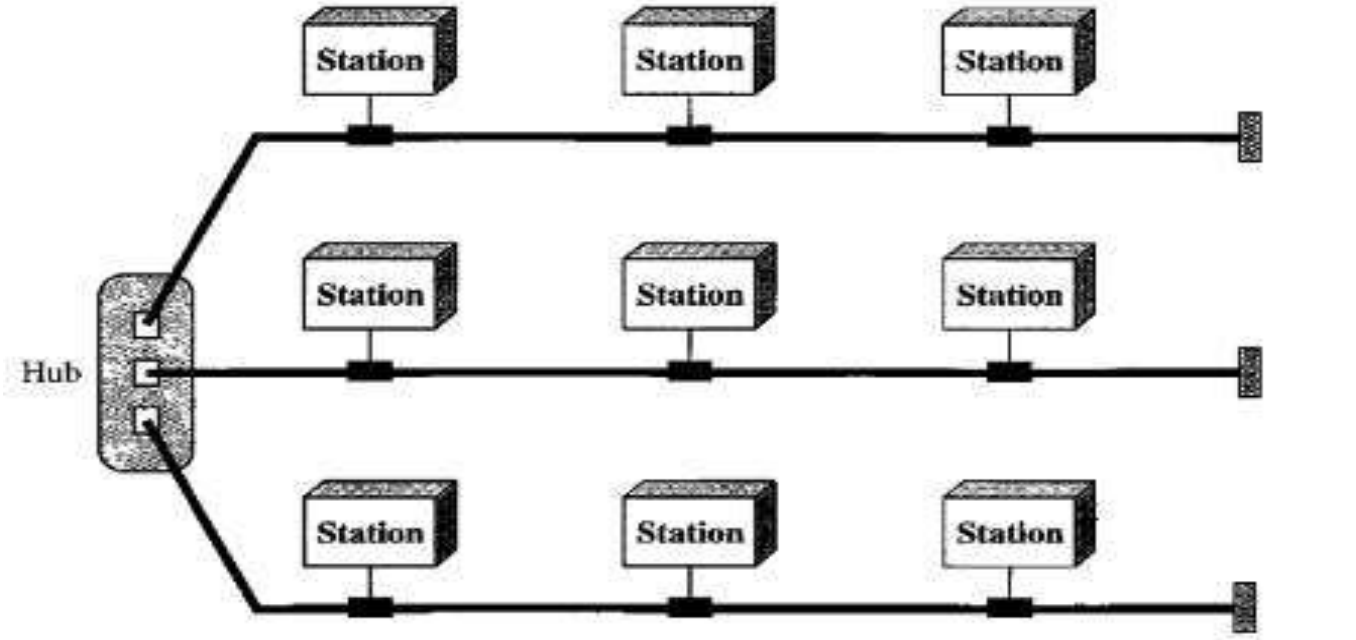
Hybrid Topology

Hybrid Topology

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies

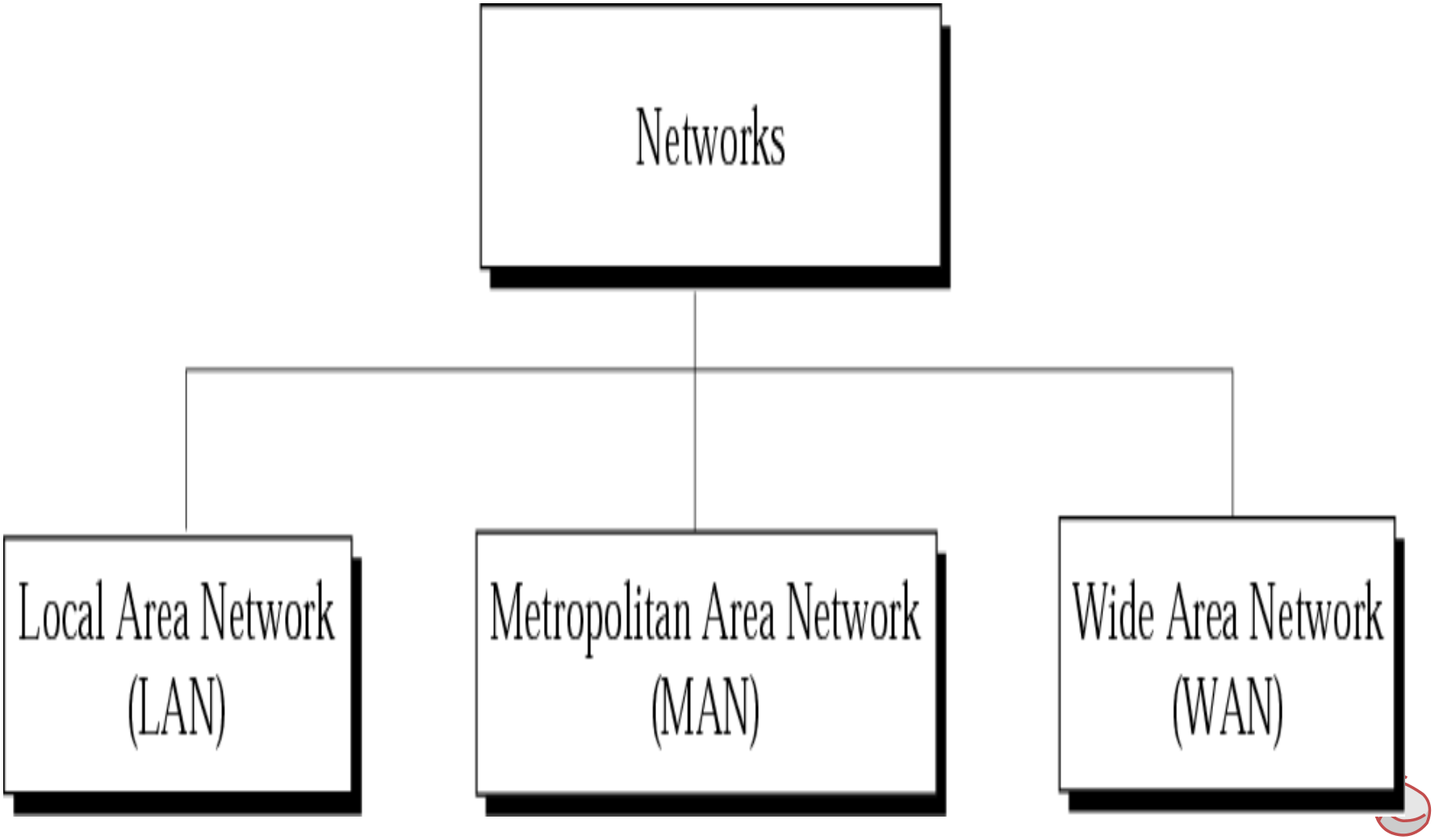
Hybrid Topology

A hybrid topology: a star backbone with three bus networks



Network Classification according to scaling

Main Categories of networks



Main Categories of Network

Local area network (LAN)

- Links computers within a building or group of buildings
- Uses direct cables, radio or infrared signals

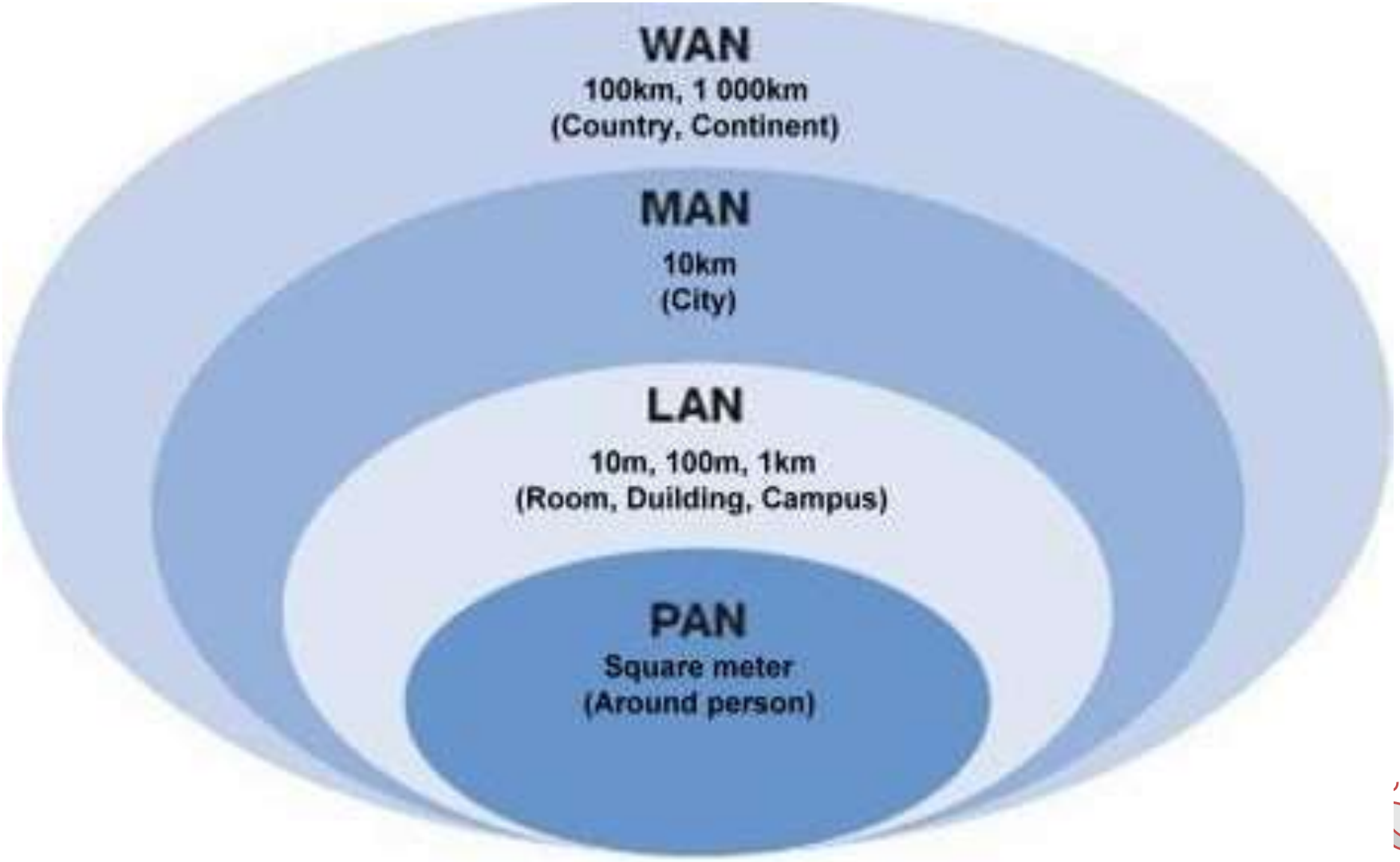
Metropolitan area network (MAN)

- Links computers within a major metropolitan area
- Uses fiber optic cables

Wide area network

- Links computers separated by a few miles or thousands of miles
- Uses long-distance transmission media

Network Scaling



Network Scaling

Inter processor distance	Processors are located in	networks
0.1 m	Same circuit board	Data flow machine
1m	Same system	Multi computer
10m	Same room	LAN
100m	Same building	LAN
1km	Same campus	LAN
10km	Same city	MAN
100km	Same country	WAN
1000km	Same continent	WAN
10000km	Same planet	Internet

PAN

PAN

Personal Area Networks (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**
  - **Wireless**

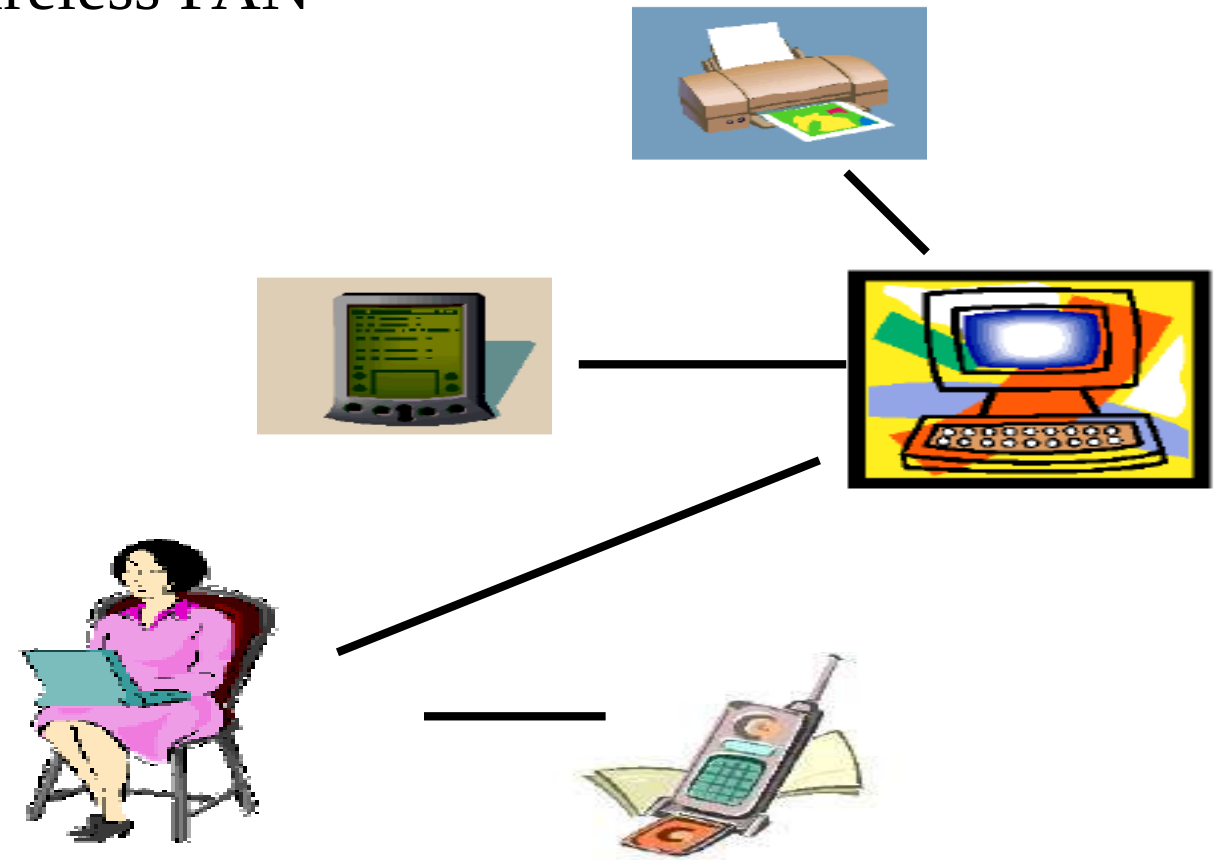
Personal Area Networks (PAN)

Personal Area Networks (PAN)

- 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, where many devices can be connected concurrently)
- PAN's can also be **wireless** through the use of ***bluetooth*** (a radio standard for interconnecting computers and devices such as telephones, printers or keyboards to the computer) or ***IrDA*** (infrared data association) technologies

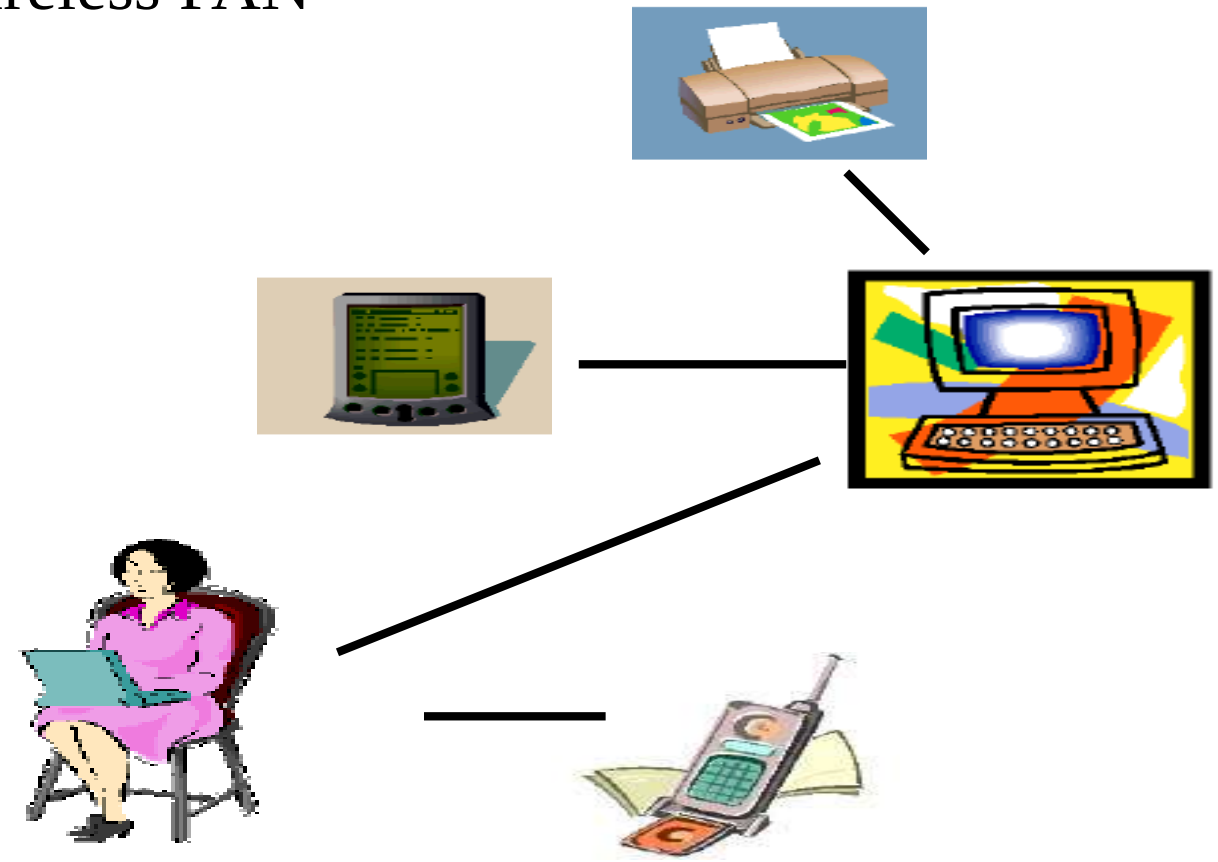
Personal Area Networks (PAN)

- Wireless PAN



Personal Area Networks (PAN)

- Wireless PAN

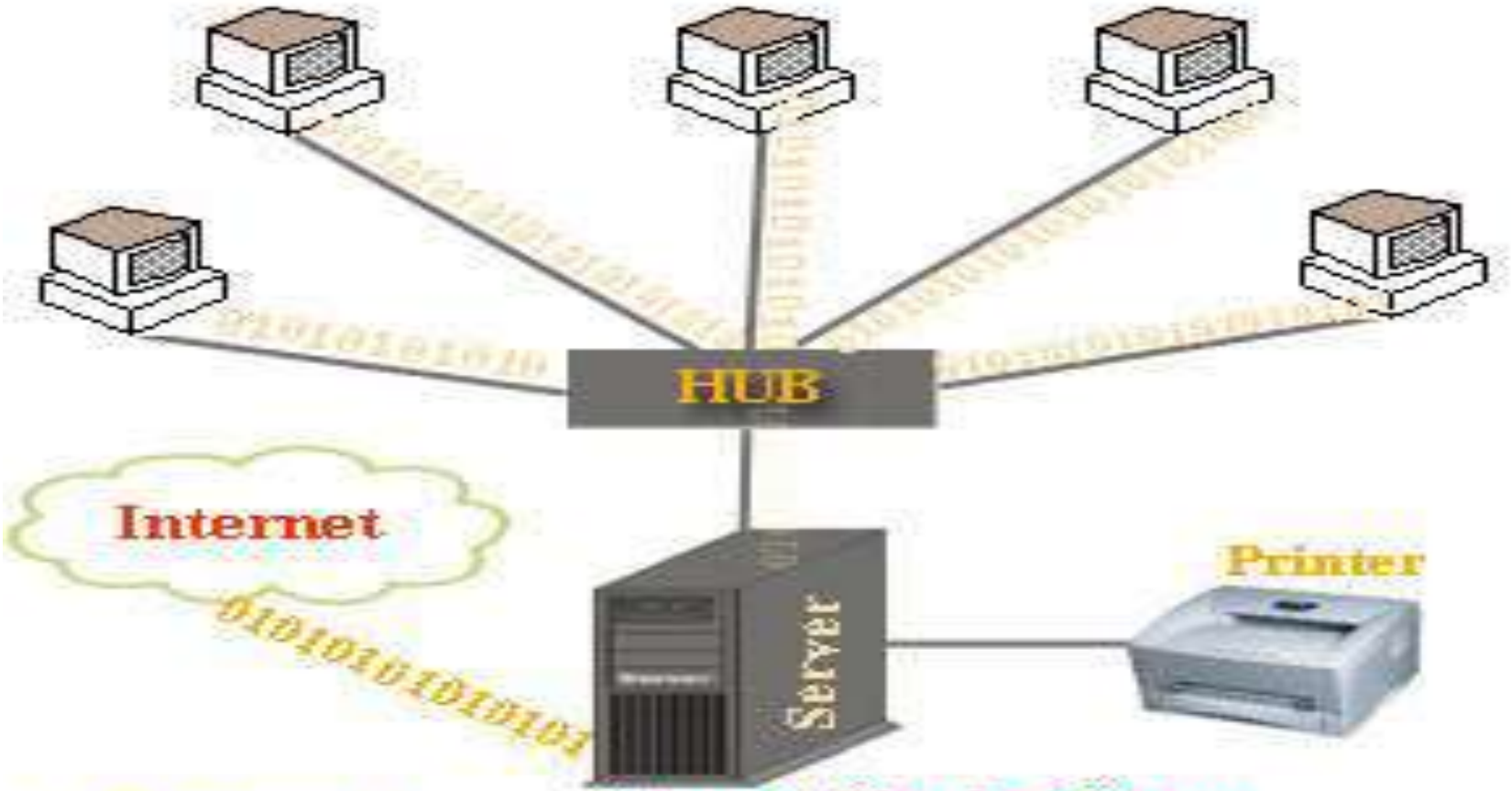


LAN

Local area networks (LAN)

- *A LAN is a network that is used for communicating among computer devices, usually within an **office building*** **or group of buildings** ***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 fast, with speeds from 100 Mbps or 1000 Mbps
- Requires **little wiring**, typically a **single cable** connecting to each device
- Most common LAN topologies are bus, ring and star.
- Has **lower cost** compared to MAN's or WAN's

Local area networks (LAN)



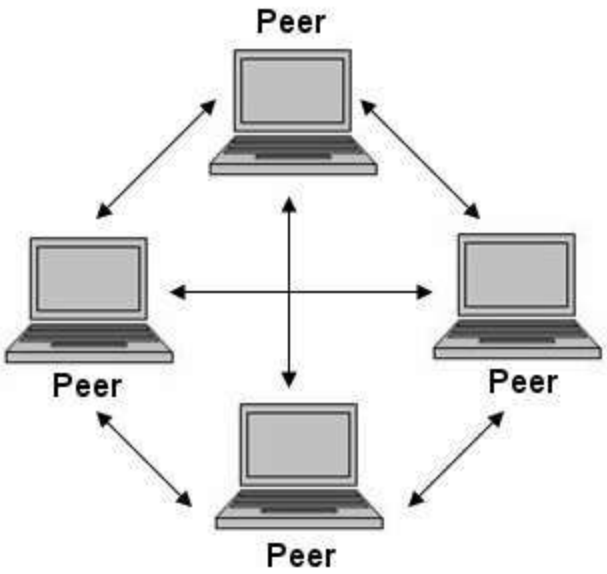
Local area networks (LAN)

- Users can **access software, data and peripherals**
- Computers connected to a LAN are called **workstations or nodes**

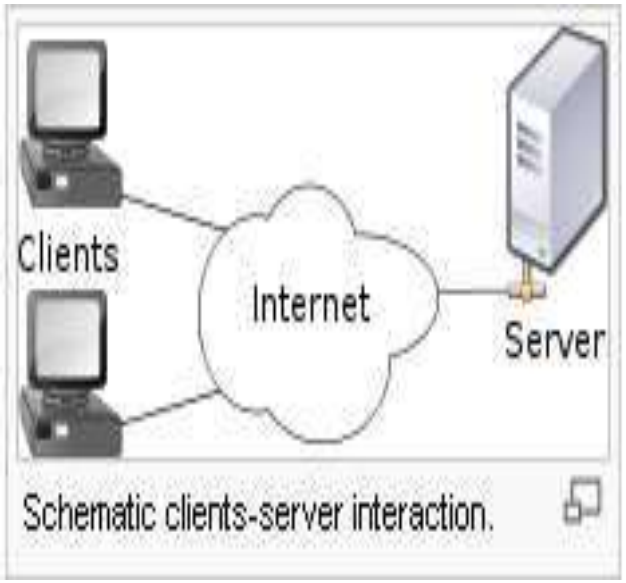
- **Different types:**
  - **Peer-to-peer**
  - **Client-server**

Local area networks (LAN)

- **Peer-to-peer**

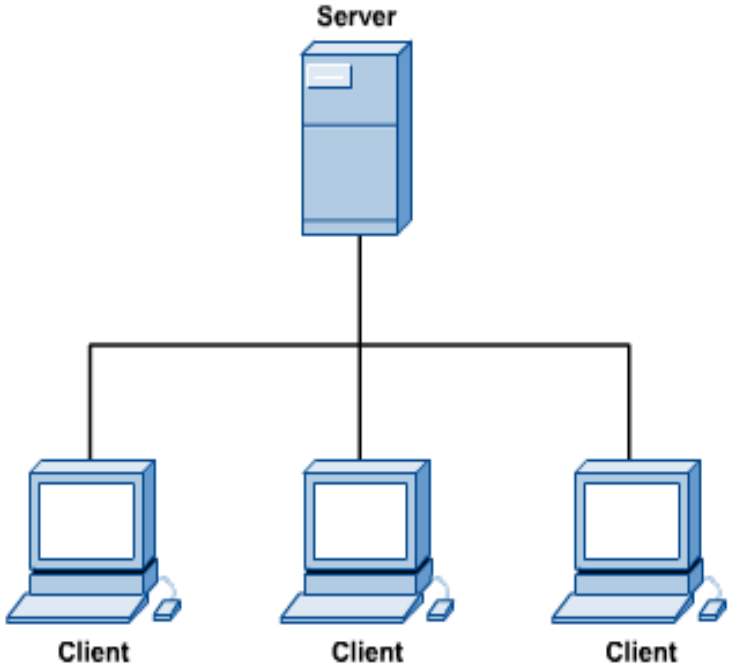


Client-server



LAN Clients and Servers

- In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.
- The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.



MAN

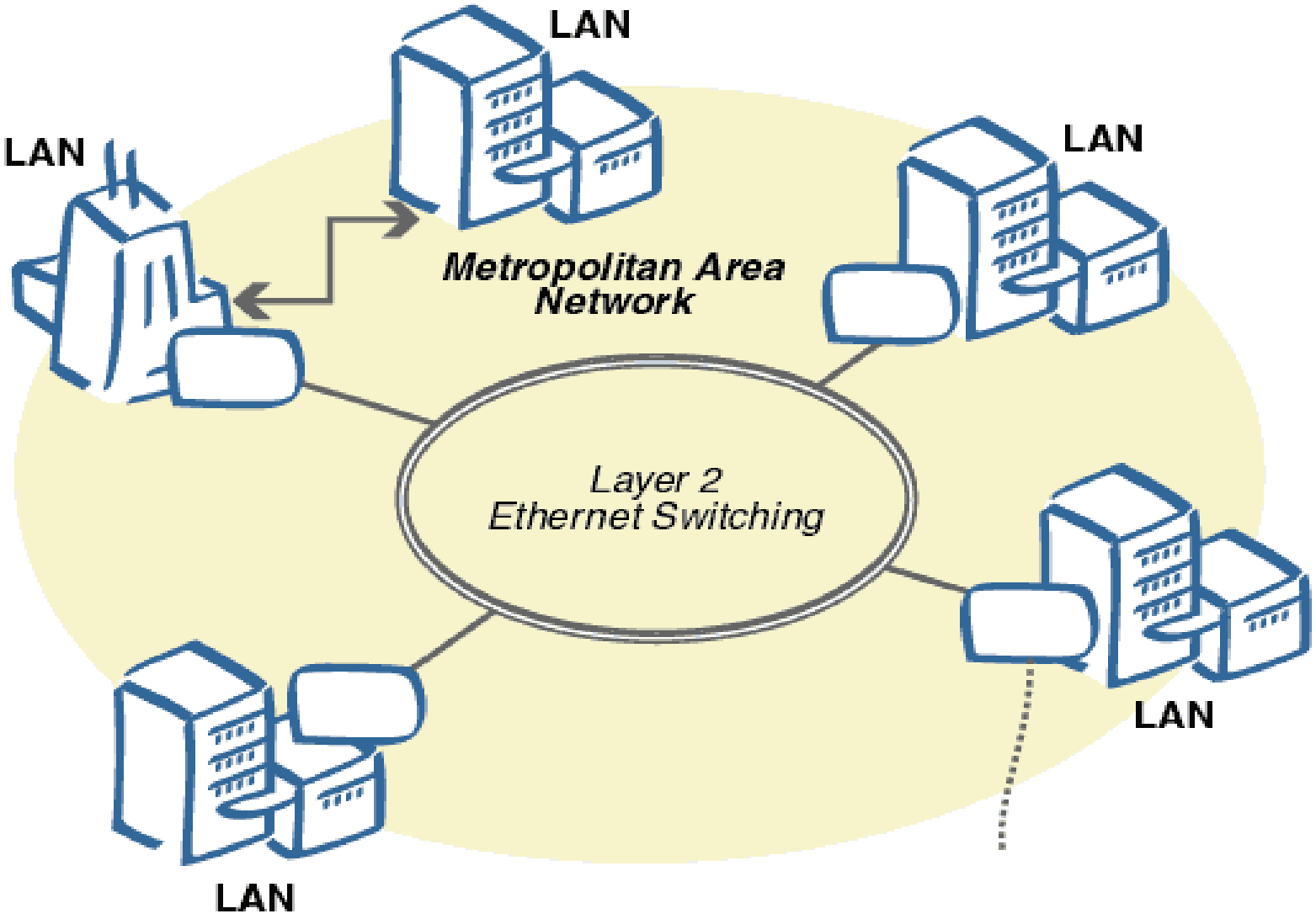
Metropolitan area network

- A **metropolitan area network (MAN)** is a computer network in which **two or more computers or communicating devices or networks which are geographically separated** but in **same metropolitan city.**

- A MAN is optimized for a **larger geographical area than a LAN**

- A MAN typically covers an area of **between 5 and 10 km diameter.**

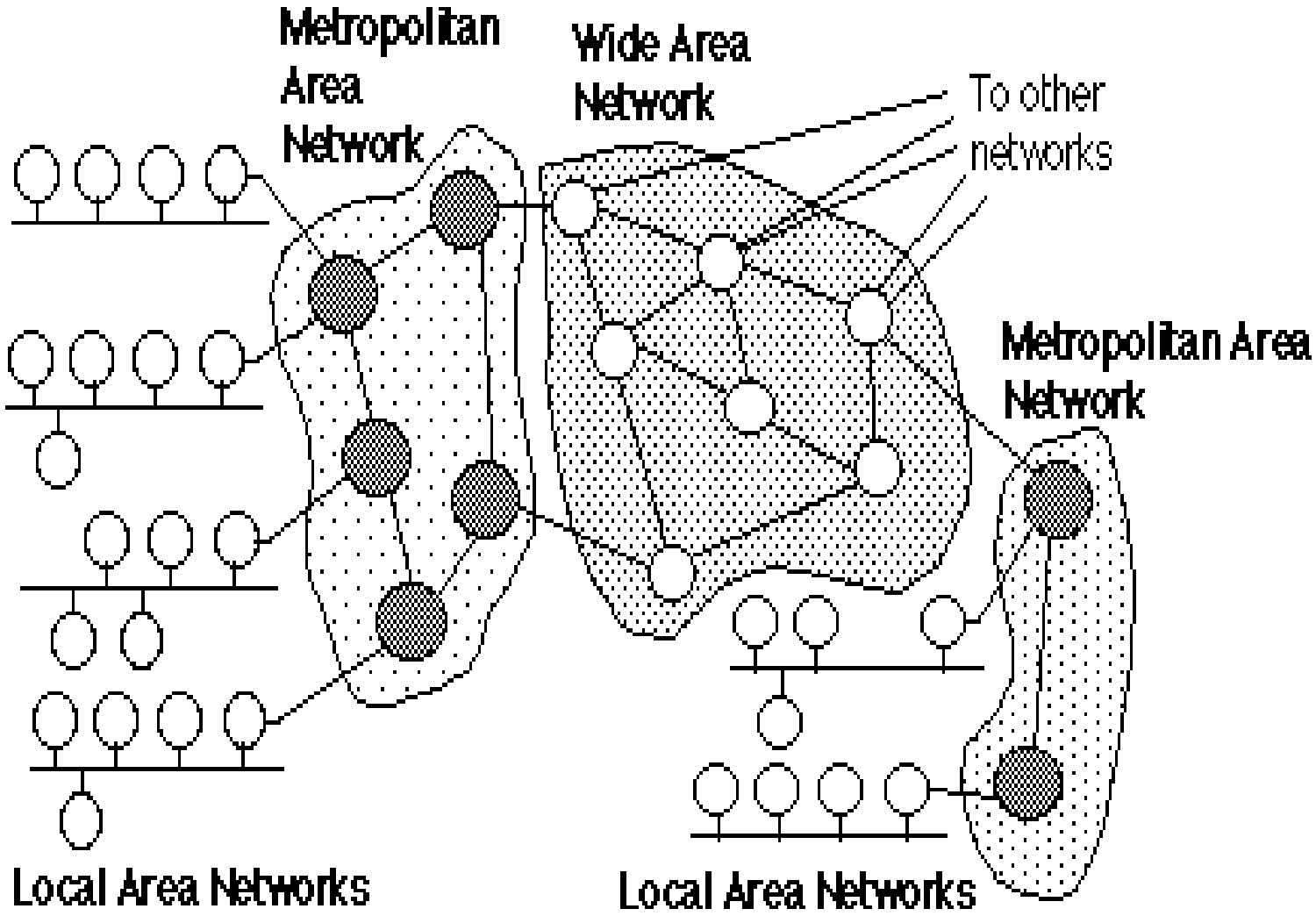
MAN


LAN
LAN
LAN
Metropolitan Area Network
Layer 2 Ethernet Switching
LAN
LAN

Metropolitan area network

- **Network in a City** is call MAN
- It is **larger than a LAN**, but **smaller than a WAN**
- It is also used to mean the **interconnection of several LANs** by bridging them together.

MAN

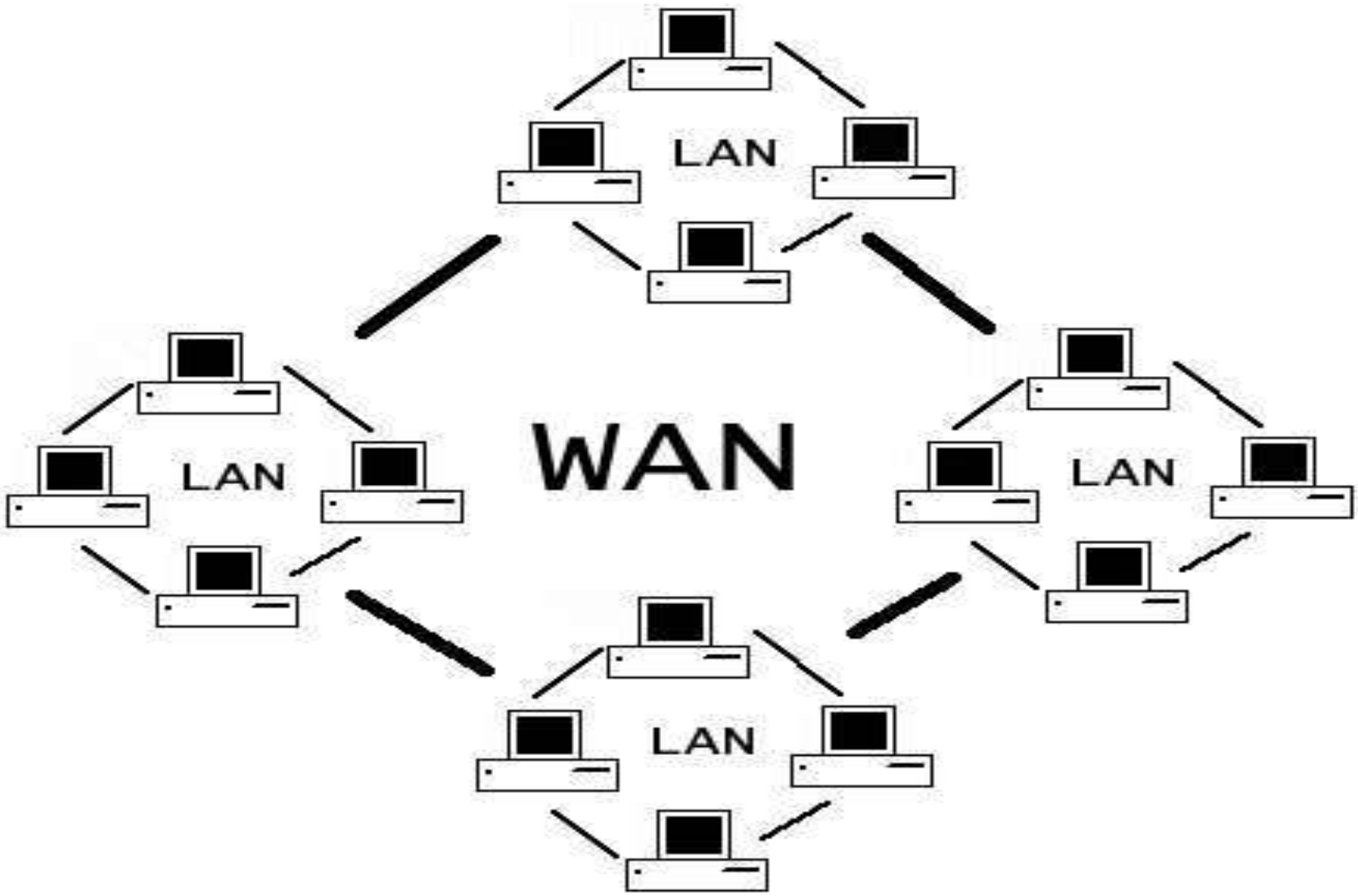

Metropolitan
Area
Network
Wide Area
Network
To other
networks
Metropolitan Area
Network
Local Area Networks
Local Area Networks

WAN

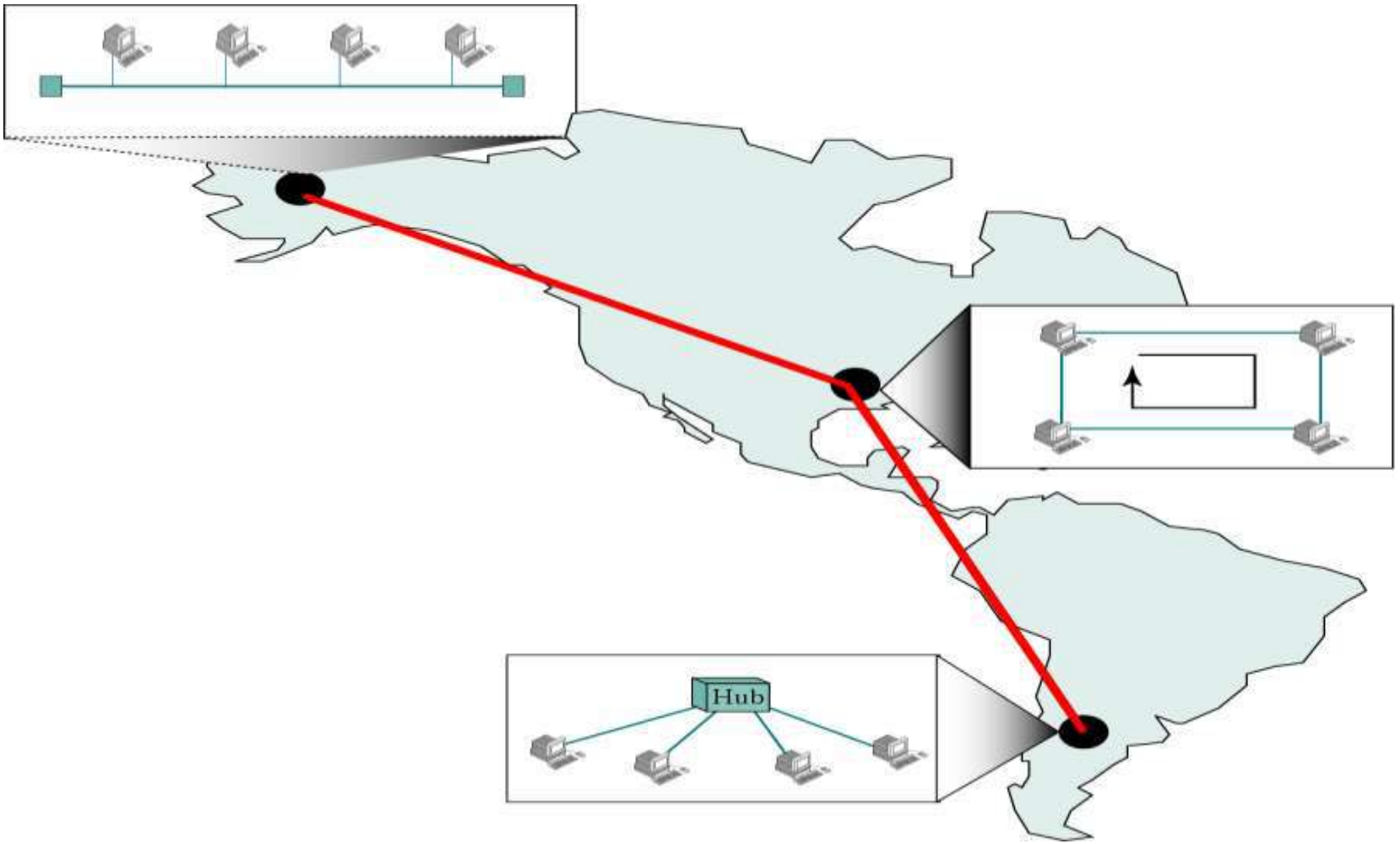
Wide area network (WAN)

- **A Wide Area Network** is a network in which a **large geographical area of around several hundred miles** to across the globe
- May be **privately owned or leased**
- Also called "**enterprise networks**" if they are privately owned by a large company
- Can be connected through **cable, fiber or satellite**
- Is typically **slower and less reliable than a LAN**

WAN



WAN



Types of WANs

Internet

- Backbone providers charge fees to Internet Service Providers (ISP)
- ISPs sell subscriptions to users
- Not secure
- Not ideal for businesses

Public Data Network (PDN)

- for-profit data communications network
- **Fees paid on a per-byte-transferred basis**
- Good security
- High bandwidth

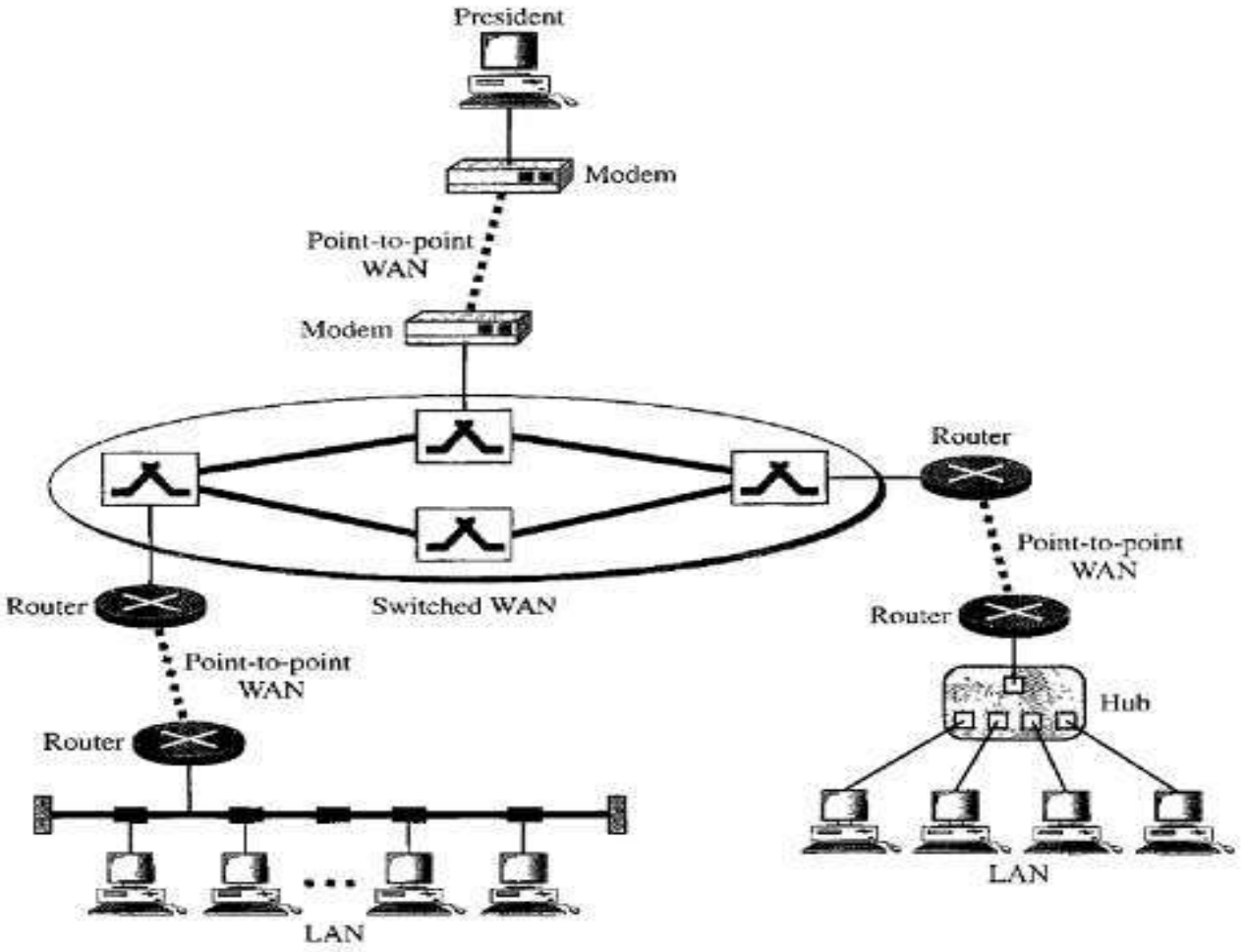
Private Data Network

- **Used by corporations, banks and governments**
- Not open to the public
- Most secure type of WAN
- Virtual private network- Lines are leased to a single company

Interconnection of Networks- Internetwork

- When two or more networks are connected, they become internetwork or internet

A heterogeneous network made of four WANs and two LANs

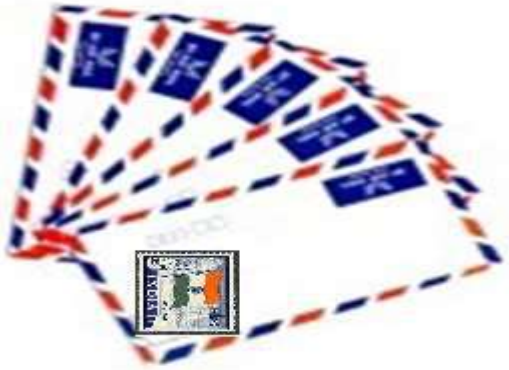


Layered Architecture

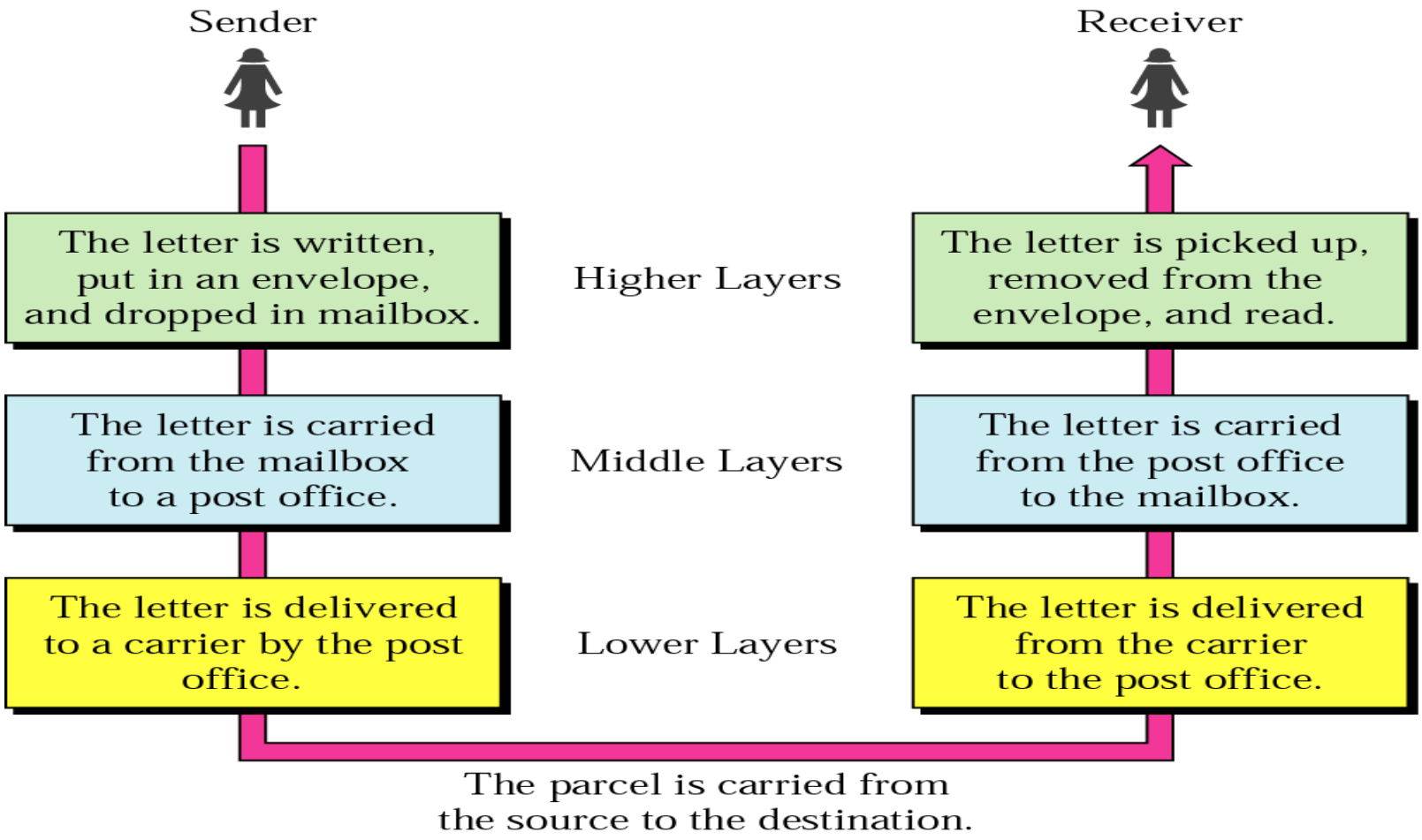
A simple example for communication

We use the concept of **layers** in our daily life.

As an example, let us consider two friends who communicate through postal mail.



simple example for communication



But 5 Steps are needed for proper delivery

simple example for communication

V. Writing letter in a paper (Raw Data)

IV. Put signature ,Fold the letter and put the letter in a cover (Adding Header1, Compression etc)

III. Seal the cover& Put signature (Provides security, Header2)

II. Dropped the letter in to mail box after fixing stamp (Adding Header3& trailer1)

I. Postman collects the letter to the post office (TRANSMISSION THROUGH A MEDIUM)

simple example for communication

- **Sorting the letter at the post office (ROUTING)**

I. Postman collects the letter from post office to the mail box **(Transmitting data bits)**

II. Letter was taken from mail box to Home **(Removing header3& Trailer)**

III. Open the cover& signature **(Removes Header2)**

IV. Take the letter from the cover **(Removing Header1)**

V. Reading letter **(Raw Data)**

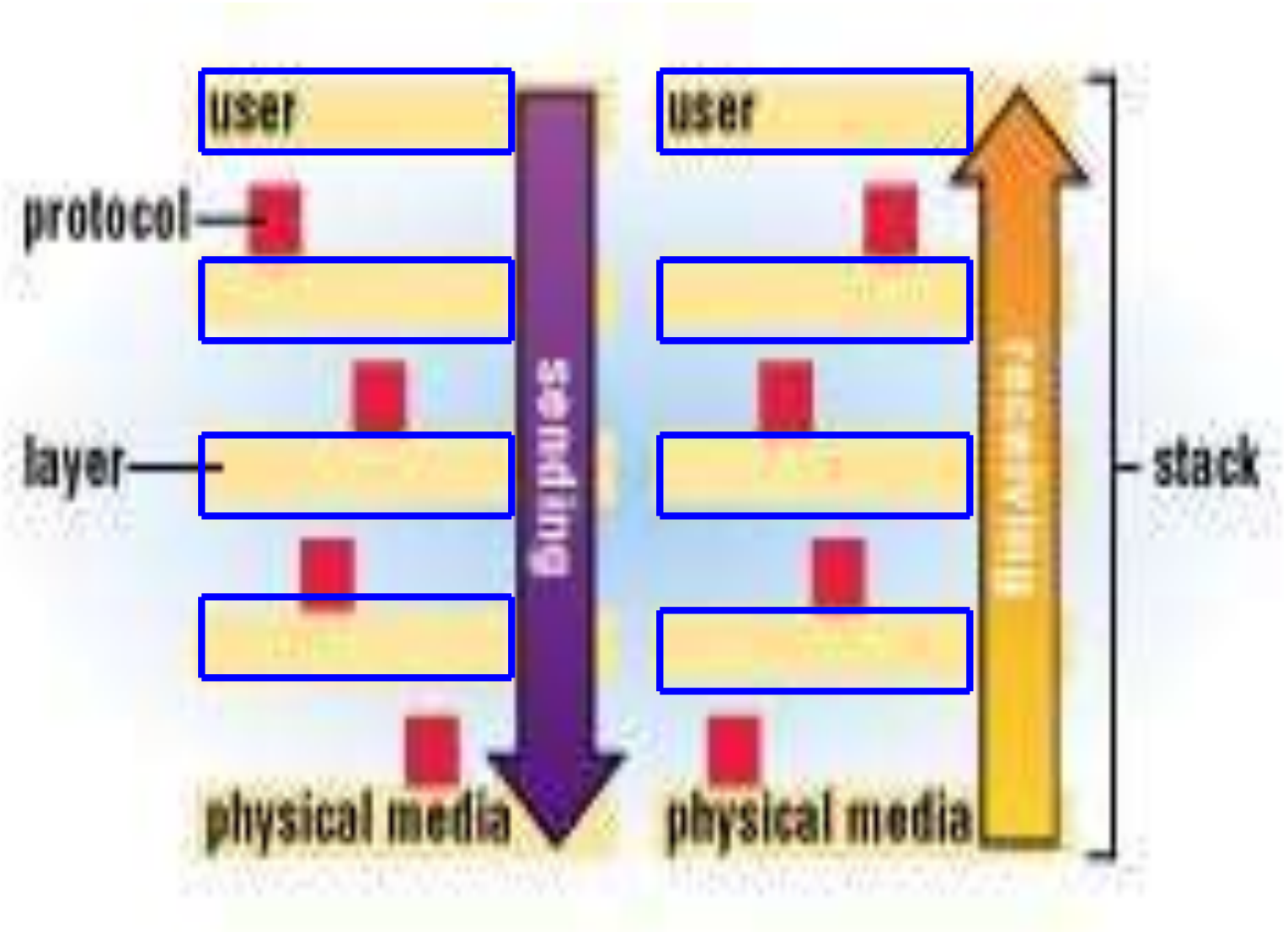
Network architecture

- **Network architecture is the overall design of a network**

- **The network design is divided into layers, each of which has a function separate of the other layers**

- **Protocol stack- The vertical (top to bottom) arrangement of the layers; Each layer is governed by its own set of protocols**

Network architecture



Virtual Communication Between layers

- **Message** is generated by 5th layer
- Layer 4 add **header** in front of message
  - Header include **control information** to send the message in the **right order.**
- Layer 3 **breaks up** the message in to small units called **packets**
- Layer 2 add **header and trailer** to packets.
- Layer 1 transmits the **raw data**.

Issues in Layered Architecture

- **Design Philosophy of Layered Architecture**

  - The complex task of communication is broken into simpler sub-tasks or modules
  - Each layer performs a subset of the required communication functions
  - Each layer relies on the next lower layer to perform more primitive functions
  - Changes in one layer **should not affect** the changes in the other layers
  - Helps in troubleshooting and identifying the problem

Network Models

Need for Network Models

- **Network communication is an extremely complex task.**
- **Layer architecture simplifies the network design.**
- **The complex task of communication is broken into simpler sub-tasks or modules**
- **Need cooperative efforts from all nodes involved**

Need for Network Models

- **A standard model helps to describe the task of a networking product or service**

- **Also help in troubleshooting by providing a frame of reference.**

The network management is easier due to the layered architecture.

.

Need for Layered Architecture

- Each layer **works with the layer below and above it**

- Each layer provides **services to next layer**

Who define Network Model?

- **Need non-profit making organizations**
  - **ISO - International Standards Organization**

    IEEE - Institute of Electrical & Electronic Engineers

    ITU - International Telecommunication Union

OSI Model

OSI Reference Model

The Open Systems Interconnection model is a theoretical model that shows how any two different systems can communicate with each other.

OSI Reference Model

- The OSI model is now considered the **primary Architectural** model for inter-computer communications.

- The OSI model **describes** how **information or data** **makes its way from application programmes** through a **network medium** (such as wire) **to another application programme located on another network.**

- This **separation into smaller more manageable functions is known as layering.**

OSI Model

- To standardize the design of communication system, the ISO created the OSI model
- ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.

- Contains **Seven layers**

- It **describes the functions** to be performed at **each layer**

OSI Model

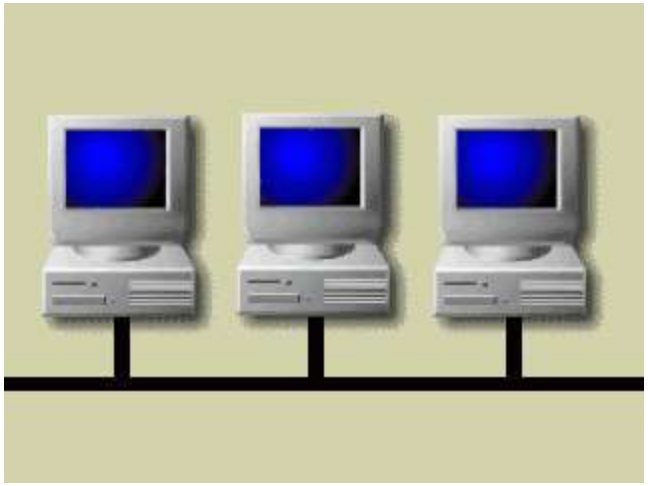
- First introduced this model in the late **1970s.**
- A **layer model**, Each layer performs a **subset** of the required communication functions
- Changes in one layer should not require changes in other layers

Important

ISO is the organization.
OSI is the model.

OSI Model

Application
Presentation
Session
Transport
Network
Data Link
Physical



The OSI 7-layer Model

All

People

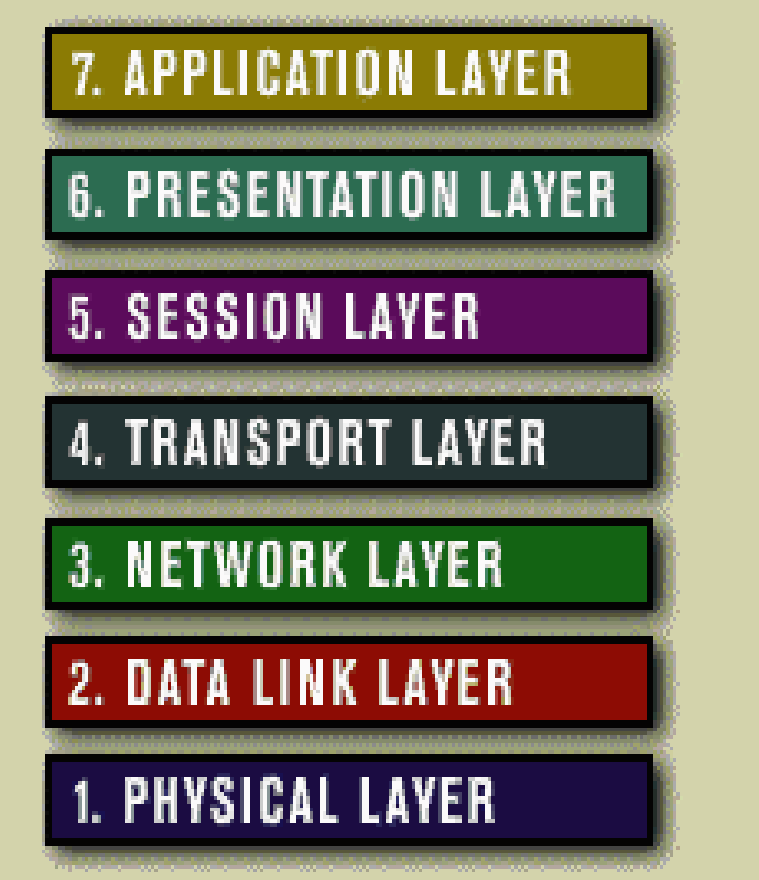
Seem

To

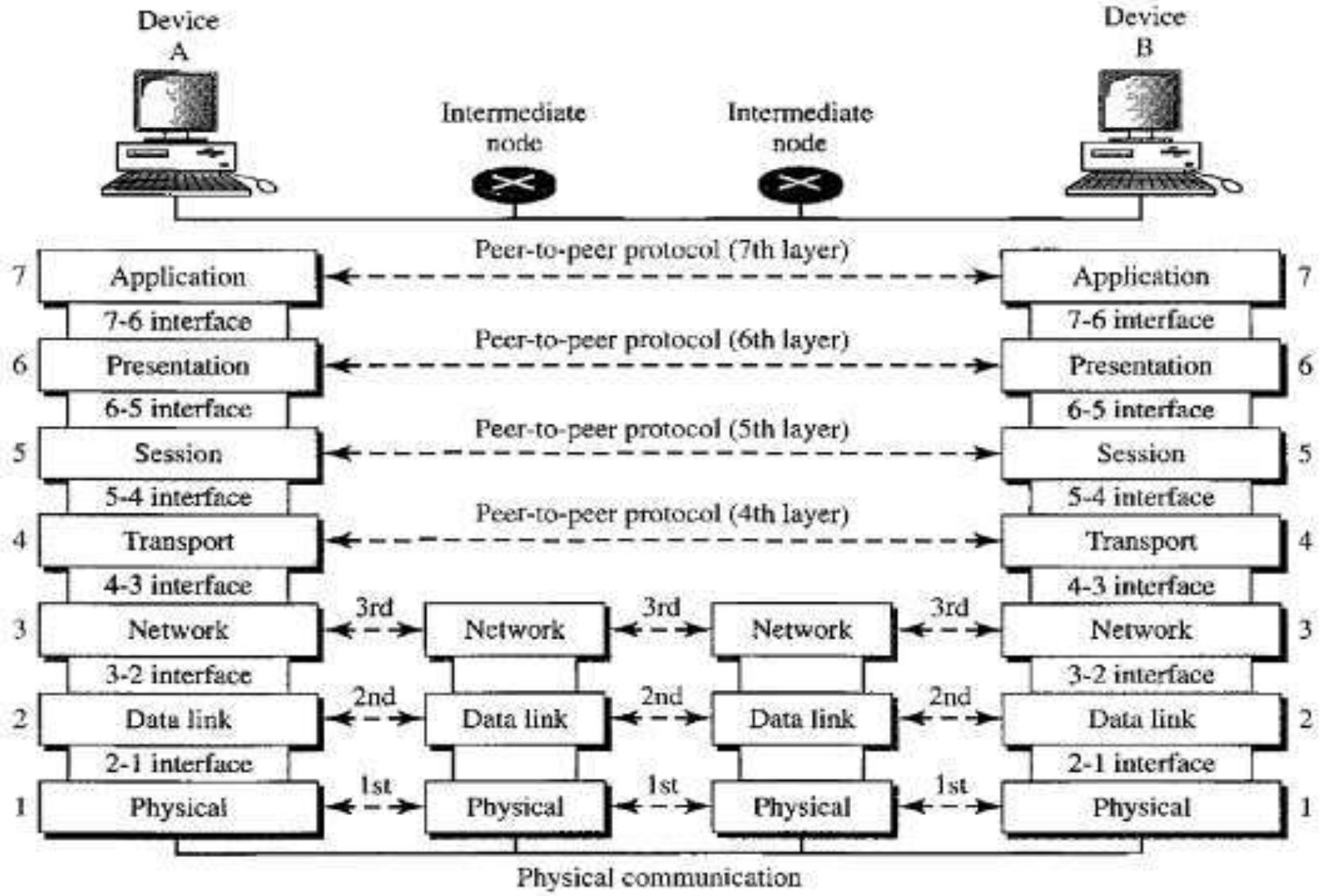
Need

Data

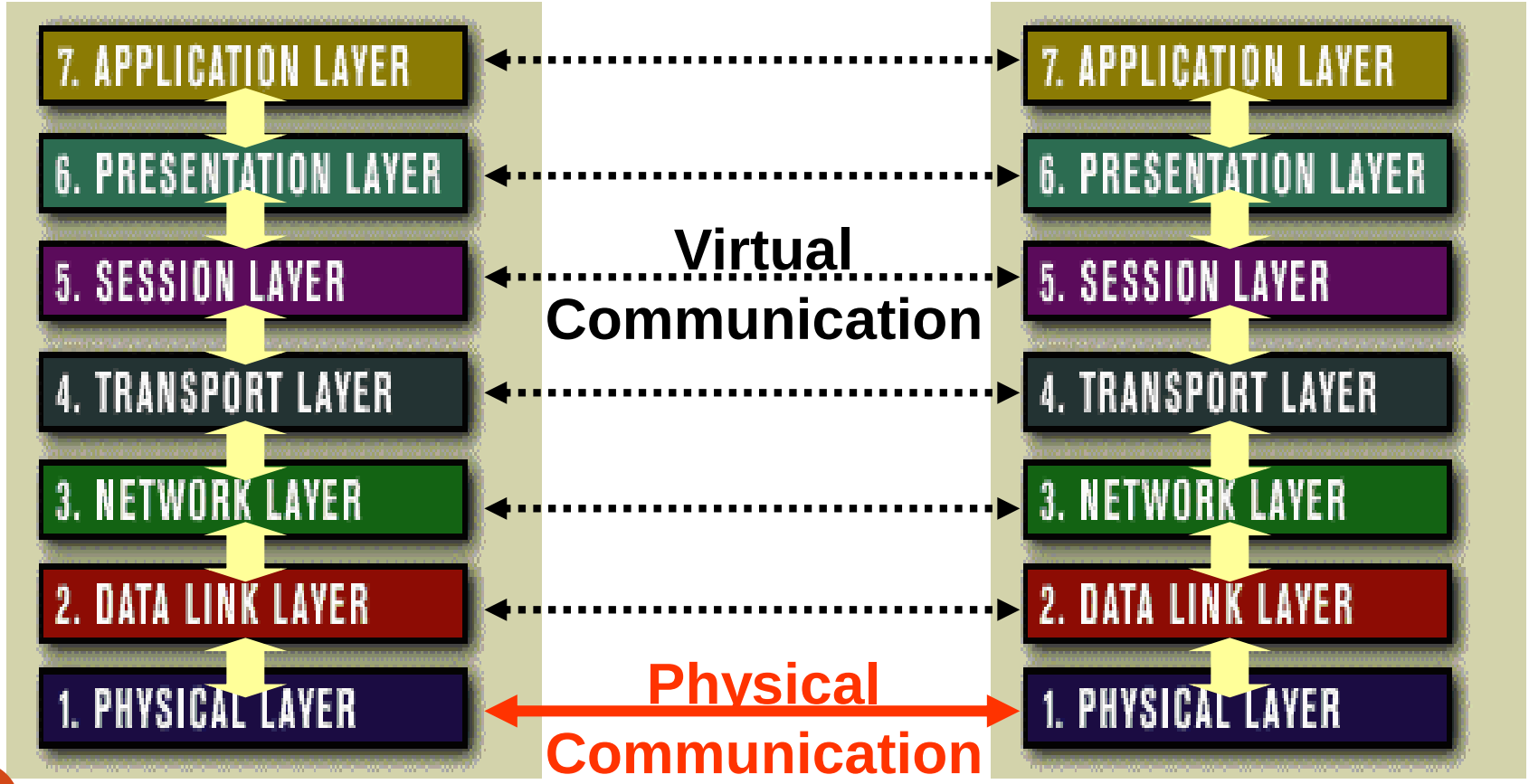
Processing



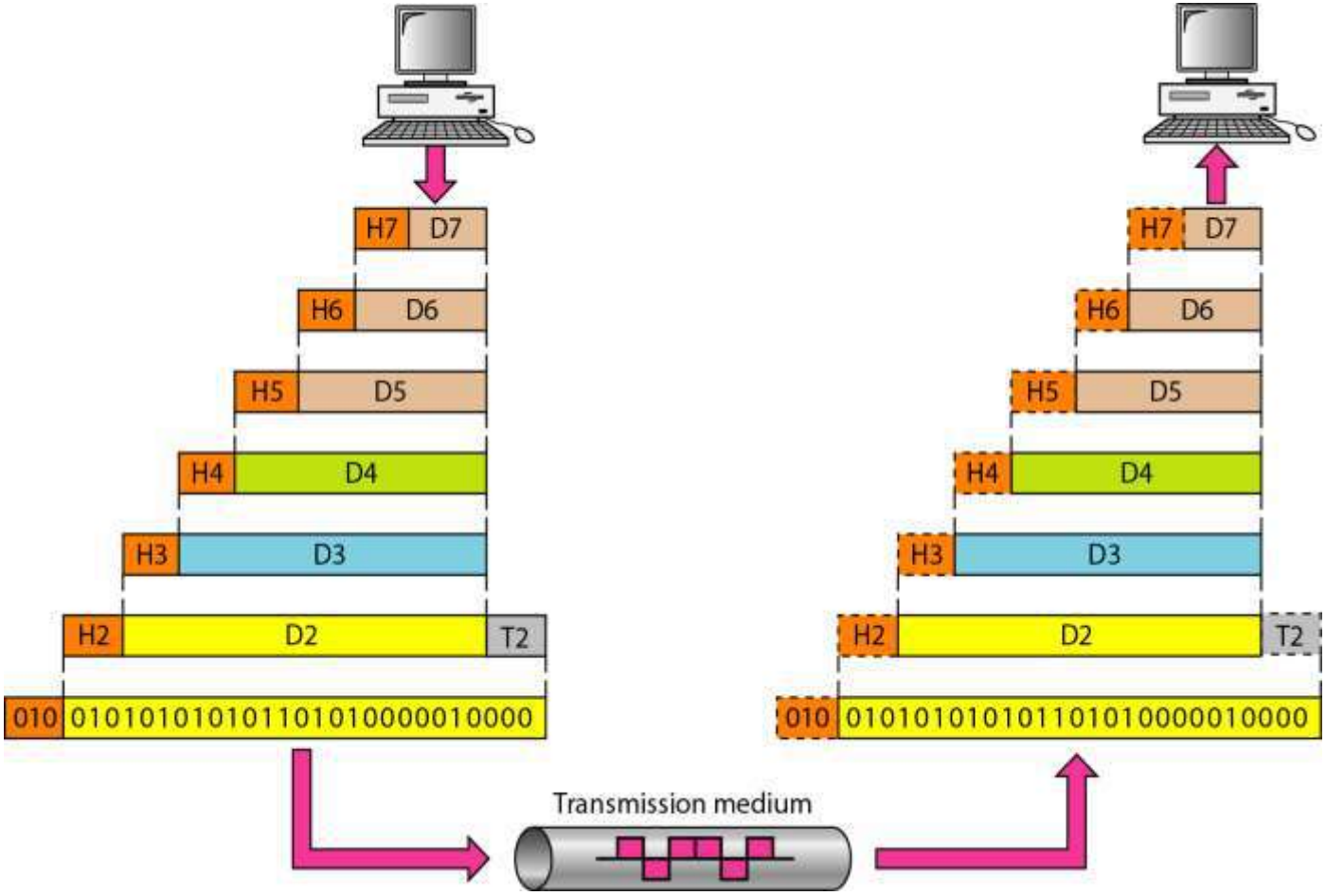
Peer-to-Peer Process using OSI



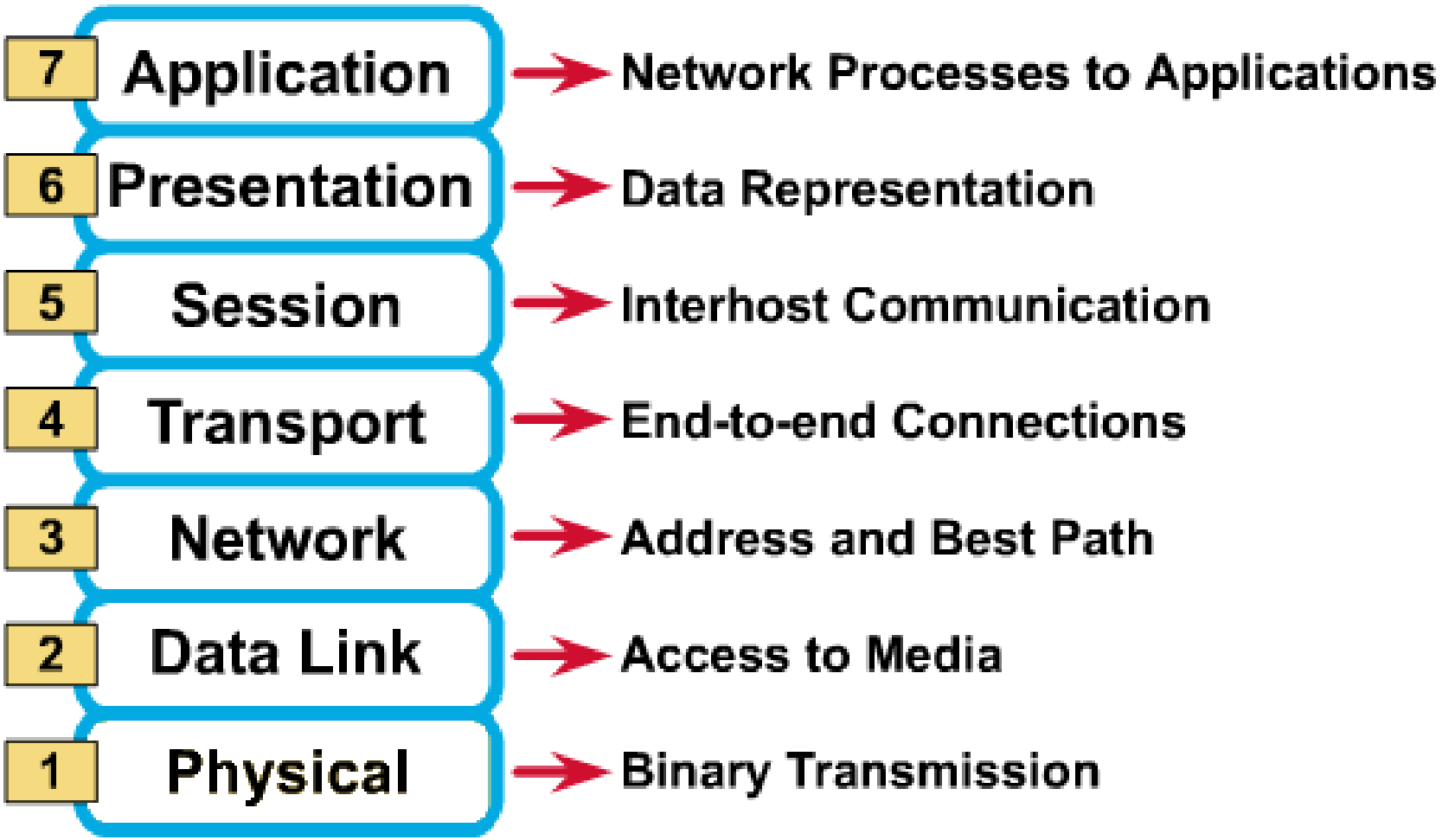
Relationship of OSI layers



Data exchange using the OSI model

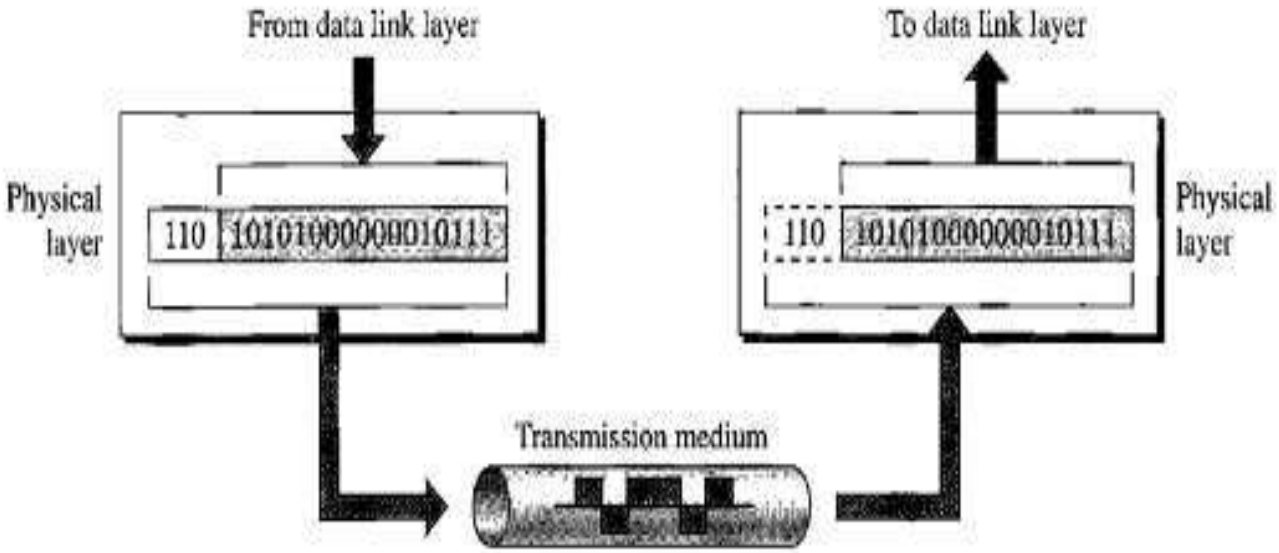


OSI Model


7 Application
Network Processes to Applications
6 Presentation
Data Representation
5 Session
Interhost Communication
4 Transport
End-to-end Connections
3 Network
Address and Best Path
2 Data Link
Access to Media
1 Physical
Binary Transmission

Functions of Physical layer

Physical Layer



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

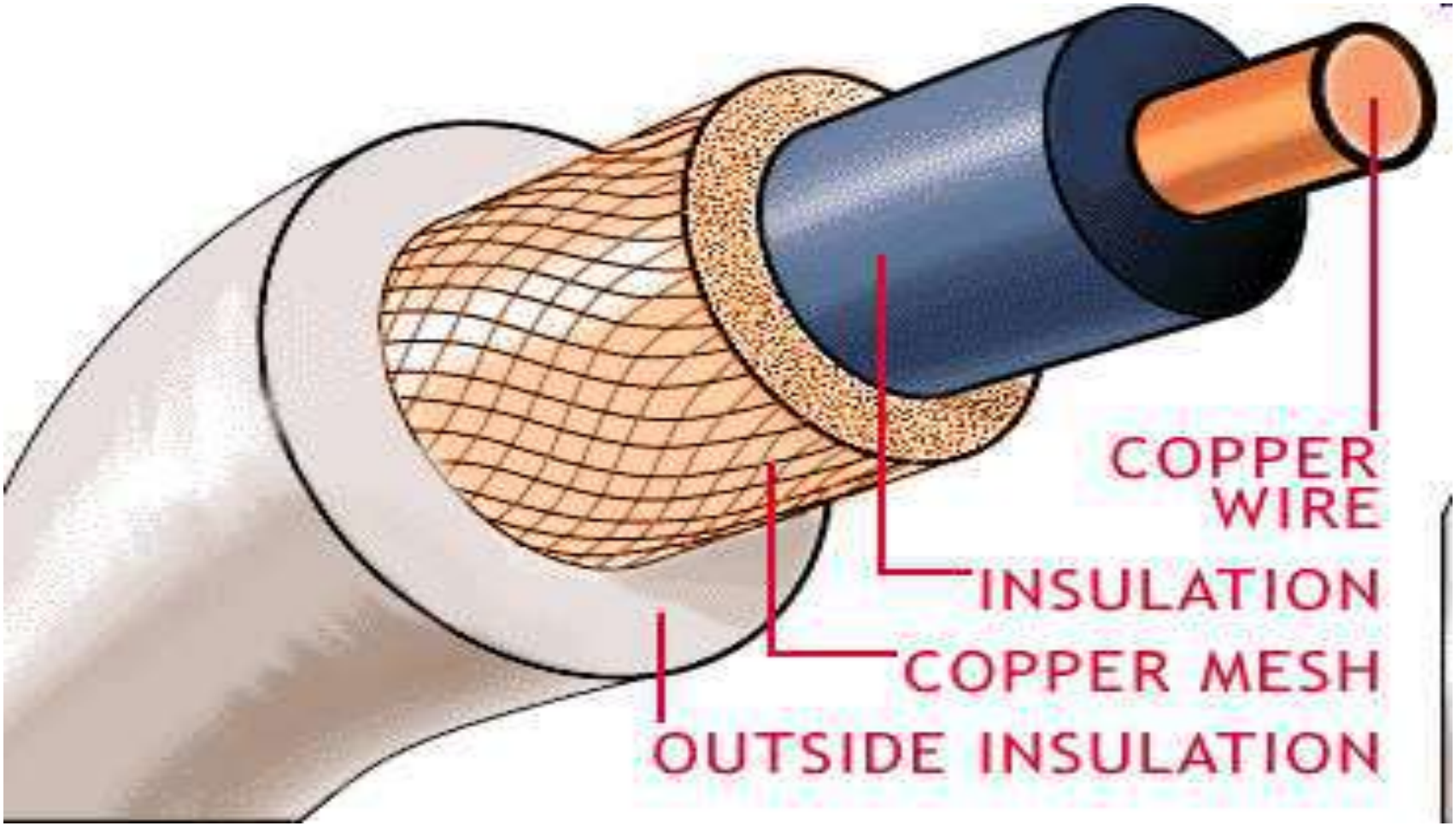
OSI Model – Physical Layer

- This layer is the **lowest layer** in the **OSI model.**
- It helps in the **transmission of data** between **two machines** that are **communicating** through a **physical medium,** which can be **optical fibres, copper wire or wireless** etc.
- **Hardware Specification:**
  - The **details of the physical cables**, **network interface cards**, **wireless radios**, etc are a **part of this layer.**
-

OSI Model – Physical Layer

- Physical interface between device and transmission medium
- Representation of bits- Bits must be encoded into electrical or optical signals
- Data rate- Number of bits transmitted per second
- Synchronization of bits- Sender and Receiver clocks must be synchronized
- Line configuration- Connection of devices to media
- Physical topology
- Transmission mode

Medium used for Physical Connections



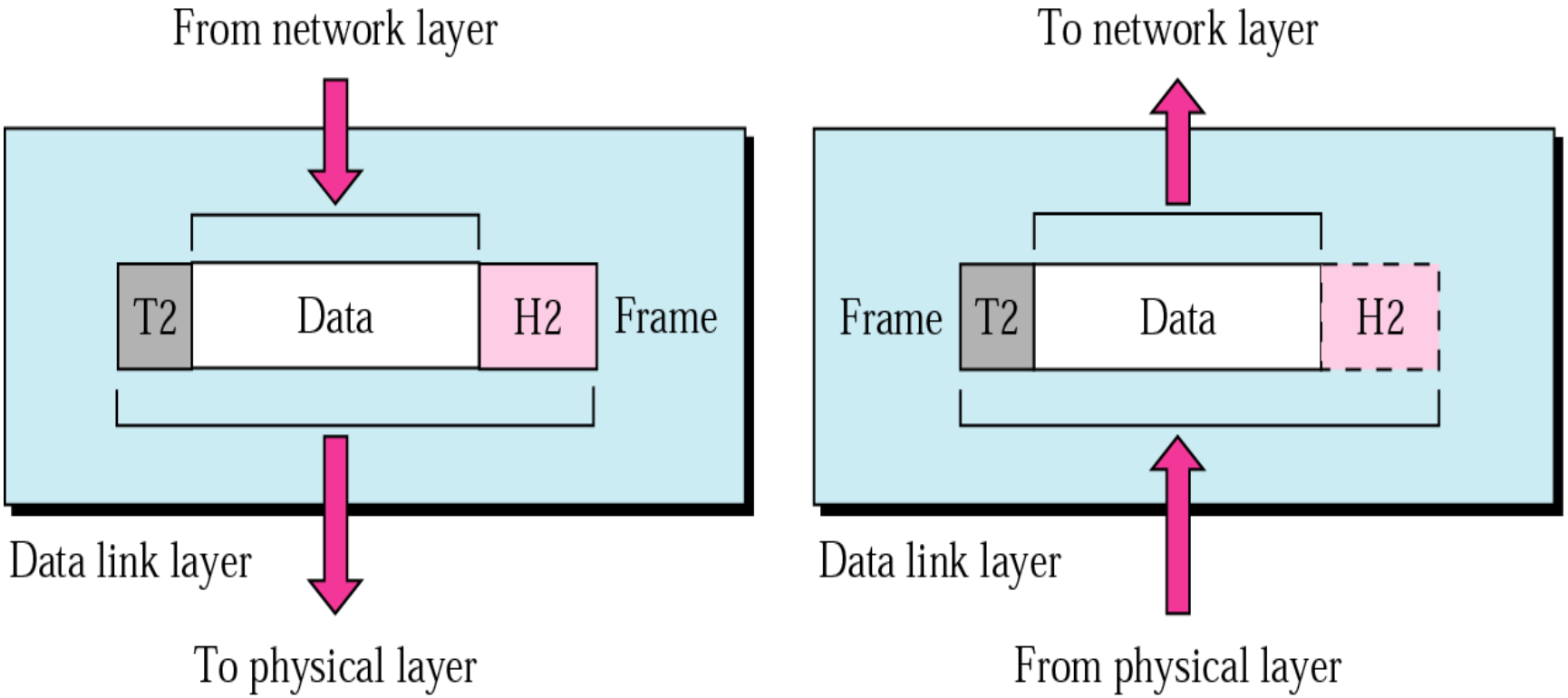
Medium used for Physical Connections

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

Functions of Data link layer

OSI Model – Data Link Layer

- **Means of activating, maintaining and deactivating a reliable link**

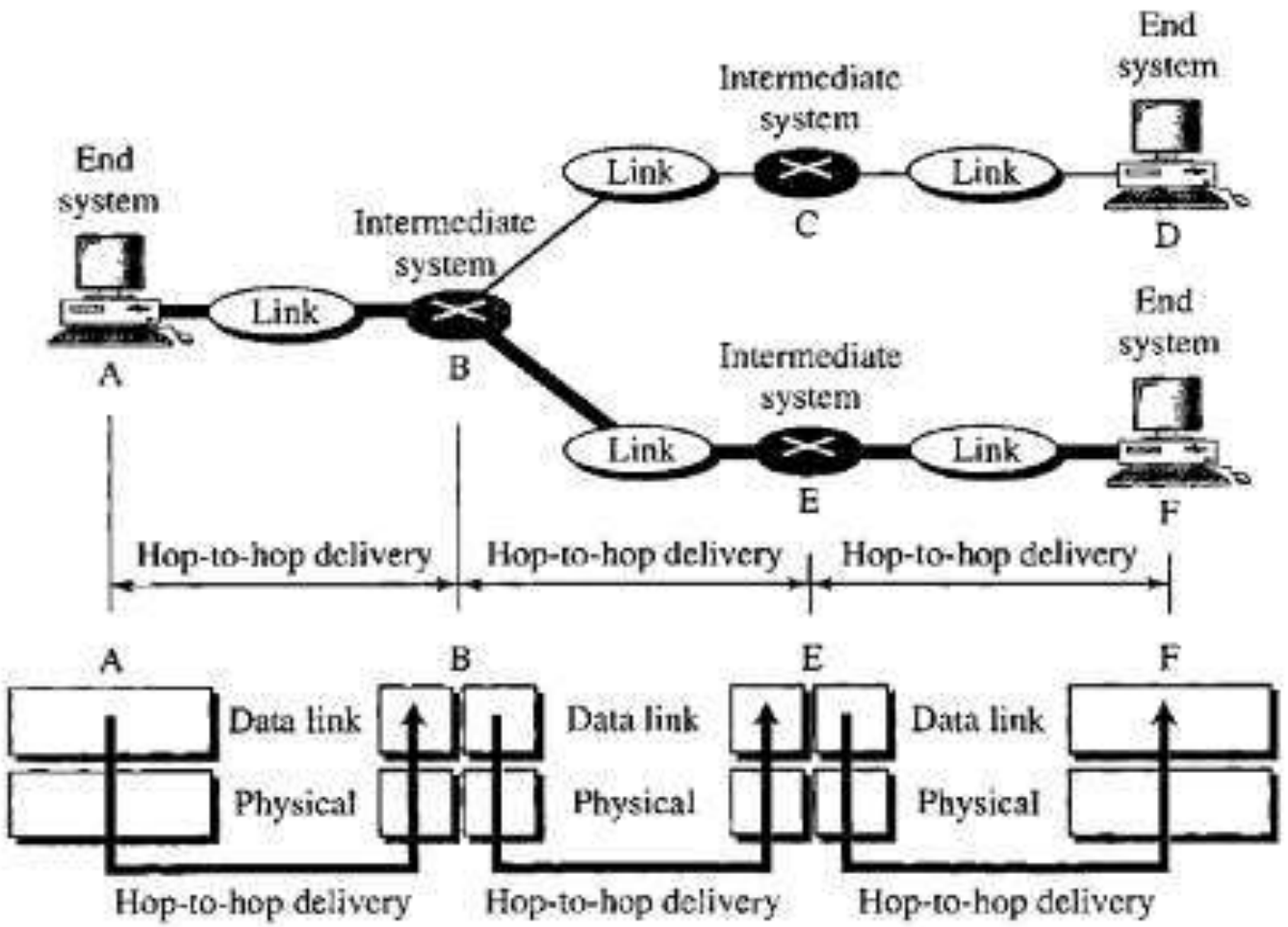


Functions of Data Link Layer

- Framing – converts stream of bits from NL into frames
- Physical Addressing- Adds header to frame to define sender/receiver of the frame
- Flow Control – If the data rate absorbed by the receiver is less than the rate at which data are produced at the sender
- Error Control – Detect and retransmits damaged of lost frames, recognize duplicate frames
- Access control – Data link layer protocols determines access of the link by a device out of many devices connected

Functions of Data Link Layer

Hop-to-hop delivery



203

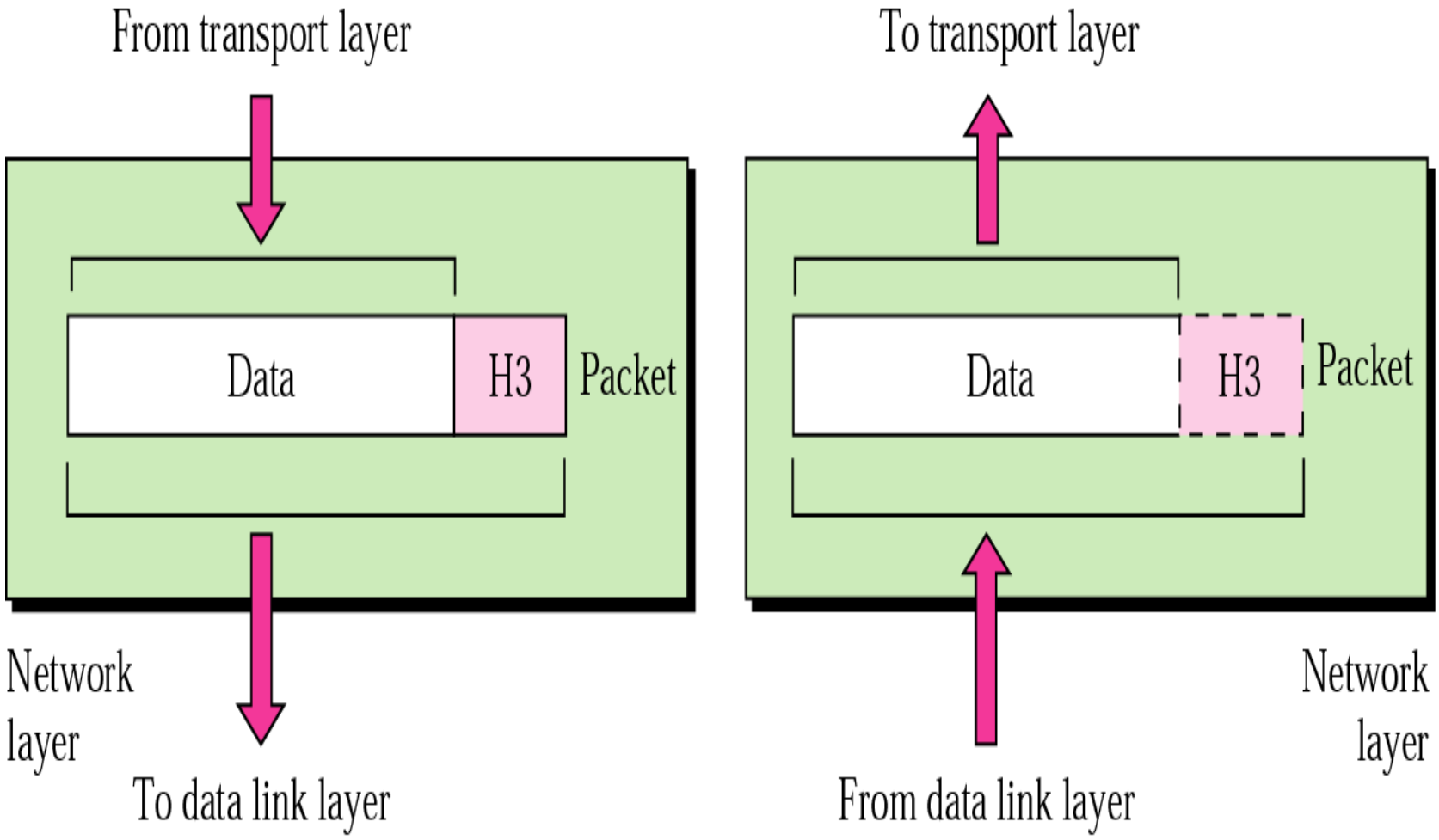
The data link layer is responsible for moving frames from one hop (node) to the next.

Functions of Network layer

OSI Model – Network Layer

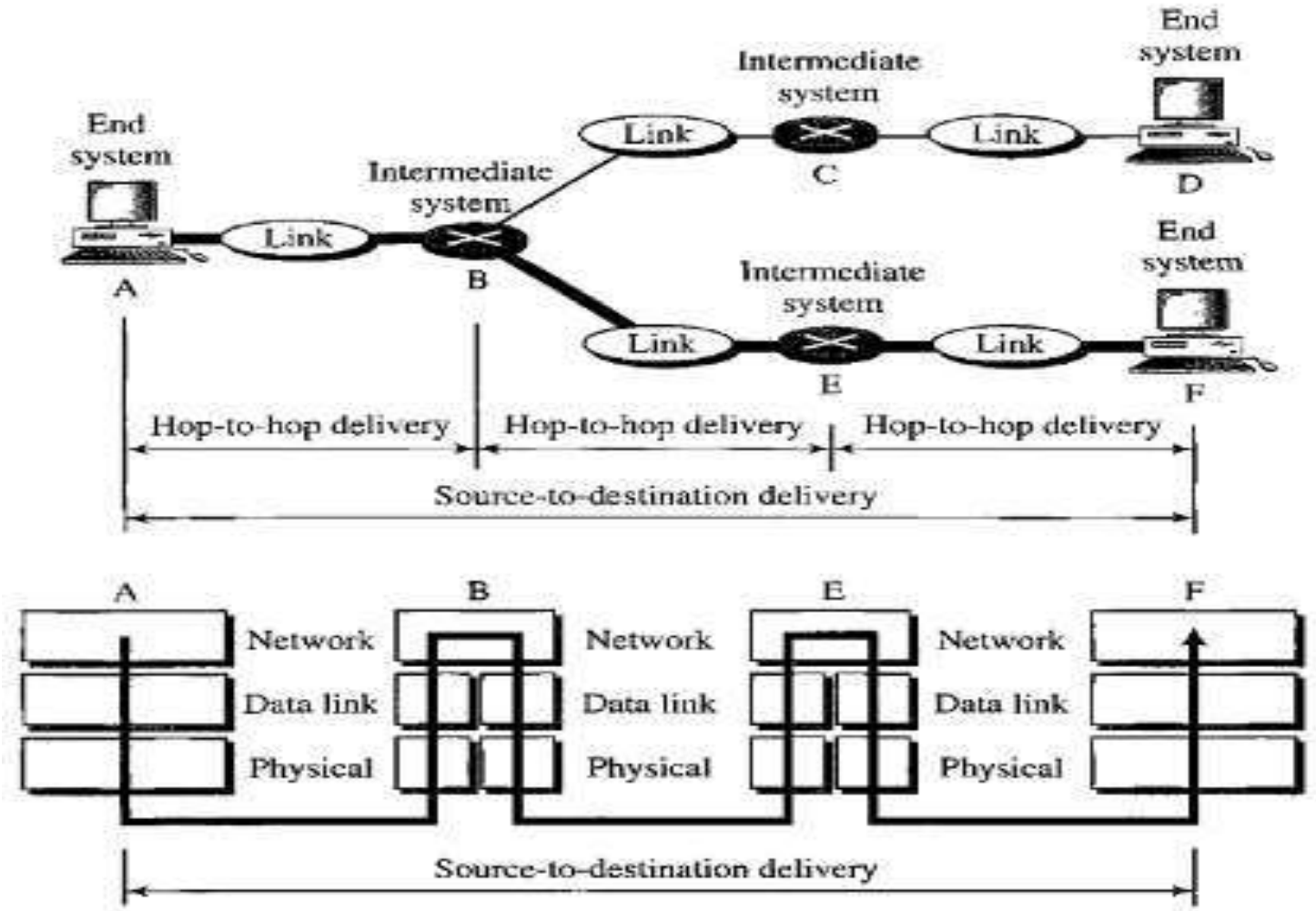
- **Responsible for source to destination delivery of a packet**
- **Logical addressing – Physical addressing implemented by Data link layer handles addressing problem locally. Network layer adds the addresses of sender and receiver.**
- **Routing**
  - Transfers a **data packet from source to final destination through nodes** in the network.
  - Every router checks the final destination address for routing

Network Layer



Source to Destination delivery

Source-to-destination delivery



y 2021

Functions of Network layer

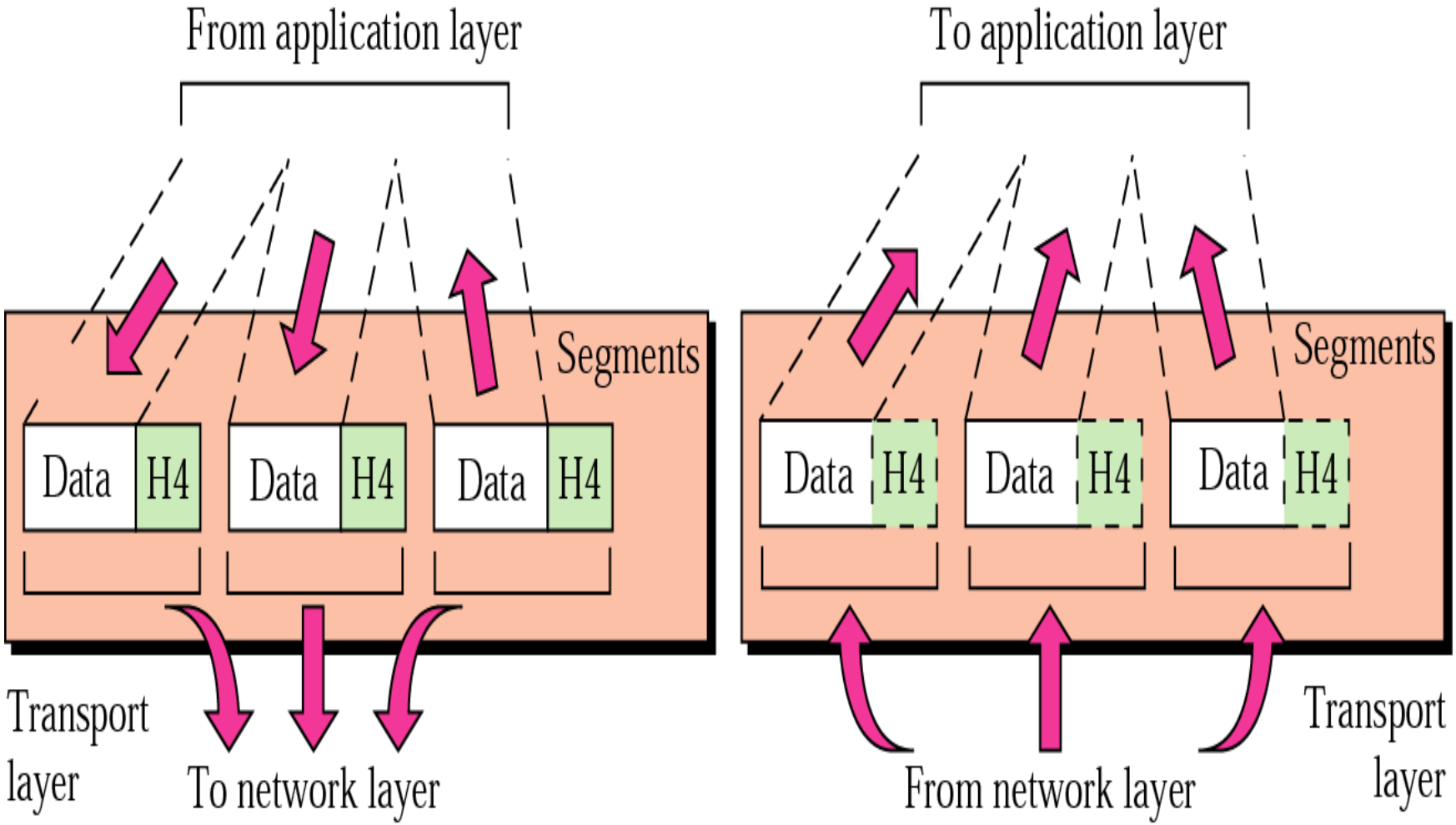
1. Routing of signals
2. Divide outgoing message in to packets
3. Act as network controller
4. Logical Addressing

209

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

Functions of Transport layer

Transport Layer



Functions of Transport layer

1. Maintain process to process delivery
2. Service point addressing
3. Segmentation and re assembly –Message is divided into transmittable segments with each segment containing a sequence number
4. Connection control

Connection oriented Service

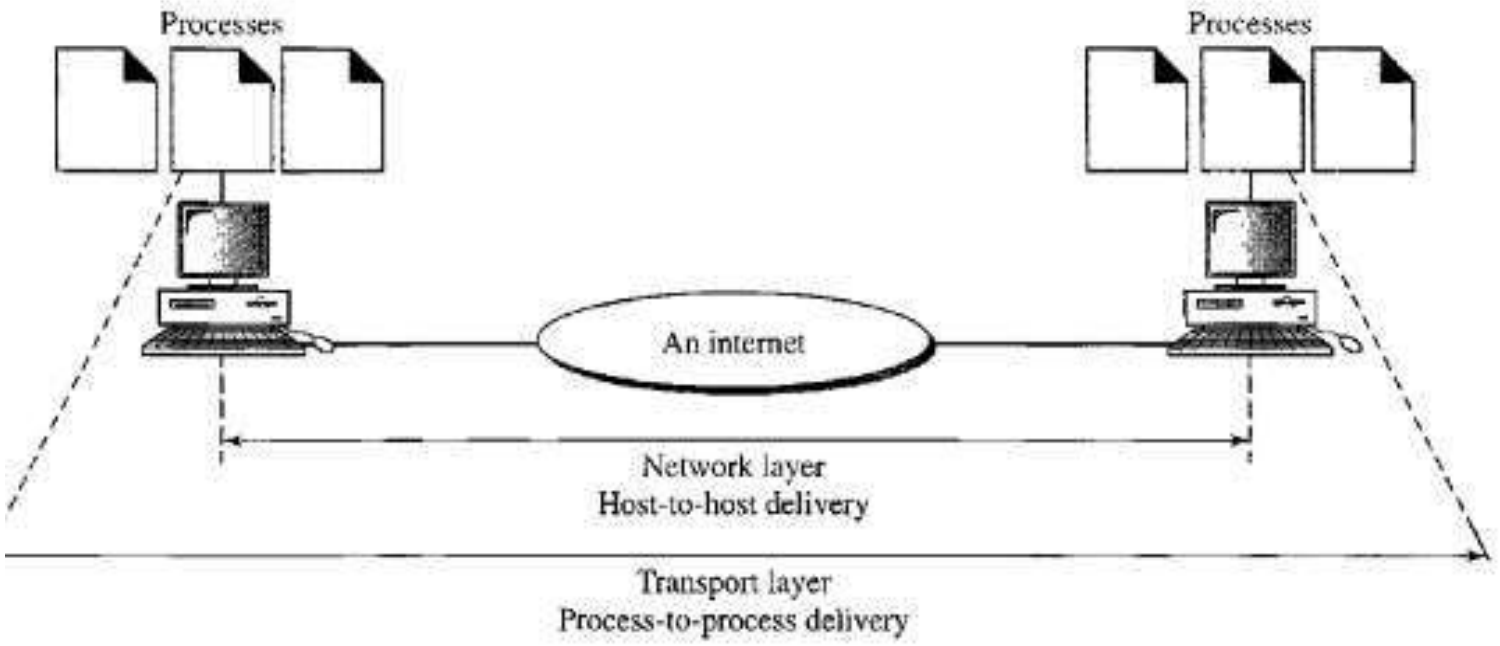
- Establish connection
- Use the connection
- Release the connection

- Connection less Service
  - Packet switching
  - Each message is routed independently

215

Functions of Transport layer

5. **Flow control – End to end rather than across a single link**
6. **Error control- End to end , Ensures that the entire message arrives at the receiving transport layer without error (damage, loss or duplication)**



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

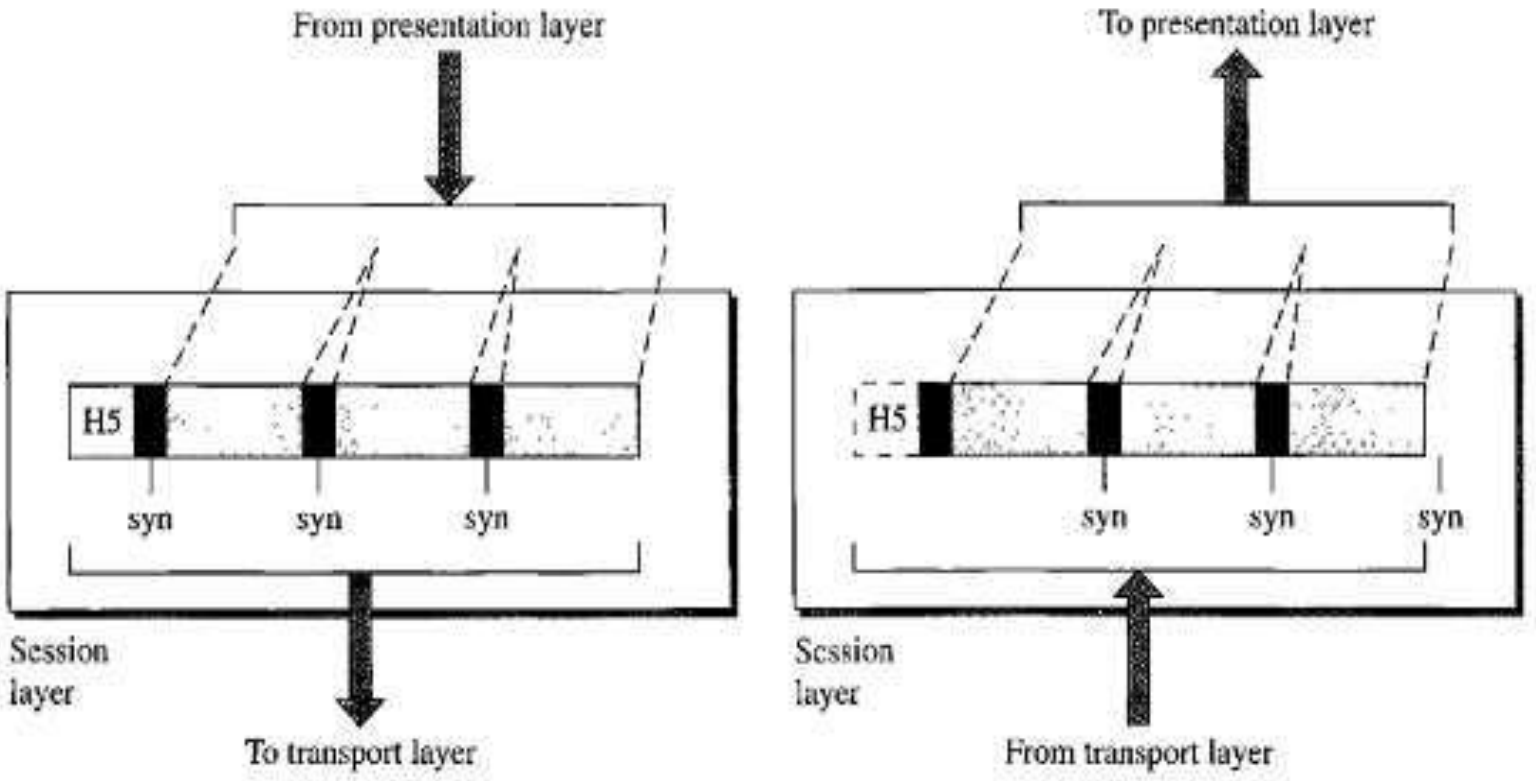
Functions of Session layer

OSI Model – Session Layer

Dialog control. The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.

Synchronization. The session layer allows a process to add checkpoints, or **synchronization points,** to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently.

Functions of Session layer



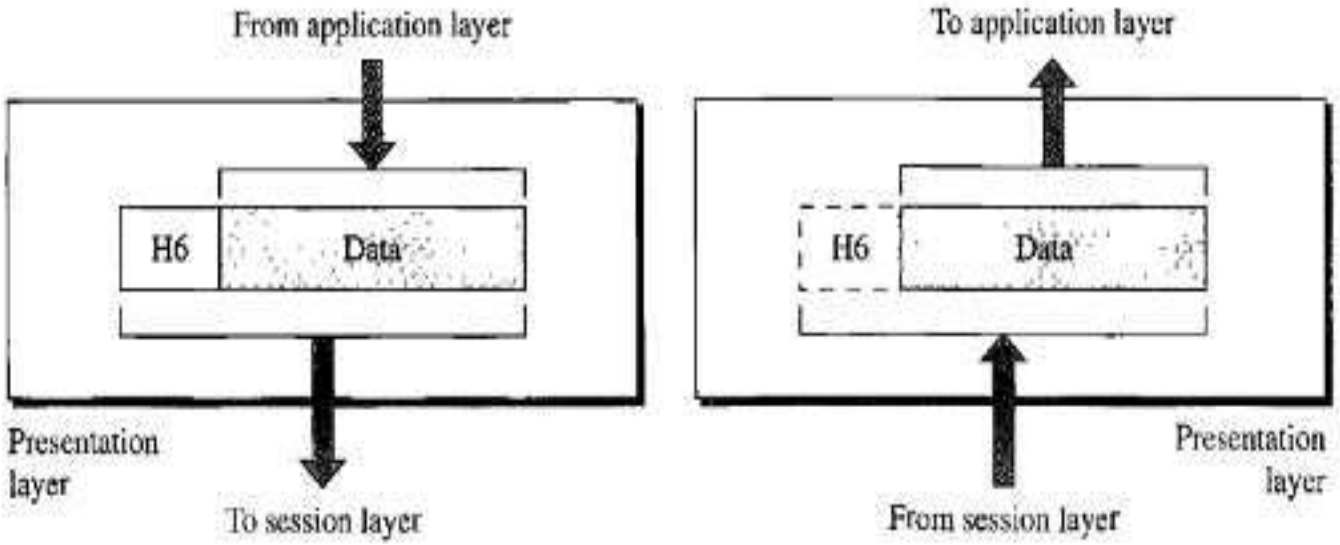
The session layer is responsible for dialog control and synchronization.

Functions of Presentation layer

OSI Model – Presentation Layer

1. **Translation – Data encoding scheme of every system is different. Presentation layer changes sender dependent format to common format. PL at receiver side changes common format to receiver dependent format**
2. **Data compression – Important in transmission of multimedia messages like text, audio and video.**
3. **Encryption – Privacy**

OSI Model – Presentation Layer



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

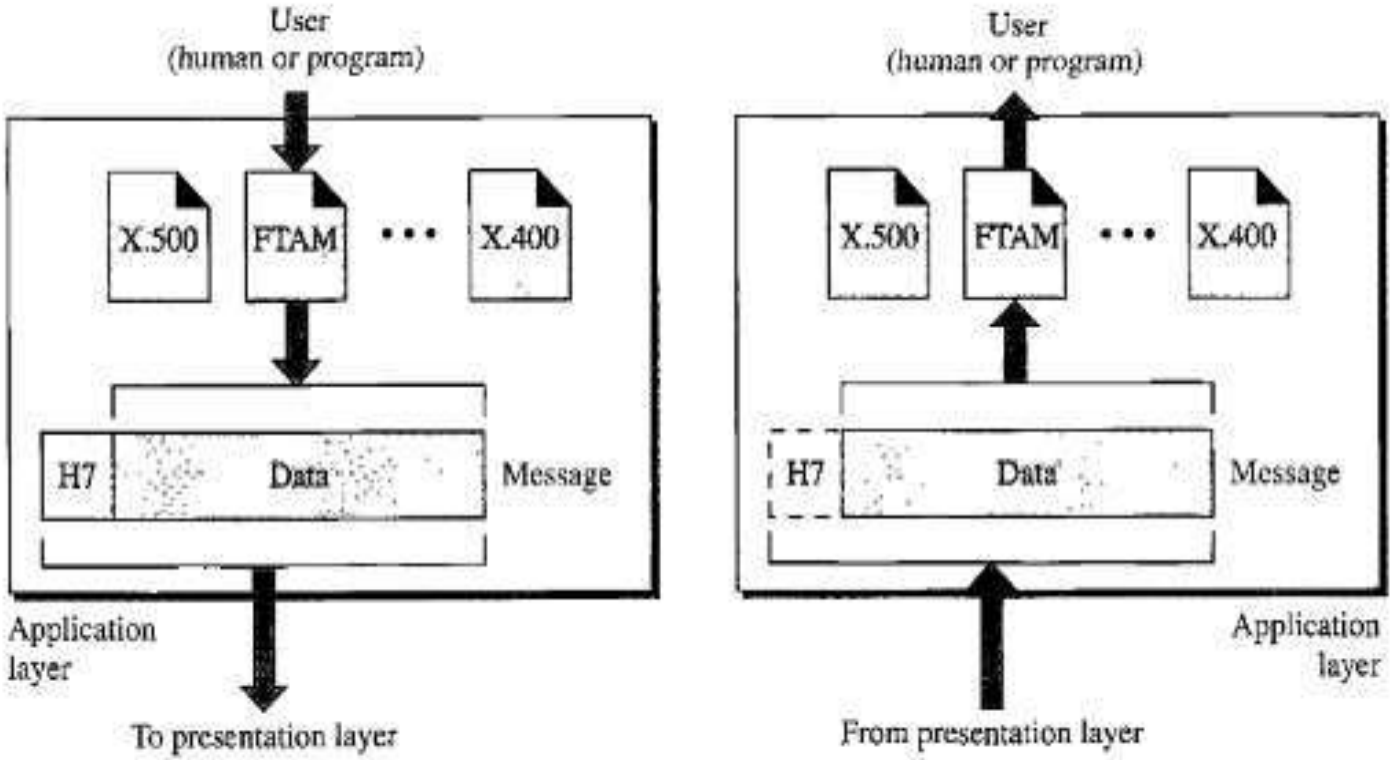
The presentation layer is responsible for translation, compression, and encryption.

Functions of Application layer

OSI Model – Application Layer

- **Application**
  - **Layer where the application using the network resides.**
  - Common network applications include
- **Remote login**
- **File transfer, Acecess and management**
- **e-mail**
- **Directory services**
- **Web page browsing etc.**
  - Means for applications to access OSI environment

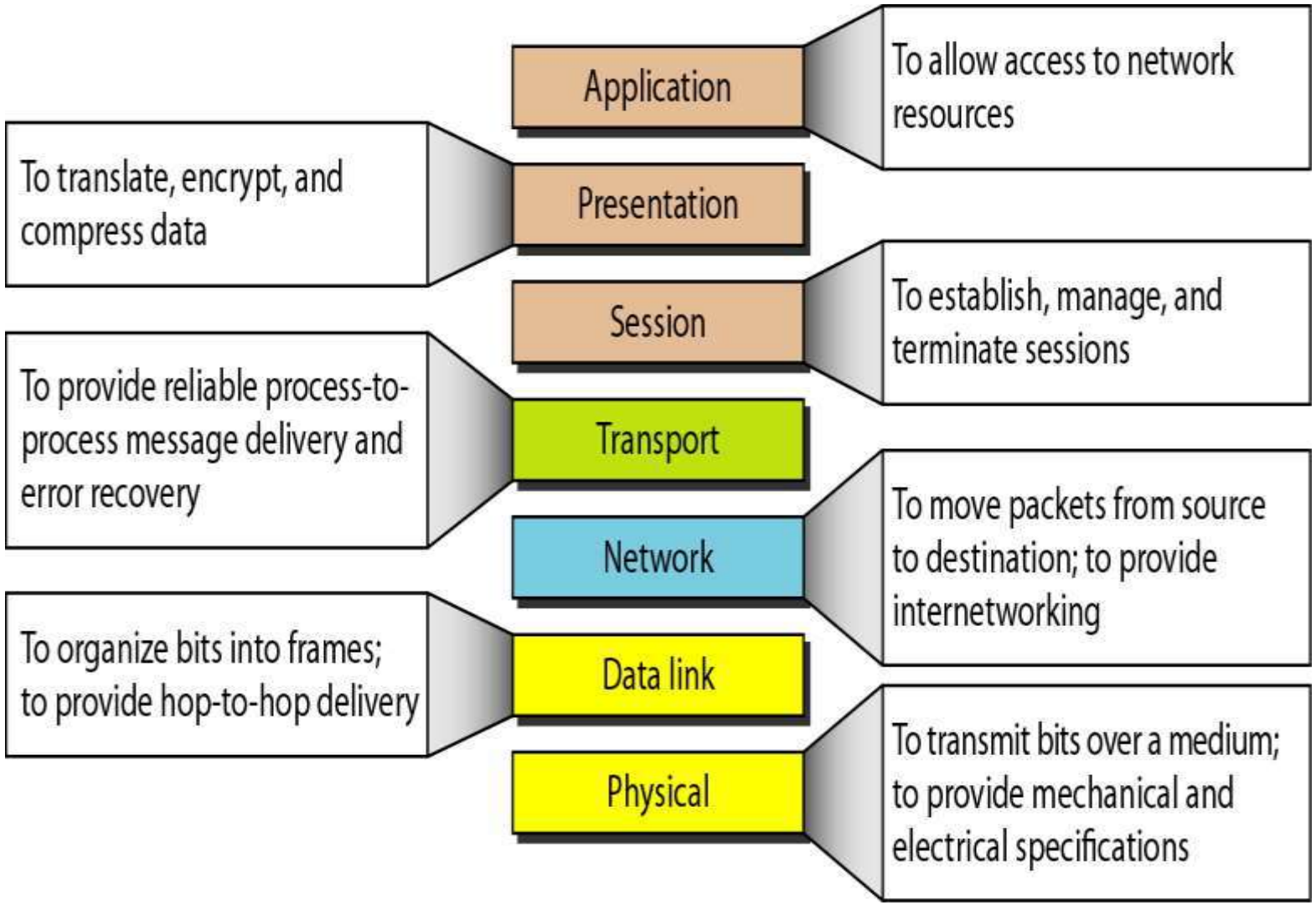
OSI Model – Application Layer

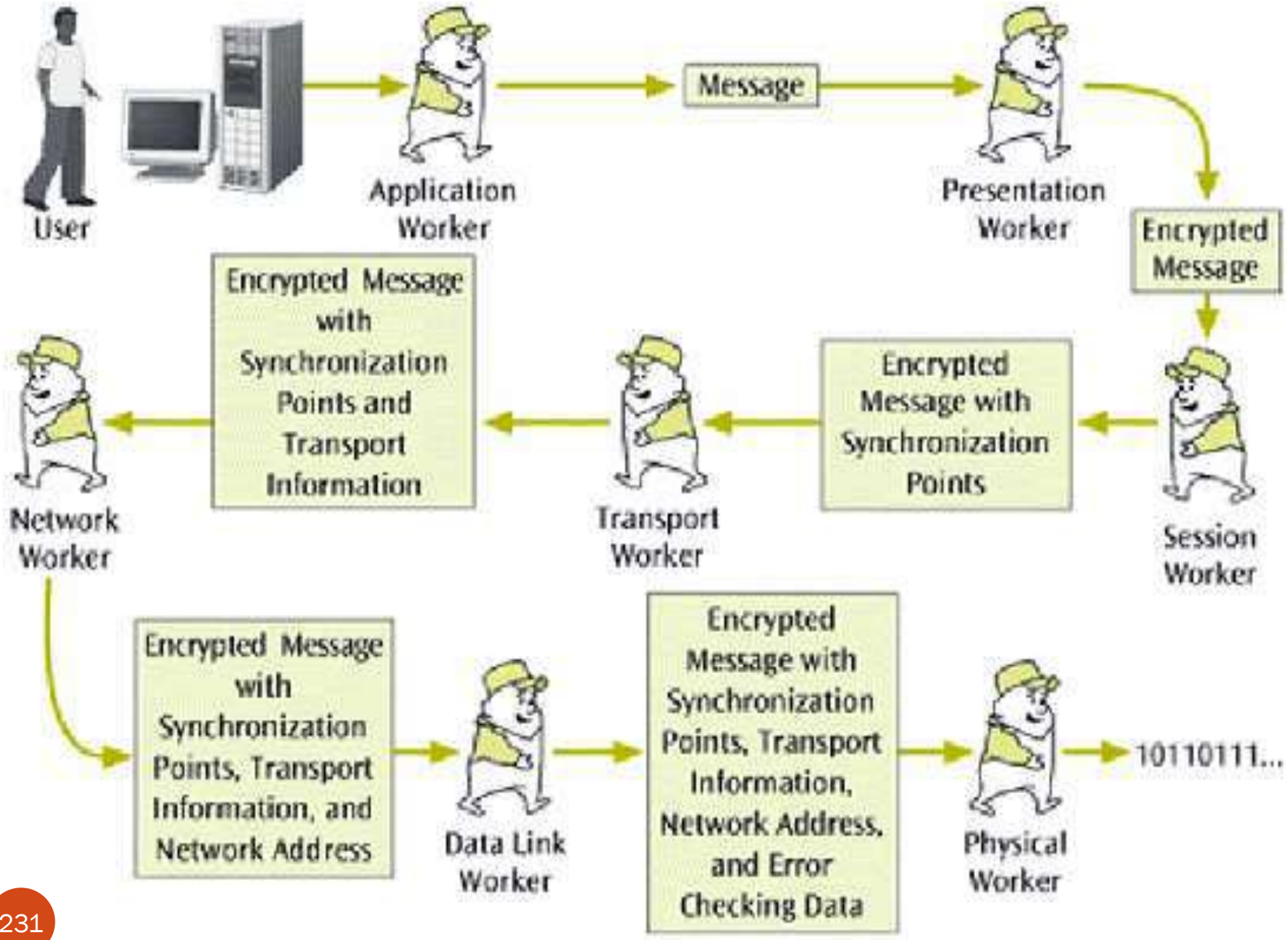


The application layer is responsible for providing services to the user.

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

Summary of layers



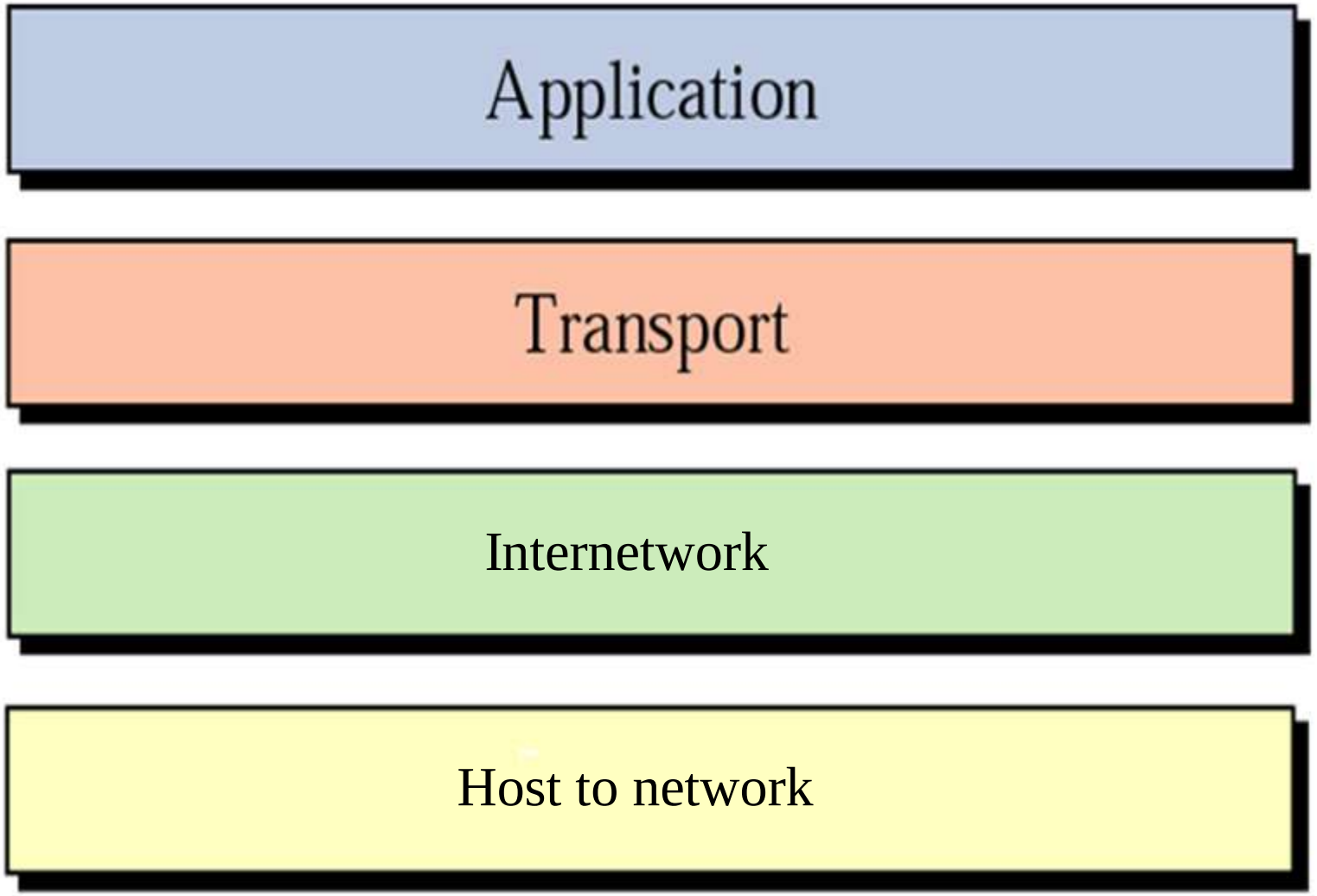

User
Application Worker
Message
Presentation Worker
Encrypted Message
Session Worker
Encrypted Message with Synchronization Points
Transport Worker
Encrypted Message with Synchronization Points and Transport Information
Network Worker
Encrypted Message with Synchronization Points, Transport Information, and Network Address
Data Link Worker
Encrypted Message with Synchronization Points, Transport Information, Network Address, and Error Checking Data
Physical Worker
10110111...

TCP/IP Model

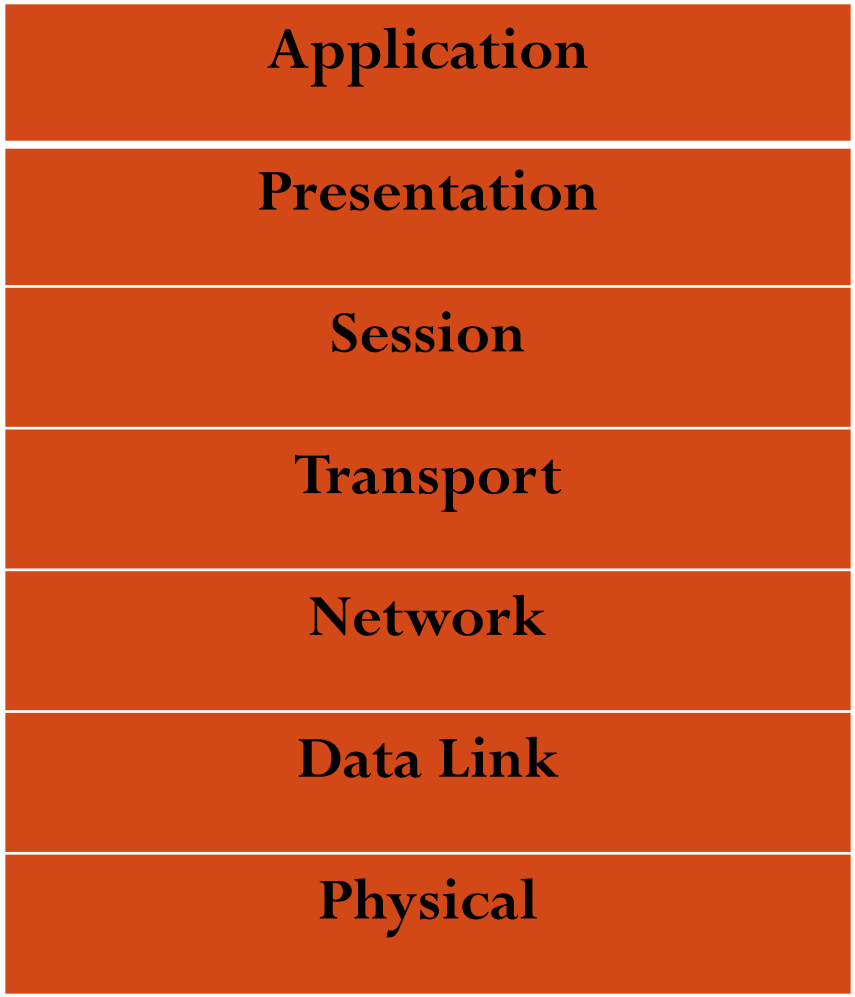
TCP/IP Protocol Suit

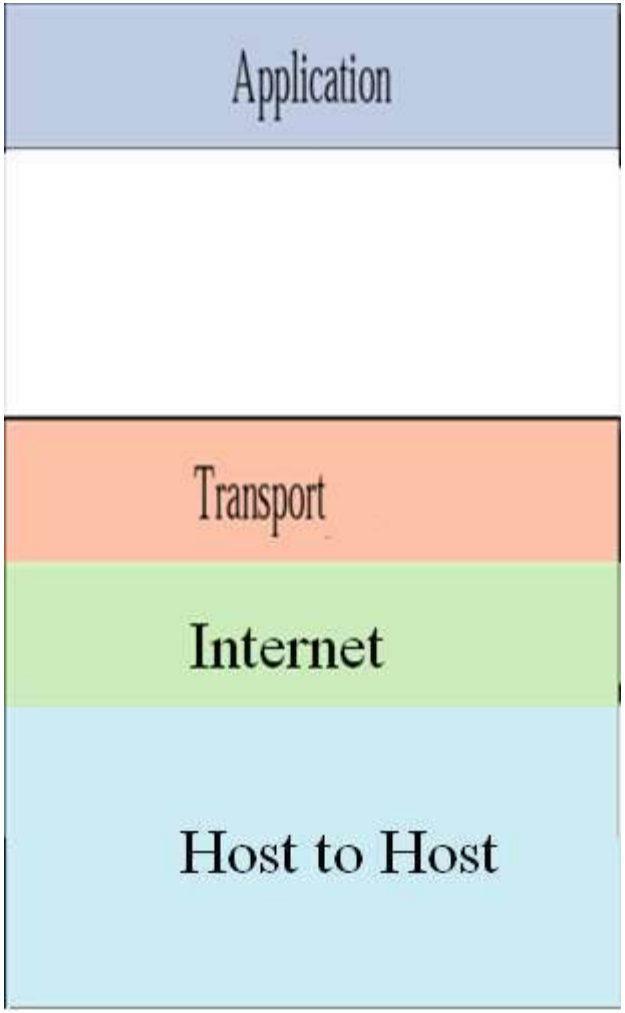
- TCP/IP suite is the **set of protocols** that implement the protocol stack on which the **Internet runs.**
- It is sometimes called the **Internet Model.**
- This model consists of **five ordered layers**
- This model was **developed prior to OSI model**

TCP/IP Model



Variation of TCP/IP

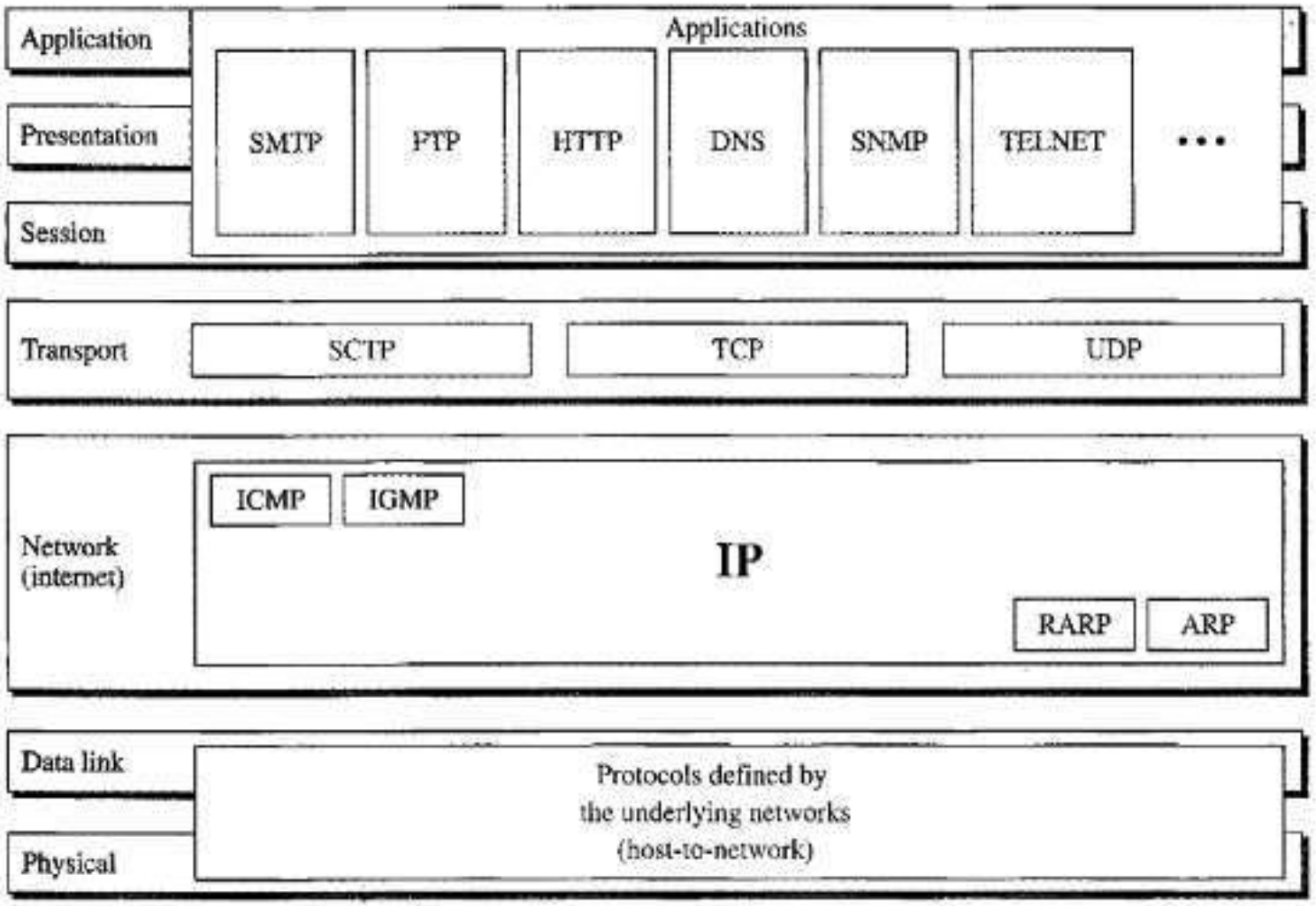




OSI vs TCP/IP

OSI	TCP/IP
7 Layer	4/5 layer
Transport layer guarantees delivery of packets	Transport layer does not guarantees delivery of packets
Separate session layer	No session Layer, Characteristics are provided by application layer
Separate presentation layer	No presentation Layer, Characteristics are provided by application layer
Network layer offer connectionless and connection oriented service	Network layer offer connectionless service
Easy to replace the protocols	Not easy to replace protocols
General Model	TCP/IP cannot be used for any other application

Some Protocols in TCP/IP Suite



Network Layer Protocols

- Internetworking protocol (IP) and four supporting protocol
- Supporting protocols are ARP, RARP, ICMP and IGMP

IP

- IP is a transmission mechanism used by TCP/IP protocols
- It is an unreliable and connectionless protocol
- IP provides no error checking or tracking
- IP transports data in packets called datagram, each of which is transported separately
- IP does not keep track of the routes and has no facility for reordering datagram once they arrive at the destination

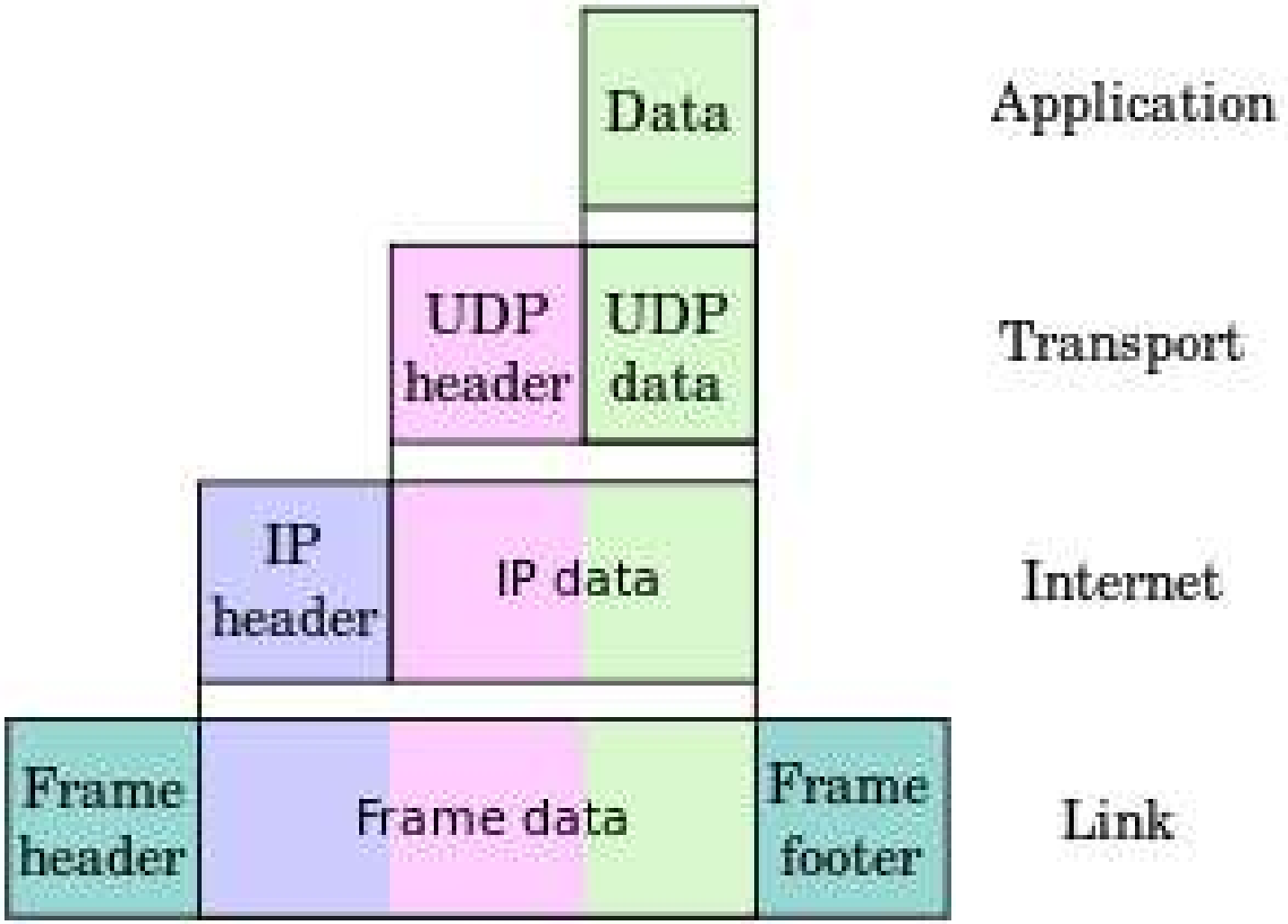
Supporting Protocols

- ARP (Address Resolution Protocols):- Used to find physical address of the node when its internet address is known
- RARP (Reverse Address Resolution Protocols):-Used to find internet address when physical address is known
- ICMP (Internet Control Message Protocol):-Mechanism used by hosts and gateways to send notification of datagram problems back to the sender. Query and error reporting messages
- IGMP (Internet Group Message Protocol):- Used to facilitate simultaneous transmission of messages to a group of recipients

Transport Layer

- UDP (User Datagram Protocol):- Process to process protocol that adds only port address, checksum error control and length information to the data from upper layer. Enables connectionless transfer of message.
- TCP (Transmission Control Protocol):-Connection oriented service. At the sending end, TCP divides stream of data into smaller segments. Each segments includes a sequence number for reordering, together with acknowledgement number for the segments received
- SCTP (Stream Control Transmission Protocol):-Provides support for newer applications such voice over the internet. Combines the best features of UDP and TCP

TCP/IP Frames



TCP/IP Services

- Two kinds of services: TCP & UDP.
-
- **TCP—Transmission Control Protocol, reliable connection oriented transfer of a byte stream.**
- **UDP—User Datagram Protocol, best-effort connectionless transfer of individual messages.**

COMPUTER COMMUNICATION
EC 407

Syllabus

COURSE CODE	COURSE NAME	L-T-P-C	YEAR OF INTRODUCTION
EC407	COMPUTER COMMUNICATION	3-0-0-3	2016

Prerequisite: NIL

Course objectives:

- To give the basic concepts of computer network and working of layers, protocols and interfaces in a computer network.
- To introduce the fundamental techniques used in implementing secure network communications and give them an understanding of common threats and its defences.

Module	Course content (42 hrs)	Hours	End Sem. Exam Marks
I	Introduction to computer communication: Transmission modes - serial and parallel transmission, asynchronous, synchronous, simplex, half duplex, full duplex communication. Switching: circuit switching and packet switching	2	15%

Syllabus

	Networks: Network criteria, physical structures, network models, categories of networks, Interconnection of Networks: Internetwork	2	
	Network models: Layered tasks, OSI model, Layers in OSI model, TCP/IP protocol suite.	2	
II	Physical Layer: Guided and unguided transmission media (Co-axial cable, UTP,STP, Fiber optic cable)	2	15%
	Data Link Layer: Framing, Flow control (stop and wait , sliding window flow control)	2	
	Error control, Error detection(check sum, CRC), Bit stuffing, HDLC	2	
	Media access control: Ethernet (802.3), CSMA/CD, Logical link control, Wireless LAN (802.11), CSMA/CA	2	
FIRST INTERNAL EXAM			

Syllabus

III	Network Layer Logical addressing : IPv4 & IPV6	2	15%
	Address Resolution protocols (ARP, RARP)	2	
	Subnetting, Classless Routing(CIDR), ICMP, IGMP, DHCP	3	
	Virtual LAN, Networking devices (Hubs, Bridges & Switches)	1	
IV	Routing: Routing and Forwarding, Static routing and Dynamic routing	1	15%
	Routing Algorithms: Distance vector routing algorithm, Link state routing (Dijkstra's algorithm)	2	
	Routing Protocols: Routing Information protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), MPLS	3	
SECOND INTERNAL EXAM			
V	Transport Layer –UDP, TCP	1	20%
	Congestion Control & Quality of Service – Data traffic, Congestion, Congestion Control, QoS and Flow Characteristics	4	
	Application Layer – DNS, Remote Logging (Telnet), SMTP, FTP, WWW, HTTP, POP3, MIME, SNMP	3	

Syllabus

VI	Introduction to information system security, common attacks	1	20%
	Security at Application Layer (E-MAIL, PGP and S/MIME). Security at Transport Layer (SSL and TLS). Security at Network Layer (IPSec).	3	
	Defence and counter measures: Firewalls and their types. DMZ, Limitations of firewalls, Intrusion Detection Systems -Host based, Network based, and Hybrid IDSs	2	
END SEMESTER EXAM			

Question Paper Pattern

The question paper shall consist of three parts. Part A covers modules I and II, Part B covers modules III and IV, and Part C covers modules V and VI. Each part has three questions uniformly covering the two modules and each question can have maximum four subdivisions. In each part, any two questions are to be answered. Mark patterns are as per the syllabus with 90% for theory and 10% for logical/numerical problems, derivation and proof.

References

Text Books:

1. Behrouz A. Forouzan, Cryptography & Network Security , , IV Edition, Tata McGraw-Hill, 2008
2. J F Kurose and K W Ross, Computer Network A Top-down Approach Featuring the Internet, 3/e, Pearson Education, 2010

References:

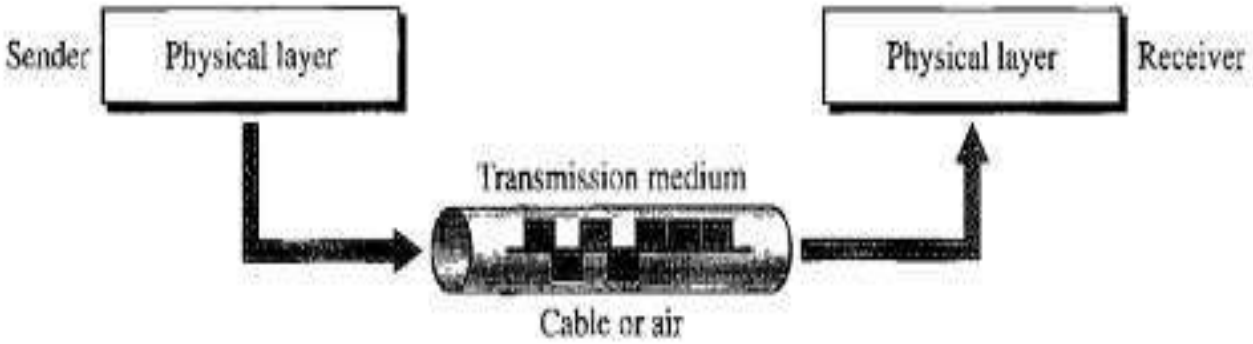
1. Behrouz A Forouzan, Data Communications and Networking, 4/e, Tata McGraw-Hill, 2006.
2. Larry Peterson and Bruce S Davie: Computer Network- A System Approach, 4/e, Elsevier India, 2011.
3. S. Keshav, An Engineering Approach to Computer Networking, Pearson Education, 2005.
4. Achyut S.Godbole, Data Communication and Networking, 2e, McGraw Hill Education New Delhi, 2011

UNIT 2

Transmission Medium

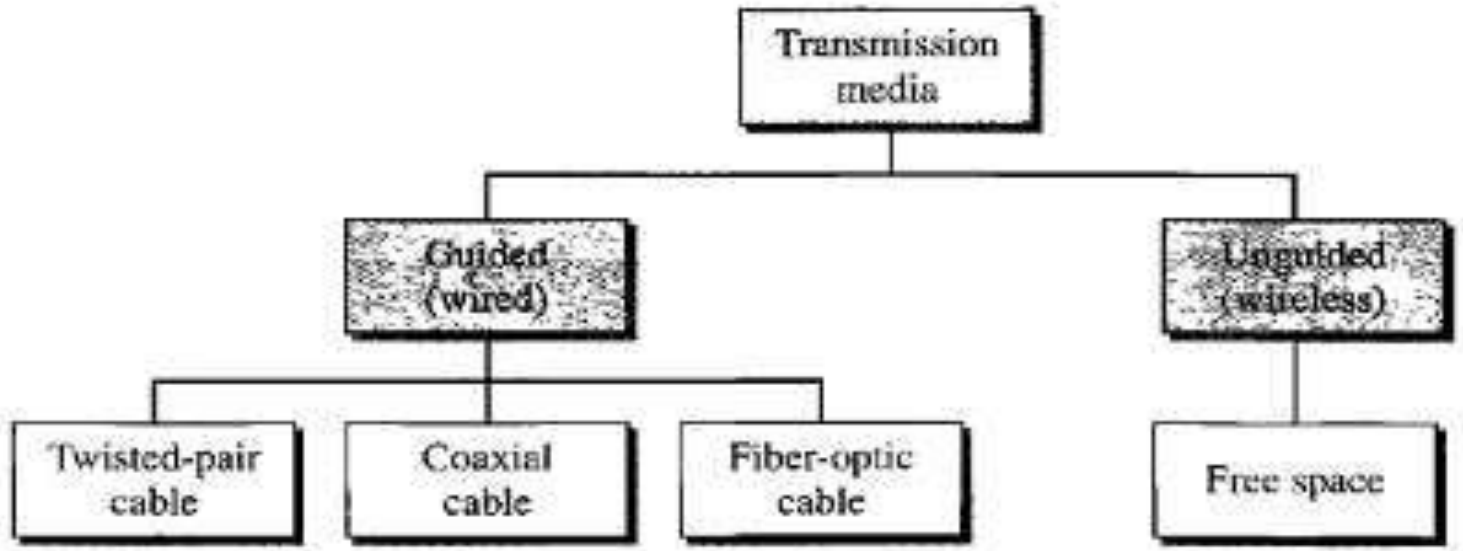
- A transmission medium can be broadly defined as anything that can carry information from a source to destination
- A transmission medium is usually free space, metallic cable or fiber optic cable

Figure 7.1 *Transmission medium and physical layer*



Transmission Medium

Classes of transmission media

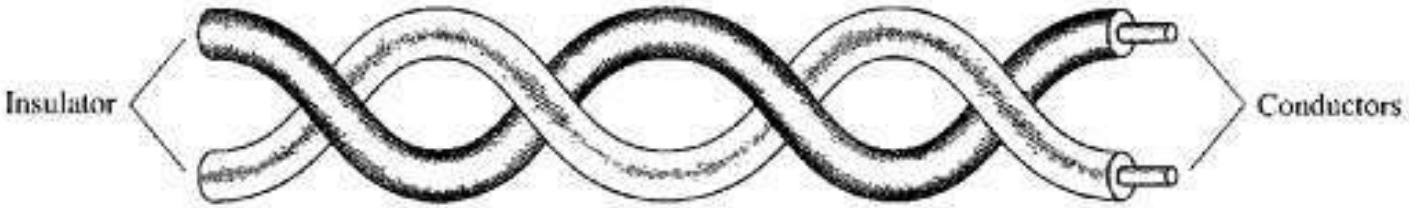


Guided Medium

- Twisted pair cable, coaxial cable and fiber optic cable
- Twisted pair and coaxial cable uses metallic conductors that accepts and transport signals in the form of electric current
- Optical fiber accepts and transports signals in the form of light

Twisted-Pair cable

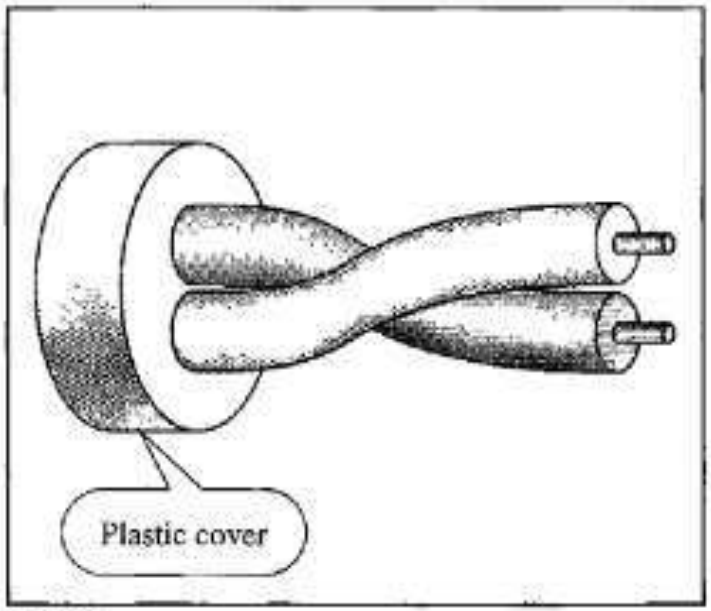
A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in Figure



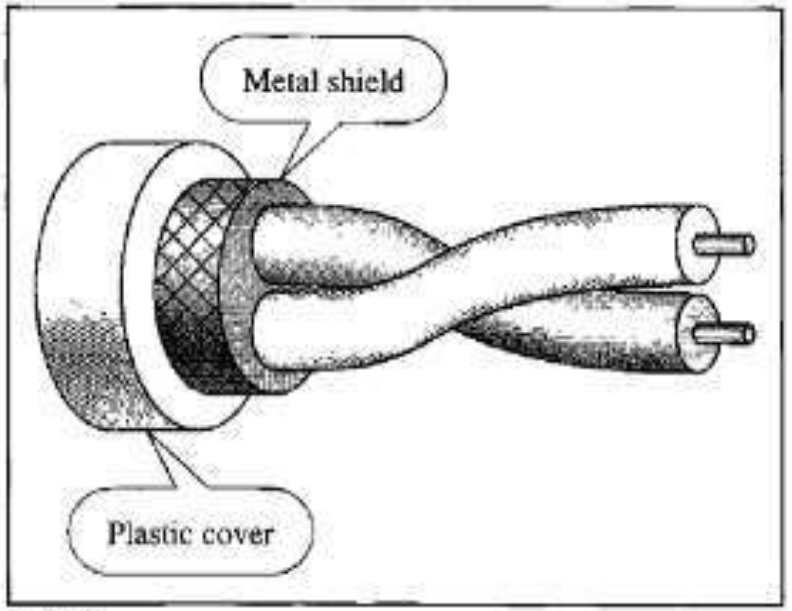
One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.

In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

Unshielded and Shielded Twisted-Pair UTP and STP



a. UTP



b. STP

Unshielded Twisted-Pair Categories

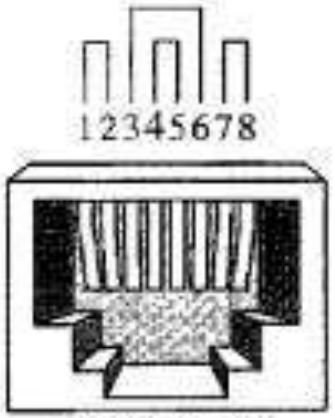
The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses.

Unshielded Twisted-Pair Categories

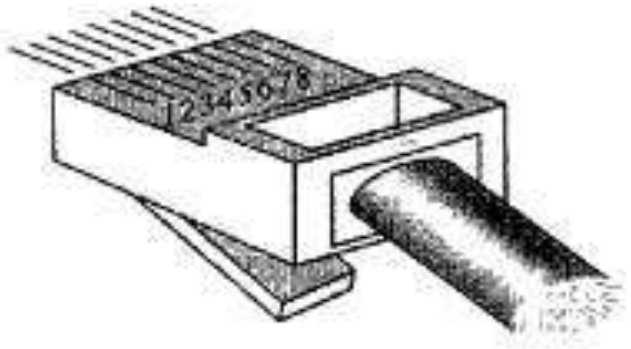
Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

UTP connectors

- Most common UTP connector is RJ45
- RJ stands for registered jack
- RJ45 is a keyed connector, meaning connector can inserted in only one way

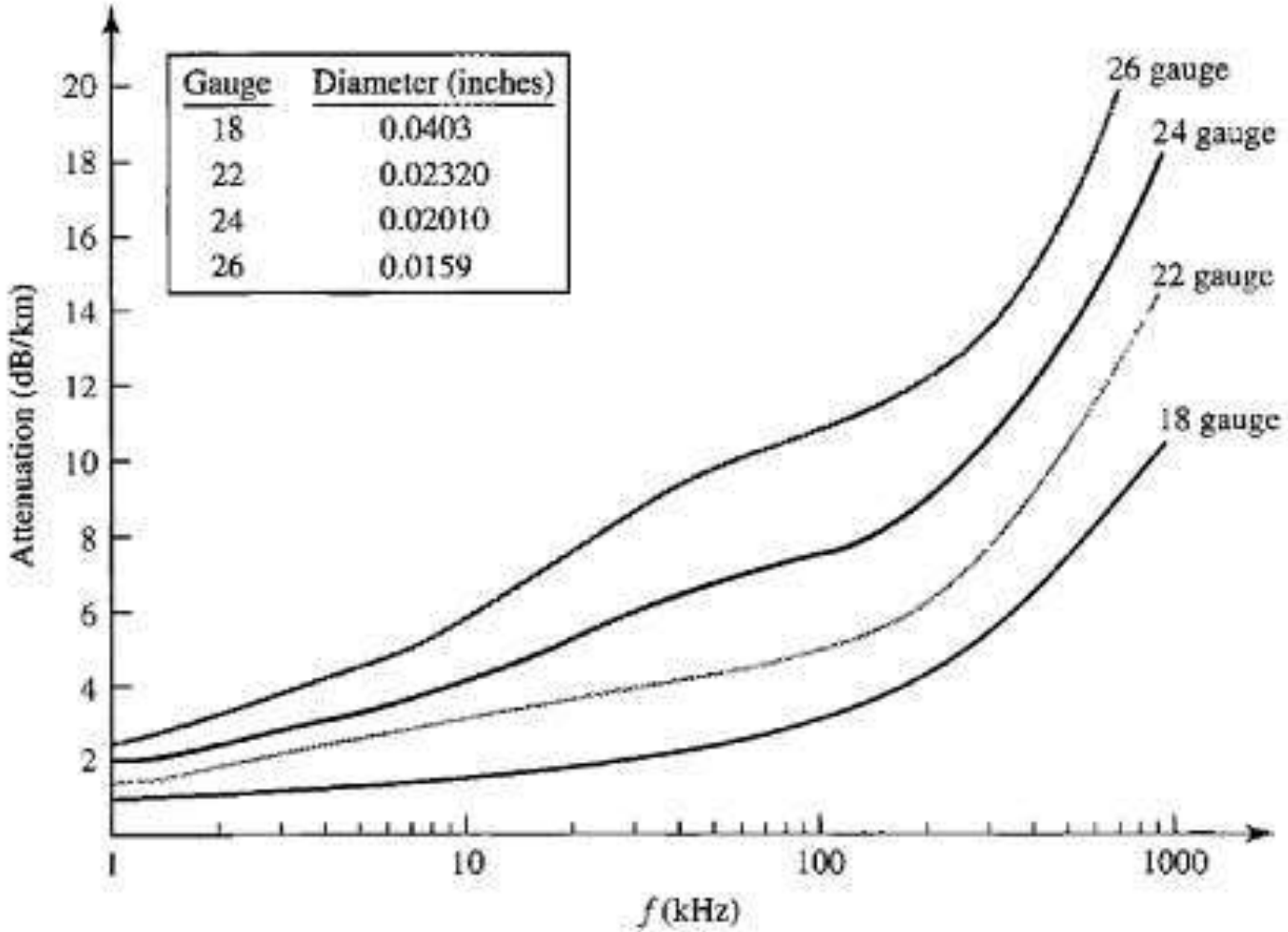


RJ-45 Female



RJ-45 Male

UTP Performances



Applications of Twisted-Pair Cable

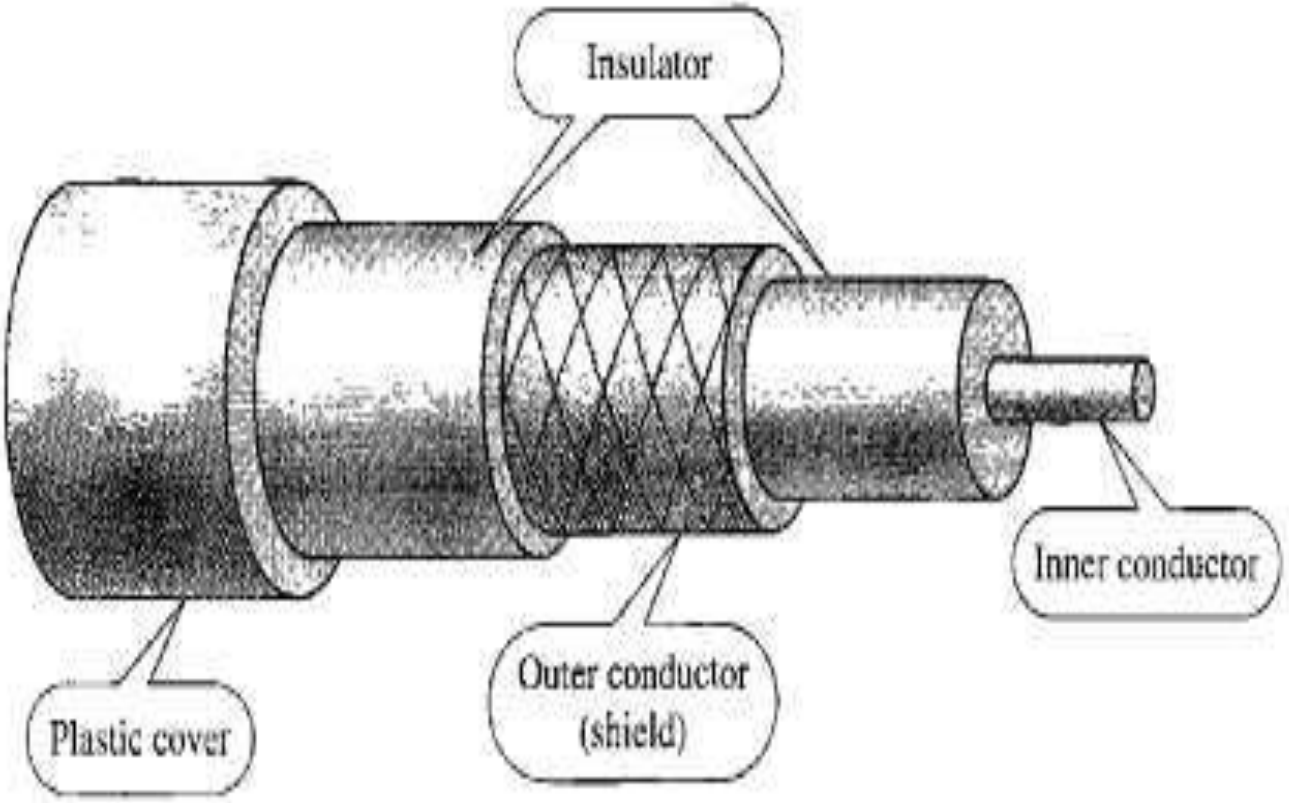
- **Used in telephone lines to provide voice and data channels**

The line that connects subscribers to central telephone office commonly consists of UTP

- **Some LANS are also using the TPC**

Coaxial Cable

- **Consists of inner conductor (copper) and Outer conductor (metal foil, braid or a combination of the two)**



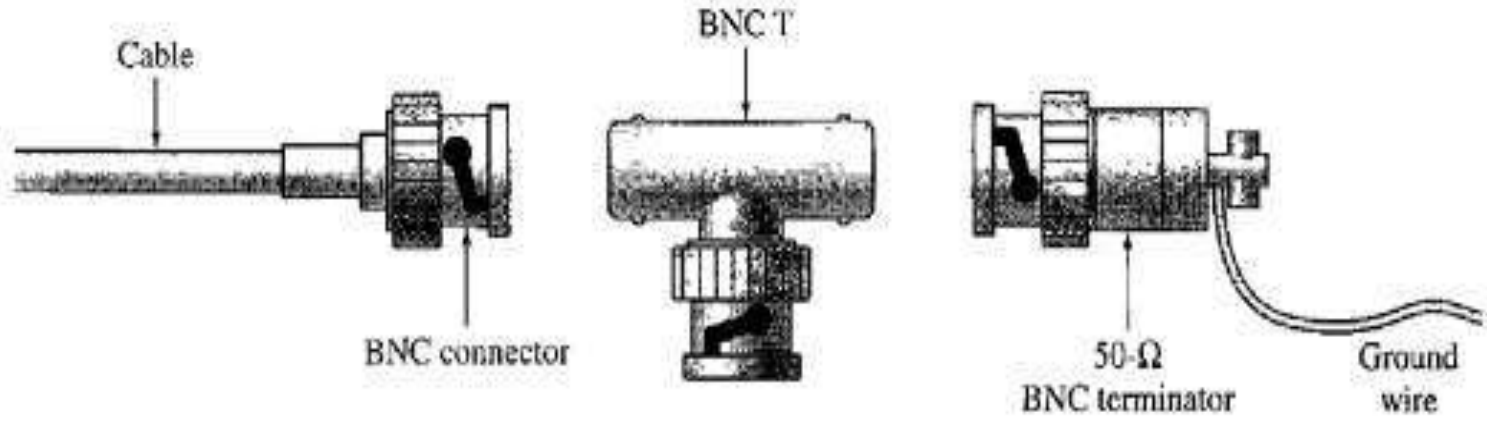
Coaxial Cable Standards

- **RG (Radio Government) number (RG ratings) denotes a unique set of physical specification including**
  - **Wire gauge of the inner conductor**
  - **Thickness and type of inner insulator**
  - **Construction of the shield**
  - **Size and type of outer casing**

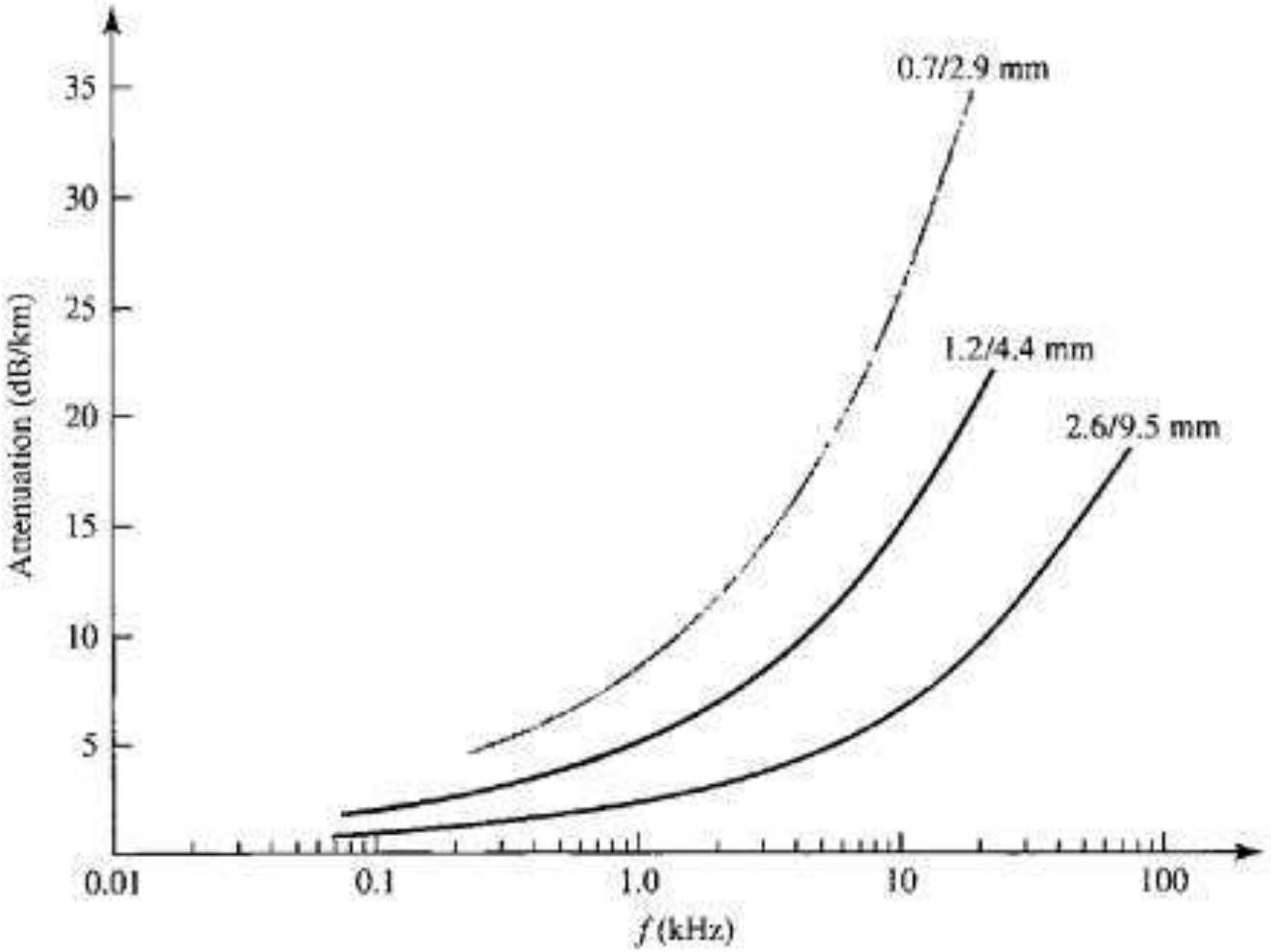
Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Coaxial Cable Connectors

- **Most common type of connector used today is Bayone-Neil-Concelman (BNC) connector**
  - **BNC used to connect end of the cable to a device such as TV set**
  - **BNC T is used for branching**
  - **BNC terminator is used at the end of the cable to prevent reflection of the signal**



Coaxial Cable Performances

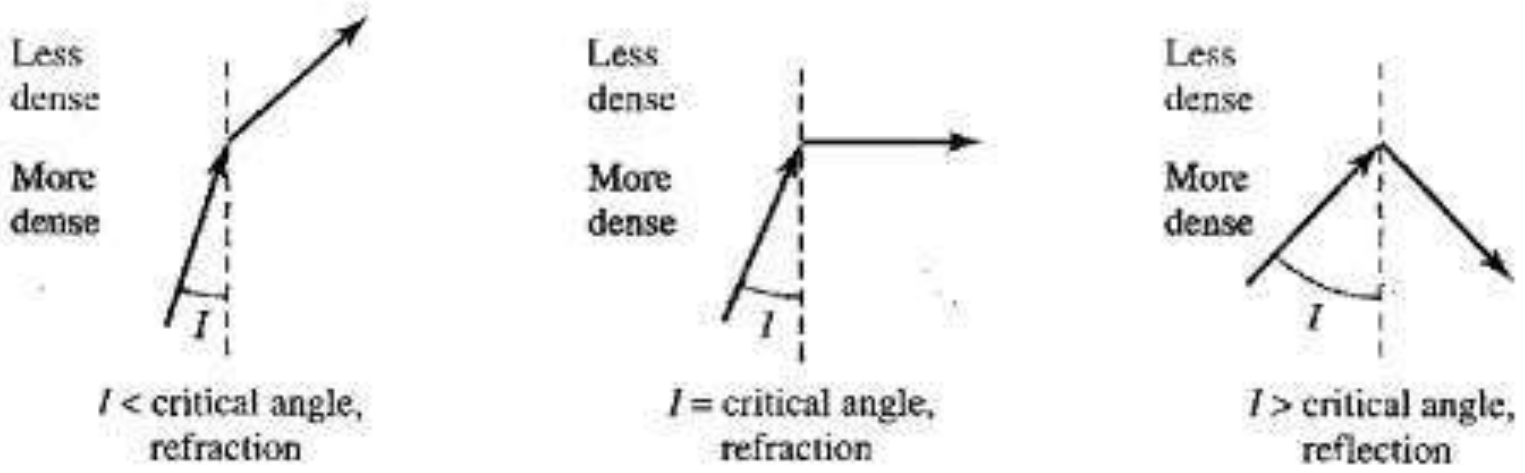


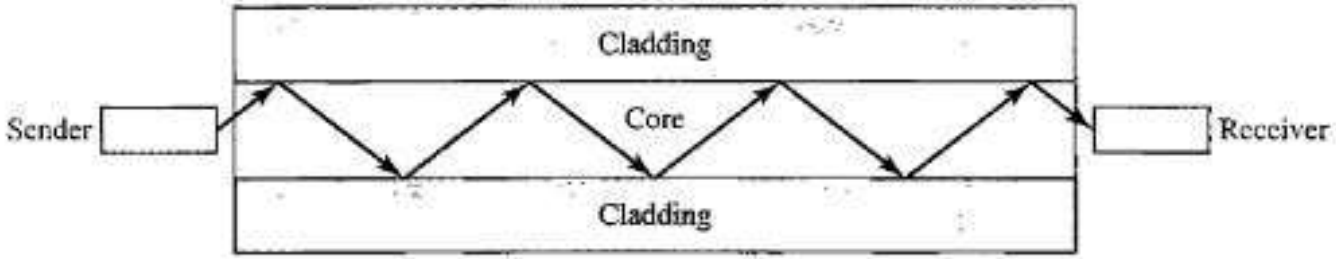
Coaxial Cable Applications

- **Used in analog telephone networks**
- **Cable TV networks**
- **Ethernet LANs**

Fiber-Optic Cable

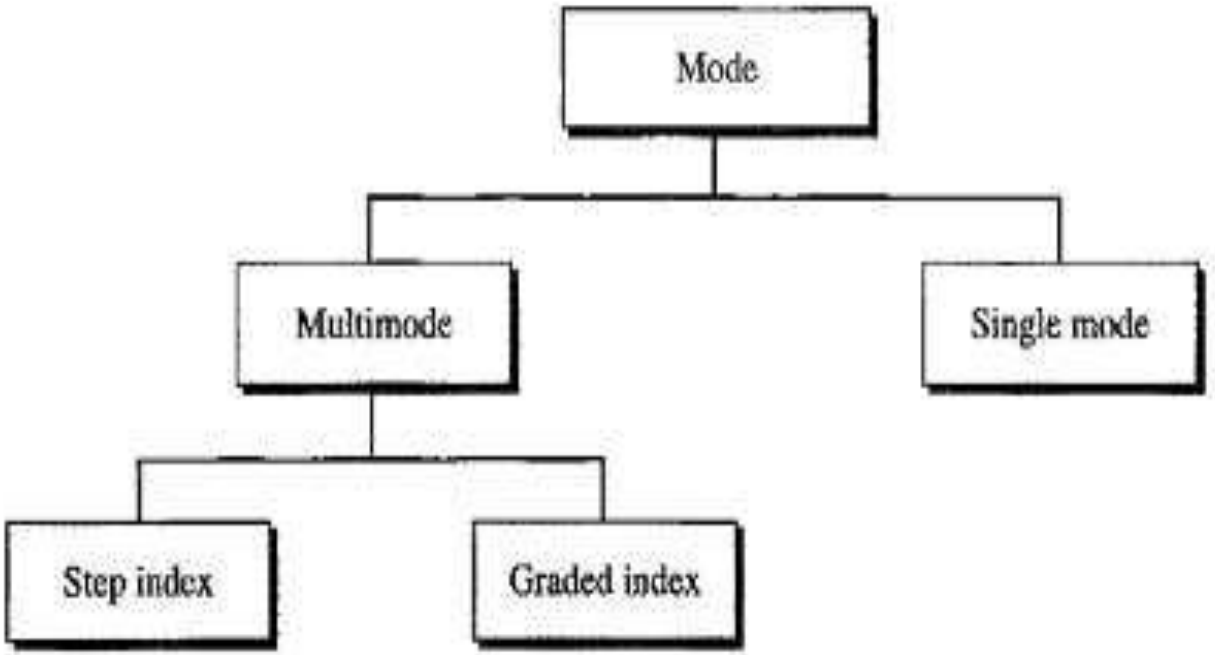
Bending of light ray



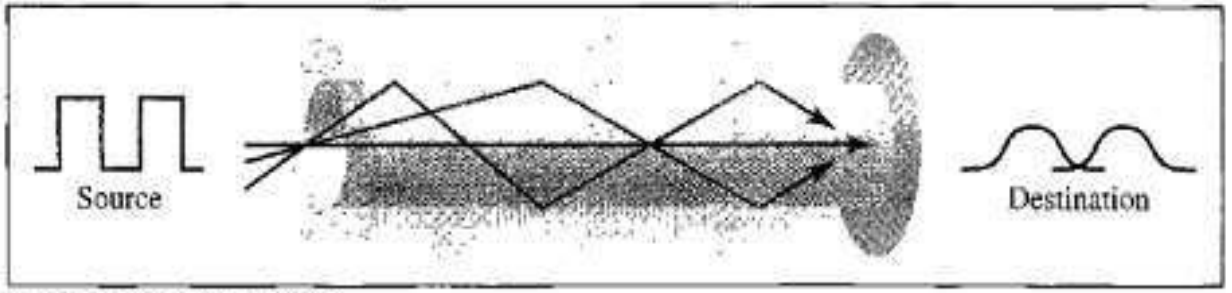


Fiber-Optic Cable-Propagation Modes

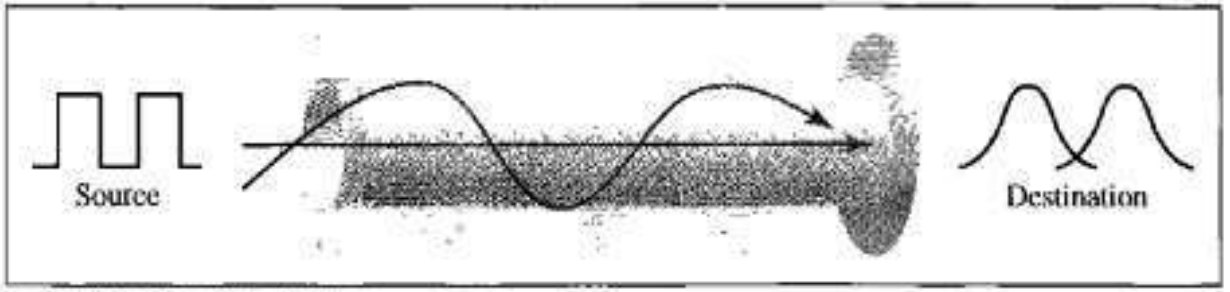
Propagation modes



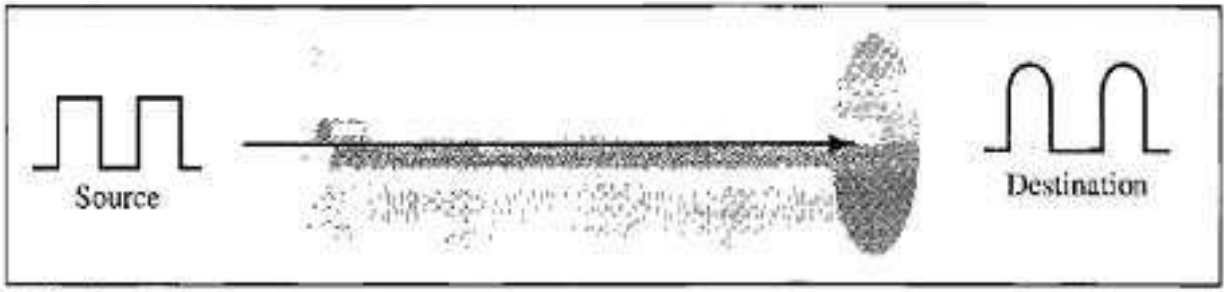
Fiber-Optic Cable-Propagation Modes



a. Multimode, step index



b. Multimode, graded index



c. Single mode

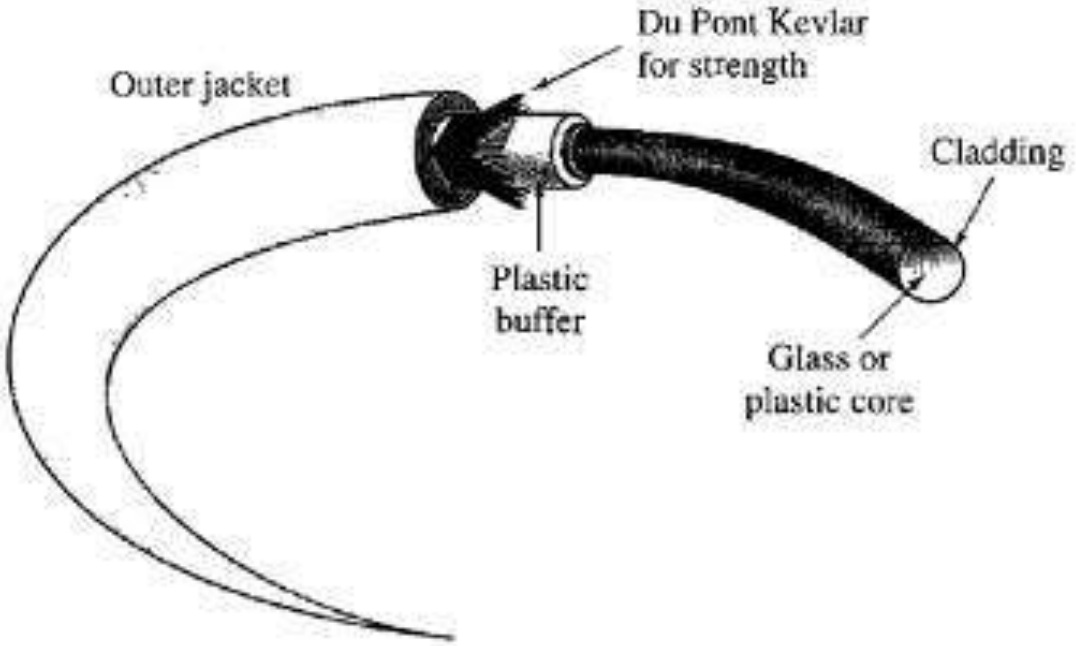
Fiber Types

Type	*Core (μm)*	*Cladding (μm)*	*Mode*
50/125	50.0	125	Multimode, graded index
62.5/125	62.5	125	Multimode, graded index
100/125	100.0	125	Multimode, graded index
7/125	7.0	125	Single mode

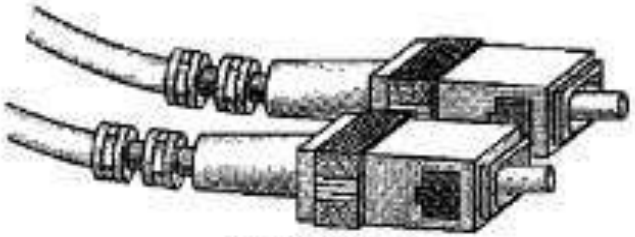
Cable Composition

Outer jacket is made up of PVC or Teflon

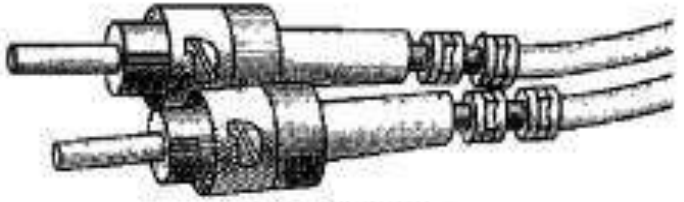
Fiber construction



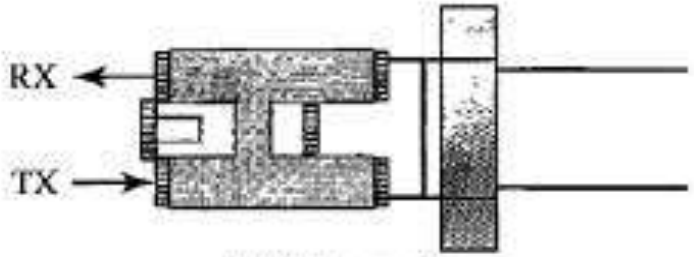
Cable Connectors



SC connector



ST connector

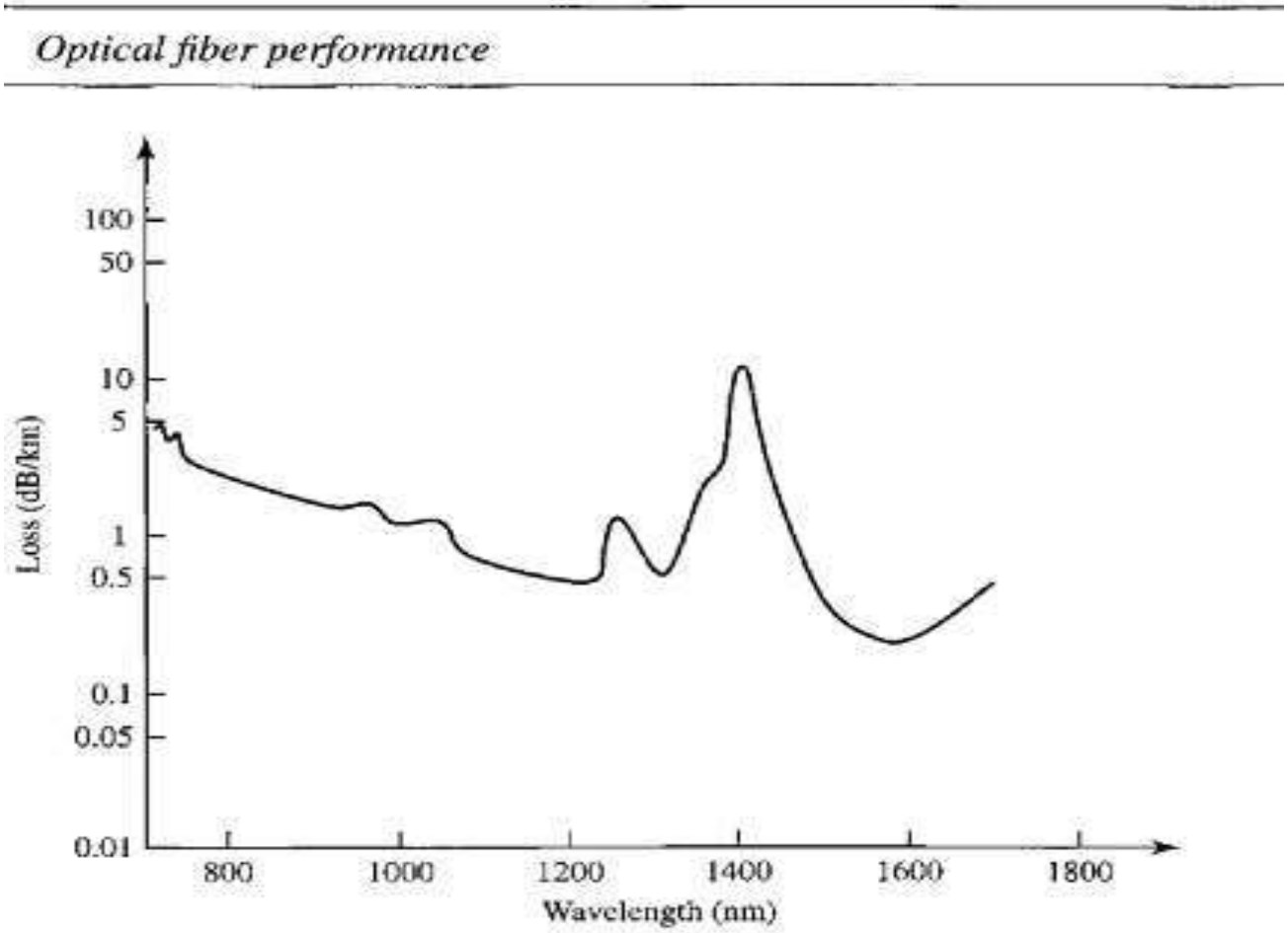


MT-RJ connector

The **subscriber channel (SC) connector** is used for cable TV. It uses a push/pull locking system. The **straight-tip (ST) connector** is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC. **MT-RJ** is a connector that is the same size as RJ45.

Performance

Attenuation is flatter than co-axial and twisted-pair cables



Applications, Advantages and Disadvantages

- **Backbone networks**
- **Cable TV**
- **LANs**

Advantages and Disadvantages of Optical Fiber

Advantages Fiber-optic cable has several advantages over metallic cable (twisted-pair or coaxial).

- **Higher bandwidth.** Fiber-optic cable can support dramatically higher bandwidths (and hence data rates) than either twisted-pair or coaxial cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.
- **Less signal attenuation.** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.
- **Immunity to electromagnetic interference.** Electromagnetic noise cannot affect fiber-optic cables.
- **Resistance to corrosive materials.** Glass is more resistant to corrosive materials than copper.

Applications, Advantages and Disadvantages

- **Light weight.** Fiber-optic cables are much lighter than copper cables.
- **Greater immunity to tapping.** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

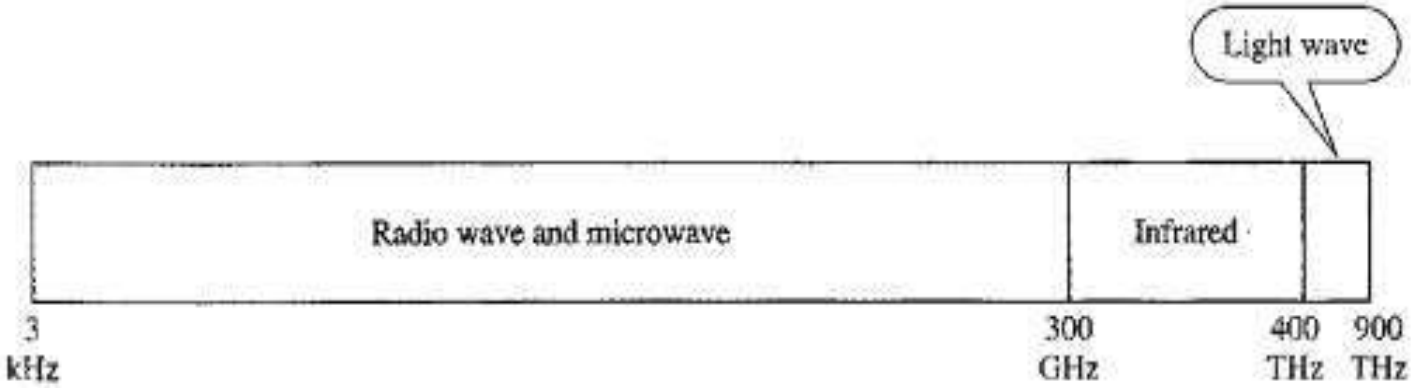
Disadvantages There are some disadvantages in the use of optical fiber.

- **Installation and maintenance.** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- **Unidirectional light propagation.** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- **Cost.** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

Unguided Transmission Media

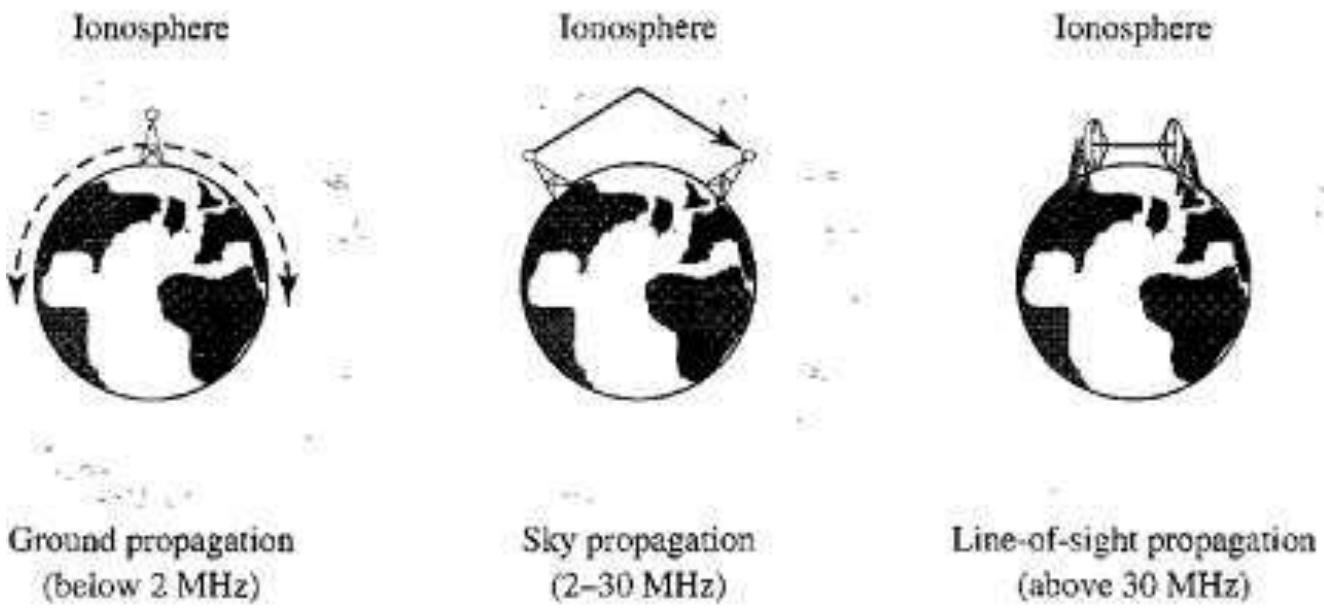
Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as **wireless communication.** Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Electromagnetic spectrum for wireless communication



Unguided Transmission Media

Propagation methods



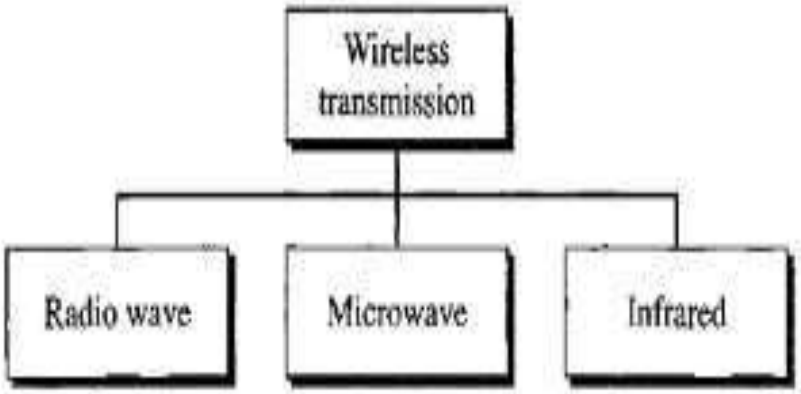
Unguided Transmission Media

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite

Unguided Transmission Media

We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves. See Figure 7.19.

Figure 7.19 *Wireless transmission waves*



Data Link Control(DLC)

- In the OSI networking model, **Data Link Control (DLC)** is the **service provided by the data link layer.**

- **Network interface cards have a DLC address** that identifies each card.
- ***DLC identifier (DLCI)*** that uniquely **identifies the node on the network.**

- For networks that conform to the **IEEE 802 standards** (e.g., Ethernet), the **DLC address is usually called the *Media Access Control (MAC) address*.**

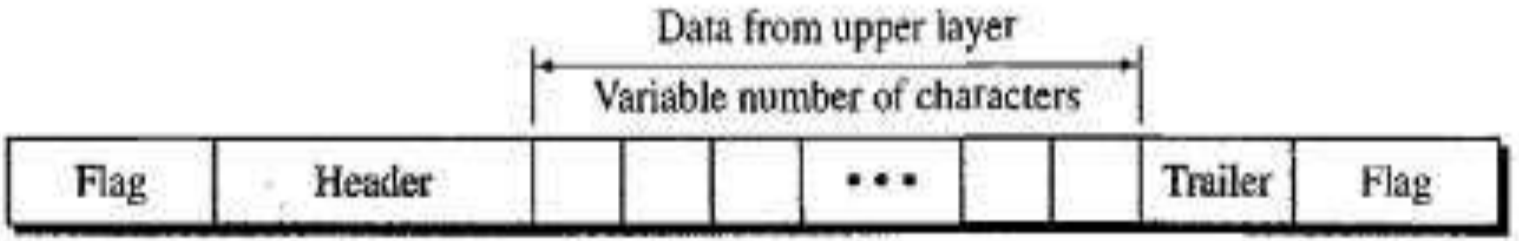
Data Link Layer-Framing

- Framing separates message of one source/destination from another source/destination by adding sender and receiver address.
- Framing can be of two types – fixed size and variable size
- In fixed size framing, there is no need of defining the boundaries of the frame.
- Size of frame itself can be used as delimiter
- In Variable size framing, the end of one frame and beginning of the next.
- For this two approaches- Character oriented approach and bit oriented approach

Character Oriented Protocol

- Uses 8 bit characters from a coding system such as ASCII-known as flag
- Flag is added at the beginning and end of each frame to separate form other frames

A frame in a character-oriented protocol



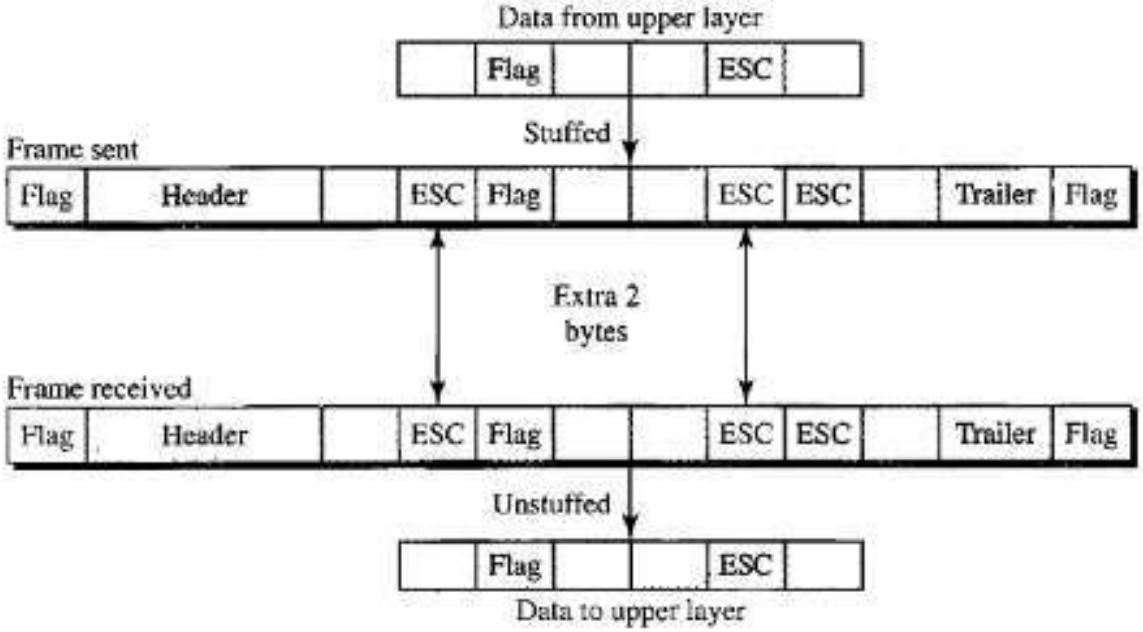
Character Oriented Protocol

- If the data contains same characters as that of flag, it is difficult to separate flag from the data
- There is another approach – Byte stuffing and unstuffing
- The data section is stuffed with an extra byte called escape character (ESC), which has a predefined pattern

What happens if the text contains one or more escape characters followed by a flag?

if the escape character is part of the text, an extra one is added to show that the second one is part of the text.

Character Oriented Protocol

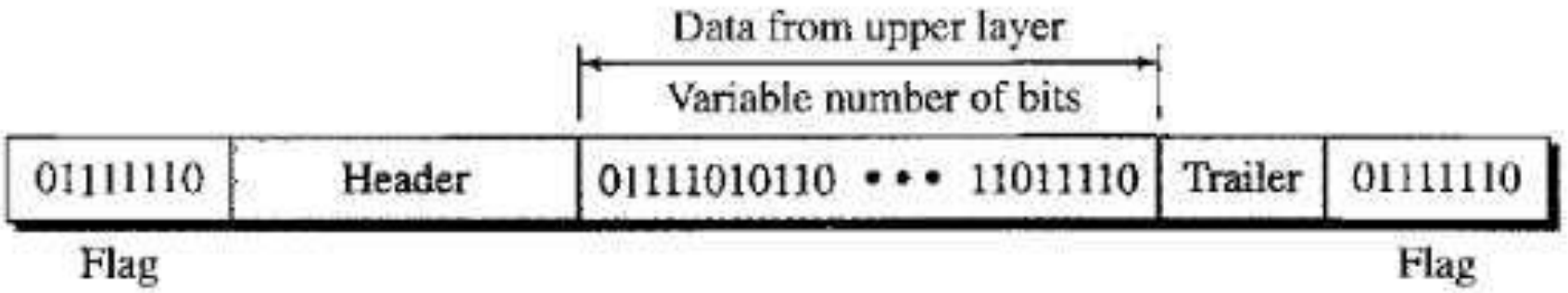


Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

Bit Oriented Protocol

- Most protocols uses a special bit pattern flag 01111110 as the delimiter to define beginning and end of the frame

A frame in a bit-oriented protocol



Bit Oriented Protocol

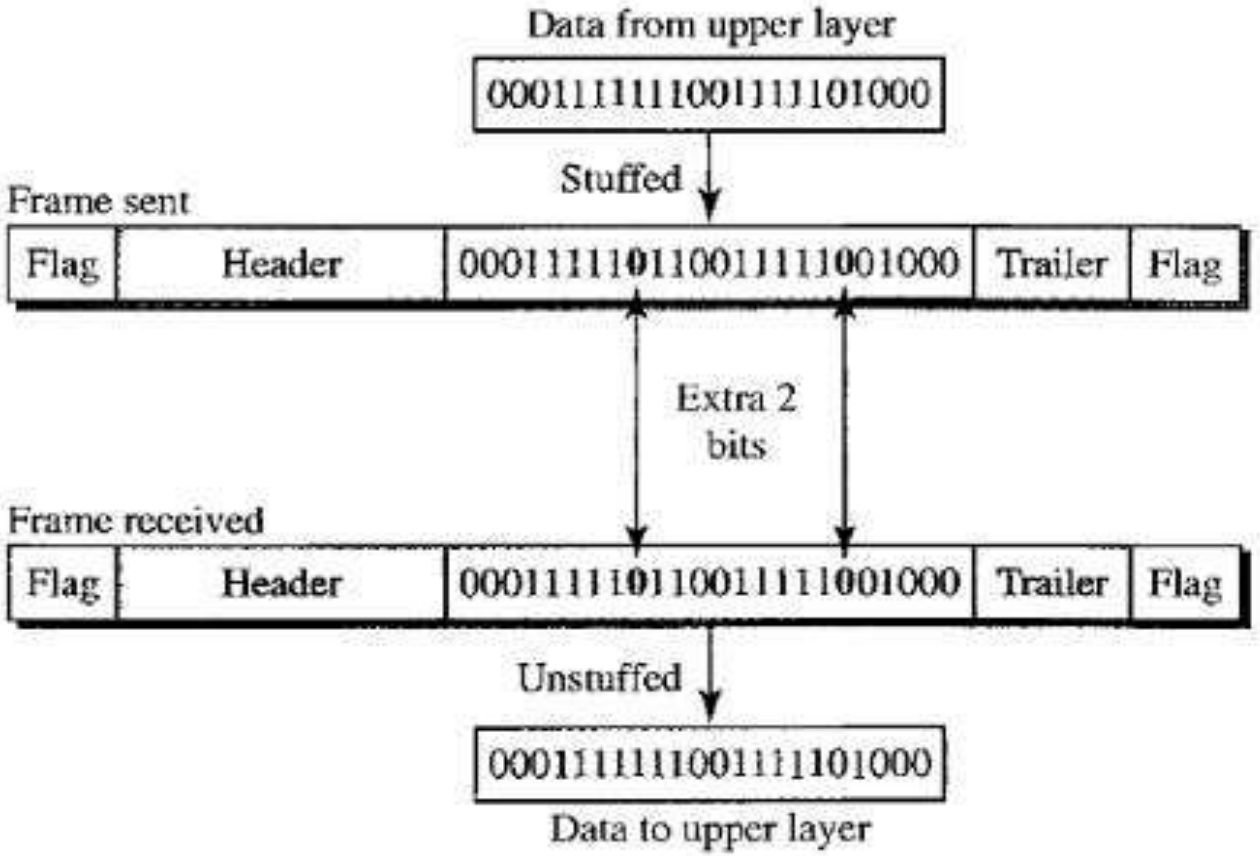
- If the flag pattern appears, bit stuffing is needed to prevent the pattern from looking like a flag.

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

This means that if the flaglike pattern 01111110 appears in the data, it will change to 011111010 (stuffed) and is not mistaken as a flag by the receiver. The real flag 01111110 is not stuffed by the sender and is recognized by the receiver.

Bit Oriented Protocol

Bit stuffing and unstuffing



Flow Control

- **Necessary when data is being sent faster than it can be processed by receiver.**

- If **sender sends faster than recipient processes, then buffer overflow occurs**
  - **Flow control prevents buffer overflow**

- Flow control can be of two types

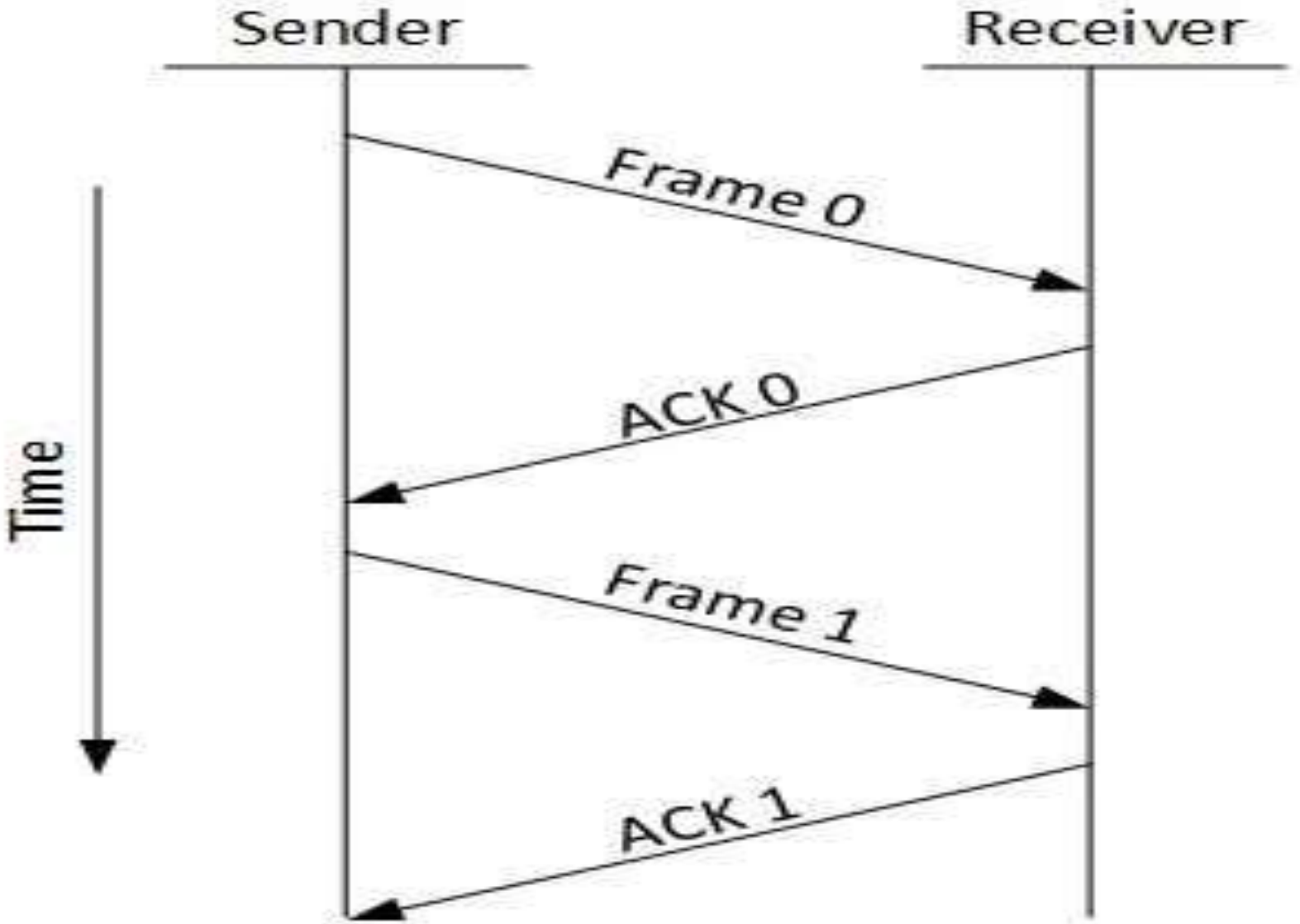
1. **Stop & Wait**
2. **Sliding window**

1. Stop and Wait Flow Control

- This **flow control mechanism forces the sender** after transmitting a data frame to **stop and wait until the acknowledgement of the data-frame sent is received.**

1. Source transmits frame
2. Destination receives frame and replies with acknowledgement (ACK)
3. Source waits for ACK before sending next frame
4. Destination can stop flow by not sending ACK
5. Works well for large frames
6. Inefficient for smaller frames

Stop and Wait Flow Control

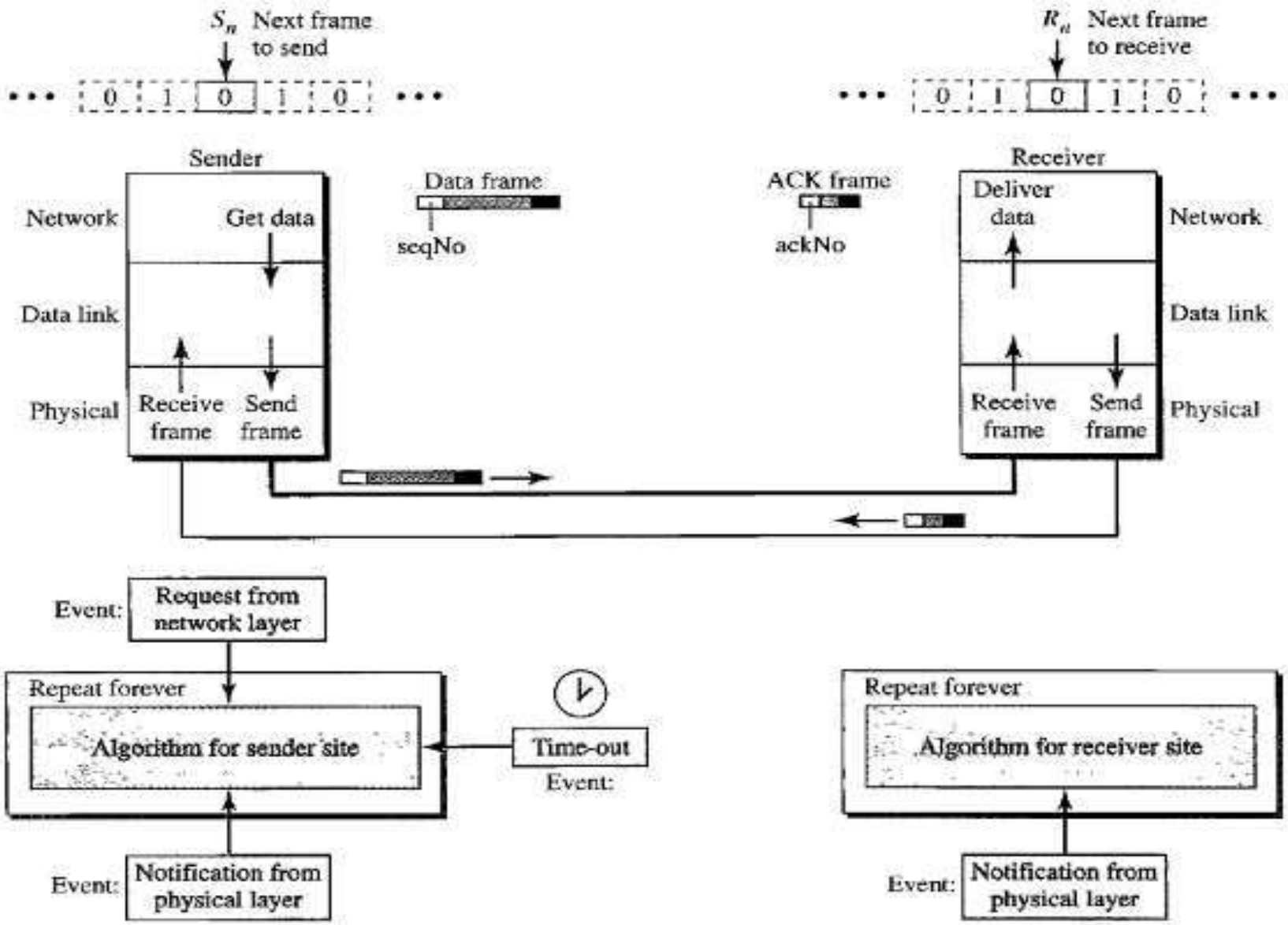


Stop and Wait Automatic Repeat Request Protocol(Stop-and-Wait ARQ)

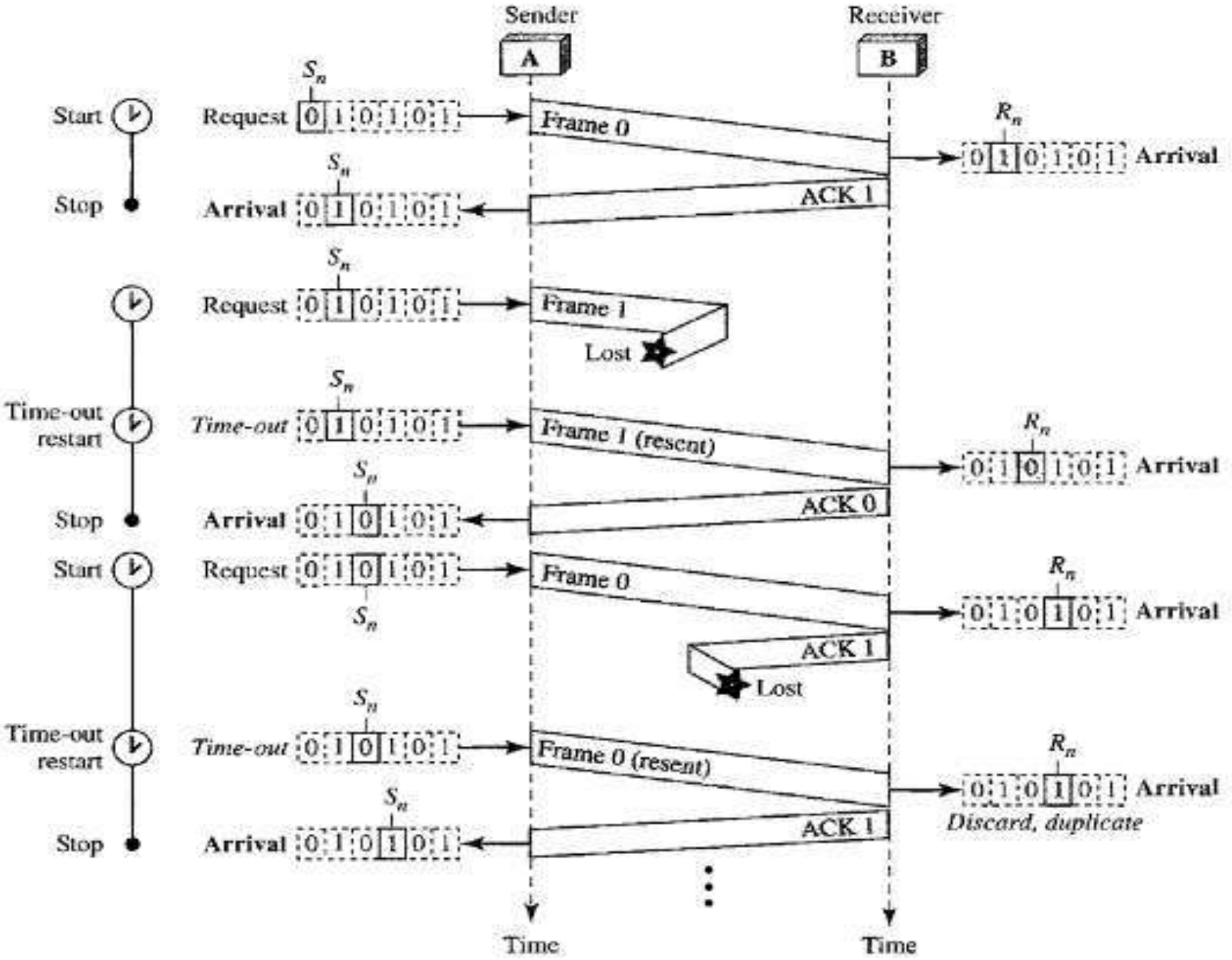
- It is an improved version of Stop and Wait protocol with error control mechanism
- Error correction in Stop-and-Wait ARQ is done by keeping a copy of send frame and retransmitting of the frame when the timer expires.

1. The frame arrives safe and sound at the receiver site; the receiver sends an acknowledgment. The acknowledgment arrives at the sender site, causing the sender to send the next frame numbered $x + 1$.
2. The frame arrives safe and sound at the receiver site; the receiver sends an acknowledgment, but the acknowledgment is corrupted or lost. The sender resends the frame (numbered x) after the time-out. Note that the frame here is a duplicate. The receiver can recognize this fact because it expects frame $x + 1$ but frame x was received.
3. The frame is corrupted or never arrives at the receiver site; the sender resends the frame (numbered x) after the time-out.

Design of Stop-and-Wait ARQ Protocol



Flow Diagram for Stop-and-Wait ARQ



Stop and Wait Flow Control

- **Generally large block of data split into small frames**
  Called "Fragmentation" and is used when

  1. Limited buffer size at receiver
  2. Errors detected sooner (when whole frame received)
  3. On error, retransmission of smaller frames is needed
  4. Prevents one station occupying medium for long periods

- **Channel Utilization is higher when**

  1. The transmission time is longer than the propagation time
  2. Frame length is larger than the bit length of the link

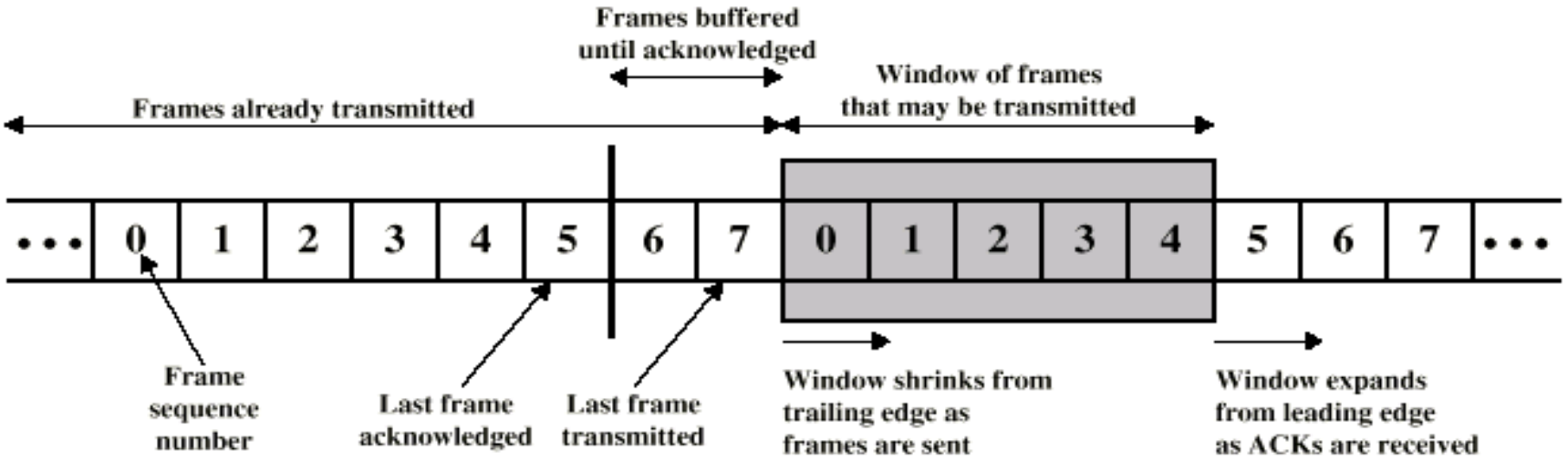
Sliding Window Flow Control

- The problem of **"Stop and Wait" is not able to send multiple packets**
- **Sliding Window Protocol** allows **multiple frames to be in transit**
- In this flow control mechanism **both sender and receiver agrees on the number of frames after which the acknowledgement should be sent.**

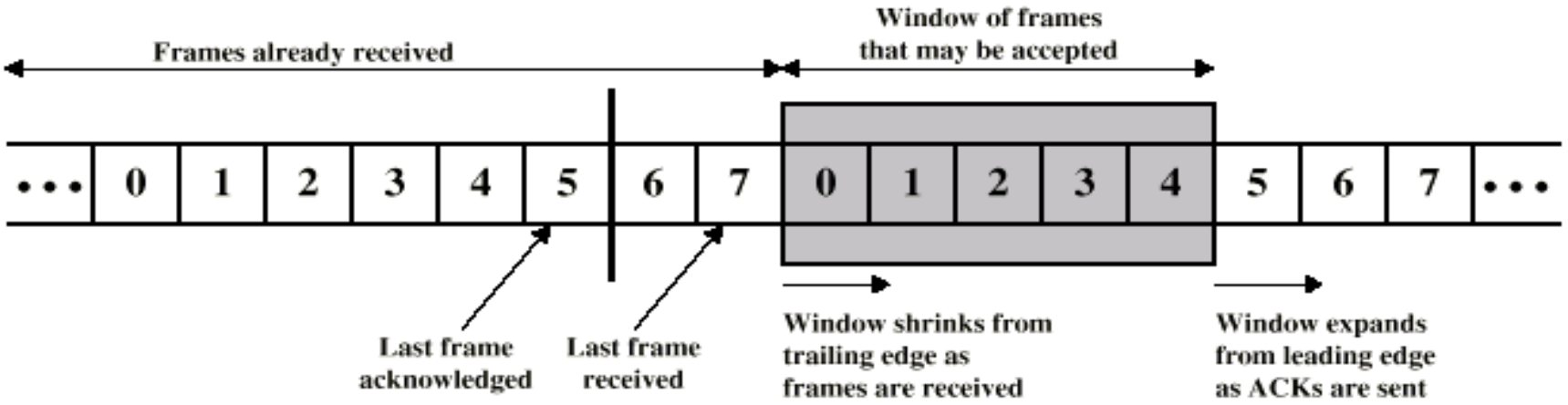
Sliding Window Flow Control

1. Receiver has buffer of W (called window size) frames
2. Transmitter can send up to *W* frames without ACK
3. Each frame is numbered
4. Sequence number bounded by size of the sequence number field
5. ACK includes number of next frame expected

Sliding Window Flow Control (W = 5)

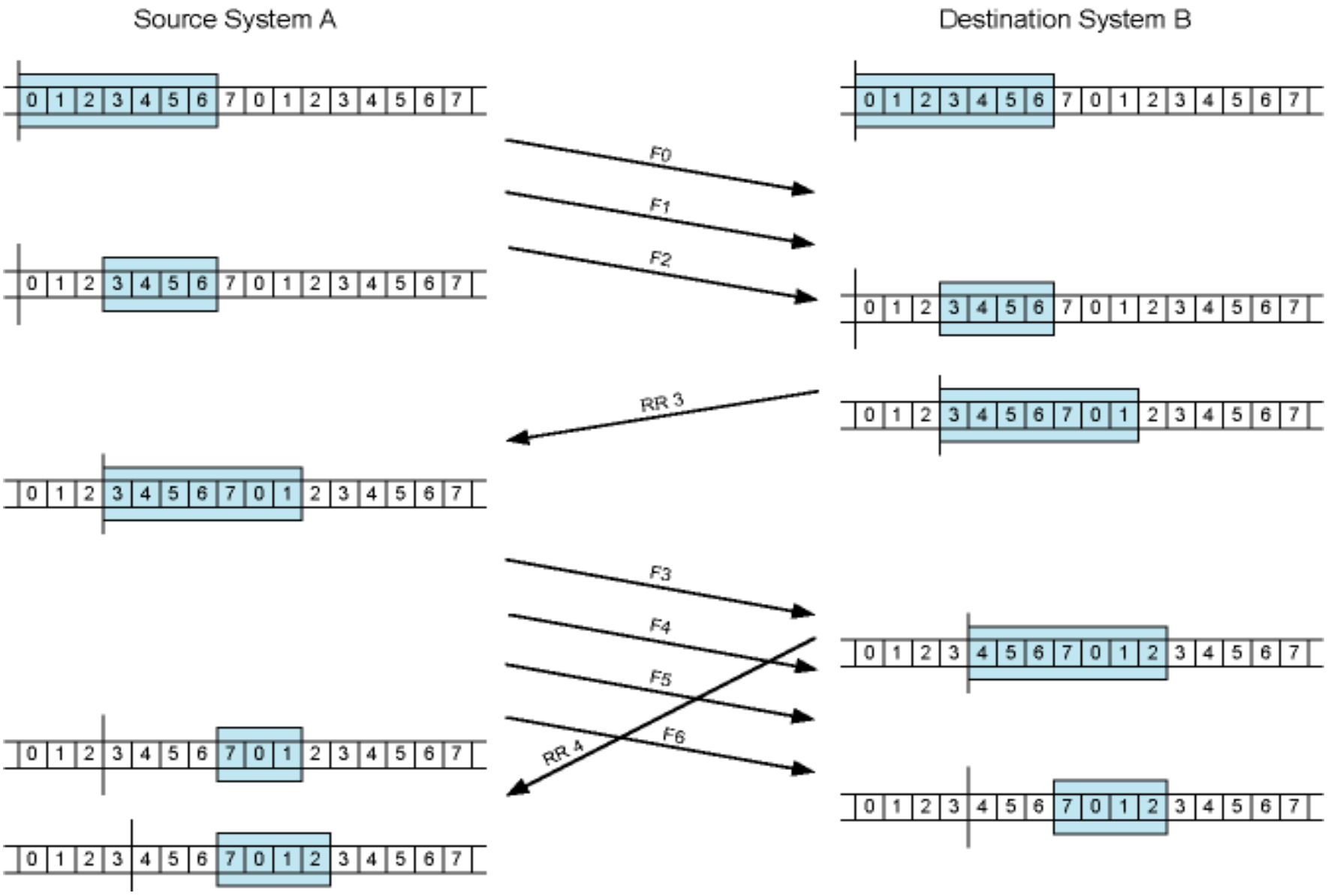


(a) Sender's perspective



(b) Receiver's perspective

Example of a Sliding Window Protocol (W = 7)



Go-Back-N Automatic Repeat Request

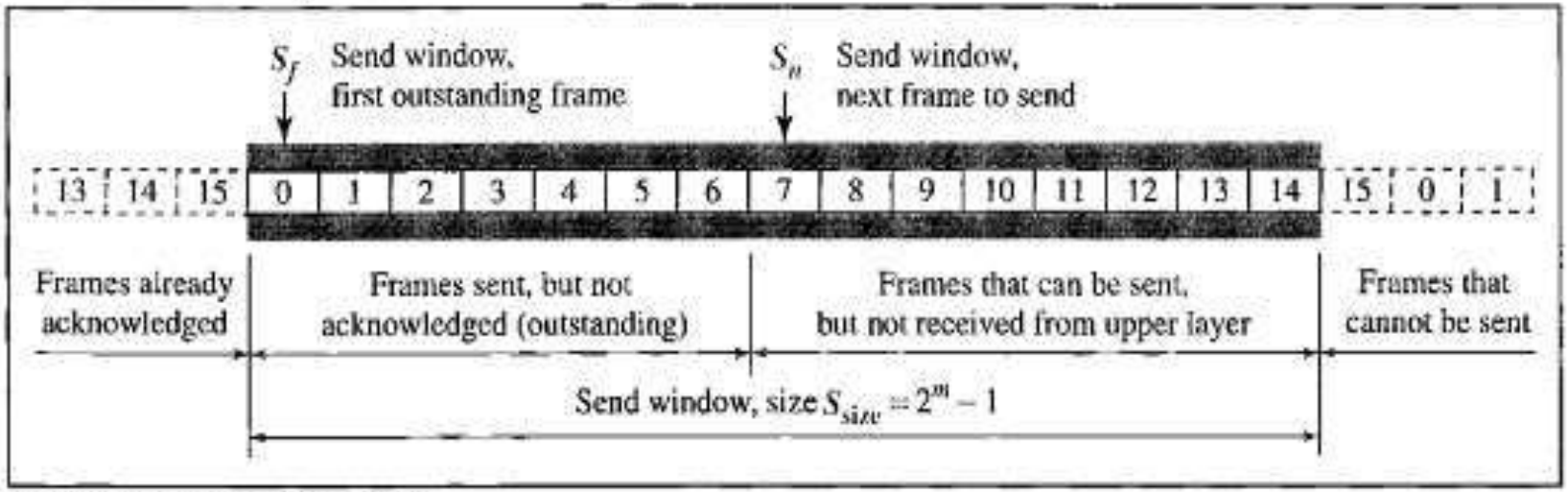
1. **Several frames can be send before receiving acknowledgement**
2. **Sender keeps a copy of these frames until ACK arrives**
3. **If the header of the frame allows ‘m’ bits for the sequence number, the sequence number range from** $0 \text{ to } 2^m - 1.$
4. **If m=4, then sequence numbers are**

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \ldots$$

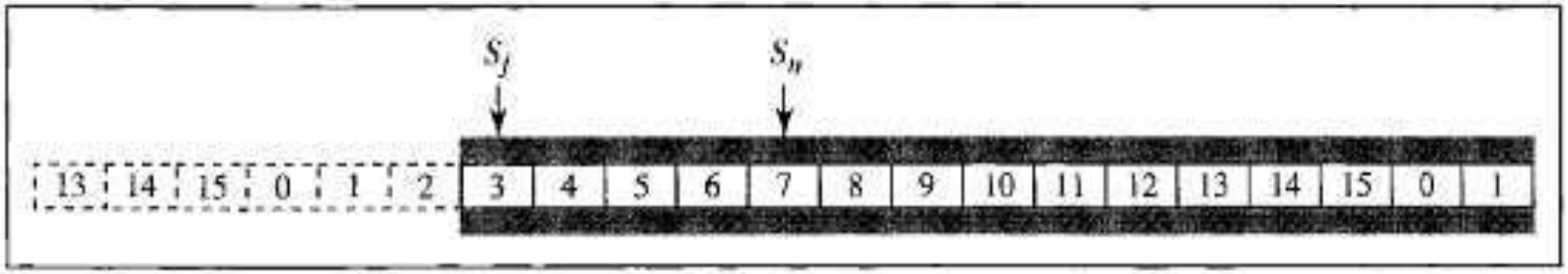
5. **Sliding window is an abstract concept that defines range of sequence numbers that is concern of sender and receiver.**

Go-Back-N ARQ

Send window for Go-Back-N ARQ



a. Send window before sliding



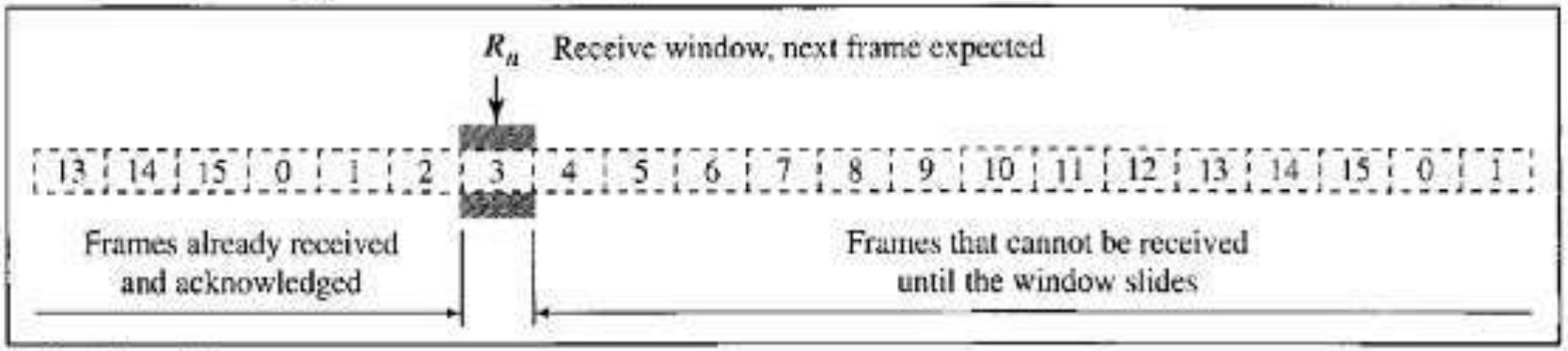
b. Send window after sliding

The send window is an abstract concept defining an imaginary box of size $2^m - 1$ with three variables: S_f, S_n, and S_{size}.

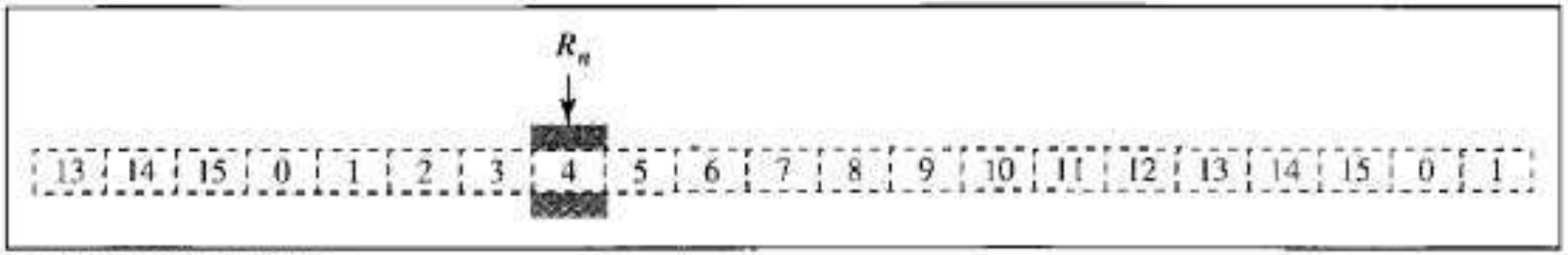
S_f (send window, the first outstanding frame), S_n (send window, the next frame to be sent), and S_{size} (send window, size).

Go-Back-N ARQ

Receive window for Go-Back-N ARQ



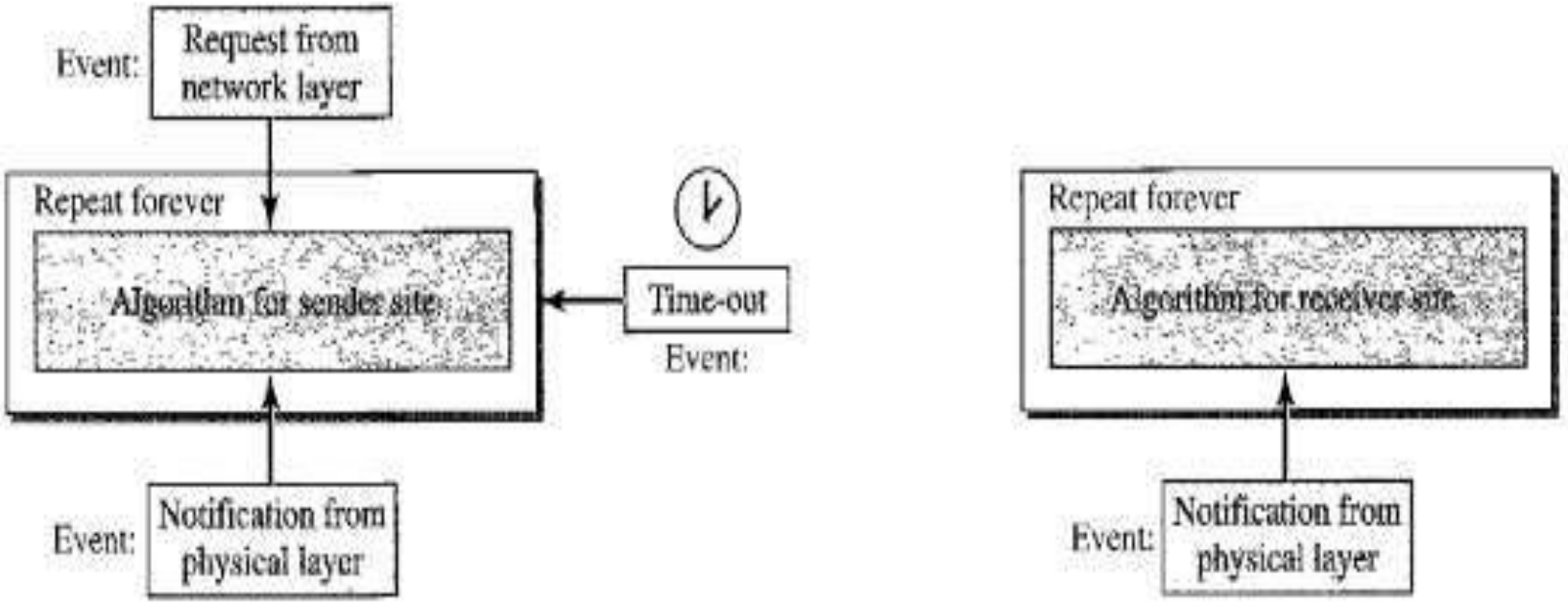
a. Receive window



b. Window after sliding

The receive window is an abstract concept defining an imaginary box of size 1 with one single variable R_n. The window slides when a correct frame has arrived; sliding occurs one slot at a time.

Go-Back-N ARQ

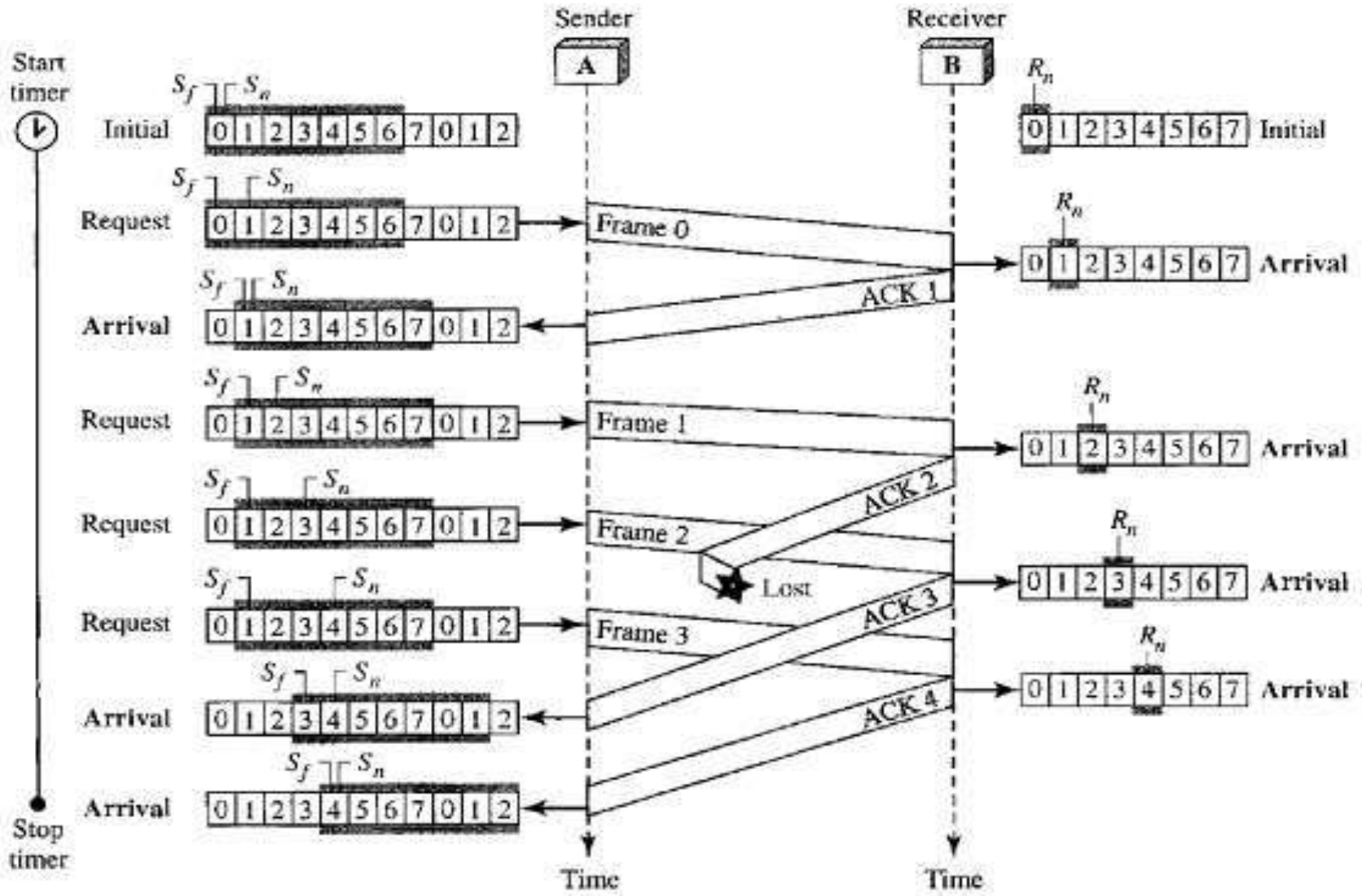

Event:
Request from network layer
Repeat forever
Algorithm for sender site
Time-out
Event:
Event:
Notification from physical layer
Repeat forever
Algorithm for receiver site
Event:
Notification from physical layer

Go-Back-N ARQ

In Go-Back-*N* ARQ, the size of the send window must be less than 2^m; the size of the receiver window is always 1.

In following example, data frames are not lost, but some Ack are lost and some are delayed. Cumulative ack solve this problem

Go-Back-N ARQ


Sender
Receiver
A
B
Start timer
Stop timer
Initial
Request
Arrival
Frame 0
Frame 1
Frame 2
Frame 3
ACK 1
ACK 2
ACK 3
ACK 4
Lost
Time
Time