DATA AND COMMUNICATION NETWORKS

Instructor:

Dr. Bhargavi Goswami,
Associate Professor,
Garden City College of Science and Management
Bangalore.

CHAPTER 1

Introduction

What is the need of Networks?

- For resource sharing.
- Major requirement of user community.
- We need to generate and disseminate information.
- Also information should be accessible by each one in user group.
- For this we need to answer few questions.

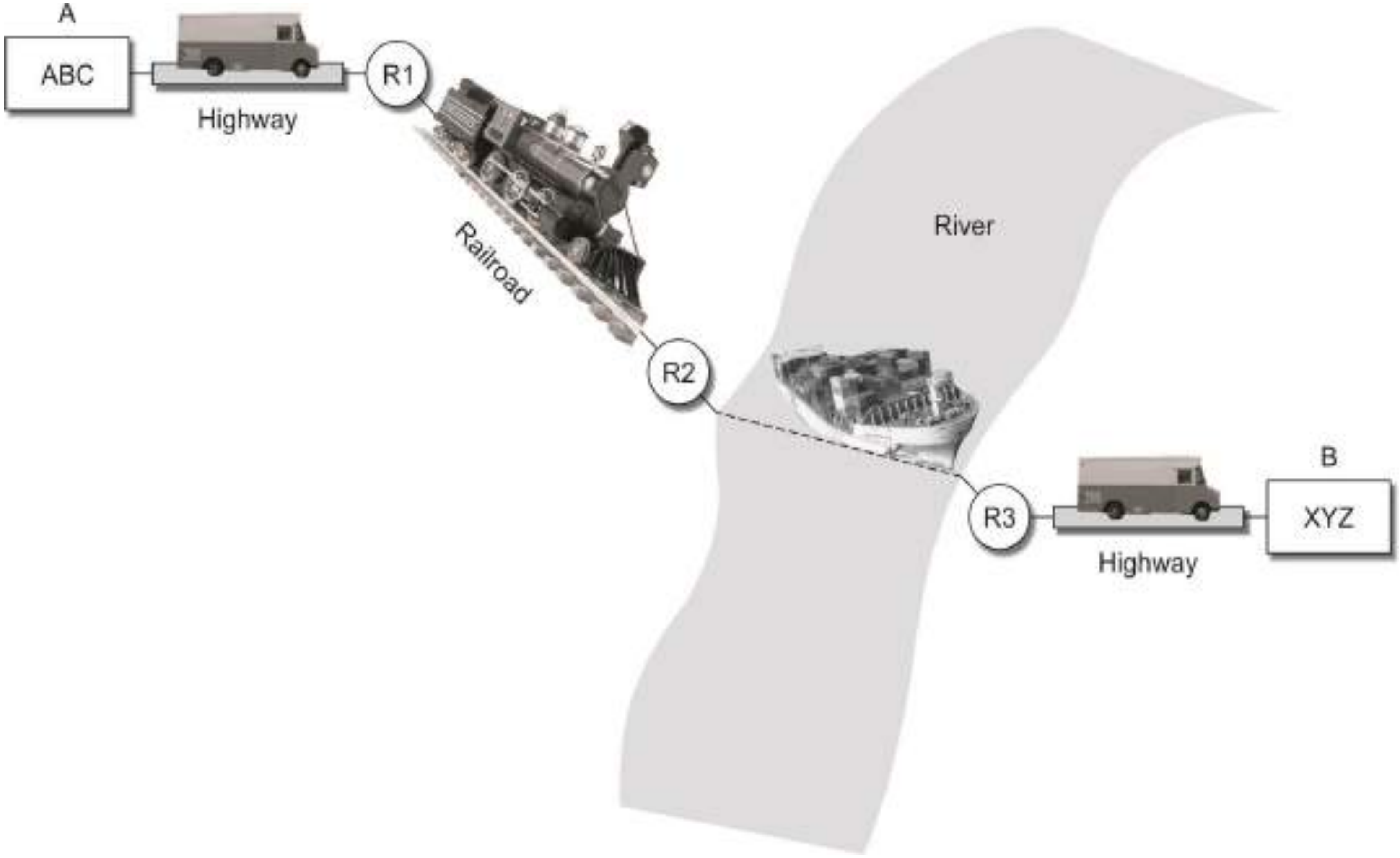
Questions to be Answered

- How is a file downloaded
- How do emails reach their intended recipients?
- How does a wired and a wireless connection work the same?
- How is receipt of new data (for example a new antivirus update), handled and by whom?

Layering Concept & Example:

- Based on Principle: Divide and Conquer.
- Each big problem divided into smaller pieces.
- Example: ABC is a middle level company, located at A, selling computers, having:
  - Manager
  - Secretary
  - Route Operator
  - Warehouse Keeper Cum Security Officer
  - Transporter
- XYZ is also a company, located at B, ordered ABC for 5000 units of computers.
- How to deliver?

Layering Example



Layering Example

- 1. Manager passes the order to deliver 5000 computers to XYZ company and keep track of the delivery.
- 2. Secretary communicates through letter with secretary of XYZ that consignment 5000 units of computer is sent, once delivered, give us acknowledgement.
- 3. Secretary tells route operator to deliver the consignment to XYZ at B. He has map, using multiple transportations, he sends box.
- 4. ABC has transport office at R1,R2,R3.
- 5. At each destination, warehouse keeper takes care of delivery and security of goods at the time of unloading and loading.

Layering Example

- Advantage:
- 1 Clear Job Distribution:
  - Work of each employee is clearly defined.
  - We can easily replace anyone of them with new employee without affecting efficiency of overall process.
  - If new employee has different style of functioning, it doesn't affect us.
  - When job is clearly divided, complex job becomes manageable.
- 2. Every employee taking or giving services. Also called interface in computer networks.

Advantages of layers

- Reducing the complexity
- Division of Work
- Standard Interfacing between Components
- Replacing a component is easy
- Independence in Protocol design

Disadvantages of layers

- Reduced Speed and Performance
- Increased Memory usage
- Sensor Networks Node

What is the need to Share Resources?

- We need to generate information and disseminate information. Eg.
- Music files can be downloaded and uploaded on internet from LAN
- Emails
- Skype Voice – Video Calls
- Access information from blogs
- Access Database at remote location
- Audio and Video Conferencing

Give functions of Each Layer in OSI/TCP Model

1. Physical Layer:

- Transmitting raw bits over a communication channel.
- Works as Transporter, to carry bits from one end to another.
- Converts the bits to voltage or light pulse and at the other end, converts incoming voltage or light pulse to bits.
- Checks whether message has to be broadcasted or unicasted.

Give functions of Each Layer in OSI/TCP Model

2. Data Link Layer:

- The No Monopoly idea and the framing
- Framing Techniques
- Error Control
- Flow Control
- Classification into 1) MAC 2) LCC

Give functions of Each Layer in OSI/TCP Model

3. Medium Access Layer

- Receive/transmit normal frames
- Half-duplex retransmission and backoff functions
- Append/check FCS (frame check sequence)
- Inter-frame gap enforcement
- Discard malformed frames
- Append(tx)/remove(rx) preamble, SFD(Start Frame Delimiter), and padding
- Half-duplex compatibility: append(tx)/remove(rx) MAC address

Give functions of Each Layer in OSI/TCP Model

4. Network Layer

- Handling accounting for usage of network resources
- Devise and implement mechanisms of identifying each machine uniquely
- Implement connectionless or connection-oriented forwarding
- Multiplexing and de-multiplexing the transport layer and the data link layer jobs

Give functions of Each Layer in OSI/TCP Model

5. Transport Layer

- Retransmission
- Adapted Retransmission Time according to Load
- Ordered Delivery
- Optimum Utilization of Bandwidth
- Flow Control
- Real Time Delivery
- Quality of Delivery

Give functions of Each Layer in OSI/TCP Model

6. Session Layer

- Allow users on different machines to establish sessions between them.
- Sessions offer various services, including
- Dialog Control (keeping track of whose turn it is to transmit),
- Token Management (preventing two parties from attempting the same critical operation at the same time), and
- Synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

Give functions of Each Layer in OSI/TCP Model

7. Presentation Layer

- The presentation layer is concerned with the syntax and semantics of the information transmitted.
- In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire."
- The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

Give functions of Each Layer in OSI/TCP Model

8. Application Layer

- Application layer contains a variety of protocols that are commonly needed by users.
- Widely-used application protocol is HTTP (Hyper Text Transfer Protocol), which is the basis for the World Wide Web.
- When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP.
- The server then sends the page back.
- Other application protocols are used for file transfer, electronic mail, and network news.

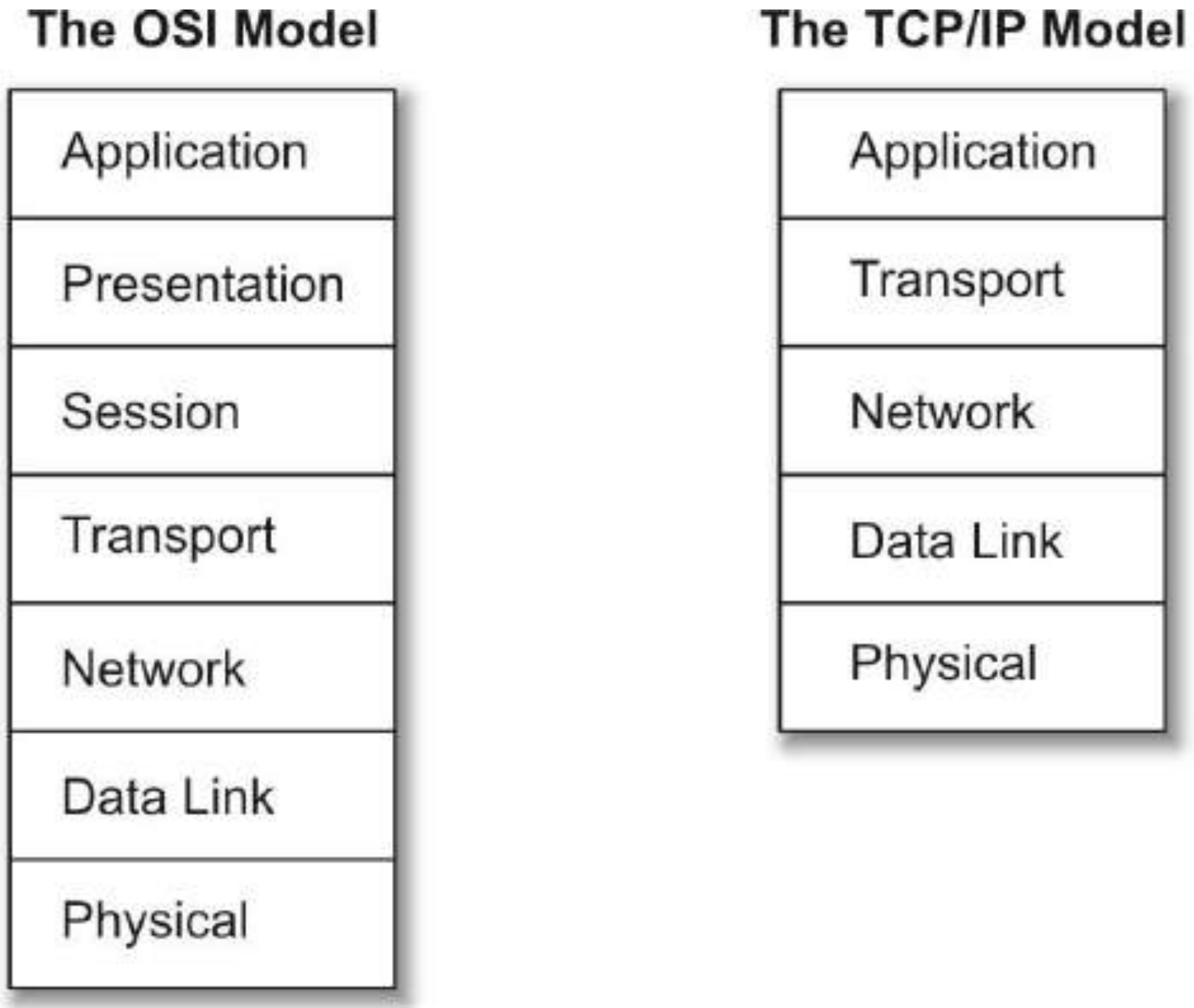
OSI v/s TCP/IP Layering Models

OSI	TCP/IP
OSI (Open System Interconnection) Designed by ISO (International Standards Organization) in 1983.	The ARPANET, a research network group connected hundreds of universities and govn installations, using leased telephone lines which later became TCP/IP.
7 Layers	5 Layers
Did not clearly distinguish between service, interface and protocol.	Distinction between these three concepts are explicit.
Protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.	Protocols in TCP/IP model are not hidden and tough to replace if technology changes.

OSI v/s TCP/IP Layering Models

OSI	TCP/IP
The protocols came first, and the model was really just a description of the existing protocols.	The model was not biased toward one particular set of protocols, a fact that made it quite general.
Designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.	Designers have much experience with the subject and have clear idea of which functionality to put in which layer.
Network Layer supports only connectionless communication.	Network Layer, supports both, connection oriented and connectionless communication.
More General.	More precise.
Describes the difference between protocol and interface.	Doesn't give emphasis on clear interface between layers. Protocol works specially for transport and network layer.

Layers for OSI and TCP/IP



Connection Oriented vs Connectionless

- Connection establishment
- Complete line occupied
- Packet can be not be compressed (Pkt Size: 64 kb = 8x8)
- Multiplexing not there, costly if transmitting small packets.
- Robustness of the connection is not very good. Single link down results to connection break.
- Cost of the connection high
- Quality of service : Reliable, Delay if greedy user occupy channel with large flow.
- Order of delivery Important.
- Eg. ISD Telephone Call

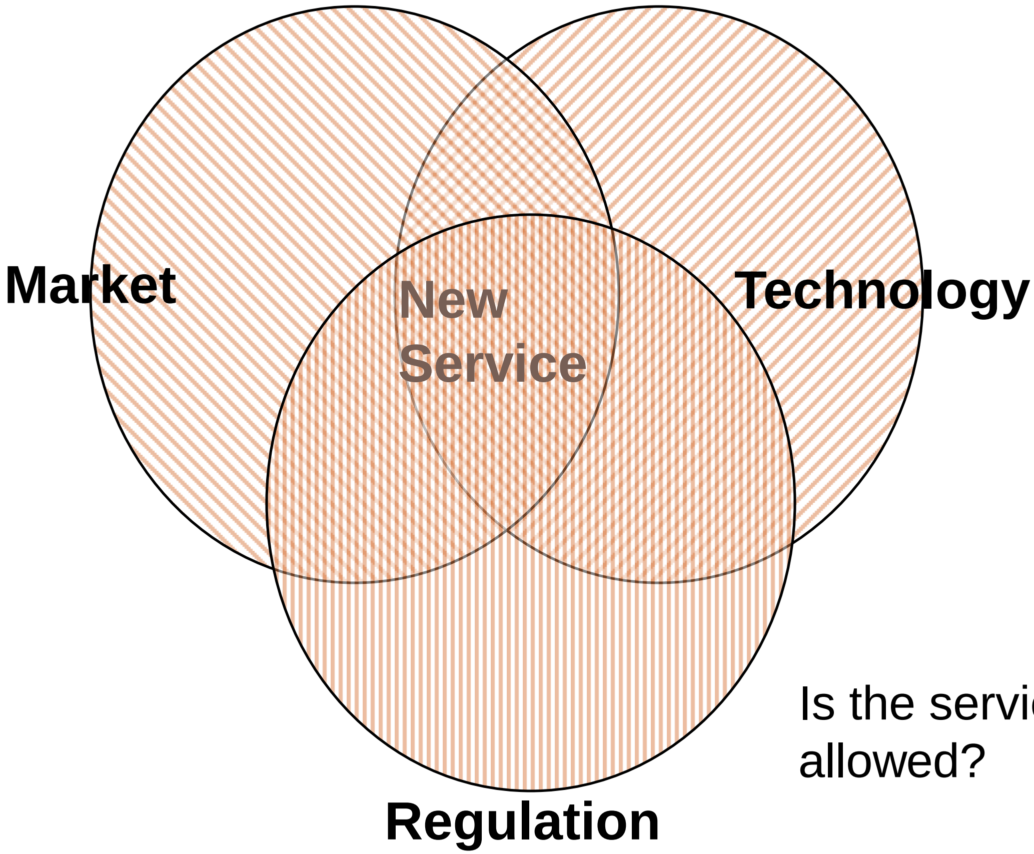
- No Connection establishment.
- Complete line not occupied
- Packet can be compressed (Pkt Size: 8kb)
- Multiplexing multiple packets in one large pkt.
- Robustness of the connection is very high. Single link down results to alternate path selection to continue connection
- Cost of the connection less
- Quality of service: Unreliable, Delay if compressed.
- Order of delivery not Important.
- Eg: Internet Voice Call

Key Factors in Network Evolution

Success Factors for New Services

- Technology not only factor in success of a new service
- Three factors considered in new telecom services

Can there be demand for the service?



Can it be implemented cost-effectively?

Is the service allowed?

Transmission Technology

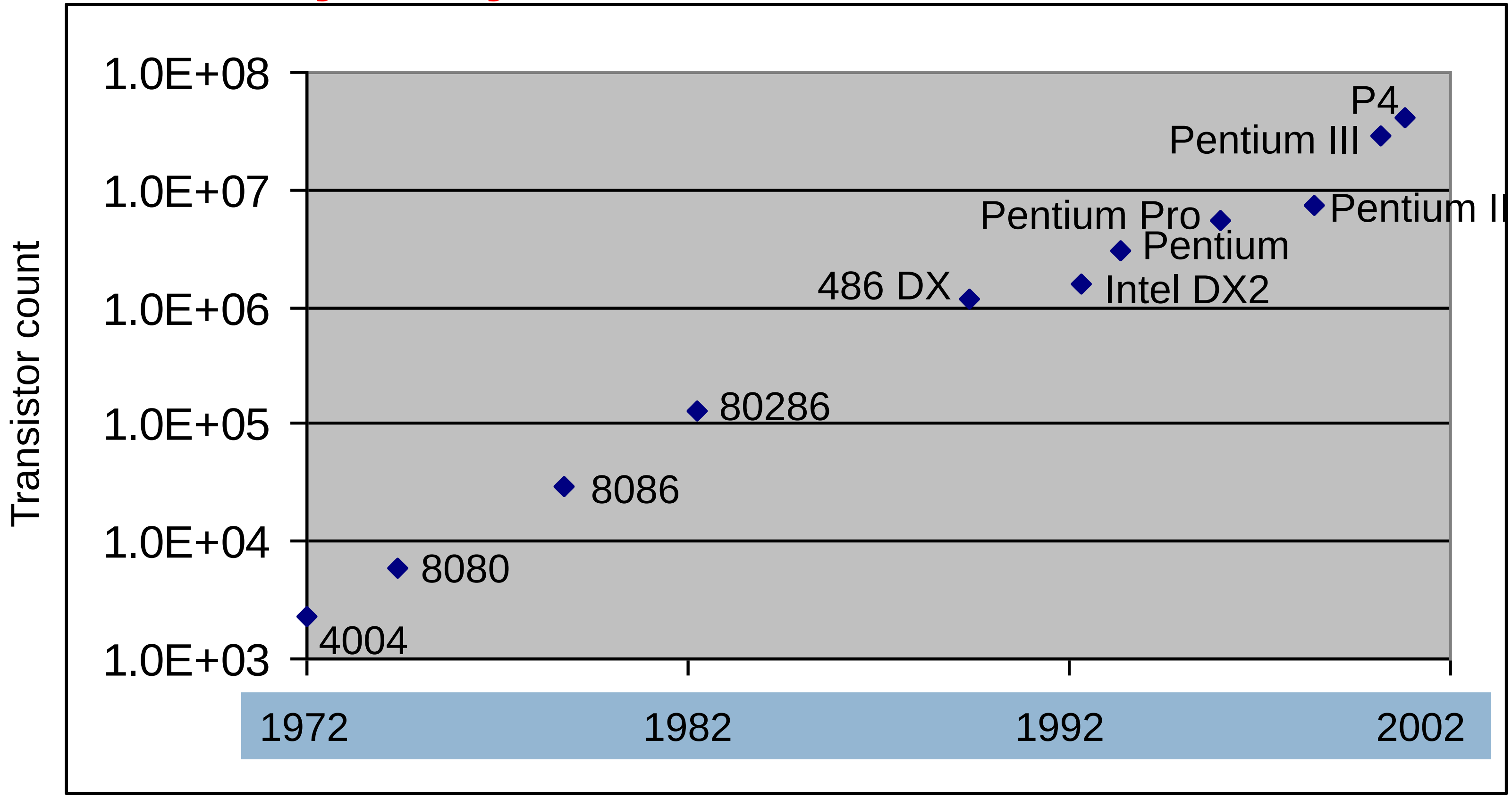
- Relentless improvement in transmission
- High-speed transmission in copper pairs
  - DSL Internet Access
- Higher call capacity in cellular networks
  - Lower cost cellular phone service
- Enormous capacity and reach in optical fiber
  - Plummeting cost for long distance telephone
- Faster and more information intensive applications

Processing Technology

- Relentless improvement in processing & storage
- Moore's Law: doubling of transistors per integrated circuit every two years
- RAM: larger tables, larger systems
- Digital signal processing: transmission, multiplexing, framing, error control, encryption
- Network processors: hardware for routing, switching, forwarding, and traffic management
- Microprocessors: higher layer protocols and applications
- Higher speeds and higher throughputs in network protocols and applications

Moore's Law

states that the <u>number of transistors on a chip doubles about every two years</u>.



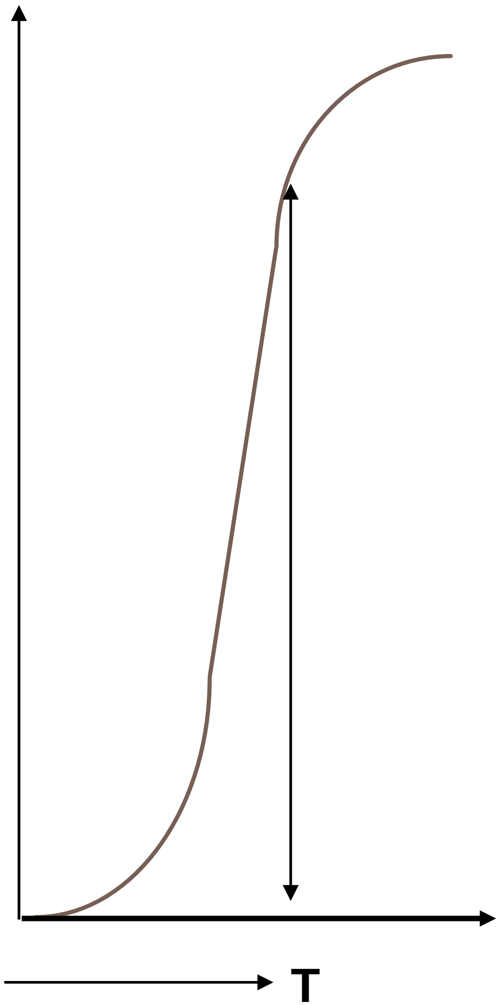
Software Technology

- Greater functionality & more complex systems
- TCP/IP in operating systems
- Java and virtual machines
- New application software
- Middleware to connect multiple applications
- Adaptive distributed systems

Market

- *The network effect*: usefulness of a service increases with size of community
  - Metcalfe's Law: usefulness is proportional to the square of the number of users
  - Phone, fax, email, …
- *Economies of scale*: per-user cost drops with increased volume
  - Cell phones, PDAs, PCs
  - Efficiencies from multiplexing
- *S-curve*: growth of new service has S-shaped curve, challenge is to reach the critical mass

The S Curve



Service Penetration & Network Effect

- Telephone: T=30 years
  - city-wide & inter-city links
- Automobile: T=30 years
  - roads
- Others
  - Fax
  - Cellular & cordless phones
  - Internet & WWW

Regulation & Competition

- Telegraph & Telephone originally monopolies
  - Extremely high cost of infrastructure
  - Profitable, predictable, slow to innovate
- Competition feasible with technology advances
  - Long distance cost plummeted with optical tech
  - Alternative local access through cable, wireless
  - Radio spectrum: auctioned vs. unlicensed
- Basic connectivity vs. application provider
  - Tussle for the revenue-generating parts

Standards

- New technologies very costly and risky
- Standards allow players to share risk and benefits of a new market
  - Reduced cost of entry
  - Interoperability and network effect
  - Compete on innovation
  - Completing the value chain
    - Chips, systems, equipment vendors, service providers
- Example
  - 802.11 wireless LAN products

Standards Bodies

- Internet Engineering Task Force
  - Internet standards development
  - Request for Comments (RFCs): www.ietf.org
- International Telecommunications Union
  - International telecom standards
- IEEE 802 Committee
  - Local area and metropolitan area network standards
- Industry Organizations
  - MPLS Forum, WiFi Alliance, World Wide Web Consortium
- Indian: BIS, Bureau of Indian Standards.

IEEE 802 Standards

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

The 802 working groups. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up.

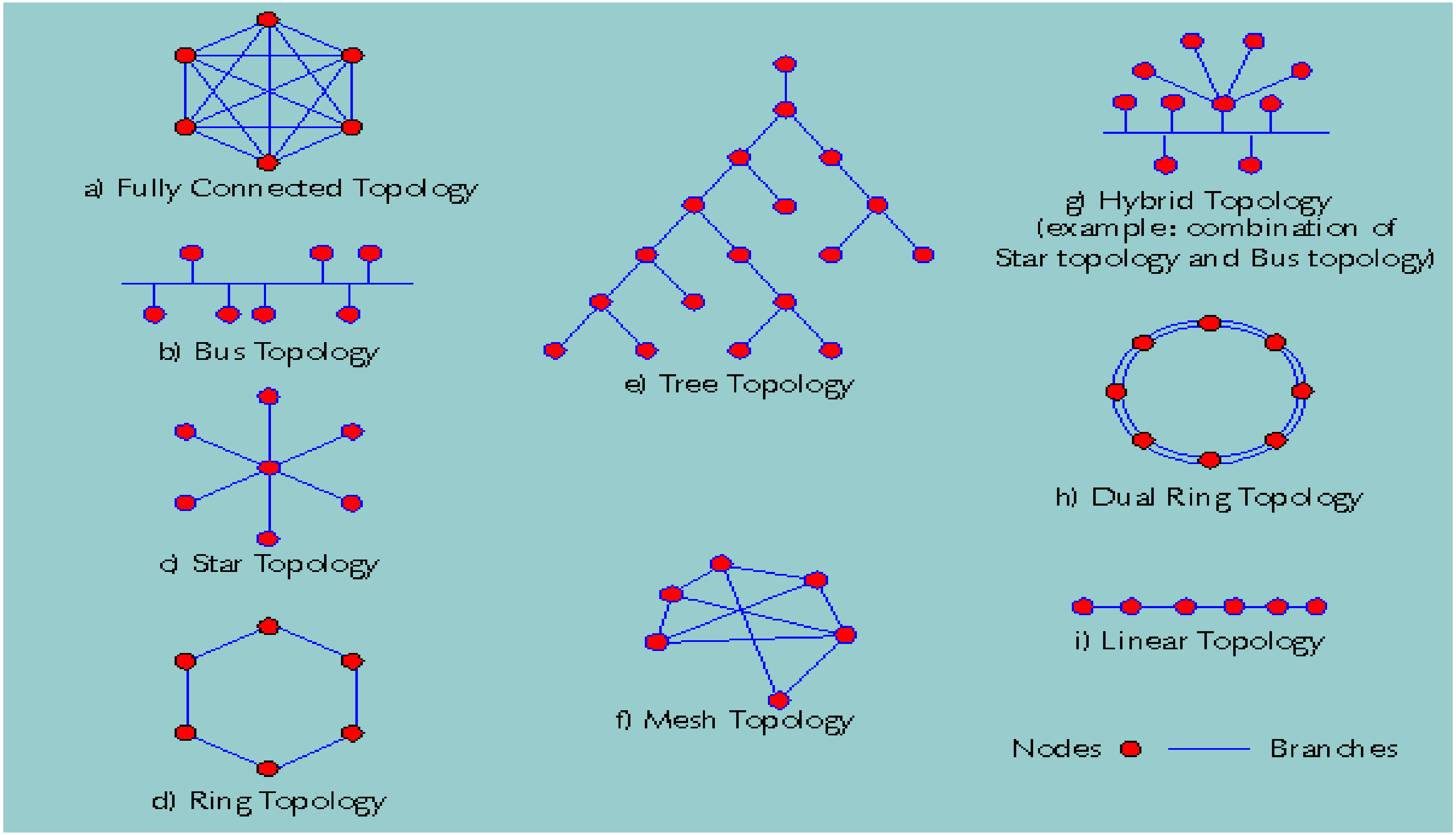
By: Dr.Bhargavi H. Goswami
Email:bhargavigoswami@gmail.com

Metric Units

Exp.	Explicit	Prefix	Exp.	Explicit	Prefix
10^{-3}	0.001	milli	10^{3}	1,000	Kilo
10^{-6}	0.000001	micro	10^{6}	1,000,000	Mega
10^{-9}	0.000000001	nano	10^{9}	1,000,000,000	Giga
10^{-12}	0.000000000001	pico	10^{12}	1,000,000,000,000	Tera
10^{-15}	0.000000000000001	femto	10^{15}	1,000,000,000,000,000	Peta
10^{-18}	0.000000000000000001	atto	10^{18}	1,000,000,000,000,000,000	Exa
10^{-21}	0.000000000000000000001	zepto	10^{21}	1,000,000,000,000,000,000,000	Zetta
10^{-24}	0.000000000000000000000001	yocto	10^{24}	1,000,000,000,000,000,000,000,000	Yotta

- The principal metric prefixes.

Network Topology:



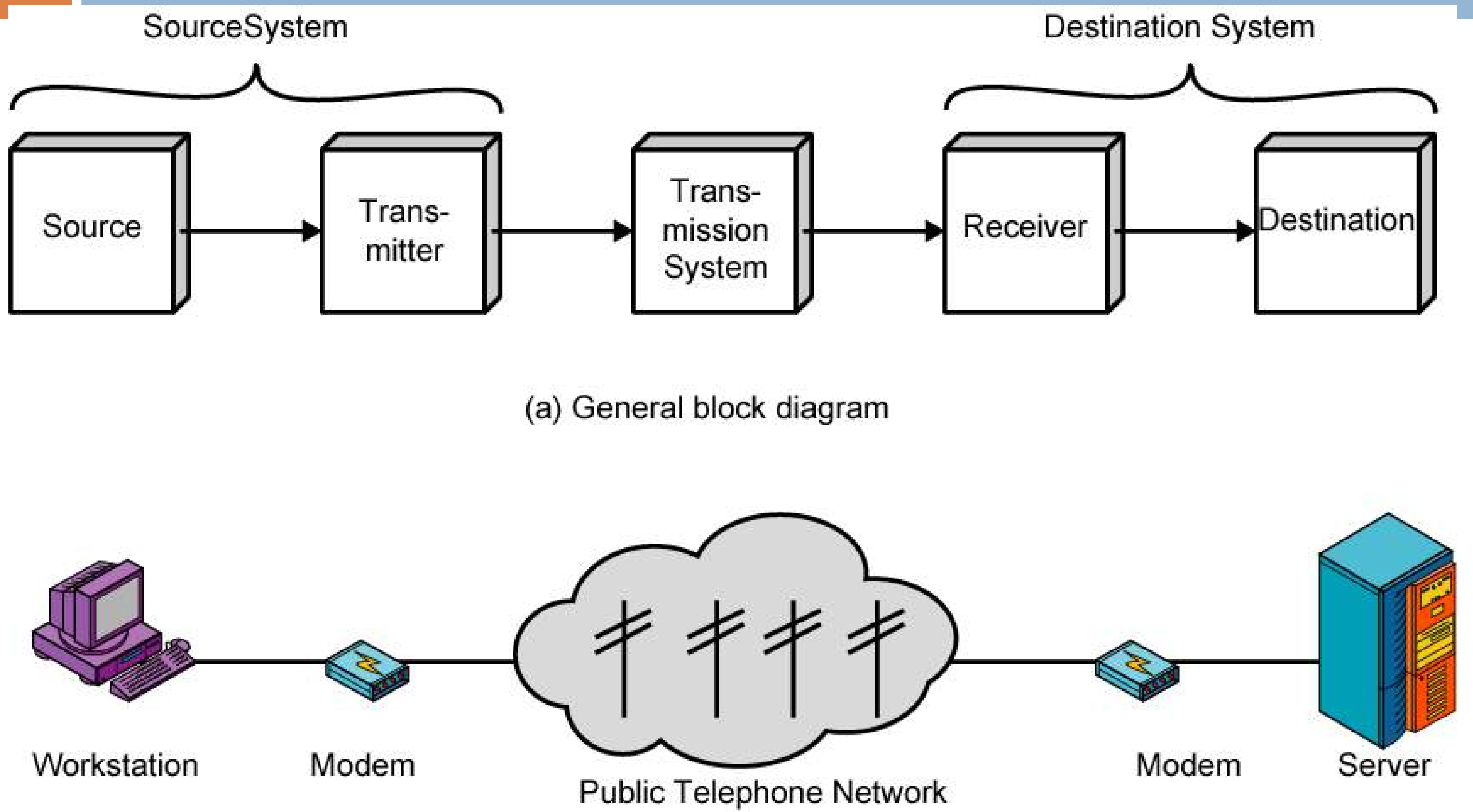
A Communications Model

- Source
  - generates data to be transmitted
- Transmitter
  - Converts data into transmittable signals
- Transmission System
  - Carries data
- Receiver
  - Converts received signal into data
- Destination
  - Takes incoming data

Communications Tasks: N/W Functions

Transmission system utilization	Addressing
Interfacing	Routing
Signal generation	Recovery
Synchronization	Message formatting
Exchange management	Security
Error detection and correction	Network management
Flow control	

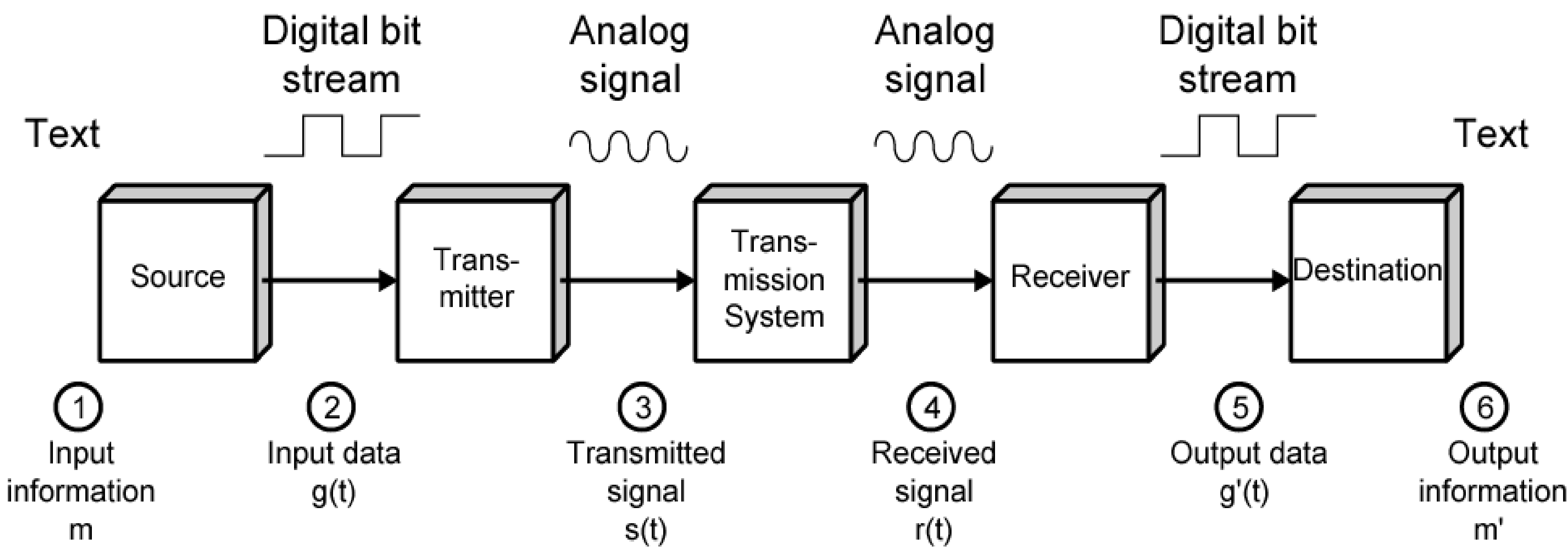
Simplified Communications Model - Diagram



(a) General block diagram

(b) Example

Simplified Data Communications Model



Networking

- Point to point communication not usually practical
  - Devices are too far apart
  - Large set of devices would need impractical number of connections
- Solution is a communications network
  - Wide Area Network (WAN)
  - Local Area Network (LAN)

Wide Area Networks

- Large geographical area
- Crossing public rights of way
- Rely in part on common carrier circuits
- Alternative technologies
  - Circuit switching (covered during switching)
  - Packet switching (covered during switching)
  - Frame relay
  - Asynchronous Transfer Mode (ATM)

Frame Relay

- Packet switching systems have large overheads to compensate for errors
- Modern systems are more reliable
- Errors can be caught in end system
- Most overhead for error control is stripped out

Asynchronous Transfer Mode

- ATM
- Evolution of frame relay
- Little overhead for error control
- Fixed packet (called cell) length
- Anything from 10Mbps to Gbps
- Constant data rate using packet switching technique

Local Area Networks

- Smaller scope
  - Building or small campus
- Usually owned by same organization as attached devices
- Data rates much higher
- Usually broadcast systems
- Now some switched systems and ATM are being introduced

LAN Configurations

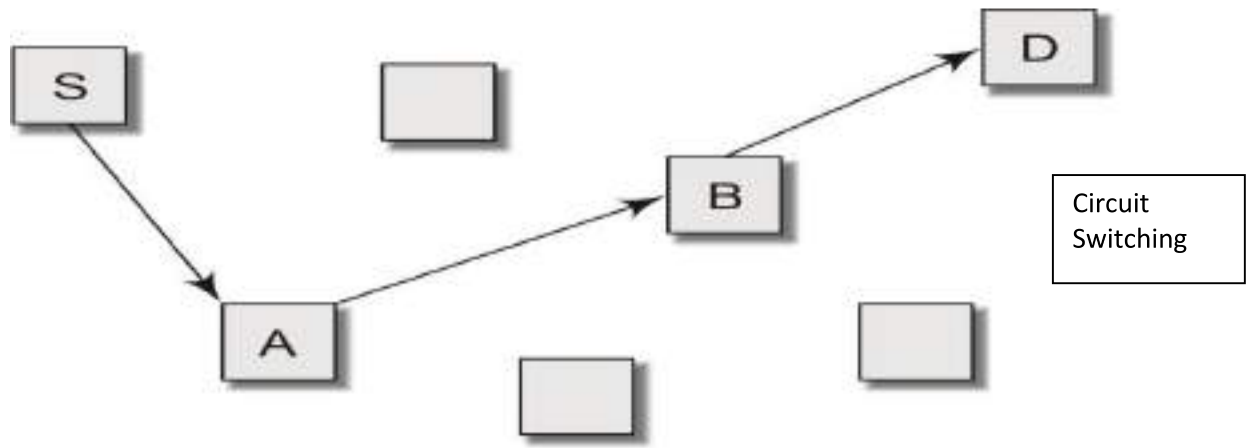
- Switched
  - Switched Ethernet
    - May be single or multiple switches
  - ATM LAN
  - Fibre Channel
- Wireless
  - Mobility
  - Ease of installation

Metropolitan Area Networks

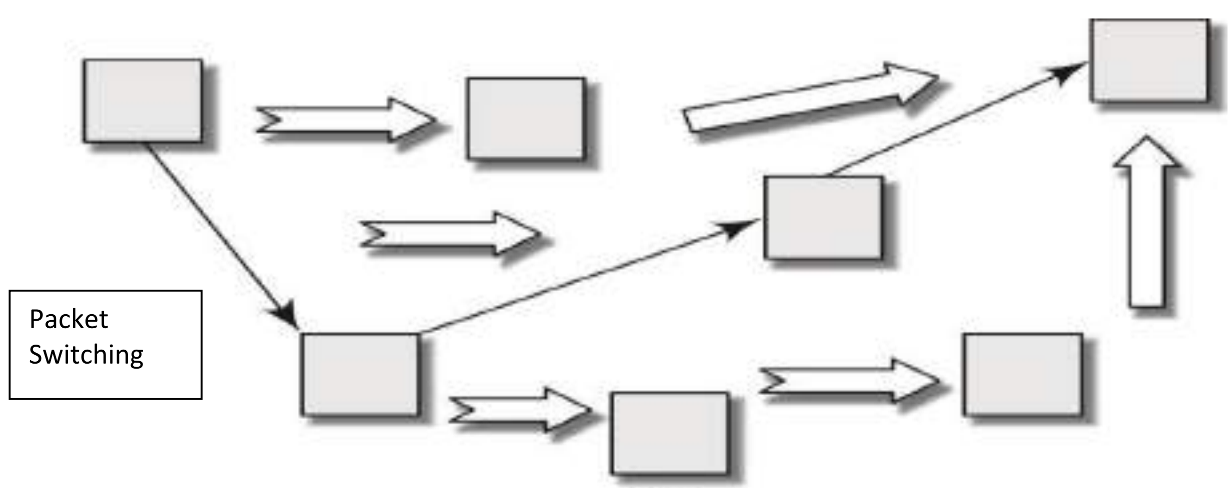
- MAN
- Middle ground between LAN and WAN
- Private or public network
- High speed
- Large area

SWITCHING

- Switching is an operation where the decision of where to send the incoming data is instantaneous and predetermined. In routing, decision is taken dynamically and hence service is little delayed than switching.
- Switching is generally done at second layer.
- Layer 4 and Layer 5 are transport and application layer where data are populated.
- Layer 4 switch separate UDP and TCP data flows.
- Layer 5 switch send mail traffic in one direction and http traffic in another direction.
- Layer 3 switches are like routers.
- Telephone Lines use switches to route the traffic at physical layer.
- Though switching is faster, it is monotonous.
- Data does not flow continuously and so, it needs store and forwarding transmission facility.
- Types: 1) Circuit Switching 2) Packet Switching 3) Message Switching.



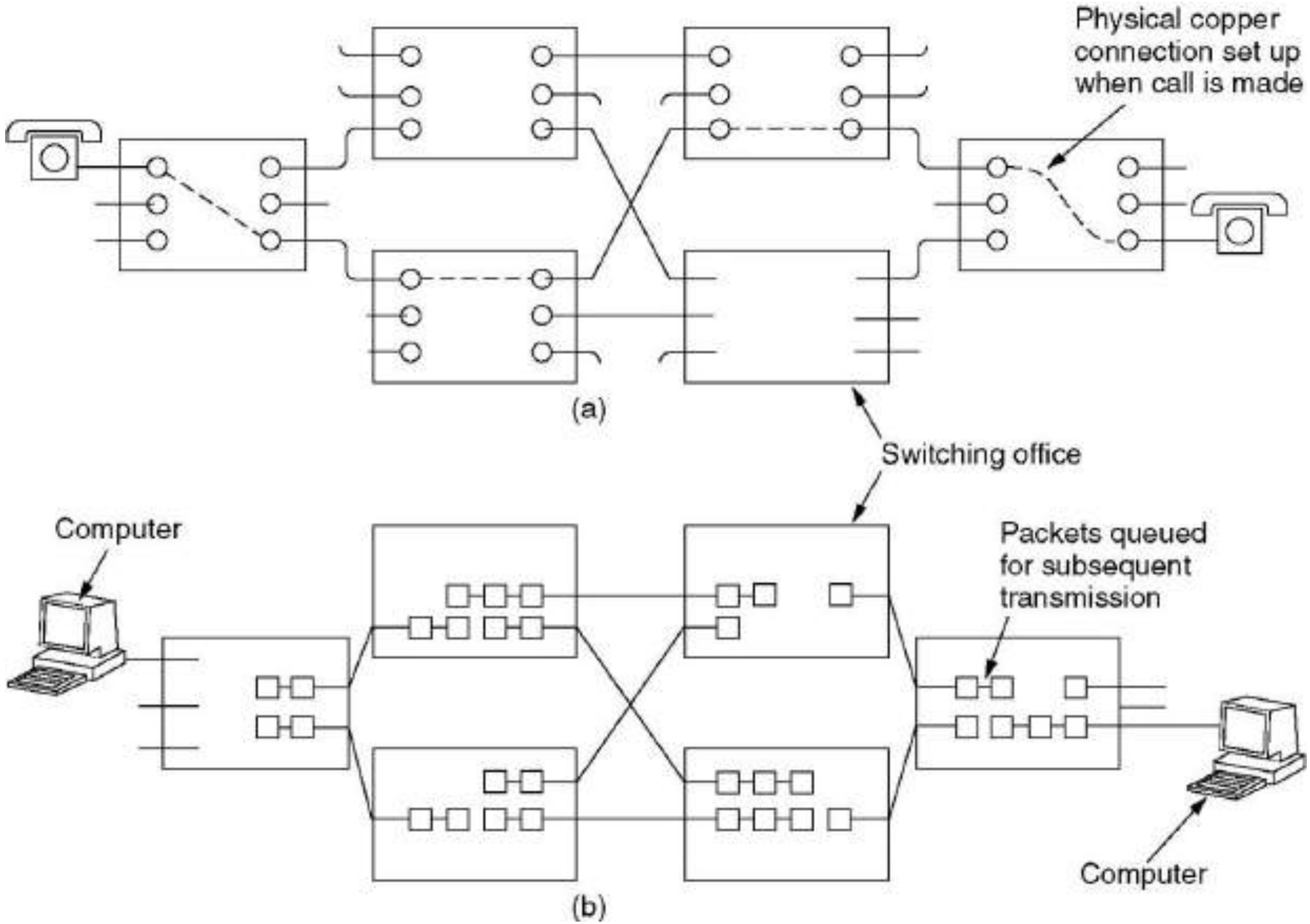
(a)



(b)

1. Circuit Switching

- In circuit switching, there is a dedicated line that connects the sender and the receiver.
- Here, path is reserved for duration of connection.
- Eg. Telephonic Conversation.
- Lets discuss advantage and disadvantage.



Physical copper
connection set up
when call is made
(a)
Switching office
Computer
Packets queued
for subsequent
transmission
Computer
(b)

Advantages of Circuit Switching

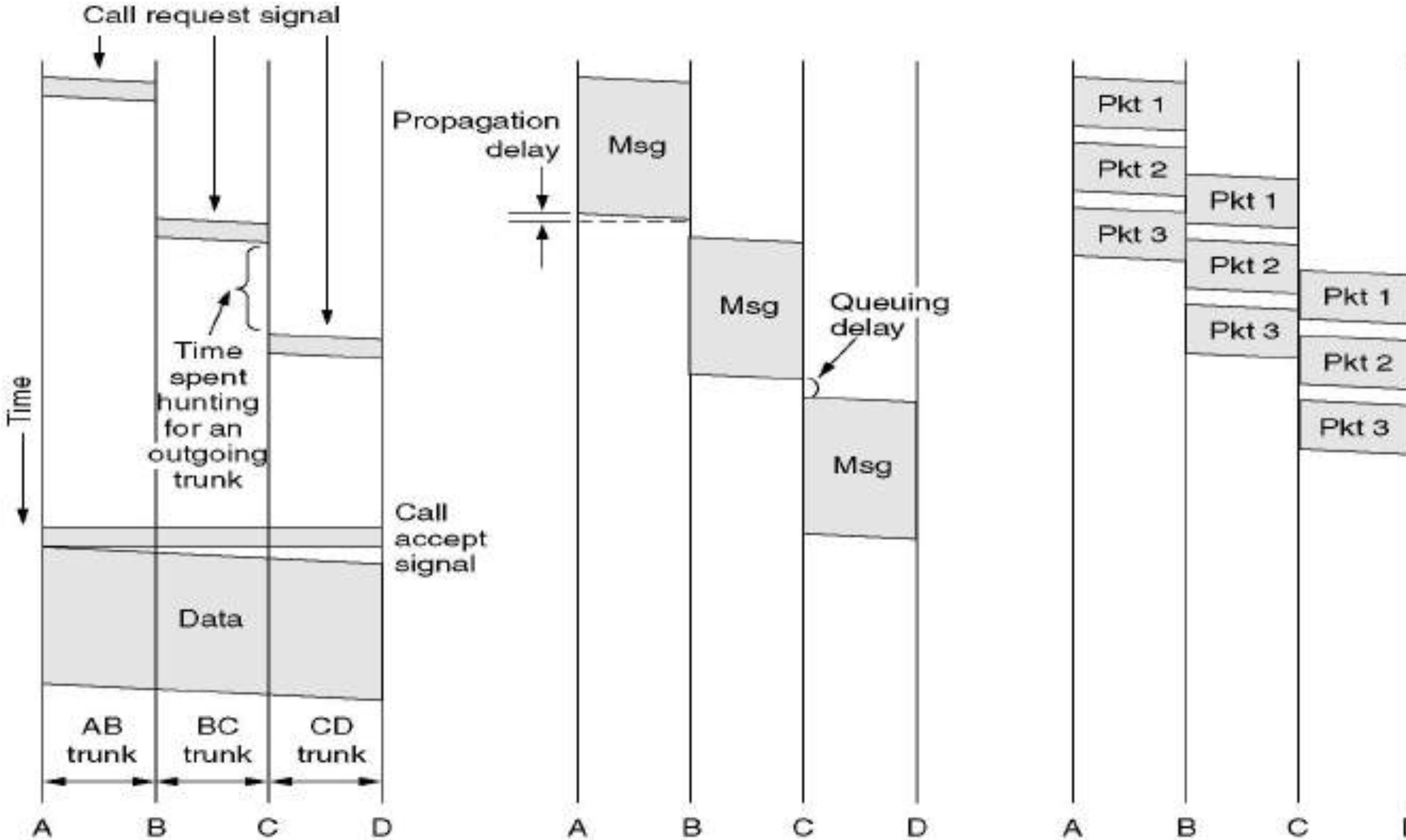
- Guaranteed bandwidth
- Predictable communication performance
- Not “best-effort” delivery with no real guarantees
- Simple abstraction
- Reliable communication channel between hosts
- No worries about lost or out-of-order packets
- Simple forwarding
- Forwarding based on time slot or frequency
- No need to inspect a packet header
- Low per-packet overhead
- Forwarding based on time slot or frequency
- No IP (and TCP/UDP) header on each packet

Disadvantages of Circuit Switching

- Wasted bandwidth
- Bursty traffic leads to idle connection during silent period
- Unable to achieve gains from statistical multiplexing
- Blocked connections
- Connection refused when resources are not sufficient
- Unable to offer "okay" service to everybody
- Connection set-up delay
- No communication until the connection is set up
- Unable to avoid extra latency for small data transfers
- Network state
- Network nodes must store per-connection information
- Unable to avoid per-connection storage and state

2) Message Switching

- It is possible to have packets that are large enough to hold entire message. Such a mechanism is not in practice is known as message switching.
- Not used nowadays.
- Communication is not continuous.
- Each packets travel independently.
- No physical path is established in advance between sender and receiver.
- Instead, when the sender has a block of data to be sent, it is stored in the first switching office (i.e., router) and then forwarded later, one hop at a time.
- Each block is received in its entirety, inspected for errors, and then retransmitted.
- A network using this technique is called a store-and-forward network.
- Used with telegrams.



Call request signal
Propagation delay
Msg
Msg
Queuing delay
Msg
Pkt 1
Pkt 2
Pkt 3
Pkt 1
Pkt 2
Pkt 3
Pkt 1
Pkt 2
Pkt 3
Time spent hunting for an outgoing trunk
Time
Call accept signal
Data
AB trunk
BC trunk
CD trunk
A
B
C
D
A
B
C
D
A
B
C
D

(a)

(b)

(c)

3) Packet Switching

- Doesn't reserve entire path in advance.
- Reserves only small portion of path.
- Data is segregated into pieces and transmitted as packets.
- In packet-based networks, the message gets broken into small data packets. These packets are sent out from the computer and they travel around the network seeking out the most efficient route to travel as circuits become available. This does not necessarily mean that they seek out the shortest route.
- Each packet may go a different route from the others.
- Each packet is sent with a 'header address'. This tells it where its final destination is, so it knows where to go.
- The header address also describes the sequence for reassembly at the destination computer so that the packets are put back into the correct order.
- One packet also contains details of how many packets should be arriving so that the recipient computer knows if one packet has failed to turn up.
- If a packet fails to arrive, the recipient computer sends a message back to the computer which originally sent the data, asking for the missing packet to be resent.

Advantages and Disadvantages

- Advantages:
  - Security
  - Bandwidth used to full potential
  - Devices of different speeds can communicate
  - Not affected by line failure (rediverts signal)
  - Availability – do not have to wait for a direct connection to become available
  - During a crisis or disaster, when the public telephone network might stop working, e-mails and texts can still be sent via packet switching
- Disadvantages
  - Under heavy use there can be a delay
  - Data packets can get lost or become corrupted
  - Protocols are needed for a reliable transfer
  - Not so good for some types data streams e.g real-time video streams can lose frames due to the way packets arrive out of sequence.

Differentiate between Circuit Switching and Packet Switching

Item	Circuit-switched	Packet-switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
When can congestion occur	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

Ping Utility:

- The ping command sends an echo request to a host available on the network. Using this command you can check if your remote host is responding well or not.
- The ping command is useful for the following −
  - Tracking and isolating hardware and software problems.
  - Determining the status of the network and various foreign hosts.
  - Testing, measuring, and managing networks
- Syntax:

  $ping hostname or ip-address

- To come out, “ctrl+C.

FTP Utility

- Here ftp stands for File Transfer Protocol. This utility helps you to upload and download your file from one computer to another computer.
- The ftp utility has its own set of UNIX like commands which allow you to perform tasks such as –
- Connect and login to a remote host.
- Navigate directories.
- List directory contents
- Put and get files
- Transfer files as ascii, ebcdic or binary
- Syntax:
- $ftp hostname or ip-address
- Above command would prompt you for login ID and password. Once you are authenticated, you would have access on the home directory of the login account and you would be able to perform various commands.

FTP Commands:

- Few of the useful commands are listed below –

Command	Description:
put filename	Upload filename from local machine to remote machine.
get filename	Download filename from remote machine to local machine.
mput file list	Upload more than one files from local machine to remote machine.
mget file list	Download more than one files from remote machine to local machine.
prompt off	Turns prompt off, by default you would be prompted to upload or download movies using mput or mget commands.
prompt on	Turns prompt on.
dir	List all the files available in the current directory of remote machine.
cd dirname	Change directory to dirname on remote machine.
lcd dirname	Change directory to dirname on local machine.
quit	Logout from the current login.

The Telnet Utility

- Many times you would be in need to connect to a remote Unix machine and work on that machine remotely.
- Telnet is a utility that allows a computer user at one site to make a connection, login and then conduct work on a computer at another site.
- Once you are login using telnet, you can perform all the activities on your remotely connect machine.

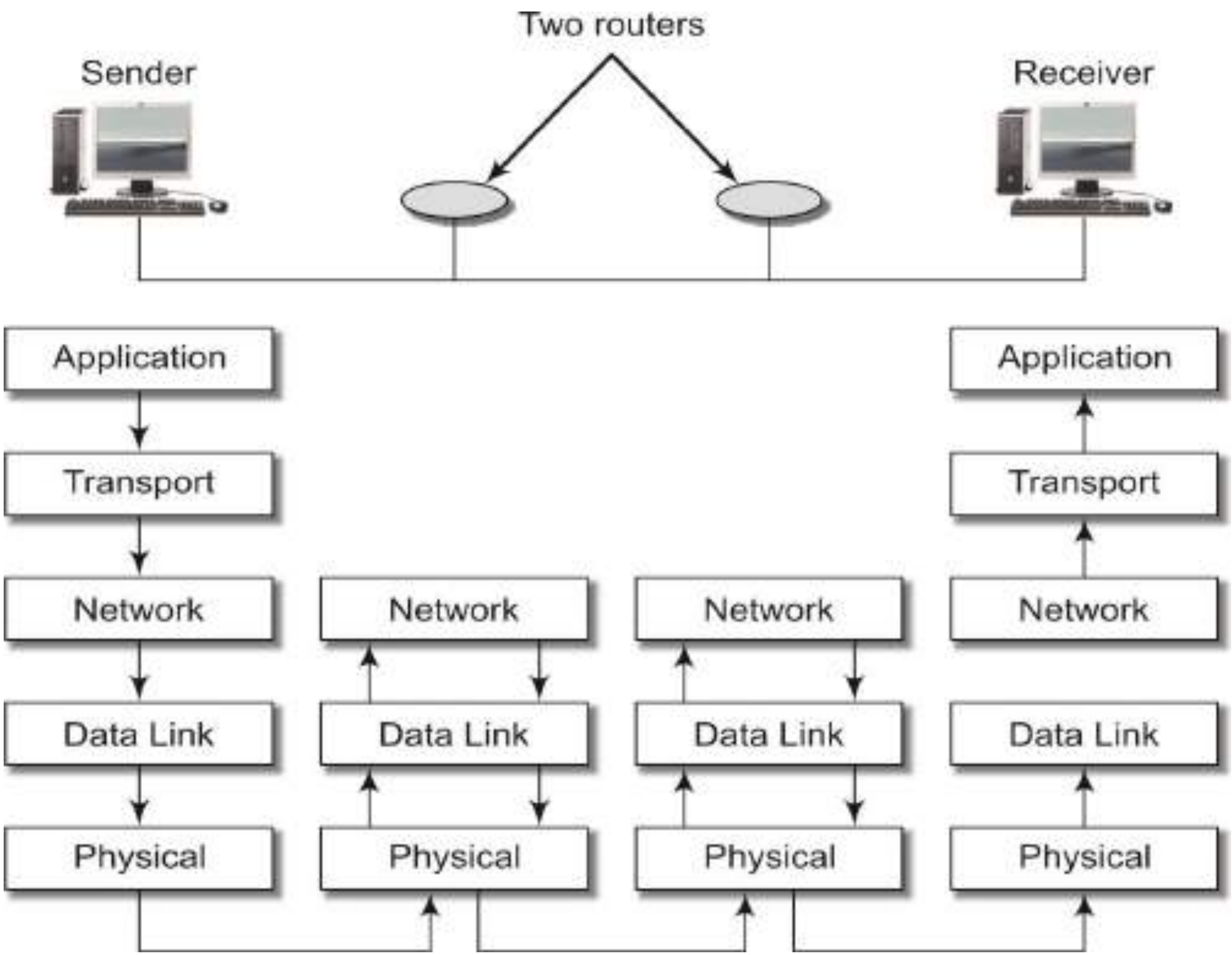
Welcome to Questions…

- Thank You.

Chapter 2: Layered Architecture, Network classification & Applications

Dr. Bhargavi Goswami
Department of Computer Science
Garden City College of Science & Management Studies.
bhargavi.goswami@gardencitycollege.edu
9426669020

Approaches to Network Design: TopDown Approach



DEFINITION

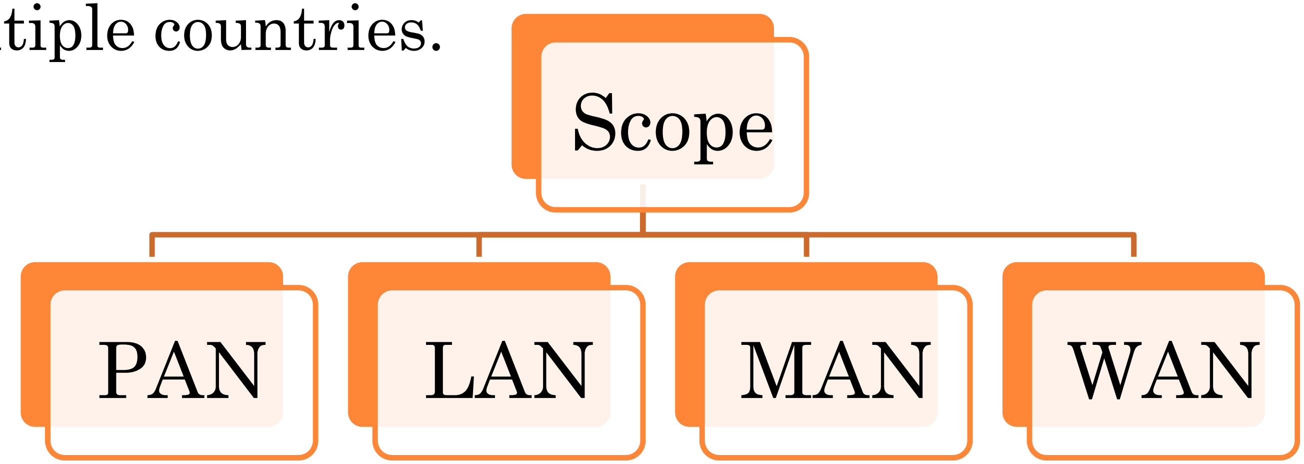
- *A computer network can be defined as a collection of computing devices (nodes) interconnected by wires or wireless means and governed by a set of standards (protocols) in order to share data and resources.*

Categorize networks based on multiple factors

1. *Division based on Scope*
2. *Division based on Connection*
3. *Division based on Communication*
4. *Division based on Usage*

1. Division based on scope

- PAN or Personal Area Network or the wireless version WPAN (Wireless PAN)
- LAN or Local Area Network which is usually confined to a moderately large building.
- MAN or Metropolitan Area Network which is confined to a city or a part of it.
- WAN or Wide Area Network which can span multiple countries.



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	Local area network
1 km	Campus	Local area network
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	Wide area network
10,000 km	Planet	The Internet

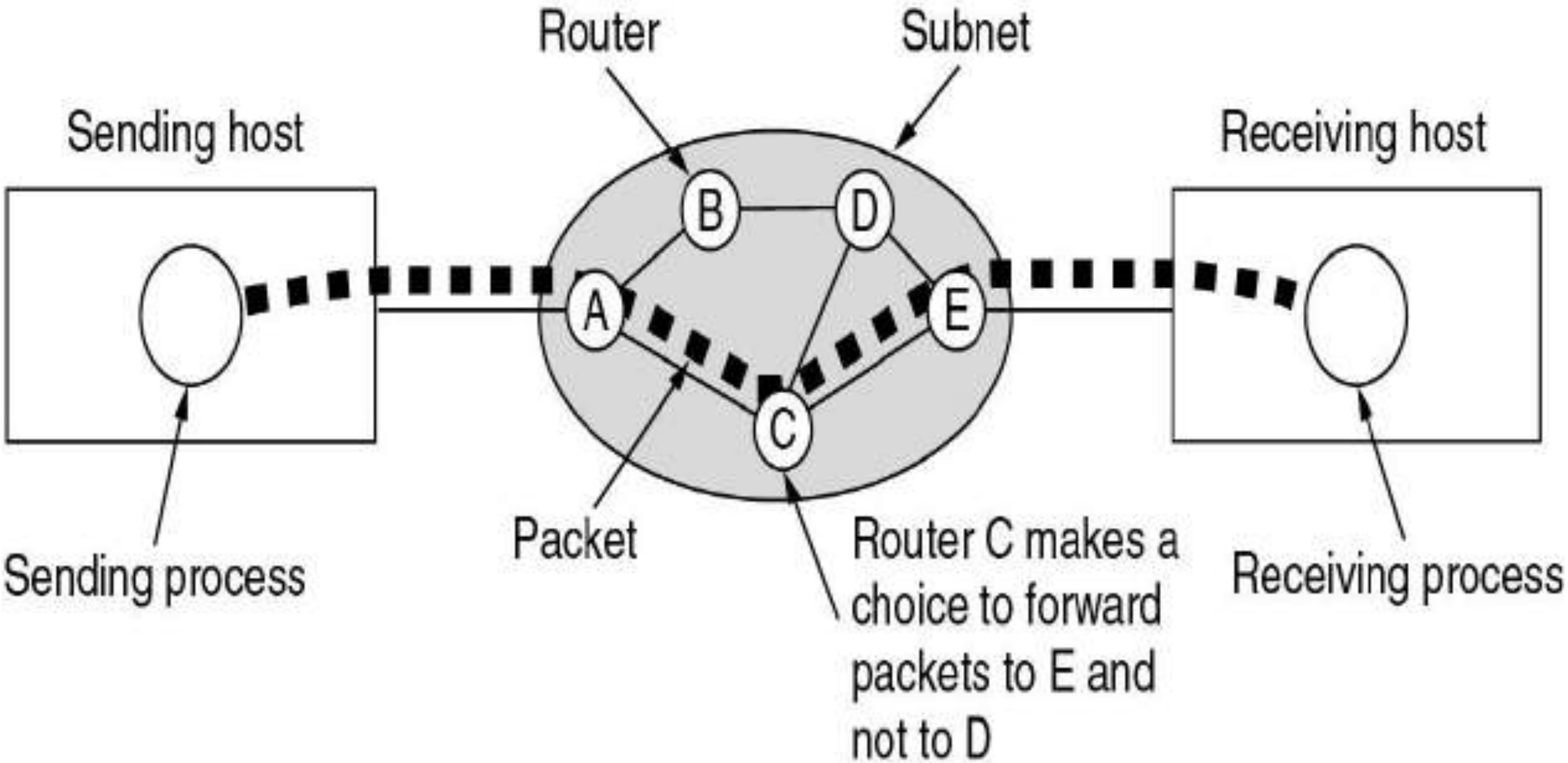
Two important mechanisms

Store & Forward

- What if congestion exist for line where packet is to be sent? Router stores that packet until congestion is resolved and once resolved, it forwards packets to that line. This is called Store & Forward Subnet.

Packet Switched Subnet

- A stream of packets from sender to receiver. Packets follow route ACE, rather than ABDE or ACDE. Some n/w predetermine route that is to be followed. First decision is taken by A with the help of some routing algorithm and then by C. All WANs are not packet switched. See next figure.



Router
Subnet
Sending host
Receiving host
B
D
A
E
C
Packet
Sending process
Router C makes a choice to forward packets to E and not to D
Receiving process

2. Division Based on Connection

Wired

- Need some sort of cables for connectivity.
- Most popular are UTP (Unshielded Twisted Pair) and Fiber Optics.
- Fast Ethernet provides 100MB/s, Gigabit Ethernet provides 1Gbps/s, 10G provides 10Gbps/s and 40/100G would come to Indian market soon.
- Fiber Optics provides nearly 5000 Times more bandwidth of conventional telephone cables.

Wireless

- First wireless network was ALOHA.
- Ethernet is successor of ALOHA.
- Other networks like Wi-Fi (802.11), Wireless Fidelity providing LAN Interpretability is widely accepted wireless networks.
- WiMax (802.16) wireless microwave access is covering large area of entire city.

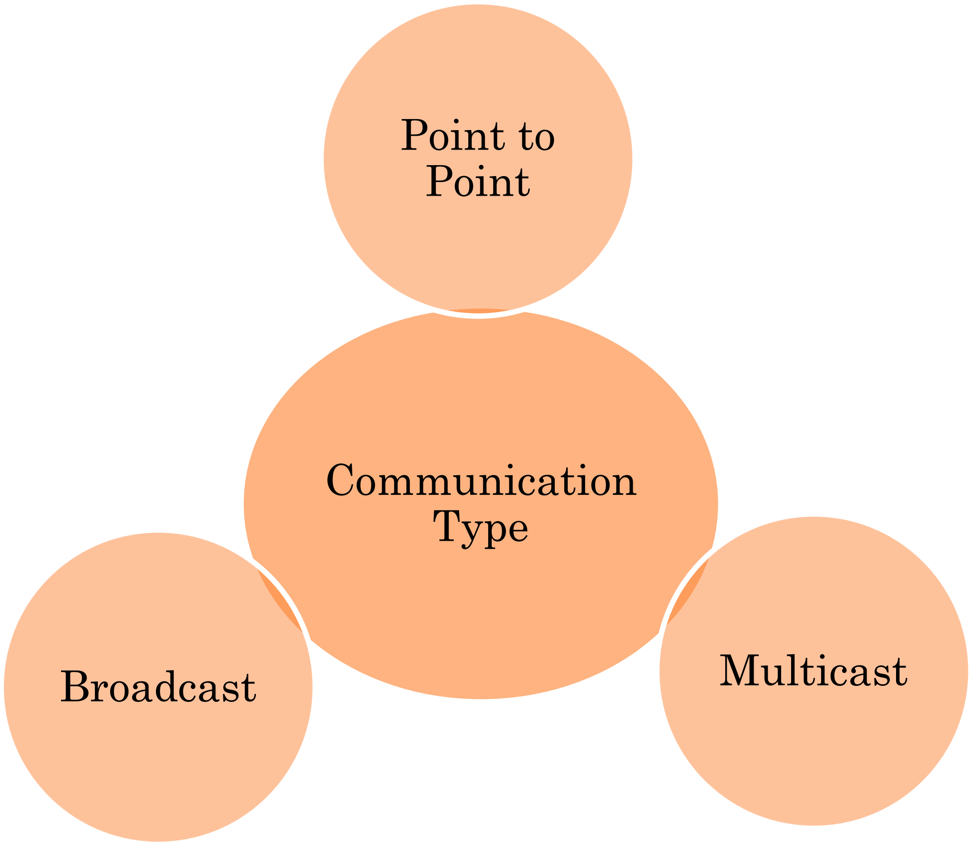
MANETS

- i) MANets:
- Mobile Ad Hoc Networks
- Nodes can come and join at their own will and leave on their own will.
- Services Provided are as follows:
  - One can access internet from hotel by joining hotel network
  - One can join network of railway station with session of 15 minutes
  - Student can access network of college from parking area or lobby
  - We can use internet during flight n share the files with co-passengers.
  - Students can exchange class notes without writing it manually.
- Issues in MANets:
  - Topology is dynamic
  - Power Consumption is important concern for mobile nodes. When A is communicating with C through intermediate node B, if the battery of B is low, it would not forward packets of A to C.
  - Security must be more stringent with such networks as we expect guest to join the network any time.
  - **War Driving**: It is a common Mechanism deployed by hackers to join wireless networks and extract information that is vital. This process is described as War Driving.

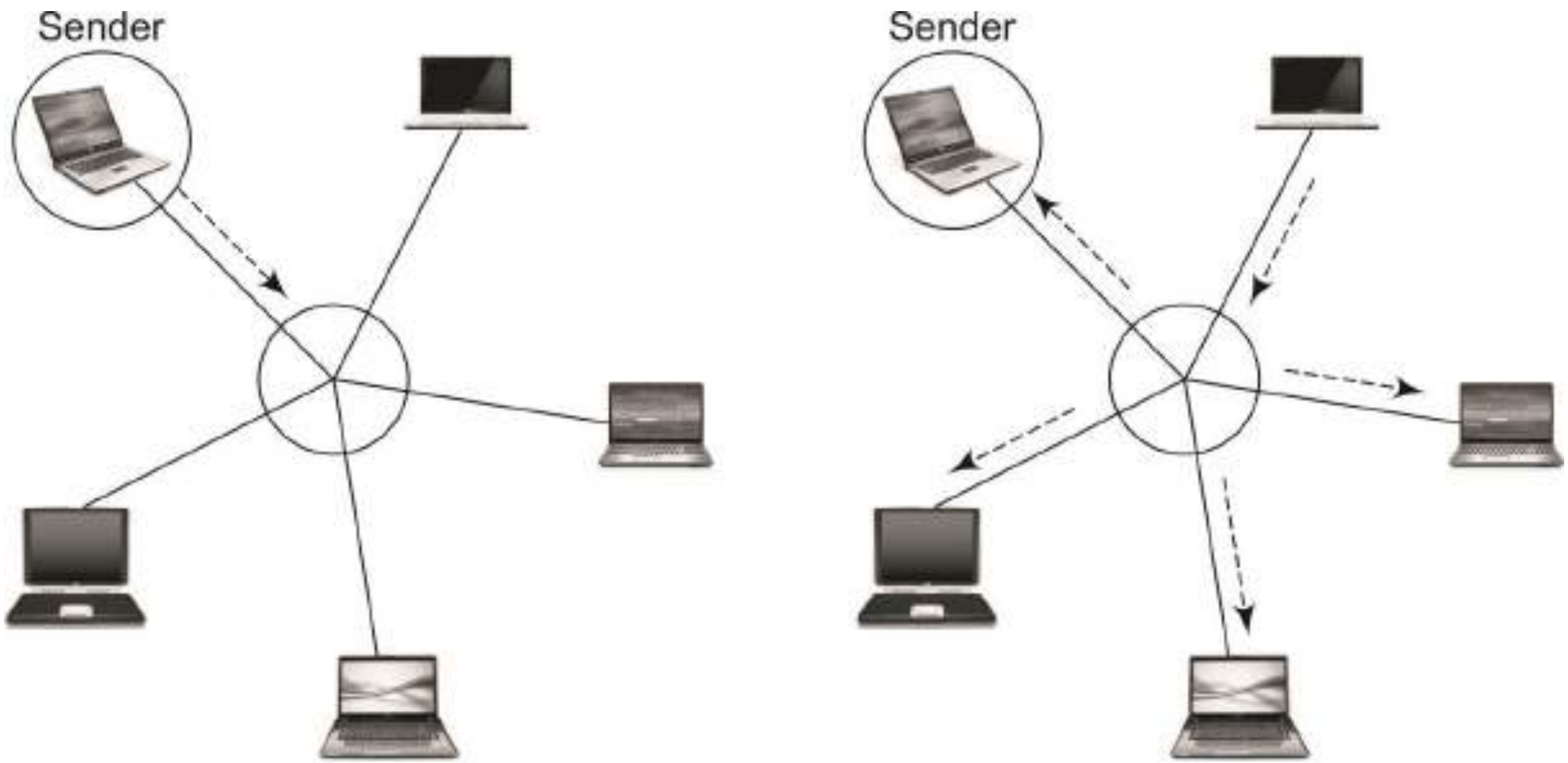
SENSORS

- <u>ii) Sensor Networks:</u>
- Sensor Networks are special type of Ad Hoc Networks, where the members of this network are tiny sensors rather than mobile computers or large devices.
- Sensors are sometimes mobile and sometimes stationary.
- Eg. Temperature Sensors detect temperature and sends it to some other nodes.
- Sensors are designed with much less memory and processing power is also too small.

3) Division Based on Communication Type



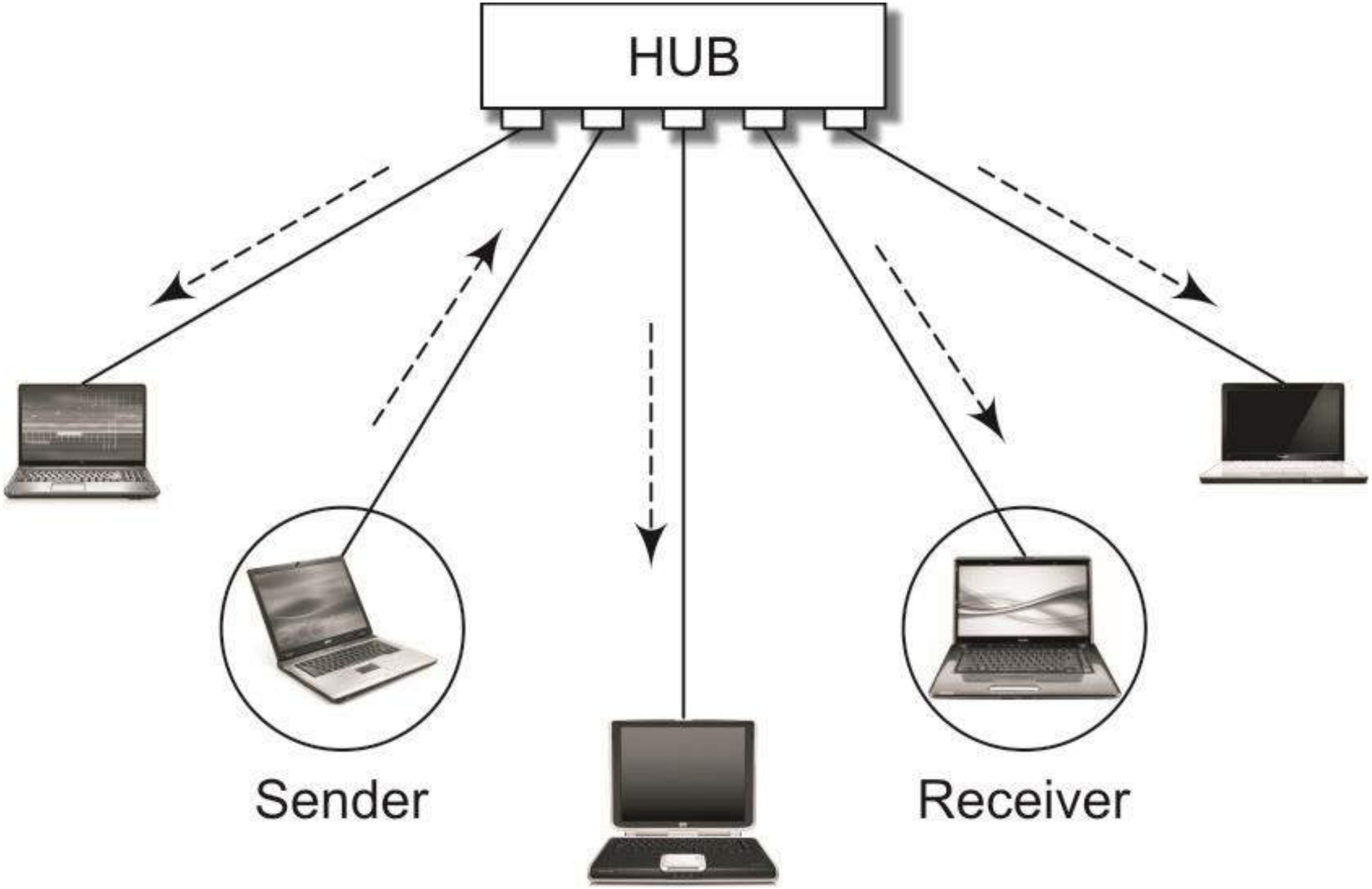
BROADCAST



Broadcast network 1 : Sender sends

Broadcast network 2 : Everybody including intended recipient as well as sender receives the packet

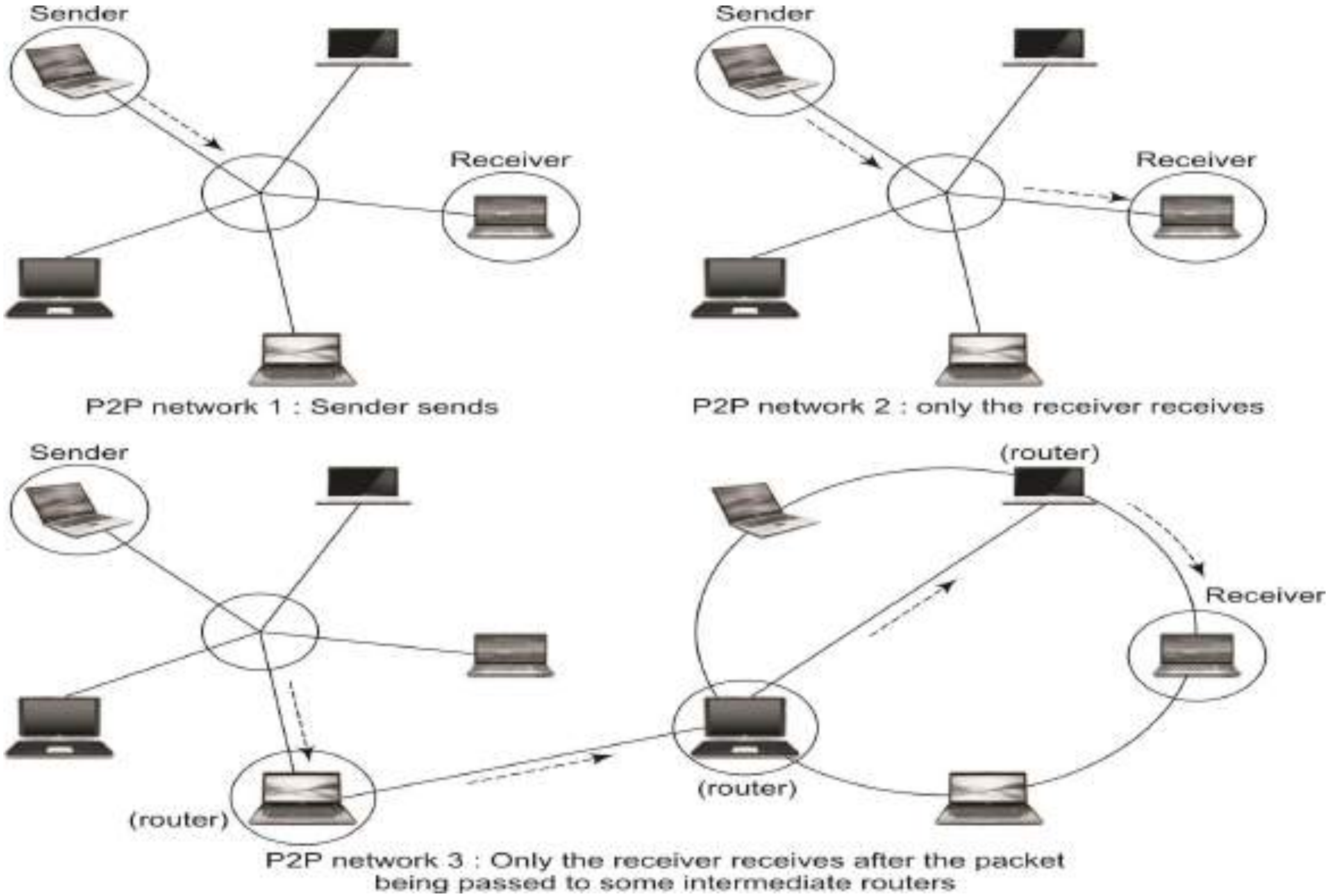
BROADCAST



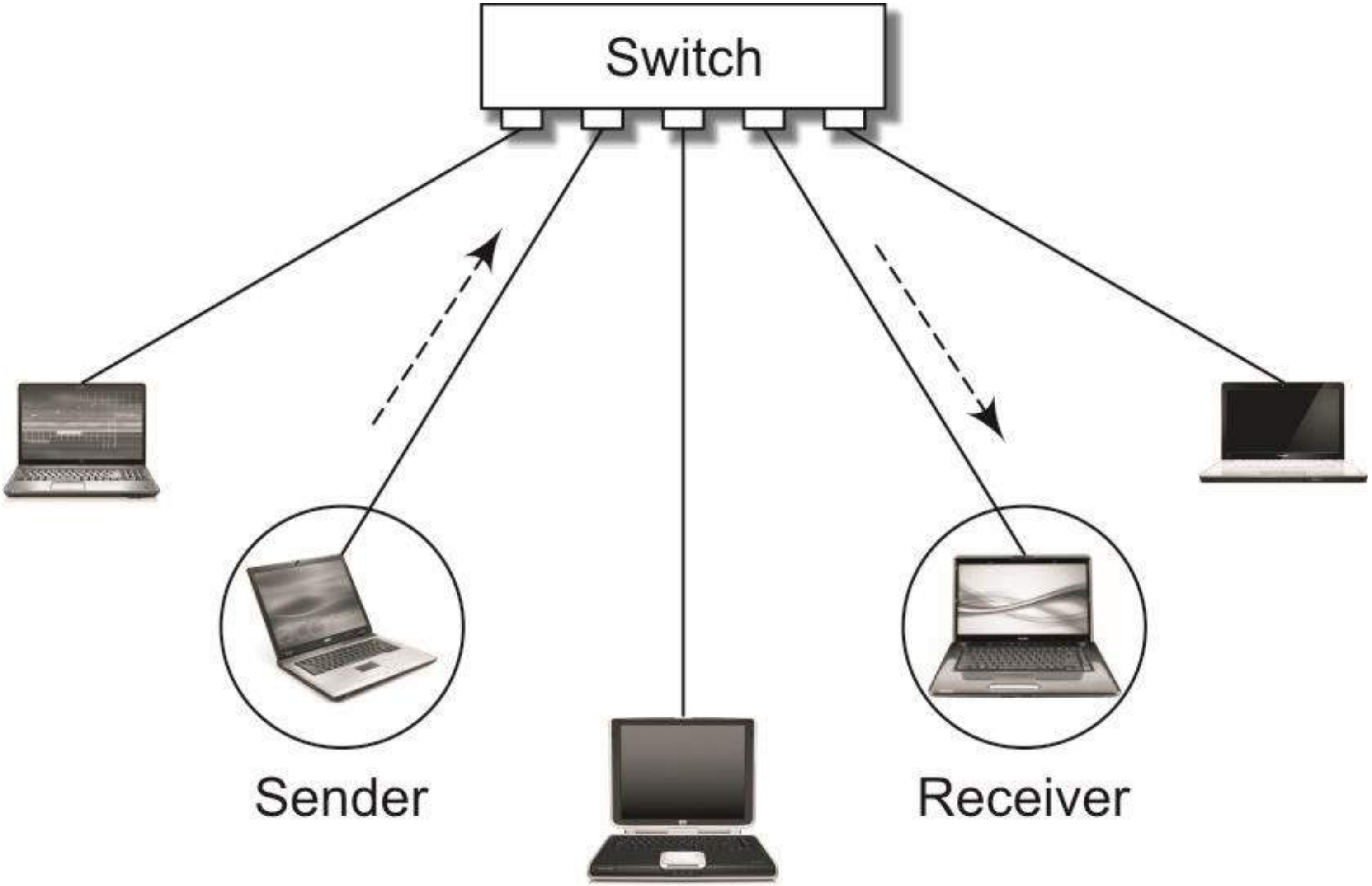
BROADCAST

- Better when a very low probability of more than one user transmitting simultaneously
- It is useful when the network is inherently a broadcast network.
- Better when routing through neighbours or addressing each node of the network is not required
- Broadcasting helps when the topology is not fixed.

Point to point



Point to point



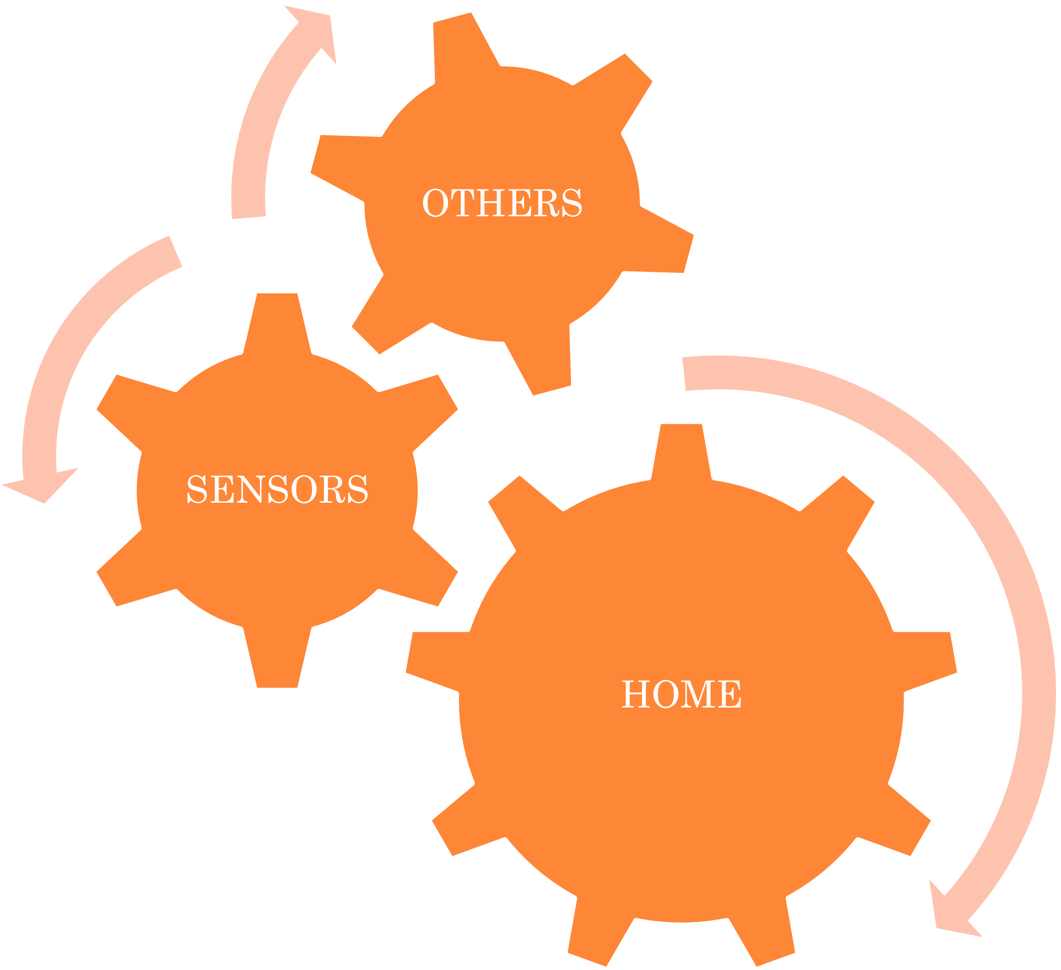
Point to point

- P2P requires to know where the recipient is
- Sender must know where each router is
- Similarly each router must be aware of where other routers are located
- For inherently broadcast network P2P communication is not possible.
- Little advantage for high bandwidth case

MULTICAST

- One sender, multiple receivers, but, not all.
- Switch is the device that provides this facility.

4. Division based on Usage



HOME NETWORKS

- Smart spectacles helps old people
- Smart Keys
- A phone receiver transfers the call automatically
- Control house via Internet or phone.
- The shower adjusts the temperature
- Single remote control for many home devices
- ISSUES:
- Robustness
- Cost
- Security issues
- Regular upgrades
- Maintenance and availability
- Wired or Wireless
- Holding the vendor responsible

Sensors

b) Sensor Networks:

- Used for specific purpose like monitoring a process or recording the outcomes of continuous experiment.
- What is the need of sensor networks?
  - Fire erupts in a warehouse in an industry can call fire brigade.
  - If sudden rainfall in Delhi (Bangalore always have rainfall) , can cause adverse effect to the farm, to what extent of humidity is there in the farm, can be determined by sensor networks
  - After the earthquake, building with sensors can monitor record vibration data to confirm that structure is safe to enter.
- Sensor networks have large number of nodes.
- Sensor networks have no fixed topology.
- Sensor nodes have less memory and processing power.
- Sensors are usually very small.
- Sensor can be immobile.
- Size, power and memory all, low.
- Sensor may not be individually addressable.
- Power consumption is crutial in Sensors
- Sensor nodes may captured, stolen.

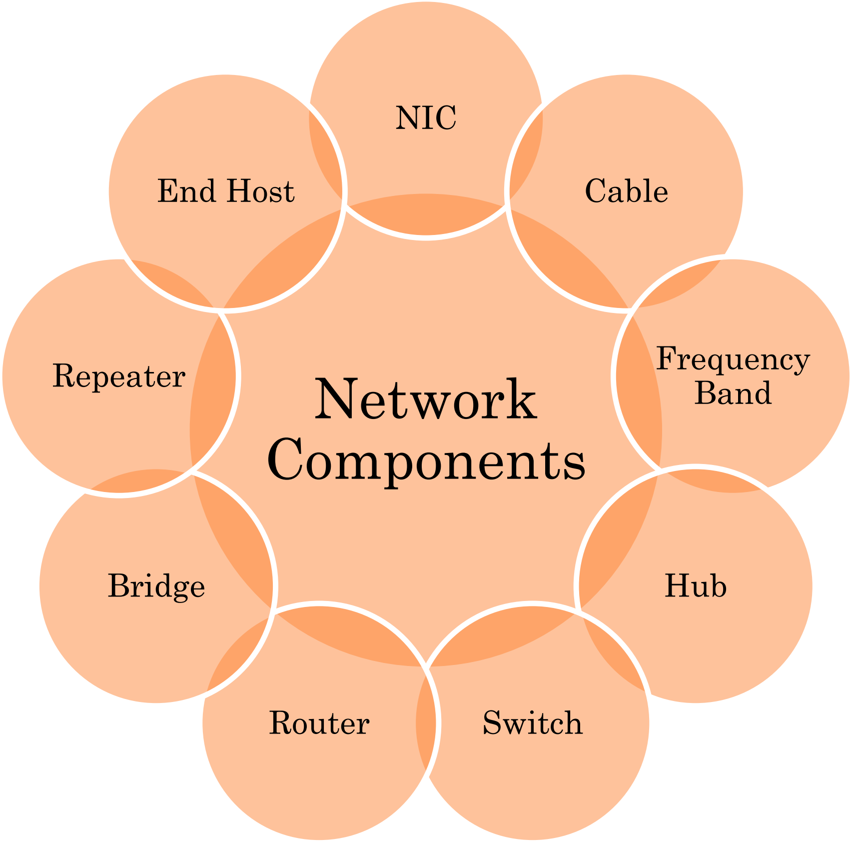
Other Networks

- Pervasive computing and research on wearable computers are helping.
- Pervasive networking means, if you are out on vacation, all the emails are copied to yr outlook and they are msged that u r on vacation.
- Wearable computers are those which can be worn on the body like a dress.
- Microprocessors are also the example for it.
- Passive Environment becomes Active: eg. U enter the room and light automatically switches on and light music starts playing.
- In today's scenario, toll booth have long queues. But if we have sensors, RFID can just pass by, all the details are recorded, and toll is deducted from the RFID card.
- Phones are used to check emails and computers answer the phone calls.

Network Components

- The Network Interface Card
- Cable for wired connection
- Frequency band for wireless transmission
- The servers and the nodes
- Interconnecting Devices

    i) Hub
    ii) Switch
    iii) Repeater
    iv) Bridge
    v) Router



Definitions

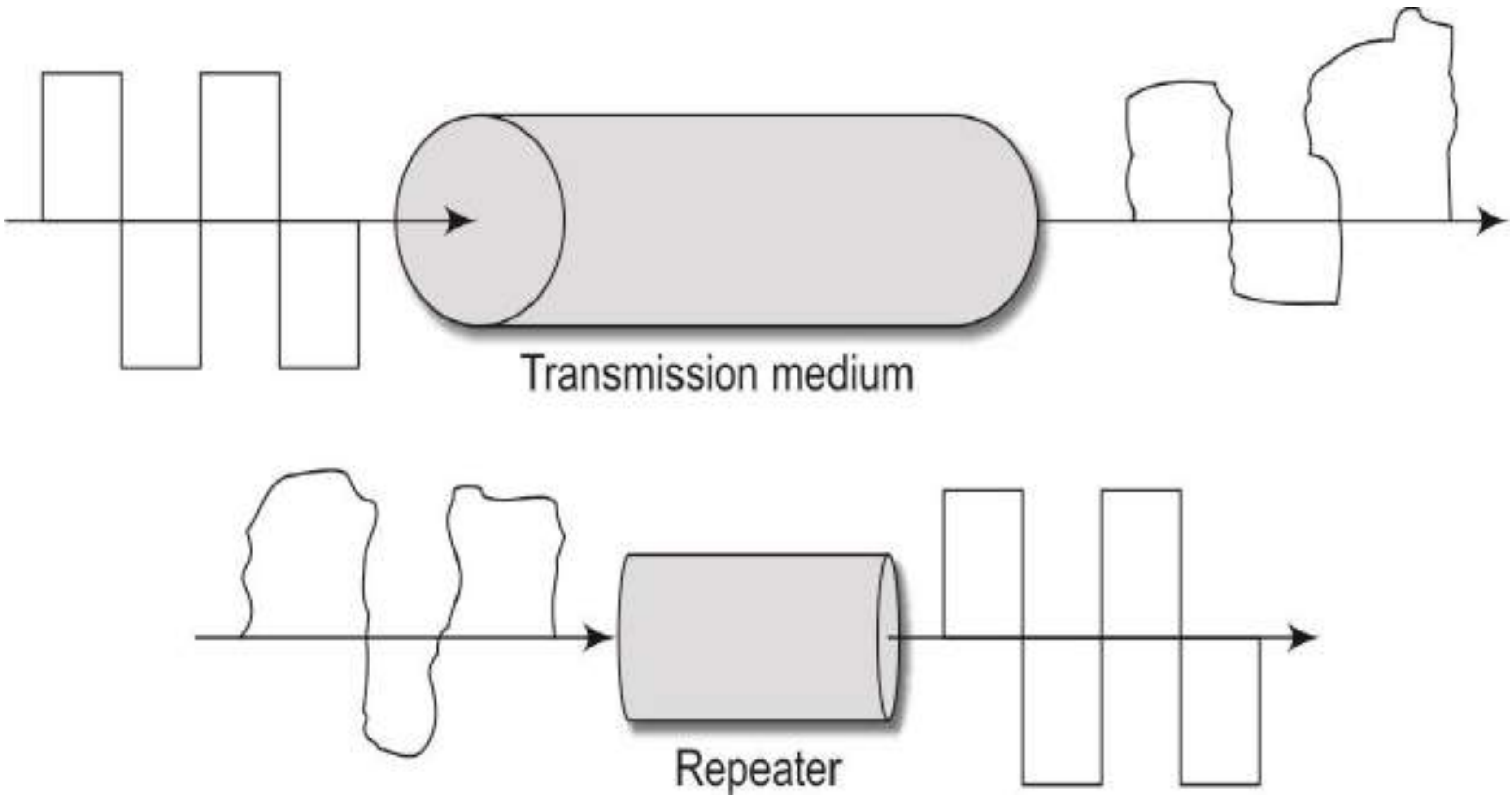
- <u>NIC</u>: The first requirement of connectivity at node's end is Network Interface Card NIC or LAN Card. Eg. Ethernet Card (Wired) and Centrino Card (Wireless).
- <u>Cables for Wired Communication</u>: There is a LAN cable slot in motherboard on which network cable fits. Cables can be for different types. Eg. UTP (Cat 3,5,6,7), Copper Cable (Thin and Thick) and Fiber Optics.
- <u>Frequency Band for Wireless Communication</u>: More the frequency more is the data rate. Rights has to be taken from Government of India, body DoT (Department of Telecommunication) to transmit data using frequency.
- <u>Servers and Nodes</u>: Networking machine in networking parlance is known as a node or host. We have LAN card and wire to connect. Nodes giving service is server and nodes demanding service is client.

DEFINITIONS

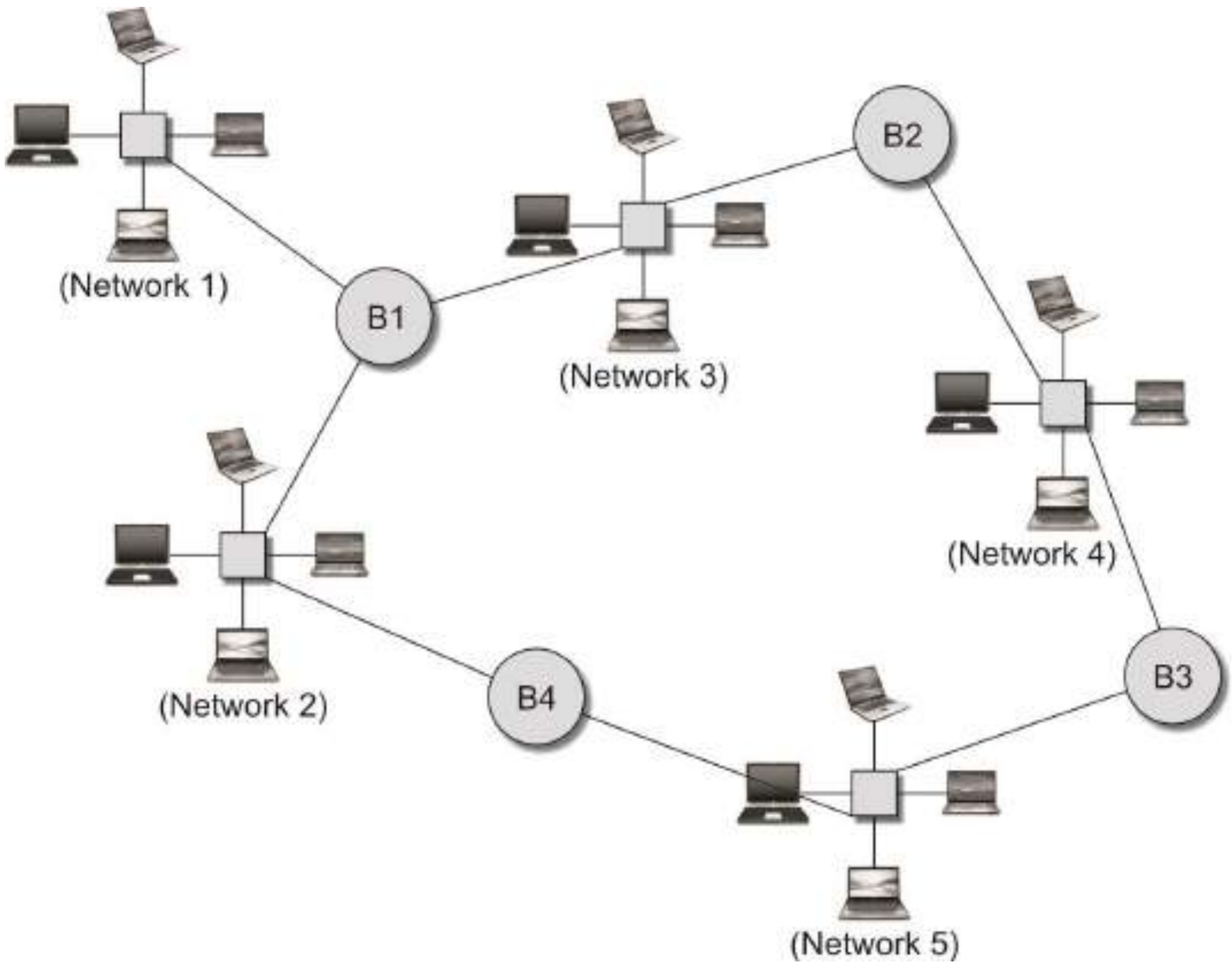
- Interconnecting Devices: It's not possible to get connected to every client directly. So we need some interconnecting device that connects each of us.
- Hub: A Hub is an intermediate device that connects to server with its clients through wires. It has multiple ports. It is broadcast by nature. Impose network load as do not store addresses of communicating clients to its memory.
- Switch: Switch is an interconnecting device that supports P2P communication in a local network. Switch stores the information of its connected nodes in its buffer so that it can utilize it for point to point communication. It reduces network load.

Definitions

- Repeater: Signal's strength reduces gradually by covering the distance. The device that reshapes the digital signal is called a repeater. For this, Amplifiers are needed by analog signals. Repeaters also remove noise from the digital signals which is not done by amplifiers for analog signals.
- Bridge: Special device called bridge is used to connect more networks. A bridge is similar to switch but is designed to provide additional services like broadcasting in a particular LAN segment, finding out the shortest path between different LAN segments. A bridge keeps broadcast in network limited to that network only. It keeps, logically separate segments physically separate. Bridge operates upon Data Link Layer.



Transmission medium
Repeater



(Network 1)
B1
B2
(Network 3)
(Network 4)
(Network 2)
B4
B3
(Network 5)

DEFINITIONS

- Router: A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. A router may create or maintain a table of the available routes and their conditions and use this information along with distance and cost algorithms to determine the best route for a given packet.
- Gateway: Gateways are conventionally used to connect the networks. It operates on higher layers like transport layer and application layer. It provide an application seamless access to remote networks. Eg. Proxy Server. Two types of gateways are there. 1) Transport gateway: connect two computers using different connection-oriented transport protocols (TCP, ATM). 2) Application gateway: translate format and contents of data. E.g., email gateway: translate Internet message into SMS for mobile phones.

Need For Protocol Architecture

- data exchange can involve complex procedures, cf. file transfer example
- better if task broken into subtasks
- implemented separately in layers in stack
  - each layer provides functions needed to perform comms for layers above
  - using functions provided by layers below
- peer layers communicate with a protocol

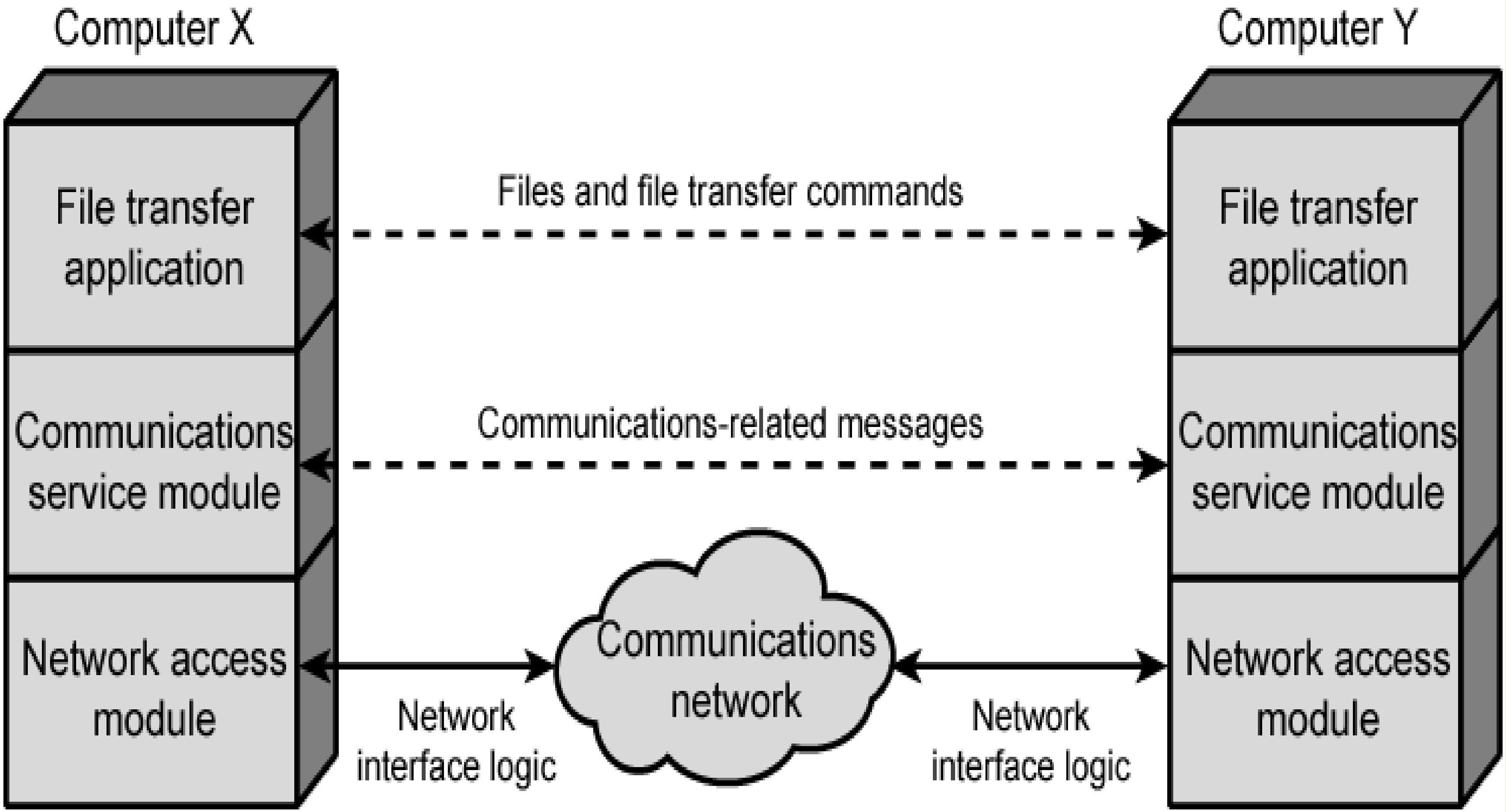
Key Elements of a Protocol

- syntax - data format
- semantics - control info & error handling
- timing - speed matching & sequencing

TCP/IP Protocol Architecture

- developed by US Defense Advanced Research Project Agency (DARPA)
- for ARPANET packet switched network
- used by the global Internet
- protocol suite comprises a large collection of standardized protocols by the Internet Activities Board (IAB).

Simplified Network Architecture



TCP/IP Layers

- no official model but a working one
  - Application layer
  - Host-to-host, or transport layer
  - Internet layer
  - Network access layer
  - Physical layer

Physical Layer

- concerned with physical interface between computer and network
- concerned with issues like:
  - characteristics of transmission medium
  - signal levels
  - data rates
  - other related matters

Network Access Layer

- exchange of data between an end system and attached network
- concerned with issues like :
  - destination address provision
  - invoking specific services like priority
  - access to & routing data across a network link between two attached systems
- allows layers above to ignore link specifics

Internet Layer (IP)

- routing functions across multiple networks
- for systems attached to different networks
- using IP protocol
- implemented in end systems and routers
- routers connect two networks and relays data between them

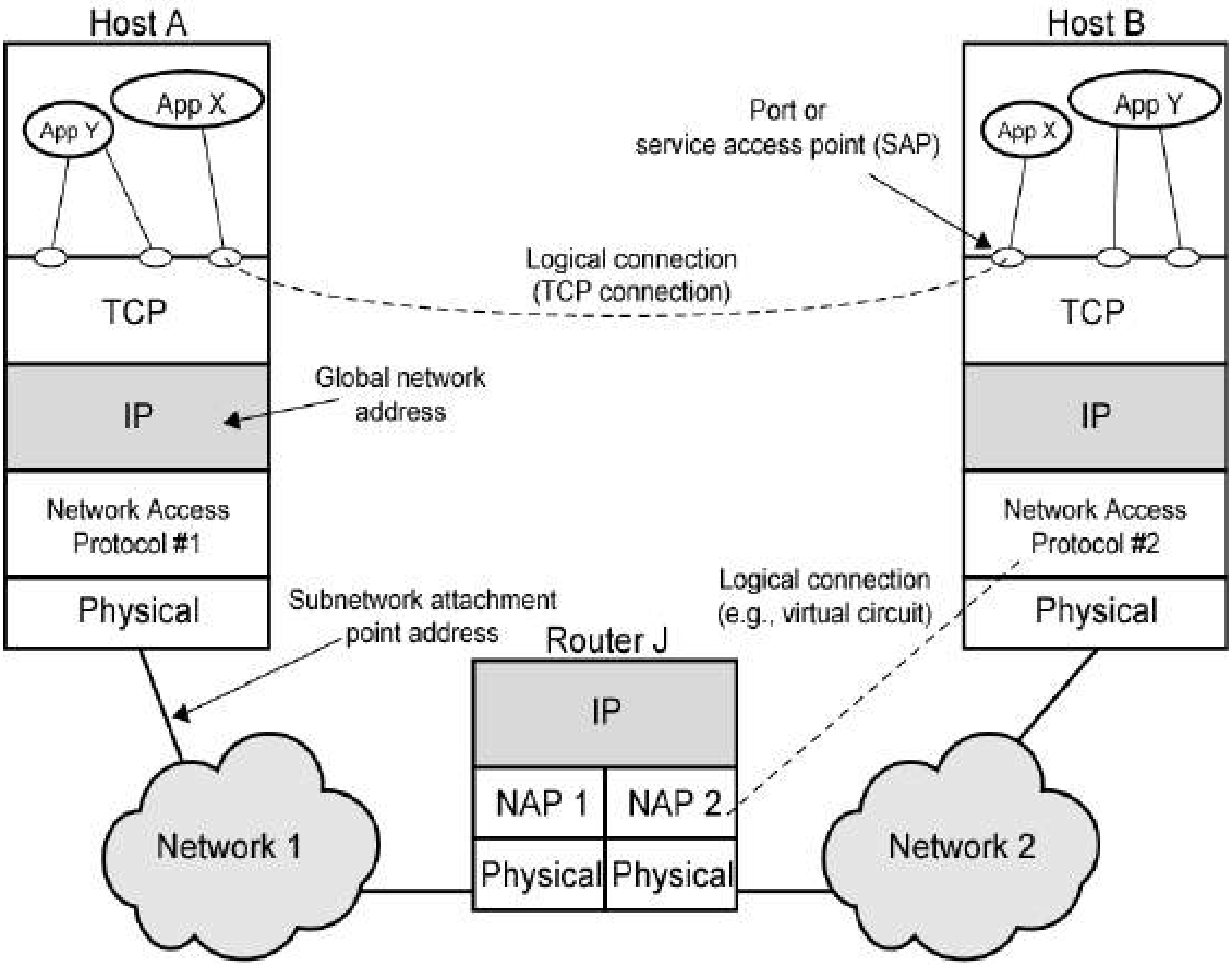
Transport Layer (TCP)

- common layer shared by all applications
- provides reliable delivery of data
- in same order as sent
- commonly uses TCP

Application Layer

- provide support for user applications
- need a separate module for each type of application

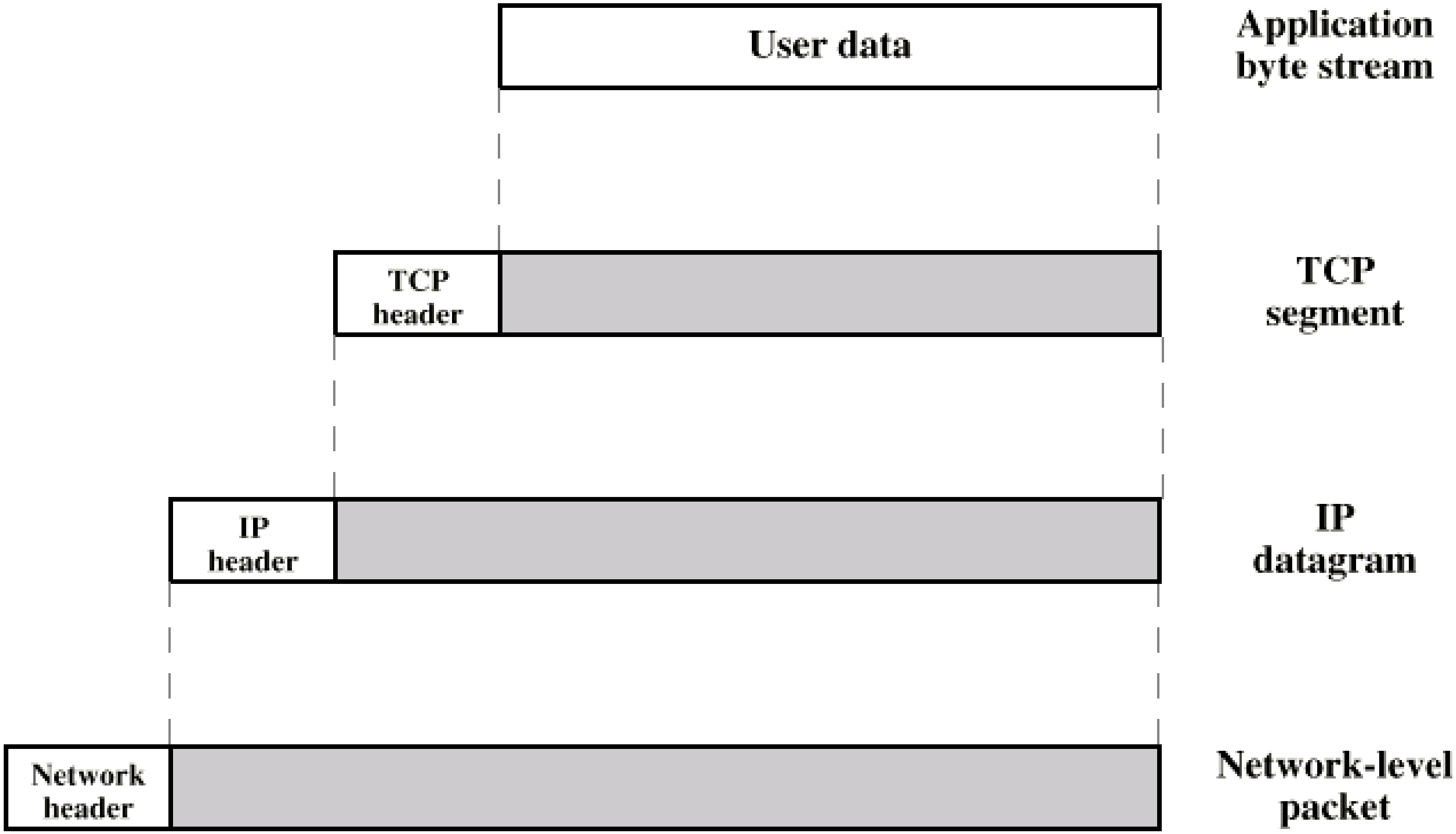
Operation of TCP and IP



Addressing Requirements

- two levels of addressing required
- each host on a subnet needs a unique global network address
  - its IP address
- each application on a (multi-tasking) host needs a unique address within the host
  - known as a port

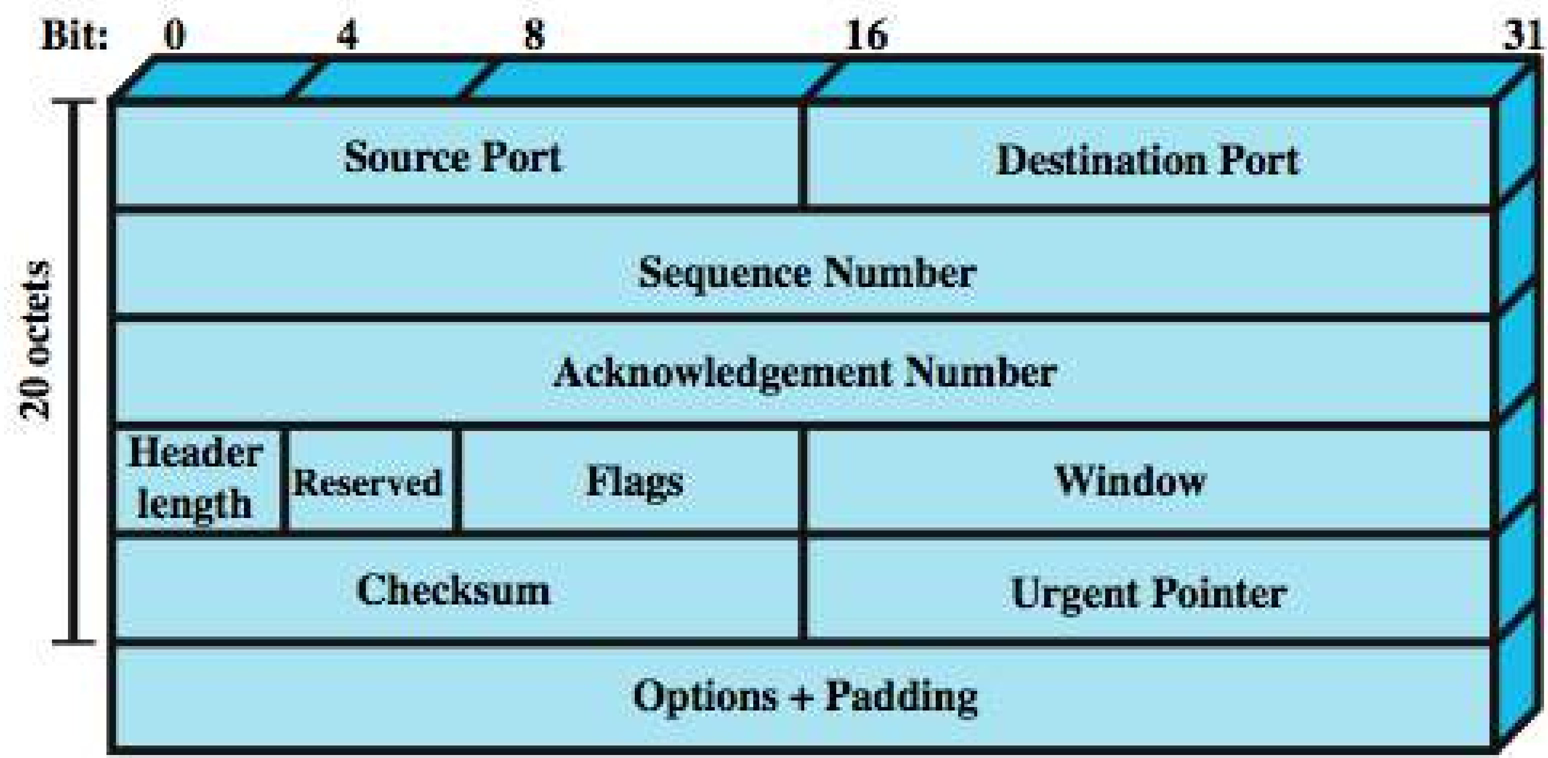
Operation of TCP/IP



Transmission Control Protocol (TCP)

- usual transport layer is (TCP)
- provides a reliable connection for transfer of data between applications
- a TCP segment is the basic protocol unit
- TCP tracks segments between entities for duration of each connection

TCP Header

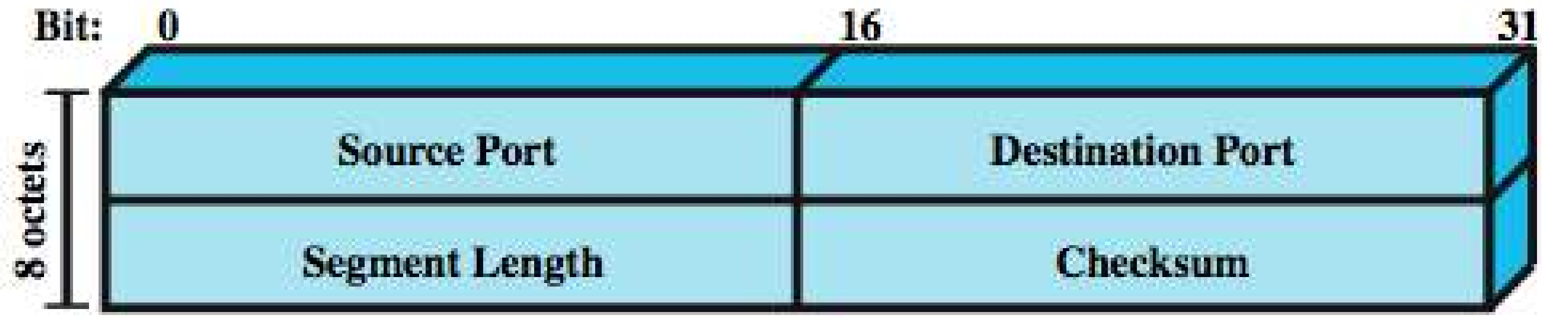


(a) TCP Header

User Datagram Protocol (UDP)

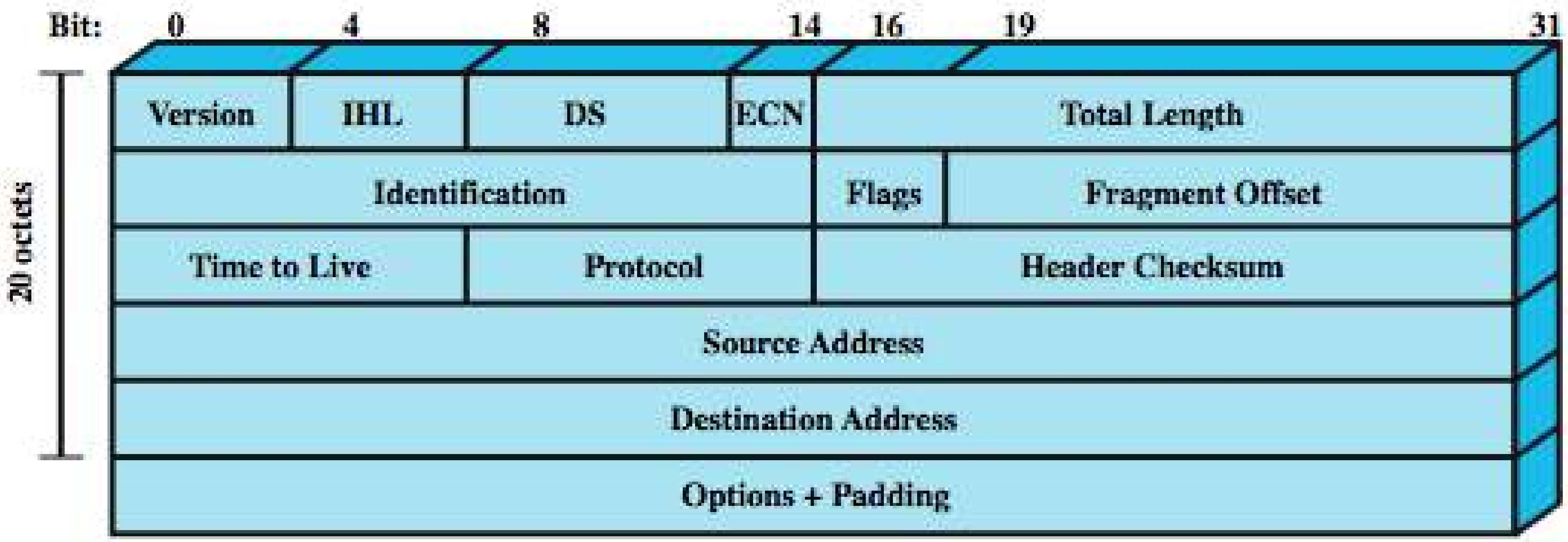
- an alternative to TCP
- no guaranteed delivery
- no preservation of sequence
- no protection against duplication
- minimum overhead
- adds port addressing to IP

UDP Header



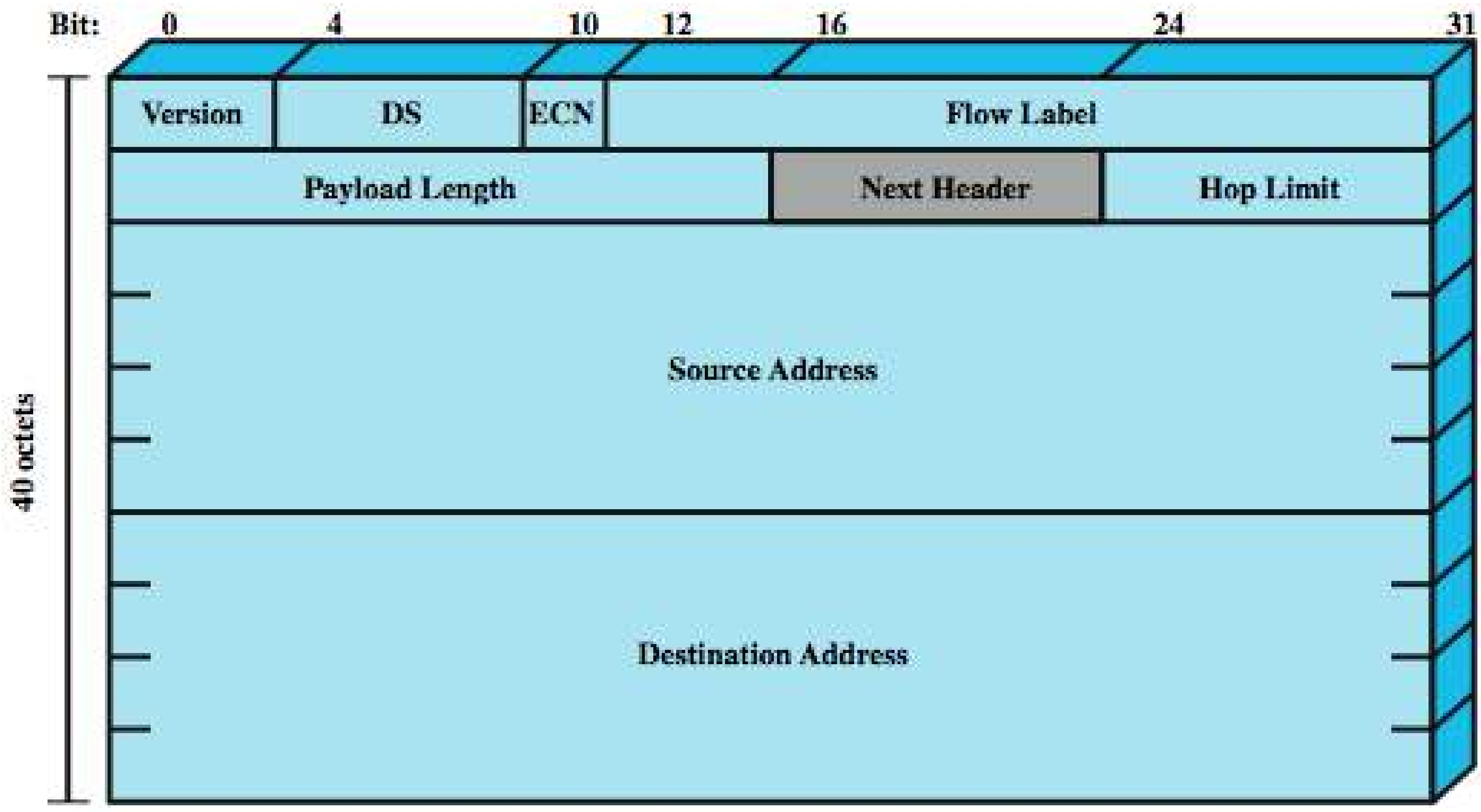
(b) UDP Header

IP HEADER



(a) IPv4 Header

IPv6 Header

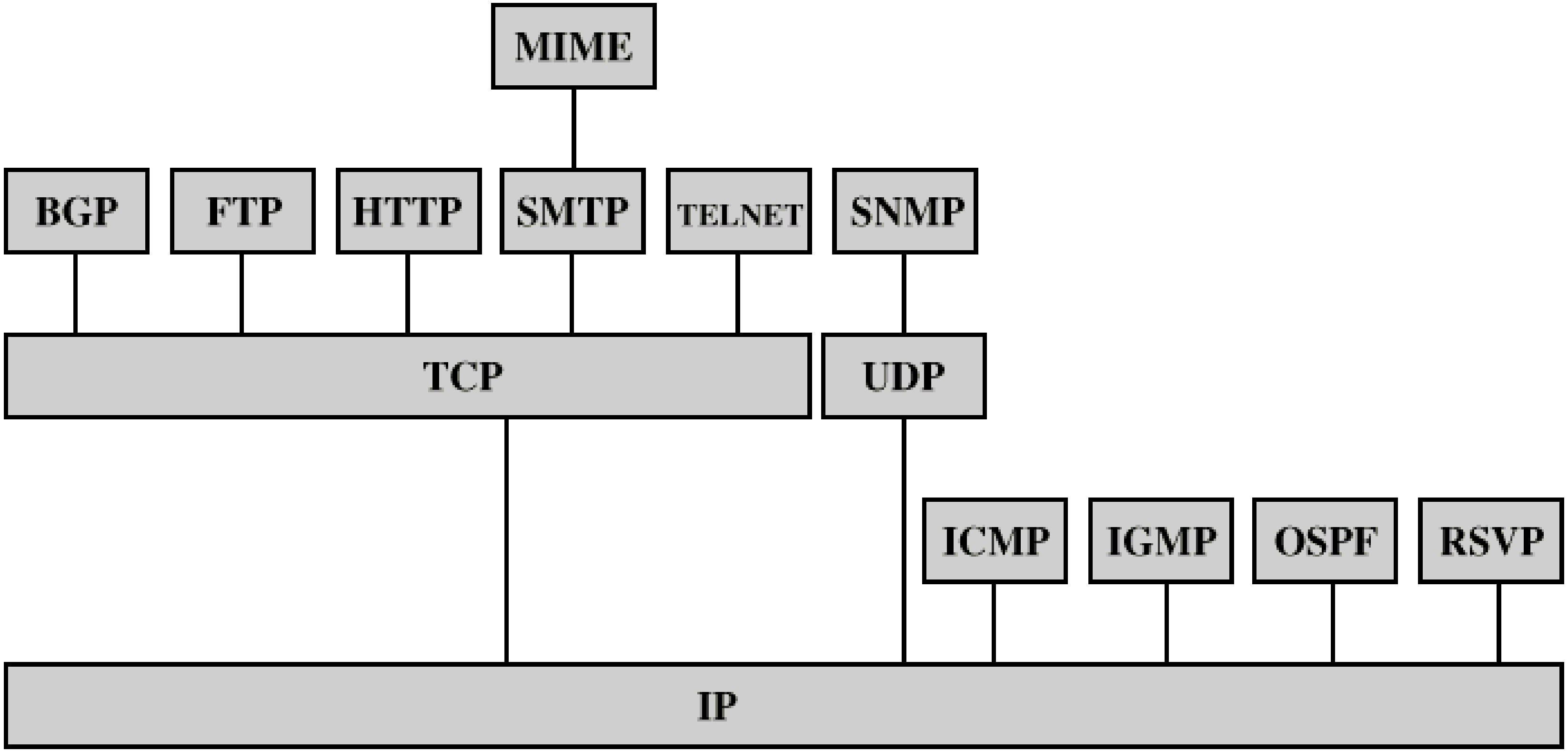


(b) IPv6 Header

TCP/IP Applications

- have a number of standard TCP/IP applications such as
  - Simple Mail Transfer Protocol (SMTP)
  - File Transfer Protocol (FTP)
  - Telnet

Some TCP/IP Protocols



BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

TCP/IP Protocol Suit

Layer	Protocols
Application Layer	Telnet, FTP, SMTP, DNS, HTTP, SNMP
Transport Layer	TCP, UDP
Internet Layer	ARP, RARP, IP, IPSEC, ICMP, IGMP
Network Access Layer	Ethernet, Token Ring, Frame Relay, ATM

OSI

- Open Systems Interconnection
- developed by the International Organization for Standardization (ISO)
- has seven layers
- is a theoretical system delivered too late!
- TCP/IP is the de facto standard

OSI Layers

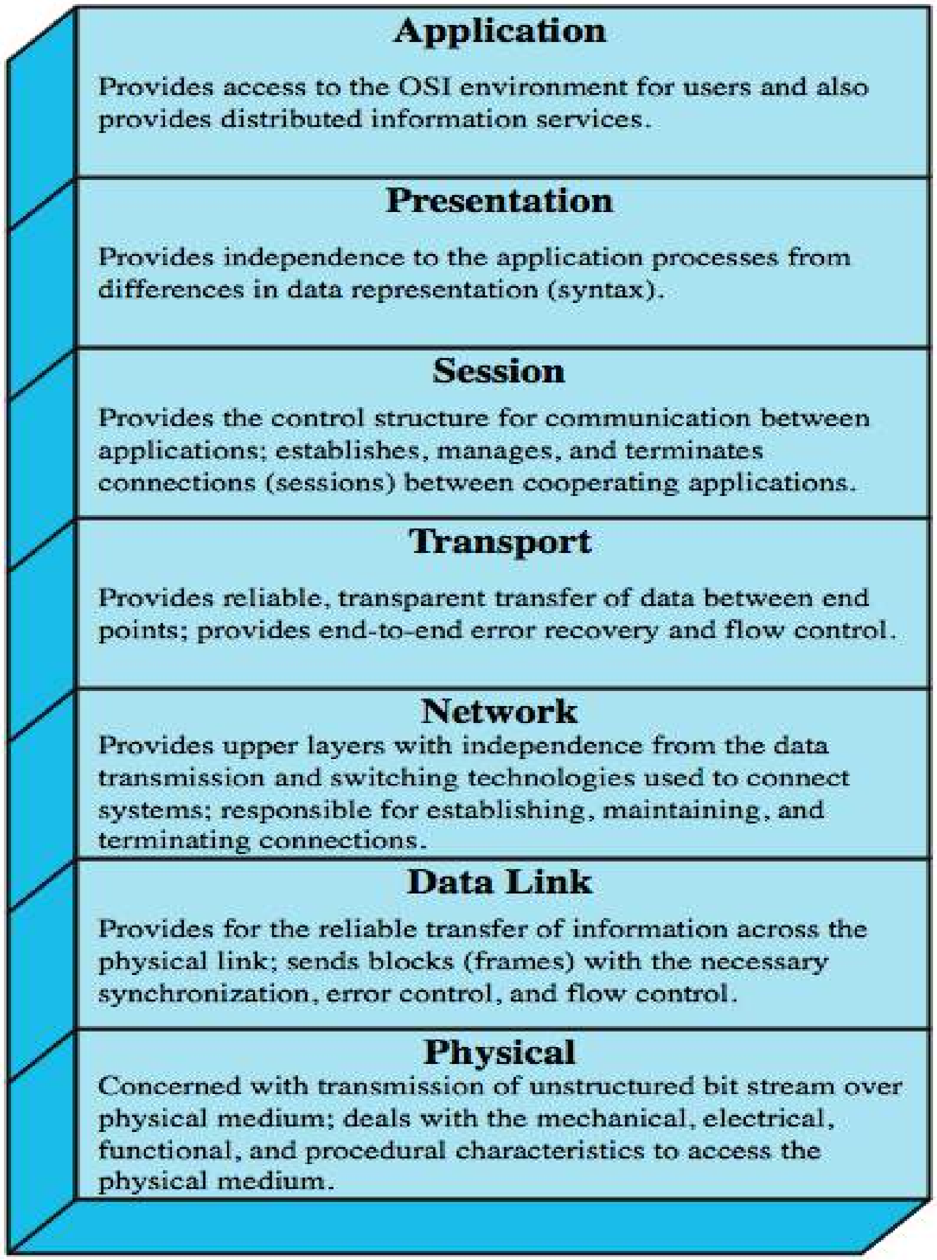
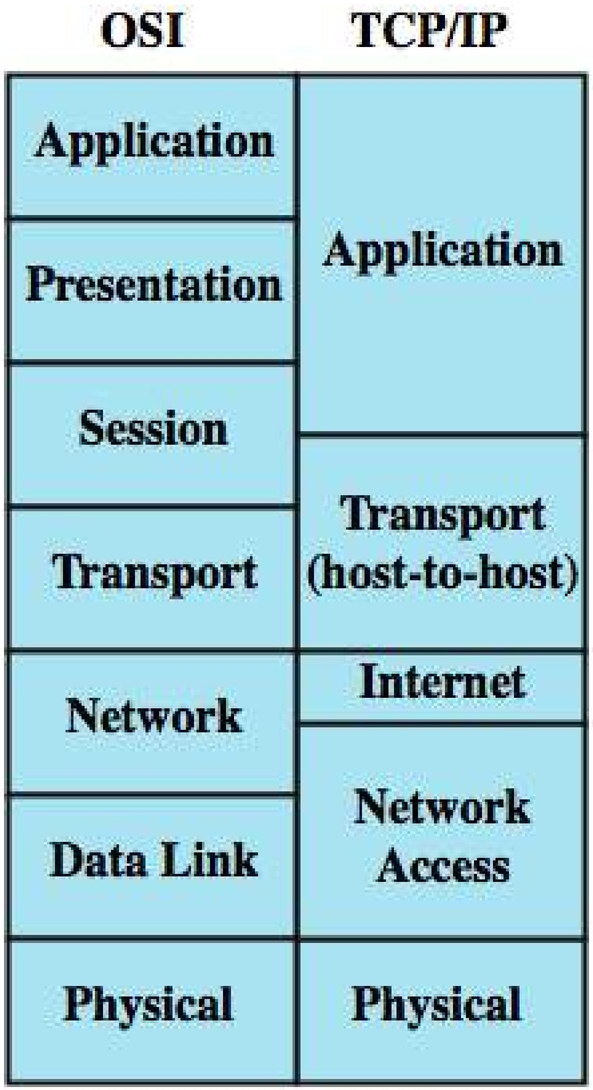
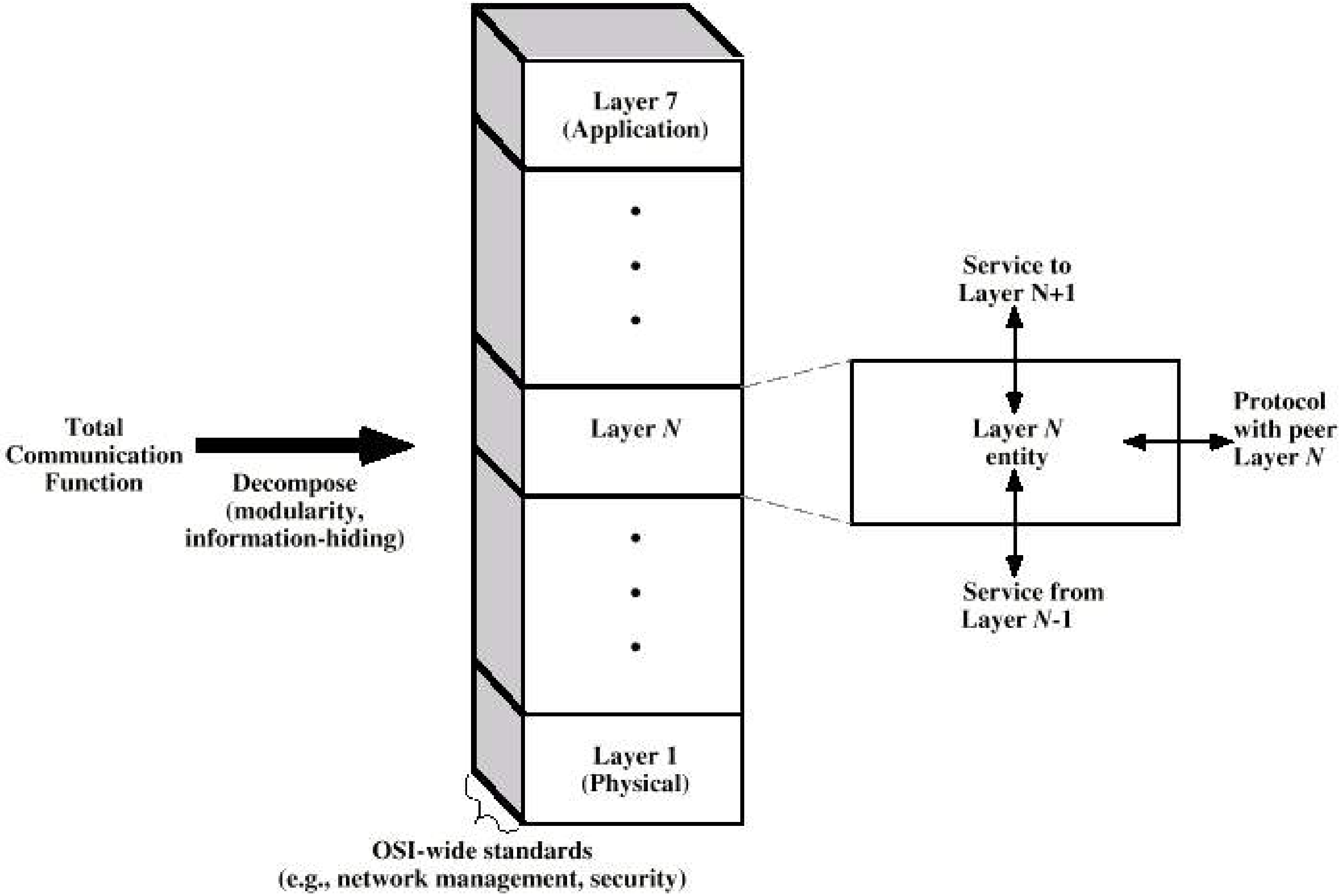


Figure 2.6 The OSI Layers

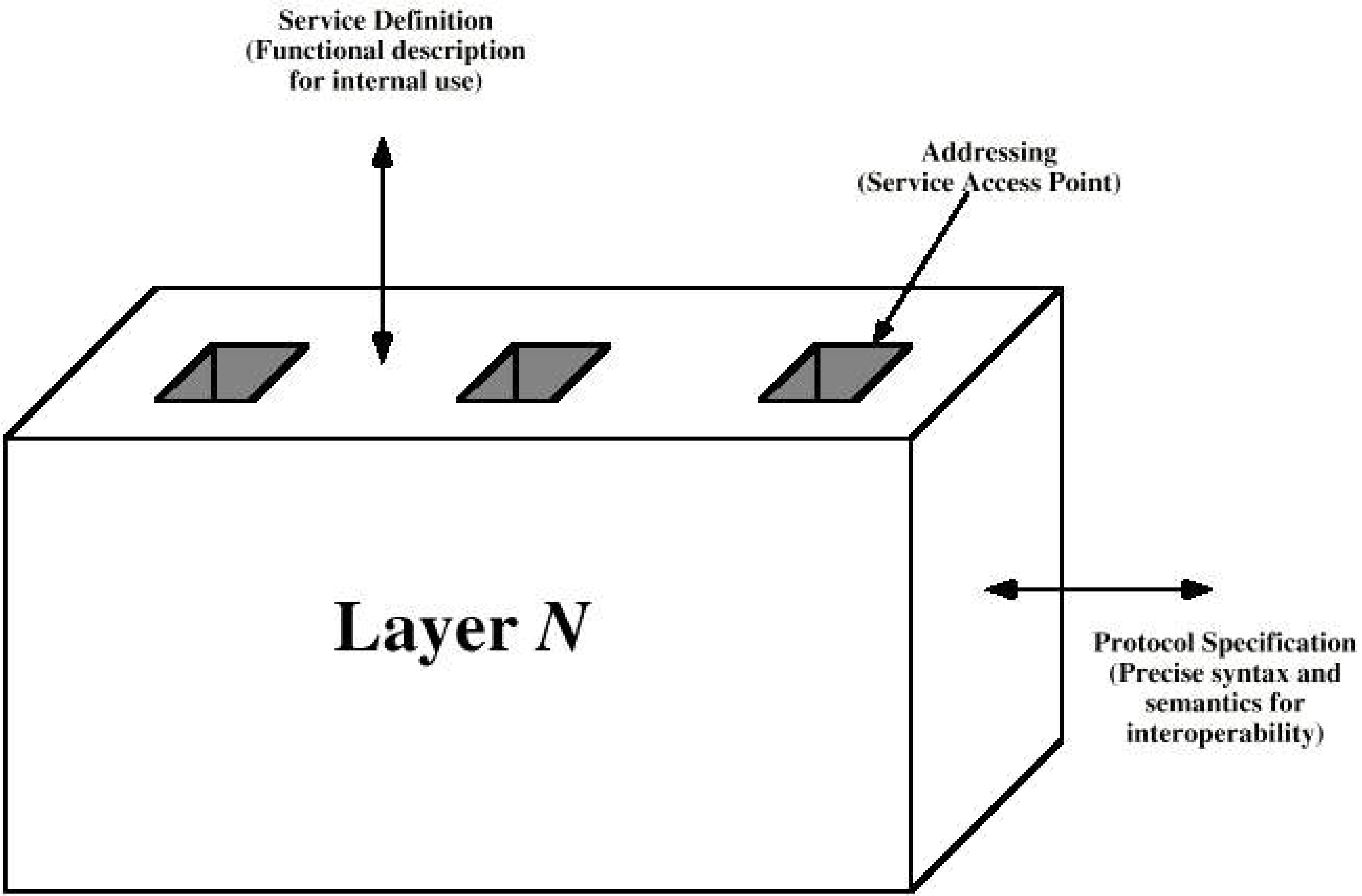
OSI v TCP/IP


OSI
TCP/IP
Application
Presentation
Session
Transport
Network
Data Link
Physical
Application
Transport
(host-to-host)
Internet
Network
Access
Physical

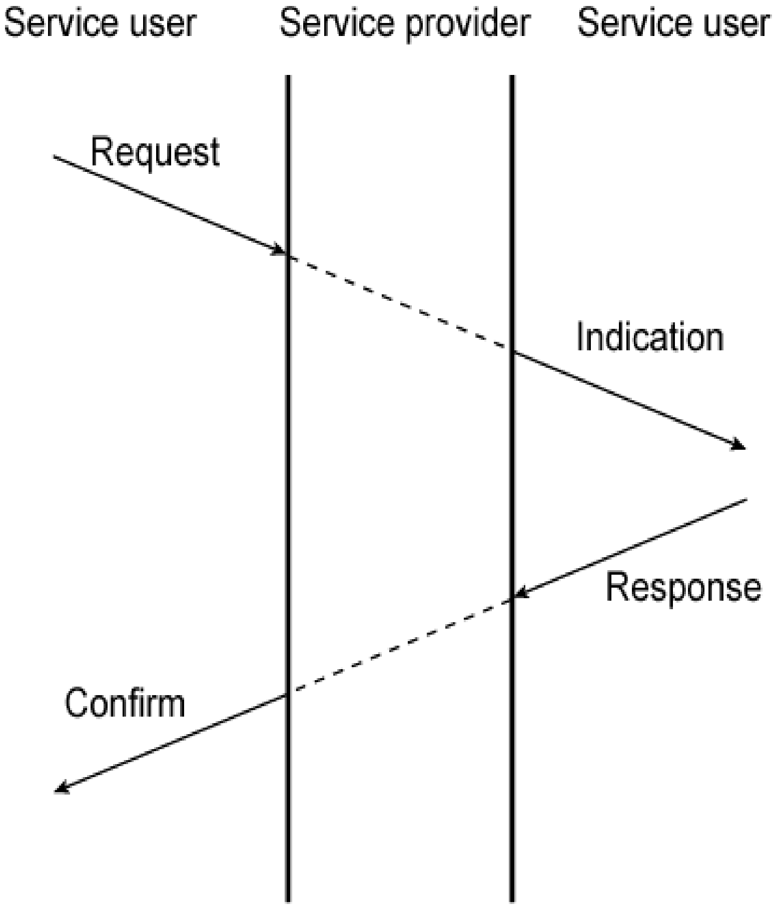
Standardized Protocol Architectures



Layer Specific Standards



Service Primitives and Parameters



(a) Confirmed Service

- define services between adjacent layers using:
- primitives to specify function performed
- parameters to pass data and control info

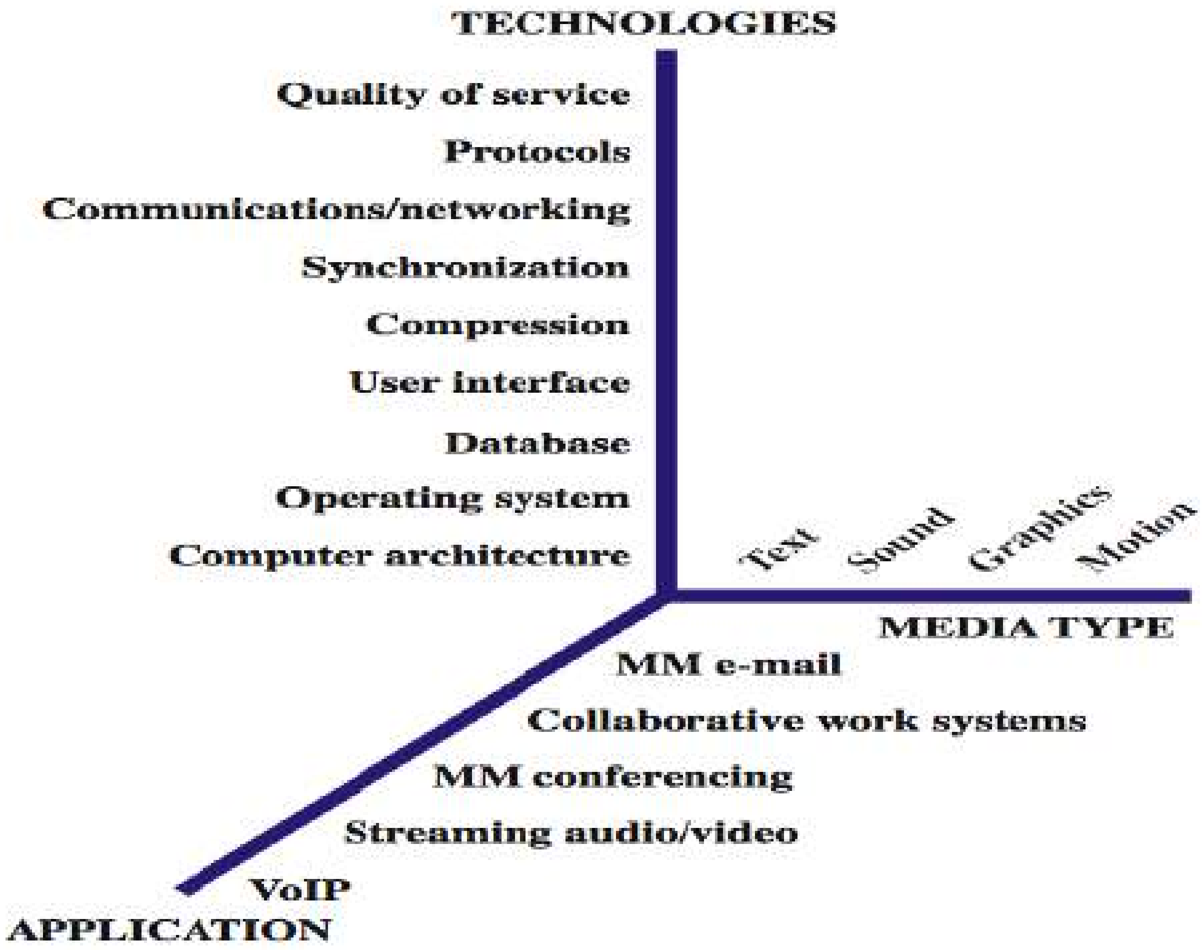
Primitive Types

REQUEST	A primitive issued by a service user to invoke some service and to pass the parameters needed to specify fully the requested service
INDICATION	A primitive issued by a service provider either to: indicate that a procedure has been invoked by the peer service user on the connection and to provide the associated parameters, or notify the service user of a provider-initiated action
RESPONSE	A primitive issued by a service user to acknowledge or complete some procedure previously invoked by an indication to that user
CONFIRM	A primitive issued by a service provider to acknowledge or complete some procedure previously invoked by a request by the service user

Traditional vs Multimedia Applications

- traditionally Internet dominated by info retrieval applications
  - typically using text and image transfer
  - eg. email, file transfer, web
- see increasing growth in multimedia applications
  - involving massive amounts of data
  - such as streaming audio and video
- Lot of applications have been standardized to operate on top of TCP. Few are
  - SMTP
  - FTP
  - Telnet

MULTIMEDIA TECHNOLOGIES



Type of Traffic generated by different applications

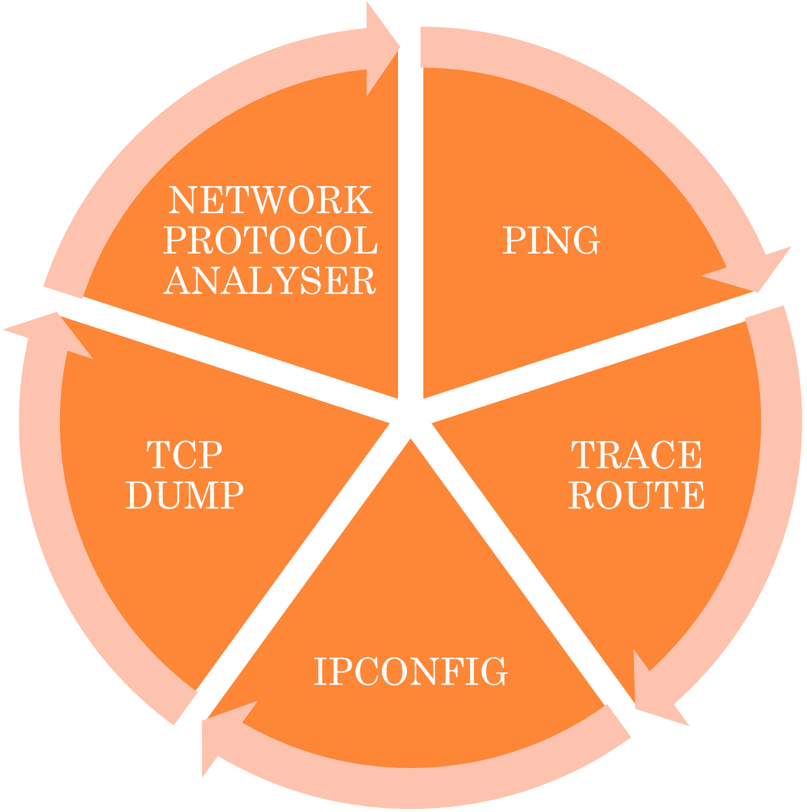
- Elastic Traffic
  - can adjust to delay & throughput changes over a wide range
  - eg. traditional "data" style TCP/IP traffic
  - Adjust with congestion by reducing rate
  - Eg. Email, file transfer, remote logon, n/w mngt, web access.
  - some applications more sensitive though. Eg. FTP, web access whereas, N/w mngt sensitive when problem occurs.
- Inelastic Traffic
  - does not adapt to such changes
  - eg. "real-time" voice & video traffic
  - need minimum requirements on net arch such as assurance about throughput, delay, no packet loss, no variation in traffic.

Summary

- introduced need for protocol architecture
- TCP/IP protocol architecture
- OSI Model & protocol architecture standardization
- traditional vs multimedia application needs

PRACTICALLY CHECK

- IP UTILITIES



PING

- Packet Inter Net Gopher
- Determines if host is reachable?
- Uses ICMP (Internet Control Message Protocol)
- Sends two or more ICMP Echo Msgs.
- Measures Round Trip Delay between two host.
- Eg. Ping www.google.com

TRACEROUTE

- Determine route that packet takes to reach the destination.
- Also gives latency & reachability.
- Generally used as debugging tool.
- Uses both, ICMP & UDP.

IPConfig

- Display TCP/IP information about host.
- Returns IP Address, Subnet Mask, Default Gateway, DNS Host Name, IP of DNS Server, Physical Address of NIC, IP, etc
- Also checks DHCP is enabled for automatic configuration of card's IP address or not.
- We can renew IP from DHCP.
- Try:
  - Ipconfig
  - renew

NETSTATE

- Provides information about network status of Host.
- It provides status of:
  - Network Drivers
  - NIC
- What information it provides?
  - # Packets
  - # Out Pkts
  - # Pkts in errors
- Also provides information about
  - Routing Table in Host
  - TCP/IP Server Active
  - TCP Connection Active

Network Protocol Analyzer: Wireshark

- Tool to capture, display & analyze PDU (Protocol Data Unit) exchanged in a network.
- Used for troubleshooting & to design new system.
- Also used for teaching the operations of protocol.
- Examining live traffic on network.
- We can apply filters by
  - Frame Address
  - IP Address
  - Protocol
  - Combination

TCP Dump ⇔ Win dump

- NIC is set to promiscuous mode.
- Card can listen & capture every frame that travels through broadcast n/w.
- N/w, Transport, Application layer content can be seen, observed & analyzed.
- To analyze these captured data, use Wireshark.
- Eg:

```
windump –D
windump –i  2 –q –w c:\perflogs\diagTraces
                         -n –C 30 –W 10 –U –s 0
```

- Where,
- i = #NIC selected
- q = queue mode
- w = prefix of file during creation
- n = no hostname, only IP
- C = size in million Byte
- W = #log files
- U = saved & written to o/p file
- s = decrease amount of pkt buffering.

TWO Chapters over, test?

THANK YOU

DATA AND COMPUTER COMMUNICATIONS

Chapter 3 – Data Transmission

DR. BHARGAVI GOSWAMI,
ASSOCIATE PROFESSOR,
GARDEN CITY COLLEGE,
BANGALORE.

TRANSMISSION TERMINOLOGY

- DATA TRANSMISSION OCCURS BETWEEN A TRANSMITTER & RECEIVER VIA SOME MEDIUM
- GUIDED MEDIUM
  - EG. TWISTED PAIR, COAXIAL CABLE, OPTICAL FIBER
- UNGUIDED / WIRELESS MEDIUM
  - EG. AIR, WATER, VACUUM

TRANSMISSION TERMINOLOGY

- DIRECT LINK
  - NO INTERMEDIATE DEVICES
- POINT-TO-POINT
  - DIRECT LINK
  - ONLY 2 DEVICES SHARE LINK
- MULTI-POINT
  - MORE THAN TWO DEVICES SHARE THE LINK

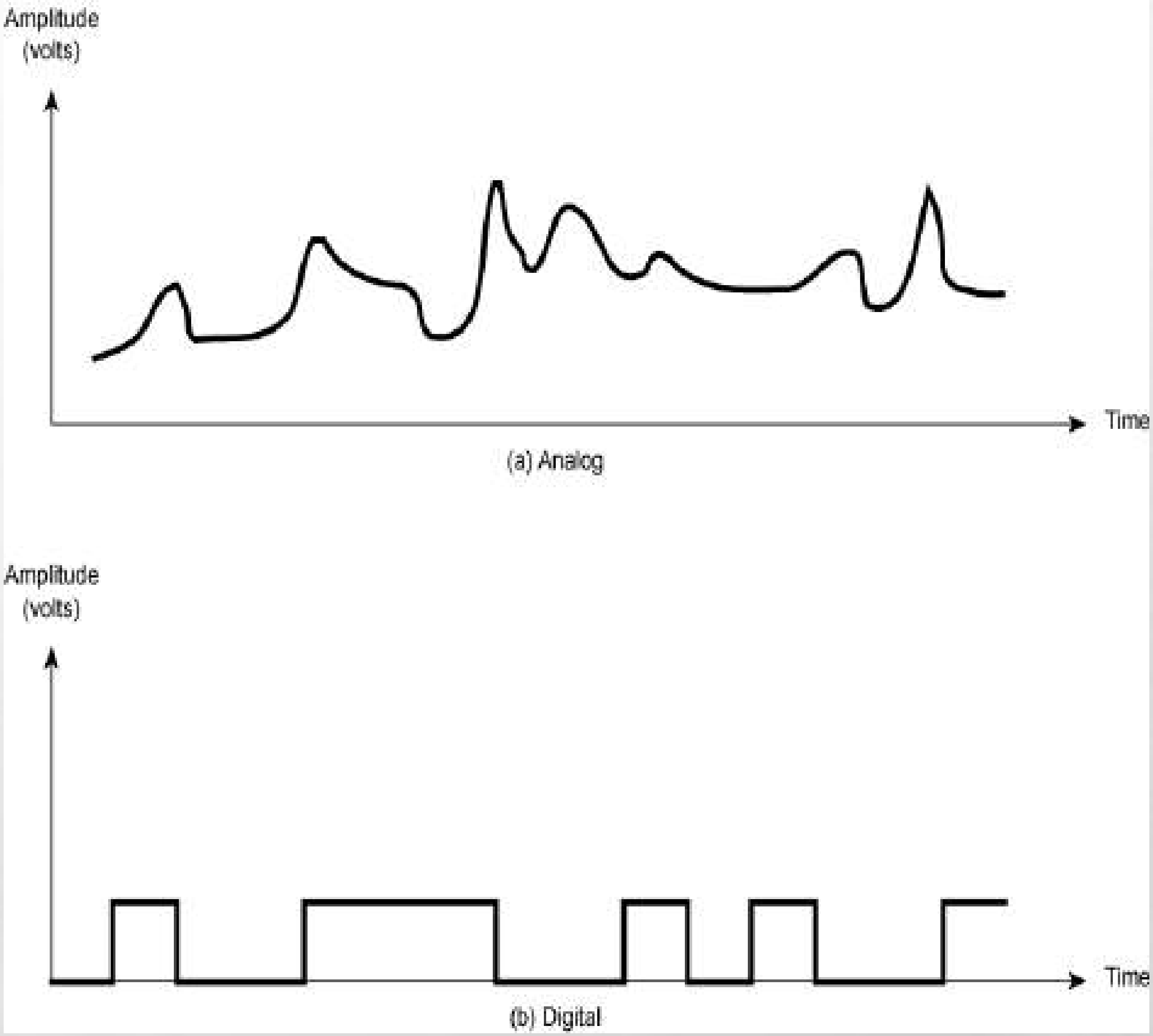
TRANSMISSION TERMINOLOGY

- SIMPLEX
  - ONE DIRECTION
    - EG. TELEVISION
- HALF DUPLEX
  - EITHER DIRECTION, BUT ONLY ONE WAY AT A TIME
    - EG. POLICE RADIO
- FULL DUPLEX
  - BOTH DIRECTIONS AT THE SAME TIME
    - EG. TELEPHONE

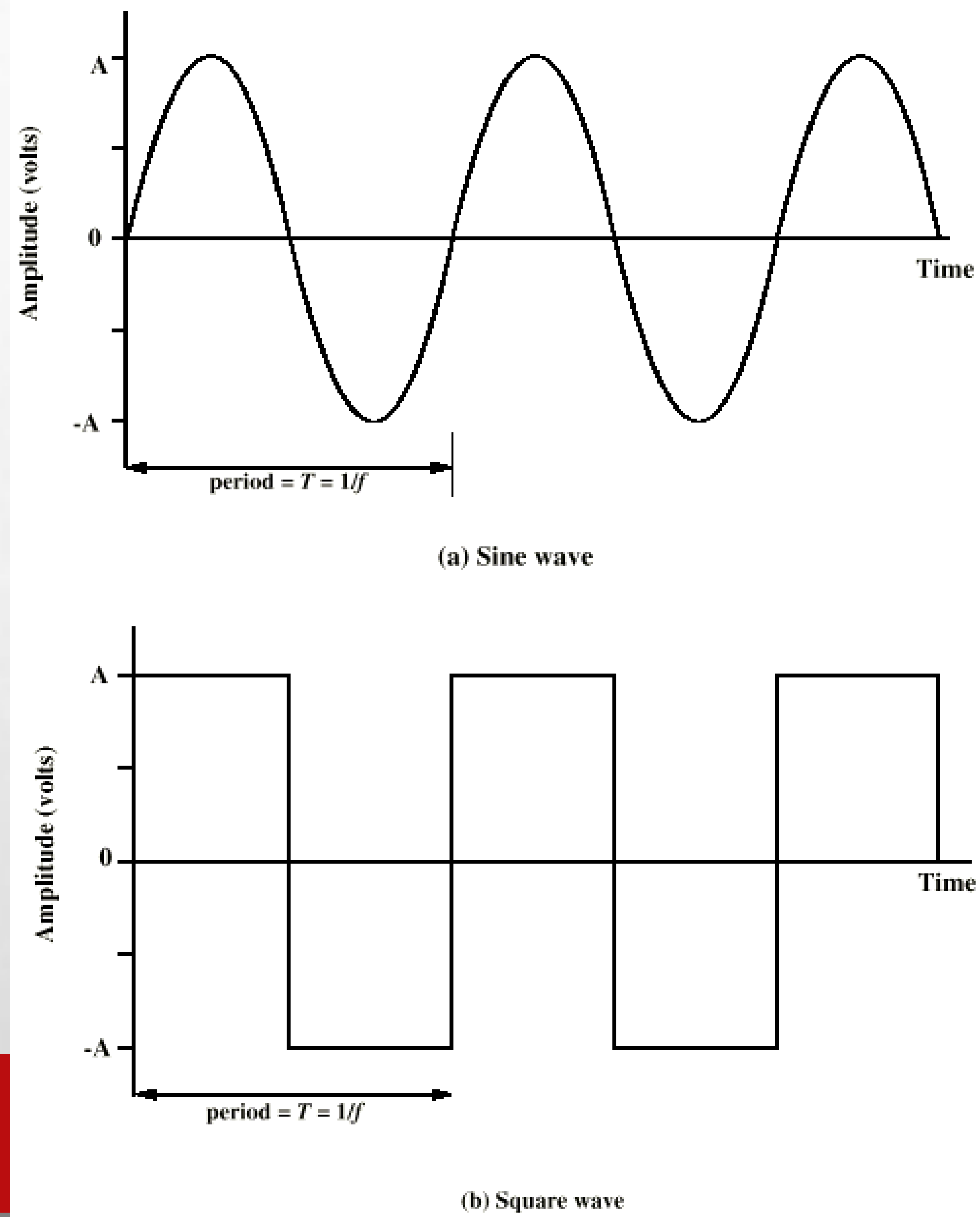
FREQUENCY, SPECTRUM AND BANDWIDTH

- TIME DOMAIN CONCEPTS
  - ANALOG SIGNAL
    - VARIOUS IN A SMOOTH WAY OVER TIME
  - DIGITAL SIGNAL
    - MAINTAINS A CONSTANT LEVEL THEN CHANGES TO ANOTHER CONSTANT LEVEL
  - PERIODIC SIGNAL
    - PATTERN REPEATED OVER TIME
  - APERIODIC SIGNAL
    - PATTERN NOT REPEATED OVER TIME

ANALOGUE & DIGITAL SIGNALS



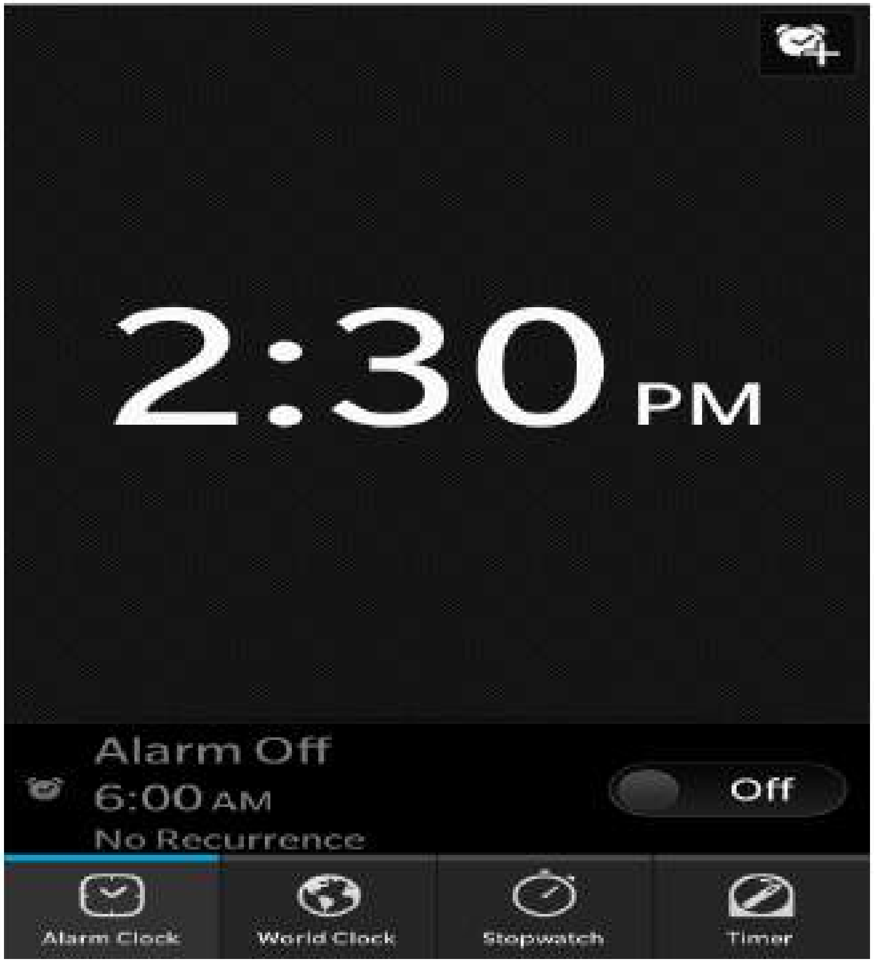
PERIODIC SIGNALS



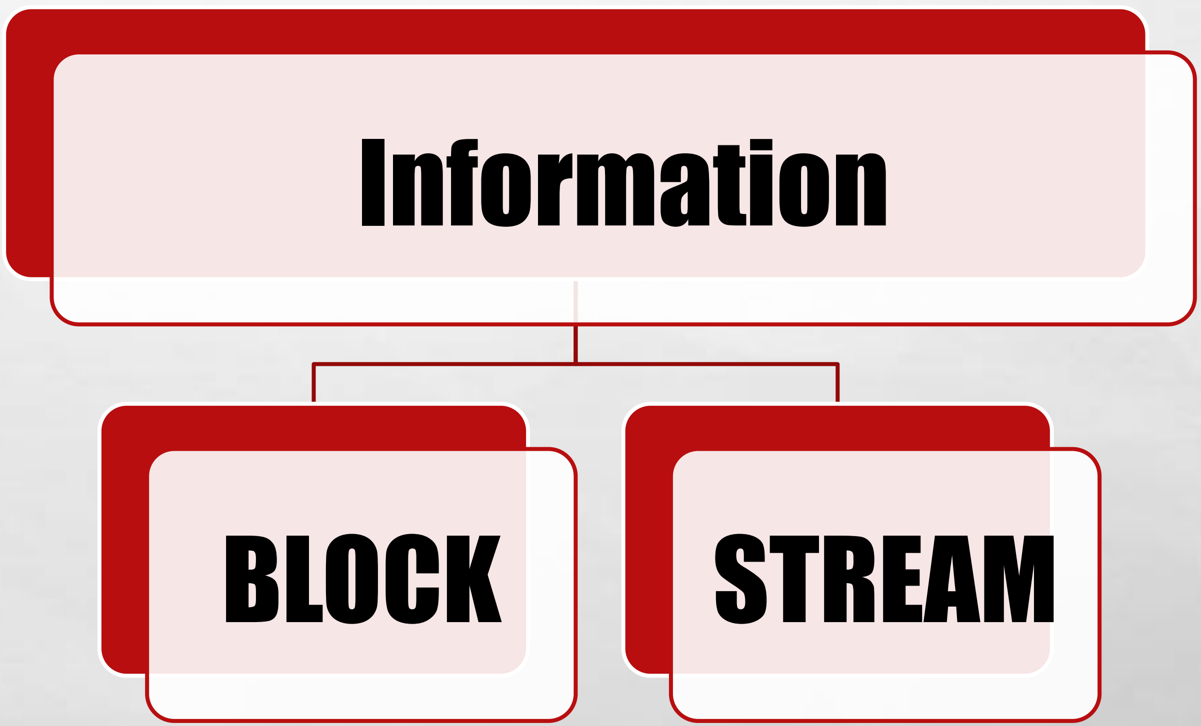
DIGITAL TRANSMISSION. WHY?

- DIGITAL TECHNOLOGY:
  - LARGE SCALE INTEGRATION (LSI) & VERY LSI (VLSI) TECHNOLOGY.
  - DROP IN COST AND SIZE OF DIGITAL CIRCUITRY.
- DATA INTEGRITY:
  - USE REPEATER.
  - NO EFFECT OF NOISE AND IMPAIRMENTS
  - BETTER THAN AMPLIFIERS.
- CAPACITY UTILIZATION:
  - MULTIPLEXING
- SECURITY & PRIVACY:
  - ENCRYPTION TECHNIQUES
- INTEGRATION:
  - VOICE
  - VIDEO
  - DIGITAL DATA
  - IMAGE
  - TEXT

ANALOG V/S DIGITAL



DIGITAL REPRESENTATION OF INFORMATION



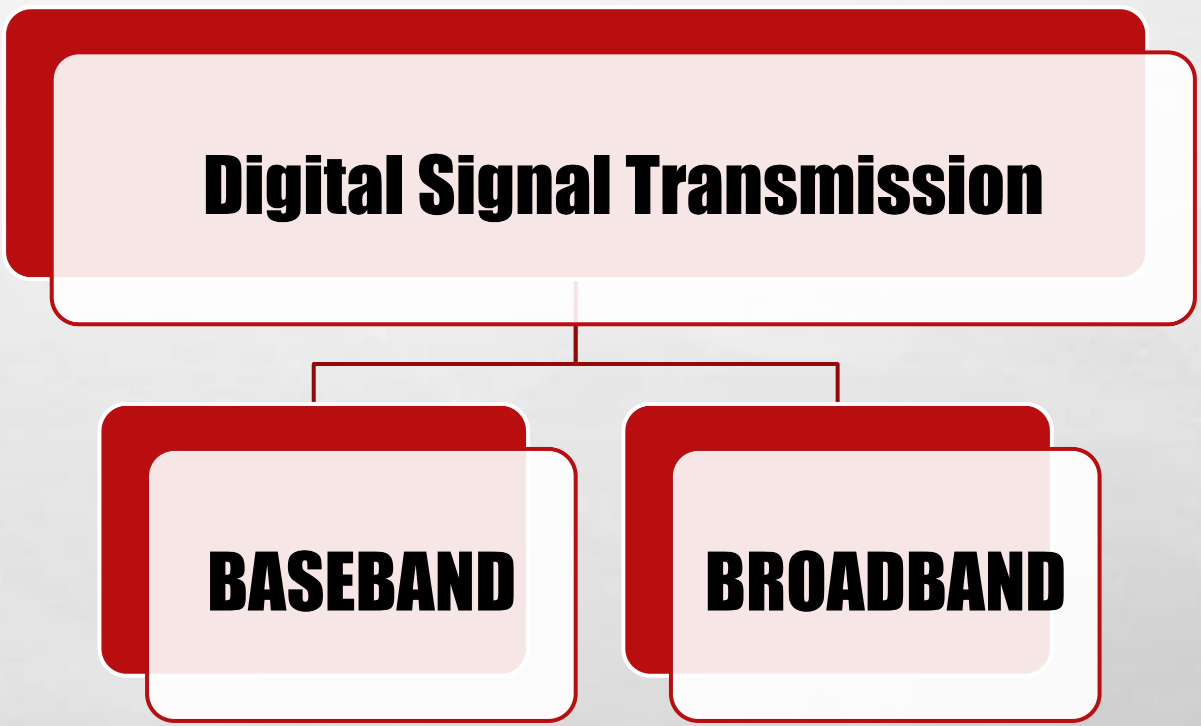
BLOCK ORIENTED INFORMATION

- INCLUDES: DATA, DOCUMENTS & PICTURES
- HAS TEXT, NUMERICAL & GRAPHICAL INFO.
- COMPRESSION? YES.
- Y? USE LESS DISK STORAGE SPACE
- BLOCK TRANSMISSION TIME? DELAY. EQUATION?
- DELAY = T_{PROP} + L/R.
- WHERE, T = TIME, L = #BLOCKS, R = RATE IN BITS/SEC.

STREAM ORIENTED INFORMATION

- TRANSMIT: VOICE, MUSIC & VIDEO
- INCLUDES VARIATIONS IN AIR PRESSURE
- EVERYTHING IN VOICE & VIDEO IS CONVERTED TO SIGNAL AND TRANSMITTED.

TRANSMISSION OF DIGITAL SIGNAL



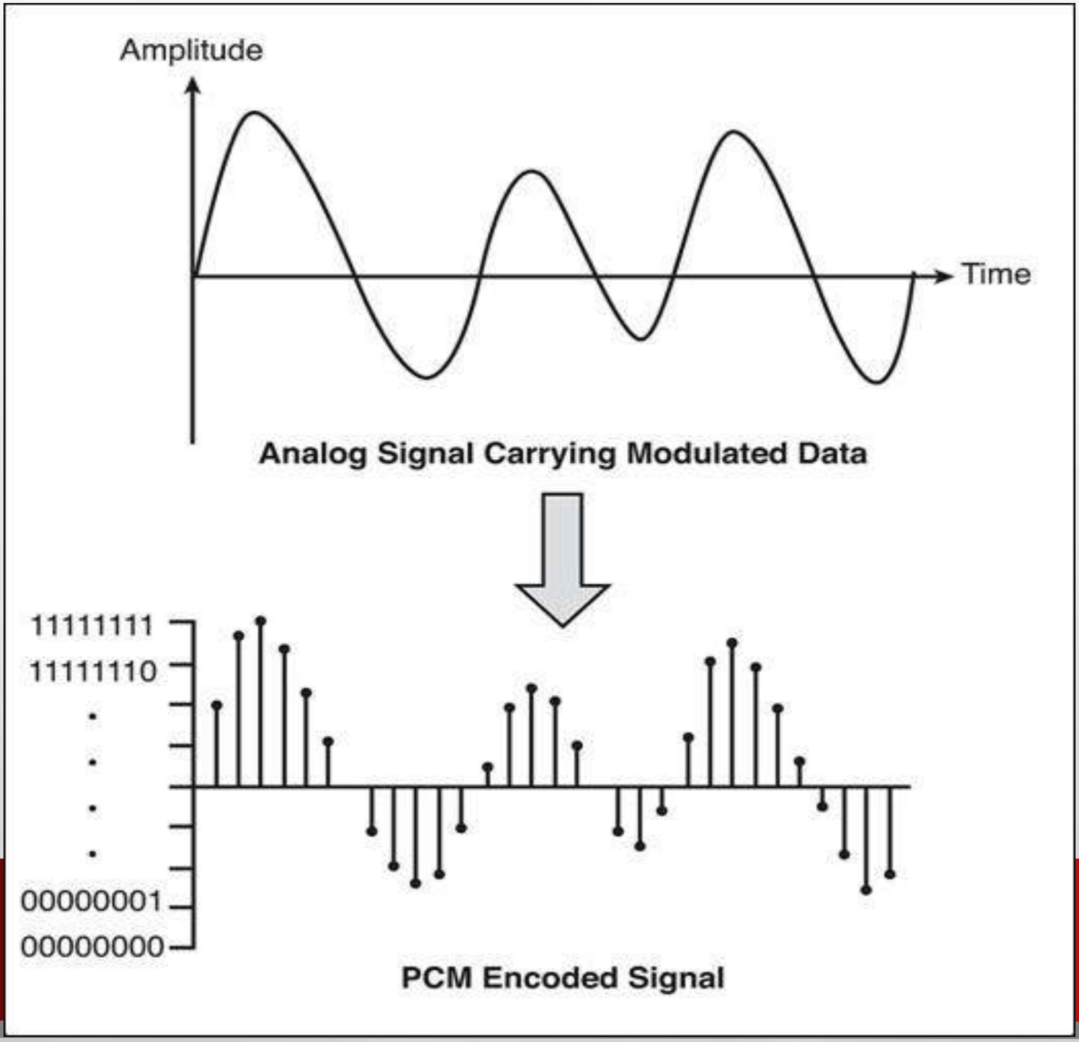
BASEBAND

- DEFINITION: ONE THAT USES DIGITAL SIGNALLING, WHICH IS INSERTED IN THE TRANSMISSION CHANNEL AS VOLTAGE PULSES.
- ENTIRE FREQUENCY SPECTRUM IS UTILIZED.
- HENCE, NO FREQUENCY DIVISION MULTIPLEXING USED.
- TRANSMISSION IS BIDIRECTIONAL.
- DISTANCE COVERED IS LIMITED B'COZ OF HIGH FREQUENCY.

BROADBAND

- USE ANALOG SIGNALLING OF HIGH FREQUENCY.
- FREQUENCY DIVISION MULTIPLEXING IS POSSIBLE.
- CAN ACCOMMODATE MULTIPLE SIGNALS.
- UNIDIRECTIONAL.

PULSE CODE MODULATION



PCM is digital scheme for transmitting analog data. Signals in PCM are binary low and high i.e 0 & 1.

PCM, DPCM & ADPCM

- PULSE CODE MODULATION, FOR DIGITIZING ANALOG DATA.
- DIFFERENTIAL PCM (DPCM) FOR REDUCING BIT RATE WHILE MAINTAINING QUALITY OF VOICE SIGNAL.
- ADAPTIVE PCM (ADPCM), ADAPTS TO VARIATIONS IN VOICE SIGNAL E.G. LOUDNESS OF VOICE.
- ADDITIONAL COST IS ADDED TO DPCM & ADPCM OVER BIT RATE.

STEPS FOR DIGITIZING ANALOG SIGNAL

1. OBTAIN SAMPLE VALUES OF SIGNAL EVERY T SECONDS.
2. QUANTIZE EACH OF SAMPLE VALUES
3. EACH QUANTIZED VALUE IS TRANSMITTED TO BINARY EQUIVALENT
4. DIGITAL DATA IS CONVERTED TO DIGITAL SIGNAL BY LINE ENCODING TECHNIQUE.

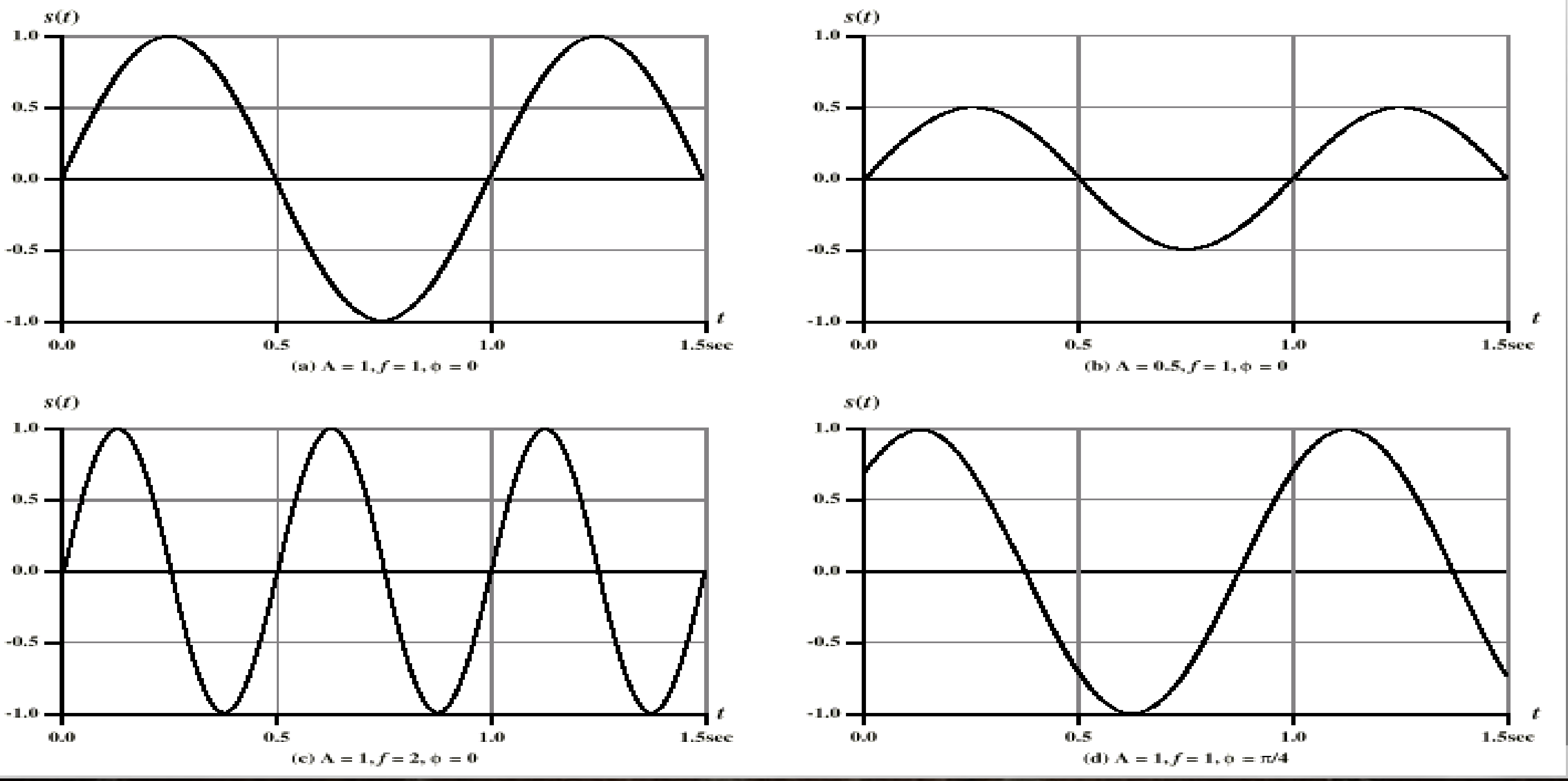
FACTORS AFFECTING TRANSMISSION CAPABILITY

- AMOUNT OF ENERGY TO TRANSMIT SIGNAL
- DISTANCE TRAVELLED BY SIGNAL
- NOISE RECEIVER CONTEND
- BANDWIDTH OF CHANNEL

SINE WAVE

- PEAK AMPLITUDE (A)
  - MAXIMUM STRENGTH OF SIGNAL
  - VOLTS
- FREQUENCY (F)
  - RATE OF CHANGE OF SIGNAL
  - HERTZ (HZ) OR CYCLES PER SECOND
  - PERIOD = TIME FOR ONE REPETITION (T)
  - T = 1/F
- PHASE (ϕ)
  - RELATIVE POSITION IN TIME

VARYING SINE WAVES: SINUSOID FUNCTION S(T) = A SIN(2πFT +Φ)



WAVELENGTH (λ)

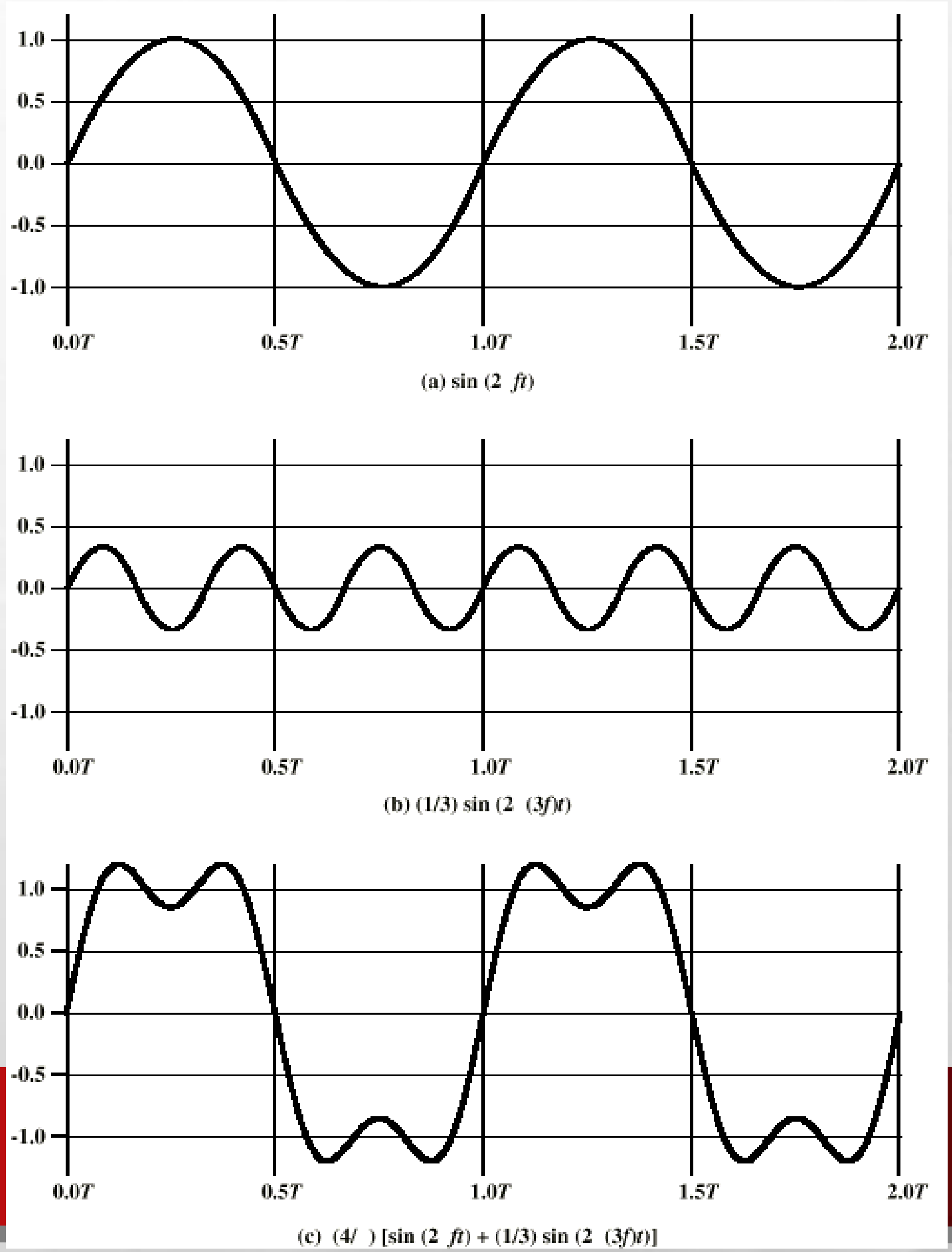
- IS DISTANCE OCCUPIED BY ONE CYCLE
- BETWEEN TWO POINTS OF CORRESPONDING PHASE IN TWO CONSECUTIVE CYCLES
- ASSUMING SIGNAL VELOCITY *V* HAVE $\lambda = VT$
- OR EQUIVALENTLY $\lambda F = V$
- ESPECIALLY WHEN $V=C$
  - $C = 3*10^8 MS^{-1}$ (SPEED OF LIGHT IN FREE SPACE)

FREQUENCY DOMAIN CONCEPTS

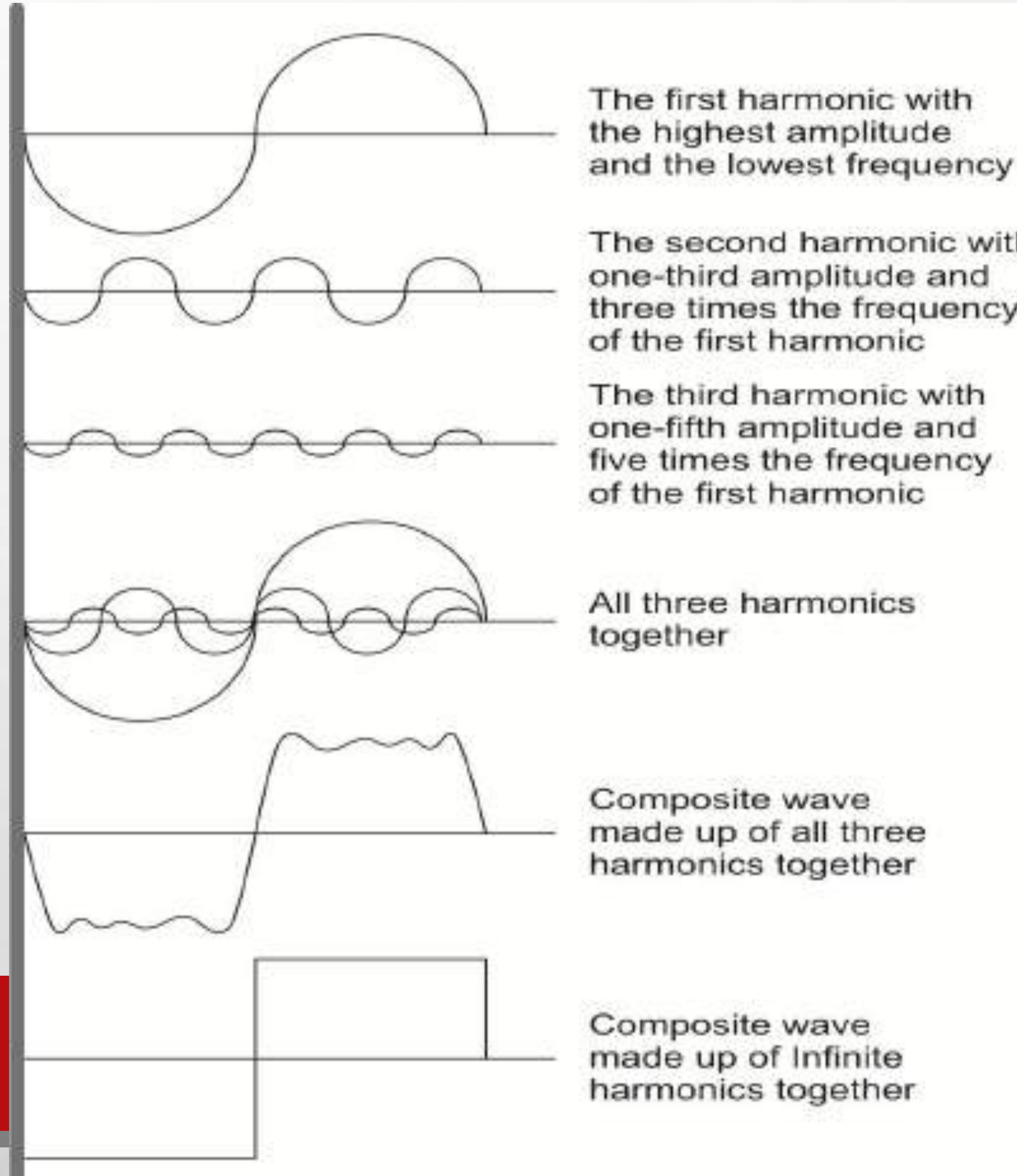
- SIGNAL ARE MADE UP OF MANY FREQUENCIES
- COMPONENTS ARE SINE WAVES
- FOURIER ANALYSIS CAN SHOWN THAT ANY SIGNAL IS MADE UP OF COMPONENT SINE WAVES
- CAN PLOT FREQUENCY DOMAIN FUNCTIONS

ADDITION OF FREQUENCY COMPONENTS (T=1/F)

- C IS SUM OF *F & 3F*



HARMONICS AND COMPOSITE WAVE



- **FOURIER COMPONENT**: COMPONENTS OF A COMPOSITE SIGNAL ARE KNOWN AS FOURIER COMPONENT.
- **COMPOSITE SIGNALS**: WHEN A SIGNAL CONTAINS MULTIPLE FREQUENCIES, IT IS CALLED COMPOSITE SIGNALS.
- **FUNDAMENTAL FREQUENCY**: FREQUENCY OF FIRST HARMONIC (FOURIER COMPONENT) IS KNOWS AS FUNDAMENTAL FREQUENCY.
- IF FIRST COMPONENT IS F, 2^{ND} IS 3F AND 3^{RD} IS 5F.
- FREQUENCY IS INVERSELY PROPORTIONAL TO AMPLITUDE.
- LARGE AMPLITUDE SIGNALS COVER SMALLER DISTANCE.

PROPERTIES OF CHANNEL

- **MORE THE BANDWIDTH OF THE MEDIA, MORE THE NUMBER OF HARMONICS THAT CAN PASS THROUGH THE MEDIA.**
- **HIGHER THE DATA RATE, LESS WILL BE THE NUMBER OF HARMONICS THAT CAN PASS THROUGH THE MEDIA.**
- ***BAUD RATE: #SIGNALS THAT PASSES THRU MEDIA IN UNIT TIME, USUALLY IN SECONDS. AS BANDWIDTH IS FIXED, BAUD RATE IS ALSO FIXED.***
- ***BIT RATE: #BITS THAT PASSES THRU A MEDIA IN UNIT TIME, USUALLY IN SECONDS. IF 1 SIGNAL CARRY N BITS THEN BAUD RATE IS 1 AND BIT RATE IS N.***
- ***SIGNAL: COMBINATION OF ZEROS AND ONES.***
- ***MAXIMUM BAUD RATE: NO OF HARMONICS THAT CAN BE ACCOMMODATED IN A GIVEN BANDWIDTH.***
- ***WE CAN OBTAIN MAXIMUM DATA RATE (MDR) IF WE KNOW BANDWIDTH AND SENSITIVITY OF RECEIVER (#HARMONICS RECOGNIZED CORRECTLY).***
- ***DATA RATE IS DOUBLED WHEN BAUD RATE IS QUADRUPLED, TRIPLED WHEN BAUD RATE IS 8 TIMES, AND SO ON….***

AMPLITUDE – RESPONSE FUNCTION

$$AF = \frac{1}{1 + 4\prod^2 F^2}$$

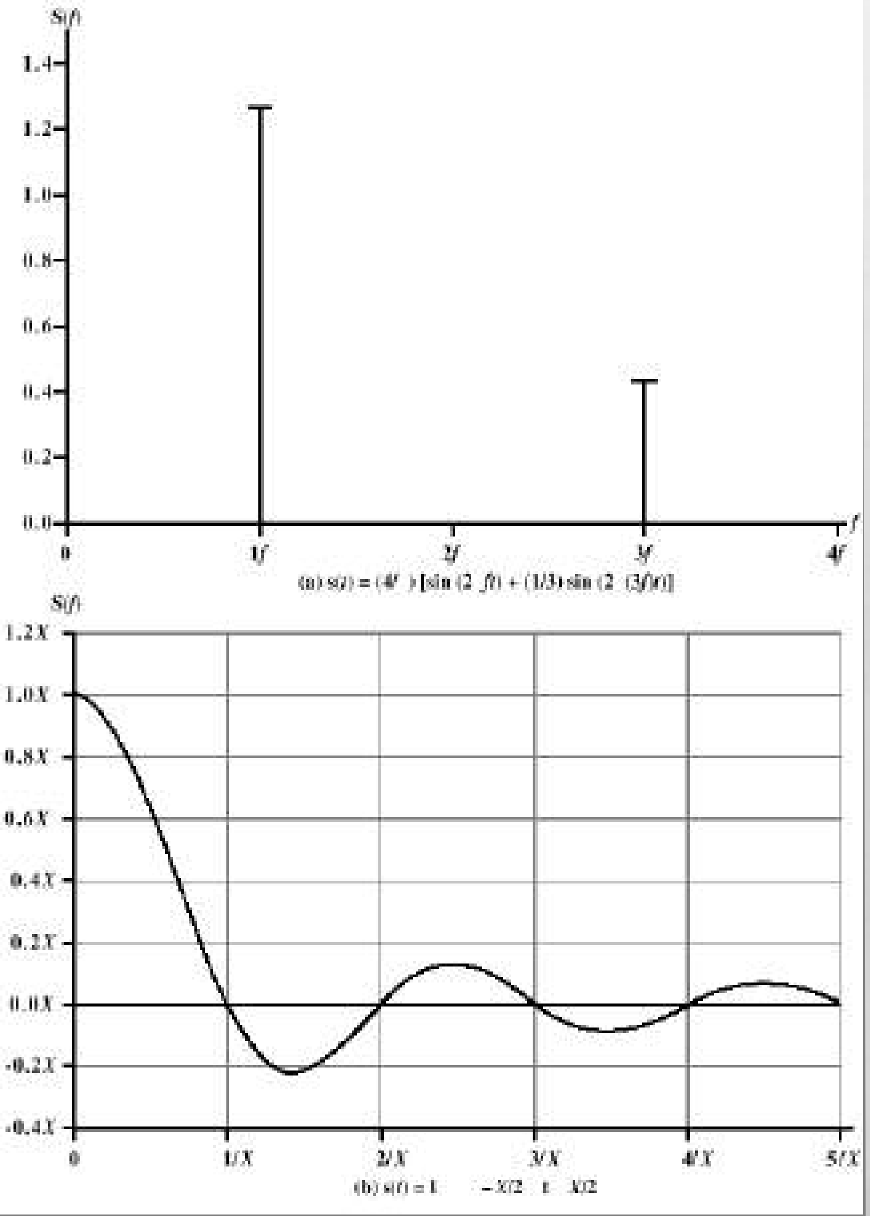
- IS THE ABILITY OF CHANNEL TO TRANSFER A TONE OF FREQUENCY F WHICH IS DEFINED AS RATIO OF AMPLITUDE OF OUTPUT TONE DIVIDED BY AMPLITUDE OF INPUT TONE.

EXAMPLES:

- IF F1 = 300 HZ AND F2 = 3000 HZ. WHAT IS BAN
- DWIDTH?
  - BANDWIDTH = F2 – F1 = 3000 – 300 = 2700 HZ.
- IF PERIODIC SIGNAL HAS BANDWIDTH OF 20 HZ. IF HIGHEST FREQUENCY IS 60 HZ, WHAT IS THE LOWEST FREQUENCY?
  - BANDWIDTH = F2 – F1
  - 20 = 60 – F1.
  - SO, F1 = 40 HZ.
- IF ANALOG SIGNAL CARRY 8 BITS IN EACH SIGNAL UNIT & 2000 SIGNAL UNITS ARE SENT PER SECOND. WHAT IS BAUD RATE & BIT RATE?
  - BAUD RATE = 2000 BAUDS / SEC
  - BIT RATE = 2000 X 8 = 16000 BITS/SEC
- IF BIT RATE = 6000 BITS / SEC & EACH SIGNAL UNIT CARRY 8 BITS, FIND BAUD RATE.
  - BAUD RATE = 6000 / 8 = 750 BAUDS / SEC
- IF SIGNAL HAS BIT RATE OF 2000 BPS. WHAT IS BIT INTERVAL?
  - BIT INTERVAL = 1 / BIT RATE = 1 / 2000 S = 0.0005 S = 500 MS

FREQUENCY & TIME DOMAIN REPRESENTATIONS

- FREQ DOMAIN FUNC OF FIG 3.4C
- FREQ DOMAIN FUNC OF SINGLE SQUARE PULSE



SPECTRUM & BANDWIDTH

- SPECTRUM
  - RANGE OF FREQUENCIES CONTAINED IN SIGNAL
- ABSOLUTE BANDWIDTH
  - WIDTH OF SPECTRUM
- EFFECTIVE BANDWIDTH
  - OFTEN JUST *BANDWIDTH*
  - NARROW BAND OF FREQUENCIES CONTAINING MOST ENERGY
- DC COMPONENT
  - COMPONENT OF ZERO FREQUENCY

DATA RATE AND BANDWIDTH

- ANY TRANSMISSION SYSTEM HAS A LIMITED BAND OF FREQUENCIES
- THIS LIMITS THE DATA RATE THAT CAN BE CARRIED
- SQUARE HAVE INFINITE COMPONENTS AND HENCE BANDWIDTH
- BUT MOST ENERGY IN FIRST FEW COMPONENTS
- LIMITED BANDWIDTH INCREASES DISTORTION
- HAVE A DIRECT RELATIONSHIP BETWEEN DATA RATE & BANDWIDTH

BANDWIDTH & DATA RATE

BANDWIDTH:

- REPRESENTS THE RANGE OF FREQUENCIES THAT CAN PASS THRU A MEDIUM.
- MORE THE BANDWIDTH LARGER THE DATA IT CAN TRANSMIT.
- FIXED
- EG. WIDER THE ROAD, LARGER #VEHICLES ACCOMMODATED.

DATA RATE:

- DATA RATE IS THE ACTUAL TRAFFIC PASSING AT GIVEN TIME.
- PURELY DEPENDS ON BANDWIDTH.
- VARIABLE.
- EG: DRIVER ASKING FOR INFINITE SPEED (BANDWIDTH) FOR TRANSMISSION.
- DATA RATE DEPENDS ON:
  - BANDWIDTH UTILIZATION
  - IF ANALOG, #CONSTELLATION POINTS
  - IF DIGITAL, NUMBER OF LEVELS
  - RECEIVER'S SENSITIVITY
  - MEDIA RESISTANCE AND TEMPERATURE

ANALOG AND DIGITAL DATA TRANSMISSION

- DATA
  - ENTITIES THAT CONVEY MEANING
- SIGNALS & SIGNALLING
  - ELECTRIC OR ELECTROMAGNETIC REPRESENTATIONS OF DATA, PHYSICALLY PROPAGATES ALONG MEDIUM
- TRANSMISSION
  - COMMUNICATION OF DATA BY PROPAGATION AND PROCESSING OF SIGNALS

ANALOG V/S DIGITAL

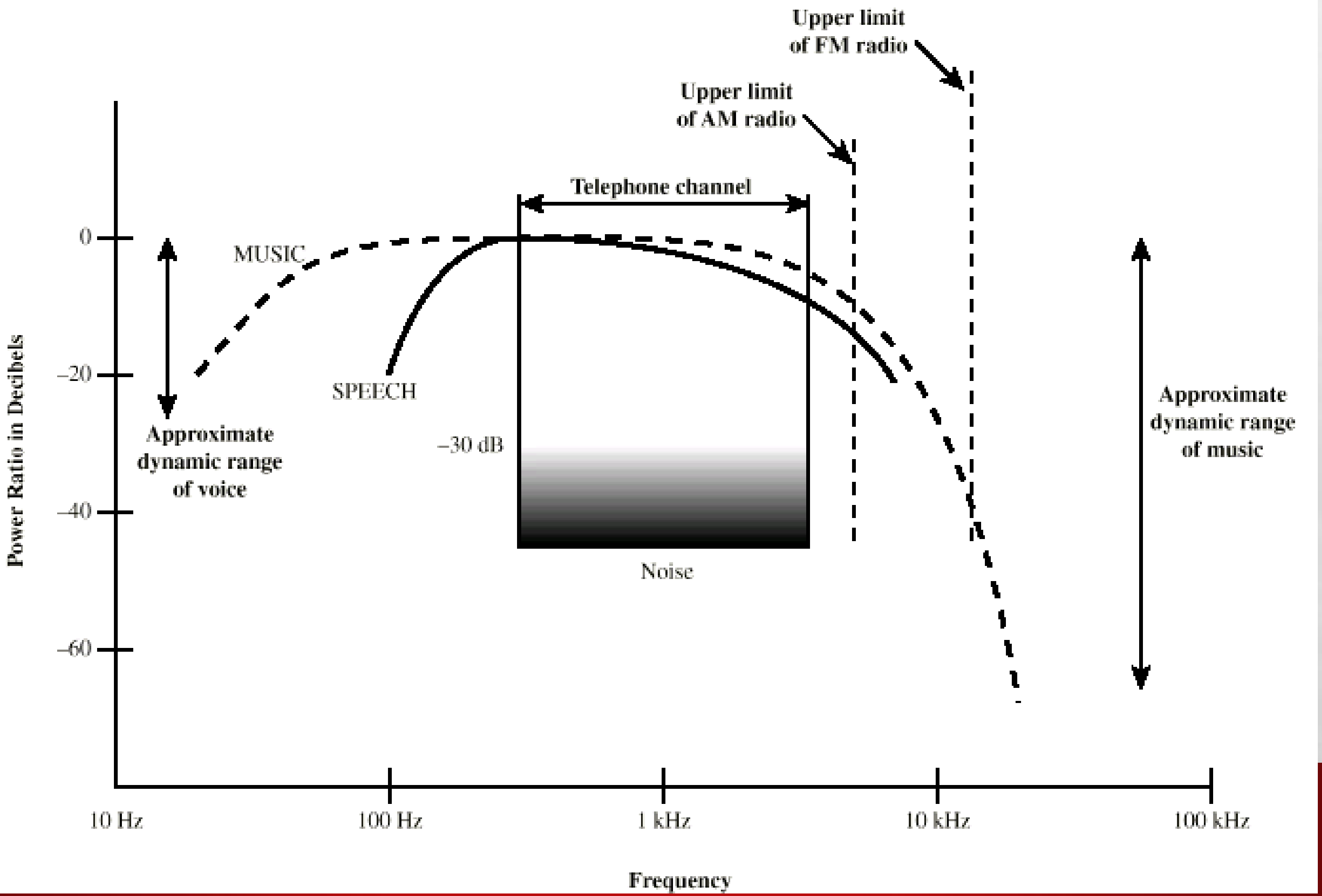
ANALOG

- USED TO TRANSMIT VIDEO AND AUDIO SIGNALS.
- USED WHEN WE DON'T HAVE LARGE BANDWIDTH.
- HIGHER ERROR RATE DUE TO SINE PROPERTY.
- CONTINUOUS BY NATURE.
- USES CURVED WAVE FORMS.
- CAN TRAVEL SHORT DISTANCE.
- AMPLIFIERS ARE USED WHICH GIVES STRENGTH TO SIGNAL BUT CAN'T CORRECT THE SIGNALS.
- ANALOG SIGNALS CAN BE USED FOR DIGITAL TRANSMISSION. EG; MODEM SENDS DIGITAL DATA OVER ANALOG TELEPHONE LINES.

DIGITAL

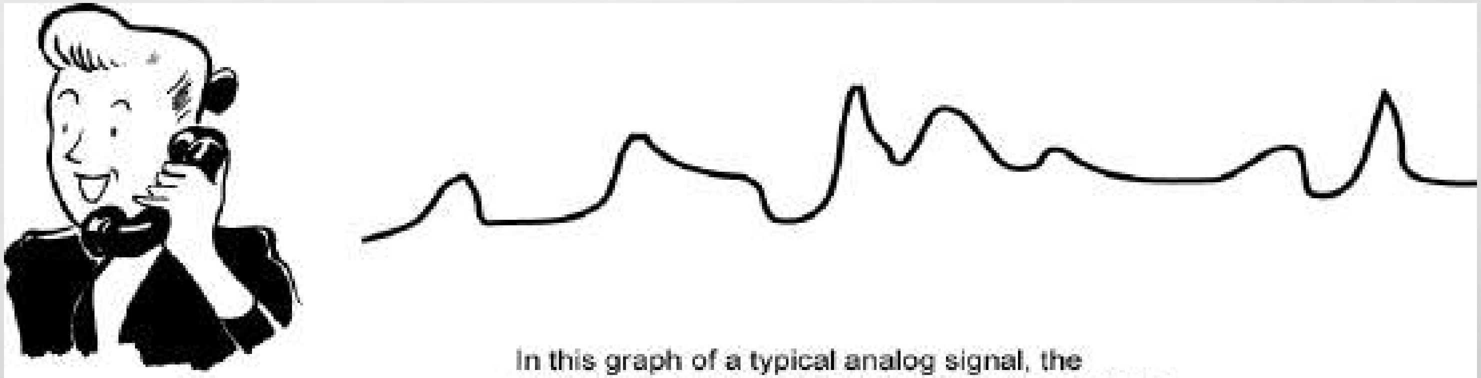
- USEUSED TO TRANSFER (0,1) BITS GENERALLY FOR FILE TRANSFER.
- USED WHEN WE HAVE LARGE BANDWIDTH.
- LOW ERROR RATE.
- DISCRETE BY NATURE.
- SQUARE WAVE FORMS.
- CAN TRAVEL LONG DISTANCE.
- REPEATERS ARE USED TO GIVE STRENGTH TO SIGNAL WHICH CAN ALSO CORRECT SIGNALS.
- DIGITAL SIGNALS CAN BE USED FOR ANALOG TRANSMISSION. EG. YOU TUBE, SKYPE TRANSMITTING AUDIO VIDEO SIGNALS USING DIGITAL SIGNALS.

ACOUSTIC SPECTRUM (ANALOG)



AUDIO SIGNALS

- FREQ RANGE 20HZ-20KHZ (SPEECH 100HZ-7KHZ)
- EASILY CONVERTED INTO ELECTROMAGNETIC SIGNALS
- VARYING VOLUME CONVERTED TO VARYING VOLTAGE
- CAN LIMIT FREQUENCY RANGE FOR VOICE CHANNEL TO 300-3400HZ



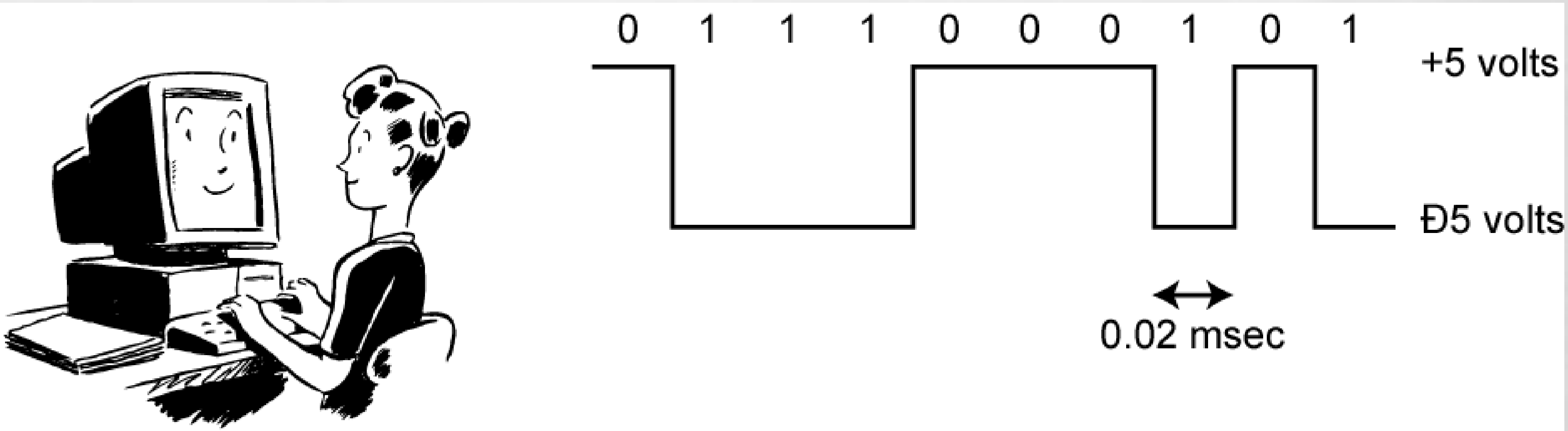
In this graph of a typical analog signal, the variations in amplitude and frequency convey the gradations of loudness and pitch in speech or music. Similar signals are used to transmit television pictures, but at much higher frequencies.

VIDEO SIGNALS

- USA - 483 LINES PER FRAME, AT FRAMES PER SEC
  - HAVE 525 LINES BUT 42 LOST DURING VERTICAL RETRACE
- 525 LINES X 30 SCANS = 15750 LINES PER SEC
  - 63.5μS PER LINE
  - 11μS FOR RETRACE, SO 52.5 μS PER VIDEO LINE
- MAX FREQUENCY IF LINE ALTERNATES BLACK AND WHITE
- HORIZONTAL RESOLUTION IS ABOUT 450 LINES GIVING 225 CYCLES OF WAVE IN 52.5 μS
- MAX FREQUENCY OF 4.2MHZ

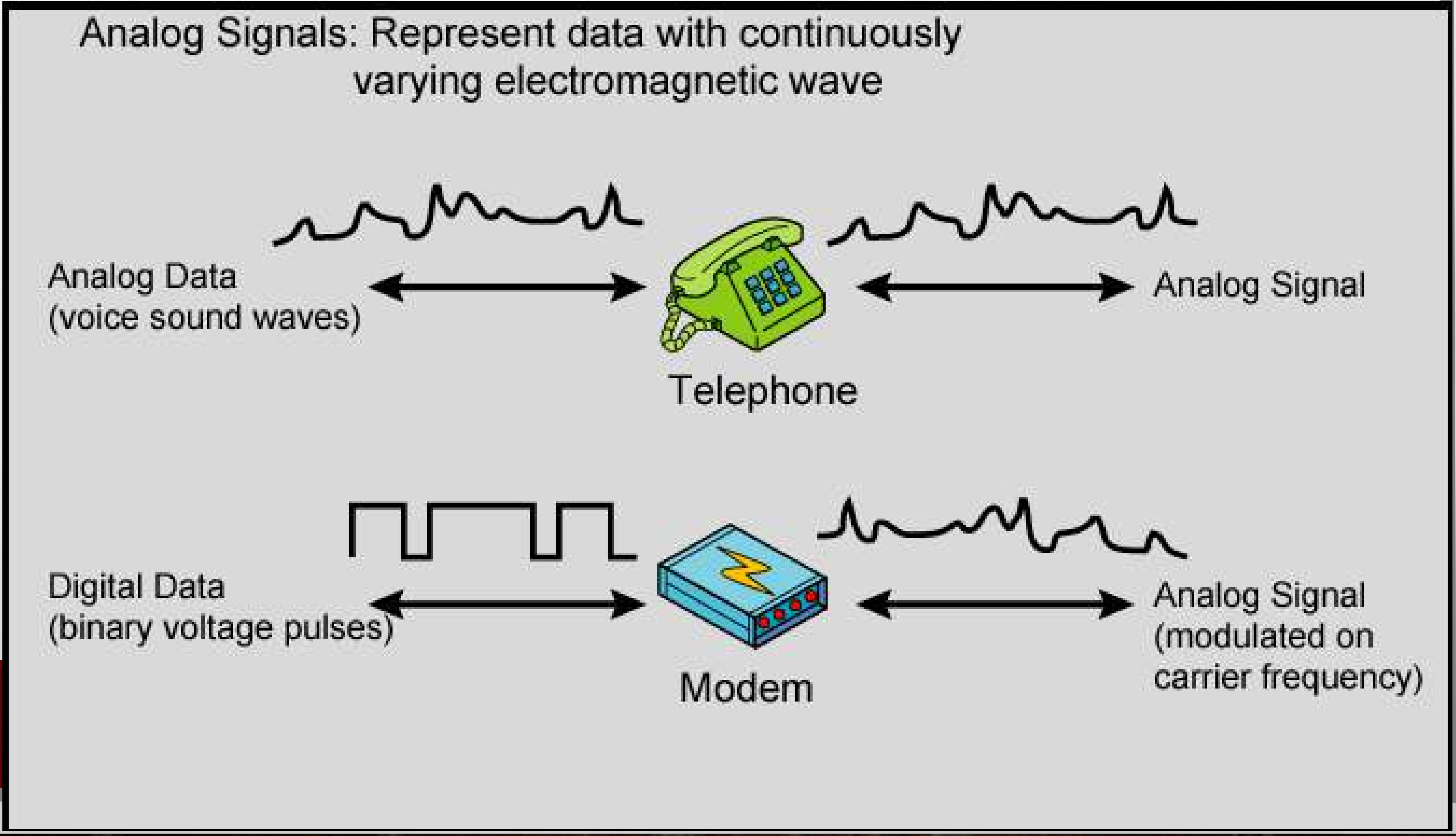
DIGITAL DATA

- AS GENERATED BY COMPUTERS ETC.
- HAS TWO DC COMPONENTS
- BANDWIDTH DEPENDS ON DATA RATE

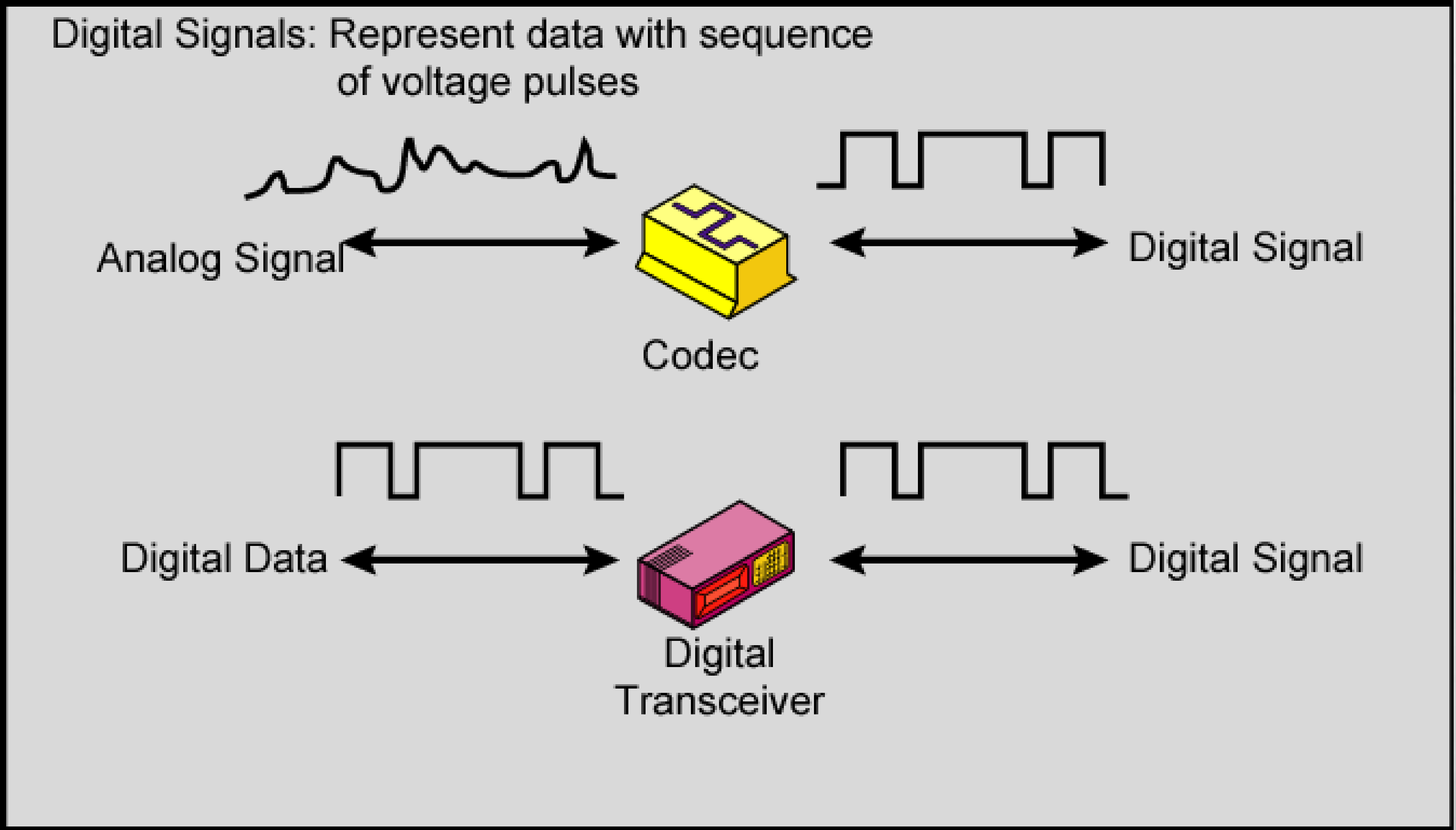


User input at a PC is converted into a stream of binary digits (1s and 0s). In this graph of a typical digital signal, binary one is represented by Đ5 volts and binary zero is represented by +5 volts. The signal for each bit has a duration of 0.02 msec, giving a data rate of 50,000 bits per second (50 kbps).

ANALOG SIGNALS

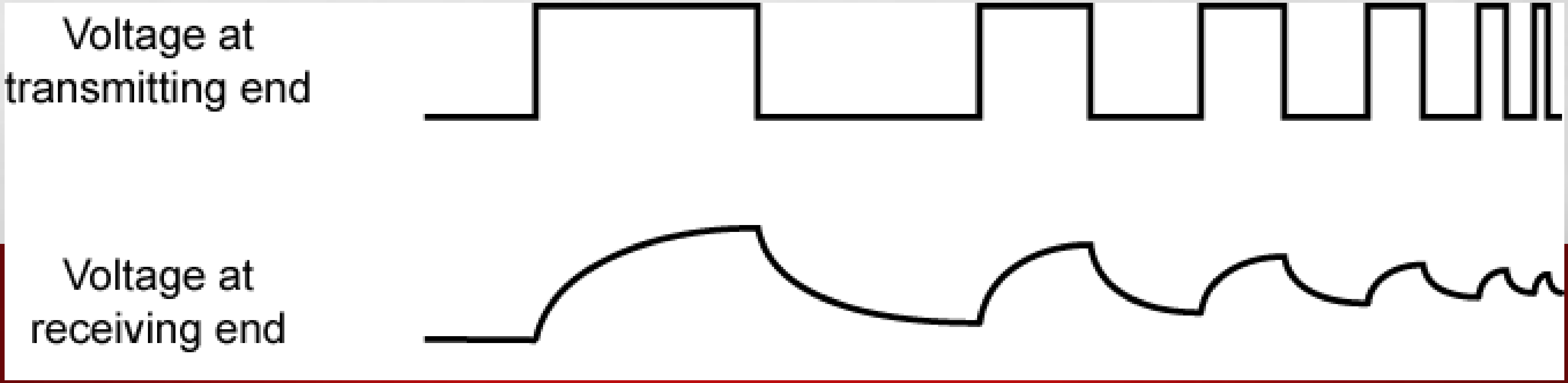


DIGITAL SIGNALS



ADVANTAGES & DISADVANTAGES OF DIGITAL SIGNALS

- CHEAPER
- LESS SUSCEPTIBLE TO NOISE
- BUT GREATER ATTENUATION
- DIGITAL NOW PREFERRED CHOICE



TRANSMISSION IMPAIRMENTS

- SIGNAL RECEIVED MAY DIFFER FROM SIGNAL TRANSMITTED CAUSING:
  - ANALOG - DEGRADATION OF SIGNAL QUALITY
  - DIGITAL - BIT ERRORS
- MOST SIGNIFICANT IMPAIRMENTS ARE
  - ATTENUATION AND ATTENUATION DISTORTION
  - DELAY DISTORTION
  - NOISE

ATTENUATION

- WHERE SIGNAL STRENGTH FALLS OFF WITH DISTANCE
- DEPENDS ON MEDIUM
- RECEIVED SIGNAL STRENGTH MUST BE:
  - STRONG ENOUGH TO BE DETECTED
  - SUFFICIENTLY HIGHER THAN NOISE TO RECEIVE WITHOUT ERROR
- SO INCREASE STRENGTH USING AMPLIFIERS/REPEATERS
- IS ALSO AN INCREASING FUNCTION OF FREQUENCY
- SO EQUALIZE ATTENUATION ACROSS BAND OF FREQUENCIES USED
  - EG. USING LOADING COILS OR AMPLIFIERS
- ATTENUATION = 10 LOG P_{IN} / P_{OUT}.
- POWER = $A^2/2$.
- ATTENUATION AT FREQUENCY F = $P_{IN} / P_{OUT} = A^2_{IN} / A^2_{OUT} = 1 / A^2 (F)$

DELAY DISTORTION

- ONLY OCCURS IN GUIDED MEDIA
- PROPAGATION VELOCITY VARIES WITH FREQUENCY
- HENCE VARIOUS FREQUENCY COMPONENTS ARRIVE AT DIFFERENT TIMES
- PARTICULARLY CRITICAL FOR DIGITAL DATA
- SINCE PARTS OF ONE BIT SPILL OVER INTO OTHERS
- CAUSING INTERSYMBOL INTERFERENCE

NOISE

- ADDITIONAL SIGNALS INSERTED BETWEEN TRANSMITTER AND RECEIVER
- THERMAL
  - DUE TO THERMAL AGITATION OF ELECTRONS
  - UNIFORMLY DISTRIBUTED
  - WHITE NOISE
- INTERMODULATION
  - SIGNALS THAT ARE THE SUM AND DIFFERENCE OF ORIGINAL FREQUENCIES SHARING A MEDIUM

NOISE

- CROSSTALK
  - A SIGNAL FROM ONE LINE IS PICKED UP BY ANOTHER
- IMPULSE
  - IRREGULAR PULSES OR SPIKES
    - EG. EXTERNAL ELECTROMAGNETIC INTERFERENCE
  - SHORT DURATION
  - HIGH AMPLITUDE
  - A MINOR ANNOYANCE FOR ANALOG SIGNALS
  - BUT A MAJOR SOURCE OF ERROR IN DIGITAL DATA
    - A NOISE SPIKE COULD CORRUPT MANY BITS

SIGNAL TO NOISE RATIO (SNR)

- SIGNAL TO NOISE RATIO IS RATIO OF SIGNAL POWER TO NOISE POWER.
- RATIO OF WANTED TO UNWANTED SIGNAL.
- HIGH SNR MEANS SIGNAL IS LESS CORRUPTED BY NOISE AND LOW SNR MEANS SIGNAL IS MORE CORRUPTED BY NOISE.
- UNIT IS DECIBEL.

$$\text{SIGNAL TO NOISE RATION (SNR)} = \frac{\text{AVERAGE SIGNAL POWER}}{\text{AVERAGE NOISE POWER}}$$

FACTORS AFFECTING TRANSMISSION SPEED

- AVAILABLE BANDWIDTH
- SIGNAL LEVELS
- CHANNEL QUALITY
- NOISE

CHANNEL CAPACITY

- MAX POSSIBLE DATA RATE ON COMMS CHANNEL
- IS A FUNCTION OF
  - DATA RATE - IN BITS PER SECOND
  - BANDWIDTH - IN CYCLES PER SECOND OR HERTZ
  - NOISE - ON COMMS LINK
  - ERROR RATE - OF CORRUPTED BITS
- LIMITATIONS DUE TO PHYSICAL PROPERTIES
- WANT MOST EFFICIENT USE OF CAPACITY

NYQUIST BANDWIDTH

- CONSIDER NOISE FREE CHANNELS
- IF RATE OF SIGNAL TRANSMISSION IS 2B THEN CAN CARRY SIGNAL WITH FREQUENCIES NO GREATER THAN B
  - IE. GIVEN BANDWIDTH B, HIGHEST SIGNAL RATE IS 2B
- FOR BINARY SIGNALS, 2B BPS NEEDS BANDWIDTH B HZ
- CAN INCREASE RATE BY USING M SIGNAL LEVELS
- NYQUIST FORMULA IS: $C = 2B \log_2 M$
- SO INCREASE RATE BY INCREASING SIGNALS
  - AT COST OF RECEIVER COMPLEXITY
  - LIMITED BY NOISE & OTHER IMPAIRMENTS

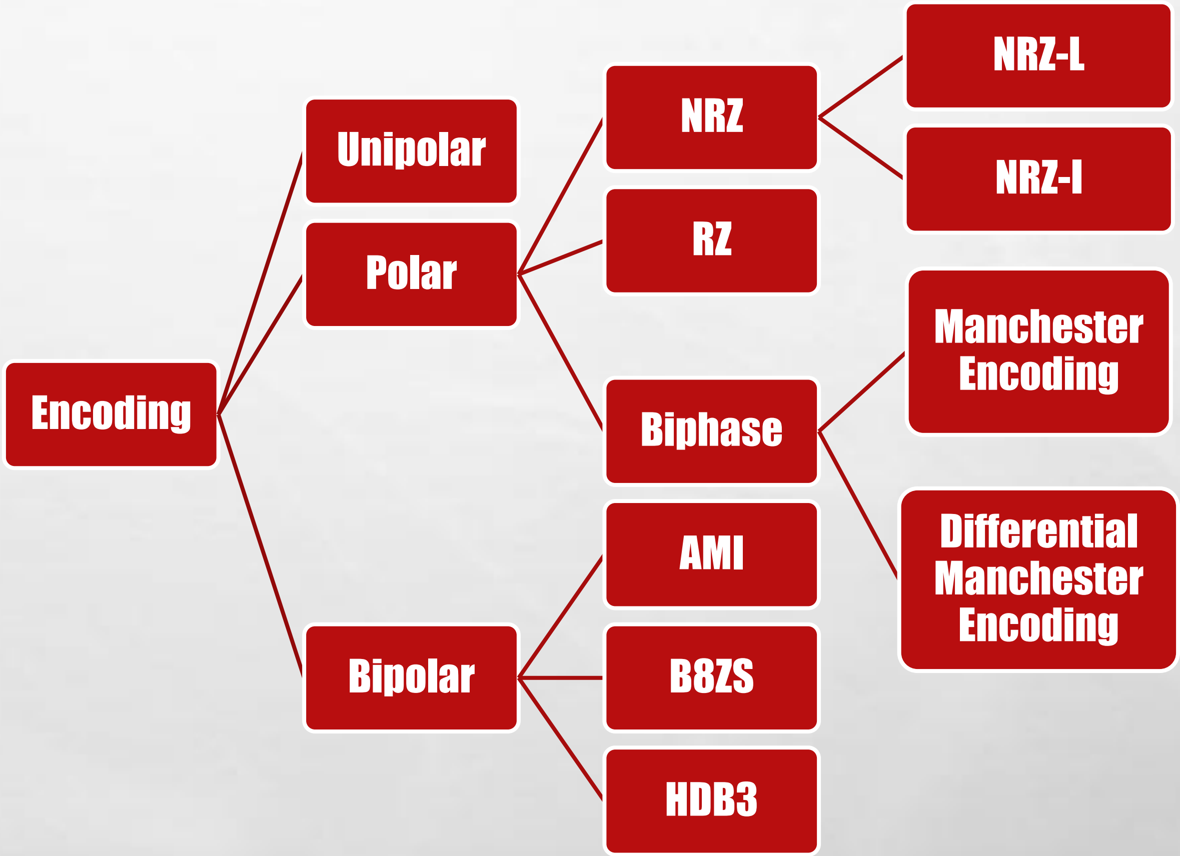
SHANNON CAPACITY FORMULA

- CONSIDER RELATION OF DATA RATE, NOISE & ERROR RATE
  - FASTER DATA RATE SHORTENS EACH BIT SO BURSTS OF NOISE AFFECTS MORE BITS
  - GIVEN NOISE LEVEL, HIGHER RATES MEANS HIGHER ERRORS
- SHANNON DEVELOPED FORMULA RELATING THESE TO SIGNAL TO NOISE RATIO (IN DECIBELS)
- SNR_{DB}=10 LOG_{10} (SIGNAL/NOISE)
- CAPACITY C=B LOG_2(1+SNR)
  - THEORETICAL MAXIMUM CAPACITY
  - GET LOWER IN PRACTISE

LINE ENCODING

- PROCESS OF CONVERTING DIGITAL DATA TO DIGITAL SIGNALS AND VISA VERSA.
- ENCODING – DECODING
- DESIRABLE PROPERTIES:
  - SELF SYNCHRONIZATION
  - LOW PROBABILITY OF BIT ERROR
  - ERROR DETECTION & CORRECTION
  - LESS INTERFERENCE BETWEEN MULTIPLE SIGNALS
  - SMALL SIGNAL TRANSMISSION BANDWIDTH

TYPES OF DIGITAL ENCODING



UNIPOLAR

- USES ONLY ONE POLARITY.
- REPRESENT 1 AND REMAINING IS 0.
- ADVANTAGE:
  - SIMPLE
  - INEXPENSIVE
- DISADVANTAGE
  - DC COMPONENT
  - SYNCHRONIZATION
  - OBSOLETE

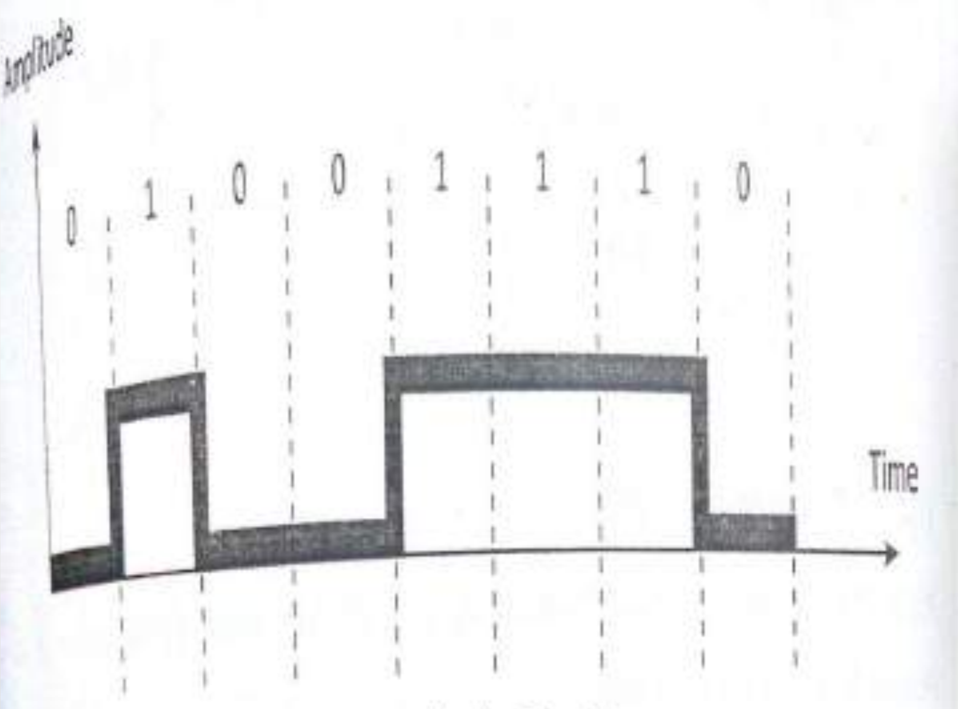


Figure 3.14 : Unipolar Encoding

POLAR ENCODING

- THREE TYPES:
  - NRZ
  - RZ
  - BIPHASE
- USES TWO VOLTAGE LEVELS, + & -.
- NO DC COMPONENT.

NRZ

- NON RETURN TO ZERO
- TWO TYPES
  - NRZ-L
    - LEVEL SIGNAL DETERMINES VALUE OF BIT.
    - POSITIVE VOLTAGE = 0, NEGATIVE VOLTAGE = 1
  - NRZ-I
    - CHANGE THE SIGNAL AT 1
    - NO CHANGE IN SIGNAL WHEN 0

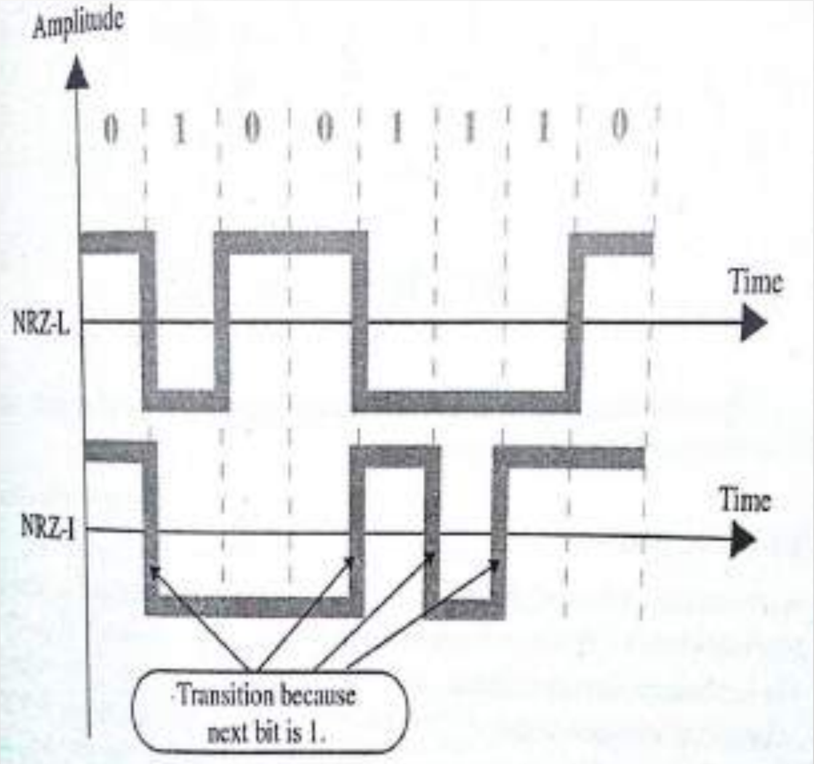


Figure 3.17 : NRZ Encoding

RZ

- TO ASSURE SYNCHRONIZATION, SIGNAL MUST CHANGE EACH BIT.
- SOLUTION, RETURN TO ZERO.
- USES THREE VALUES, POSITIVE, NEGATIVE & ZERO.
- 1 = POSITIVE TO ZERO
- 0 = NEGATIVE TO ZERO
- DISADVANTAGE: REQUIRES TWO SIGNAL CHANGE FOR EACH BIT.

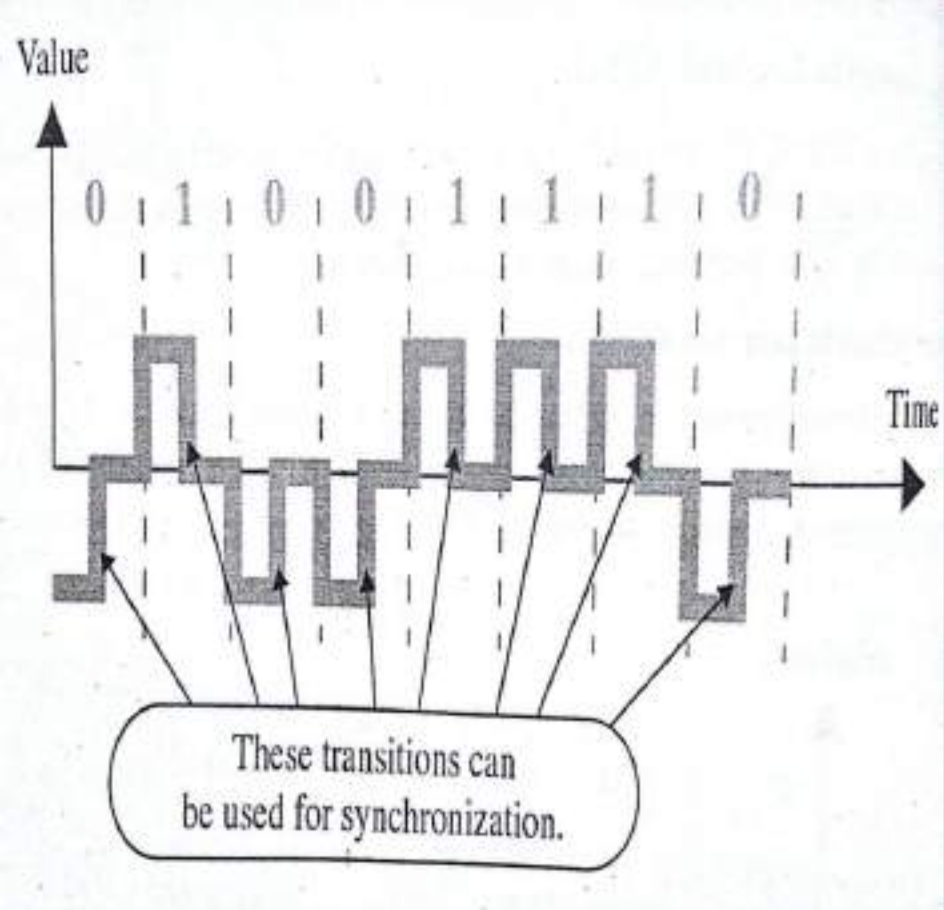


Figure 3.18 : RZ encoding

BI-PHASE ENCODING

- SIGNAL CHANGES AT MIDDLE OF THE BIT BUT, INSTEAD OF RETURNING TO ZERO, RETURNS OPPOSITE POLE.
- TWO TYPES:
  - MANCHESTER ENCODING
  - DIFFERENTIAL MANCHESTER ENCODING
- MANCHESTER ENCODING
  - 1 = NEGATIVE TO POSITIVE
  - 0 = POSITIVE TO NEGATIVE
- DIFFERENTIAL MANCHESTER ENCODING
  - 1 = NO TRANSITION
  - 0 = TRANSITION

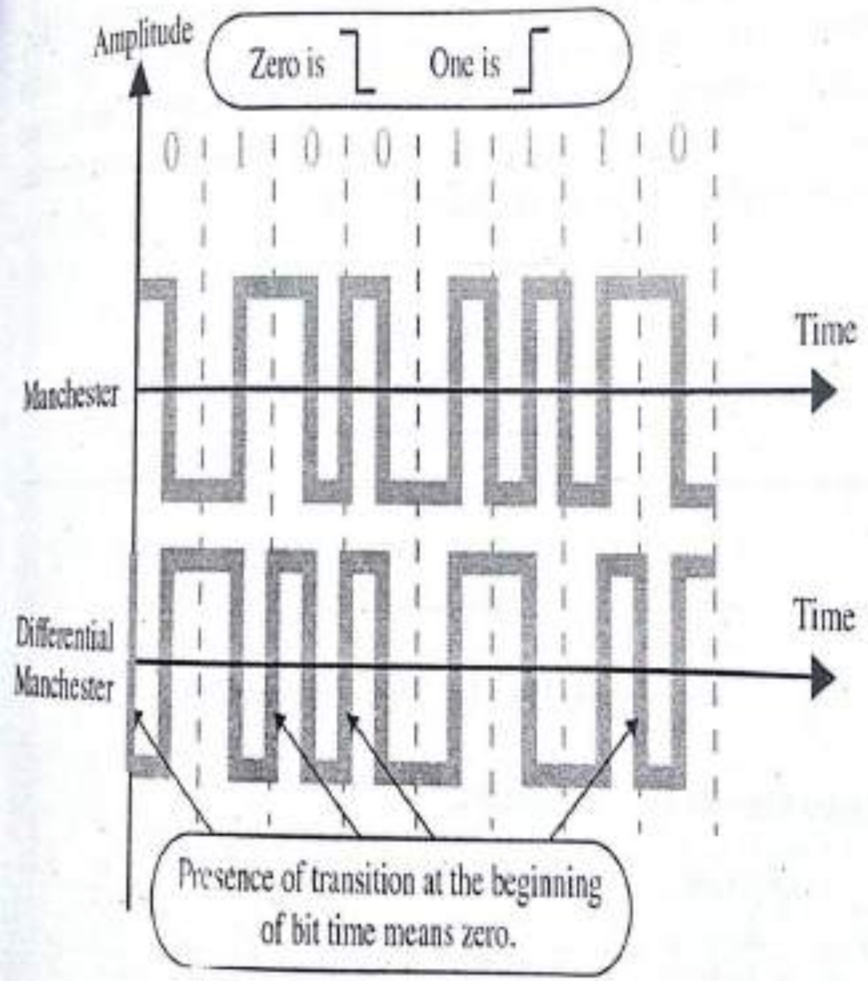


Figure 3.20 : Biphase Encoding

BIPOLAR ENCODING

- USES THREE VOLTAGE LEVELS: POSITIVE, NEGATIVE & ZERO.
- 1 = ALTERNATIVE, POSITIVE OR NEGATIVE
- 0 = ZERO BIT
- ALTERNATION OCCURS WHEN THERE ARE NO CONSECUTIVE 1 BITS
- TYPES
    - AMI
    - B8ZS
    - HDB3

Bipolar Alternate Mark Inversion (AMI)

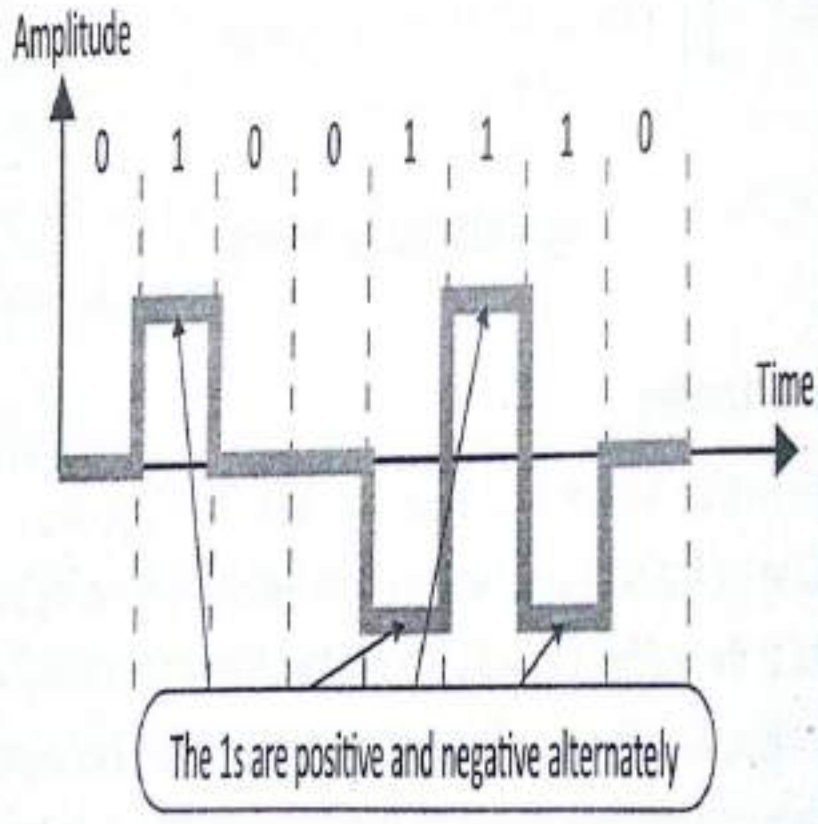


Figure 3.22 : Bipolar AMI

AMI – BIPOLAR ALTERNATIVE MARK INVERSION

- 1 = ALTERNATIVE POSITIVE & NEGATIVE
- 0 = NEUTRAL
- ADVANTAGE:
  - NO DC COMPONENT
  - SYNCHRONIZATION

BIPOLAR WITH 8 ZEROS SUBSTITUTION (B8ZS)

- 8 CONSECUTIVE ZERO VOLTAGES ARE REPLACED BY SEQUENCE 000BOVB.
- ARTIFICIAL SIGNAL CHANGES (CALLED VIOLATIONS) ARE FORCED.
- V = VIOLATION
- NON ZERO VOLTAGE BREAKS AMI RULE OF ENCODING.
- B = BIPOLAR
- WHENEVER 8 ZEROS OCCUR IN SUCCESSION, SCHEME INTRODUCES CHANGES IN PATTERN.

BIPOLAR WITH 8 ZEROS SUBSTITUTION (B8ZS)

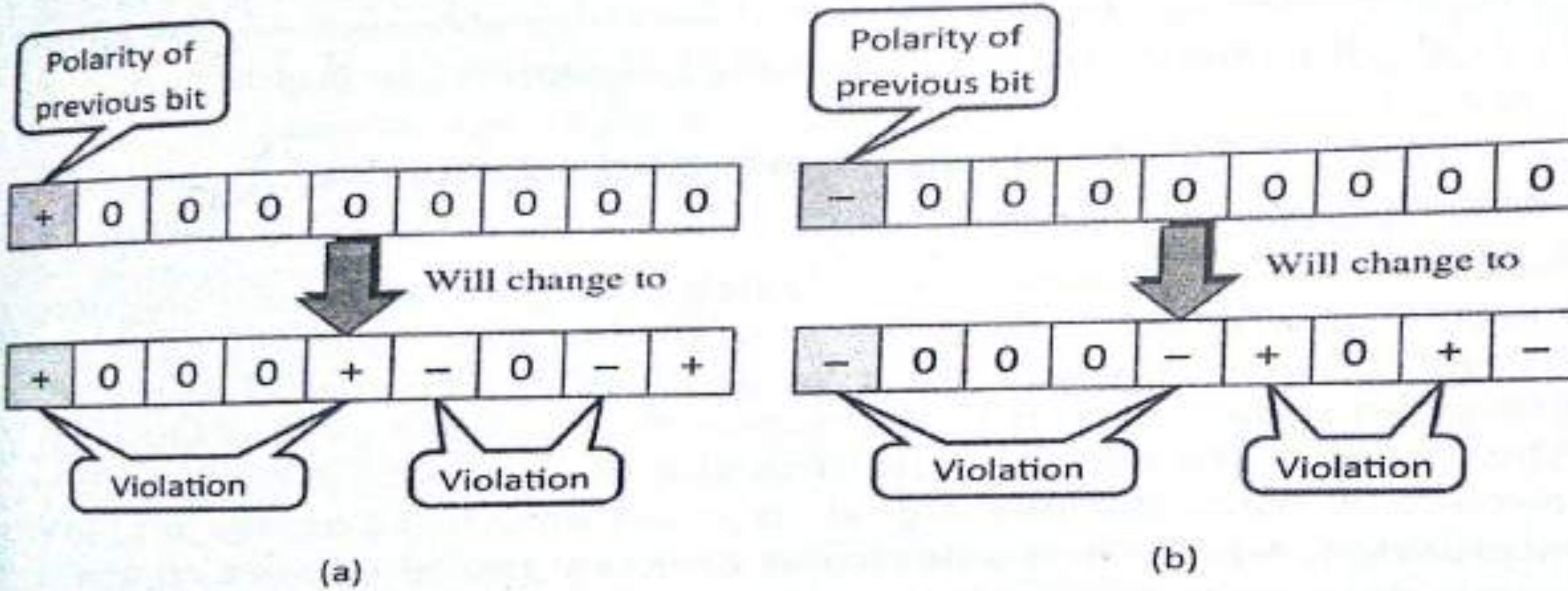
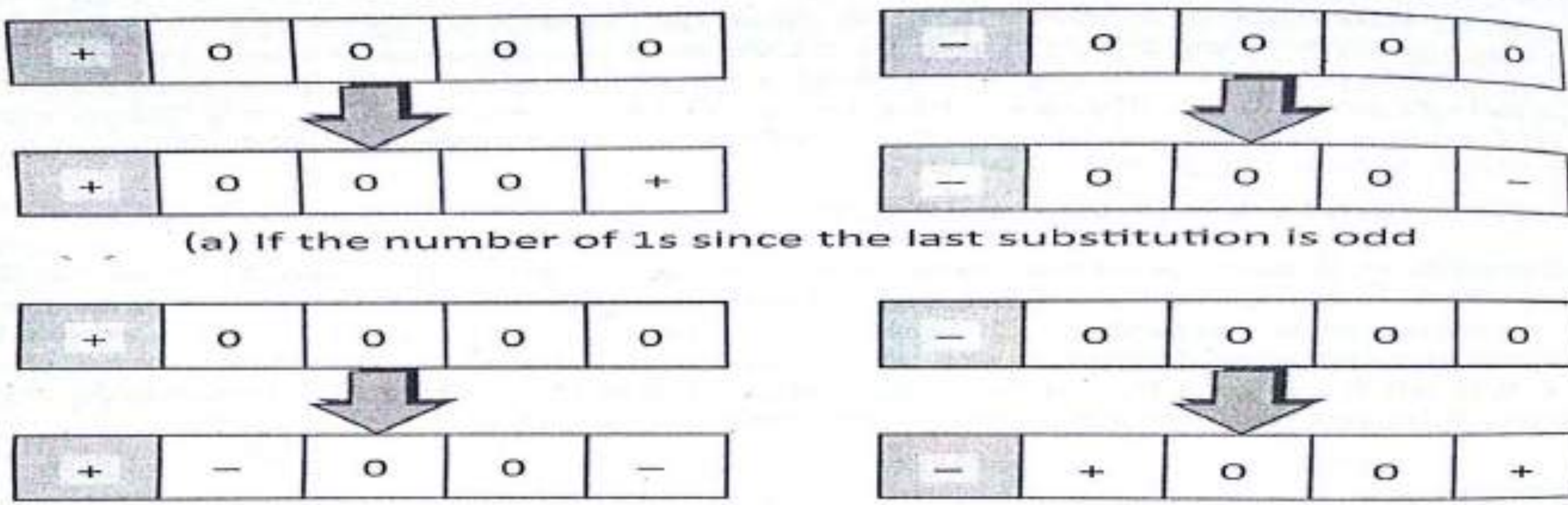


Figure 3.23 : Bipolar with 8 Zeroes Substitution Encoding

HIGH DENSITY BIPOLAR 3 [HDB3]

- IF FOUR 0'S OCCUR ONE AFTER ANOTHER, PATTERN CAN BE CHANGED BASED ON POLARITY OF PREVIOUS 1.



(a) If the number of 1s since the last substitution is odd

(b) If the number of 1s since the last substitution is even

Figure 3.24 : High density Bipolar 3 encoding

MODEMS

- MODULATION & DEMODULATION.
- TWO CATEGORIES
  - EXTERNAL MODEMS
  - INTERNAL MODEMS
- STANDARD INTERFACE USED
  - FOR EXTERNAL MODEMS, RS-232.
  - FOR INTERNAL MODEMS, PORT CONNECTIVITY ON ISA & PCI.

CHARACTERISTICS & TYPES

CHARACTERISTIC

- BPS
- VOICE/DATA
- AUTO ANSWER
- DATA COMPRESSION
- FLASH MEMORY
- FAX CAPABILITY

TYPES

- STANDARD FAX/PHONE MODEM
- DIGITAL CABLE MODEM
- ISDN MODEM
- DSL MODEM
- SATELLITE MODEM

DIGITAL MODULATION

- AMPLITUDE SHIFT KEYING (ASK]
- FREQUENCY SHIFT KEYING [FSK]
- PHASE SHIFT KEYING [PSK]
  - BINARY PHASE SHIFT KEYING [BPSK]
  - DIFFERENTIAL PHASE SHIFT KEYING [DPSK]
  - QUADRATURE PHASE SHIFT KEYING [QPSK]

SUMMARY

- LOOKED AT DATA TRANSMISSION ISSUES
- FREQUENCY, SPECTRUM & BANDWIDTH
- ANALOG VS DIGITAL SIGNALS
- TRANSMISSION IMPAIRMENTS

Data and Computer Communications

Chapter 4 –Transmission Media

Dr. Bhargavi Goswami,
HOD – CS, Associate Professor,
Garden City College,
Bangalore.

Transmission Media

Communication channels in the animal world include touch, sound, sight, and scent. Electric eels even use electric pulses. Ravens also are very expressive. By a combination voice, patterns of feather erection and body posture ravens communicate so clearly that an experienced observer can identify anger, affection, hunger, curiosity, playfulness, fright, boldness, and depression. —Mind of the Raven, Bernd Heinrich

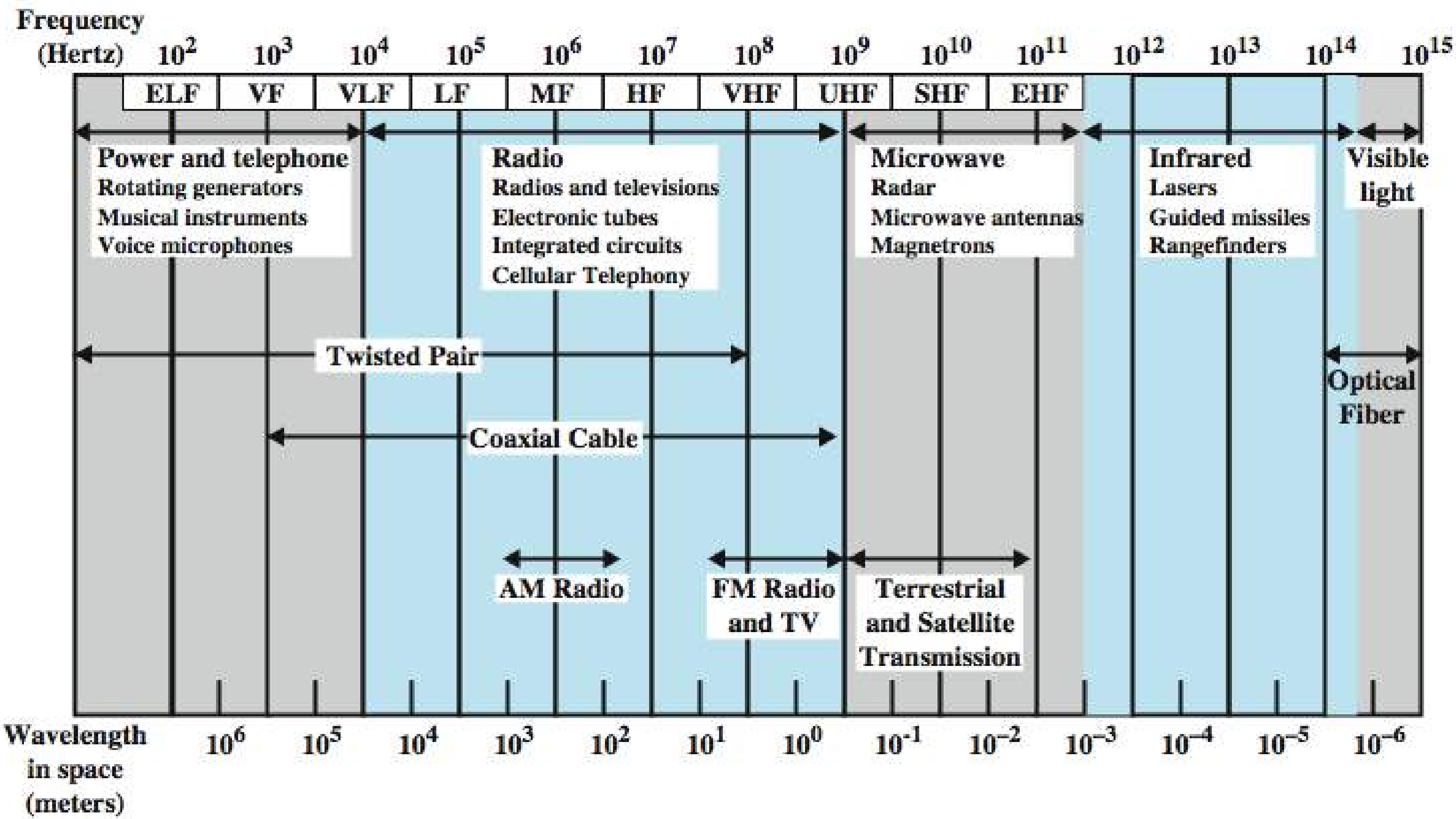
Overview

- guided - wire / optical fibre
- unguided - wireless
- characteristics and quality determined by medium and signal
  - in unguided media - bandwidth produced by the antenna is more important
  - in guided media - medium is more important
- key concerns are data rate and distance

Design Factors

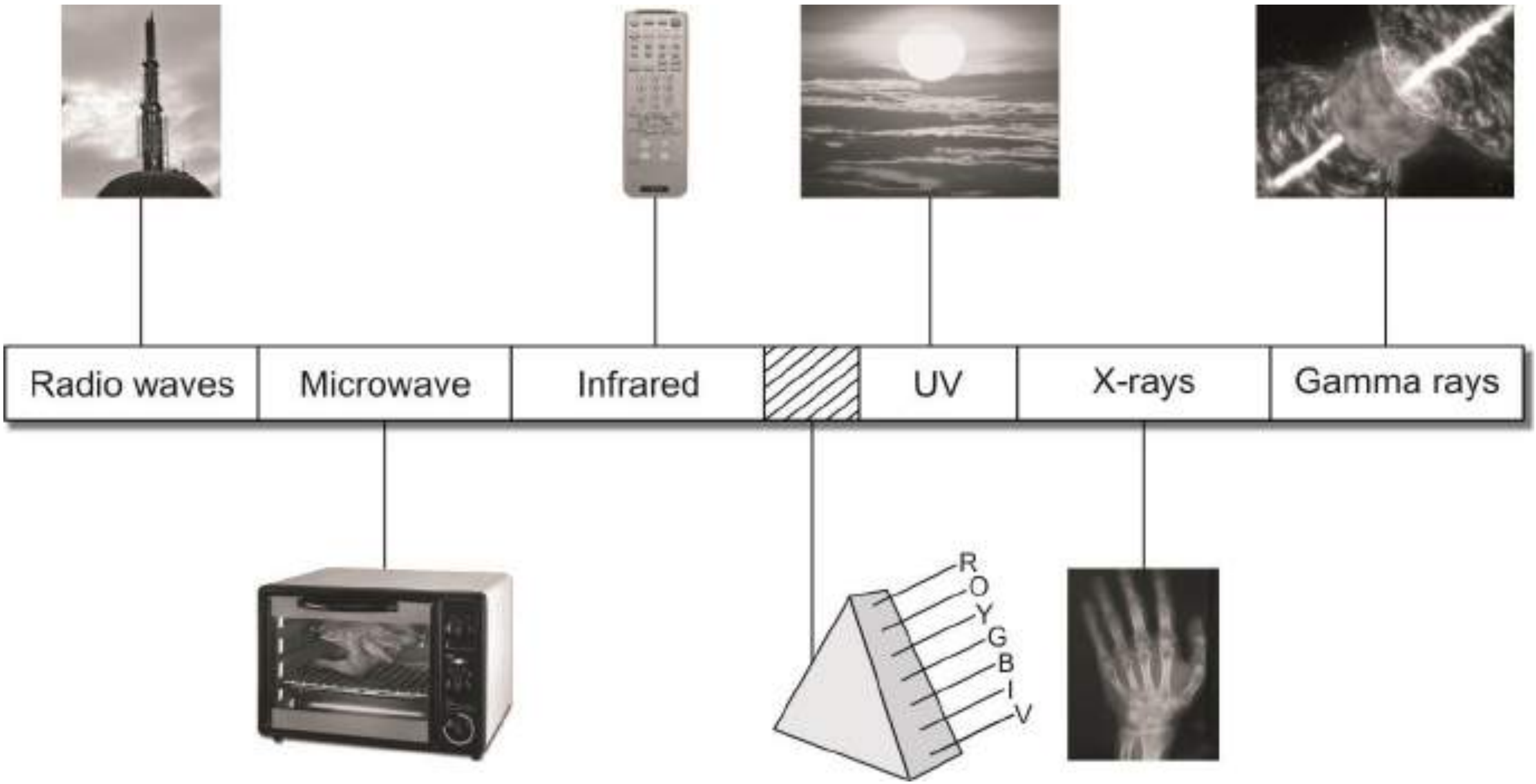
- bandwidth
  - higher bandwidth gives higher data rate
- transmission impairments
  - eg. attenuation
- interference
- number of receivers in guided media
  - more receivers introduces more attenuation

Electromagnetic Spectrum

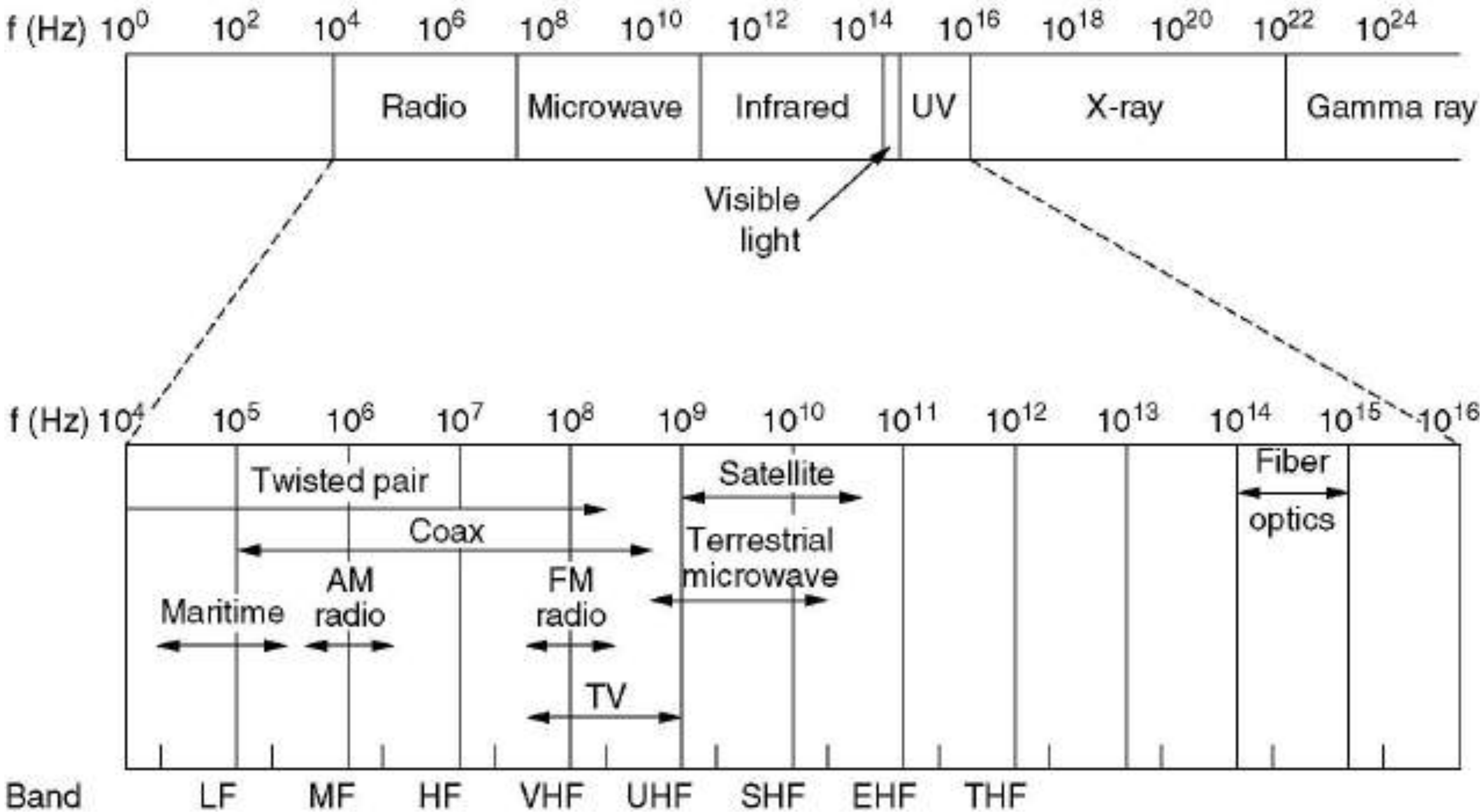


ELF = Extremely low frequency
VF = Voice frequency
VLF = Very low frequency
LF = Low frequency
MF = Medium frequency
HF = High frequency
VHF = Very high frequency
UHF = Ultrahigh frequency
SHF = Superhigh frequency
EHF = Extremely high frequency

The spectrum



Electromagnetic Spectrum with Range Specification

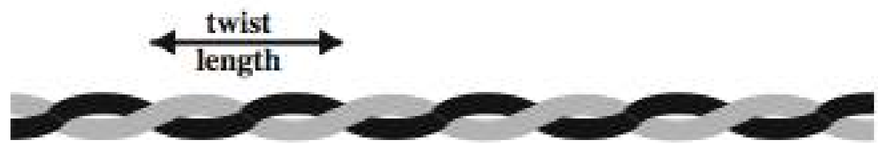


Transmission Characteristics of Guided Media

	Frequency Range	**Typical Attenuation**	**Typical Delay**	**Repeater Spacing**
Twisted pair (with loading)	0 to 3.5 kHz	0.2 dB/km @ 1 kHz	50 μs/km	2 km
Twisted pairs (multi-pair cables)	0 to 1 MHz	0.7 dB/km @ 1 kHz	5 μs/km	2 km
Coaxial cable	0 to 500 MHz	7 dB/km @ 10 MHz	4 μs/km	1 to 9 km
Optical fiber	186 to 370 THz	0.2 to 0.5 dB/km	5 μs/km	40 km

Twisted Pair

- Separately insulated
- Twisted together
- Often "bundled" into cables
- Usually installed in building during construction



(a) Twisted pair

Twisted Pair - Transmission Characteristics

- analog
  - needs amplifiers every 5km to 6km
- digital
  - can use either analog or digital signals
  - needs a repeater every 2-3km
- limited distance
- limited bandwidth (1MHz)
- limited data rate (100MHz)
- susceptible to interference and noise

Unshielded vs Shielded TP

- unshielded Twisted Pair (UTP)
  - ordinary telephone wire
  - cheapest
  - easiest to install
  - suffers from external EM interference
- shielded Twisted Pair (STP)
  - metal braid or sheathing that reduces interference
  - more expensive
  - harder to handle (thick, heavy)
- in a variety of categories - see EIA-568

UTP Categories

	Category 3 Class C	Category 5 Class D	Category 5E	Category 6 Class E	Category 7 Class F
Bandwidth	16 MHz	100 MHz	100 MHz	200 MHz	600 MHz
Cable Type	UTP	UTP/FTP	UTP/FTP	UTP/FTP	SSTP
Link Cost (Cat 5 =1)	0.7	1	1.2	1.5	2.2

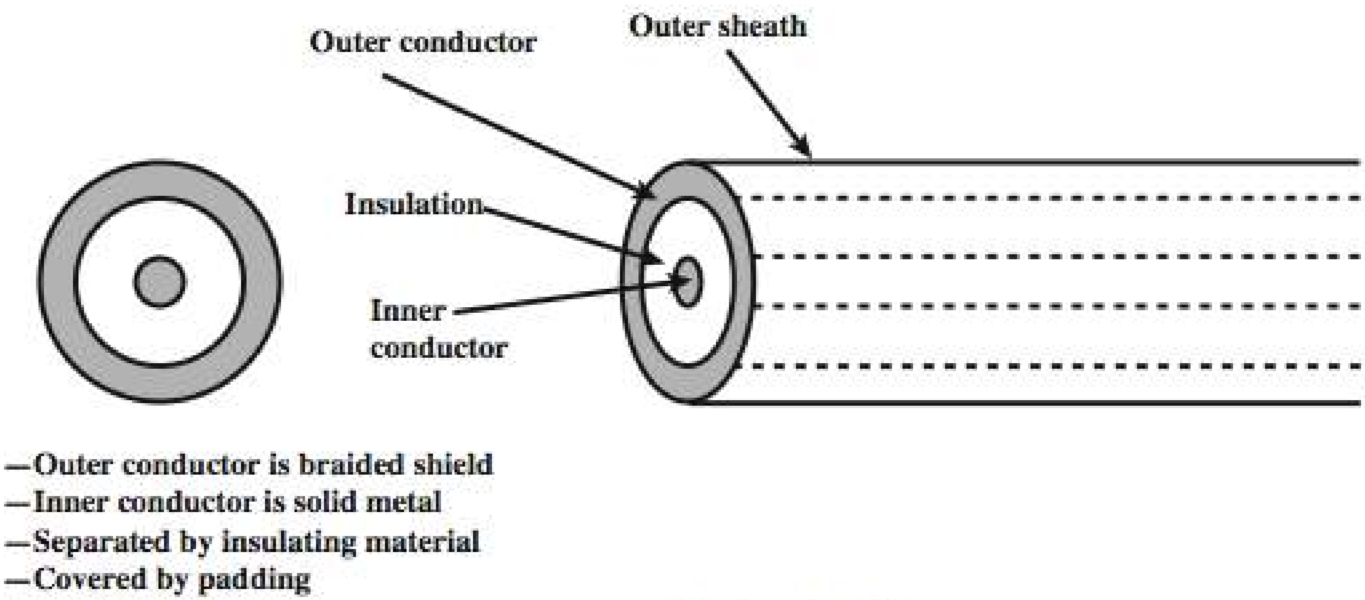
Comparison of Shielded and Unshielded Twisted Pair

	Attenuation (dB per 100 m)			Near-end Crosstalk (dB)		
Frequency (MHz)	Category 3 UTP	Category 5 UTP	150-ohm STP	Category 3 UTP	Category 5 UTP	150-ohm STP
1	2.6	2.0	1.1	41	62	58
4	5.6	4.1	2.2	32	53	58
16	13.1	8.2	4.4	23	44	50.4
25	—	10.4	6.2	—	41	47.5
100	—	22.0	12.3	—	32	38.5
300	—	—	21.4	—	—	31.3

Near End Crosstalk

- coupling of signal from one pair to another
- occurs when transmit signal entering the link couples back to receiving pair
- ie. near transmitted signal is picked up by near receiving pair

Coaxial Cable

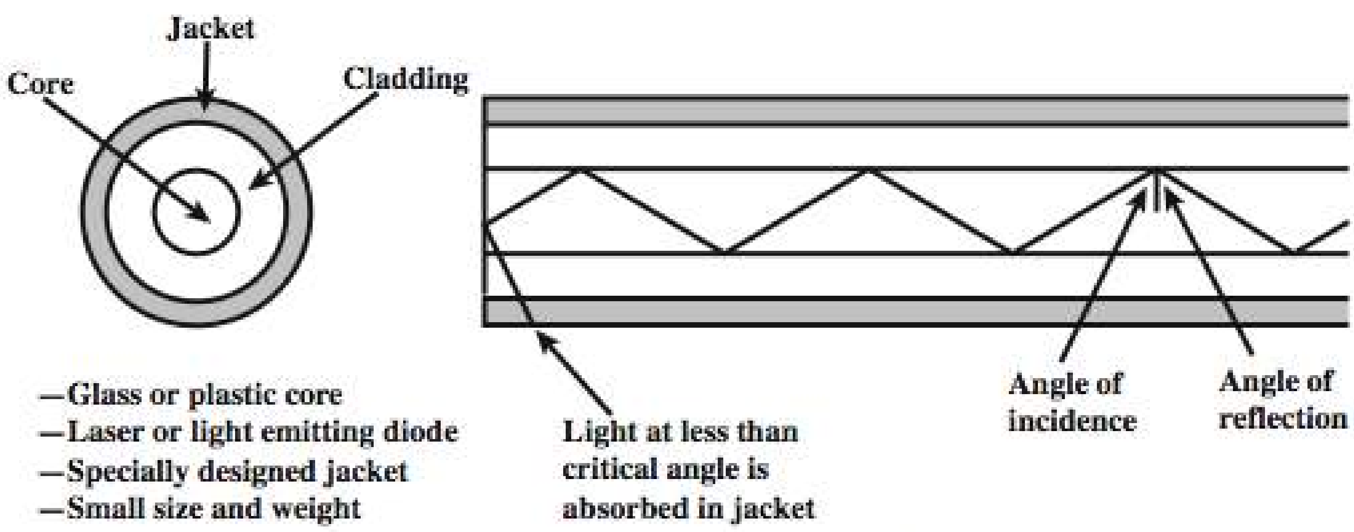


(b) Coaxial cable

Coaxial Cable - Transmission Characteristics

- superior frequency characteristics to TP
- performance limited by attenuation & noise
- analog signals
  - amplifiers every few km
  - closer if higher frequency
  - up to 500MHz
- digital signals
  - repeater every 1km
  - closer for higher data rates

Optical Fiber



(c) Optical fiber

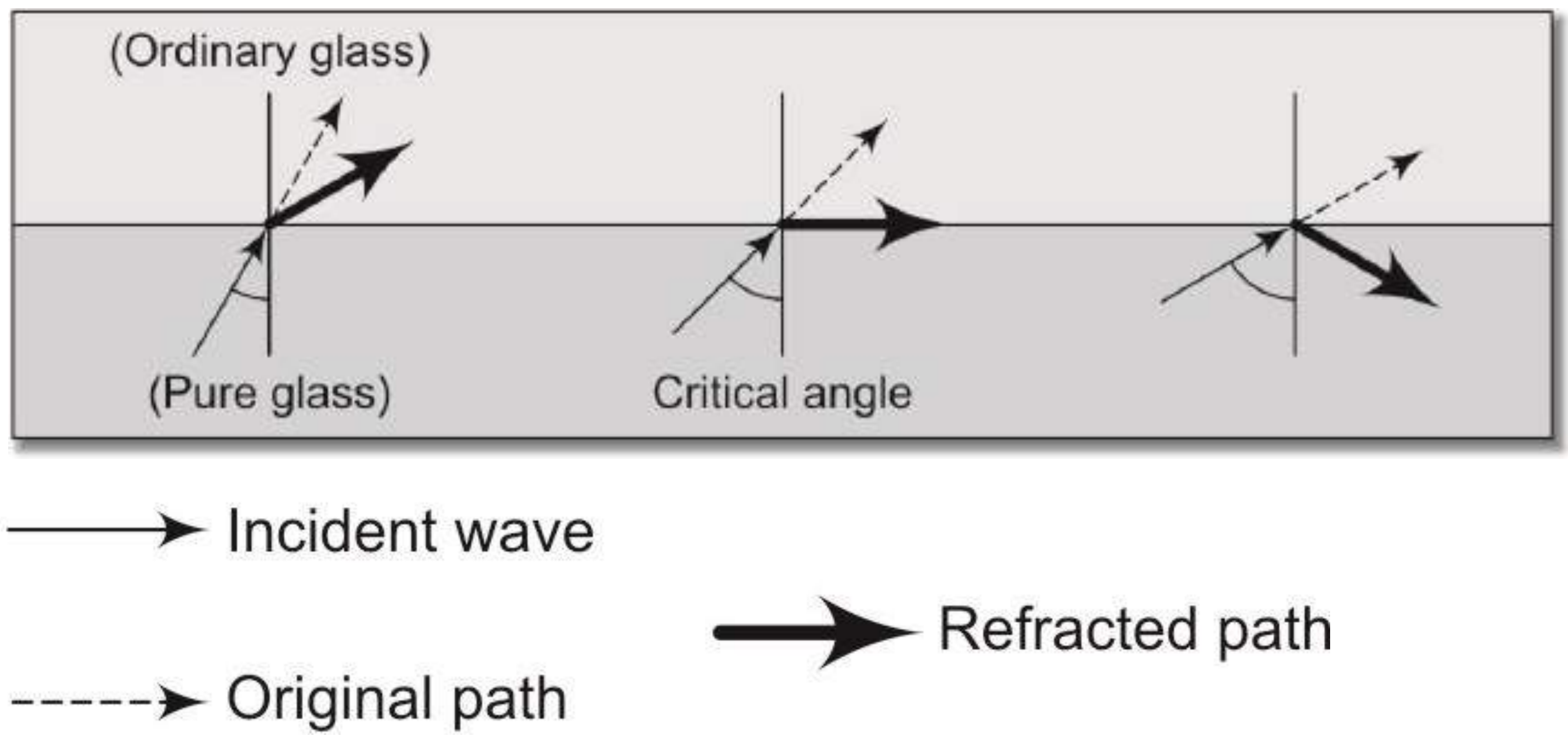
Optical Fiber - Benefits

- greater capacity
  - data rates of hundreds of Gbps
- smaller size & weight
- lower attenuation
- electromagnetic isolation
- greater repeater spacing
  - 10s of km at least

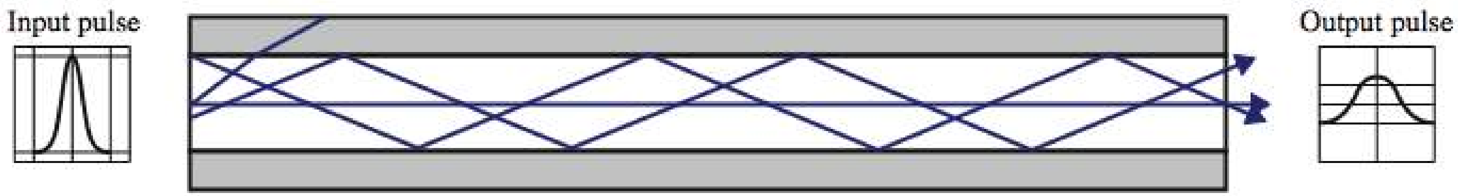
Optical Fiber - Transmission Characteristics

- uses total internal reflection to transmit light
  - effectively acts as wave guide for 10^{14} to 10^{15} Hz
- can use several different light sources
  - Light Emitting Diode (LED)
    - cheaper, wider operating temp range, lasts longer
  - Injection Laser Diode (ILD)
    - more efficient, has greater data rate
- relation of wavelength, type & data rate

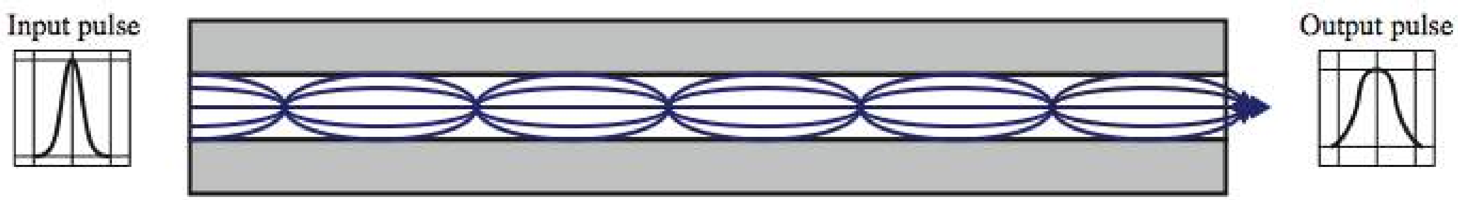
Total Internal Reflection



Optical Fiber Transmission Modes



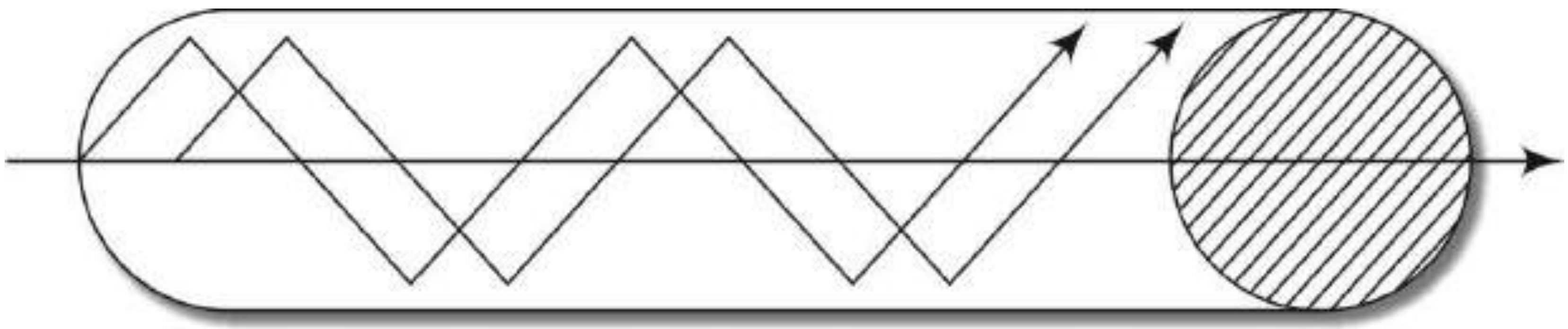
(a) Step-index multimode



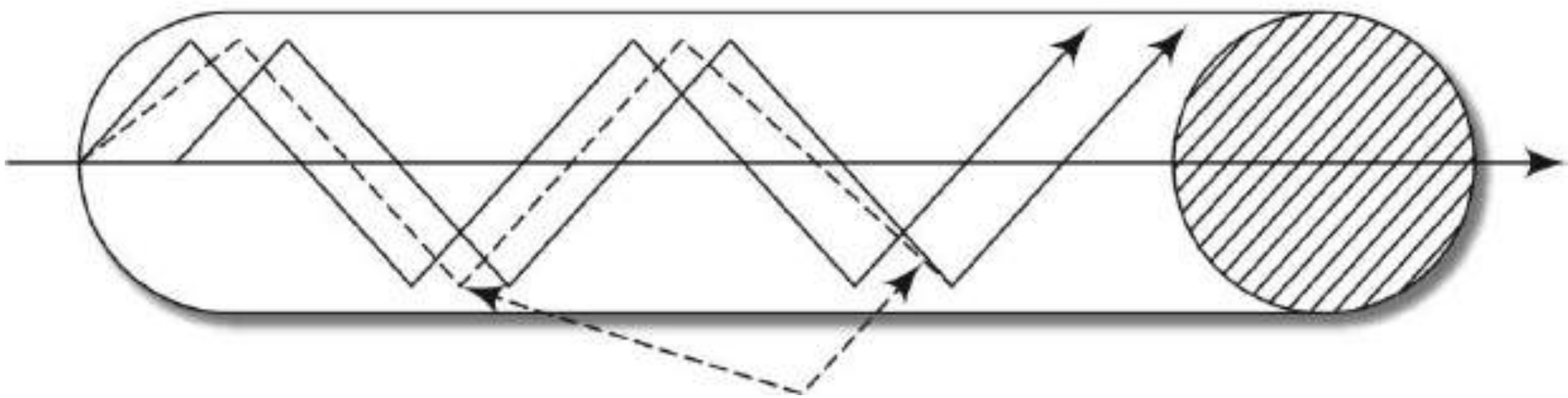
(b) Graded-index multimode

(c) Single mode

Dispersion in fiber optic



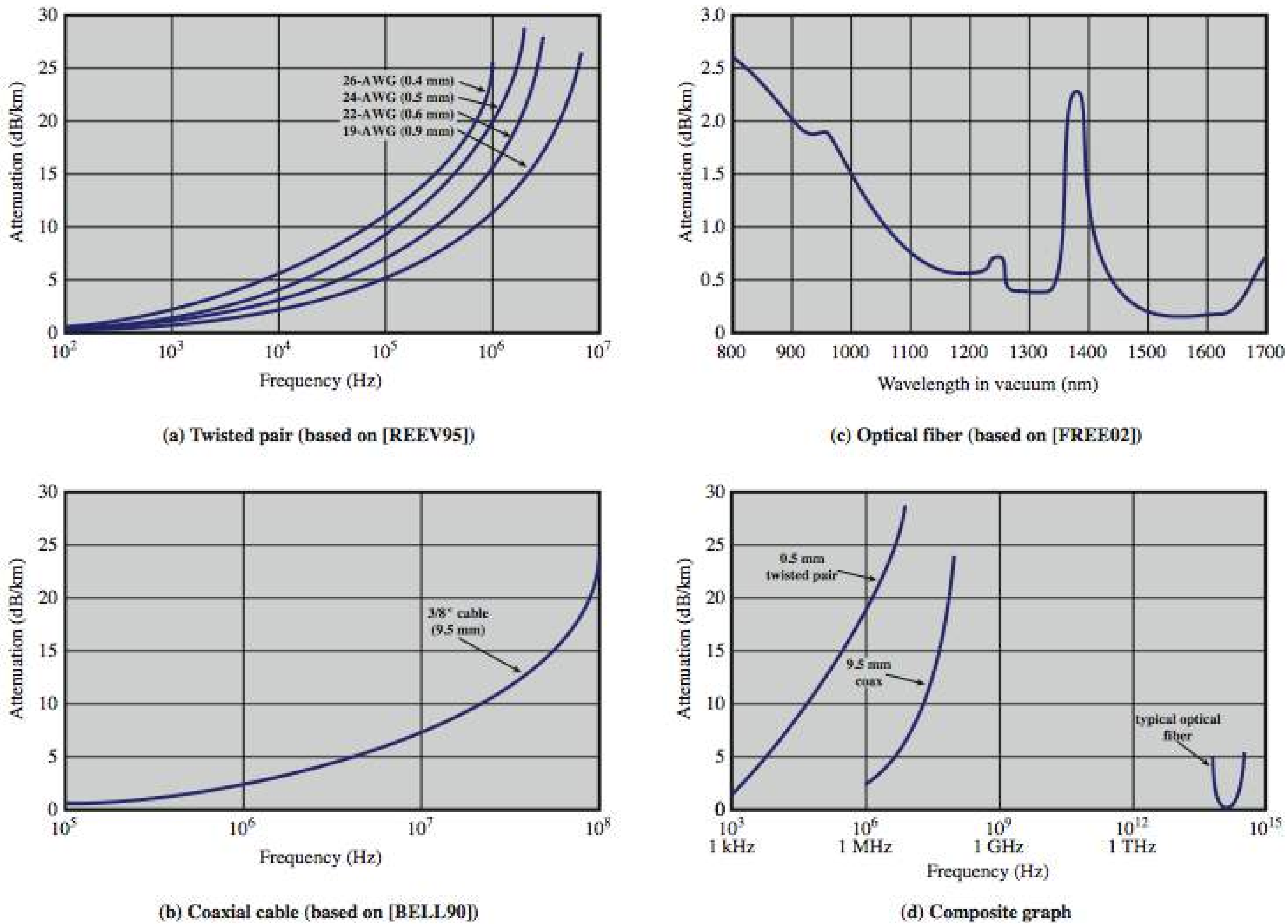
Normal transmission where two different waves travelling together



Frequency Utilization for Fiber Applications

Wave length (in vacuum) range (nm)	Frequency Range (THz)	Band Label	Fiber Type	Application
820 to 900	366 to 333		Multimode	LAN
1280 to 1350	234 to 222	S	Single mode	Various
1528 to 1561	196 to 192	C	Single mode	WDM
1561 to 1620	192 to 185	L	Single mode	WDM

Attenuation in Guided Media



Comparison: UTP vs. FO

- Thickness (FO thicker than UTP)
- Weight (FO 1/100th of UTP)
- Photons vs. electrons (Electrons feel more resistance, temperature, hence cross talk. Photons immune to them)
- Attenuation (FO need amplification after 60km, UTP needs amplification every 5km)
- Erosion (Copper erode faster, Glass has less environmental effects.

Comparison: UTP vs. FO

- Effect of EM interference (High on UTP and less on FO)
- Leaking (High risk of eavesdropping and tapping attack in UTP then FO)
- Bandwidth (Far more in FO then UTP)
- Cost (FO far more expensive than UTP)
- Need for skilled engineer (in FO and not in UTP)
- Technology Complexity (High in FO and easy in UTP)
- Flexibility (High in UTP and low in FO)

Wireless Transmission Frequencies

- 2GHz to 40GHz
  - microwave
  - highly directional
  - point to point
  - satellite
- 30MHz to 1GHz
  - omnidirectional
  - broadcast radio
- 3 x 10^{11} to 2 x 10^{14}
  - infrared
  - local

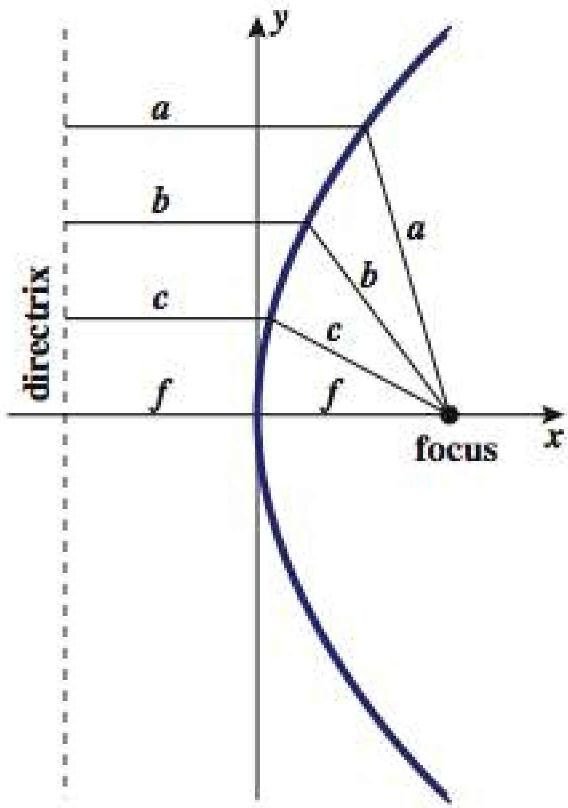
Antennas

- electrical conductor used to radiate or collect electromagnetic energy
- transmission antenna
  - radio frequency energy from transmitter
  - converted to electromagnetic energy byy antenna
  - radiated into surrounding environment
- reception antenna
  - electromagnetic energy impinging on antenna
  - converted to radio frequency electrical energy
  - fed to receiver
- same antenna is often used for both purposes

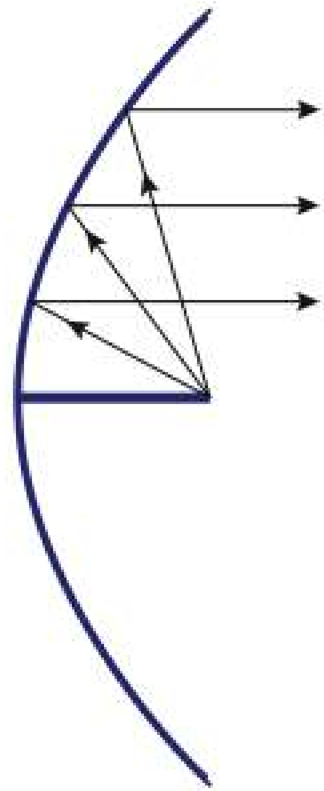
Radiation Pattern

- power radiated in all directions
- not same performance in all directions
  - as seen in a radiation pattern diagram
- an isotropic antenna is a (theoretical) point in space
  - radiates in all directions equally
  - with a spherical radiation pattern

Parabolic Reflective Antenna



(a) Parabola



(b) Cross-section of parabolic antenna showing reflective property

Antenna Gain

- measure of directionality of antenna
- power output in particular direction verses that produced by an isotropic antenna
- measured in decibels (dB)
- results in loss in power in another direction
- effective area relates to size and shape
  - related to gain

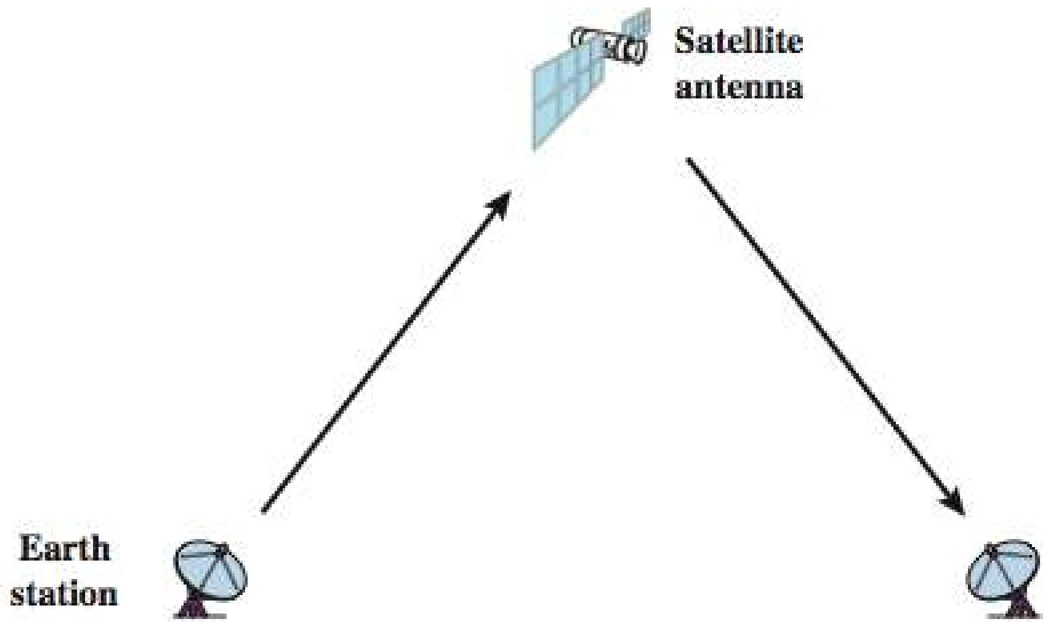
Terrestrial Microwave

- used for long haul telecommunications
- and short point-to-point links
- requires fewer repeaters but line of sight
- use a parabolic dish to focus a narrow beam onto a receiver antenna
- 1-40GHz frequencies
- higher frequencies give higher data rates
- main source of loss is attenuation
  - distance, rainfall
- also interference

Satellite Microwave

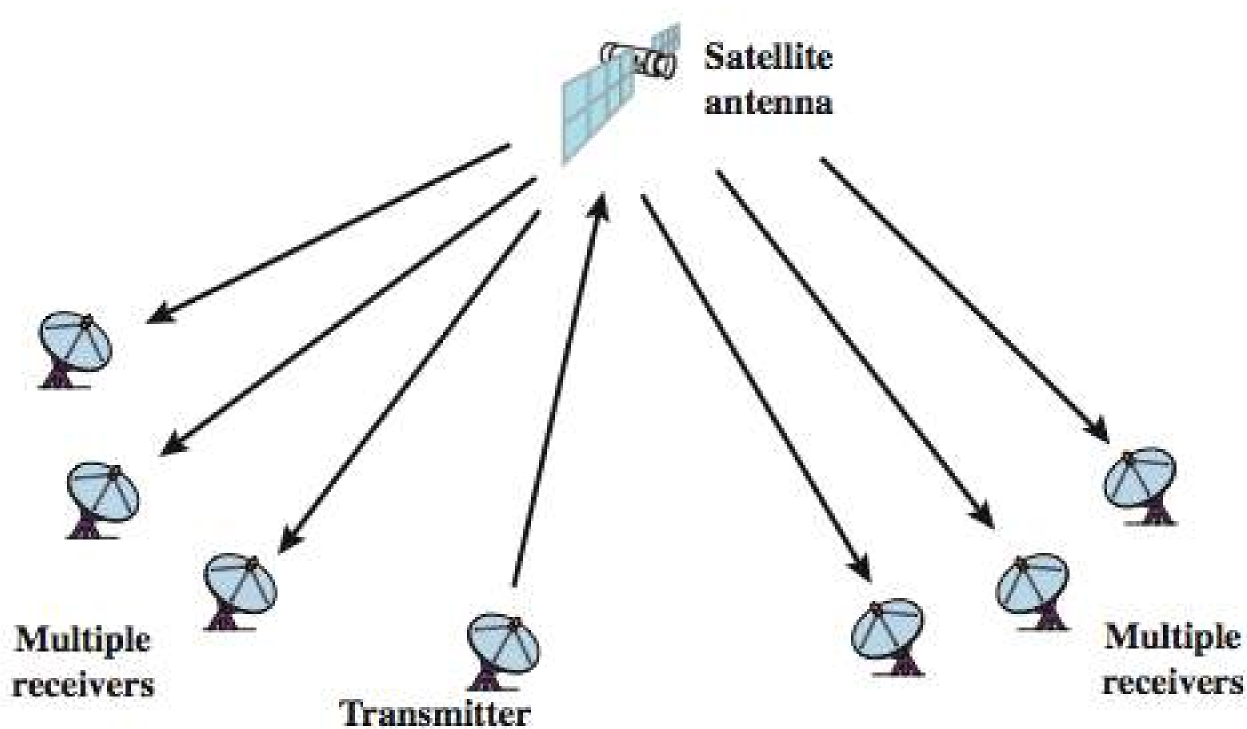
- satellite is relay station
- receives on one frequency, amplifies or repeats signal and transmits on another frequency
  - eg. uplink 5.925-6.425 GHz & downlink 3.7-4.2 GHz
- typically requires geo-stationary orbit
  - height of 35,784km
  - spaced at least 3-4° apart
- typical uses
  - television
  - long distance telephone
  - private business networks
  - global positioning

Satellite Point to Point Link



(a) Point-to-point link

Satellite Broadcast Link



(b) Broadcast link

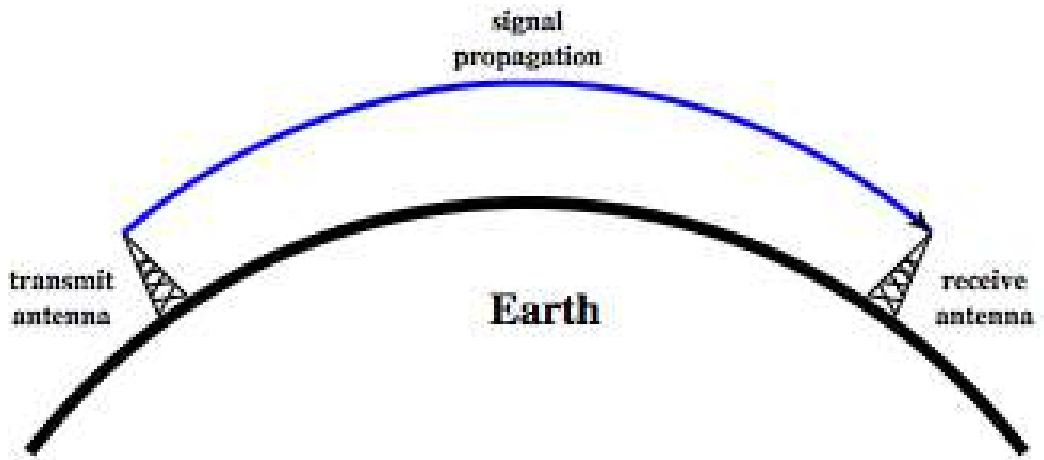
Broadcast Radio

- radio is 3kHz to 300GHz
- use broadcast radio, 30MHz - 1GHz, for:
  - FM radio
  - UHF and VHF television
- is omnidirectional
- still need line of sight
- suffers from multipath interference
  - reflections from land, water, other objects

Infrared

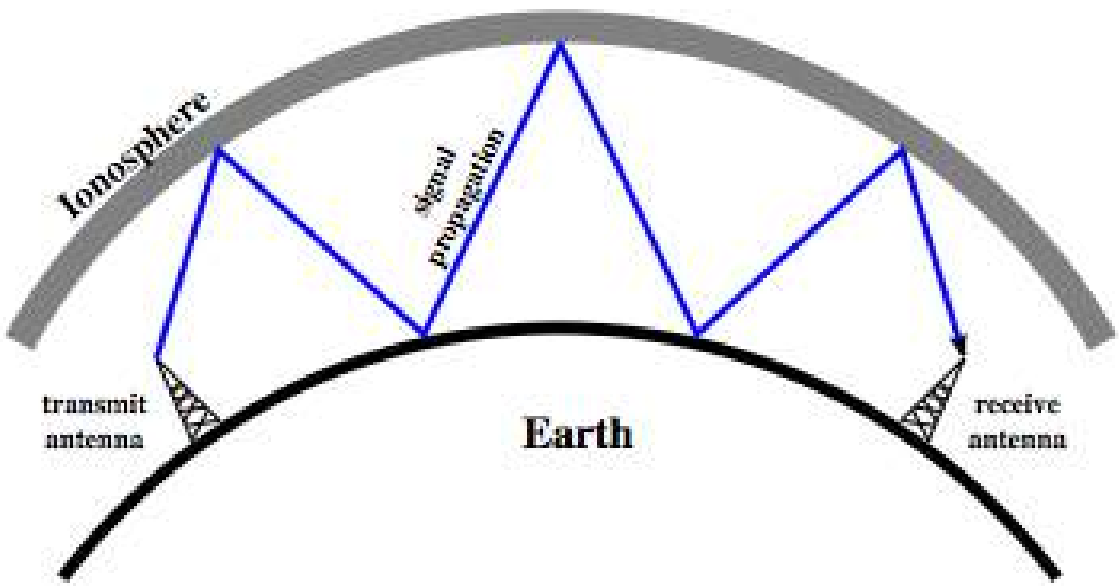
- modulate noncoherent infrared light
- end line of sight (or reflection)
- are blocked by walls
- no licenses required
- typical uses
  - TV remote control
  - IRD port

Wireless Propagation Ground Wave



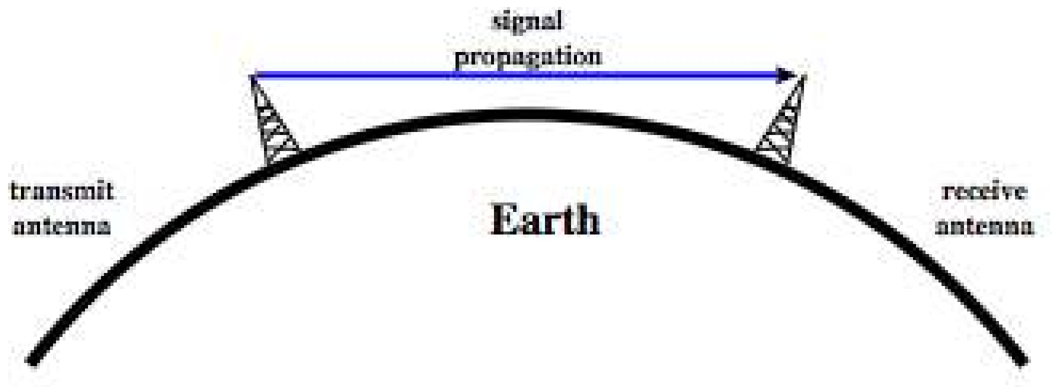
(a) Ground-wave propagation (below 2 MHz)

Wireless Propagation
Sky Wave



(b) Sky-wave propagation (2 to 30 MHz)

Wireless Propagation
Line of Sight



(c) Line-of-sight (LOS) propagation (above 30 MHz)

Refraction

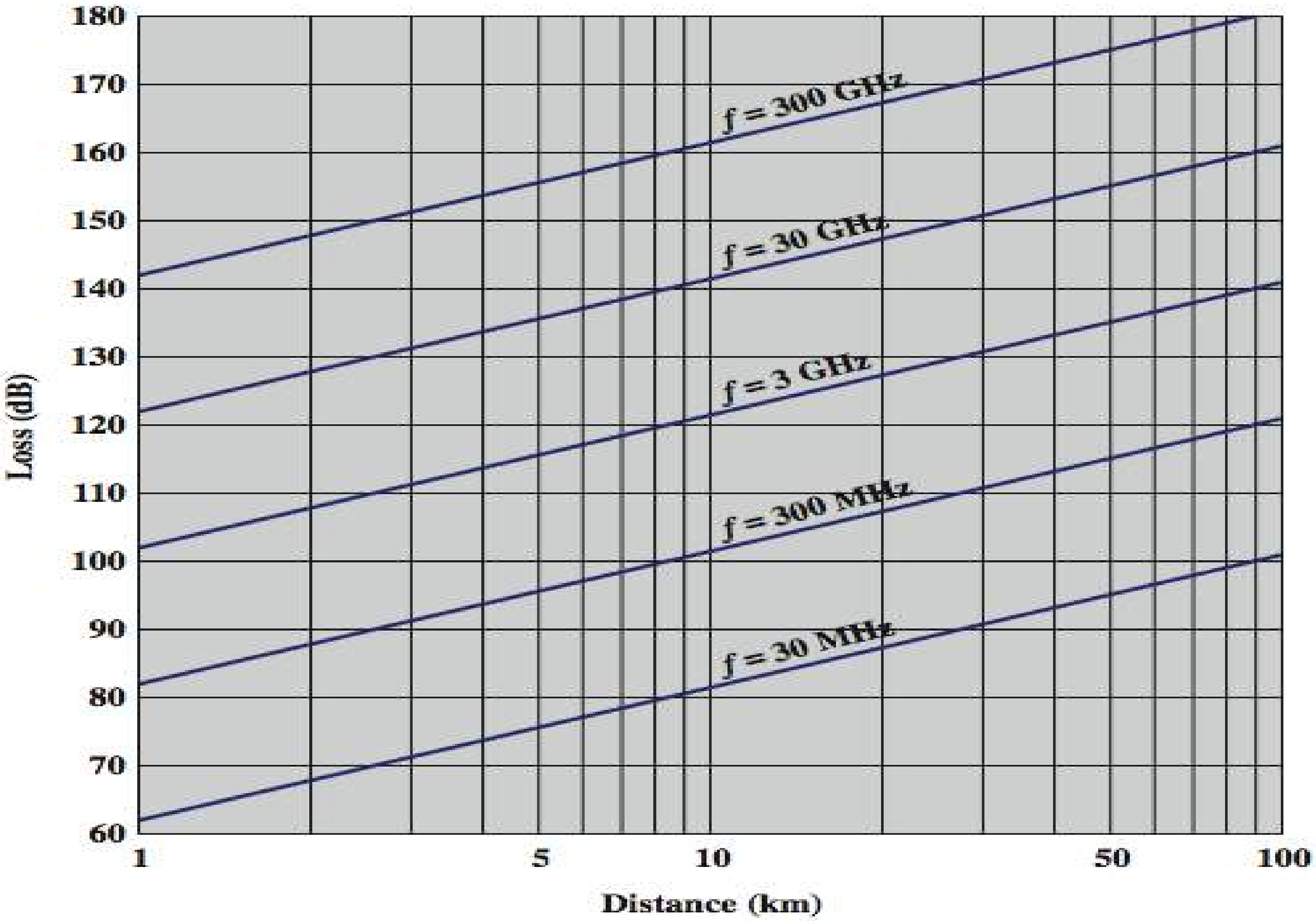
- velocity of electromagnetic wave is a function of density of material

  ~3 x 10^8 m/s in vacuum, less in anything else
- speed changes as move between media
- Index of refraction (refractive index) is
  - `sin(incidence)/sin(refraction)`
  - varies with wavelength
- have gradual bending if medium density varies
  - density of atmosphere decreases with height
  - results in bending towards earth of radio waves
  - hence optical and radio horizons differ

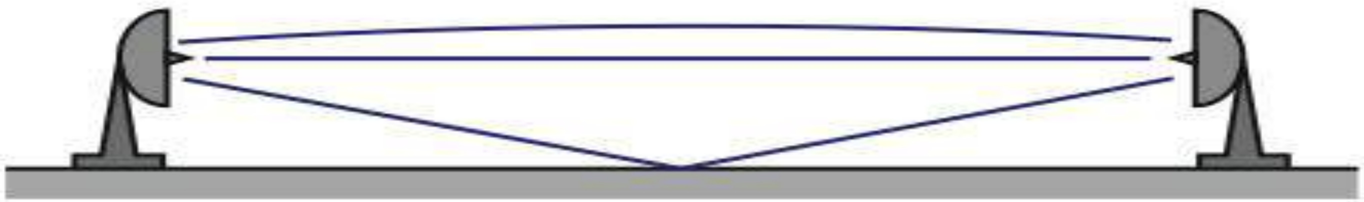
Line of Sight Transmission

- Free space loss
  - loss of signal with distance
- Atmospheric Absorption
  - from water vapour and oxygen absorption
- Multipath
  - multiple interfering signals from reflections
- Refraction
  - bending signal away from receiver

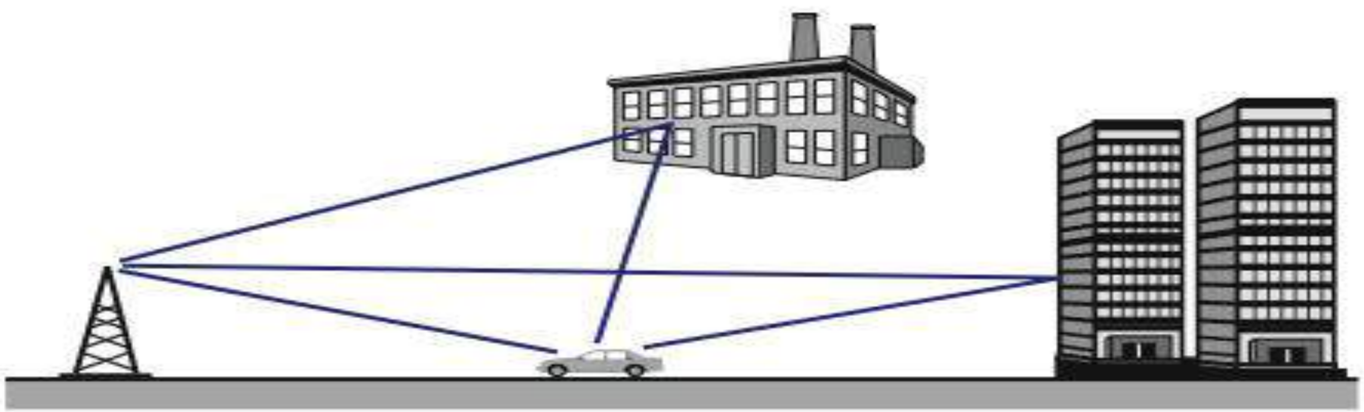
Free Space Loss



Multipath Interference



(a) Microwave line of sight



(b) Mobile radio

Fiber Optics v/s Satellite Wire v/s Wireless

- Practically? Single fiber has, more potential bandwidth than all the satellites ever launched but, this bandwidth is not available to most users practically.
- Mobile Communication? Terrestrial fiber optic links are of no use to them.

- With satellites, it is practical for a user to erect an antenna on the roof of the building and completely bypass wired system to get high bandwidth.
- satellite links potentially are most suitable for mobile communication.

Fiber Optics v/s Satellite Wire v/s Wireless

- Broadcasting?
  Not suitable for broadcasting.
- Cost?
  Costly for communication in places with hostile terrain or a poorly developed terrestrial infrastructure.
- Right of Way? for laying fiber is difficult or unduly expensive.
- Rapid Deployment?
  Fiber optics is costly in terms of skilled engineers.

- Message sent by satellite can be received by thousands of ground stations at once. Best suited.
- Launching one satellite was cheaper than stringing thousands of undersea cables among the 13,677 islands.
- Instead launching one satellite would be cheaper.
- When rapid deployment is critical, as in military communication systems in time of war, satellites win easily

MULTIPLEXING

- MUX – DEMUX
- TYPES
  - FREQUENCY DIVISION MULTIPLEXING
  - TIME DIVISION MULTIPLEXING
    - ASYNCHRONOUS V/S SYNCHRONOUS TDM
  - WAVELENGTH DIVISION MULTIPLEXING
  - SONET MULTIPLEXING (SYNCHRONOUS – OPTICAL NETWORK MULTIPLEXING)

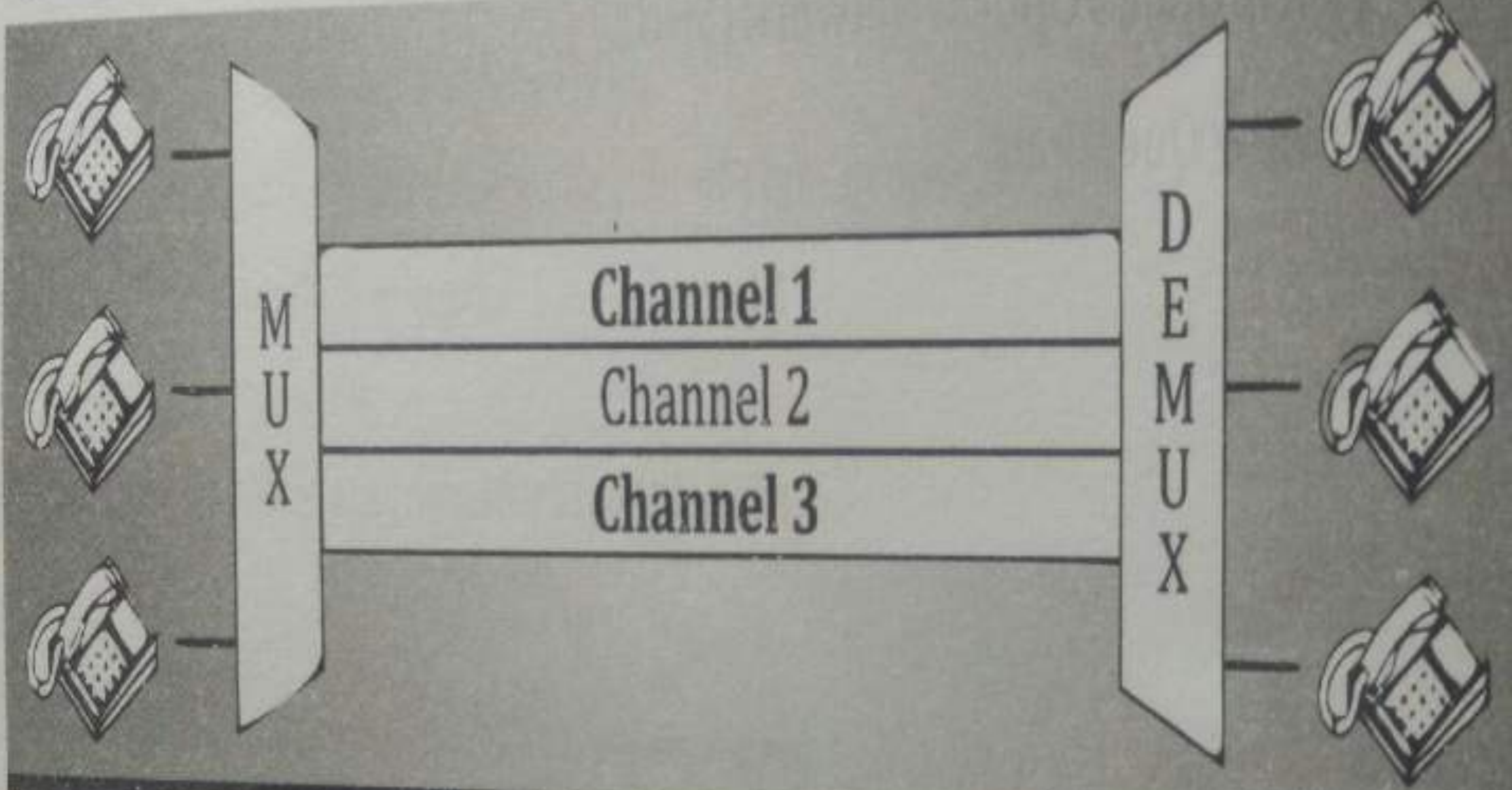


Figure 7.1 Multiplexing and Demultiplexing

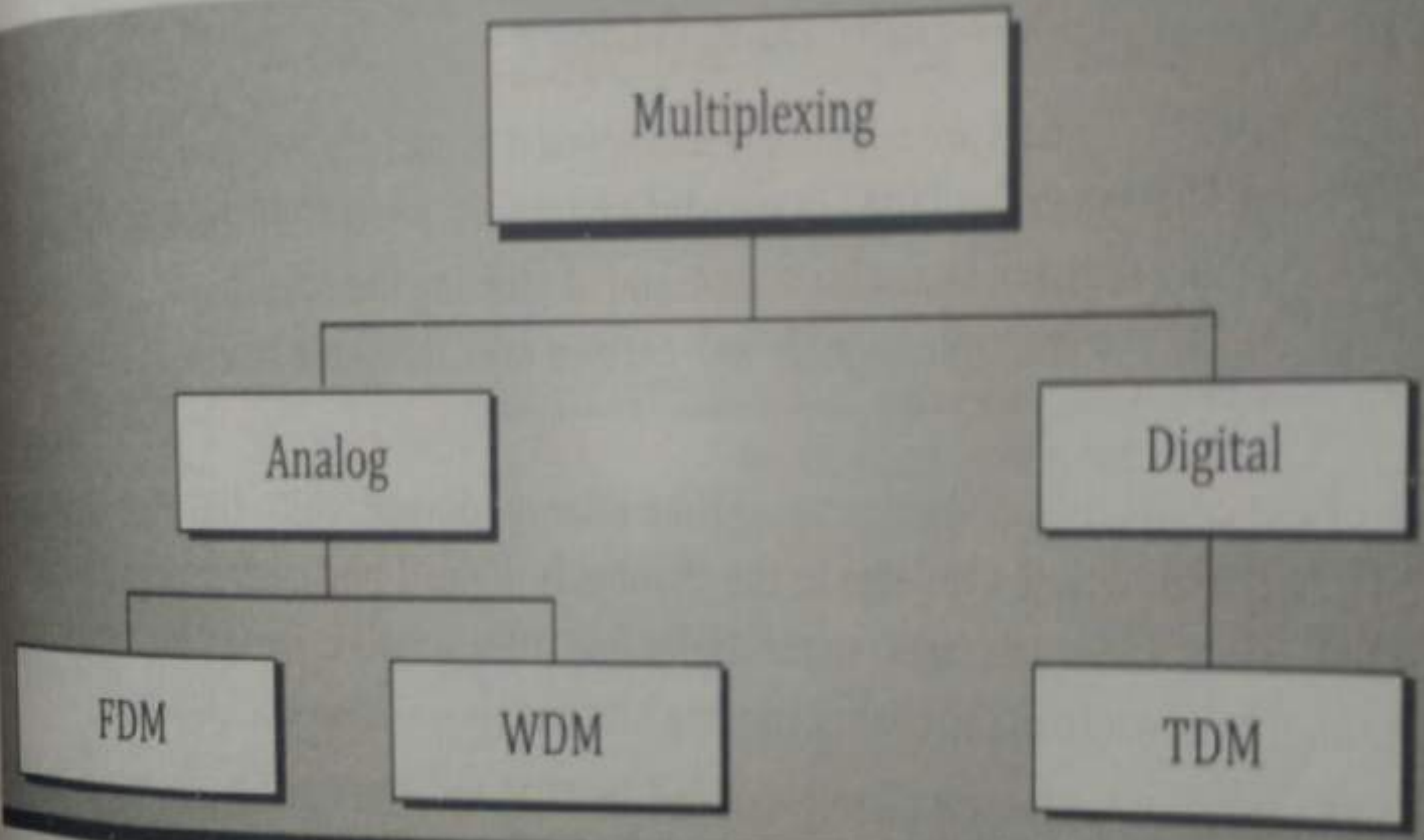
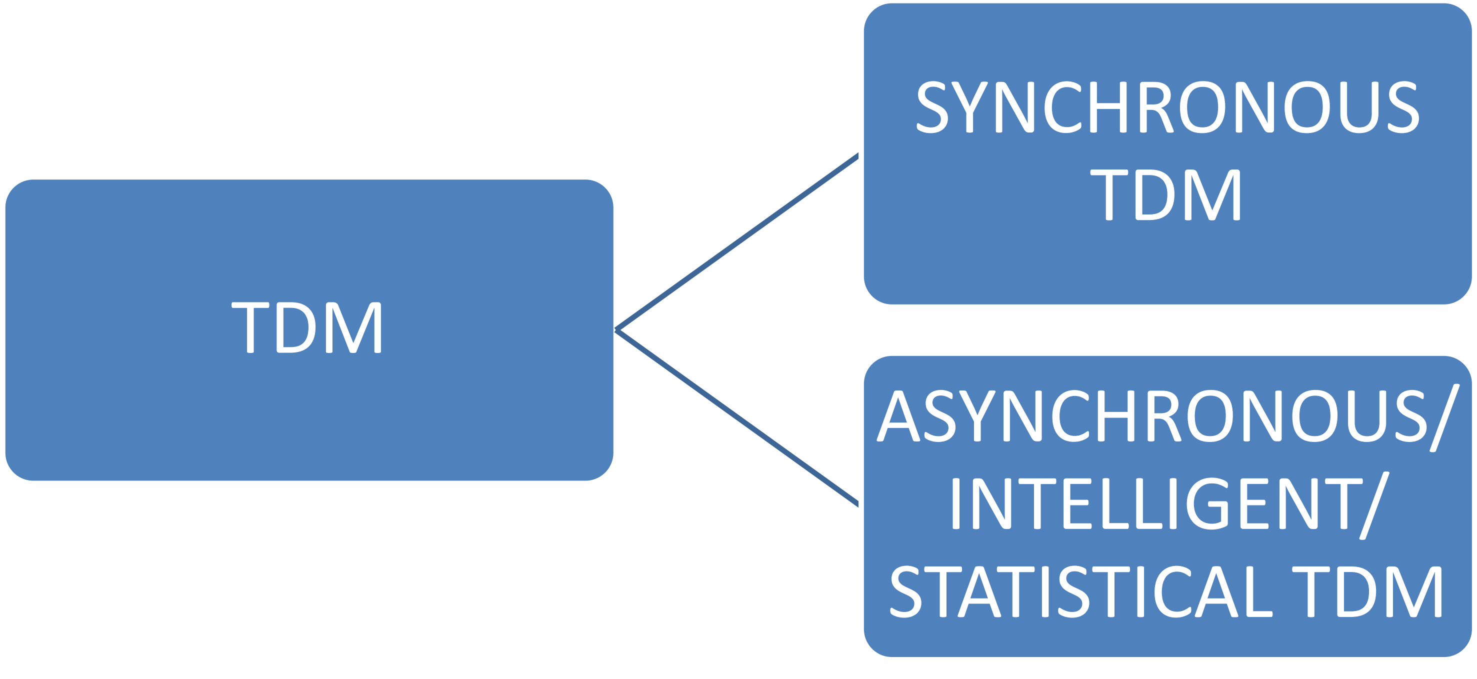


Figure 7.2 Types Of Multiplexing


TDM
SYNCHRONOUS TDM
ASYNCHRONOUS/ INTELLIGENT/ STATISTICAL TDM

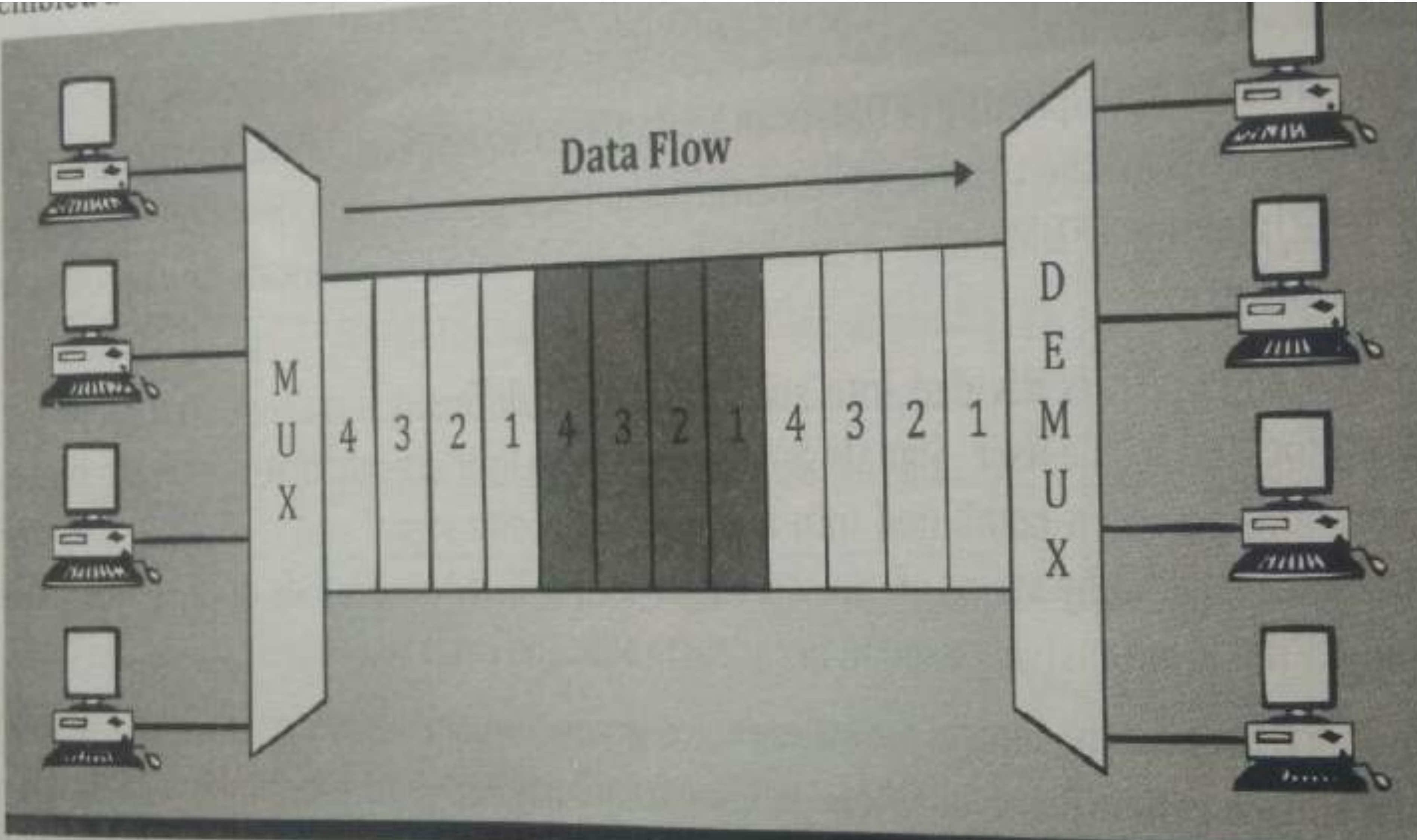


Figure 7.4 TDM Process

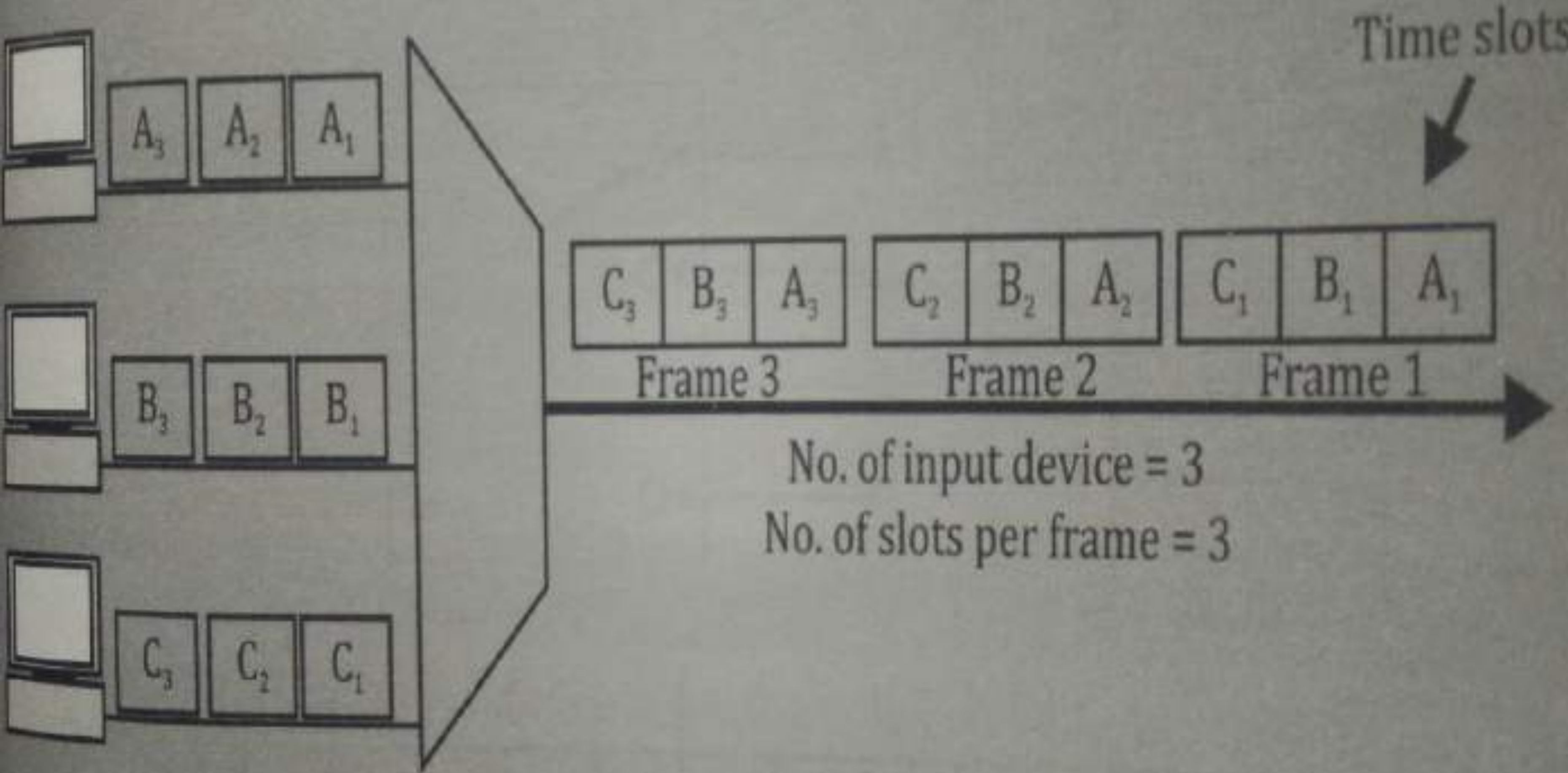


Figure 7.5 (a) Synchronous TDM

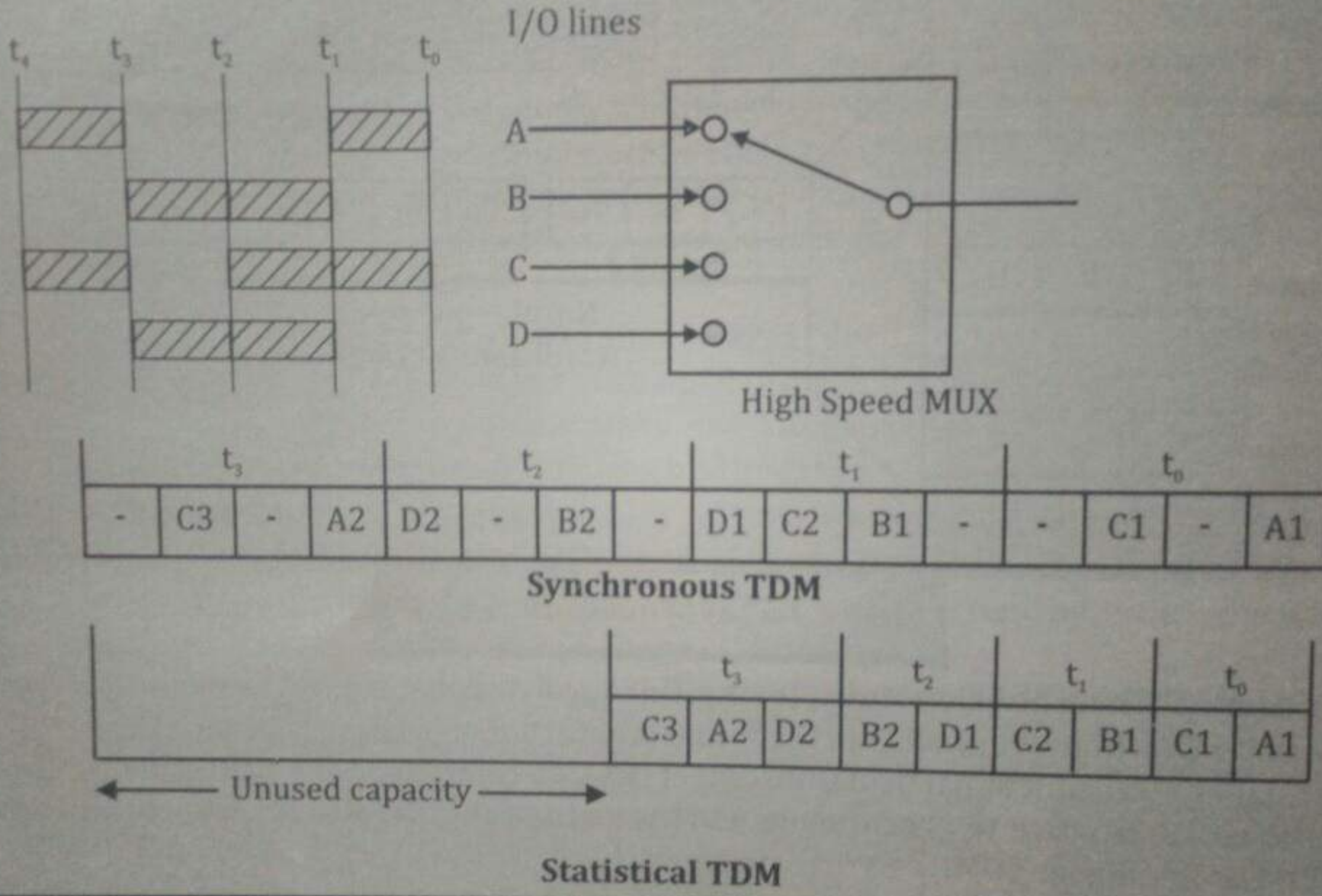


Figure 7.5 (b) Comparison of Synchronous and Statistical TDM

WDM – Wavelength Division Multiplexing

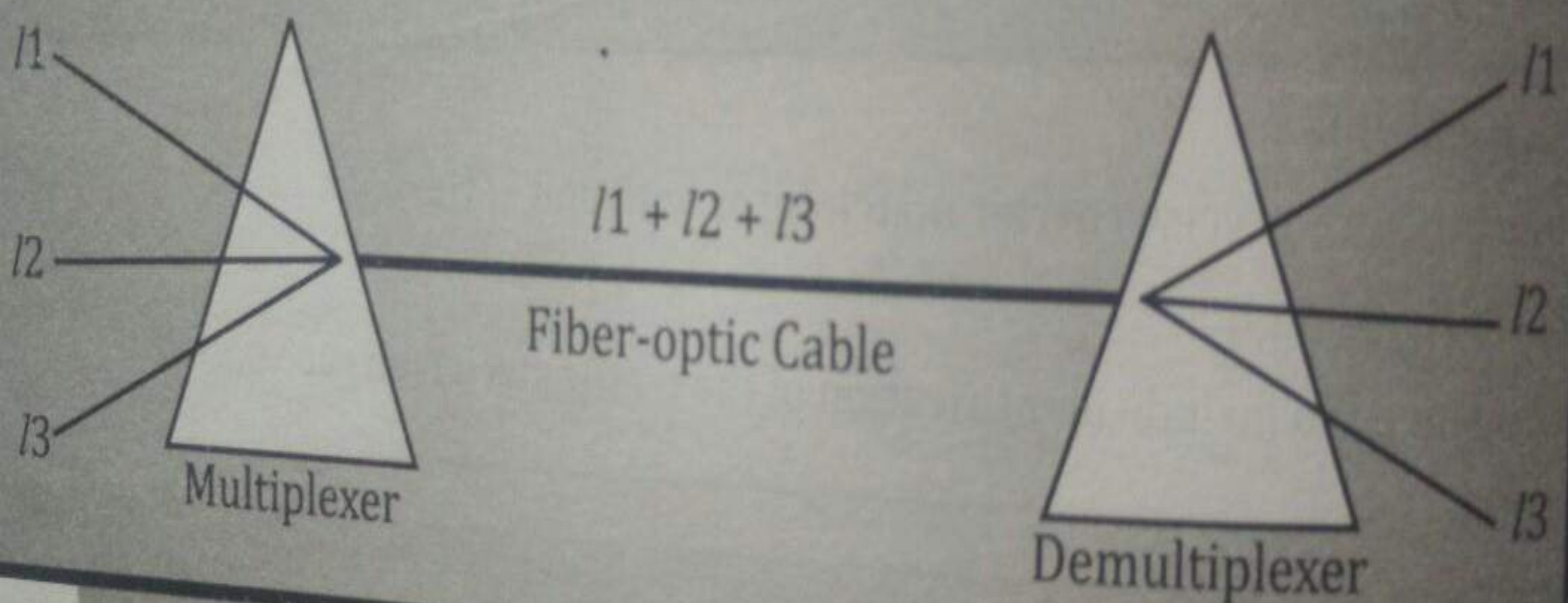


Figure 7.6 Prisms used in wave length -division multiplexing

SONET – Synchronous Optical Network

- Is an Optical Transmission Interface having synchronous network.
- Proposed by Bellcore and standardized by ANSI.
- Used in North America, while Japan and Europe uses SDH – Synchronous Digital Hierarchy.
- Solved issue of interoperability among the vendors and technology.
- Single clock is used to handle the timings.
- Used for Broadcast services, particularly ATM and B-ISDN.

Synchronous Transport Signal

Signal Name	Data Rate(Mbps)
STS-1 - OC-1	51.84
STS-3 STM-1 OC-3	155.52
STS-12 STM-4 OC-12	622.08
STS-48 STM-16 OC-48	2488.32
STS-192 STM-64 OC-192	9953.28
STS-768 STM-256 OC-768	40 Gbps

PHYSICAL CONFIGURATION

- STS Multiplexers
- Regenerators
- Add/Drop Multiplexers

Physical Configuration

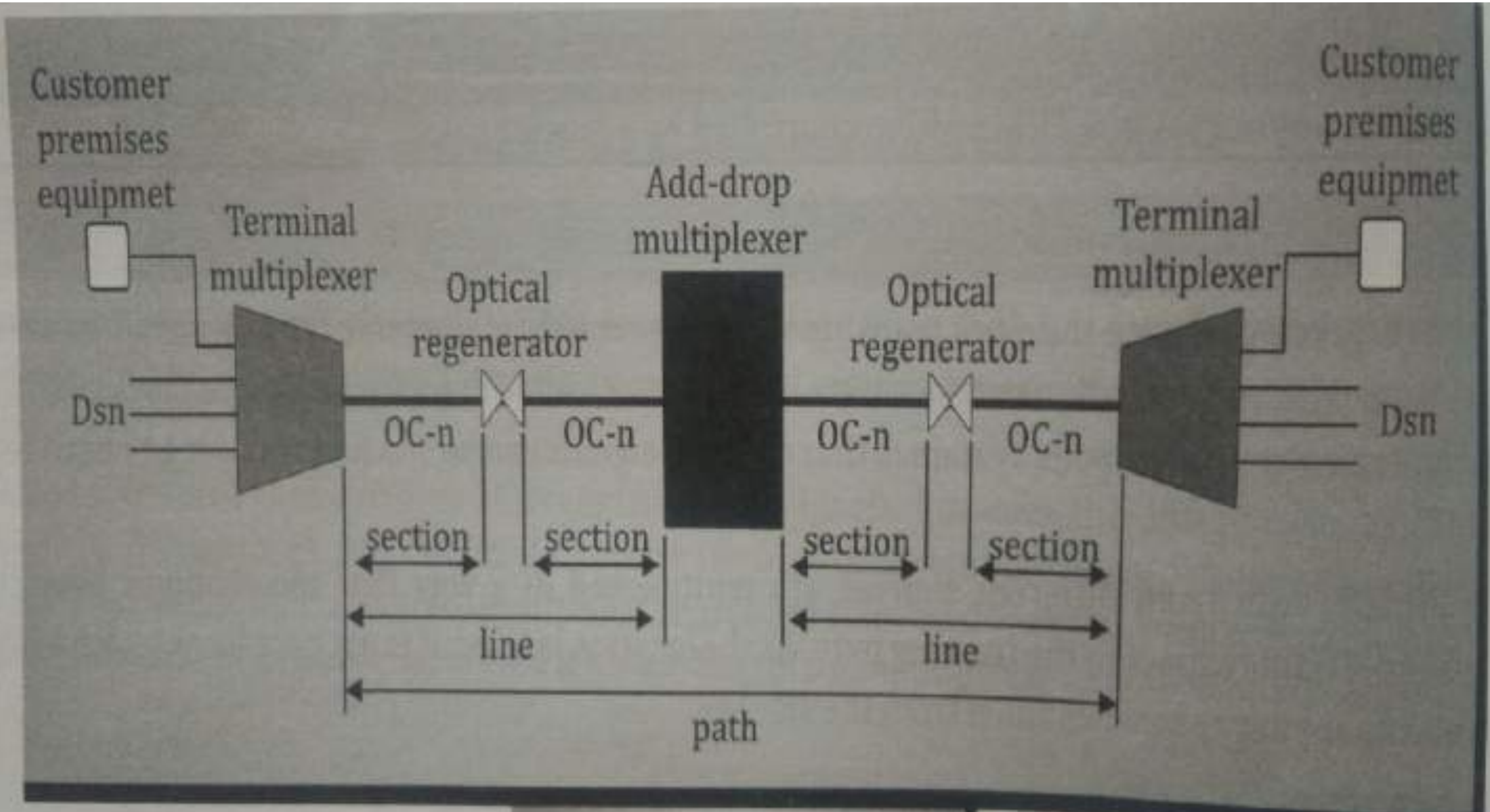
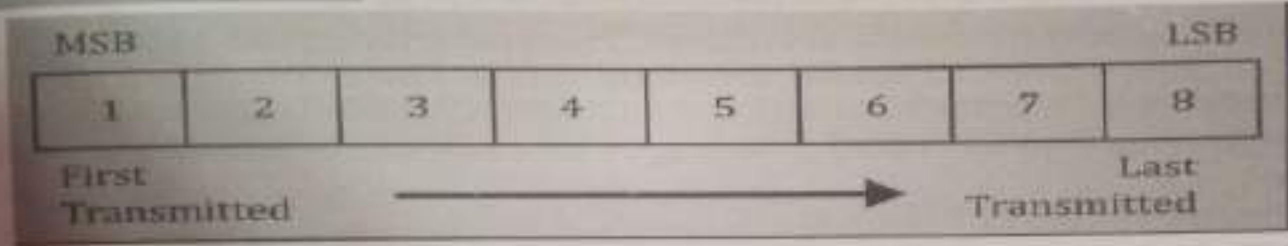


Figure 7.7 A SONET system

7.2.4 SONET Framing



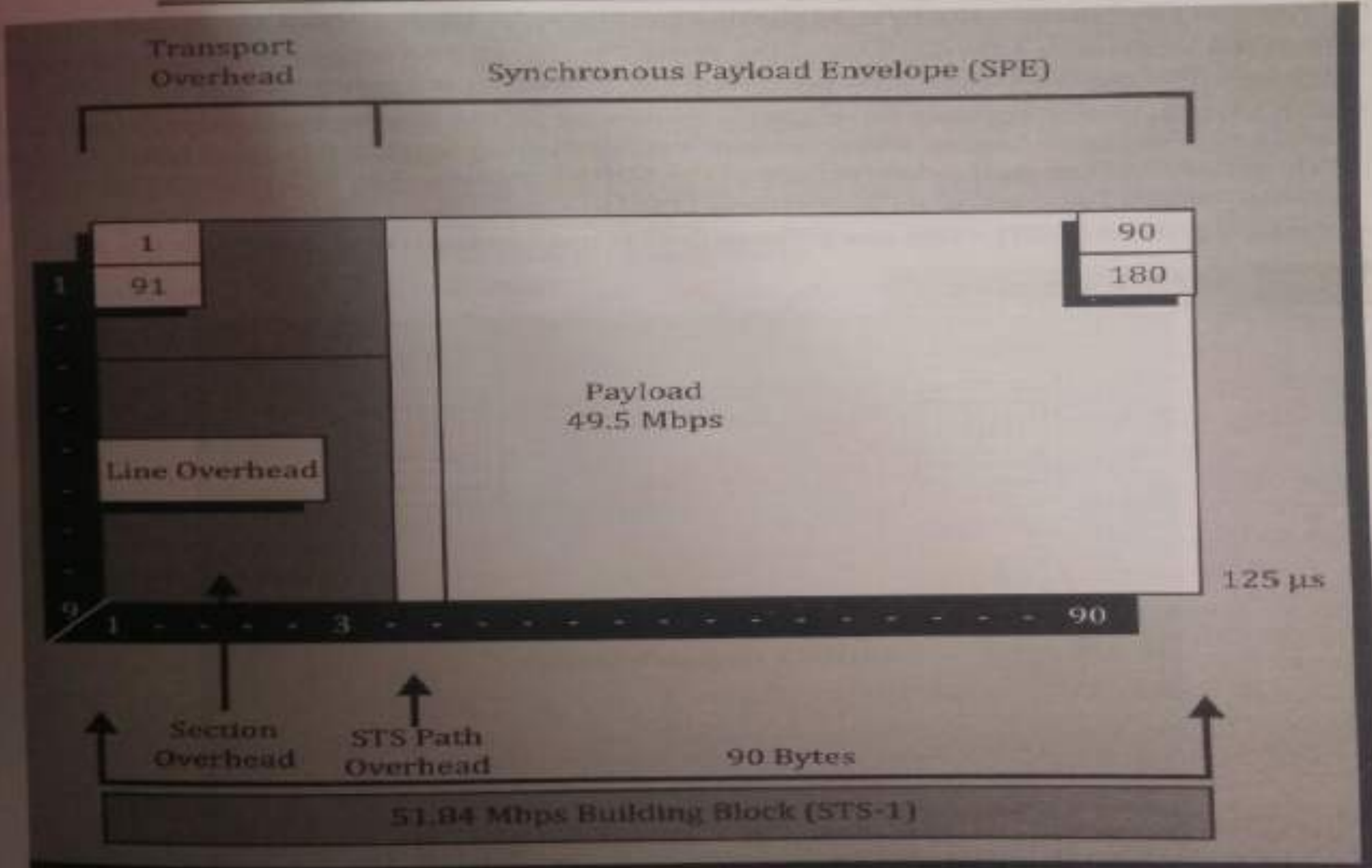


Figure 7.8 SONET Frame Structure

Frame Structure

- Has 9 rows of 90 bytes i.e 9x90=810 bytes.
- Transmitted from left to right and top to bottom.
- TOH – First three columns are called Transport Overhead.
- SPE – Remaining 87 columns are called Synchronous Payload Envelop
- POH – First column of SPE is called Payload Overhead.
- Every SONET Frame repeats every 125 microseconds no matter what is line speed.
- As line rate goes up, SONET frame gets bigger, to keep frame rate at 8000 frames/sec.

SONET Topology

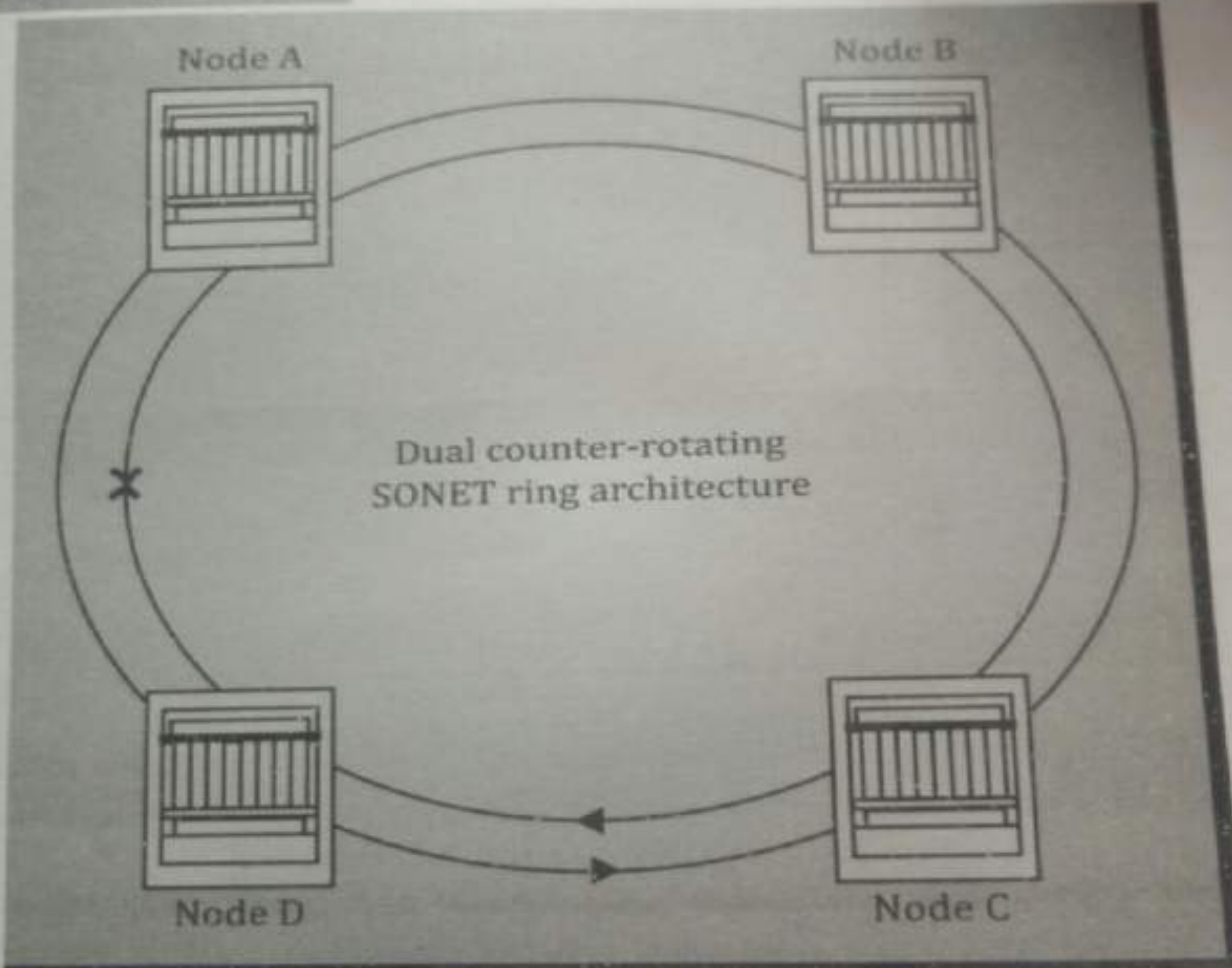
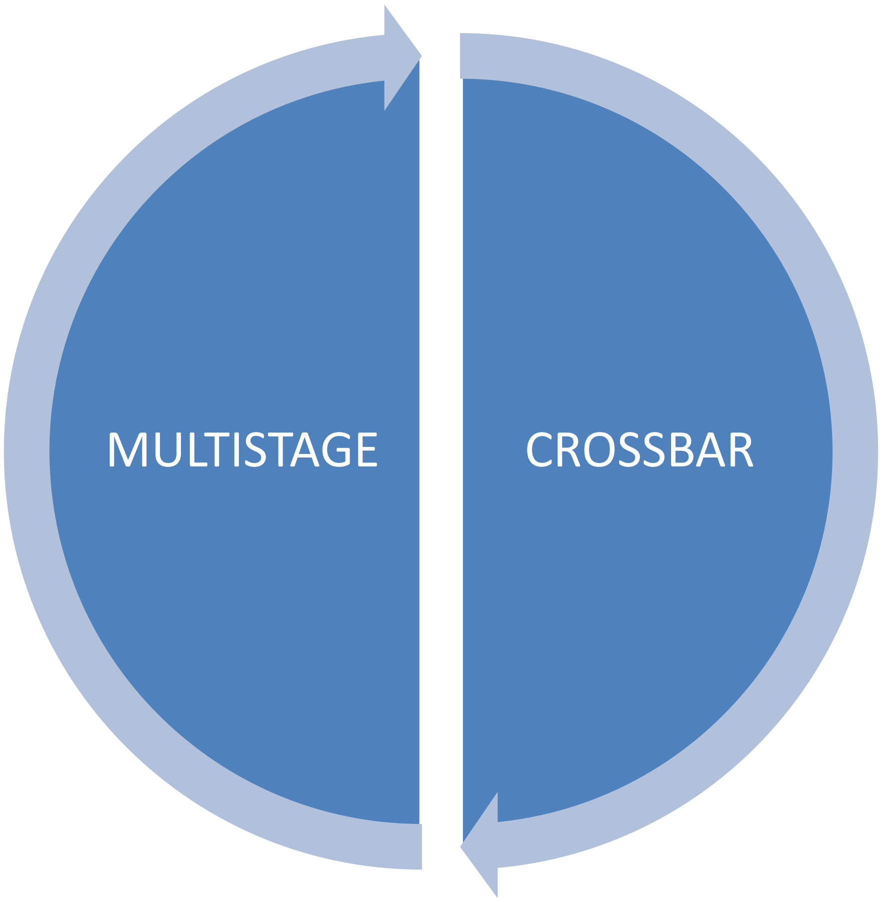
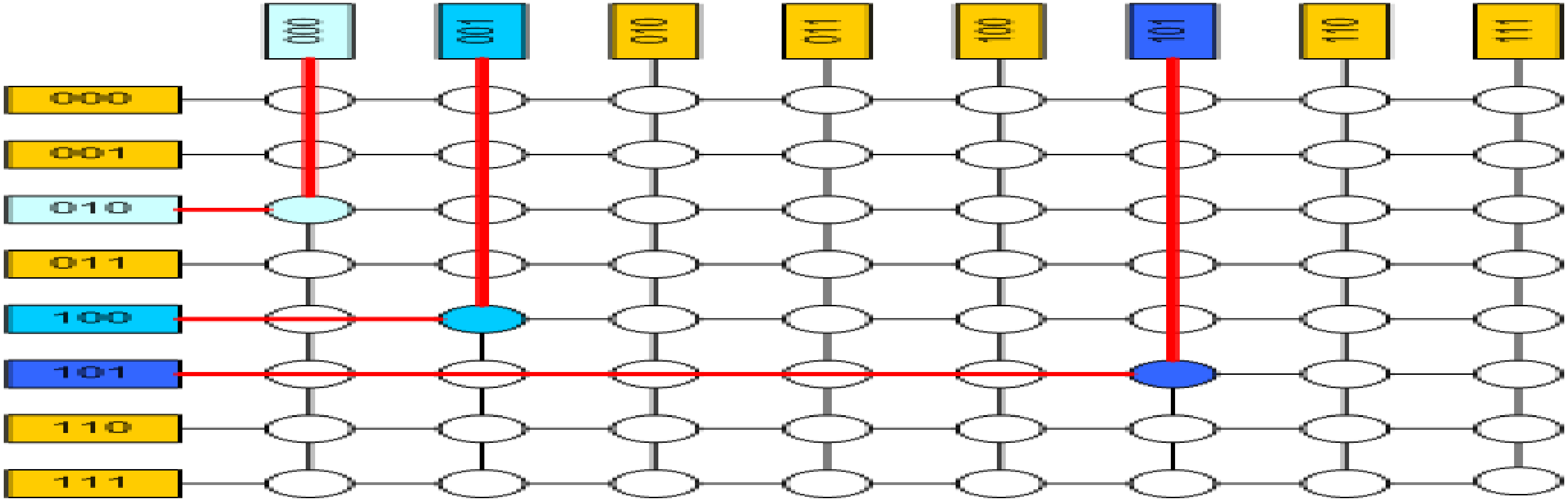


Figure 7.9 SONET Topology

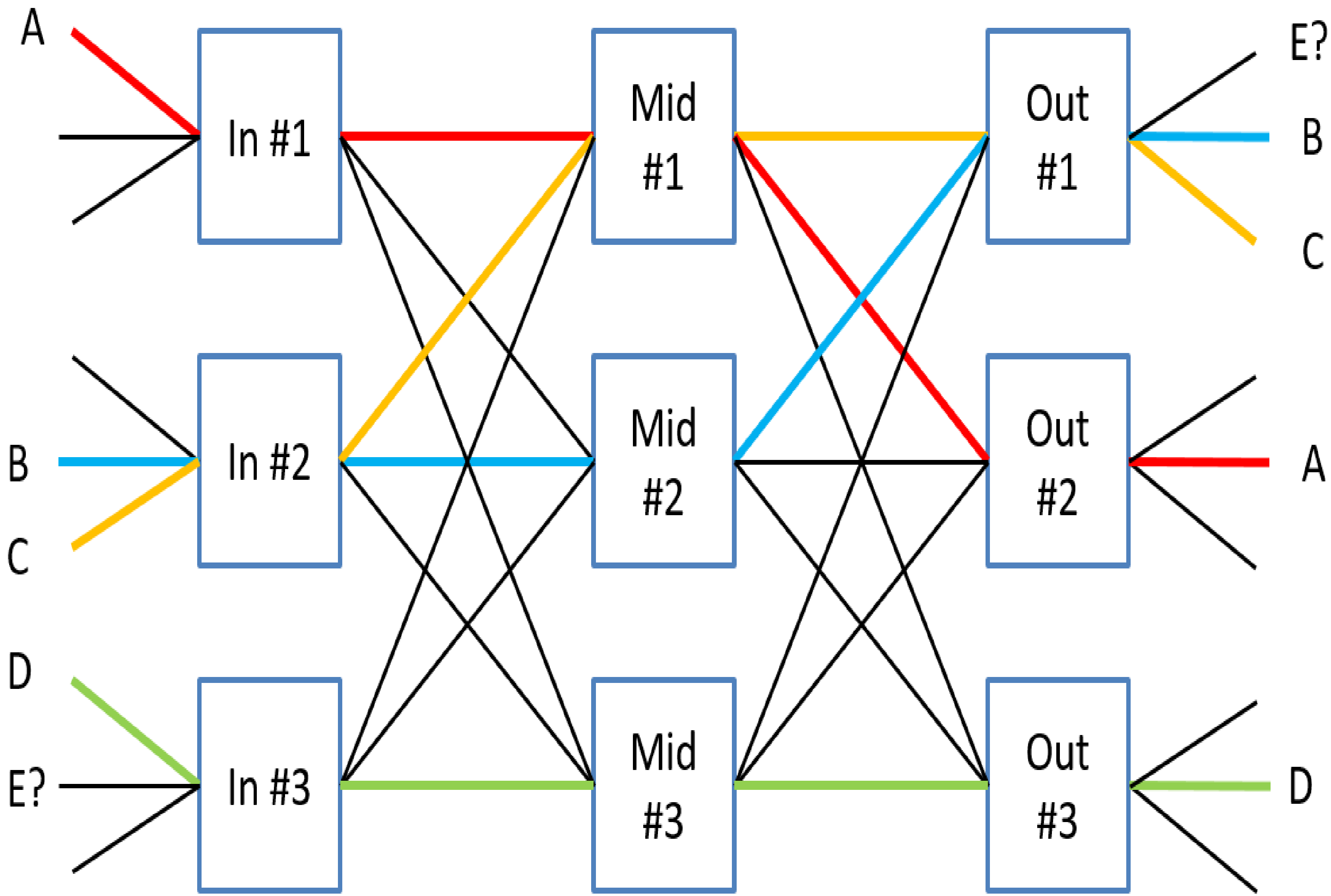
CIRCUIT SWITCHING



CROSSBAR SWITCH



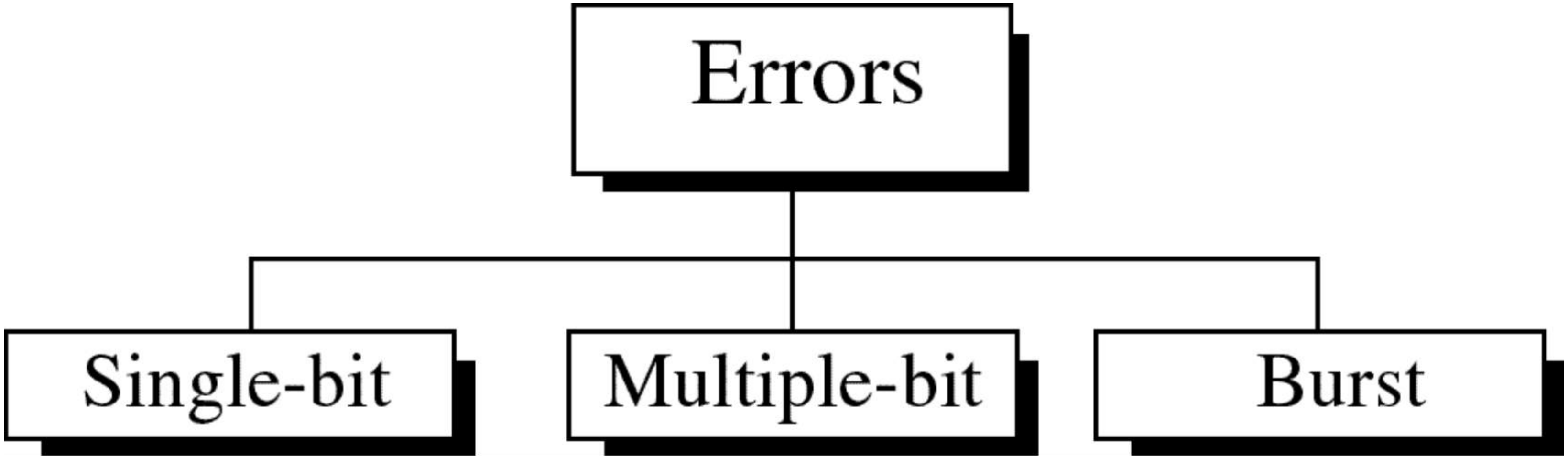
MULTI STAGE SWITCH



ERROR DETECTION AND CORRECTION

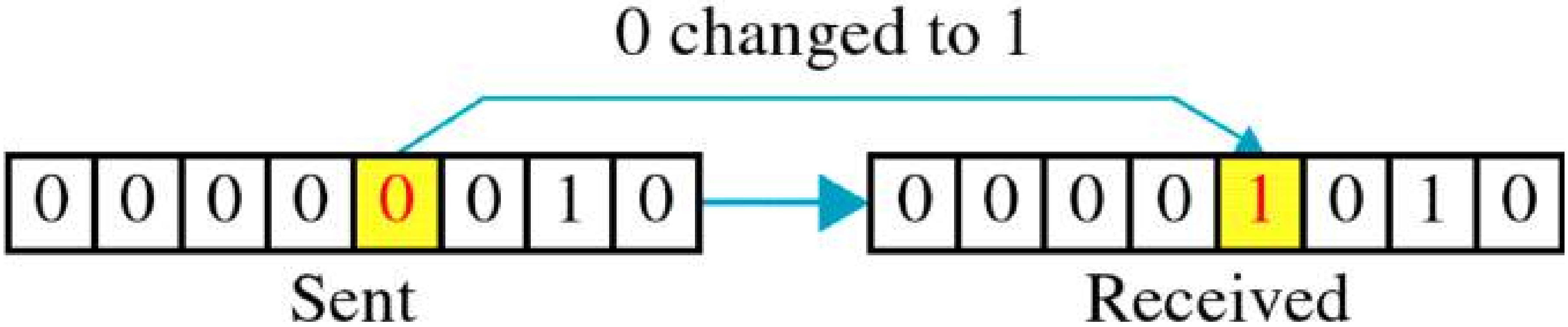
- TYPES OF ERRORS
- BIT STUFFING
- BYTE STUFFING
- BURST ERRORS
- VRC
- LRC
- CRC
- HAMMING CODE
- CHECKSUM

Types of Errors:

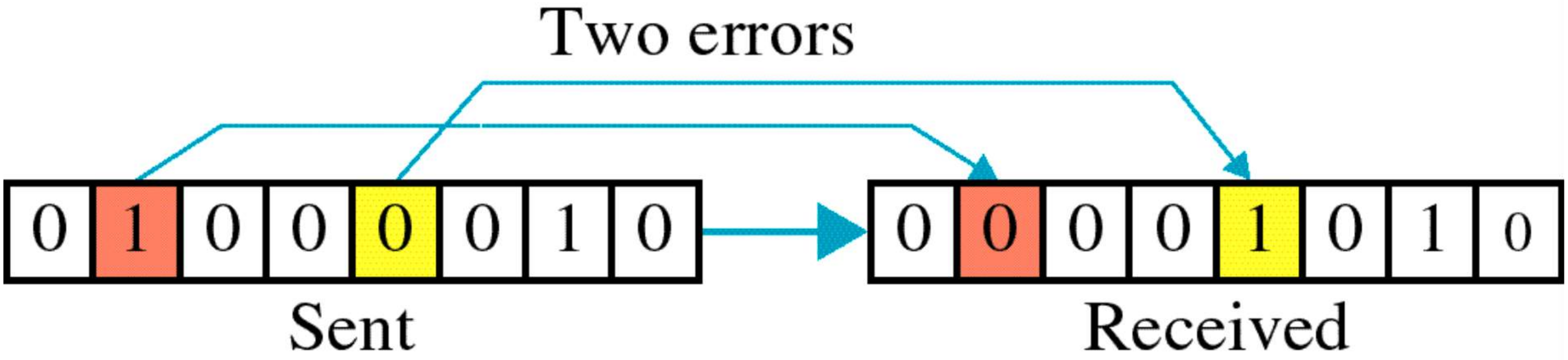


By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

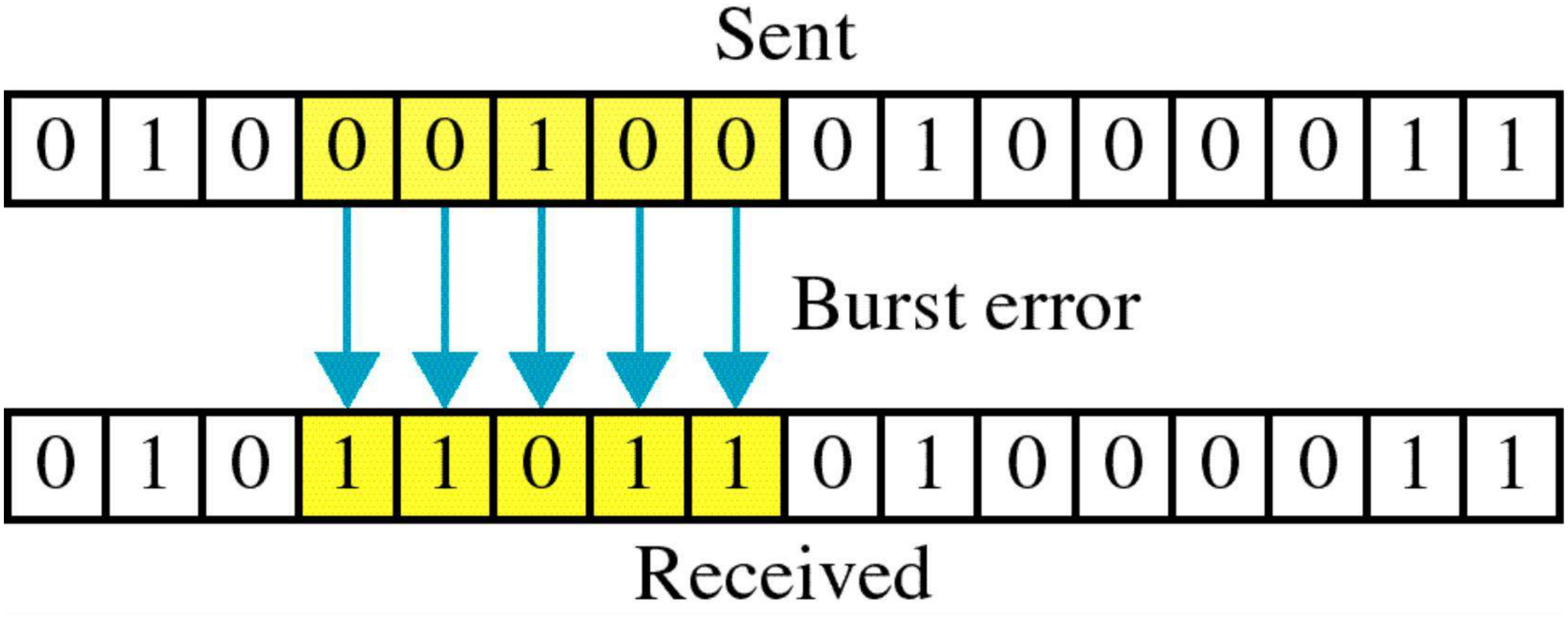
Single-bit error



Multiple-bit error



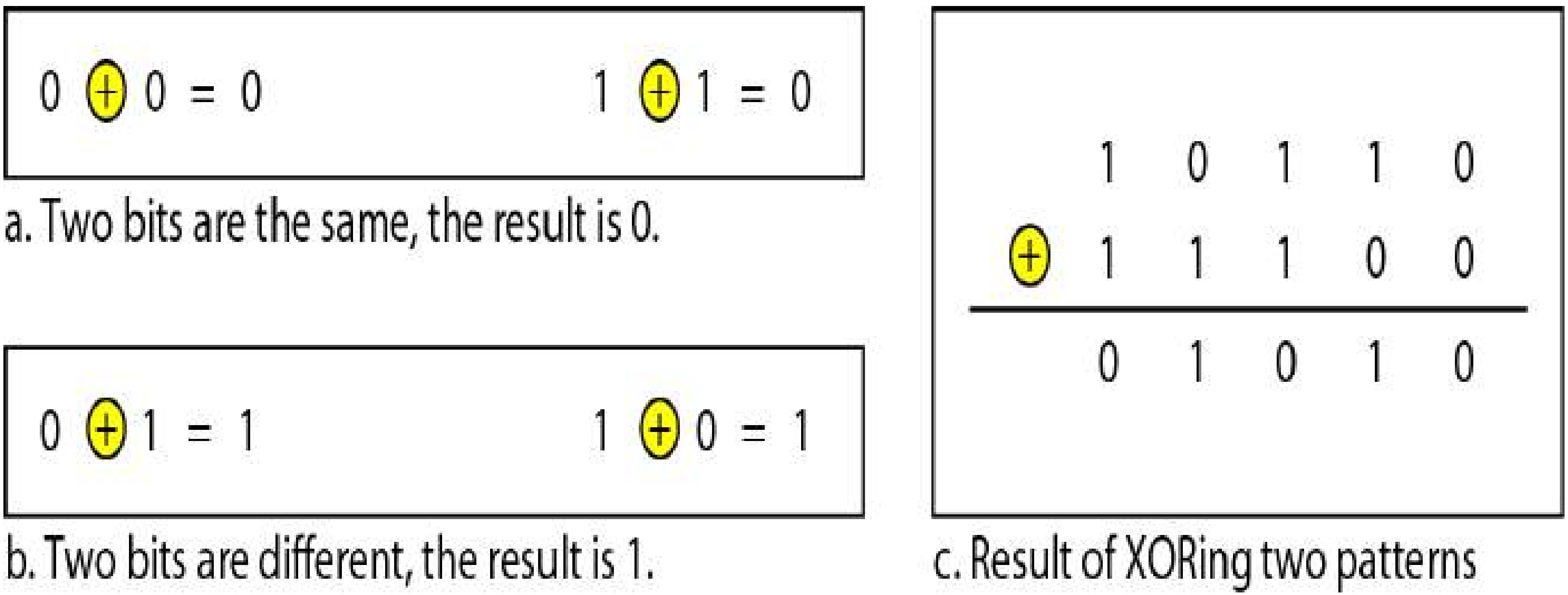
Burst error



By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

XORing of two single bits or two words

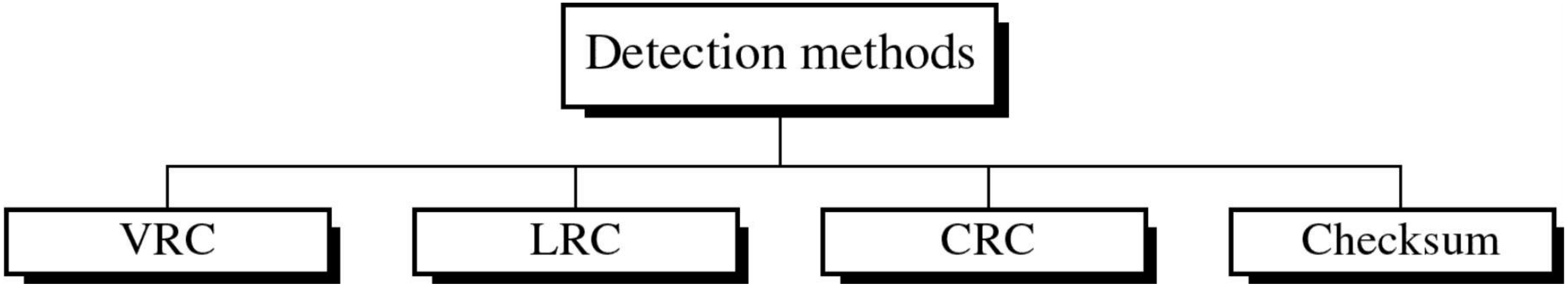
- To detect or correct errors, we need to send extra (redundant) bits with data.



By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

Detection Methods:

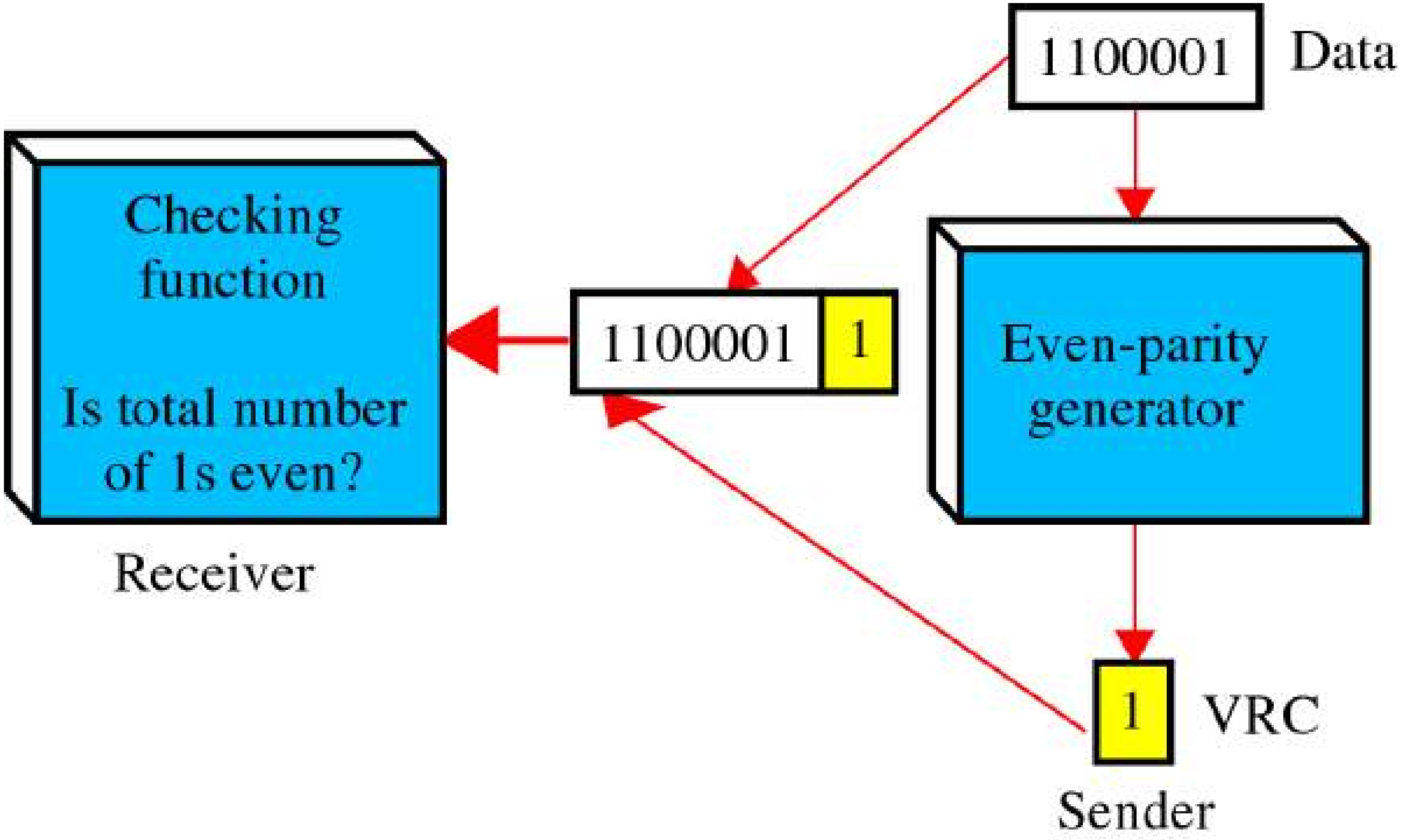
- Detection methods
  - VRC(Vertical Redundancy Check)
  - LRC(Longitudinal Redundancy)
  - CRC(Cyclical redundancy Check)
  - Checksum



VRC

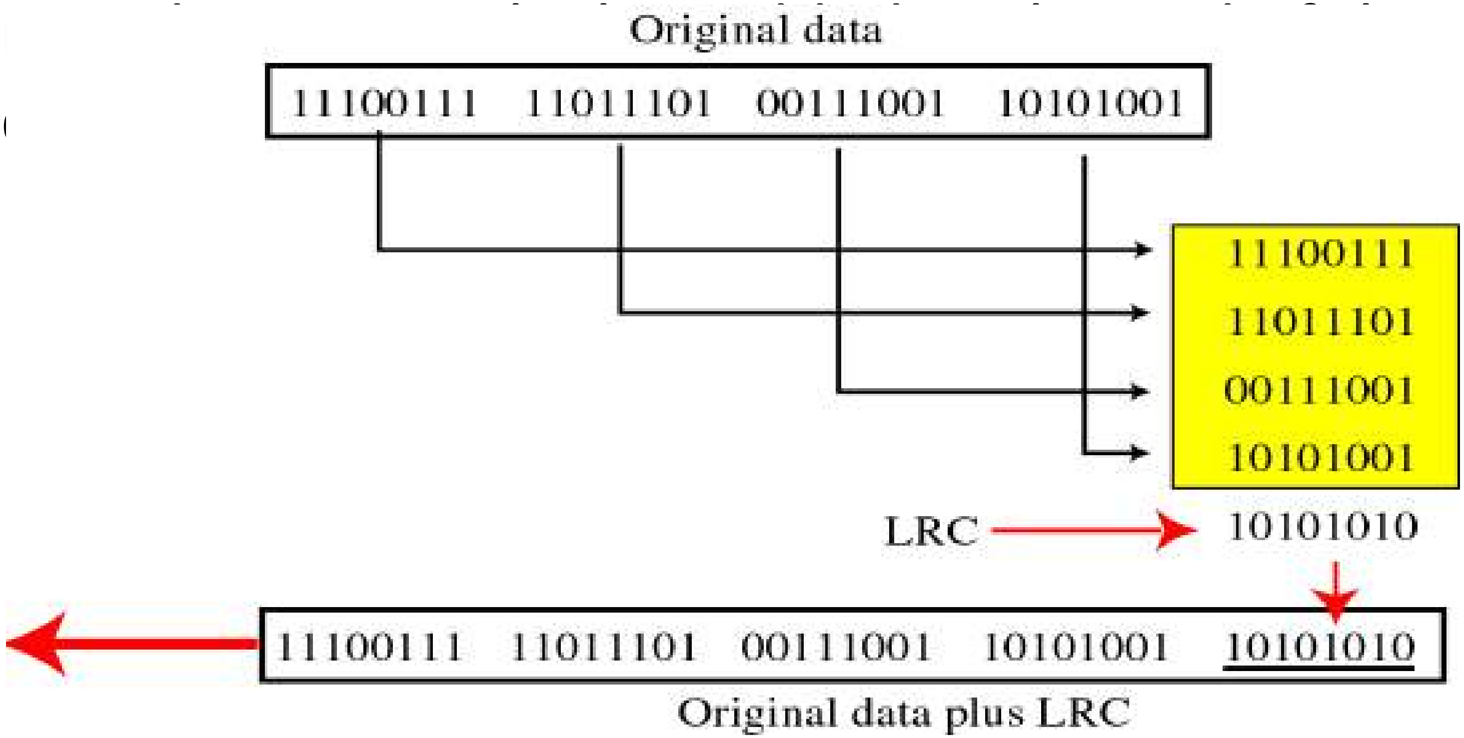
- VRC(Vertical Redundancy Check)
  - A parity bit is added to every data unit so that the total number of 1s(including the parity bit) becomes even for even-parity check or odd for odd-parity check
  - VRC can detect all single-bit errors.
  - It can detect multiple-bit or burst errors only the total number of errors is odd.
- Even parity VRC concept is given in next fig

VRC


1100001
Data
Checking
function
Is total number
of 1s even?
Receiver
1100001
1
Even-parity
generator
1
VRC
Sender

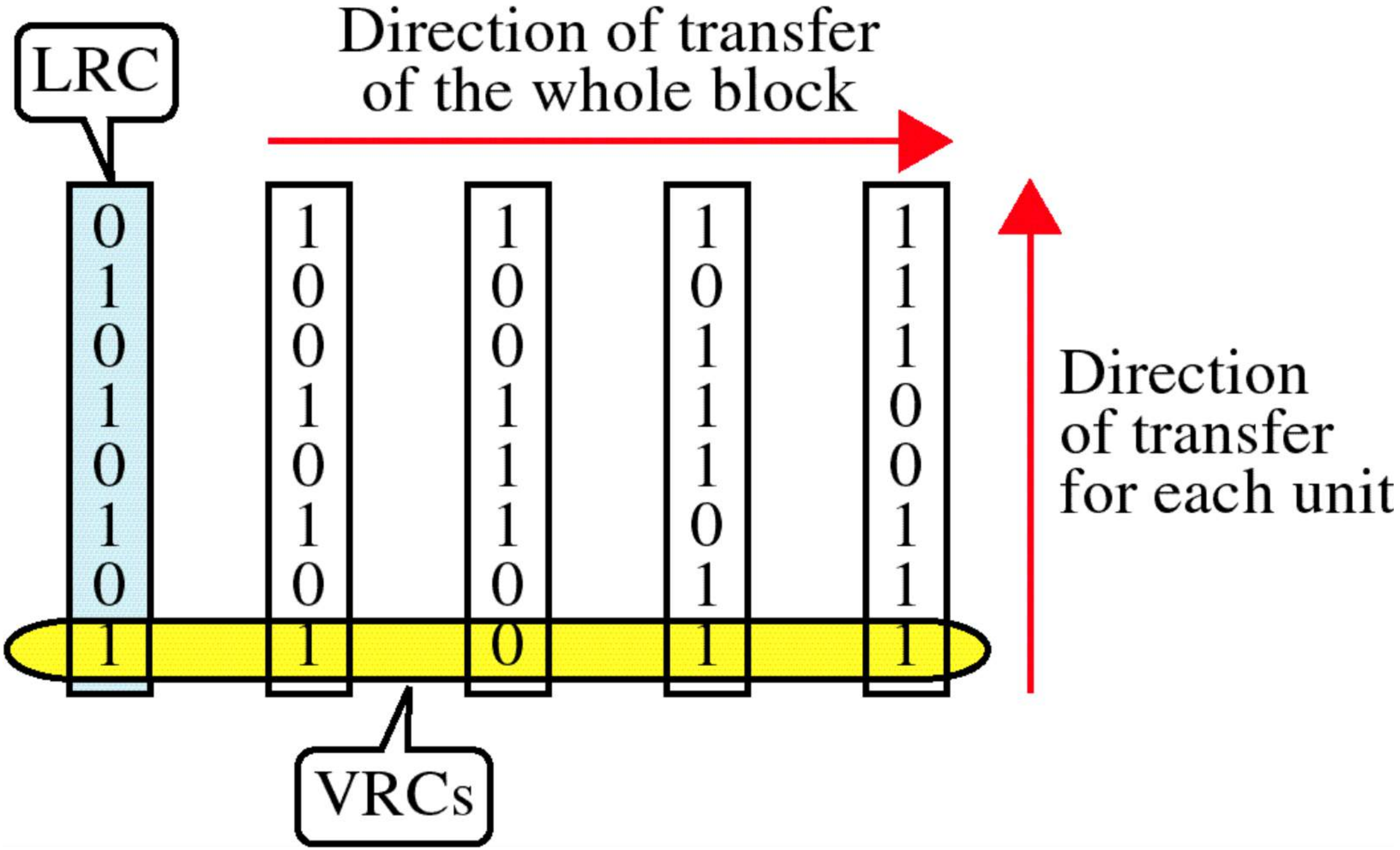
LRC

- LRC(Longitudinal Redundancy Check)
  - Parity bits of all the positions are assembled into a



By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

VRC & LRC

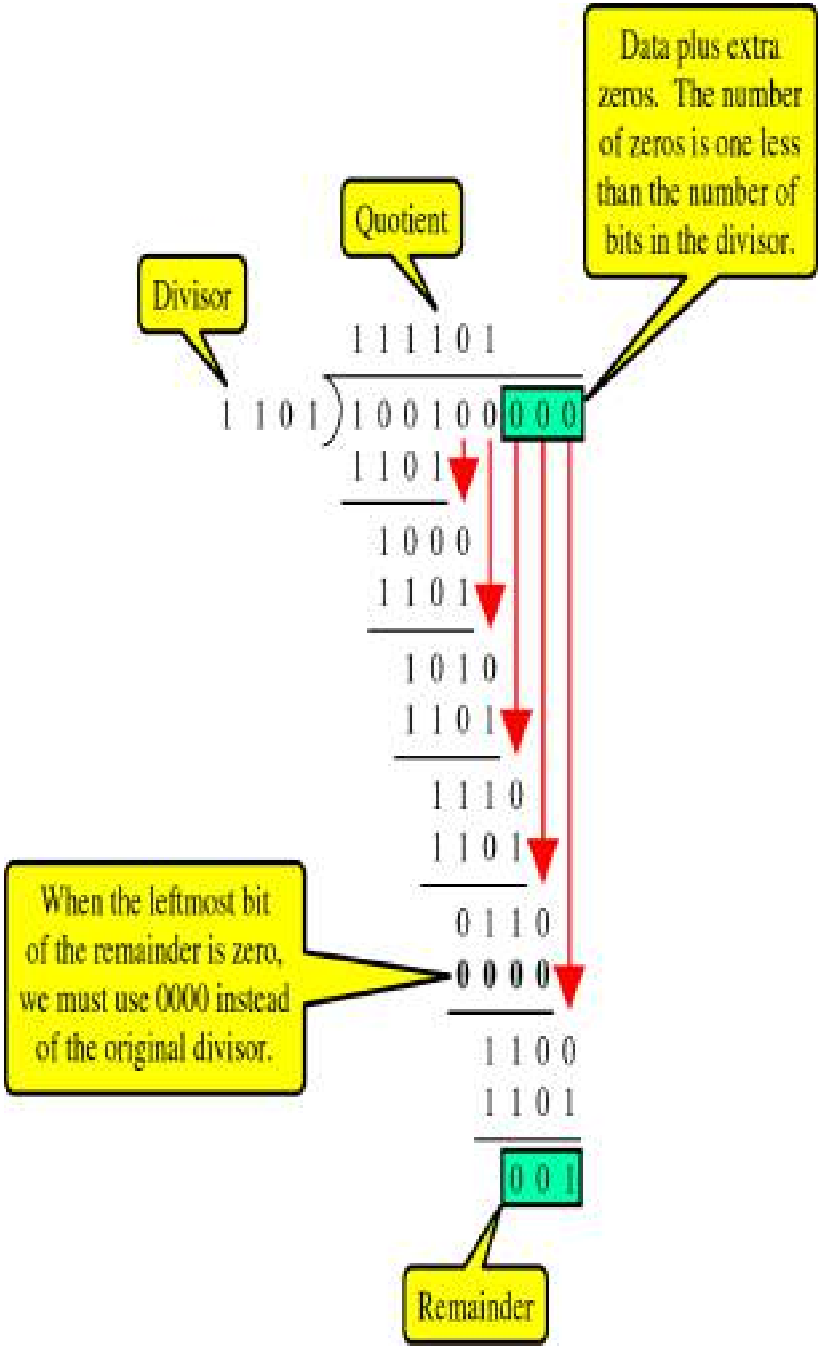


By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

CRC Generator

- CRC generator
- uses modular-2 division.

Binary Division
in a CRC Generator

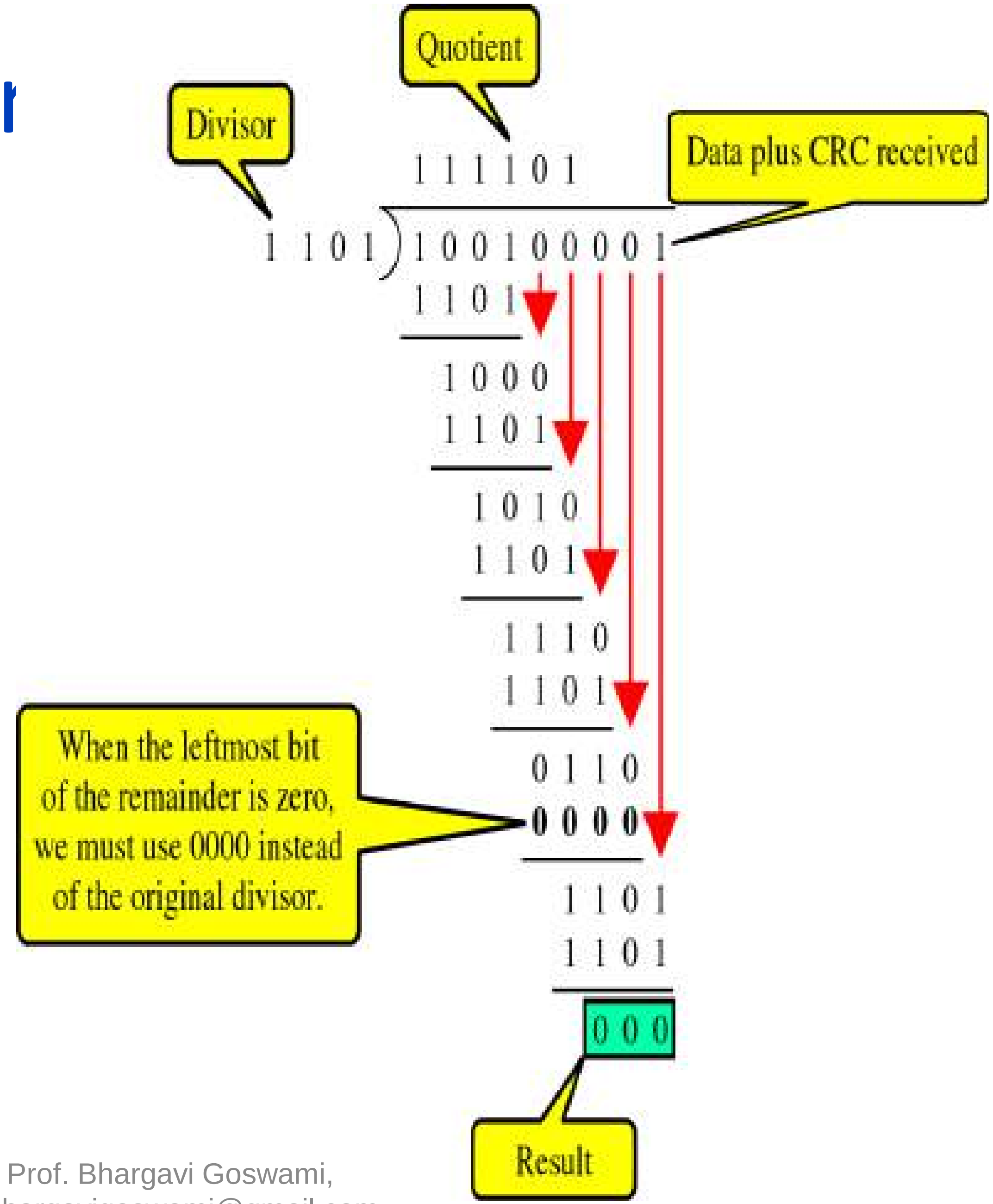


CRC Checker

Binary Division

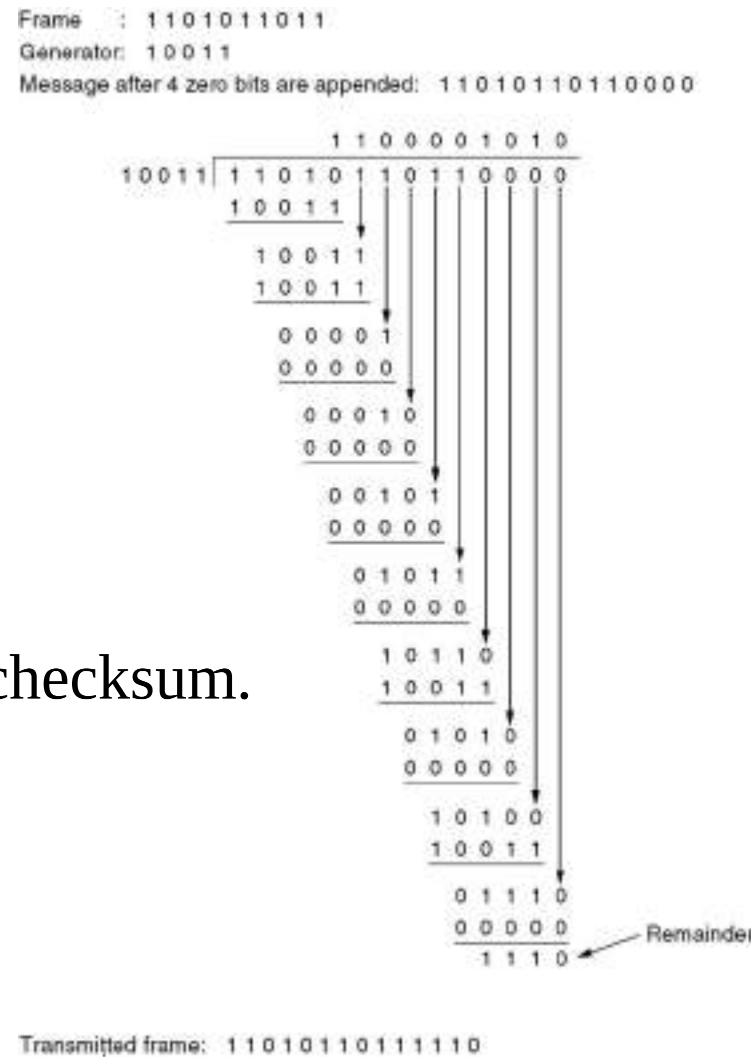
in a

CRC Checker



By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

As per text book:



Calculation of the polynomial code checksum.

By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

Checksum:

- Checksum is used by the higher layer protocols
- And is based on the concept of redundancy(VRC, LRC, CRC …. Hamming code)
- To create the checksum the sender does the following:
  - The unit is divided into K sections, each of n bits.
  - Section 1 and 2 are added together using one's complement.
  - Section 3 is added to the result of the previous step.
  - Section 4 is added to the result of the previous step.
  - The process repeats until section k is added to the result of the previous step.
  - The final result is complemented to make the checksum.

Checksum Example

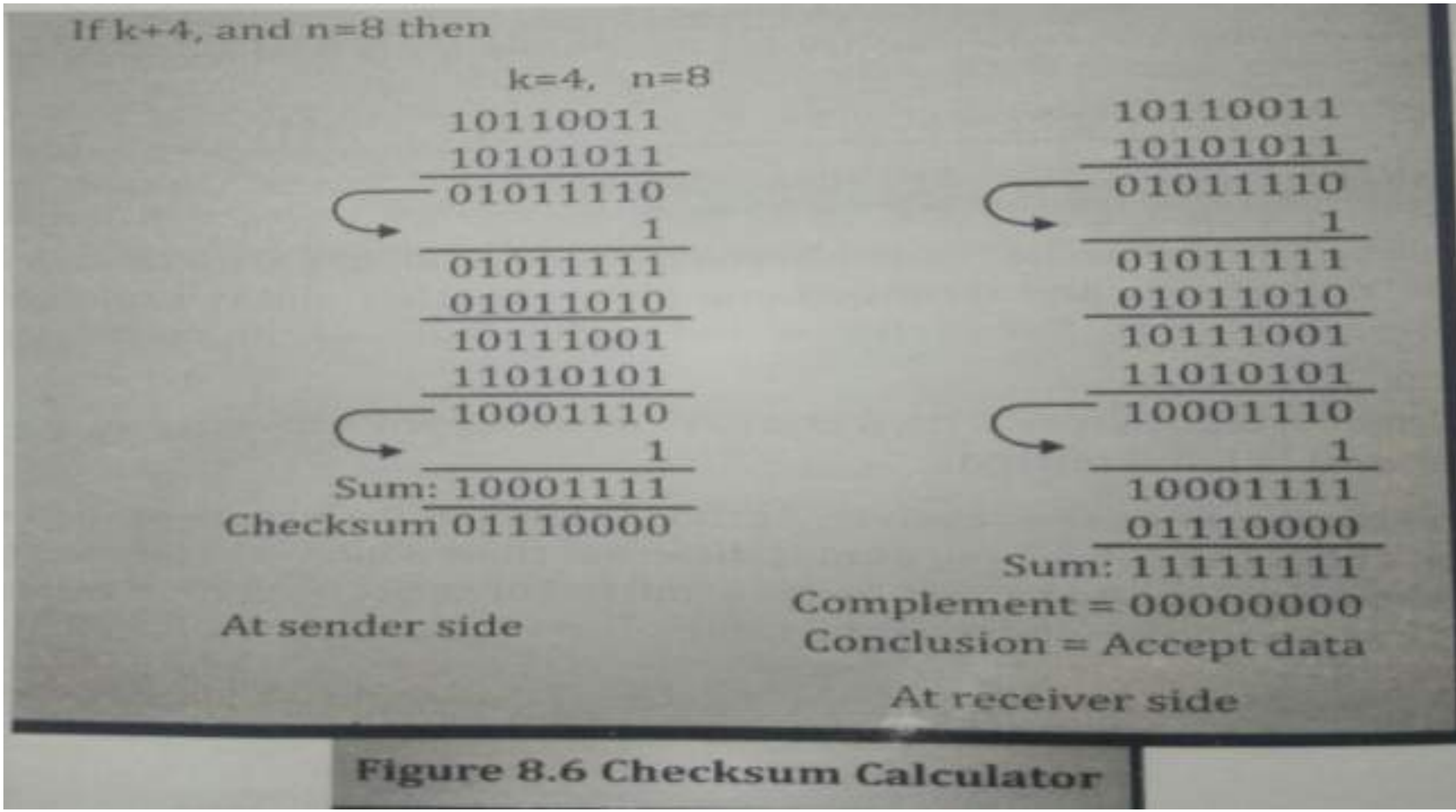


Figure 8.6 Checksum Calculator

Hamming code and Error

- *Redundancy for error handling*
- *m* data bits and *r* redundant bits
- for *m* + *r* bits only one correct value of *r* for a given *m*
- one correct bit pattern requires *m* + *r* incorrect patterns
- $m + r + 1 < 2^r$

0	0	1	1	0	0	1	0	0	0	0
1	2	3	4	5	6	7	8	9	10	11

Hamming code calculations

R1	R2	M1	R3	M2	M3	M4	R4	M5	M6	M7
1	2	3	4	5	6	7	8	9	10	11

(a)

R1	R2	1	R3	0	0	1	R4	0	0	0
1	2	3	4	5	6	7	8	9	10	11

(b)

R1	R2	M1	R3	M2	M3	M4	R4	M5	M6	M7
1	2	2+1	4	4+1	4+2	4+2+1	8	8+1	8+2	8+2+1

(c)

R1 to R4 = Redundant bits
M1 to M7 = Data bits

R1,R2,R3 and R4 calculations

- R1 represents the parity of M1, M2, M4, M5, and M7 = M1 + M2 + M4 + M5 + M7 = 1 + 0 + 0 + 1 + 0 + 0 = 0
- R2 represents the parity of M1, M3, M4, M6, and M7 = 1 + 1 + 0 + 0 =0
- R3 represents the parity of M2, M3, and M4=1
- R4 represents the parity of M5, M6, and M7=0

Error Correction Using Hamming Code

can be handled in two ways:

- when an error is discovered, the receiver can have the sender retransmit the entire data unit.
- a receiver can use an error-correcting code, which automatically corrects certain errors.
- Hamming Code

  ~ developed by R.W. Hamming
- positions of redundancy bits in Hamming code, lets see how.
- each r bit is the VRC bit for one combination of data bits

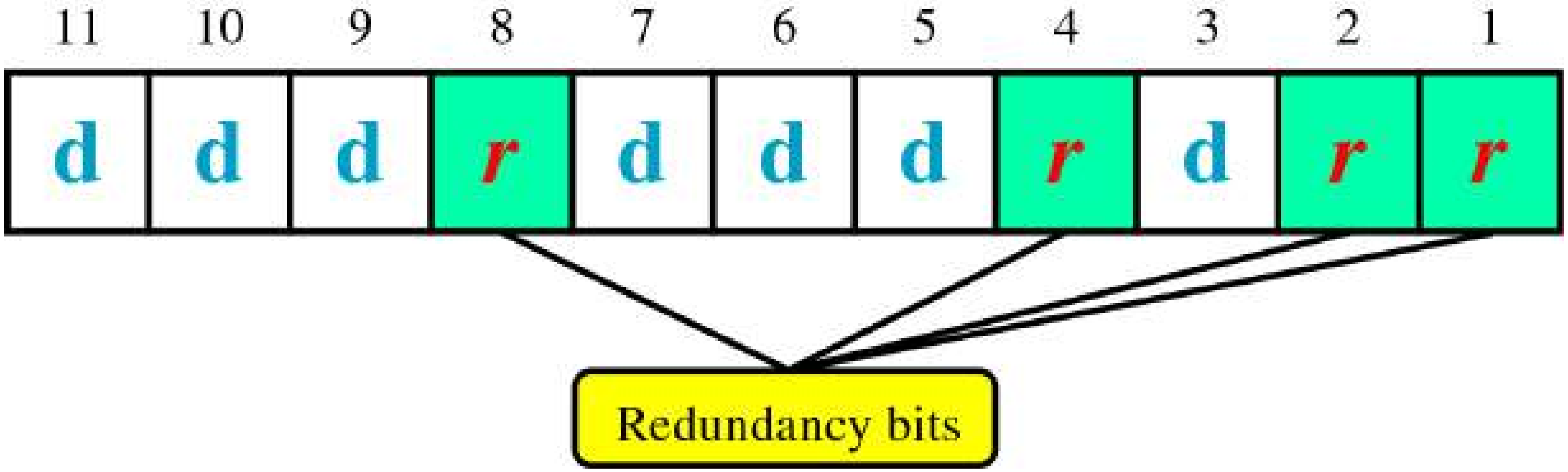
  r_1 = bits 1, 3, 5, 7, 9, 11

  r_2 = bits 2, 3, 6, 7, 10, 11

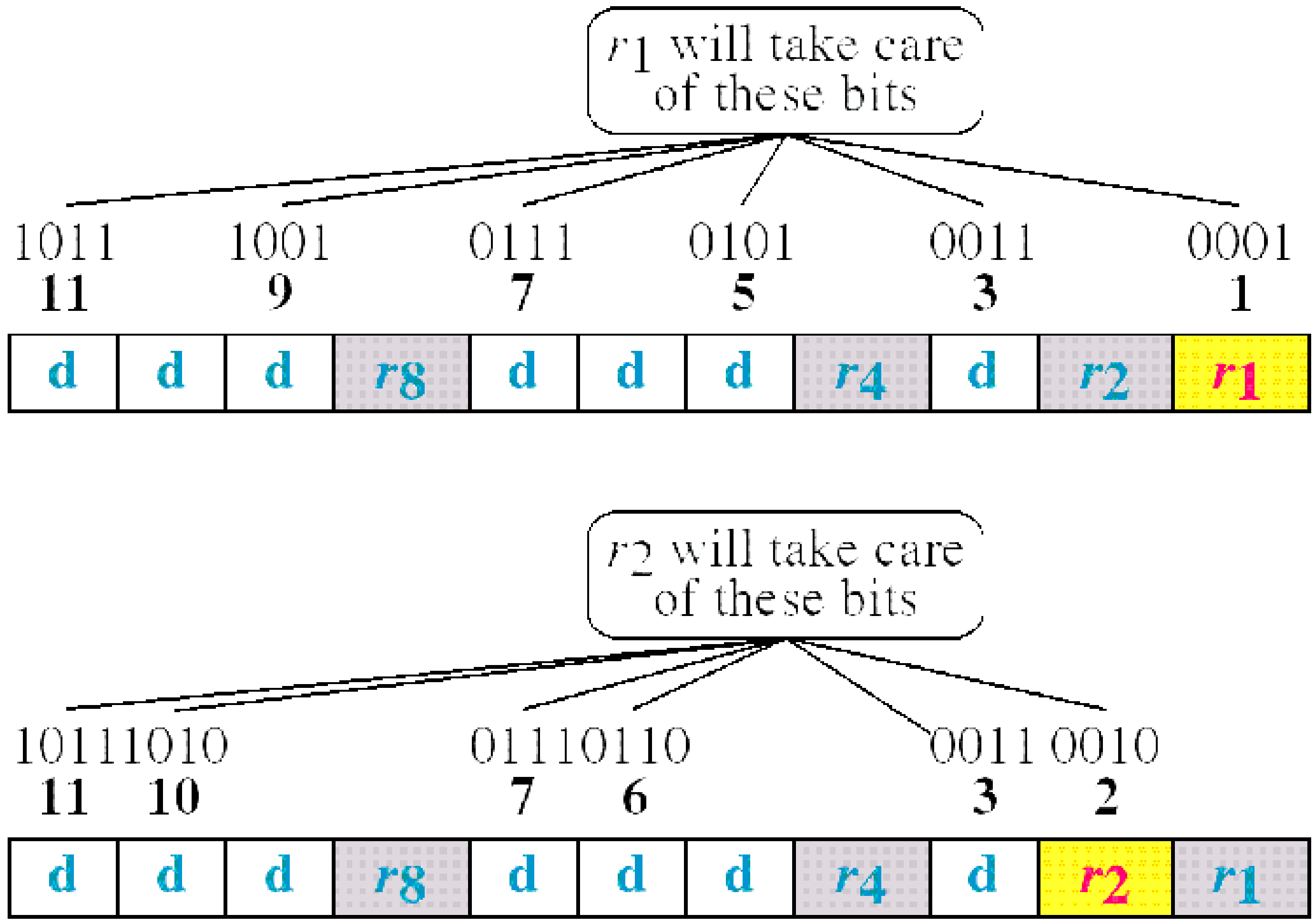
  r_4 = bits 4, 5, 6, 7

  r_8 = bits 8, 9, 10, 11

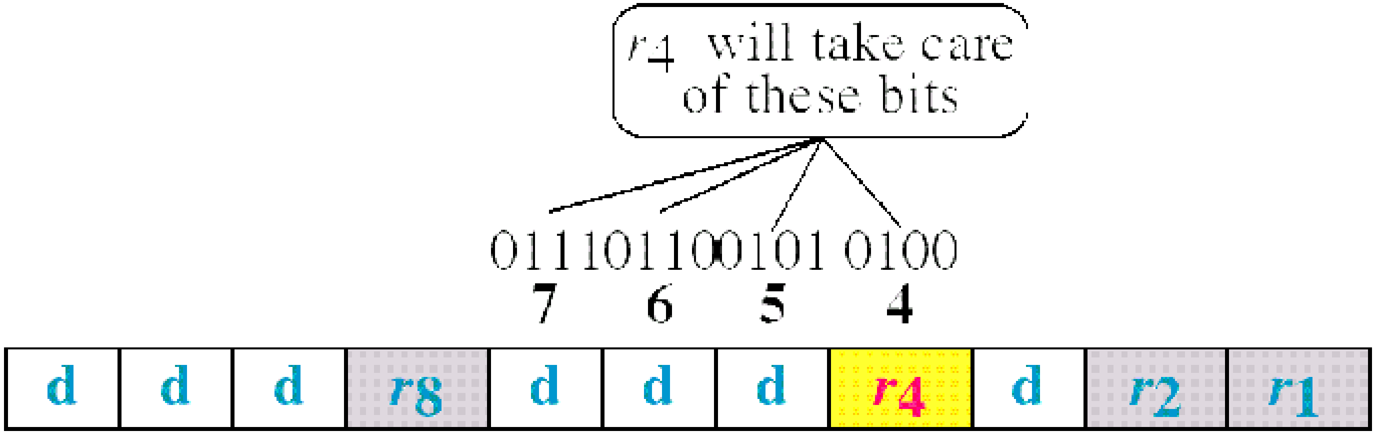
Redundant Bit Position

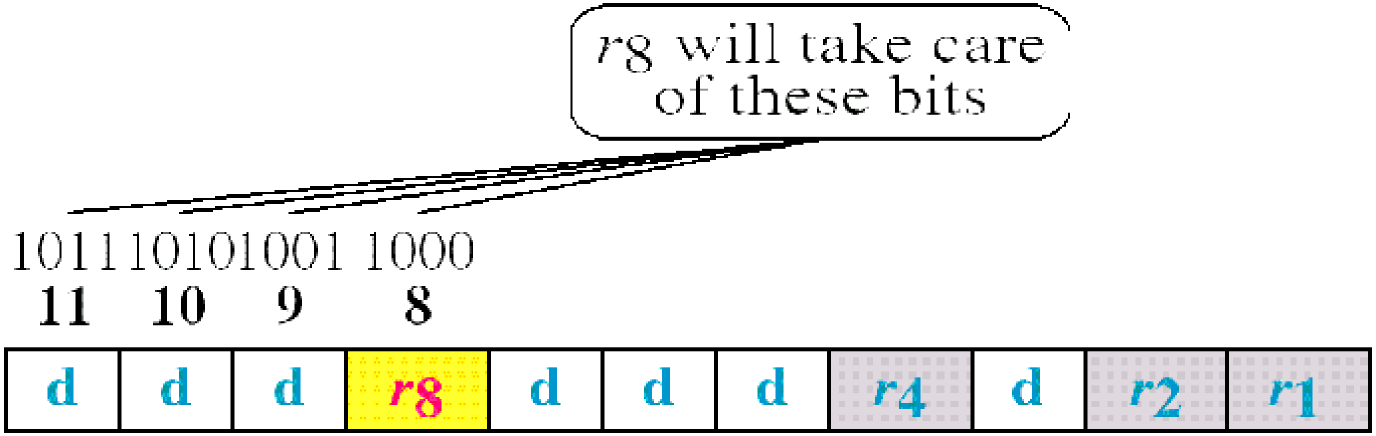


By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996



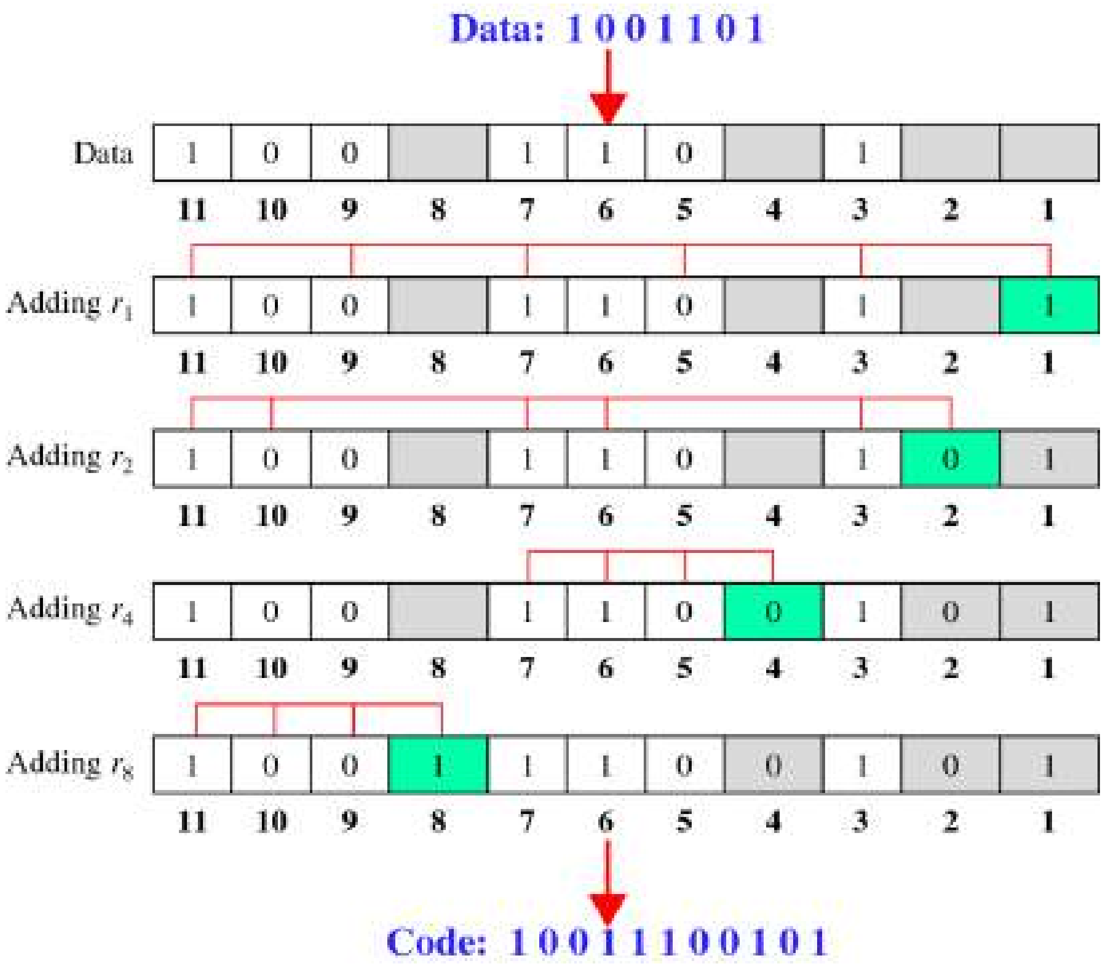
r1 will take care of these bits
1011 1001 0111 0101 0011 0001
11 9 7 5 3 1
d d d r8 d d d r4 d r2 r1
r2 will take care of these bits
1011 1010 0111 0110 0011 0010
11 10 7 6 3 2
d d d r8 d d d r4 d r2 r1



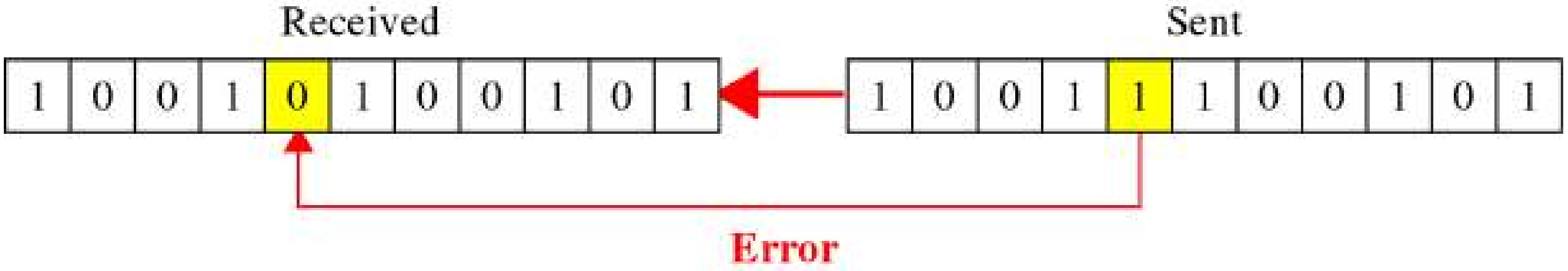


By: Prof. Bhargavi Goswami,
Email:bhargavigoswami@gmail.com,
Mob:+917383816996

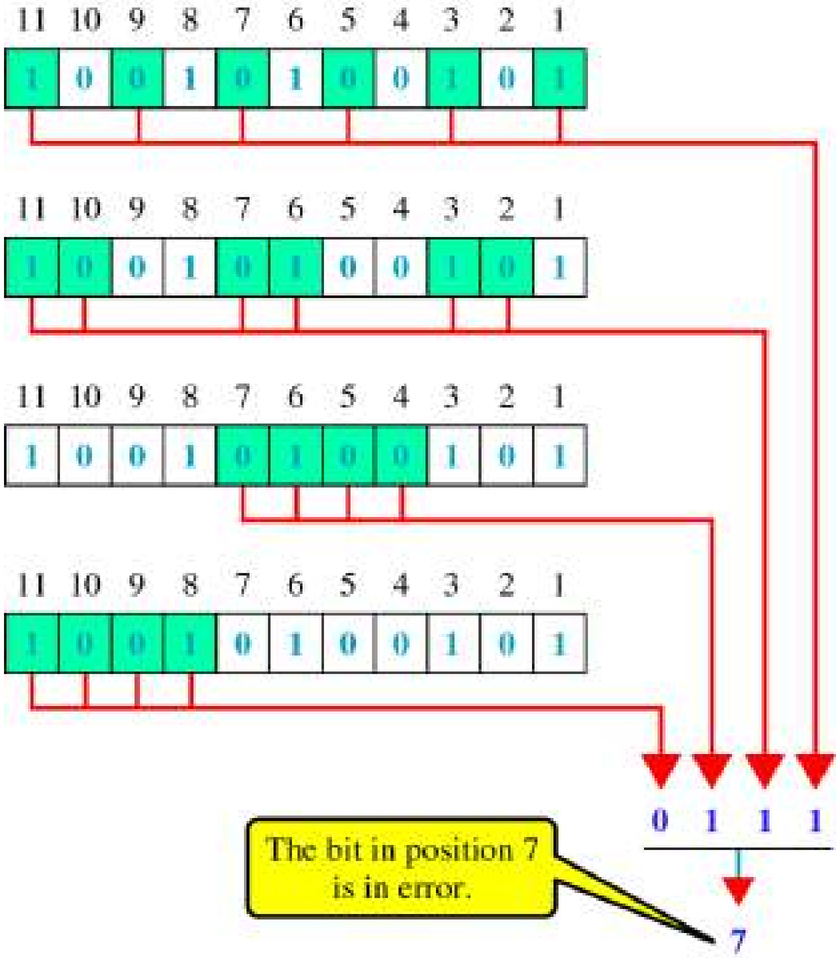
Calculating the r values **Calculating Even Parity**



Example:



Error Detection Using Hamming Code:



Start preparation for final exam….

THANK YOU

Chapter 6:Peer to Peer Protocols

Dr. Bhargavi Goswami

Associate Professor – Head

Department of Computer Science

Garden City College – Bangalore.

Peer to Peer Protocol

- Involves interaction of two or more processes or entities through the exchange of messages, called protocol data unites (PDUs).
- Process layer n protocol
- Passes Service Data Unit (SDU) to layer n+1
- Exchange PDUs to transfer to receiver's layer n
- Delivers SDU to Destination of layer n+1

Service Models

- Constant Bit Rate
- Variable non real time Bit Rate
- Variable real time Bit Rate
- Best Effort Service
- Quality of Service (QoS)

Features of Services

- Arbitrary Message Size or structure
- Sequencing
- Reliability
- Timing
- Pacing
- Flow Control
- Multiplexing
- Privacy, Integrity and Authentication

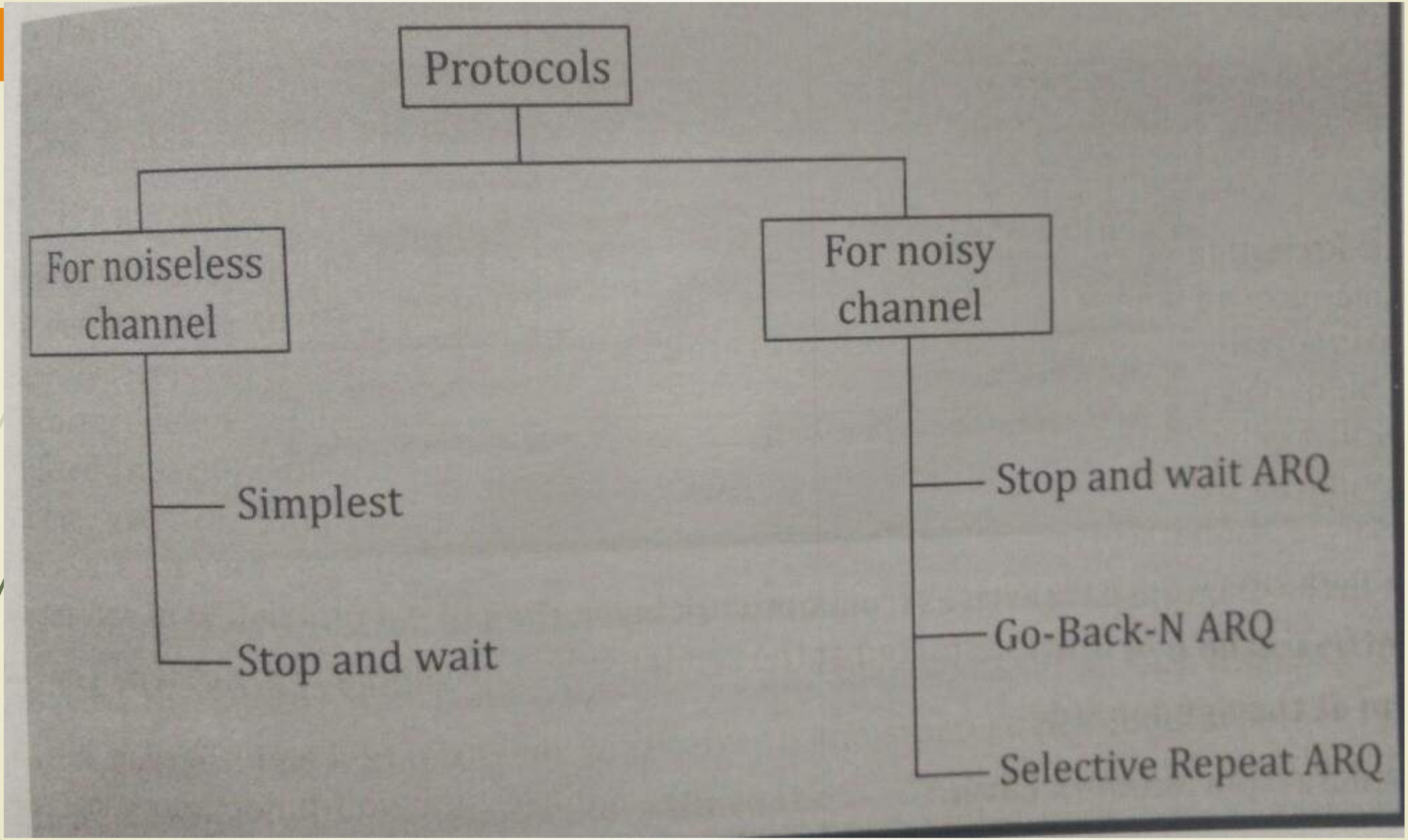
Basic Settings of Peer to Peer Protocol

HOP BY HOP

- Initiates error recovery quickly
- More reliable service
- Node processing is complex
- Every element should process correctly.
- Impose small delay
- Frame arrive in order
- Not recommended in Noisy Unreliable channel

END TO END

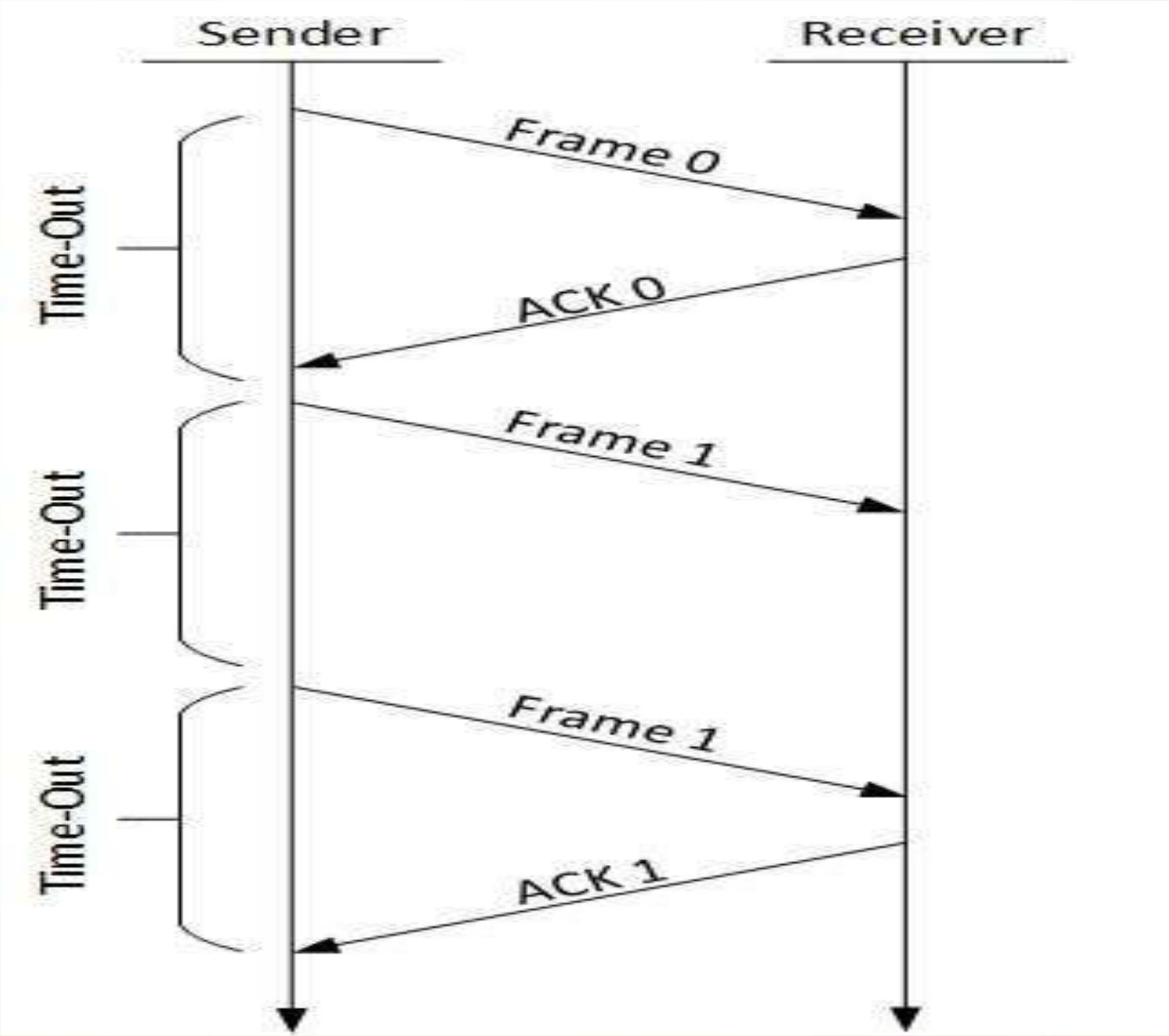
- Uses network layer services
- Recommended for environment with less errors
- Intermediate nodes are free from responsibility of error recovery
- Blocks of information are forwarded across the path
- Error recovery is performed only by end systems


Protocols
For noiseless channel
Simplest
Stop and wait
For noisy channel
Stop and wait ARQ
Go-Back-N ARQ
Selective Repeat ARQ

ARQ

- Automatic Repeat Request Protocols
- Does error control
- Provide reliable data transfer
- Is a control mechanism for data transfer
- Based on Acknowledgement and Non Acknowledgement
- i.e ACK and NACK
- Elements
  - Protocol
  - Frames (Data and Control)
  - Timeout Mechanism

STOP & WAIT ARQ



Stop & Wait

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

Frame Lost

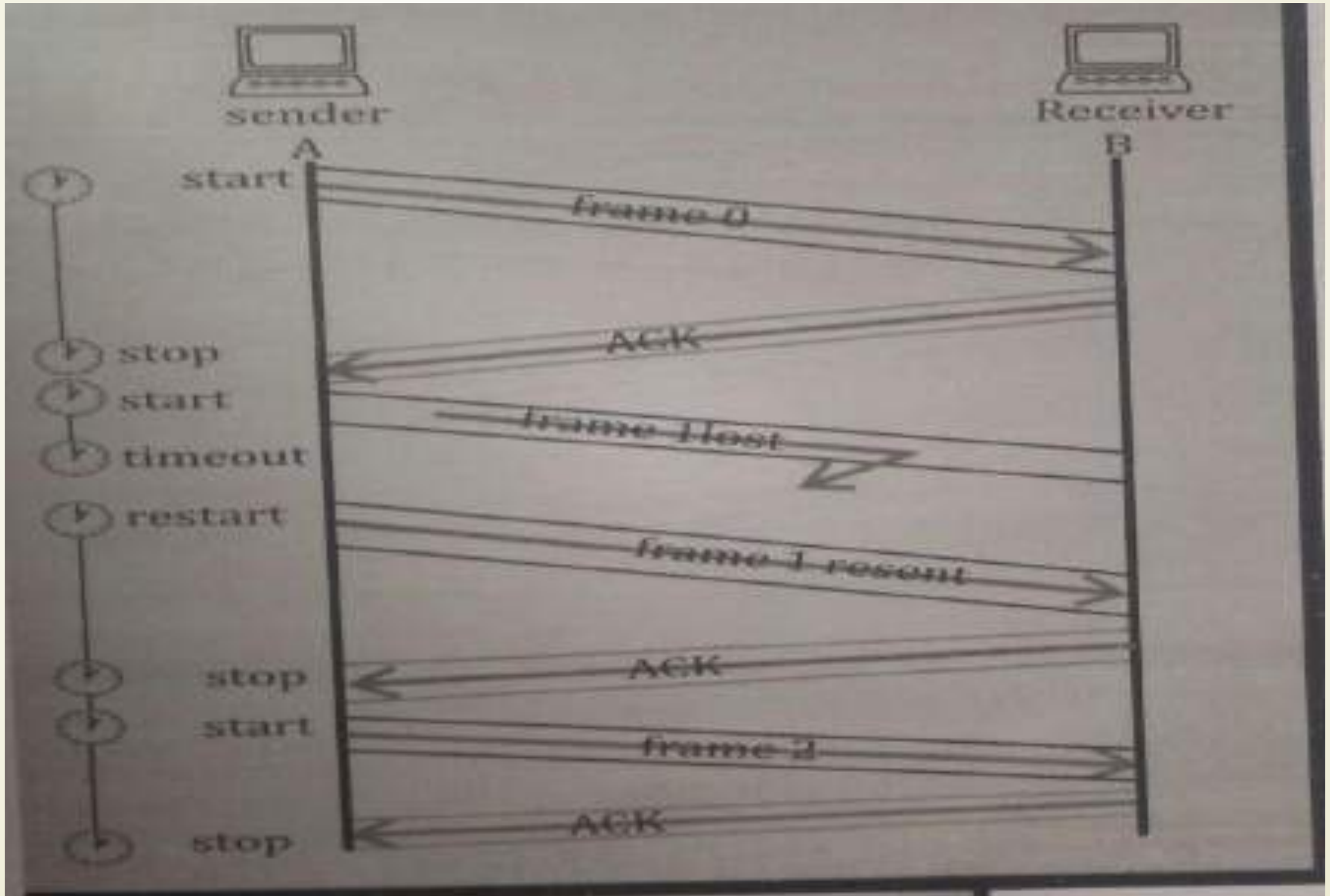


Figure 9.3 Frame 1 lost

Delayed ACK Frame

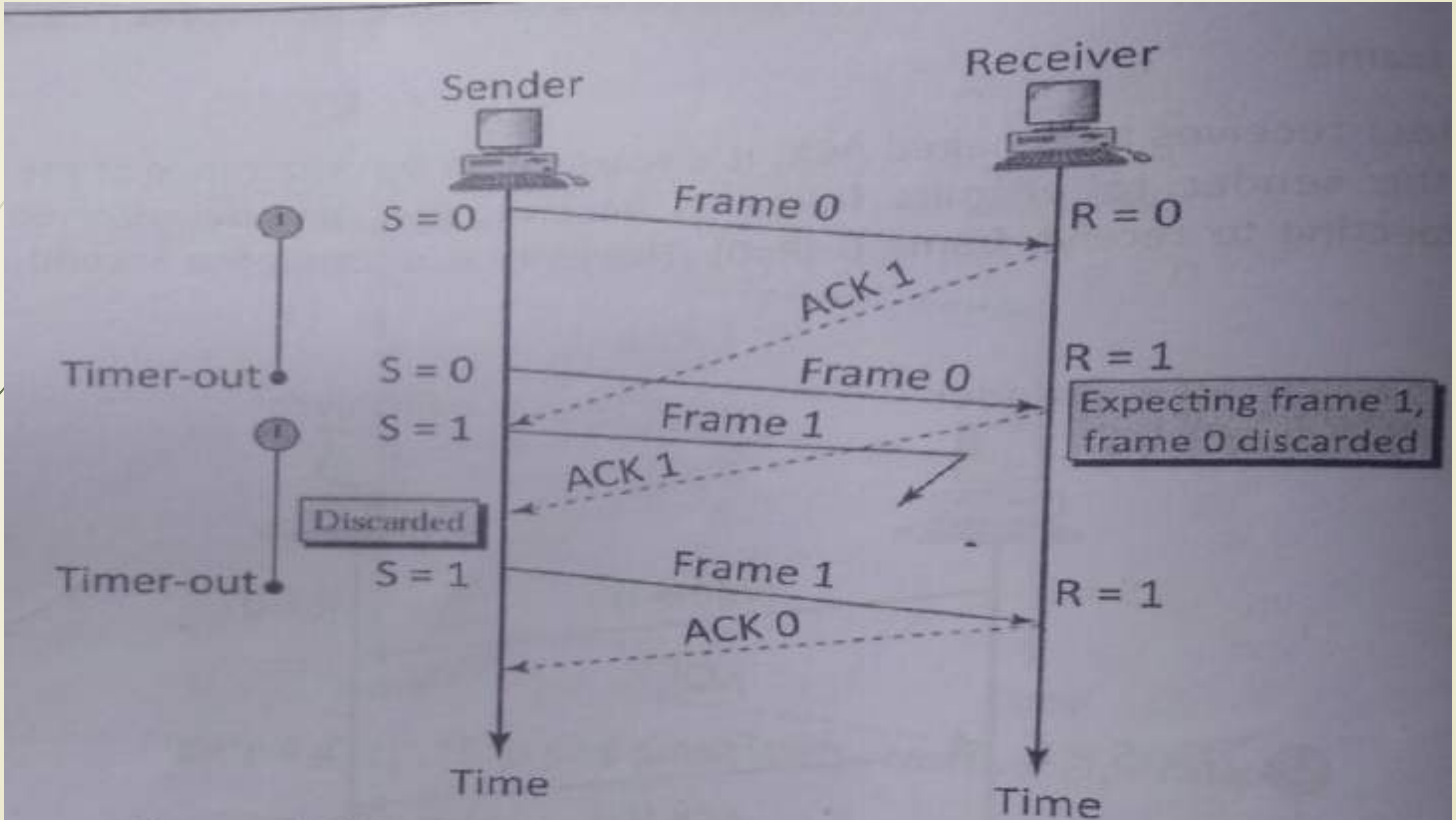


Figure 6.7(d) : Stop and Wait ARQ - Delayed ACK Frame

Requirement of ACK Number

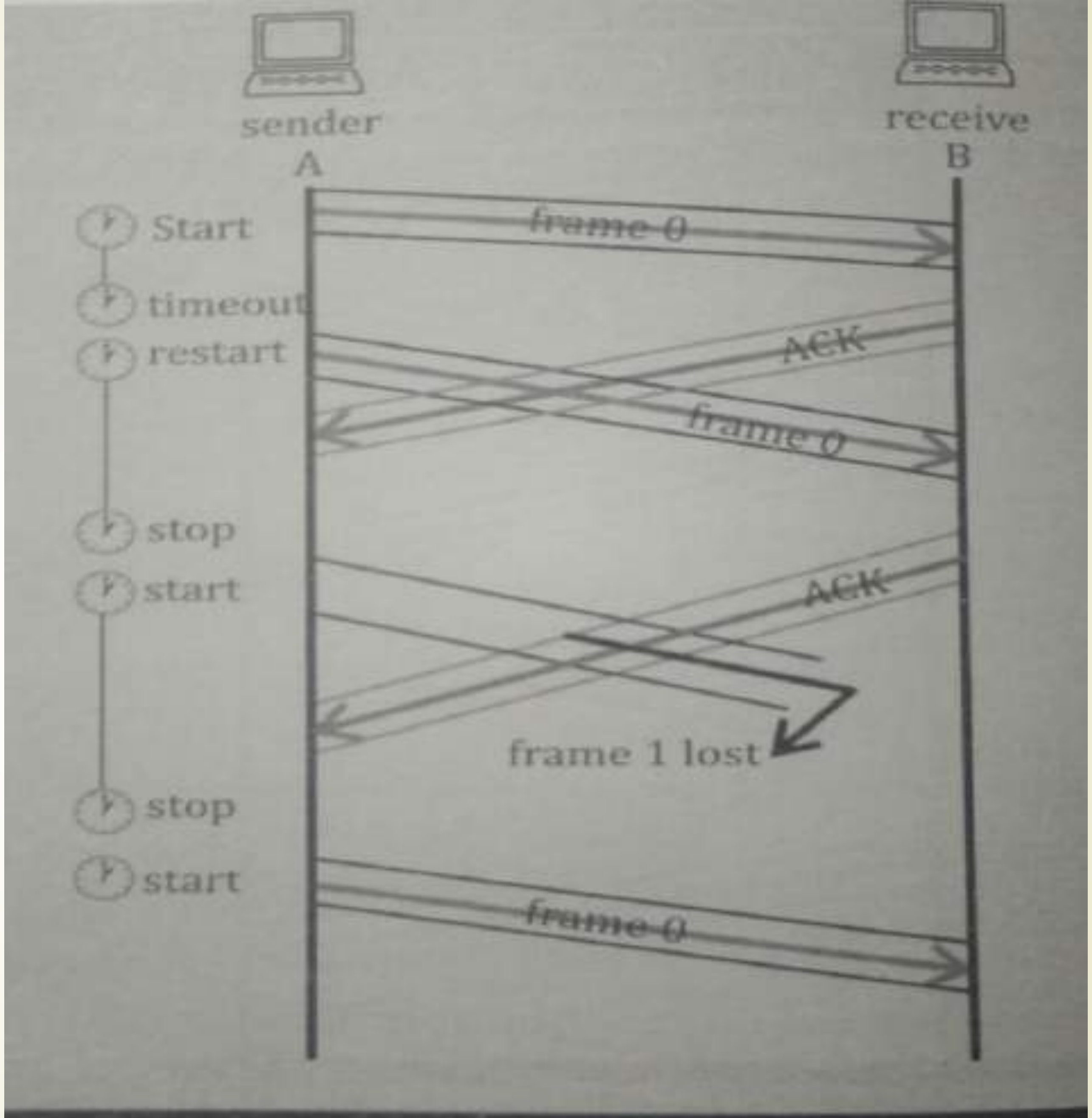


Figure 9.6 Need for Acknowledgement Number

Solution:
ACK Number

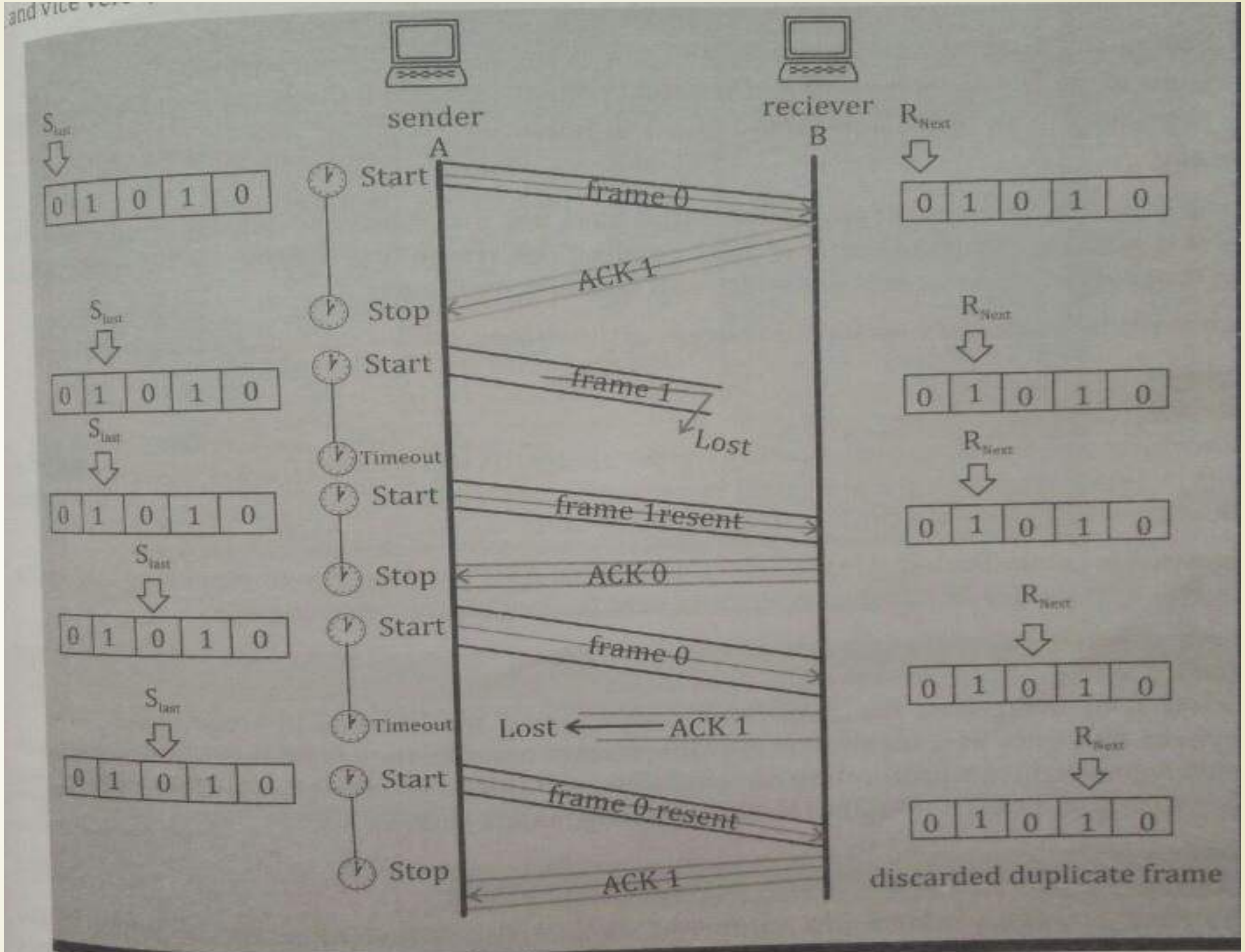


Figure 9.7 Use of ACK Numbers

Piggybacking

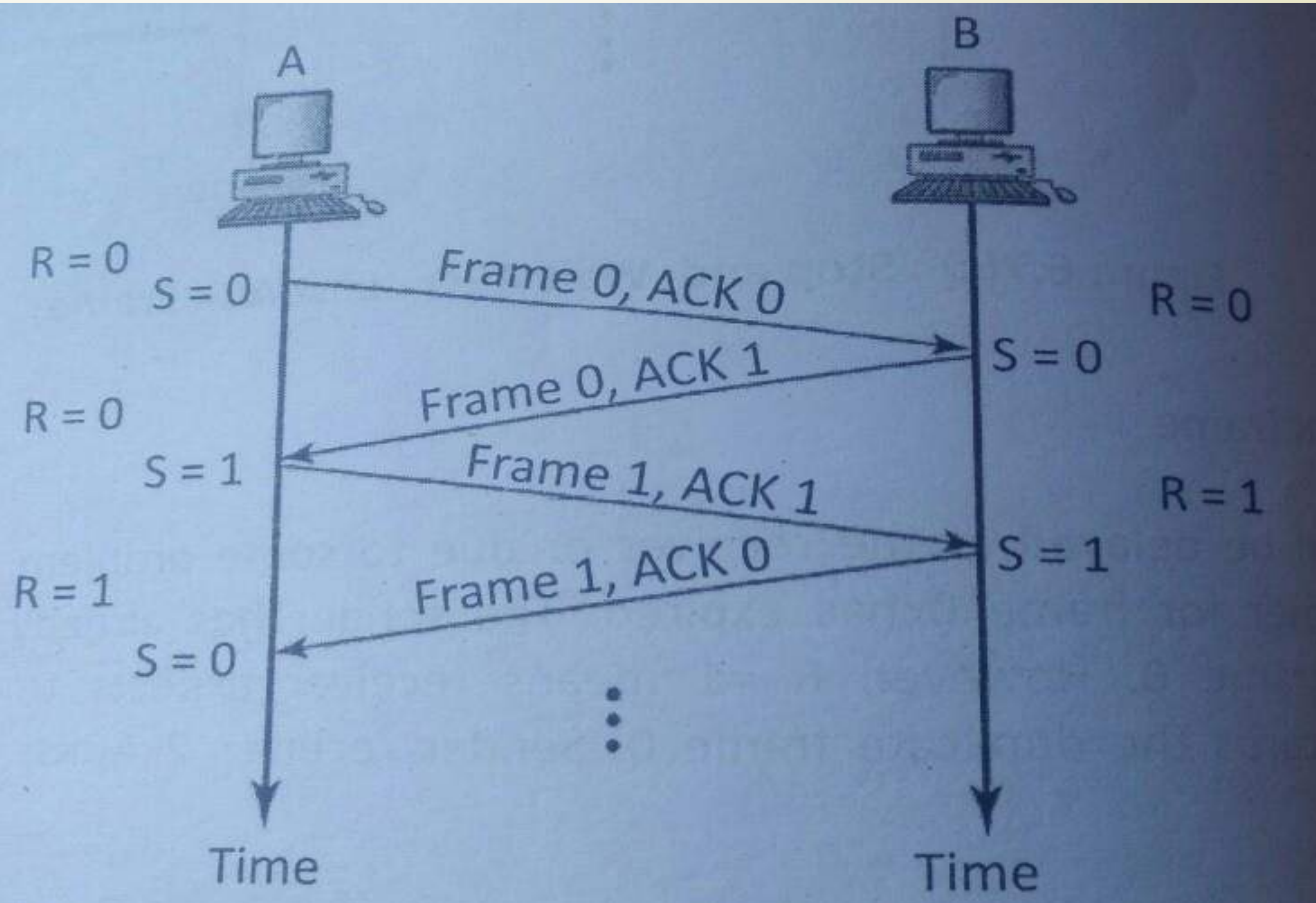


Figure 6.7(e) : Stop and Wait ARQ - Piggybacking

Same Piggybacking

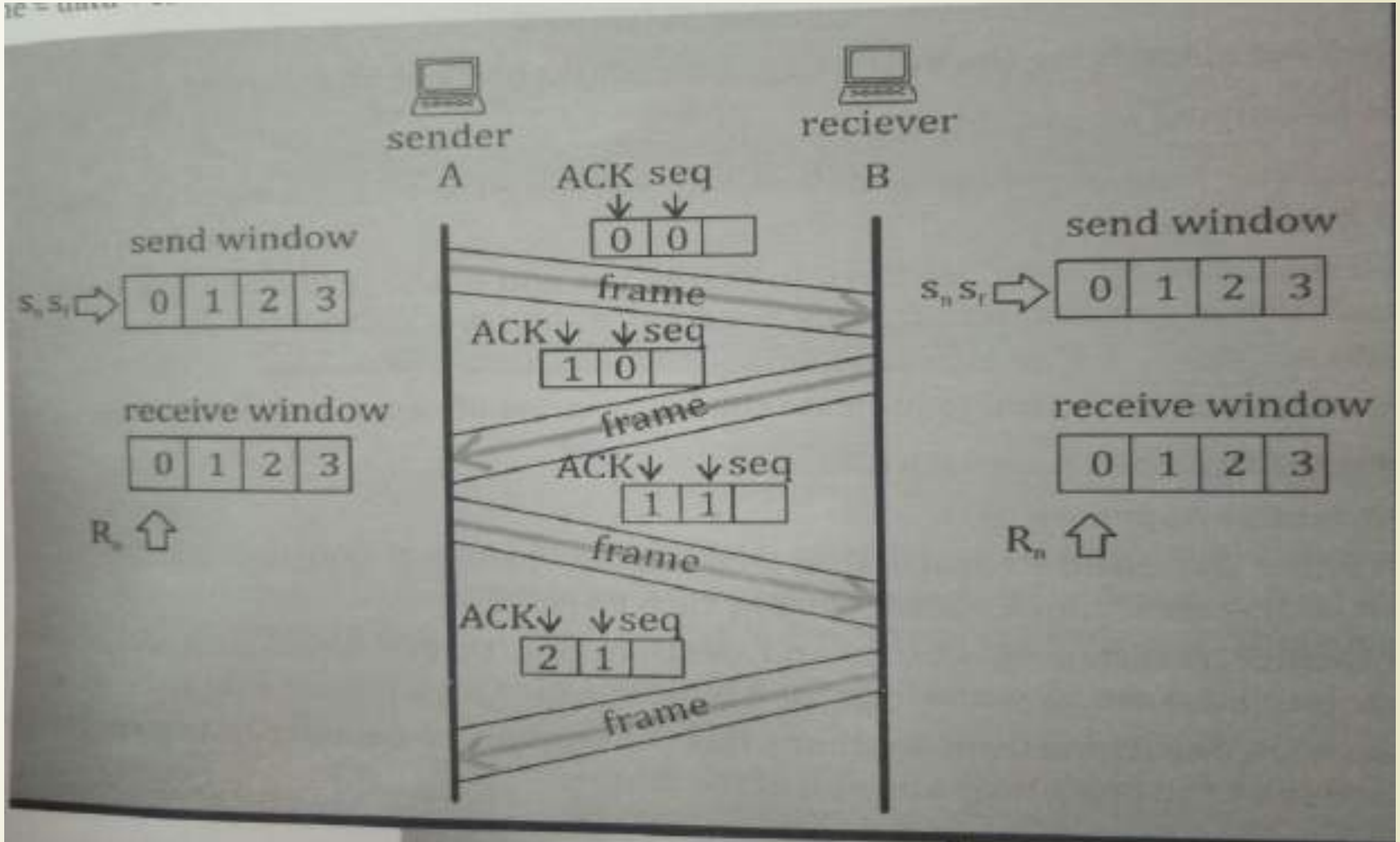
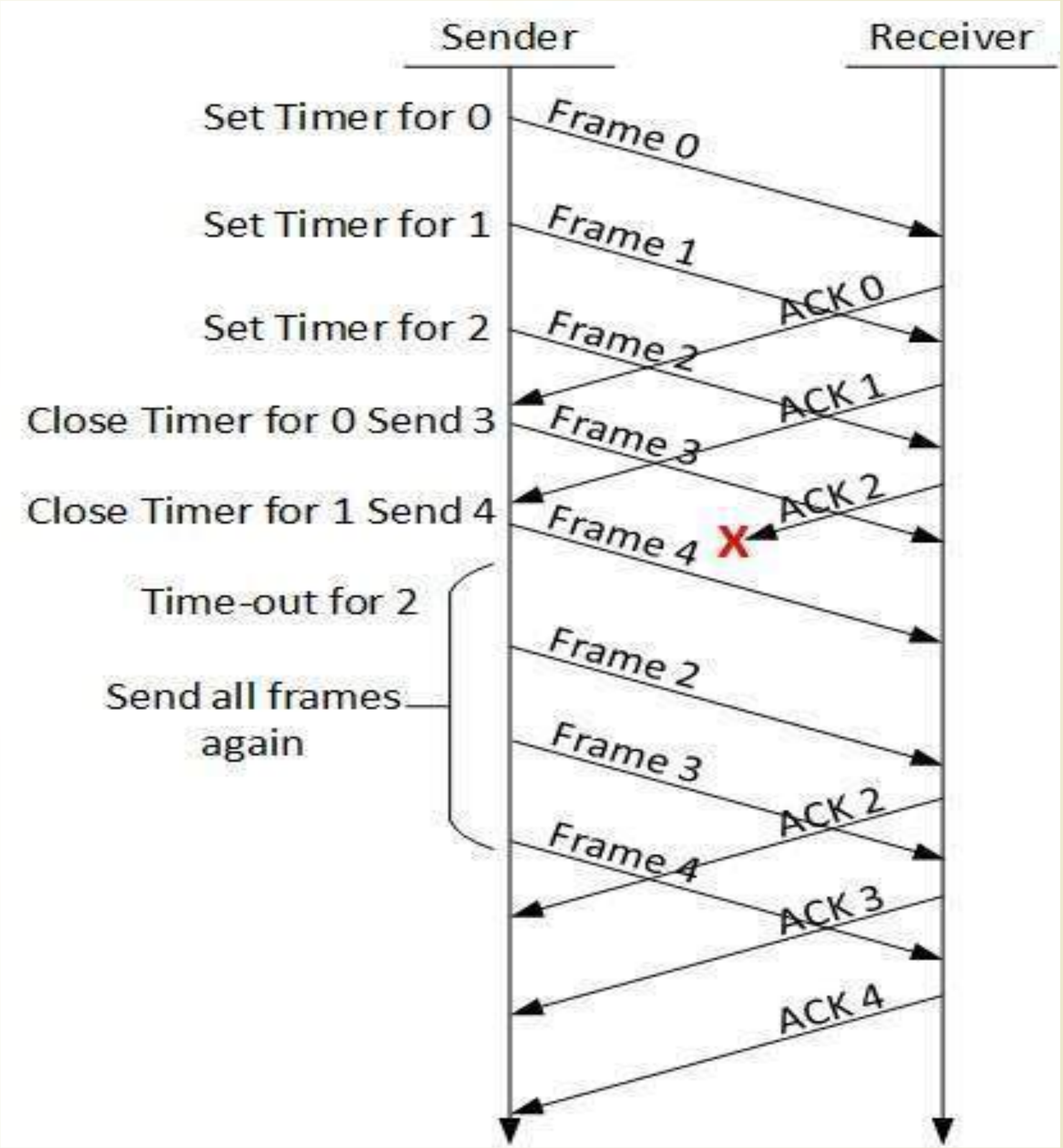


Figure 9.14 Piggybacking

Go Back N



Sender
Receiver
Set Timer for 0
Frame 0
Set Timer for 1
Frame 1
ACK 0
Set Timer for 2
Frame 2
ACK 1
Close Timer for 0 Send 3
Frame 3
ACK 2
Close Timer for 1 Send 4
Frame 4
X
Time-out for 2
Frame 2
Send all frames again
Frame 3
ACK 2
Frame 4
ACK 3
ACK 4

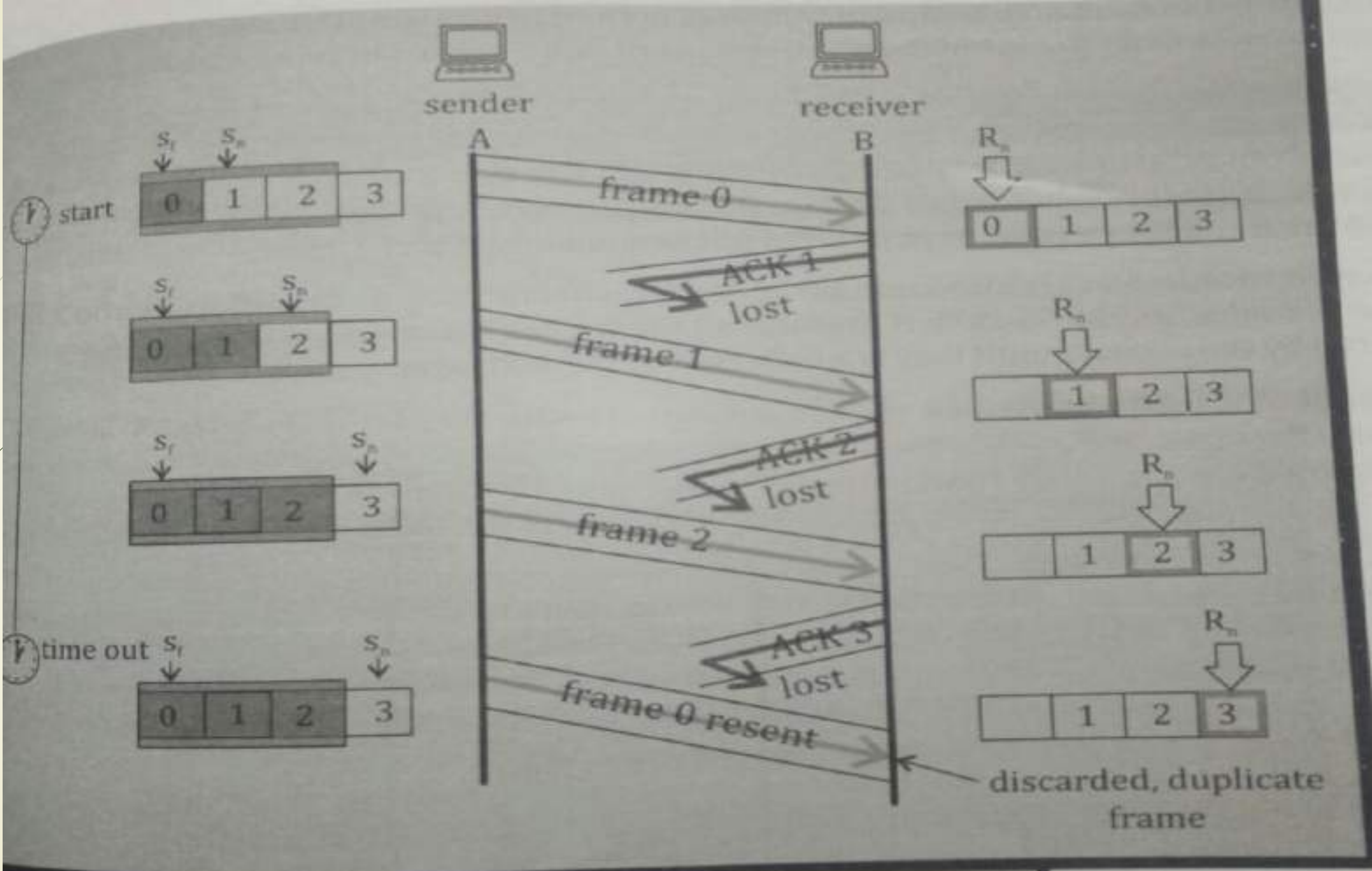
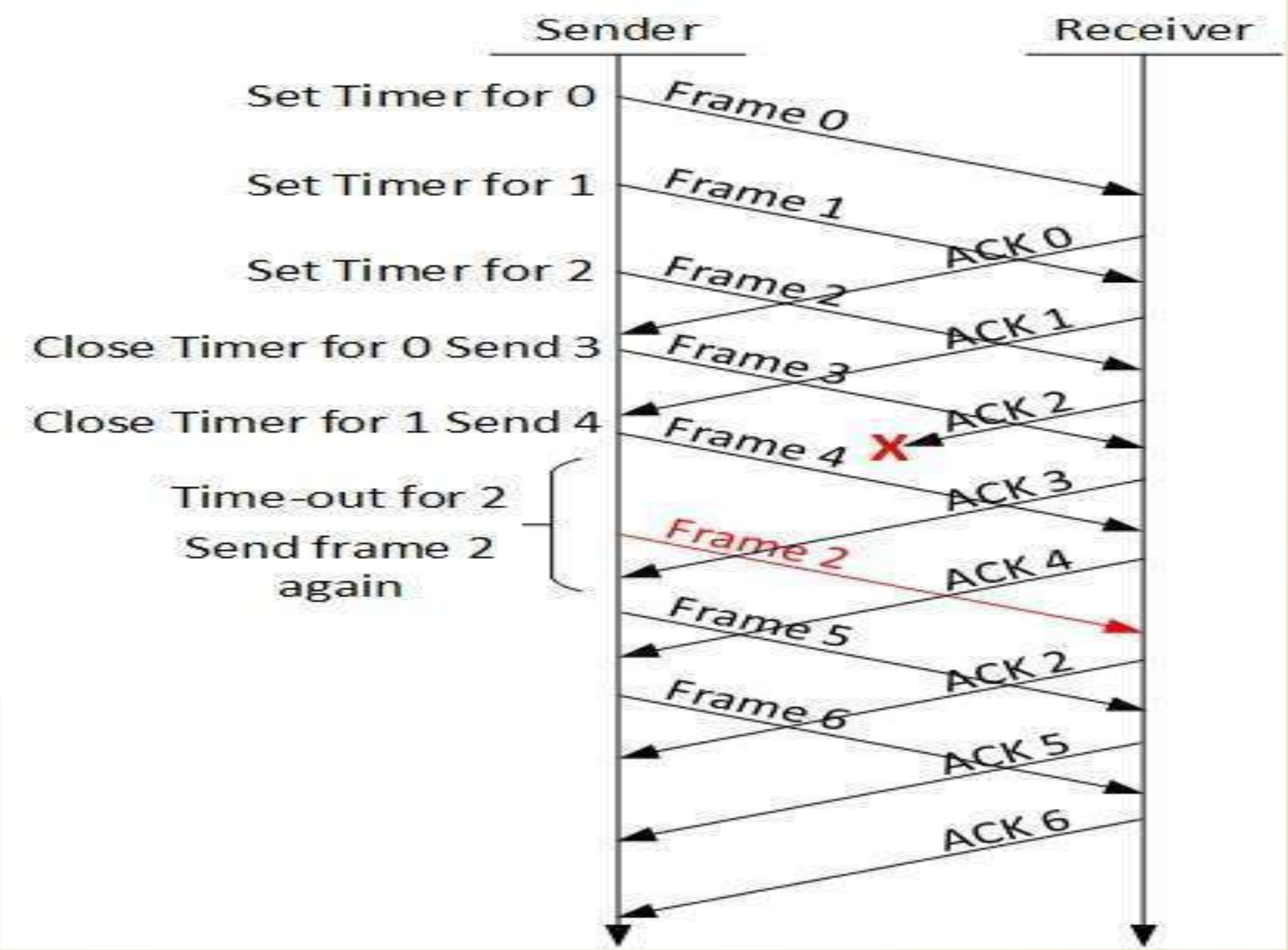


Figure 9.12 Flow diagram of Go-Back-N ARQ

Selective Repeat



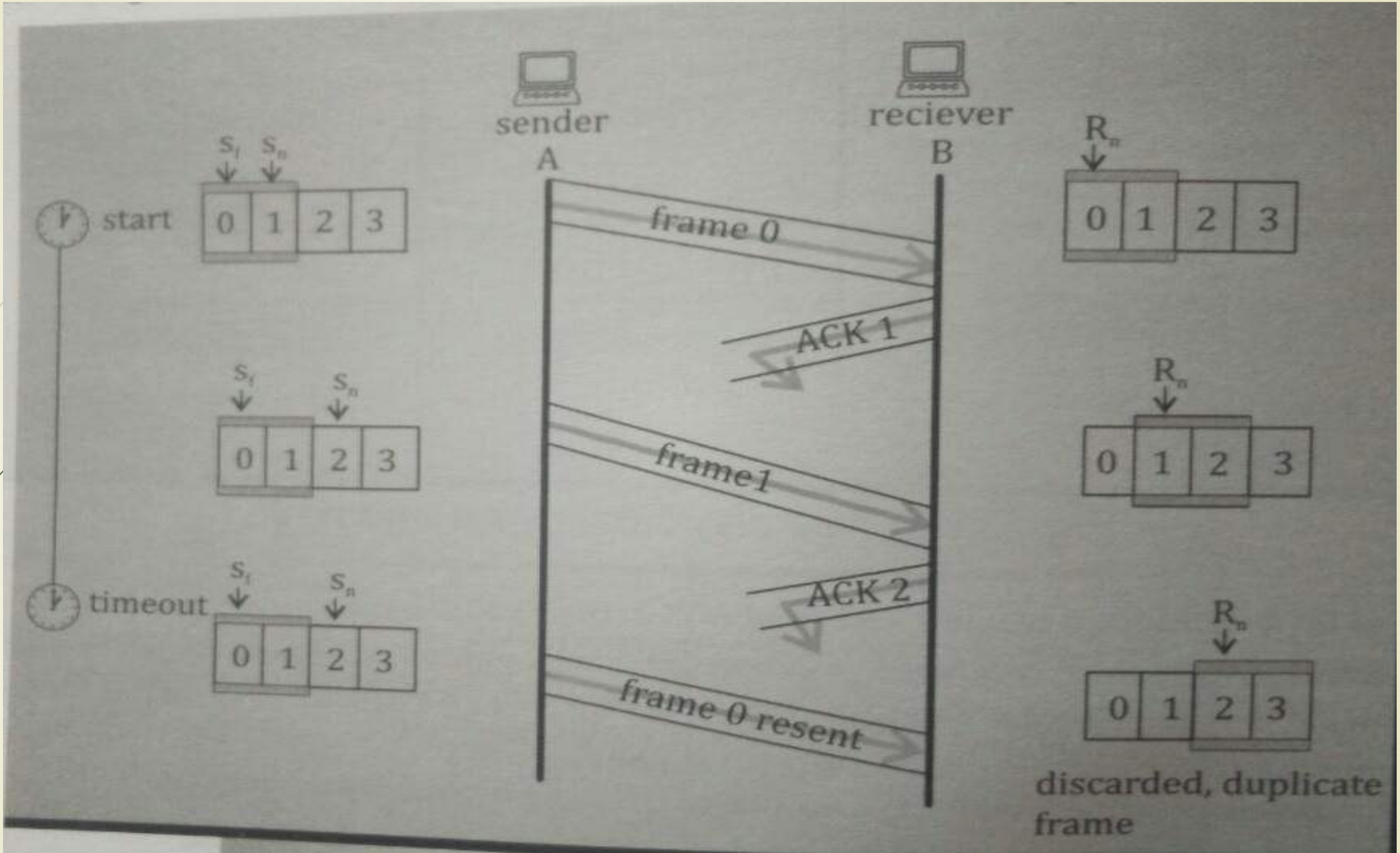


Figure 9.13 Flow diagram of Selective Repeat ARQ

Sliding Window

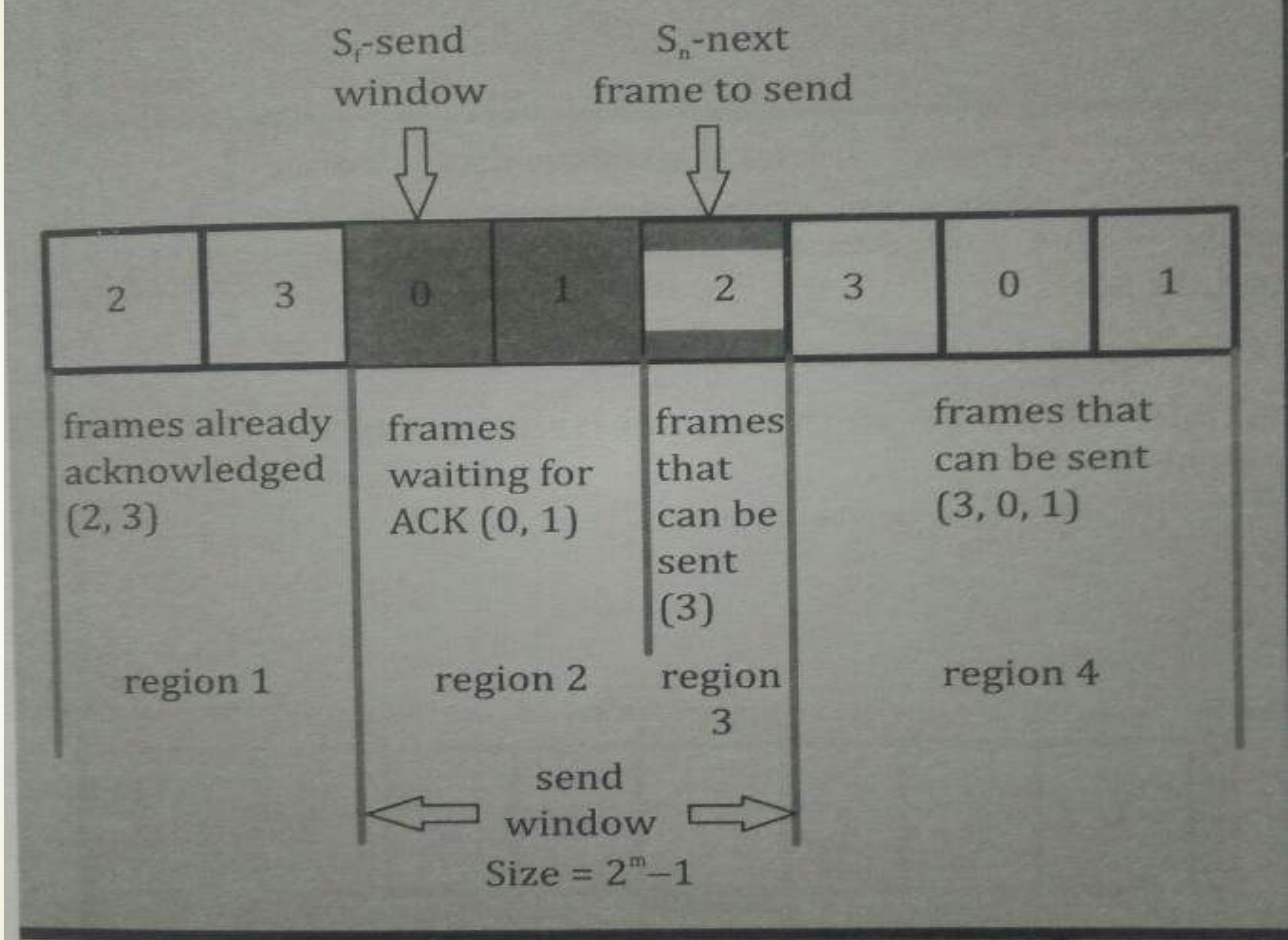


Figure 9.8 Send Window Before Sliding

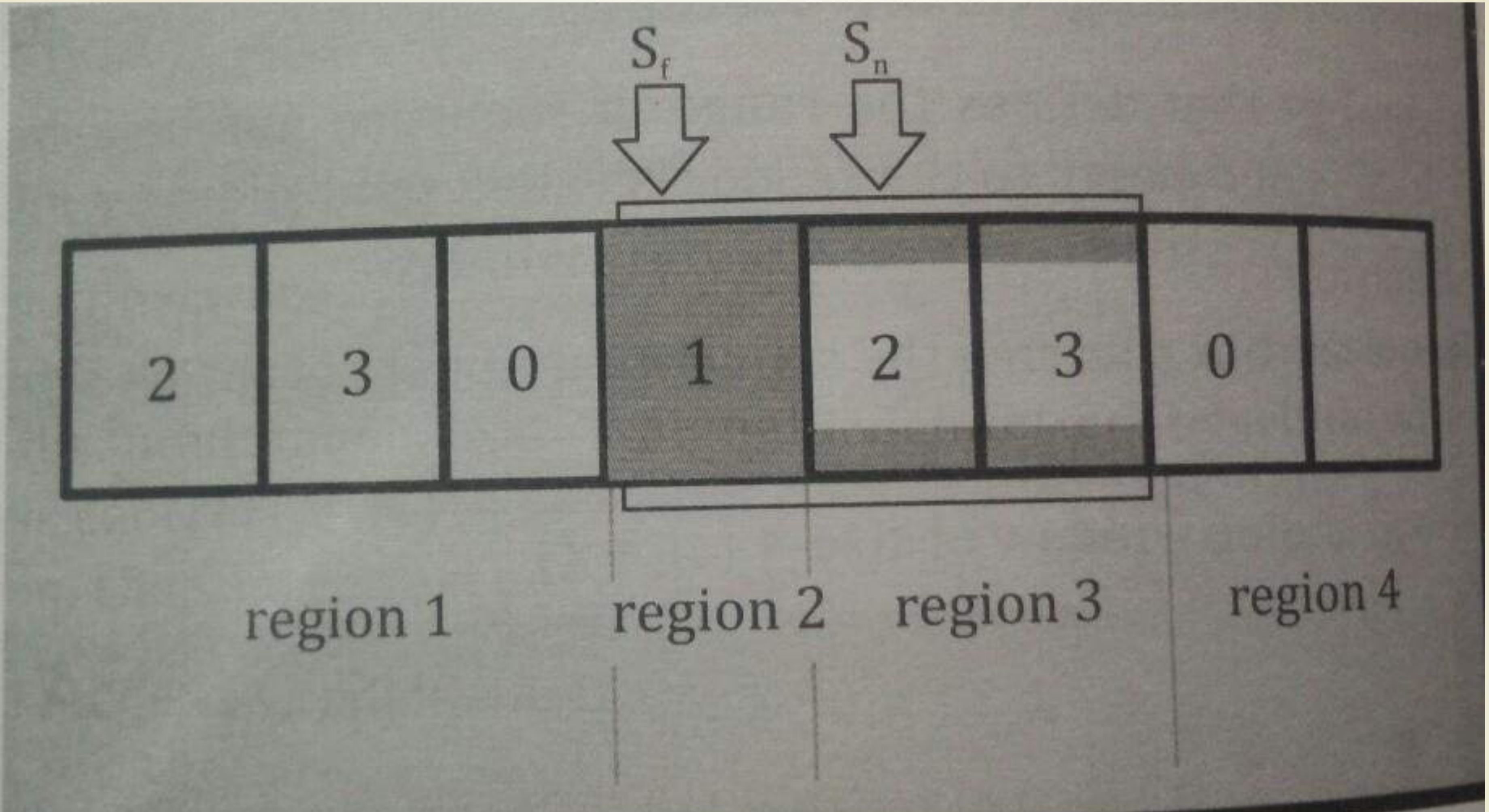


Figure 9.9 Send window after sliding

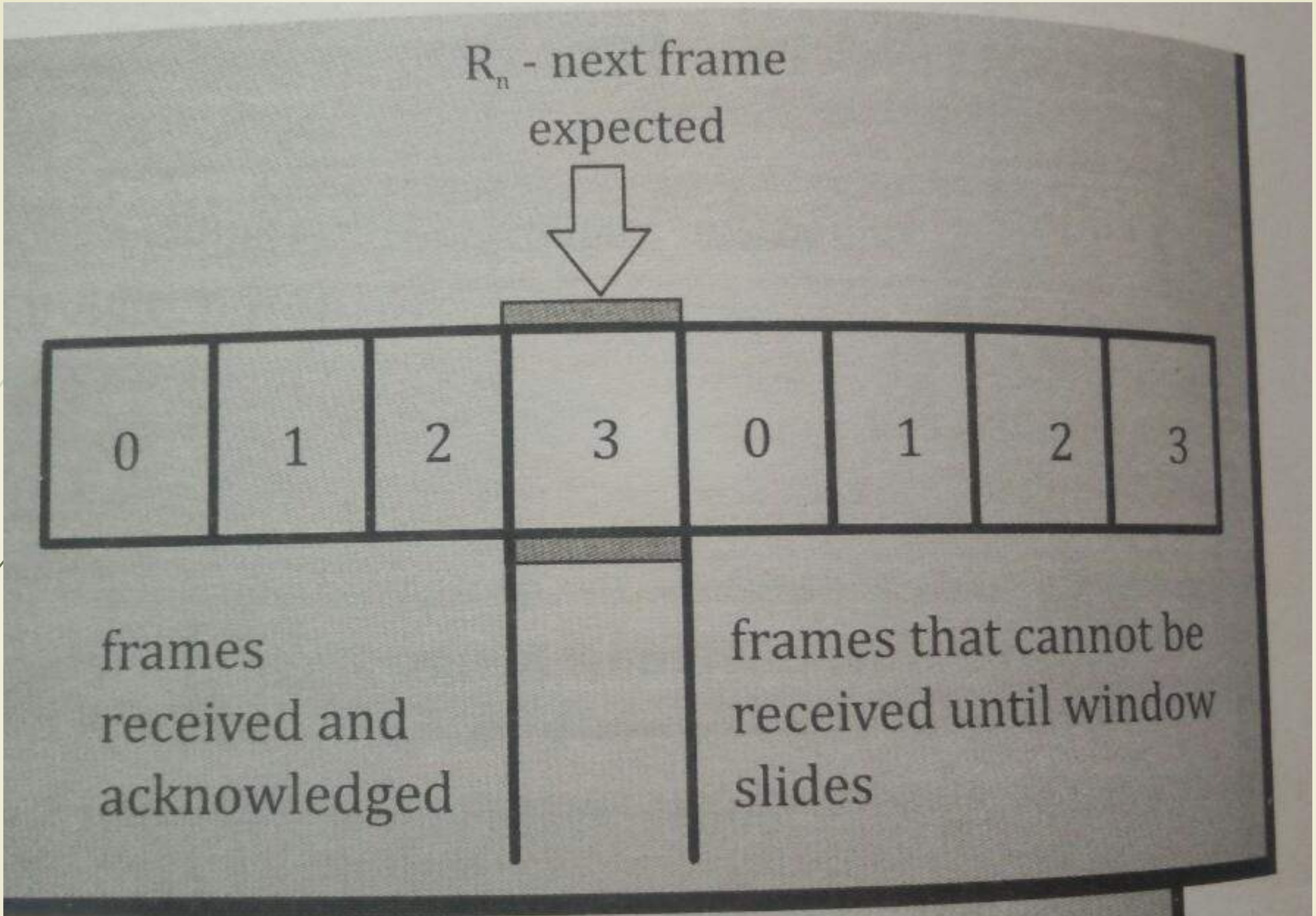


Figure. 9.10 Receive window before sliding

Sliding Window Flow Control

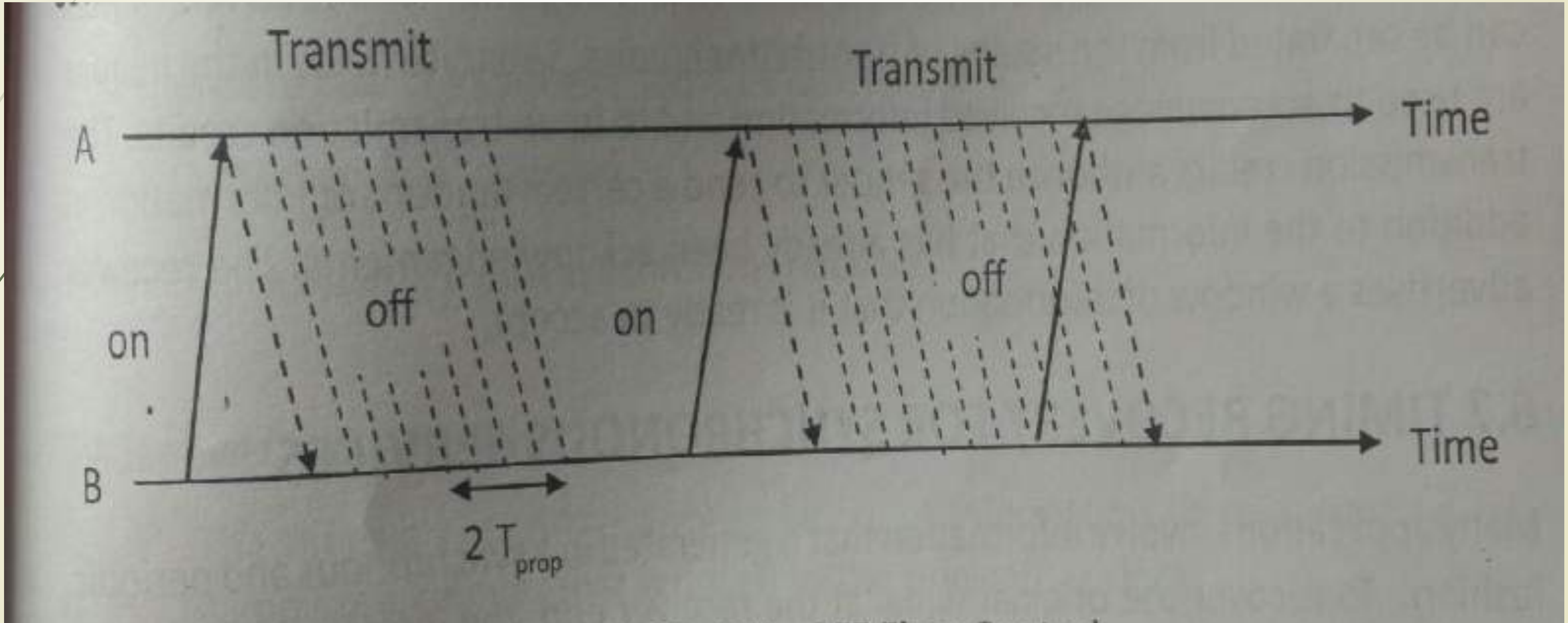


Figure 6.10 : ON - OFF Flow Control

Sliding Window Flow Control

- It guarantees the reliable delivery of data
- It ensures that data delivers in order
- It enforce flow control between sender and receiver
- Two types
  - On – Off Flow Control
  - Sliding Window Flow Control

TIMING RECOVERY FONR SYNCHRONOUS SERVICES

- The information must be input to decoder at the same rate at which it was produced at encoder.
- But, in reality, network impose delay.
- This effect is called Timing Jitter.
- Solution: Timing Recovery protocols.
- Timestamp can be added to the blocks before transmission begins.
- These timestamps are used by receivers for further time synchronization.
- Clock Recovery Procedure: Procedure to synchronize the receiver clock to transmitter clock.
- Two techniques:
  - Adaptive Clock Recovery
  - Clock Recovery with Synchronous Network

Adaptive Clock Recovery

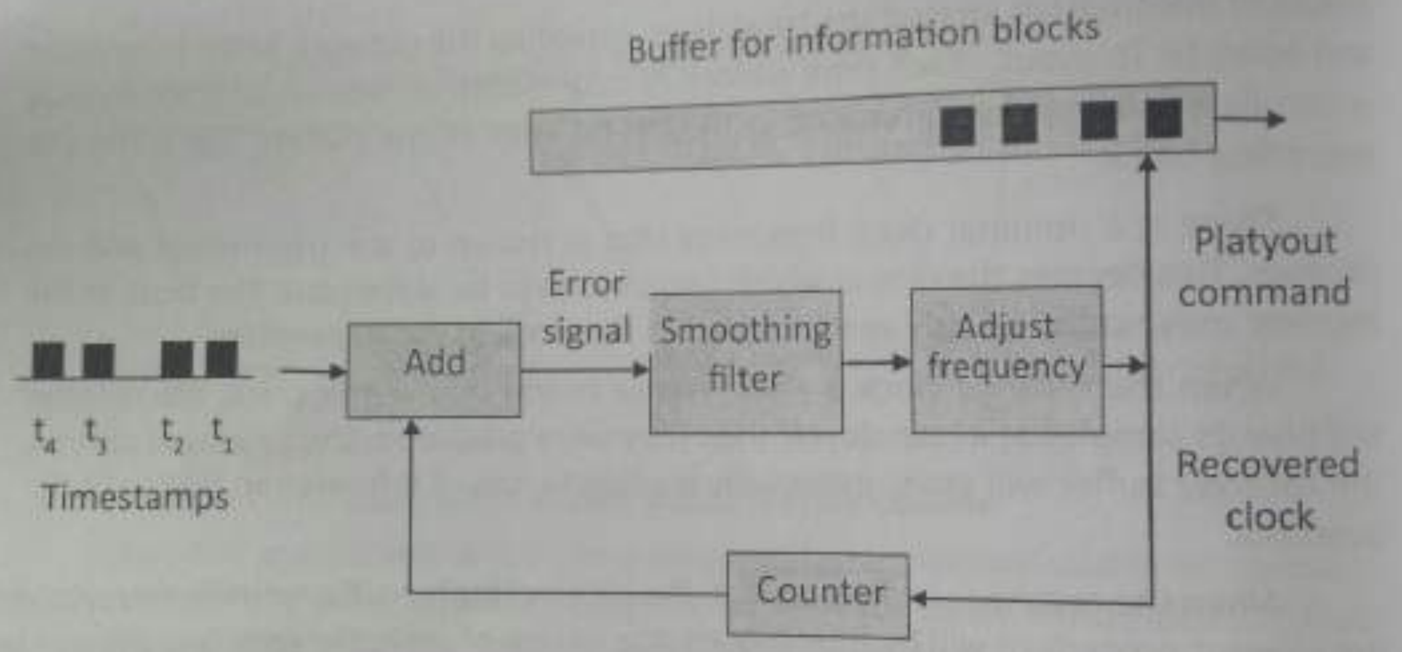


Figure 6.12 : Adaptive Clock Recovery

Clock Recovery with Synchronous N/w

- All the elements are synchronized to common clock
- Use GPS – Global Positioning System

$$\frac{Fn}{Fs} = \frac{(1/M)}{(1/N)}$$

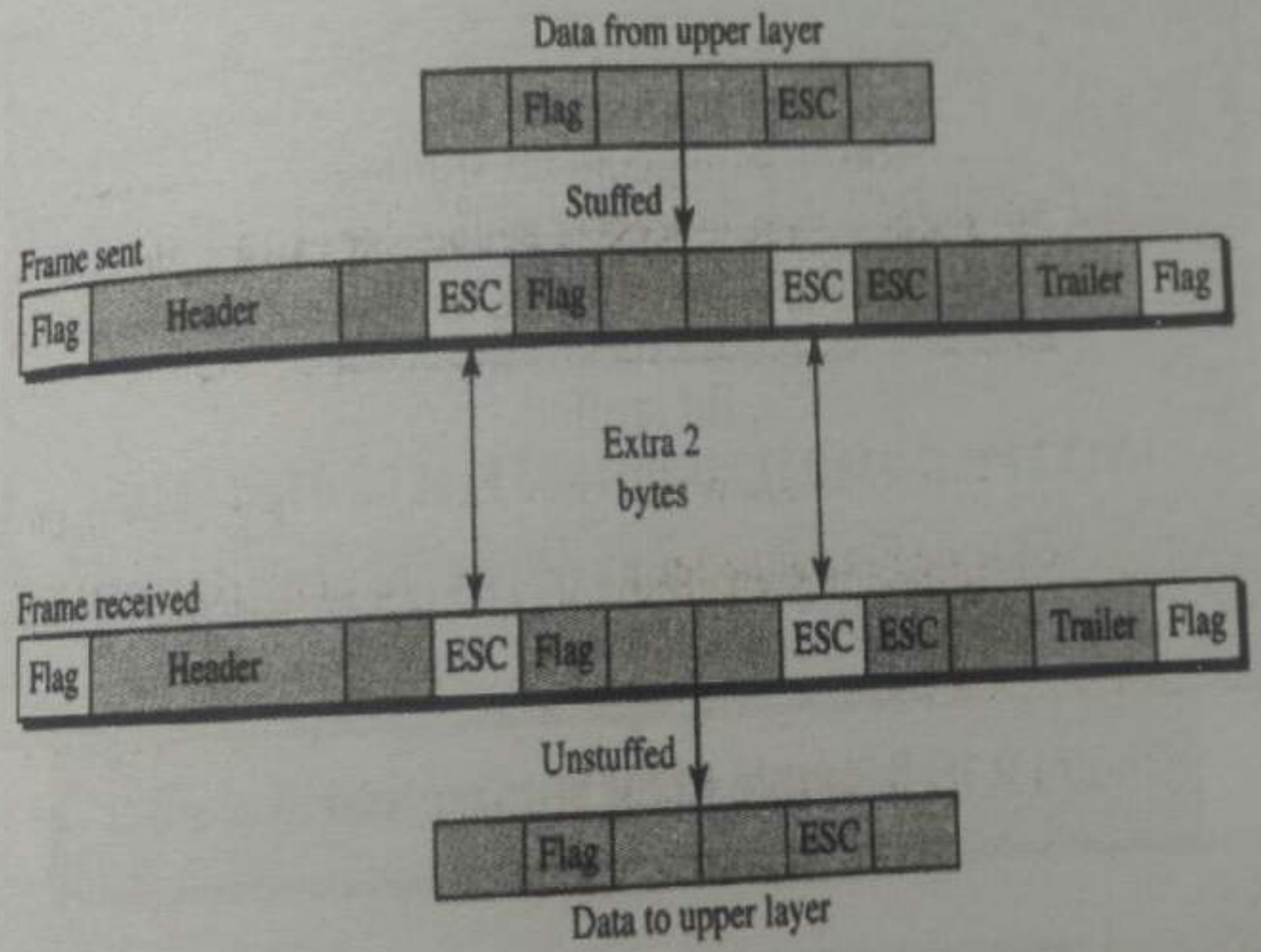
$$Fr = Fn - \Delta F$$

- Fs – Frequency of sender
- Fn – Frequency of network
- N – Cycles of Sender
- M – Cycles of Network
- ΔF – Difference of frequency, Delta Frequency
- Fr – Received Frequency
- Fn – Network Frequency

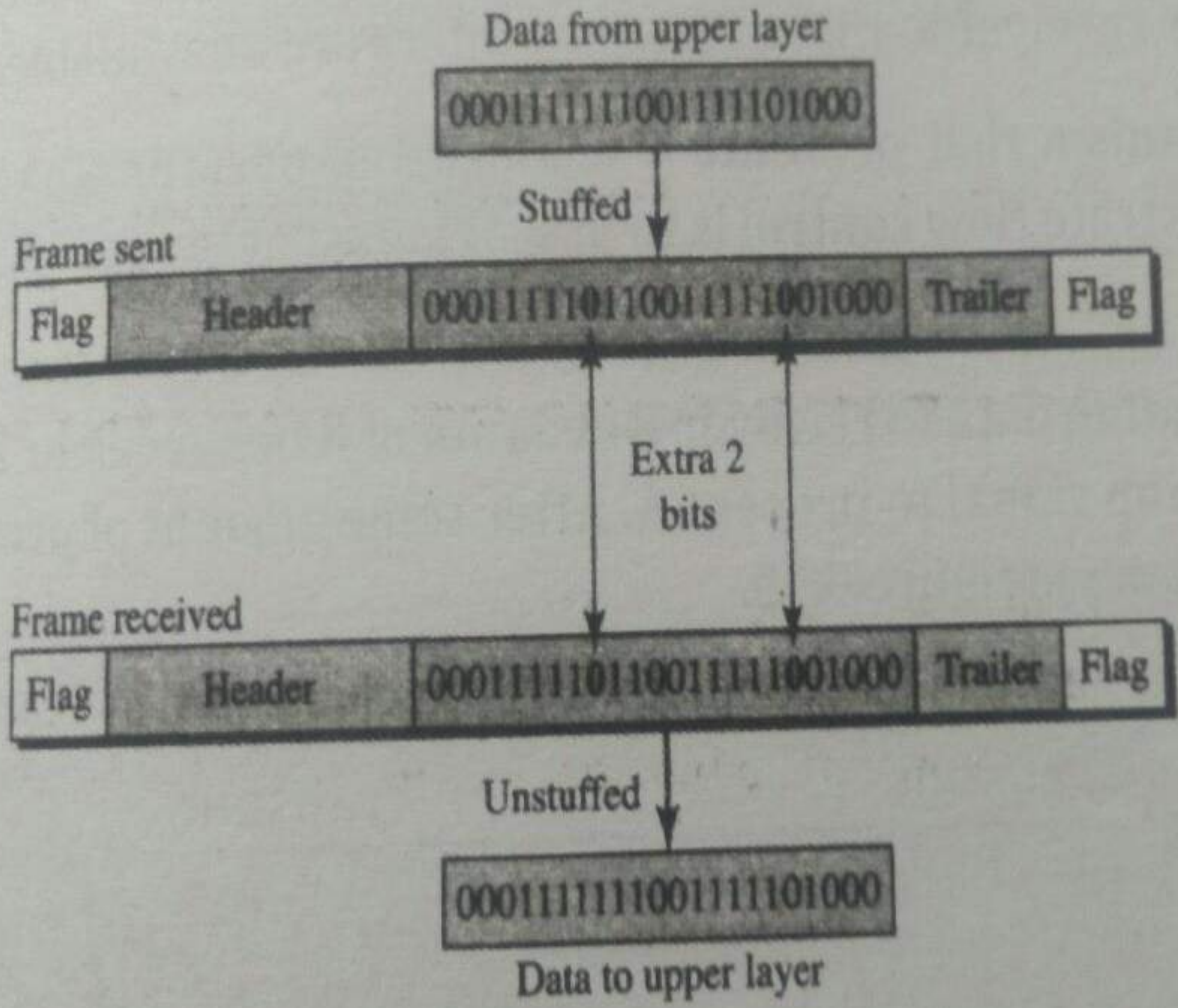
FRAMING

- Two Types:
  - Character Based / Byte Stuffing
  - Flag Based / Bit Stuffing
- Practice examples taught on board.
- Check next two figures.

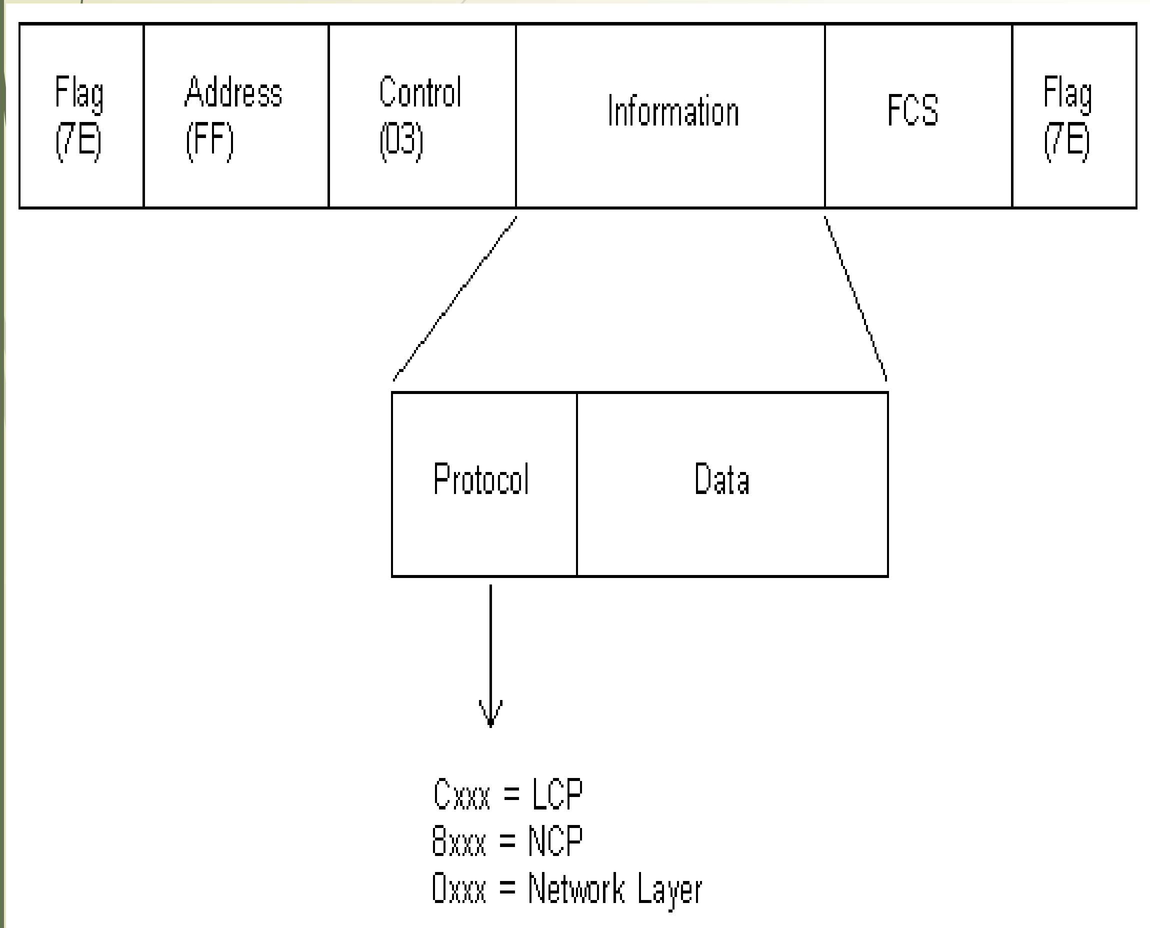
Byte Stuffing

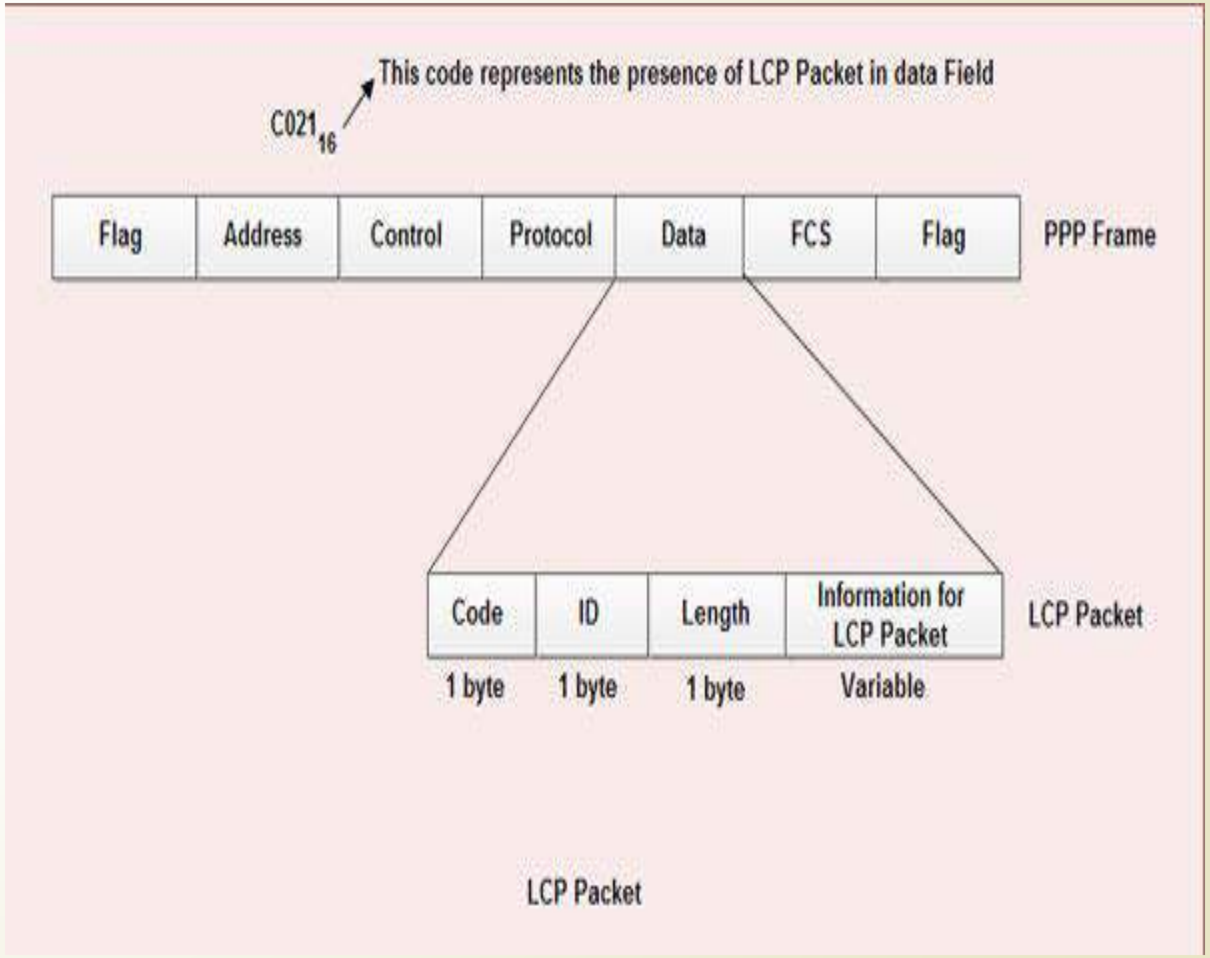


Bit Stuffing



Point to Point Protocol (PPP)





Transition Phase in PPP

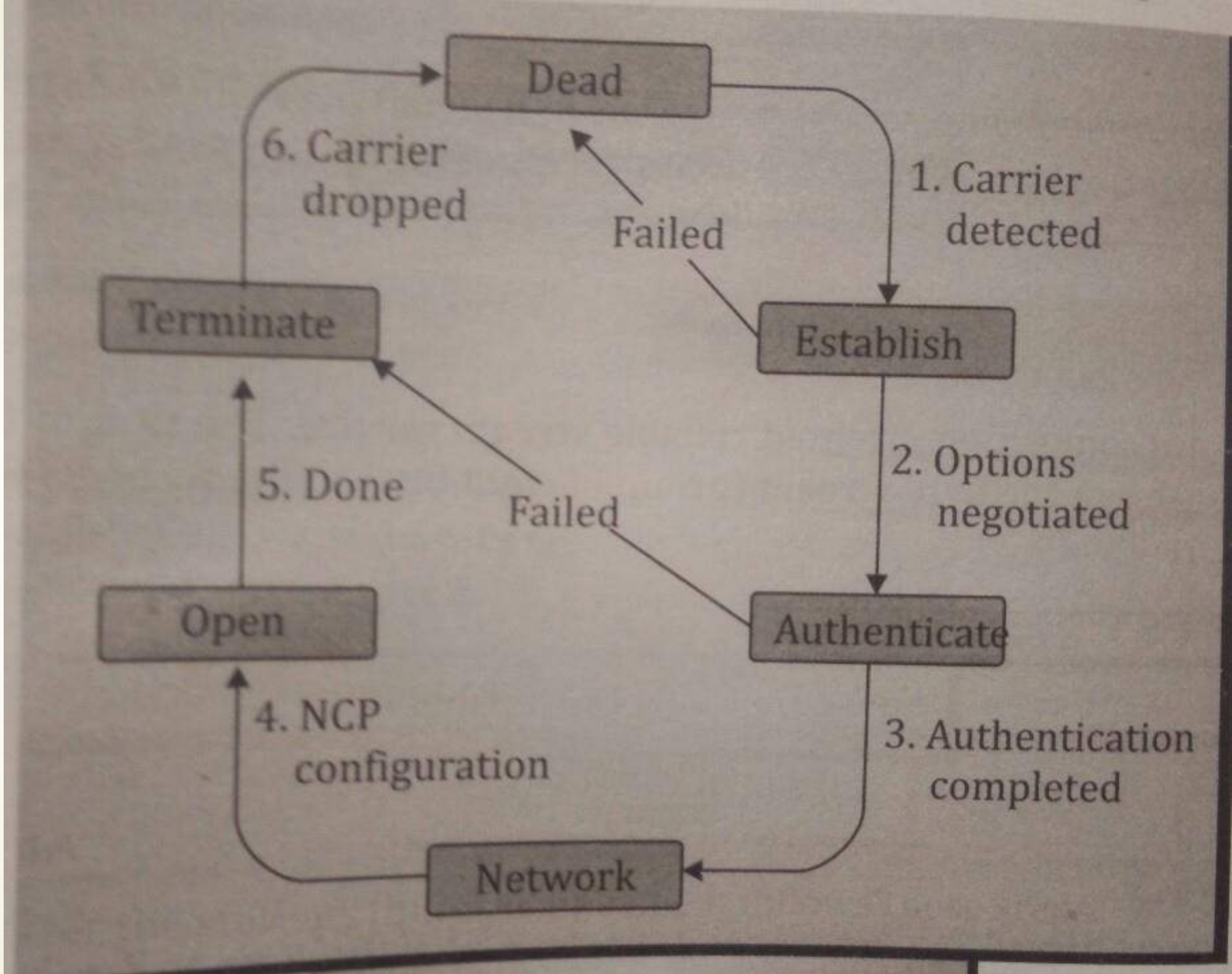


Figure 9.20 PPP phase diagram

Example

Home PC to Internet Service Provider.

1. PC Calls router via Modem
2. PC and Router Exchange LCP Packet to negotiate PPP Parameters
3. Check on Identities
4. NCP Packet exchanged to configure the network layer eg. TCP/IP needs IP.
5. Data Transport started
6. NCP Used to tear down the network layer connection (free the IP). And LCP shutdown the link.
7. Modem hangs up.
8. Closed.

HDLC – High Level Data Link Control

- It is Bit Oriented Protocol for communication over Point to Point and Multipoint links.
- It implement ARQ Techniques.
- Topics:
  - Configuration and Transfer Modes
  - Frame Format
  - Frame Types
  - Control Field

HDLC Configuration and Transfer Modes

- Provides two modes
  - NRM – Normal Response Mode
  - ABM – Asynchronous Balanced Mode

NRM – Normal Response Mode (Unbalanced)

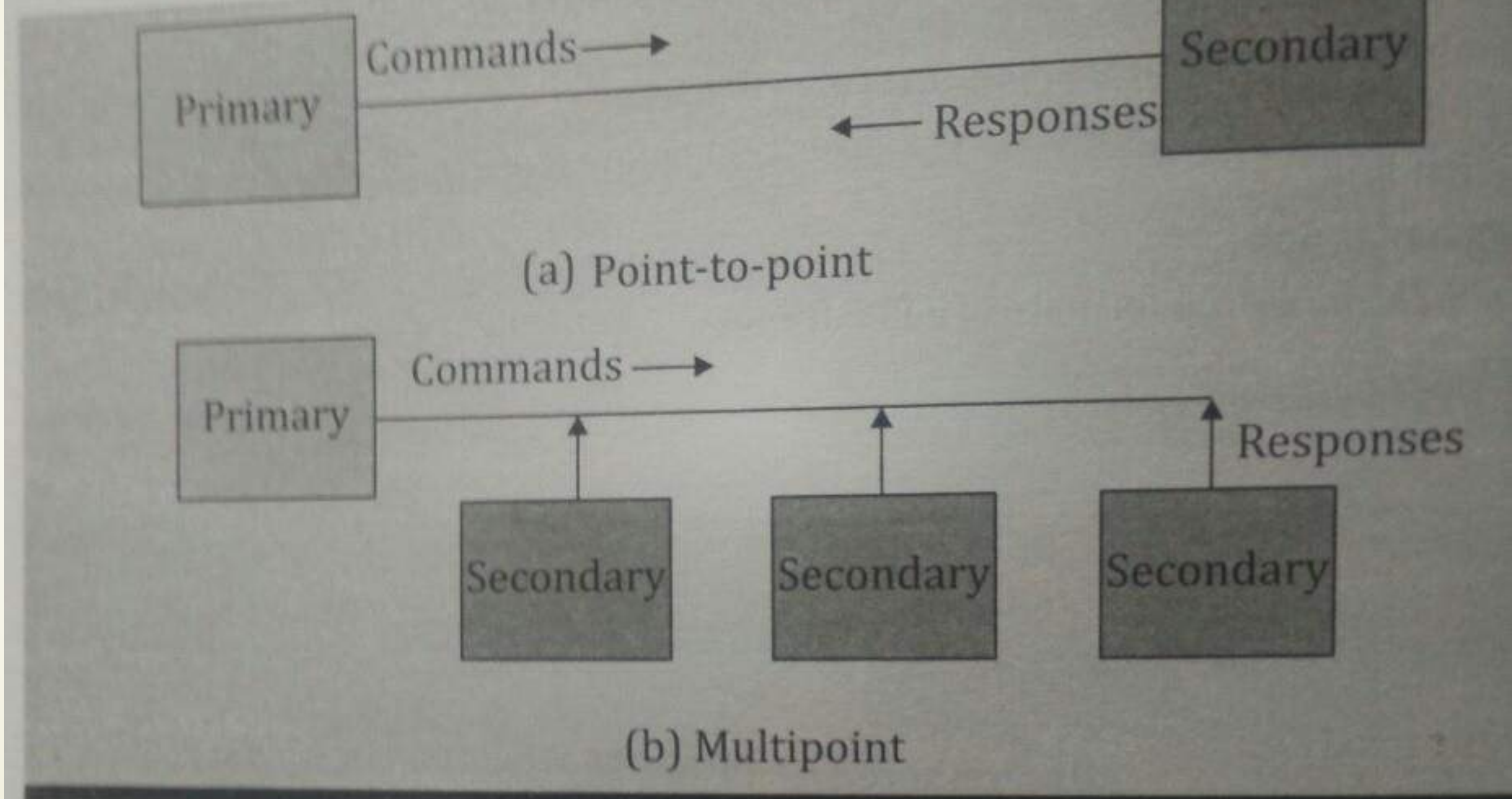


Figure 9.22 HDLC configurations

ABM – Asynchronous Balanced Mode (Balanced)

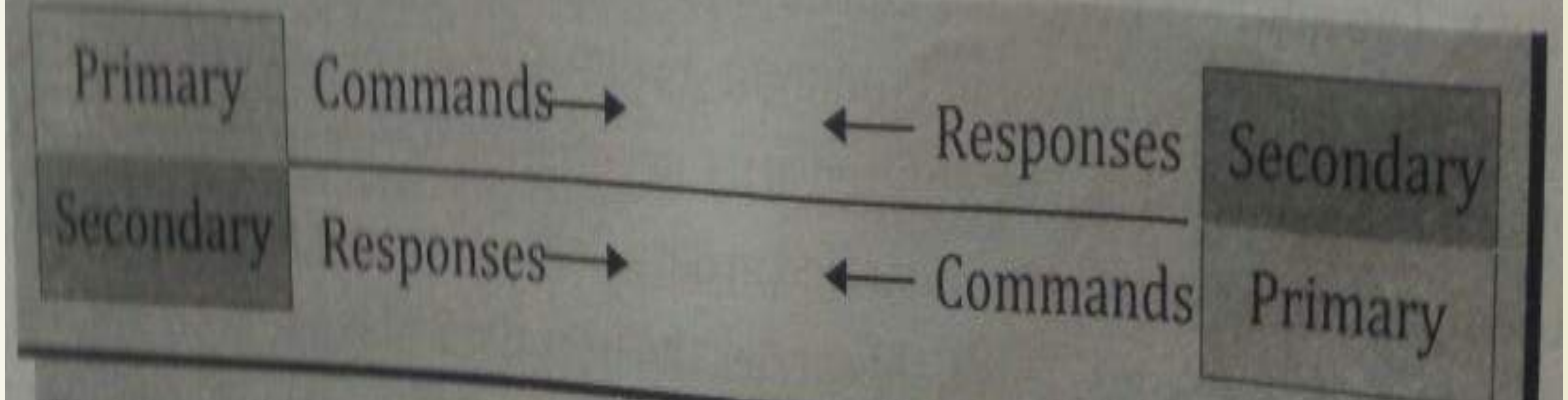


Figure 9.23 Balance point-to-point link between combined stations

HDLC Frame Format

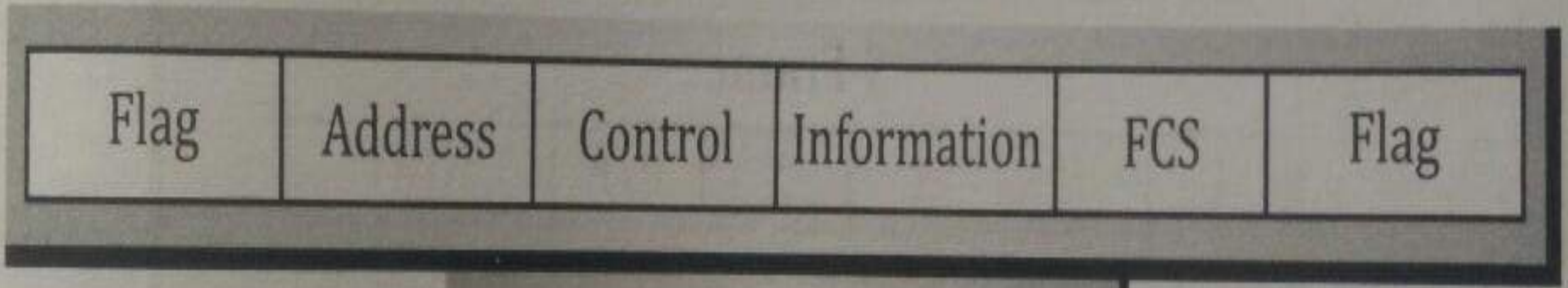


Figure 9.24 HDLC Frame format

HDLC Frame Types

- INFORMATION FRAME: Used to transport data and control information relating to user data.
- SUPERVISORY FRAME: Used only to transport control information
- UNNUMBERED FRAME: Reserved for system management. Eg. For Connection Establishment and Termination.

Control Field

- Information Frame. Value 0
- Supervisor Frame. Value 10.
- Unnumbered Frames. Value 11.
- P – Poll
- F – Final
- M – Specific set of unnumbered bits
- N(S) – Sequence Number
- N(R) – Acknowledgement Number
- S-Frame Control Field has two bits:
- 00 – Receive Ready (RR)
- 01 – Reject (REJ)
- 10 – Receiver Not Ready (RNR)
- 11 – Selective Reject (SREJ)

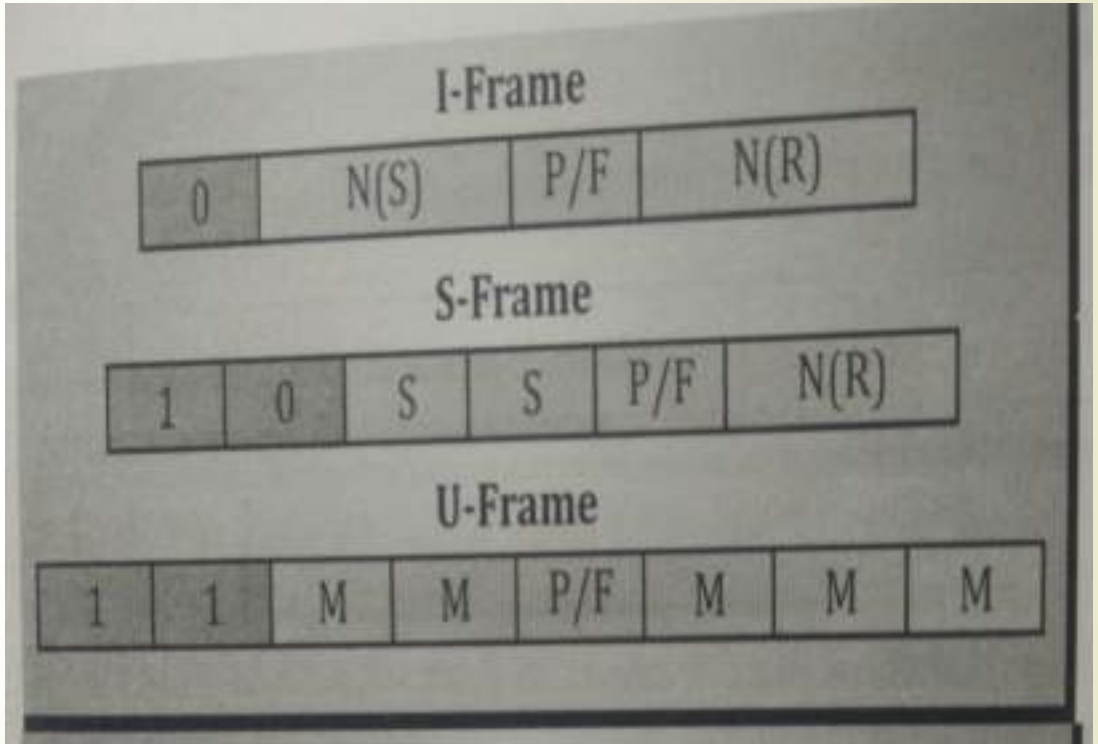


Figure 9.25 Control field format for the definite frame types

STATISTICAL MULTIPLEXING

- A type of Communication Link Sharing
- Here, a communication channel is divided into an arbitrary number of variable bit rate digital channels or data streams.
- Adaptive to instantaneous traffic demands.
- Alternative of TDM and FDM.
- Provides improved link utilization, called statistical multiplexing gain.
- Facilitated through packet mode.
- Each stream is divided into packets that are delivered asynchronously in FCFS – First Come First Served fashion.
- Some scheduling techniques like fair queuing or differentiated QoS.

STATISTICAL MULTIPLEXING

- Supports wireless schemes:
  - Random Frequency Hopping Orthogonal Frequency Division Multiple Access (RFH-OFDMA)
  - Code Division Multiple Access (CDMA).
- Normally imply "On Demand" service rather than "Pre-allocated resources".
- Here, each packet contains complete destination address information.
- Examples:
  - Digital TV Transmission. Channel#=Program ID. Has Constant Length.
  - UDP and TCP Protocols. Channel#=Port#. Variable Length.
  - X.25 and Frame Relay. Channel#=Virtual Connection ID (VCI). Varying Length. Packet Switched Network.
  - ATM – Asynchronous Transfer Mode. Fixed Length. VCI and VPI – Virtual Path Identifier.

Comparison

Statistical Multiplexing

- Fixed (Time Slot) / Variable (data frames) length.
- Frames experience variable delay.
- Bandwidth divided into arbitrary variable number of channels.
- Ensures no slot wastage.
- Performed over Data Link Layer.

Time Division Multiplexing

- Assigned to same recurrent time slot in every TDM Frame.
- Frames experience fixed delay.
- #Channels and Data Rate are fixed.
- TDM can waste slots.
- Performed over Physical Layer.

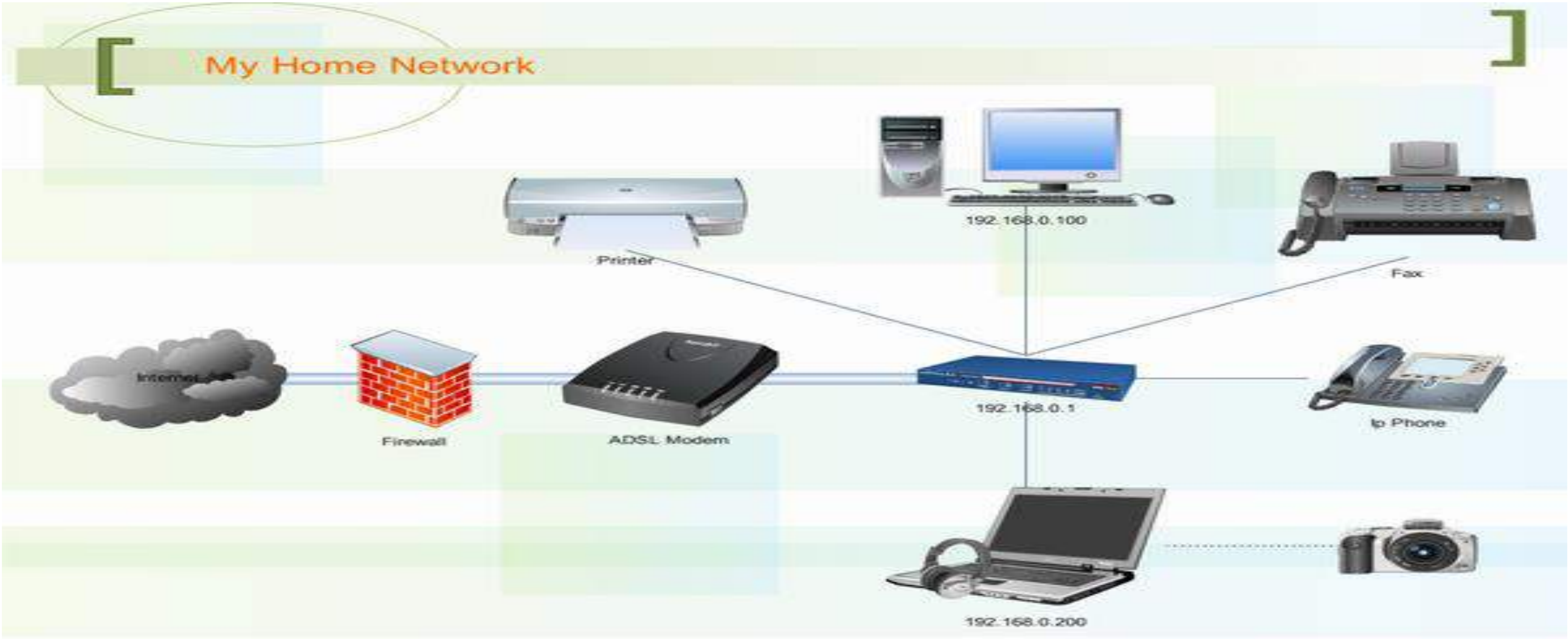
THANK YOU.

UNIT 3 OVER. TOMORROW WE WILL START WITH UNIT 4.

CHAPTER 8:
LAN Standards

DR. BHARGAVI GOSWAMI,
ASSOCIATE PROFESSOR – HEAD,
DEPARTMENT OF COMPUTER SCIENCE,
GARDEN CITY COLLEGE – BANGALORE.

LAN STRUCTURE



NETWORK INTERFACE CARD

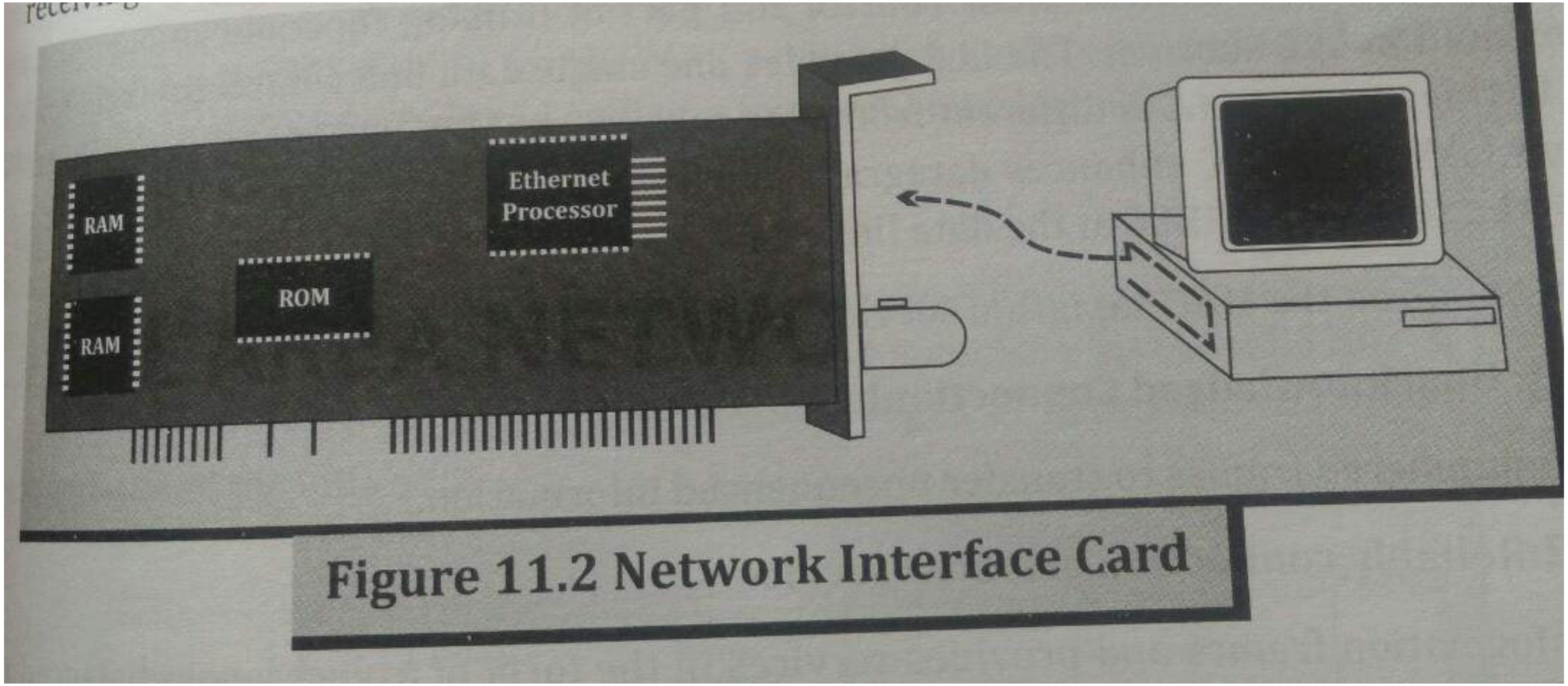


Figure 11.2 Network Interface Card

MEDIUM ACCESS CONTROL SUB LAYER

- DATA LINK LAYER
  - LLC - Logical Link Control
  - MAC - Medium Access Control

LOGICAL LINK CONTROL (LLC)

Unacknowledged Connectionless Service

Reliable Connection Oriented Service

Acknowledged Connectionless Service

802 LAN STANDARDS

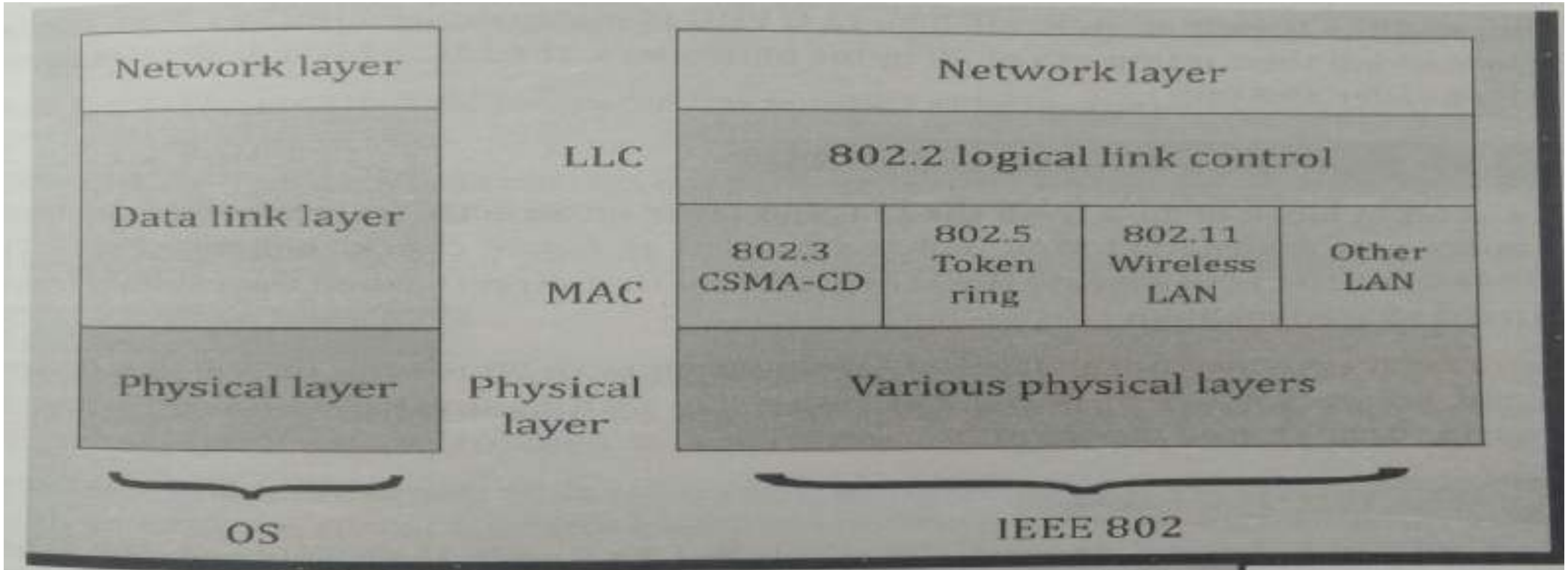
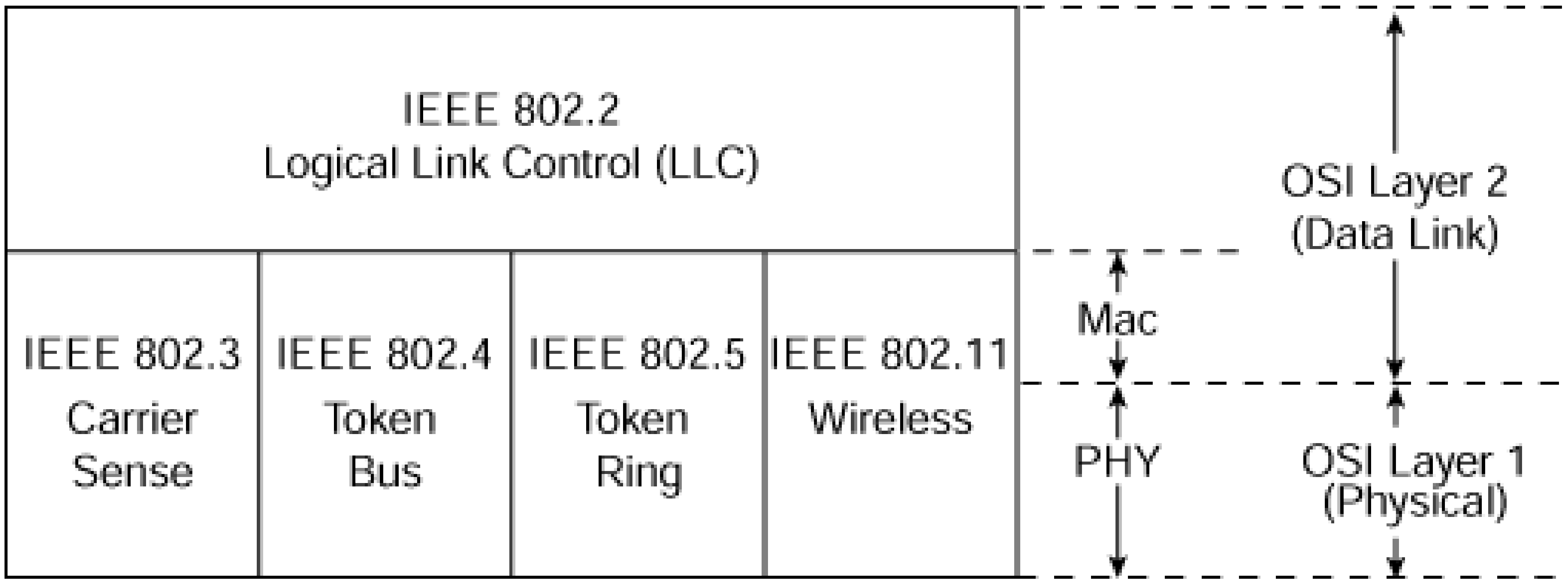


Figure 11.3 IEEE 802 LAN standards

802 LAN STANDARDS



ETHERNET 802 STANDARD

- TOPIC LIST:
- FRAME STRUCTURE
- PHYSICAL LAYER
- TOKEN RING IN STAR TOPOLOGY
- TOKEN FRAME STRUCTURE
- DATA FRAME STRUCTURE

802.3 FRAME STRUCTURE

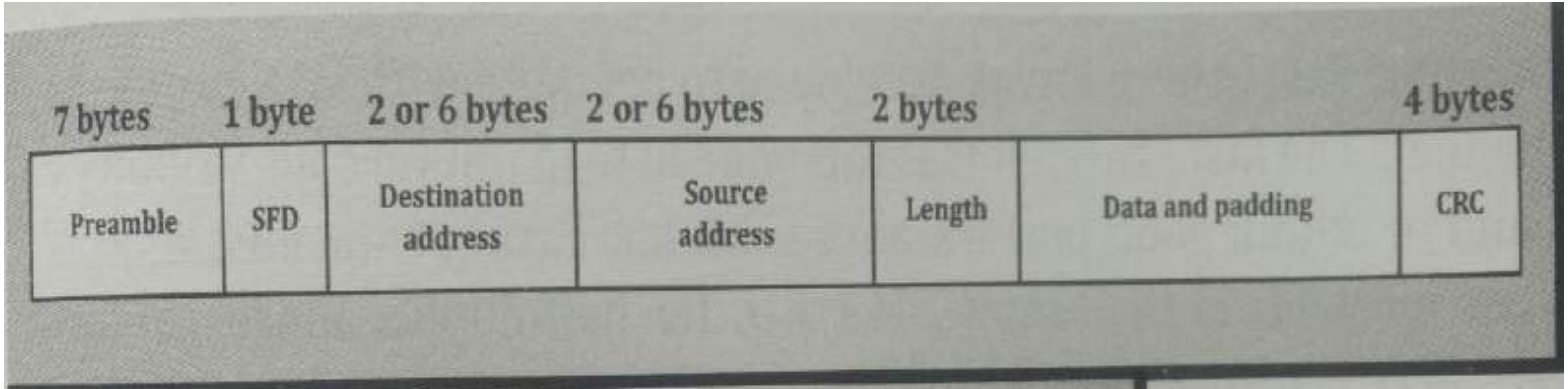
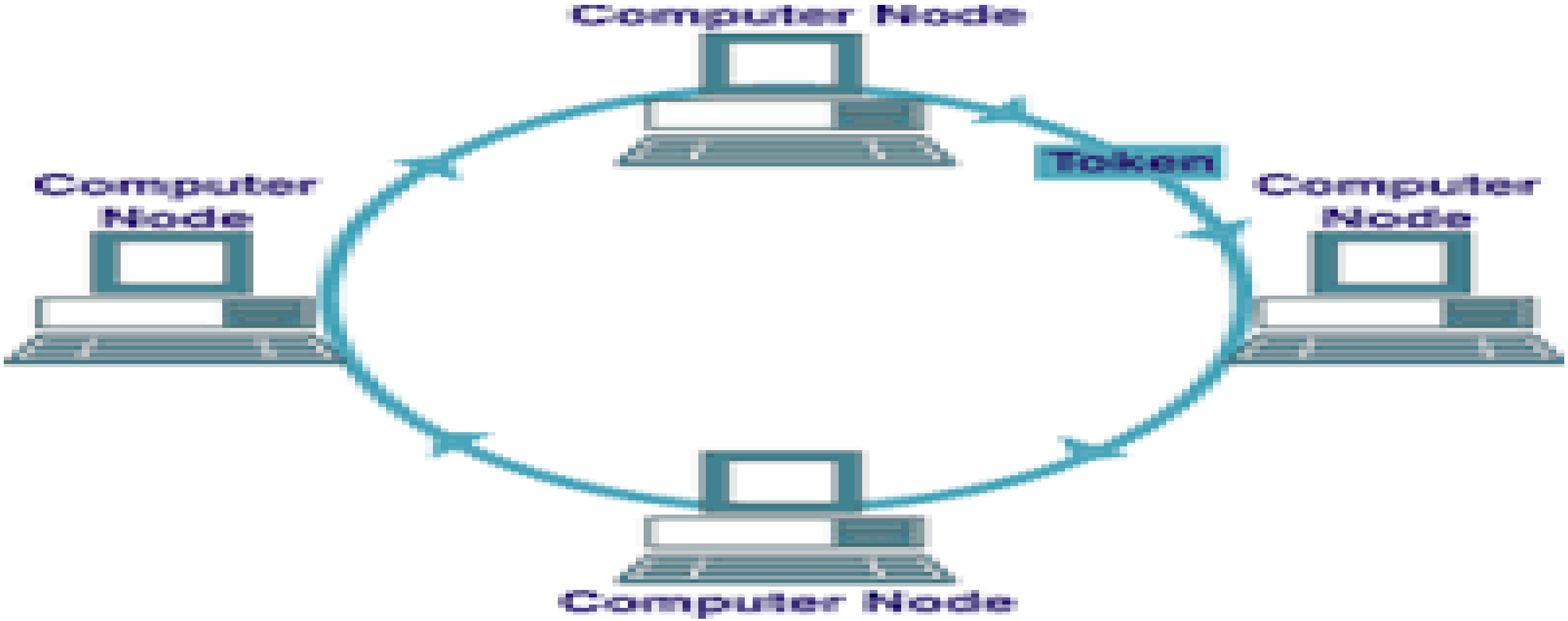


Figure 11.4 IEEE 802.3 MAC Frame Format

PHYSICAL LAYER

SQ. NO.	PROGRESS OF ETHERNET	Data Rate	Distance
1	10Base5: Thick Ethernet	10 Mbps	500 m
2	10Base2: Thin Ethernet	10 Mbps	185 m
3	10BaseT: Twisted Pair Ethernet	10 Mbps	100 m
4	10BaseF: Fiber Ethernet	10 Mbps	2 km
5	Fast Ethernet	100 Mbps	2 km
6	Gigabit Ethernet	1000 Mbps	10 km
7	10 Gigabit Ethernet	10000 Mbps	40 km

TOKEN RING in STAR TOPOLOGY



TOKEN Frame Format: 802.5

SD = Start Delimiter, AC = Access Control, ED = End Delimiter

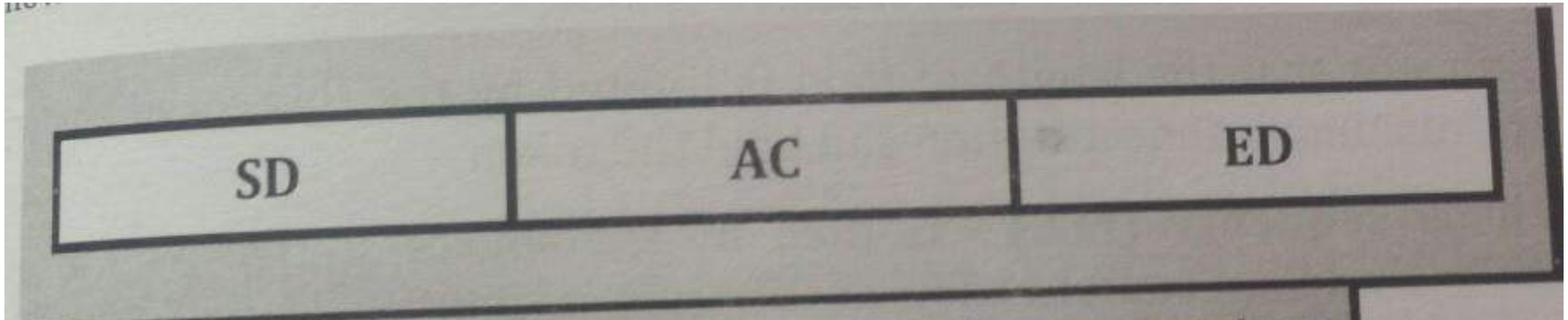
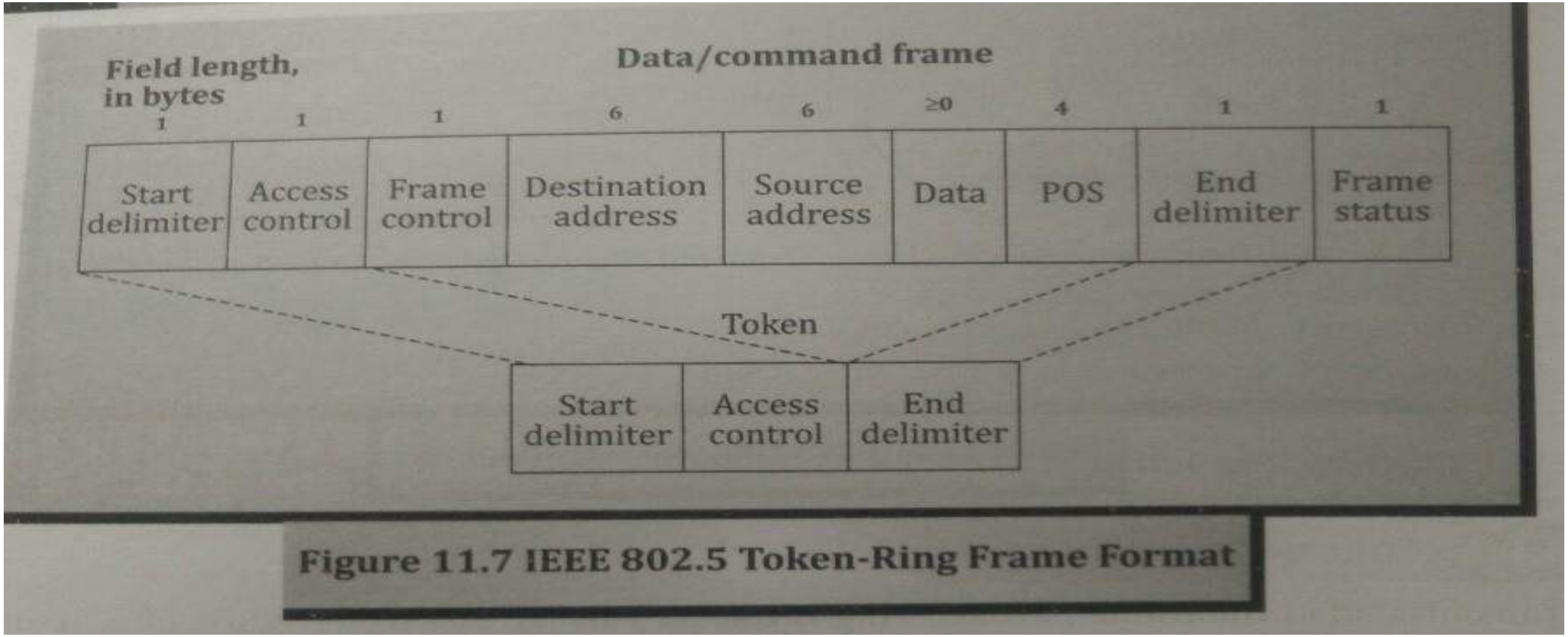


Figure 11.6 IEEE 802.5 Token frame structure

TOKEN-RING Frame Format: IEEE 802.5



FDDI – Fiber Distributed Data Interface

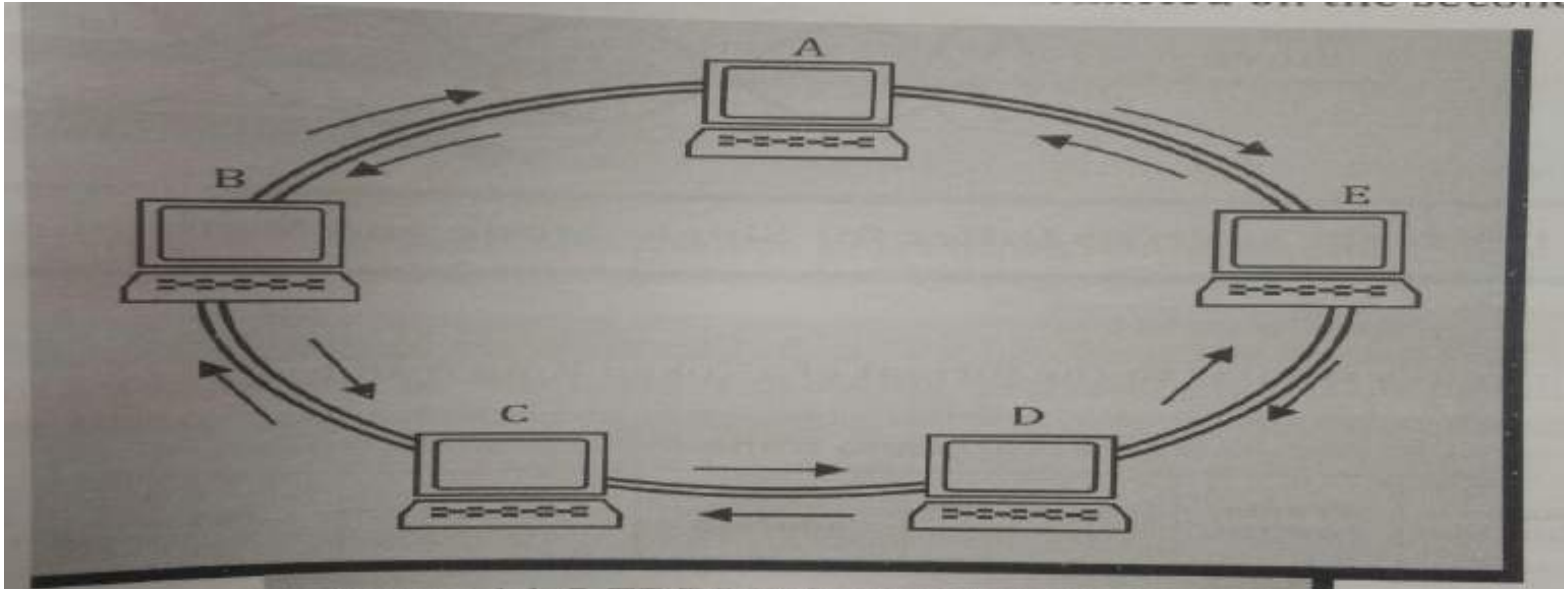


Figure 11.8 FDDI Token-Ring Network

FDDI Transmission Media

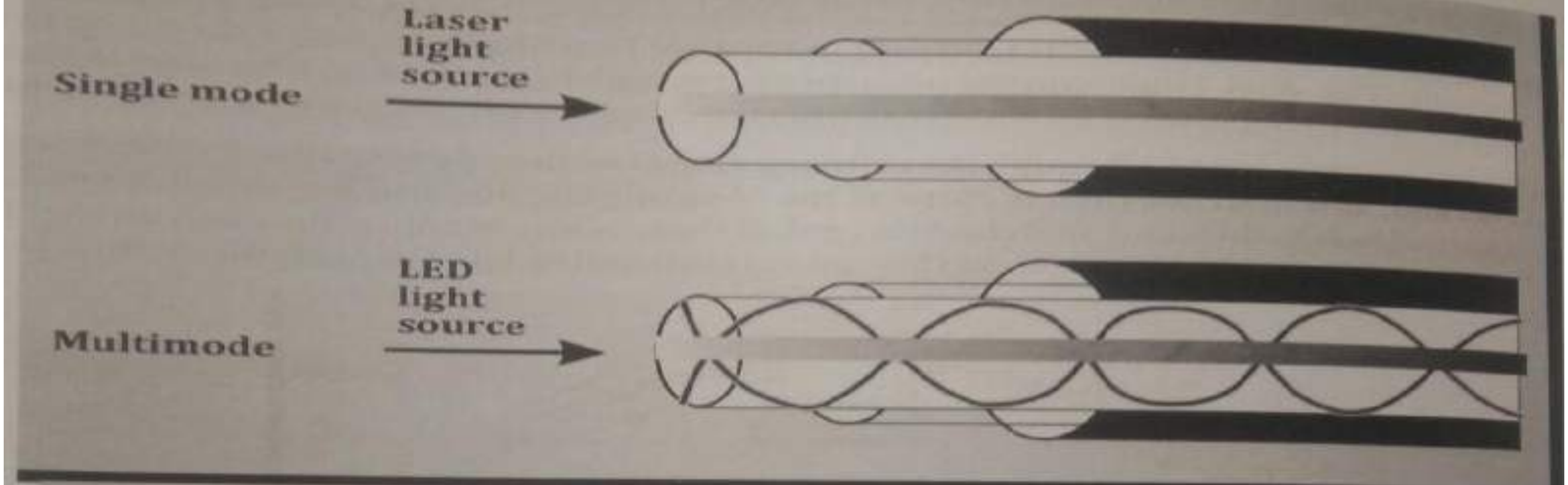


Figure11.9: Light Sources Differ for Single-Mode and Multimode Fibers

FDDI Frame Format

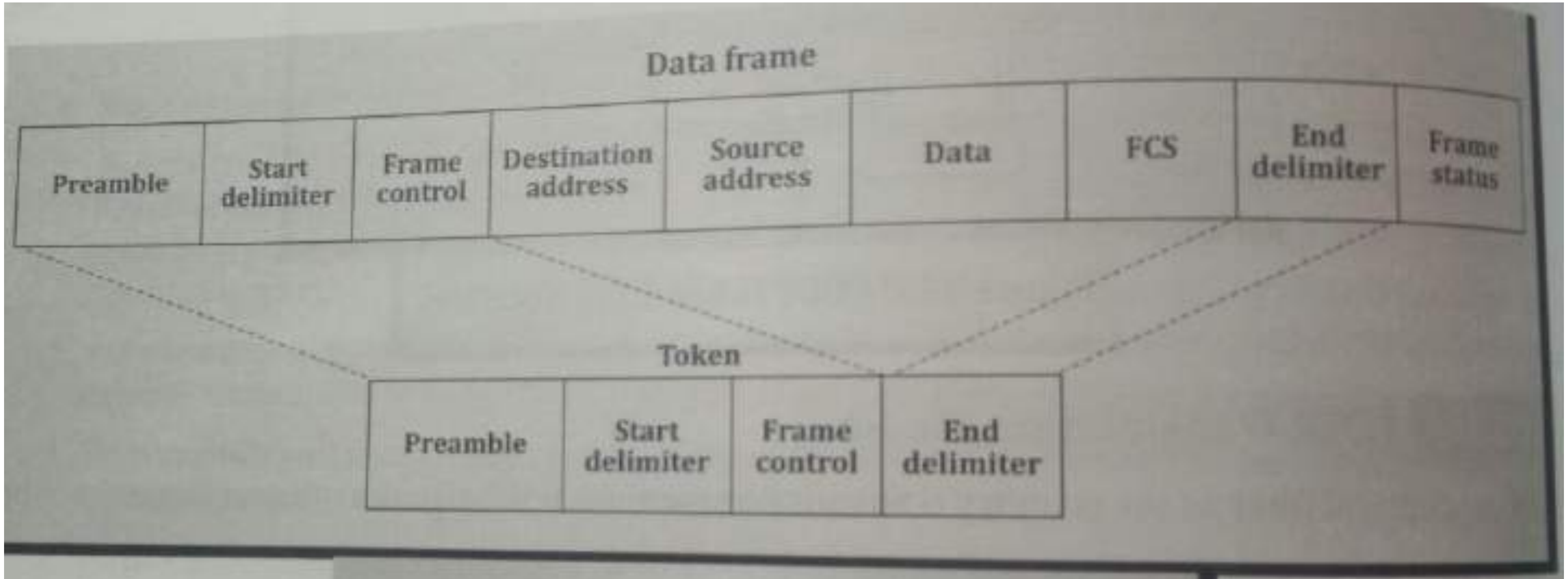
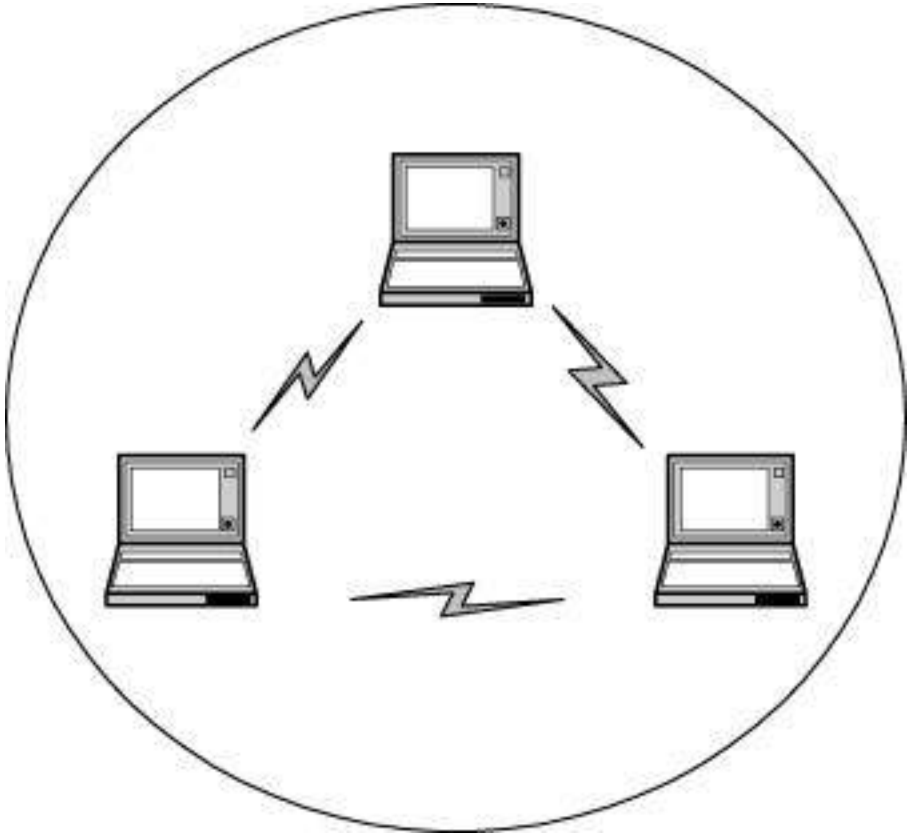


Figure 11.10 IEEE FDDI Frame Format

BSS – Basic Service Set



ESS – Extended Service Set

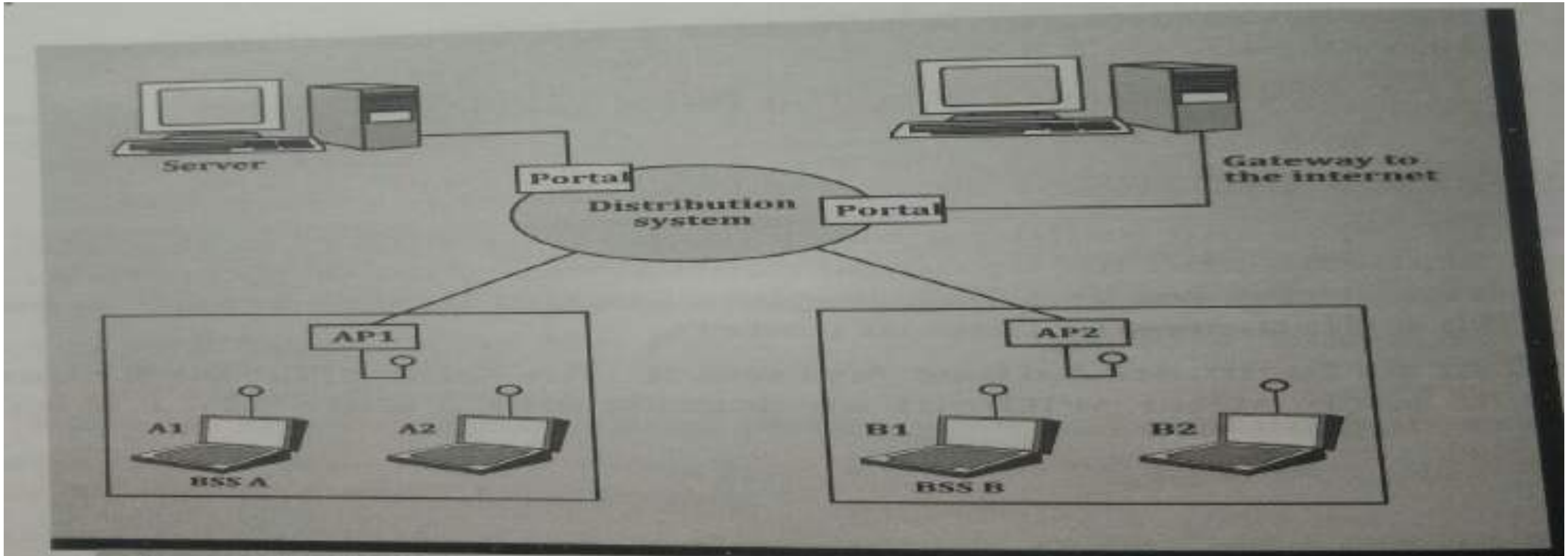


Figure 11.12 Infrastructure network and Extended service set

MAC Architecture

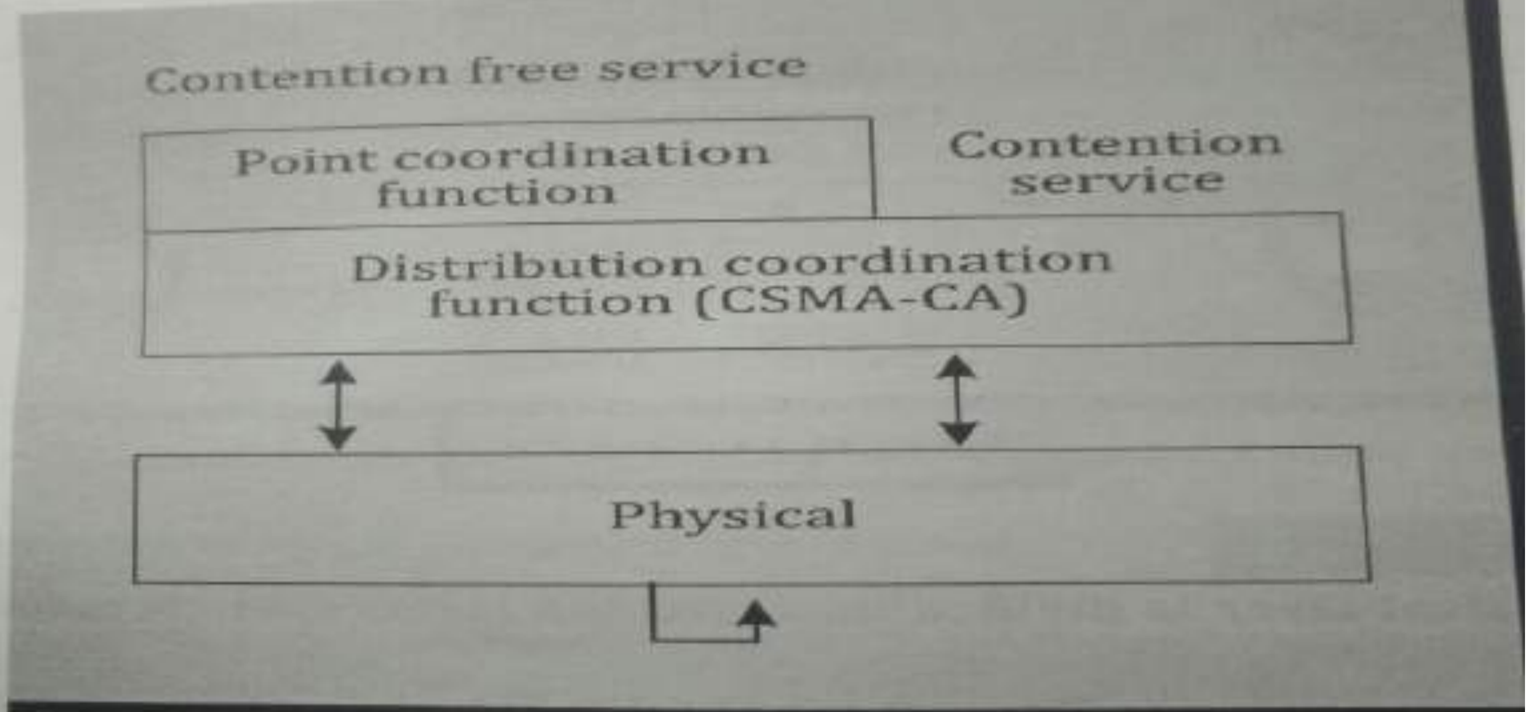


Figure 11.13 IEEE 802.11 MAC Architecture

PCF & DCF Modes

DCF and PCF impose delay but they are the best design to prioritize transmission.

PCF is given higher priority over DCF

Before starting any communication, each user need to wait for SIFS and already communicating parties to complete the communication.

Each ad hoc mode needs to wait for DIFS which is longer than PIFS to let PCF flows complete communication.

Priority from higher to lower goes like this, ACK, CTS, Fragments, then comes PCF and at last comes DCF and then if errors, NACK.

Similarly, SIFS then PIFS, DIFS and then EIFS.

Still there is a chance of collision if at same time two users sends RTS.

DCF (Ad Hoc) mode

Computers communicate directly

No access point control

Compulsory mode

With or without CSMA/CA

Collision invites Binary exponential backoff

Unlike Ethernet, stop and wait is used

Without CSMA/CS uses Fragmentation which are sent when noise is higher

The PCF mode

Access point determines who will send when.

beacon frames for polling each station every few milliseconds announcing SSID and MAC address.

Two modes, Default and protected

Default(unprotected) mode

- Must know the SSID(service set identifier)

Protected Mode

- MAC address
- IP address
- Or both

Data transmitting is always encrypted and SSID is never encrypted.

CSMA/CA, RTS & CTS

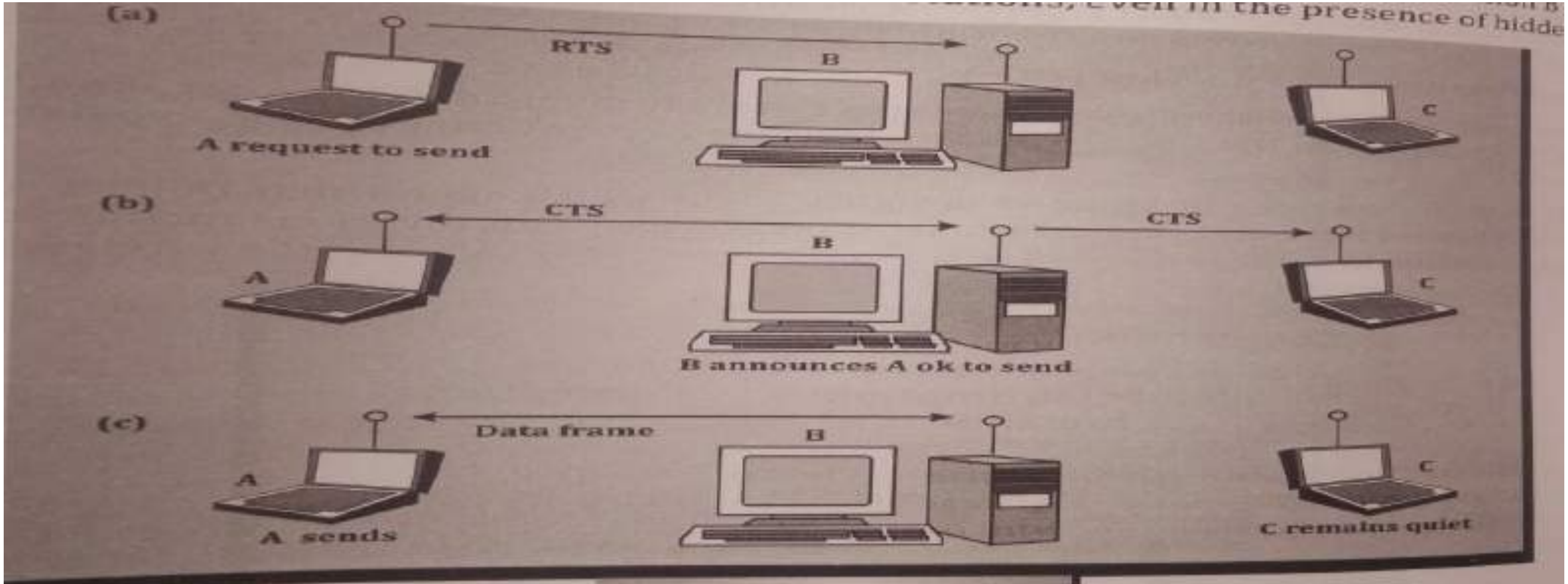
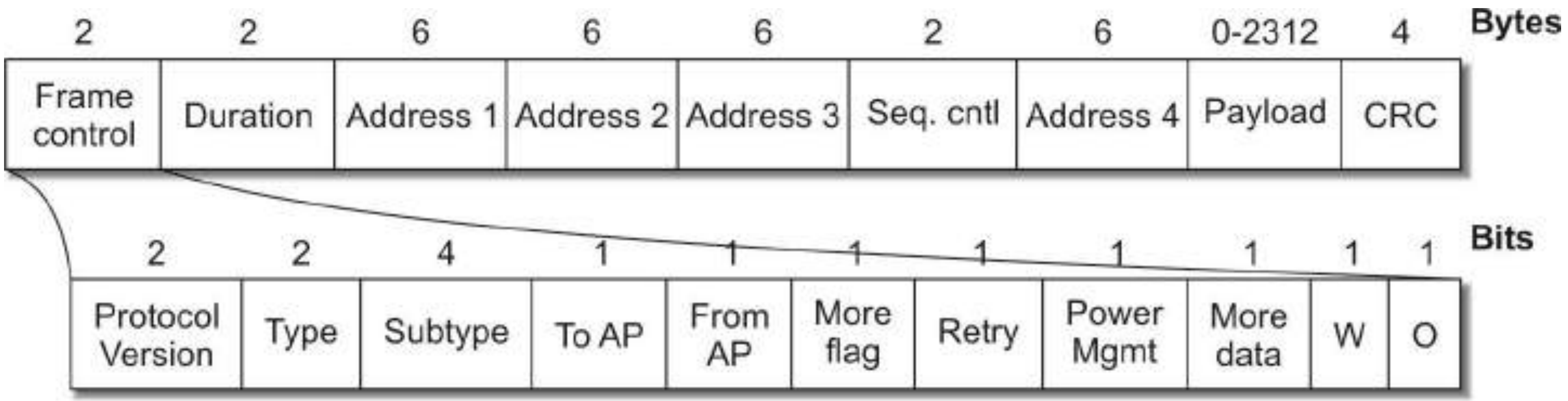


Figure 11.14 CSMA/CA

Physical Layer

- 1. Physical Layer Convergence Procedure (PLCP)
- 2. Physical Medium Dependence (PMD)

802.11 Frame


2
2
6
6
6
2
6
0-2312
4
Bytes
Frame control
Duration
Address 1
Address 2
Address 3
Seq. cntl
Address 4
Payload
CRC
2
2
4
1
1
1
1
1
1
1
1
Bits
Protocol Version
Type
Subtype
To AP
From AP
More flag
Retry
Power Mgmt
More data
W
O

802.11 Frame

Duration: RTS, CTS an NAV process based on this duration observation.

DSS, BSS and 4 Address Fields:

- Wireless area having 1 access point is called cell or BSS (Basic Service Set).
- There is a need of interconnection between two cells (AP) for forwarding packets if not in range.
- This network becomes distributed and denotes DSS (Distributed Service Set).
- We need 4 addresses here to manage inter-cell and intra-cell transmission.
- Issue here: conversion of wired to wireless and wireless to wired frames.

Sequence: Sq no. Is allocated to individual frame and fragment.

Payload: carries network layer data like IP datagram, max size is 2312 but usually kept 1500 for compatibility with ethernet.

CRC: most important in wireless medium as error rate is very high, same method as Ethernet.

Frame Control:

Two bytes (16 bits) length

Protocol version, current 0.

Type of Frame: 1st Control, 2nd Management and 3rd Data.

Subtypes:

Control types : RTS, CTS, ACK.

Management types: beacon, authentication, de-authentication, association, dis association, re association, etc.

Data: Data.

To AP and From AP: where the frame is coming and going. Used for inter and intra cell communication.

More flag: indicates More Fragments expected in DCF mode.

Retry: To eliminate duplication, frame indicates that this frame is sent again.

Power Management: wireless transmission handles battery low situation. After completion of transmission, device enters into power save or sleep mode.

More Data: indicates if current transmission is over or not.

W: whether WEP (Wired Equivalence Privacy) is implemented or not.

O: indicates whether frames are to be processed in ORDER or not.

Wireless LANs, IEEE 802.11 Standard

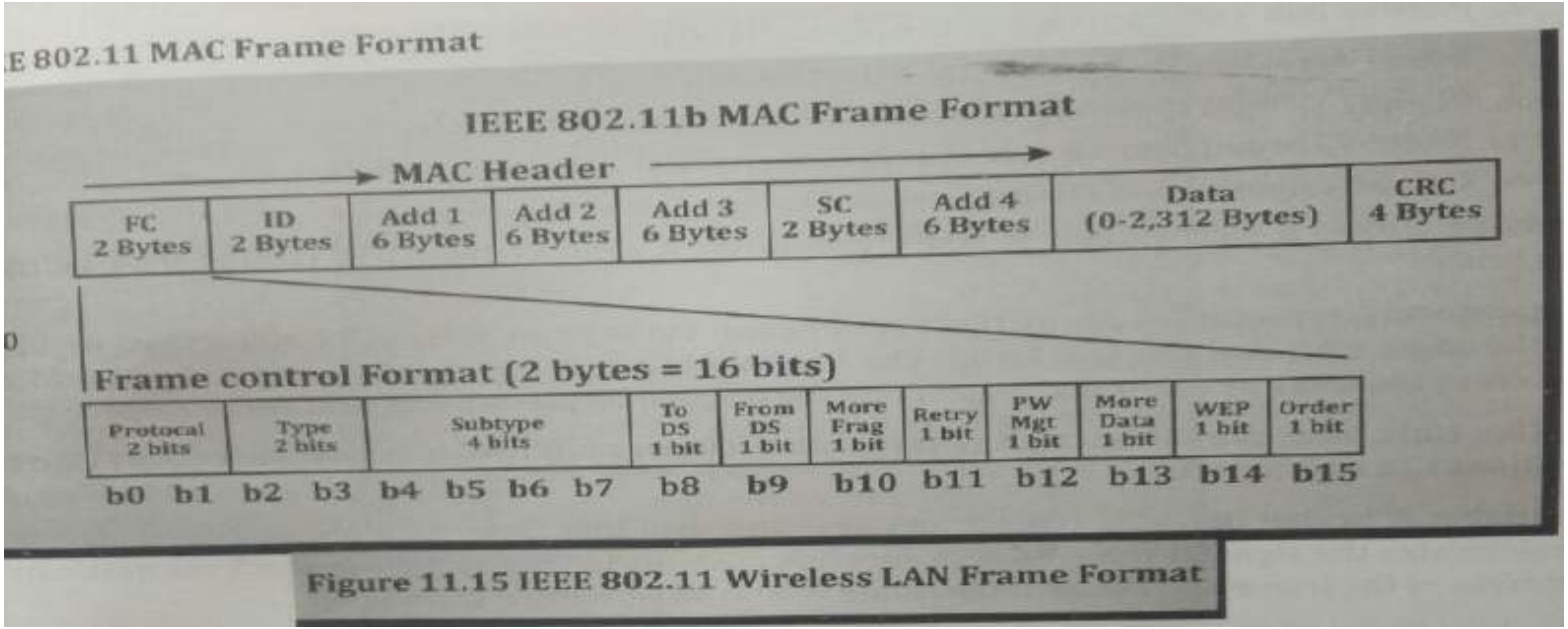


Figure 11.15 IEEE 802.11 Wireless LAN Frame Format

BRIDGE

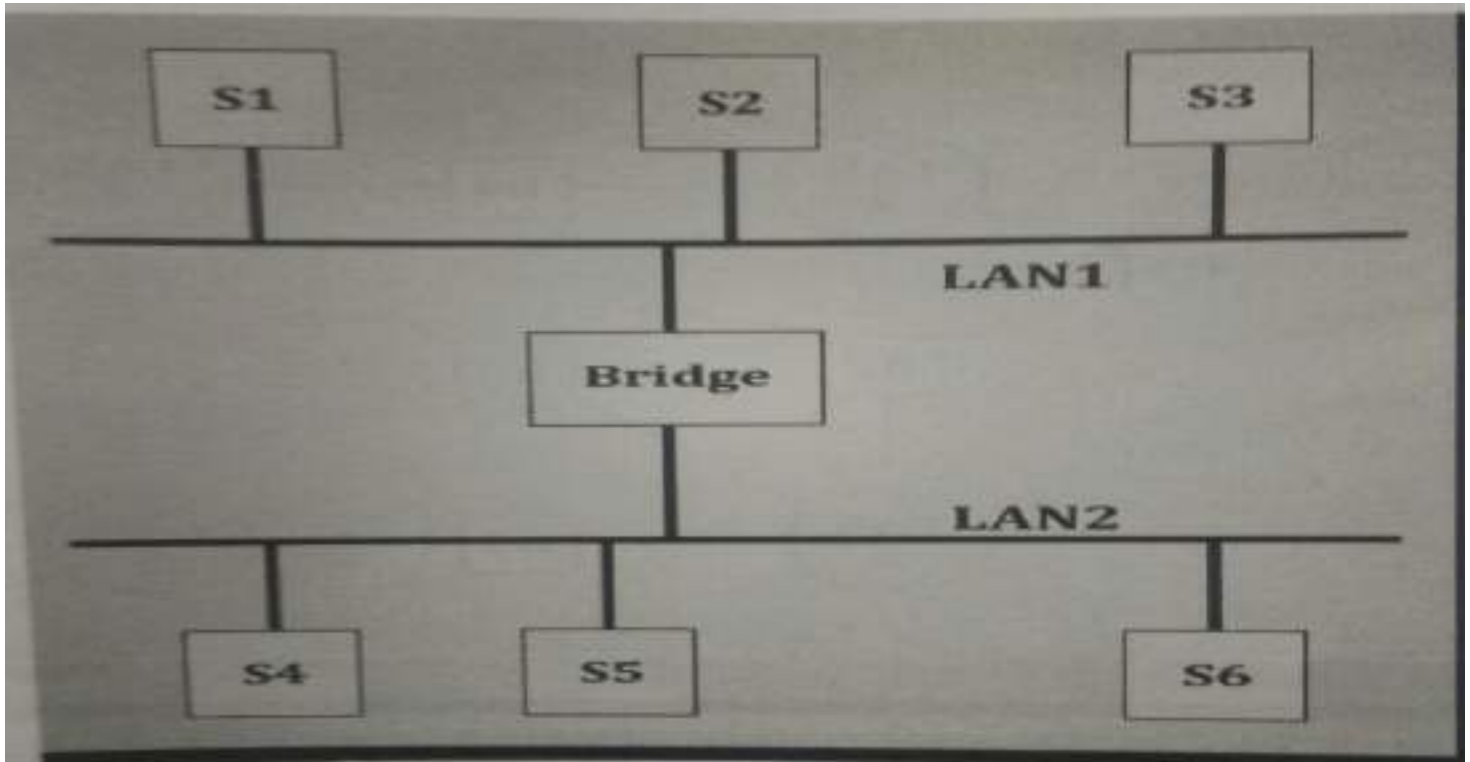
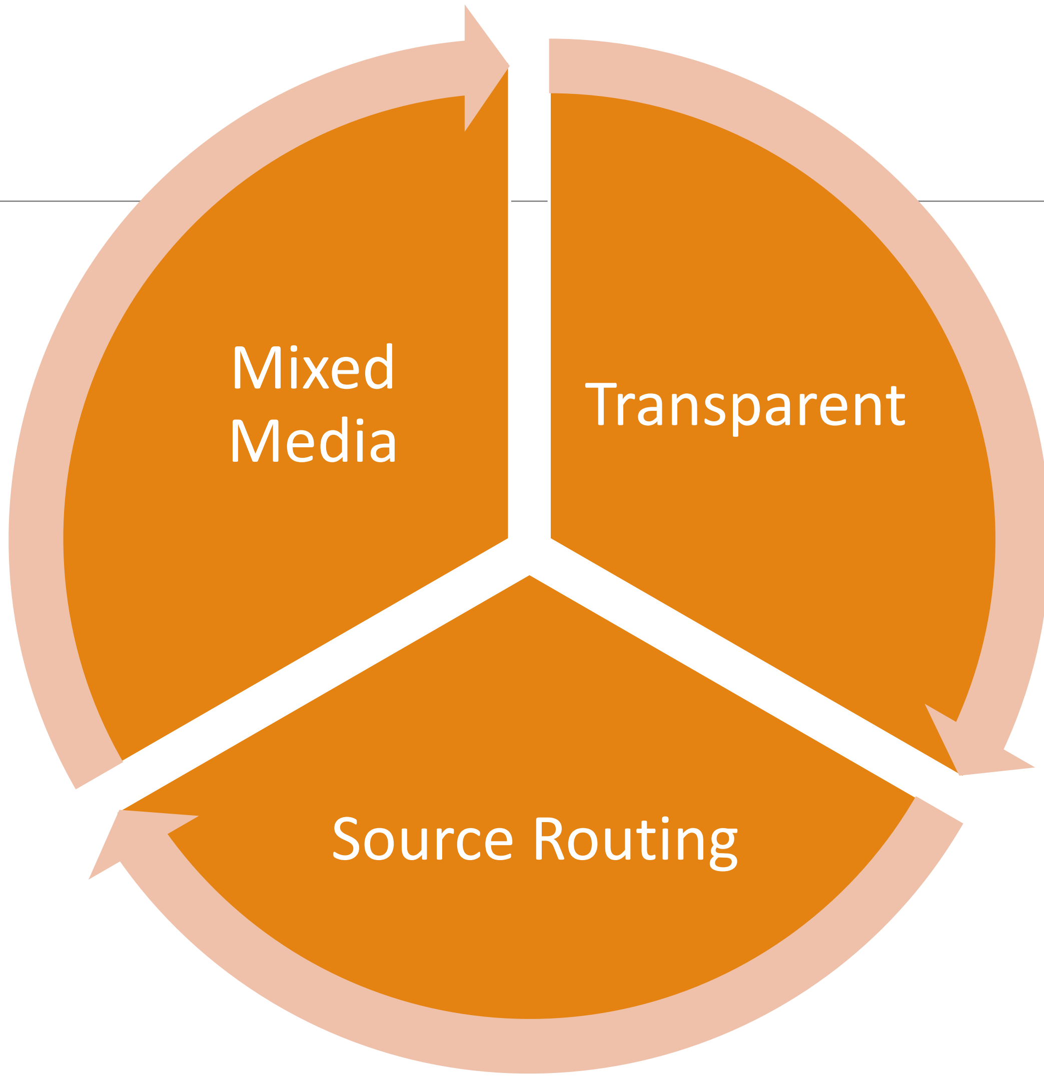


Figure 11.16 A bridged LAN

Types of Bridge



Transparent Bridge

Stations are unaware of the presence of bridge.

So, reconfiguration of stations in not required when bridge enters or leaves.

Three basic function:

1) Forward frames from one LAN to another.

2) Learns where stations are attached to LAN

3) Prevents loops in topology.

Source Routing Bridge

Primarily used for connecting Token Ring Networks.

Unlike transparent bridge, it keeps functions for end stations to perform.

Includes route information in header of frame.

Finds good routes efficiently.

Check next figure for example.

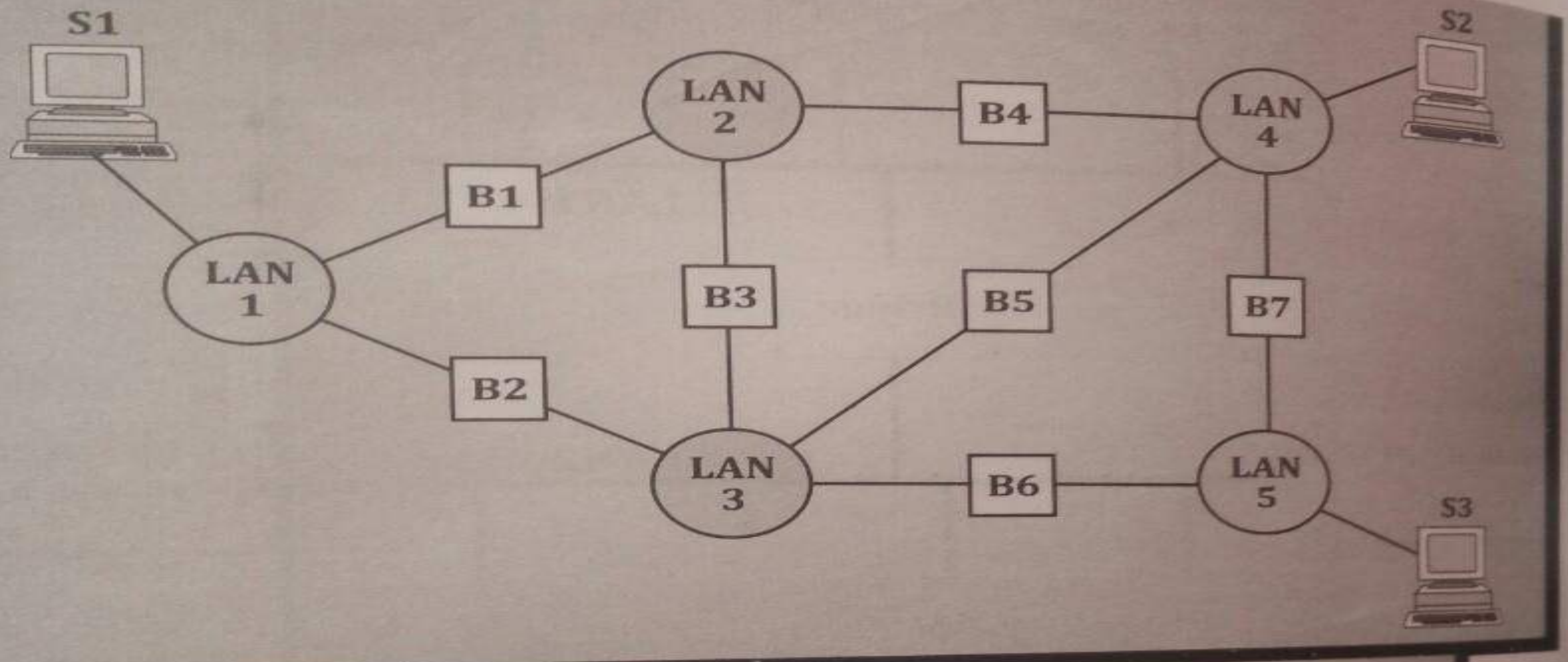


Figure 11.17 LAN interconnection with source routing bridges

... are referred

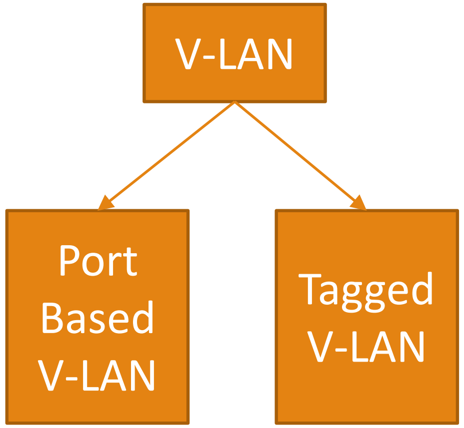
Mixed Media Bridge

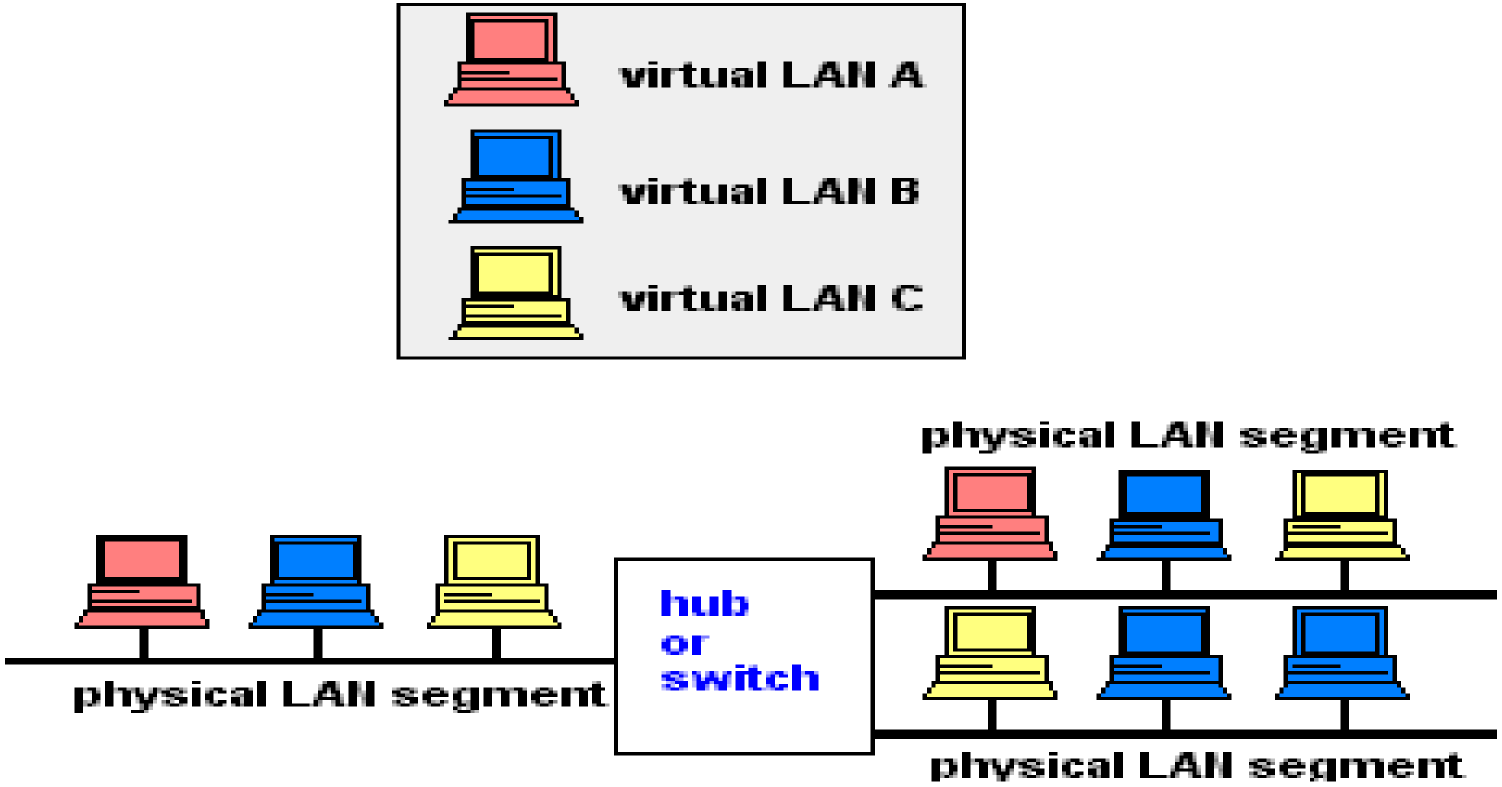
Interconnects LAN of different types.

Its not simple. Eg. Ethernet connecting to Token Ring.

Different frame structures, speed, operations, etc needs to be resolved and sync is performed.

VIRTUAL LAN


V-LAN
Port Based V-LAN
Tagged V-LAN


virtual LAN A
virtual LAN B
virtual LAN C
physical LAN segment
hub or switch
physical LAN segment
physical LAN segment

THANK YOU. KEEP HEALTHY, YOU NEED TO STUDY HARD AS YOUR EXAMS ARE .

LAST CHAPTER WILL START FROM NEXT LECTURE.

CHAPTER 9: PACKET SWITCHING N/W & CONGESTION CONTROL

Dr. Bhargavi Goswami,
Associate Professor – head,
Department of Computer Science,
Garden City College – Bangalore.

PACKET SWITCHED NETWORKS

Transfer blocks of information called packets.

Packets are the connectivity between two users for communication.

Two perspectives:

1) External View: Related to service provided to transport layer.

2) Internal View: Concerned with Topology, links, switches and routers.

Two approaches:

1) Virtual Circuits

2) Datagrams

ROUTING AND FORWARDING

Routing is

- to know about other routers
- where each of them is located
- which networks they are connected to

Forwarding is

- finding out one's own neighboring routers
- forward a specified packet to its nearest neighbor to make it reach to a given destination

ROUTING AND FORWARDING

Routing table contains information about nearest router for given destination

Routing algorithms decide placement of routers

Virtual circuit is mechanism used for connection oriented forwarding

Datagrams are units of data sent in connectionless forwarding

NETWORK LAYER DUTIES

Handling accounting for usage of network resources

Devise and implement mechanisms of identifying each machine uniquely

Implement connectionless or connection-oriented forwarding

Multiplexing and demultiplexing the transport layer and the data link layer jobs

Routing & Forwarding

Scheduling & Quality of Service

Handle Addressing

TWO DIFFERENT TYPES OF ROUTING

Collection of networks organized by a single party is known as an *autonomous system* (AS)

Exterior routing is across AS

- BGP (Border Gateway Protocol)

Interior routing is within AS

- Distance Vector
- Link state
- AODV

REQUIREMENTS/GOALS OF A GOOD ROUTING ALGORITHMS

Packets continuously forwards them to their destinations in minimum possible time.

Impartial to all the nodes.

Simple enough to be implemented

Should not oscillate frequently to make packet forwarding erratic.

Good path to receiver is recorded.

Fault tolerance: Must continue functioning irrespective of nodes and links going up and down.

Must not be bogged by increasing or decreasing number of nodes.

Fast enough to reflect changes in network topology in real time.

Speed is maintained.

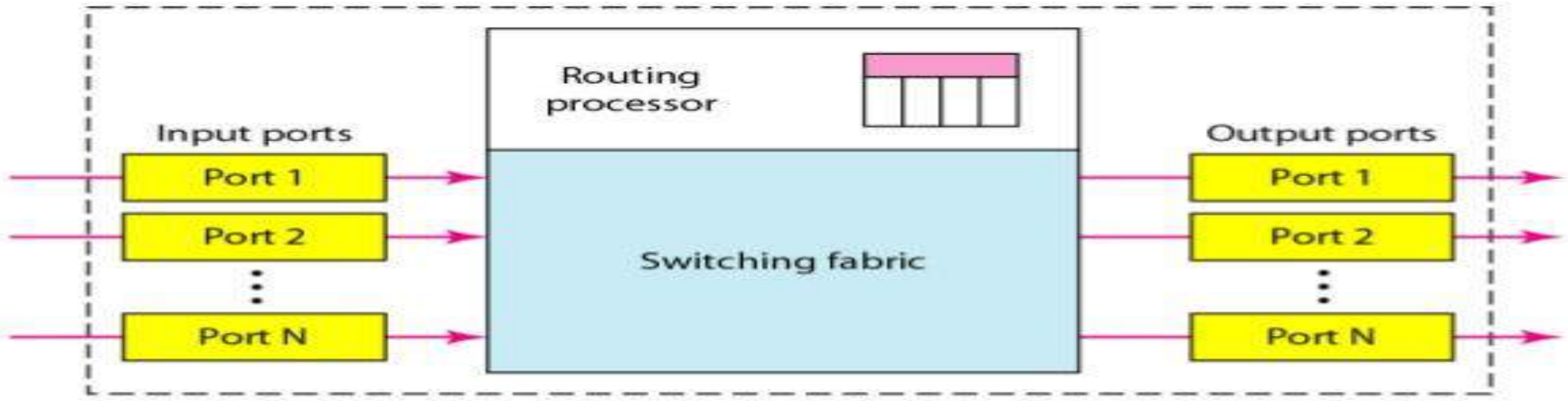
Other requirements:

- *Dynamism and flexibility*
- *Performance*
- Robustness

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

STRUCTURE OF PACKET SWITCH

Packet switch components



8.35

STRUCTURE OF PACKET SWITCH

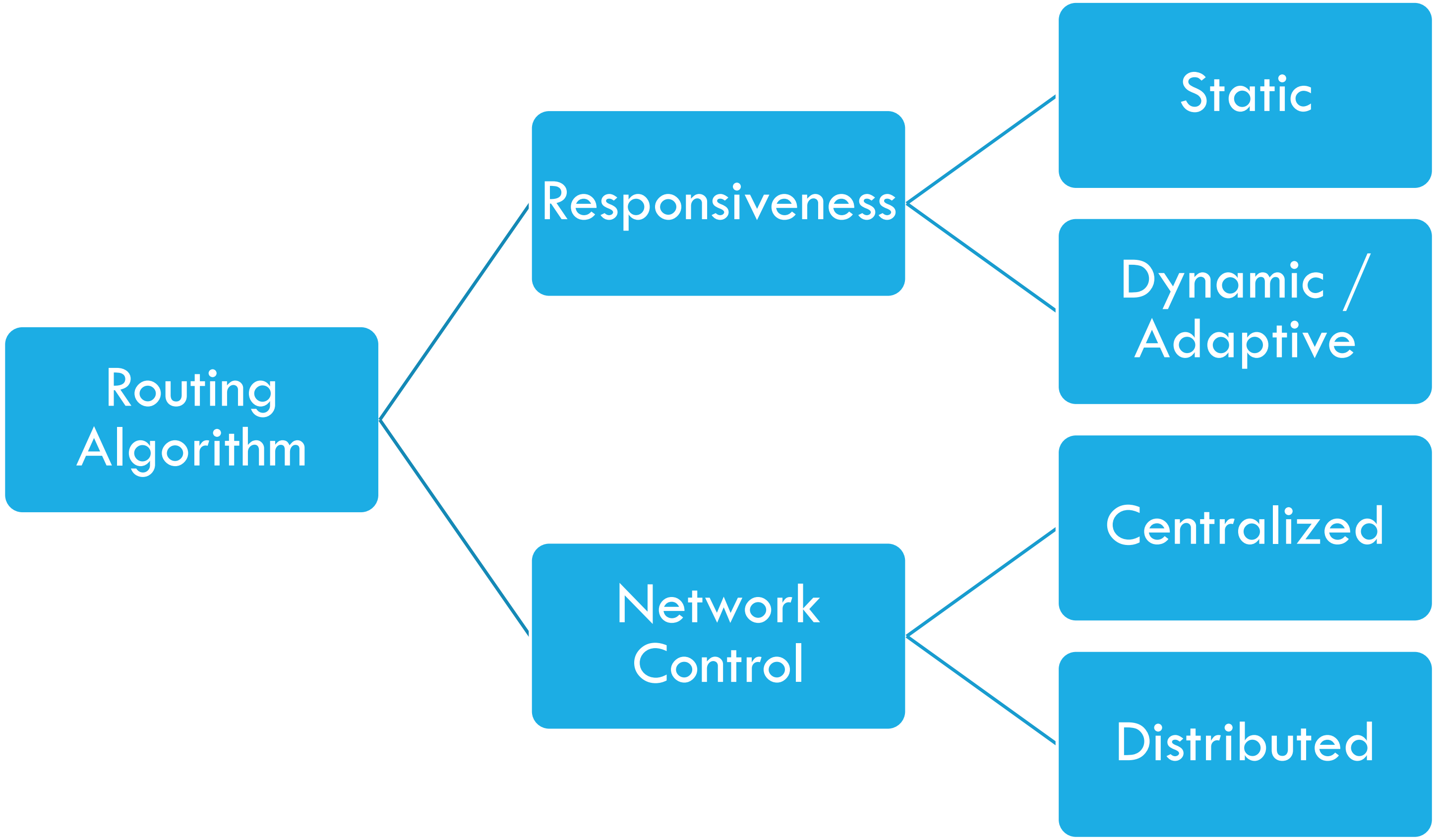
Input & Output Ports: They are generally connected.

Line Card: Made up of various chipsets. Performs task such as lookup and scheduling. Has several input output ports. High speed link assures complete utilization of line. Implements network layer functions. Does jobs like timing, line coding, framing, error checking, addressing, etc. Handles broadcast networks. Has routing tables. Lookup is performed to search through the tables. Also has buffers for queuing.

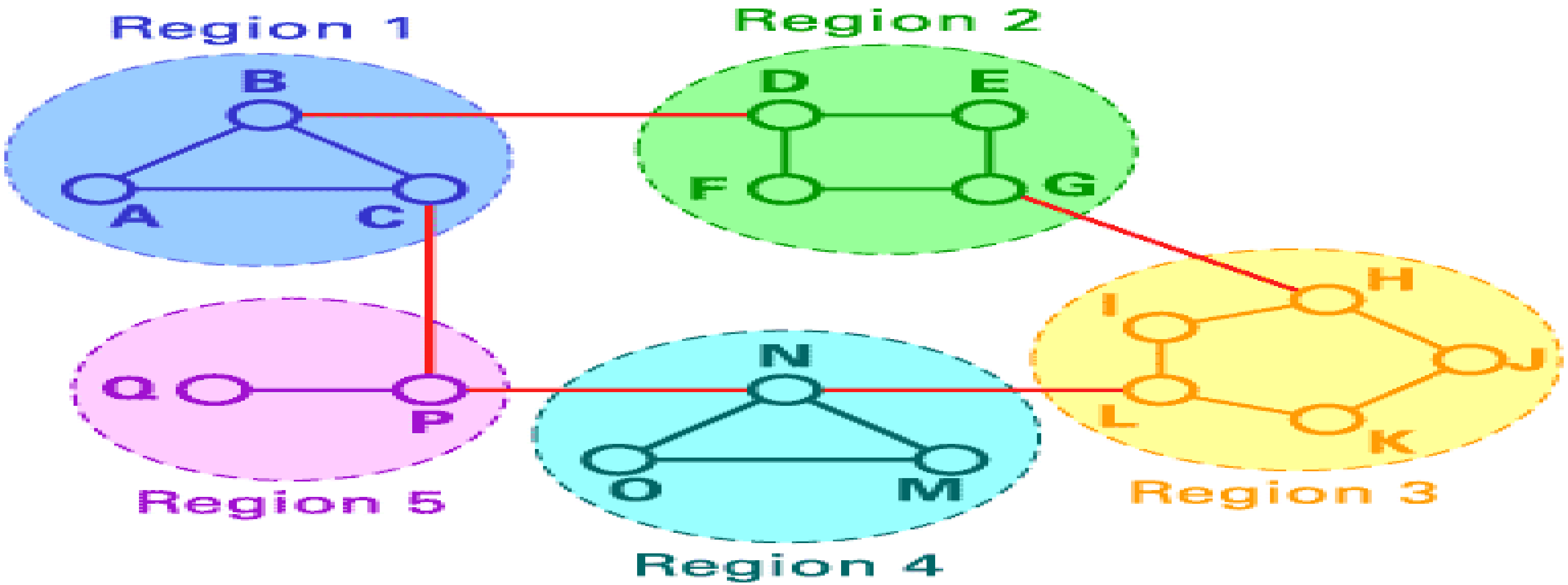
Controller: Contains general purpose processors for control and management functions. Executes routing protocols. Communicates with line cards & interconnected fabrics. Acts as central coordinator.

Interconnection Fabric: It transfers packets between line cards. It may get bottleneck because of presence of multiple high speed line cards. Types: 1)Bus 2) Cross Bar

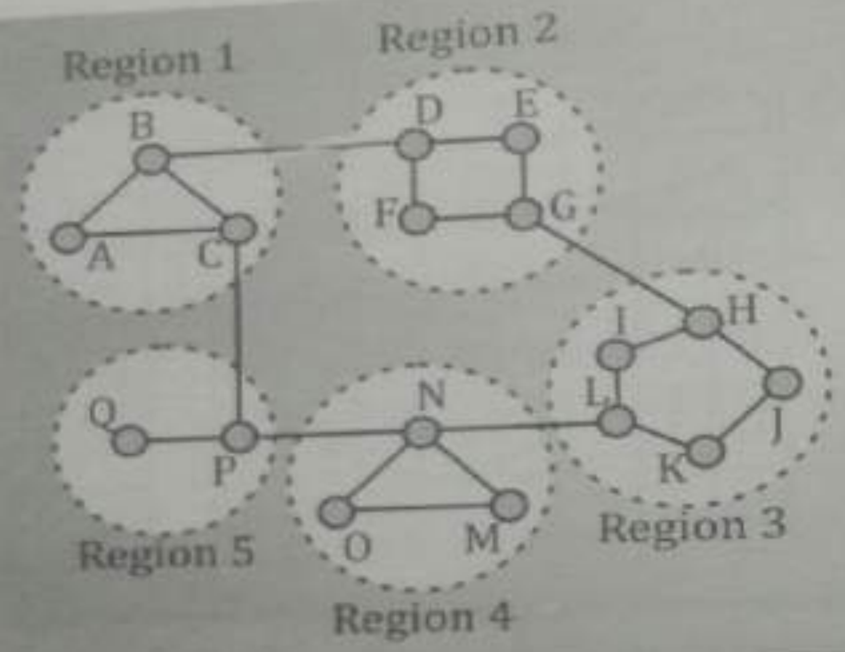
CLASSIFICATION OF ROUTING ALGORITHM



HIERARCHICAL ROUTING



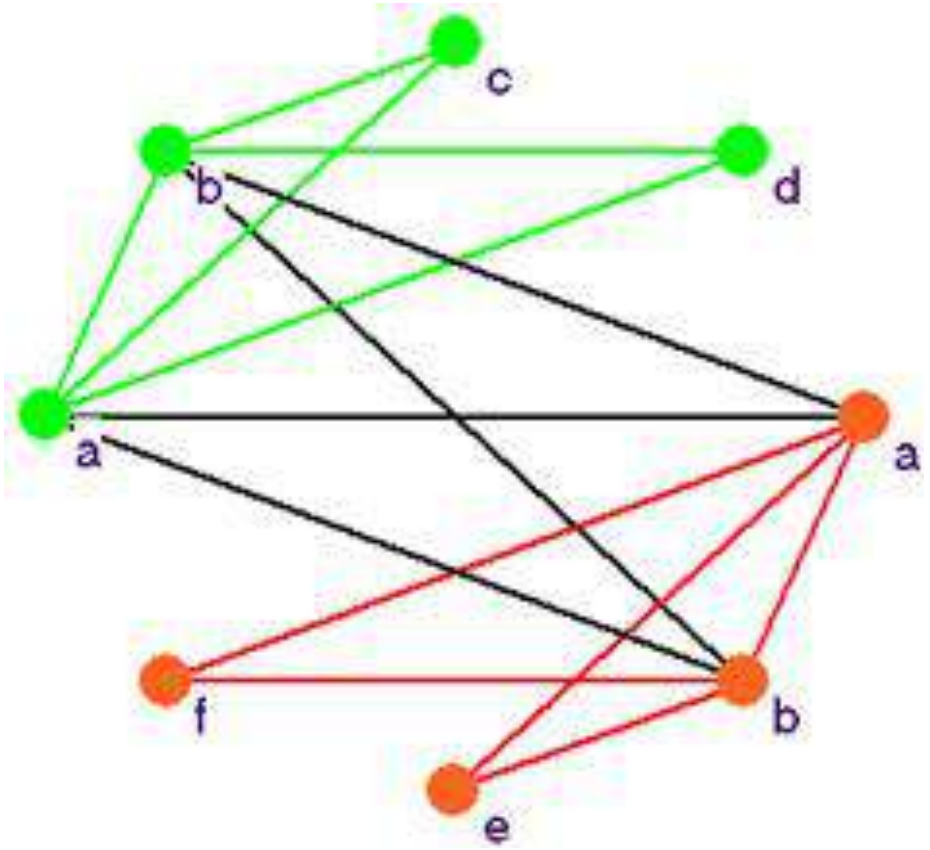
HIERARCHICAL ROUTING



Destination	Line	Weight
A	---	---
B	B	1
C	C	1
Region 2	B	2
Region 3	C	2
Region 4	C	3
Region 5	C	4

Figure 12.17 Hierarchical routing

FLOODING



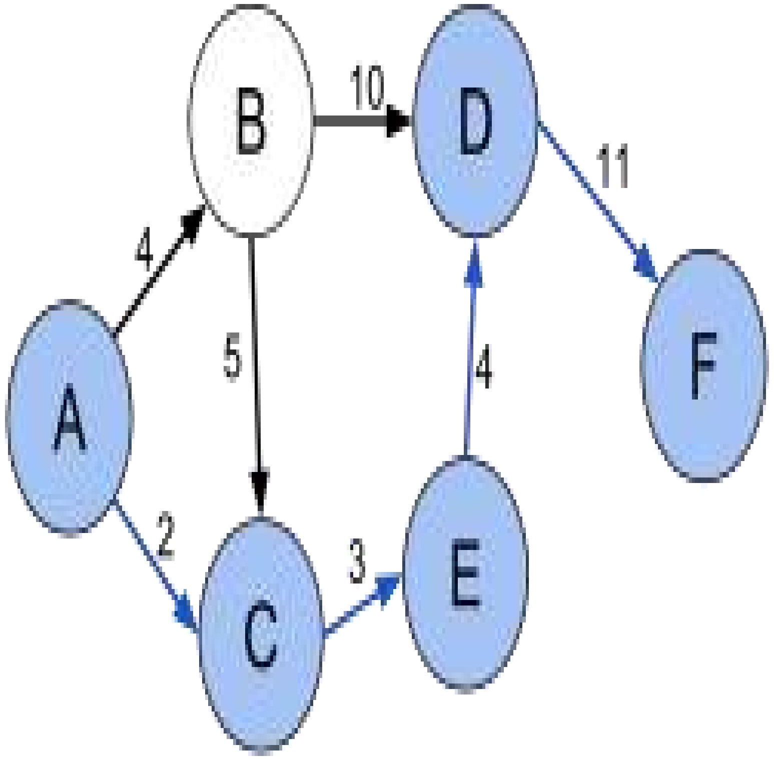
Incoming packet is forwarded to all the ports other than the one it is received from.

Useful when routing path to destination does not exist.

Generates exponential growth rate and unnecessary network traffic and load.

As a solution we can implement TTL-Time to Live, Loop avoidance & Sequence#.

SHORTEST PATH ROUTING



To reach from A to F, shortest path is selected.

A – C

A – C – E

A – C – E – D

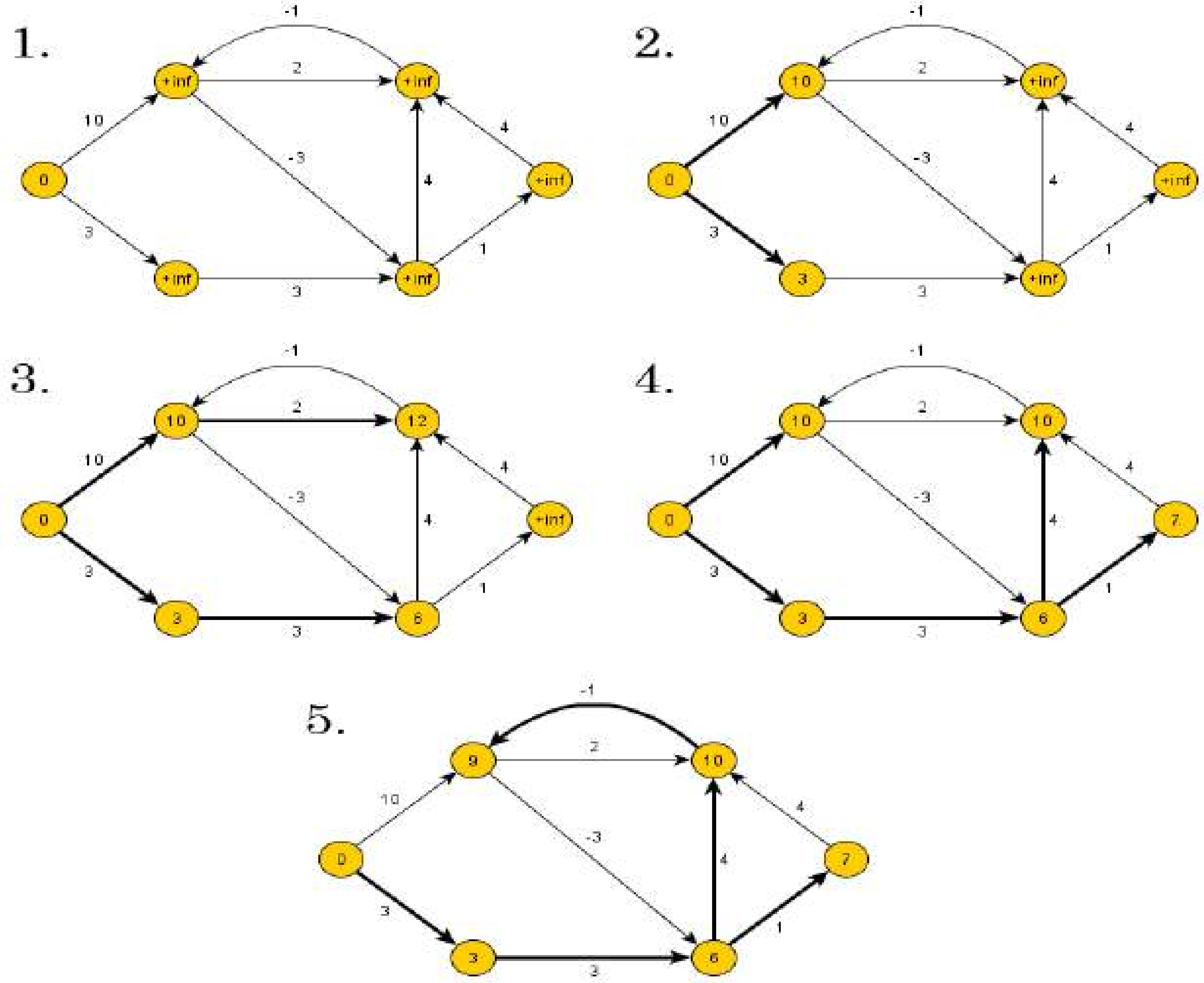
A – C – E – D - F

BELLMAN FORD ALGORITHM

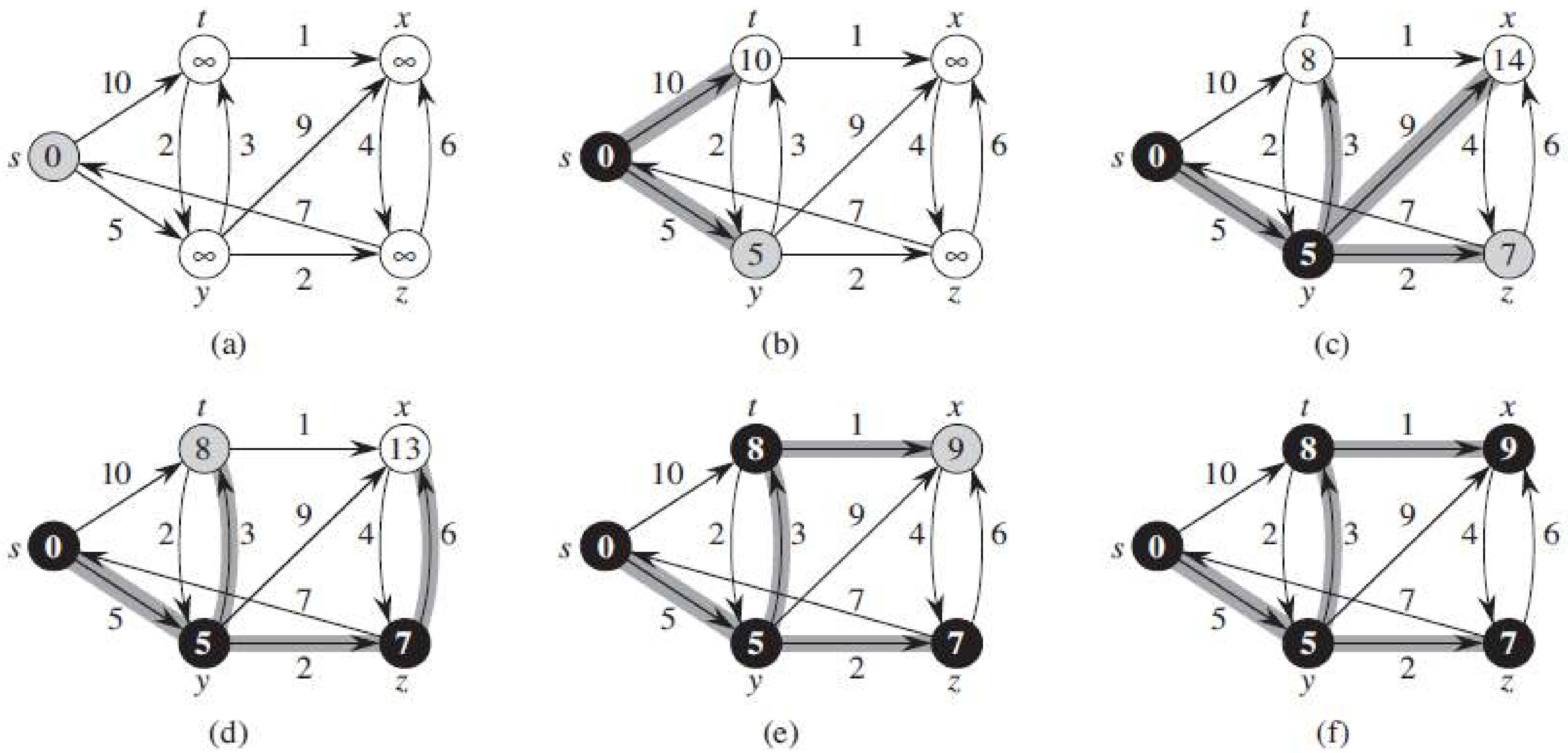
Also called Ford Fulkerson Algorithm.

Each neighbor of node knows path to destination.

Take advice from each neighbor and select the shortest path.



DIJKSTRA'S ALGORITHM



DISTANCE VECTOR ROUTING ALGORITHM

So far we have studied Static Routing Algorithms.

But practically dynamic Routing Algorithms are used.

Following two are Dynamic Routing Algorithms:

- 1. Distance Vector Routing Algorithm.
- 2. Link State Routing Algorithm.

Distance Vector Routing Algorithm:

At each step within a router:

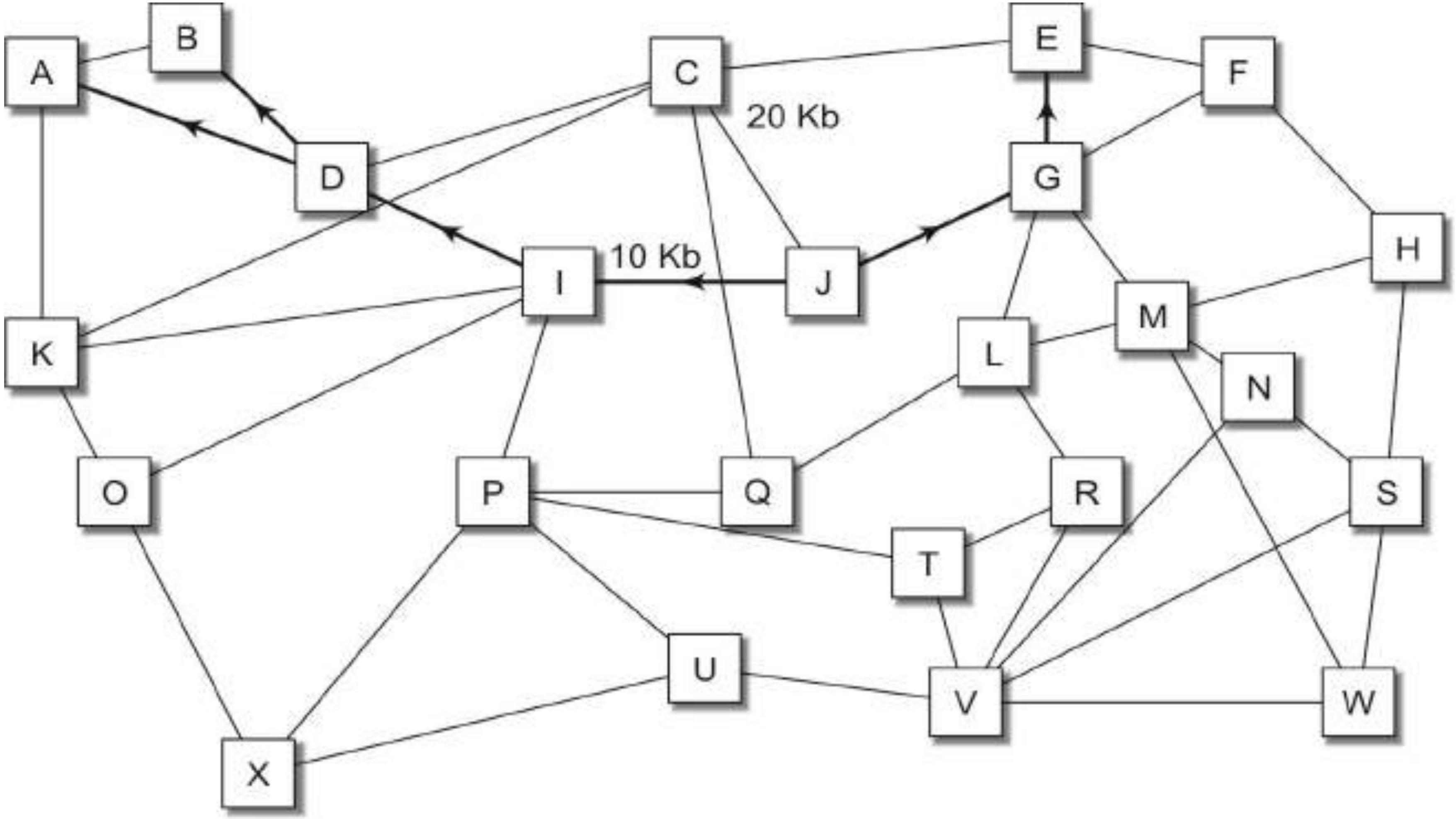
- Get routing tables from neighbours
- Compute distance to neighbours
- Compute new routing table

1. Router transmits its *distance vector* to each of its neighbors.
2. Each router receives and saves the most recently received *distance vector* from each of its neighbors.
3. A router **recalculates** its distance vector when:
   a. It receives a *distance vector* from a neighbor containing different information than before.
   b. It discovers that a link to a neighbor has gone down (i.e., a topology change).

The DV calculation is based on minimizing the cost to each destination.

The distance vector routing algorithm is sometimes called by other names, the **distributed Bellman-Ford** routing algorithm and the **Ford-Fulkerson algorithm**

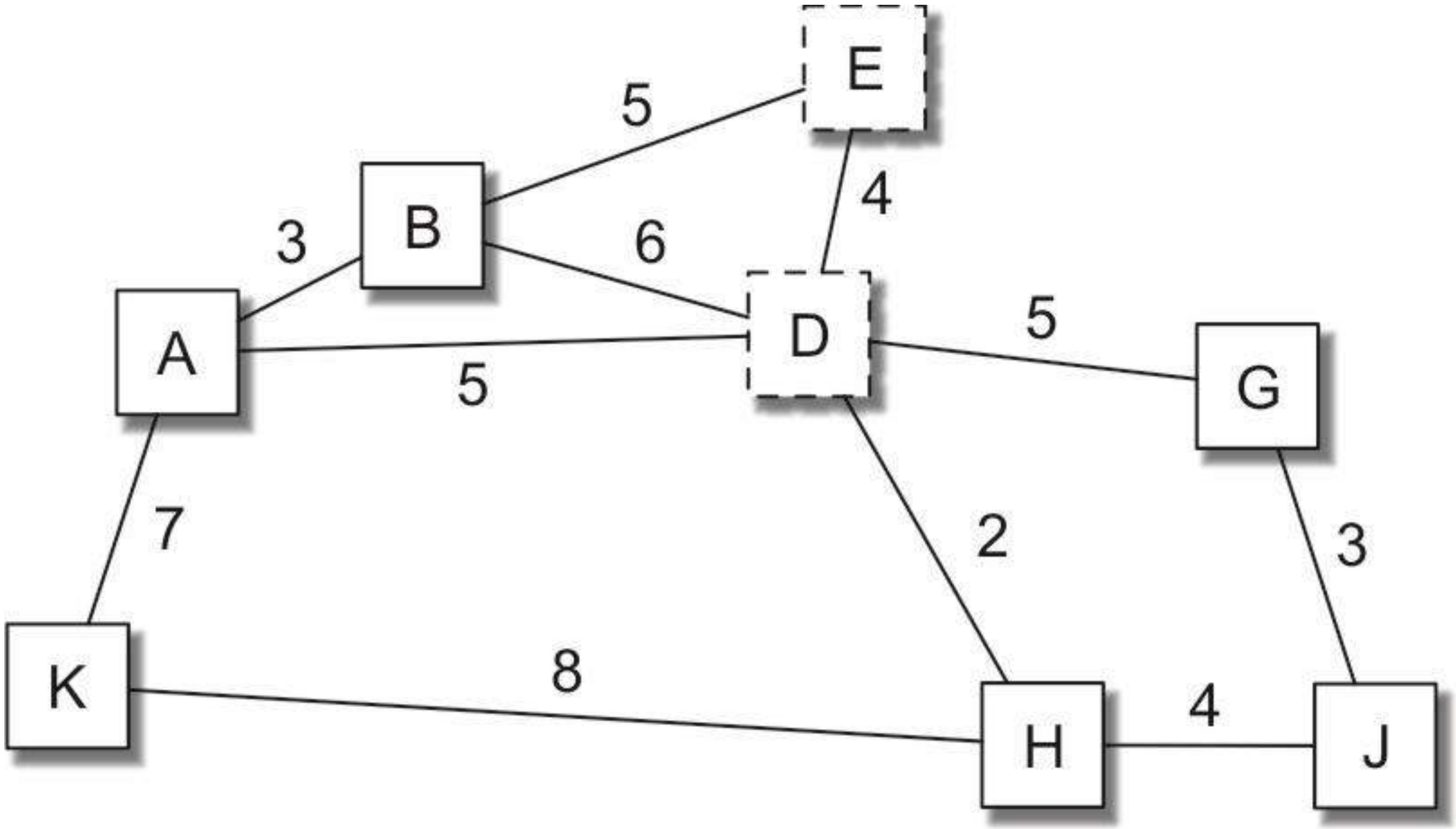
THE SUBNET FOR ROUTING AND J SENDER



PARTIAL ROUTING TABLE FOR J

Network	Next router	Interface
E	G	1
A	I	2
B	I	2
X	I	2
V	G	1
W	G	1
Q	C	3
…..	…..	…..

CONSTRUCTING ROUTING TABLES
ANOTHER EXAMPLE



CONSTRUCTING ROUTING TABLES
ANOTHER EXAMPLE

Estimated delay from B			Estimated delay from D		
Network	**Next router**	**Delay**	**Network**	**Next router**	**Delay**
A	A	3	A	A	5
D	D	6	B	B	6
K	A	10	K	A	12
H	D	8	H	H	2
J	D	12	J	H	6
G	D	11	G	G	5

COUNT TO INFINITY PROBLEM:

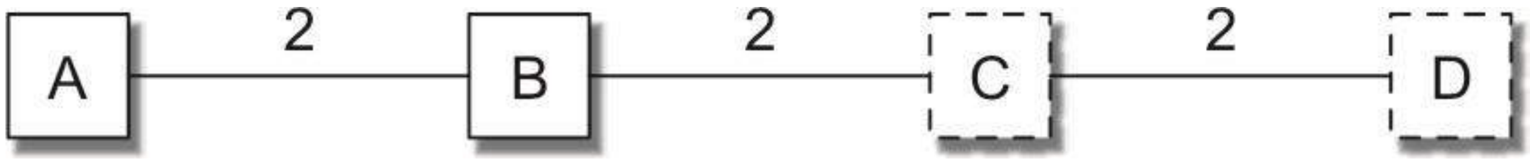
Drawback of Distance Vector Routing:

- Count to Infinity Problem:
- It reacts rapidly to good news,
- But, leisurely to bad news.
- Updates value fast when neighbor is down, but not when neighbor is again up. How?
- Lie to neighbour about distance if routing via neighbour
- The core of the problem is that when A tells B that it has a path to D, B has no way of knowing whether it itself(B) is on the path? This is how problem is created.
- It does not take bandwidth into account.
- Take too long to converge changes in one node to all other nodes.

Solution?

Split Horizon Hack. Lets see what it is.

COUNT TO INFINITY PROBLEM
ANOTHER EXAMPLE



COUNT TO INFINITY: C'S AND B'S ROUTING TABLES BEFORE D IS DOWN

Network	Next router	Delay
A	B	4
B	B	2
D	D	2

Network	Next router	Delay
A	A	2
C	C	2
D	C	4

A'S ROUTING TABLE AND C'S MODIFIED ROUTING TABLE WHEN D IS DOWN

Network	Next router	Delay
C	B	4
B	B	2
D	B	6

Network	Next router	Delay
A	B	4
B	B	2
D	B	6

SOLUTION BY LYING: THE SPLIT HORIZON HACK

B's routing table		
Network	Next router	Delay
A	A	2
C	C	2
D	C	infinity

- Rule: If B ask A, distance from A to D, and if B lies in the path, A should reply to B that A has path to D equal to infinite.
- This would avoid trapping of B into the loop of infinity.
- The best remedy is not to enter into Count to Infinity problem.
- This is called Split Horizon Hack.

LINK STATE ROUTING ALGORITHM

Each router must do the following:

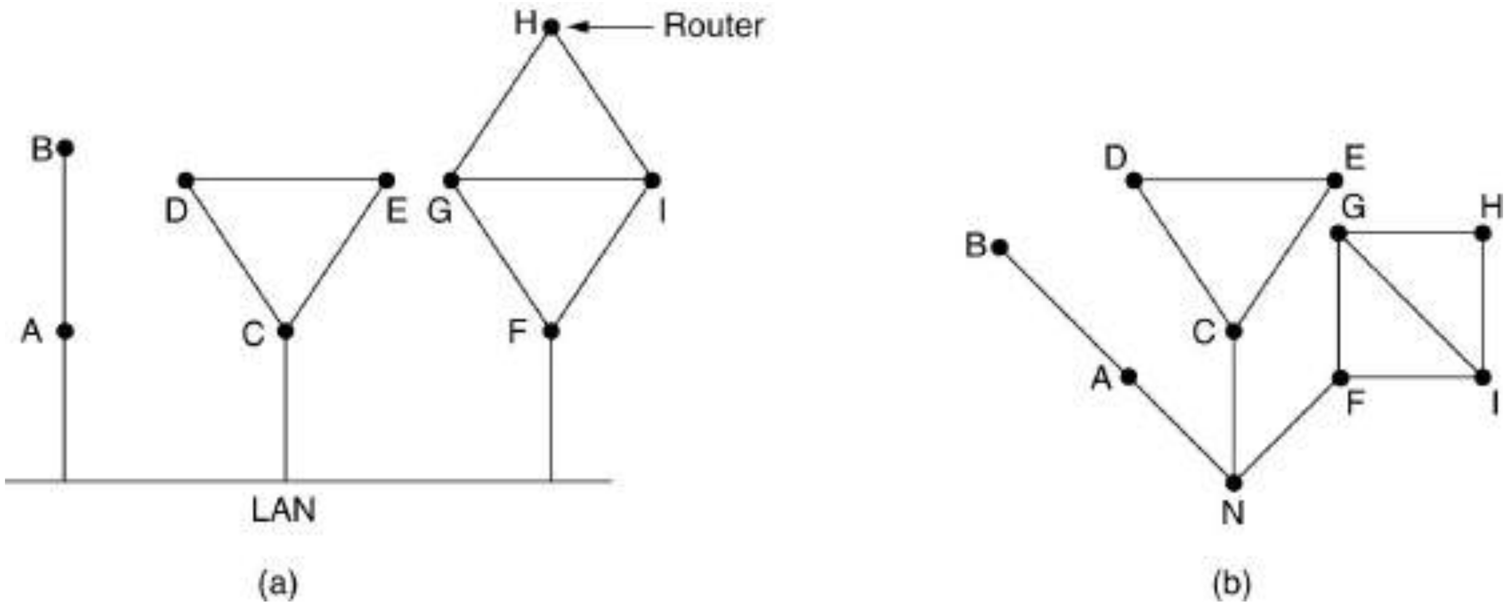
1. Discover its neighbors, learn their network address.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

A complete topology is developed. Then Dijkstra’s Algorithm can be used to compute the shortest path.

Following 5 steps are followed to implement it.

1. **Learning about the Neighbors**
2. **Measuring Line Cost.**
3. **Building Link State Packets.**
4. **Distributing the Link State Packets.**
5. **Computing the New Routes.**

STEP1: LEARNING ABOUT THE NEIGHBORS



(a) Nine routers and a LAN. (b) A graph model of (a).

Step 1: Learning about the Neighbours:

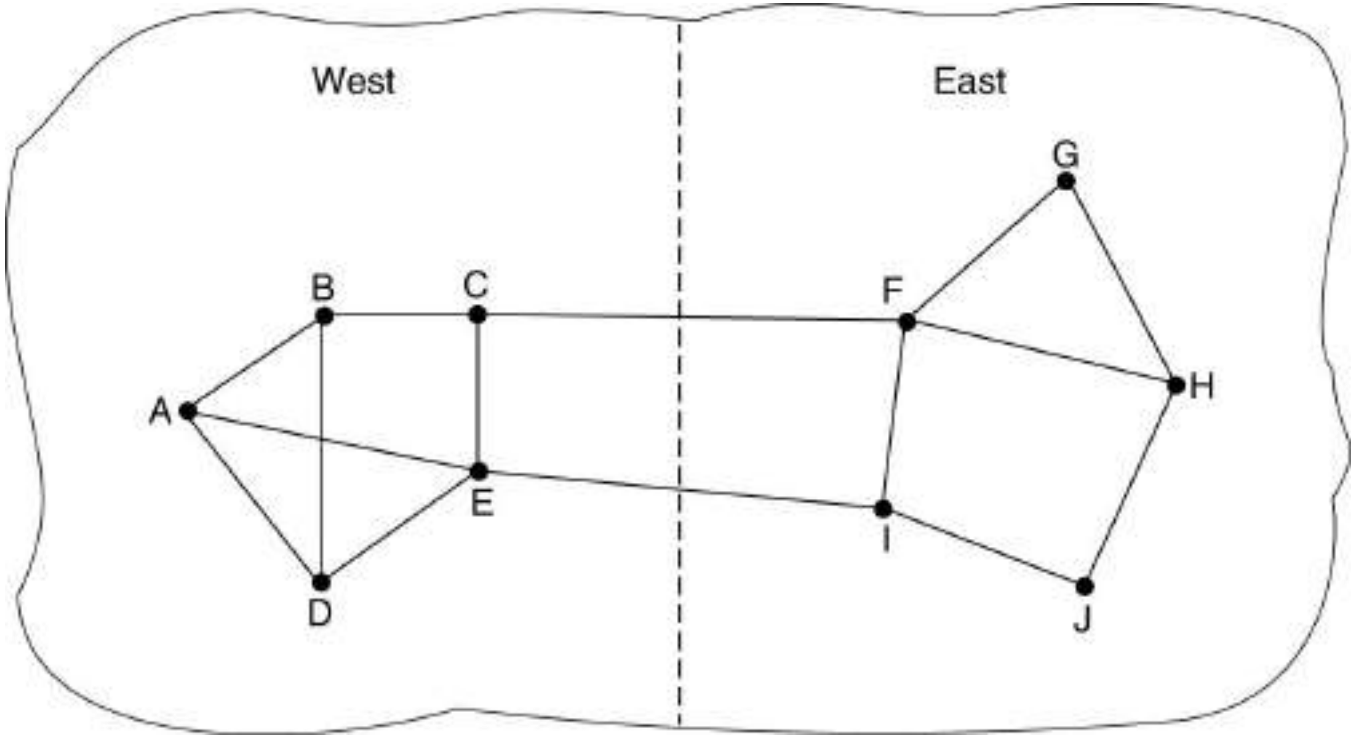
- Upon boot of router,
  - Send HELLO packet on each point-to-point line
  - Routers are supposed to send reply with a globally unique name

Step 2: Measuring the Line Cost:

- Measure round-trip delay using ECHO Packet and wait for its reply
- Take load into account? Yes. Arguments both ways: when choice is given to router having same number of hops from S to D.
  - Yes! preference for unloaded line as shortest path.
  - No! where oscillations are possible.
- Better Solution? Distribute Load over multiple lines.

2. MEASURING LINE COST

A subnet in which the East and West parts are connected by two lines.

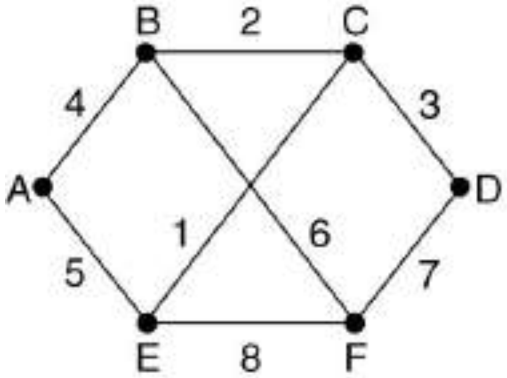


Step 3: Building Link State Packets:

- Packet containing:
  - Identity of sender
  - Sequence number + age
  - For each neighbour:
  - name + distance
- When to build the link state packets?
  - Periodically
  - when significant events occur

See next figure.

3. BUILDING LINK STATE PACKETS



(a)

Link State Packets

A	B	C	D	E	F
Seq.	Seq.	Seq.	Seq.	Seq.	Seq.
Age	Age	Age	Age	Age	Age
B 4	A 4	B 2	C 3	A 5	B 6
E 5	C 2	D 3	F 7	C 1	D 7
	F 6	E 1		F 8	E 8

(b)

(a) A subnet. (b) The link state packets for this subnet.

Step 4: Distributing Link State Packets:

Distributing link state packets

- Trickiest part of algorithm
  - Arrival time for packets different
  - How to keep consistent routing tables?
- Basic algorithm
  - Flooding +
  - Sequence number (in each packet) to limit duplicates.
- Manageable problems
  - Wrap around of sequence numbers results to wrong data. Solution? Use 32 bit sequence number.
  - Wrong sequence number used in case of :
    - lost in case of crash
    - Corrupted data transmitted.
- Solution? include the age of each packet after the sequence number and decrement it once per second. When the age hits zero, the information from that router is discarded.
    - duplicates are discarded
    - Old packets are thrown out

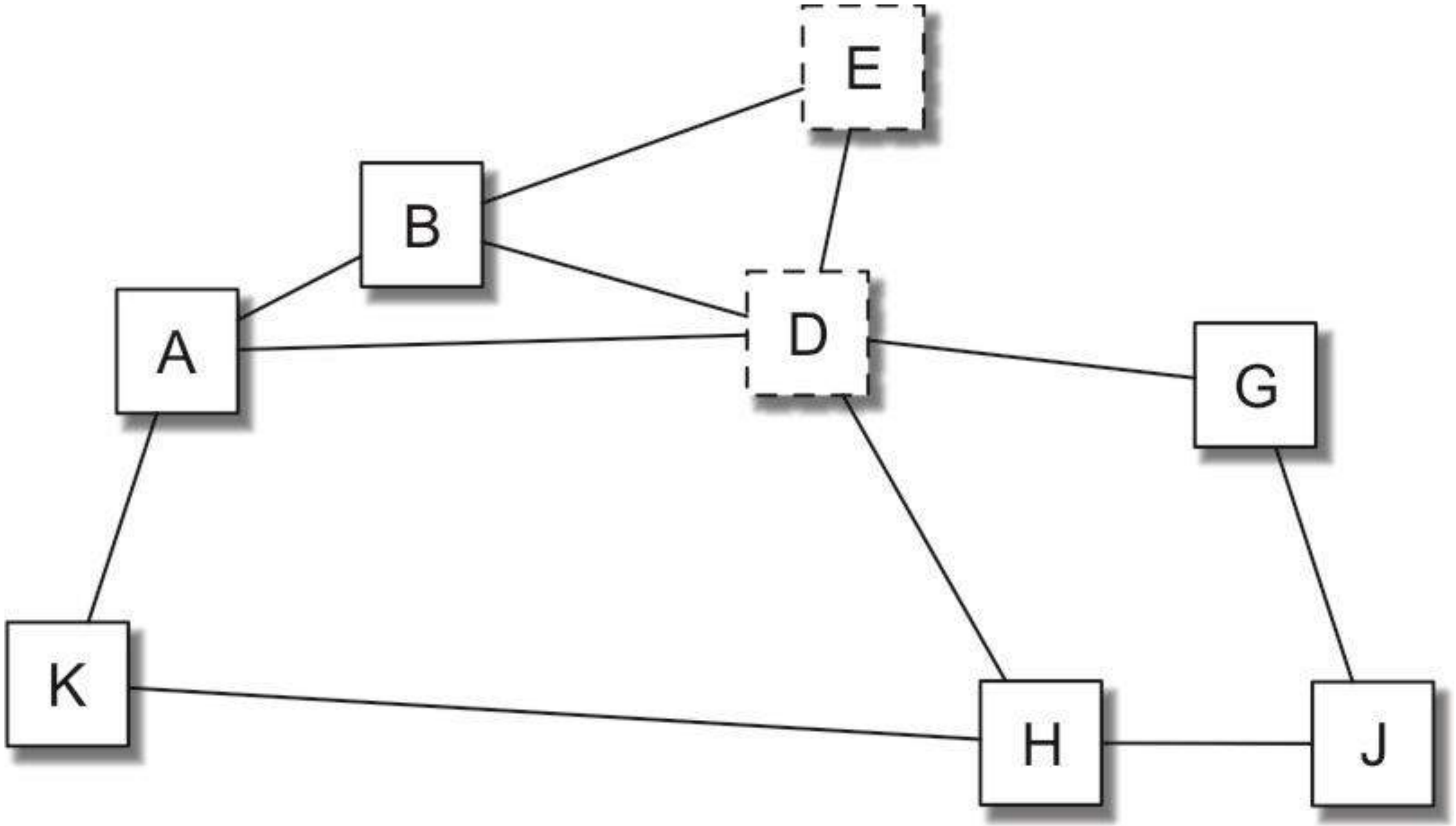
Step 5: Computing new routes:

- With a full set of link state packets, a router can:
  - Construct the entire subnet graph
  - Run Dijkstra's algorithm to compute the shortest path to each destination
- Problems for large subnets
  - Memory to store data
  - Compute time for developing these tables.

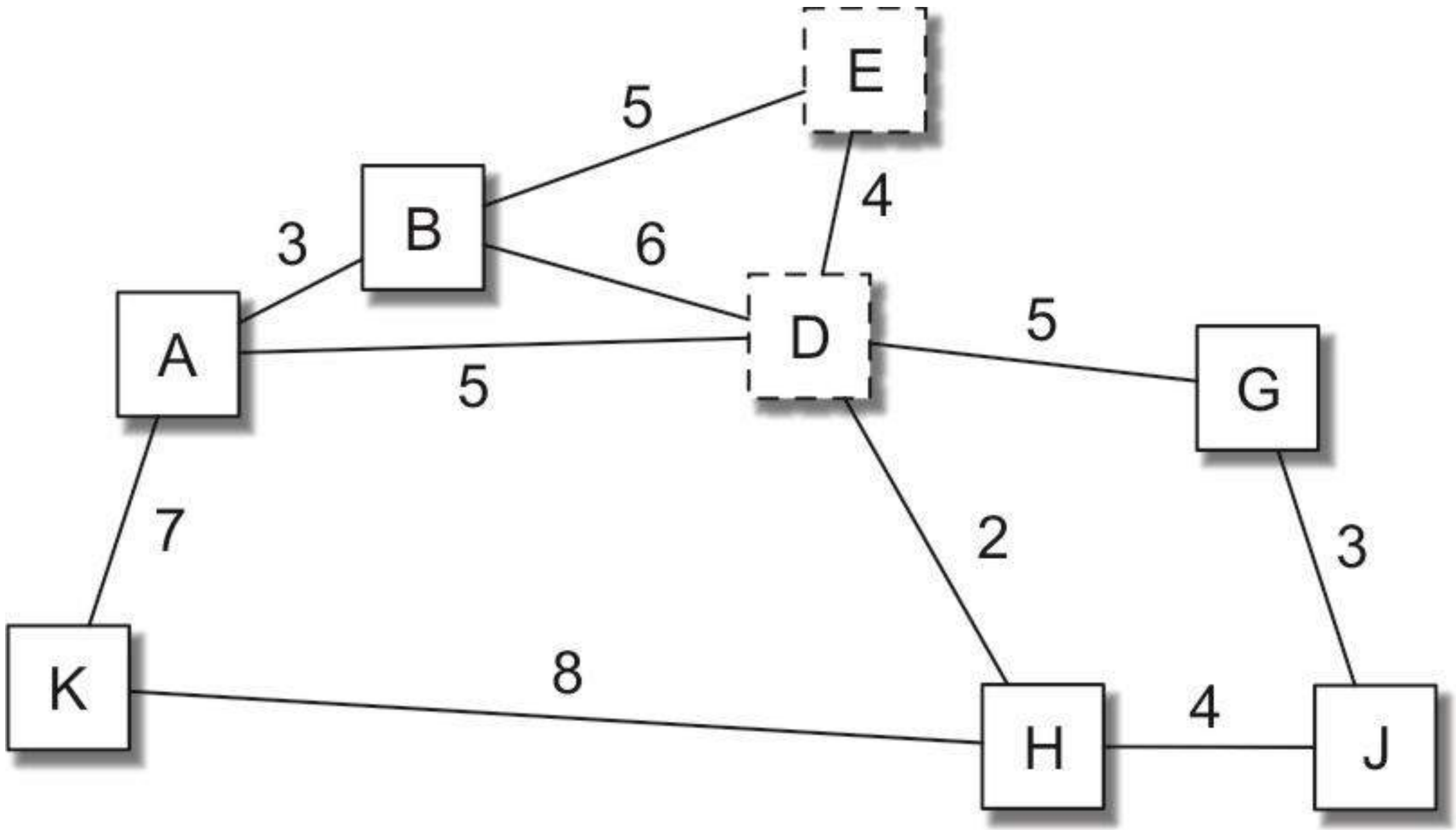
Usage:

- IS-IS protocol (Intermediate System, Intermediate System)
  - Designed for DECnet(digital equipment corporation network protocol suite), adopted by ISO(international standardization organization), used still in internet.
  - Supports multiple network layer protocols
- OSPF(Open Shortest Path First) protocol used in Internet
- Common features:
  - Self-stabilizing method of flooding link state updates
  - Concept of a designated router on a LAN
  - Method of computing and supporting path splitting and multiple metrics.
  - Useful in Multi Protocol Environment.

LINK STATE ALGORITHM



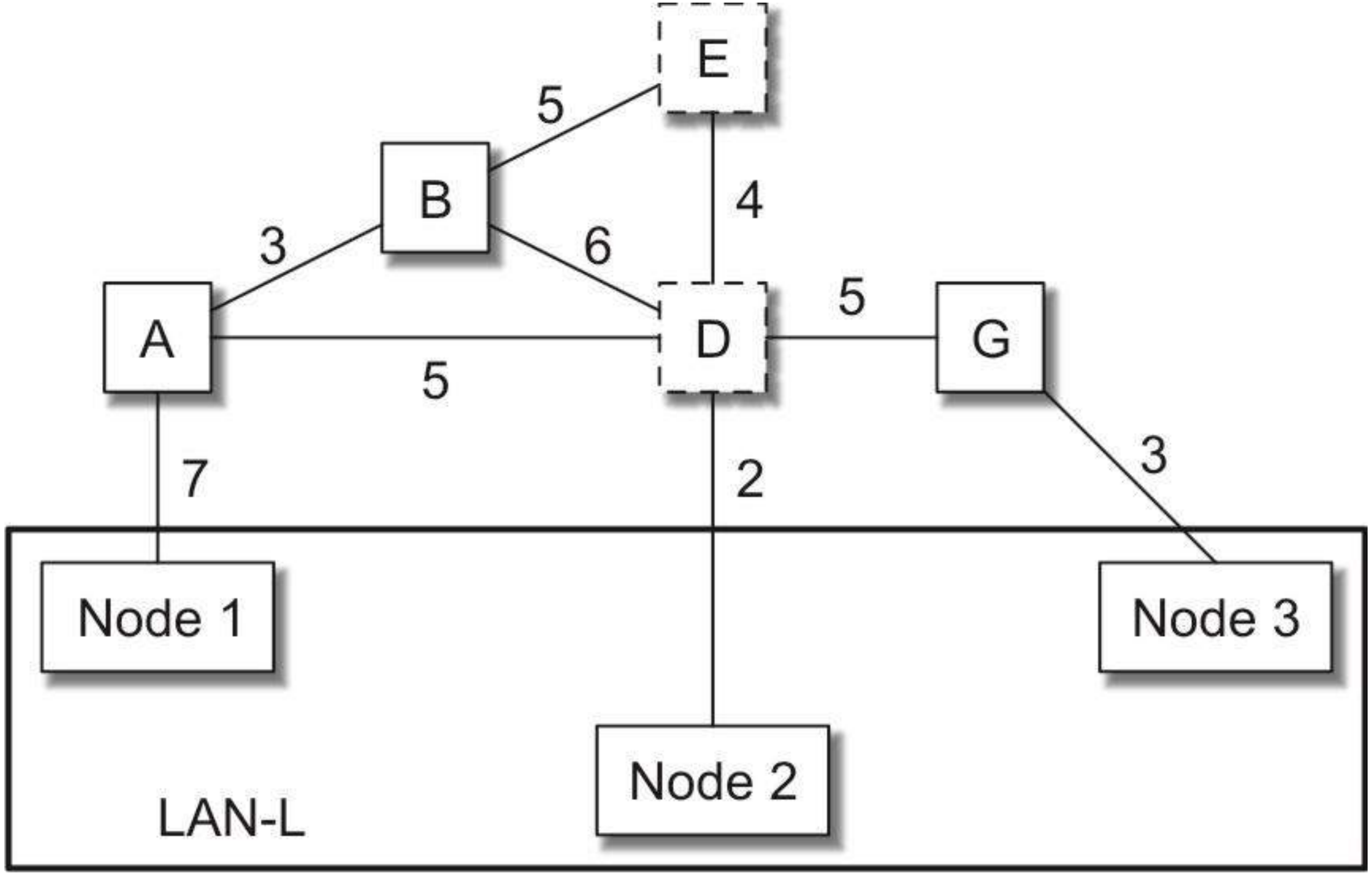
THE GRAPH CONSTRUCTED FROM ALL THE PACKETS



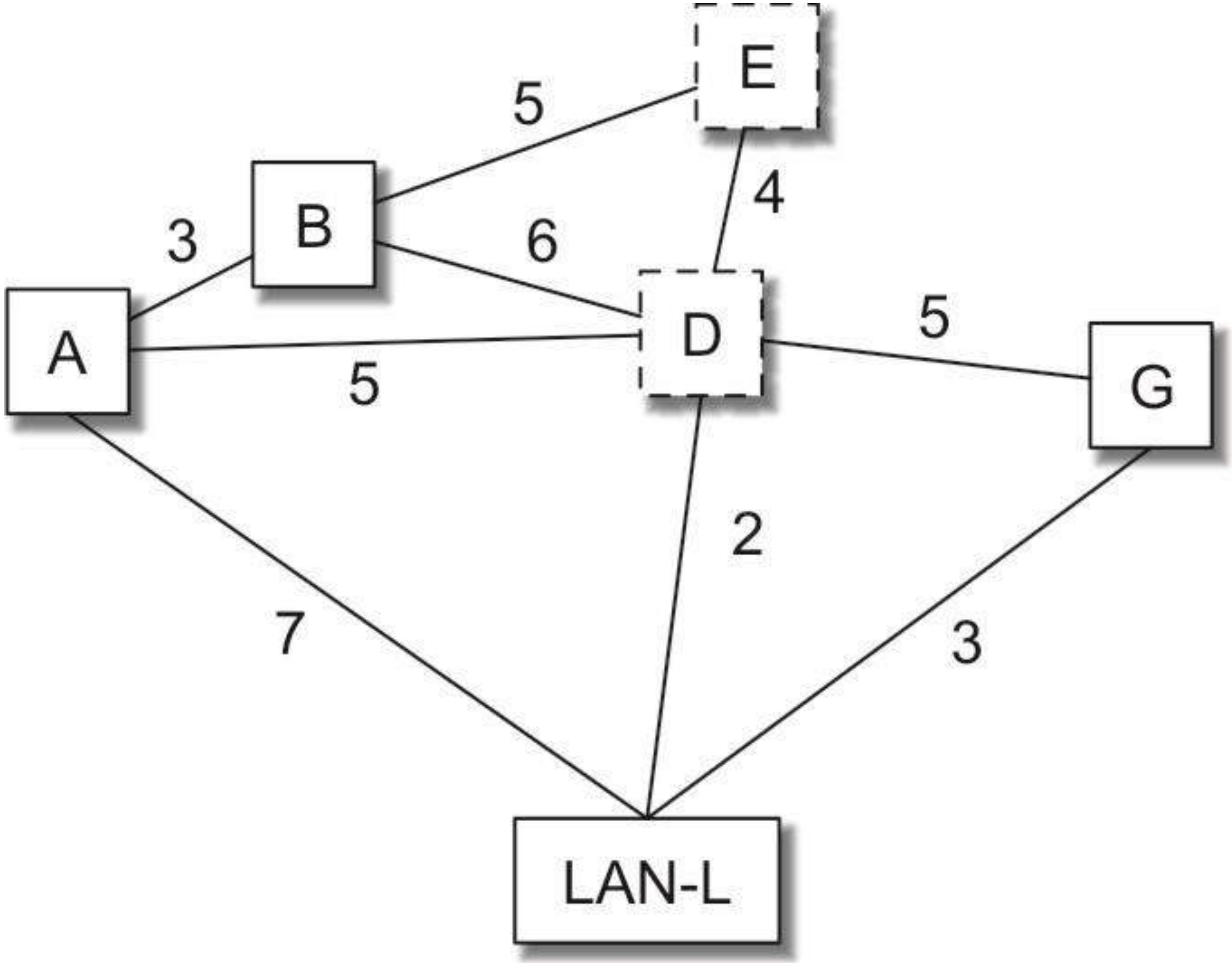
E'S ROUTING TABLE

Network	Next router	Delay
A	B	8
B	B	5
D	D	4
K	B	15
H	D	6
G	D	9
J	D	10

THE ISSUE WHEN LAN IS A PART



SOLUTION: DEPICT LAN AS A NODE



Link State	**Distance Vector**
link states algorithm is an algorithm **using global information**	the distance vector algorithm is **iterative, asynchronous, and distributed**
each node **talks with all other nodes**, but tell them only the cost of it's directly comparison of some of their attribute	each node **talks to only its directly connected neighbors**, but provides its neighbor with least cost estimates from itself to all the nodes.
Message complexity: With link state, every node has to keep the information about the cost of each link within the network.	**Message complexity**: with distance vector algorithm, message is exchanged between two hosts which are directly connected to each other.
very times, if any of the link cost is changed, all the nodes are **updated.**	change of cost in the link which is belong to the least cost path for one of the nodes, the DV algorithm will update the new value. But if the change doesn't belong to the least cost part between 2 hosts, there will **no updating**.
Speed of convergence: can converge faster in comparison of later.	**Speed of convergence**: can converge slowly and have routing loops while the algorithm is converging.
Such probability is less.	DV algorithm also suffers from the **count to infinity** problem.
Robustness: For LS, when a router is down, it can broadcast a wrong cost for the closest one. LS node is computing for its own forwarding table and other node do the calculation for themselves. **Better than DV.**	**Robustness:** DV, the wrong least cost path can be passed to more than one or all of the node so the wrong calculation will be process in the entire net work. This problem of DV is much **worse than LS algorithm**.

CONGESTION CONTROL ALGORITHMS

1) Open Loop Control

2) Admission Control

3) Policing

4) Leaky Bucket Algorithm

5) Traffic Shaping

6) Closed Loop Control

7) End to End v/s Hop by Hop

8) Implicit v/s Explicit Feedback

CONGESTED SWITCH

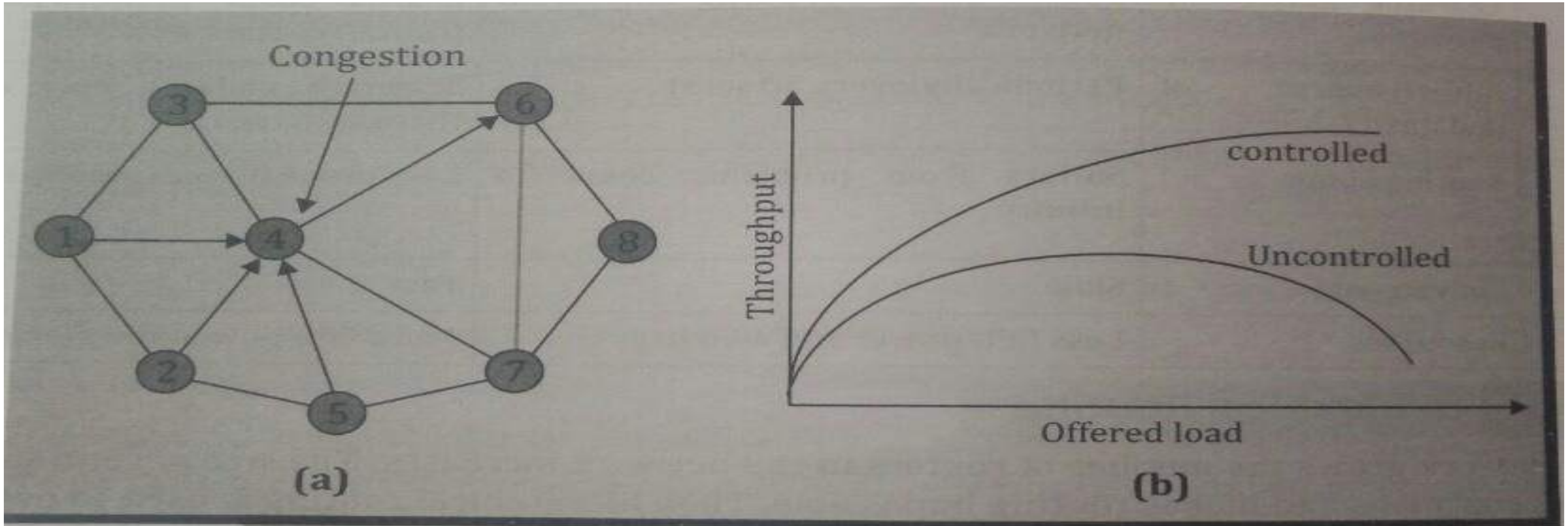


Figure12.18 (a) A Congested switch
(b) Throughput with and without congestion switch

POLICY IMPLEMENTATION

Congestion Control Policies Implemented At Various Levels

Layer	Policies
Transport	• Retransmission policy • Acknowledgement policy • Timeout determination • Out-of-order caching policy • Flow control policy
Network	• Virtual circuits versus datagram inside the subnet • Packet queuing and service policy • Routing algorithm • Packet discard policy • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

ADMISSION CONTROL

Makes decision based on congestion whether to accept or reject new traffic flow.

Used in virtual circuit packet switching such as ATM over connections n so called CAC – Connection Admission Control.

If QoS parameters like delay, loss probability, variance, bandwidth, etc can be satisfied by available resources, packets/flows are accepted, else rejected.

Effective bandwidth is obtained when the flow lies between average rate and peak rate.

POLICING

When the flow is accepted by admission control, QoS is satisfied negotiated traffic parameters during lifetime of flow.

To prevent source from violating its negotiated parameters, monitoring of traffic flow is required continuously.

This process of monitoring and enforcing the traffic flow is called policing.

Network may discard the flows that violates the negotiated contracts.

To do so, tagging is done to set lowest priority.

When network resources are exhausted, tagged traffic is first to be discarded.

LEAKY BUCKET ALGORITHM / TRAFFIC SHAPING

Water poured in the bucket with a hole at bottom.

Bucket leaks at constant rate.

Hole ensures that bucket will never overflow.

Process of altering traffic flow to ensure conformation.

Incoming packets are stored in bucket and stream of packets are served to server so that output is smooth.

Bucket has buffer that store momentary bursts of water/packets.

Incoming packets are discarded when buffer is full.

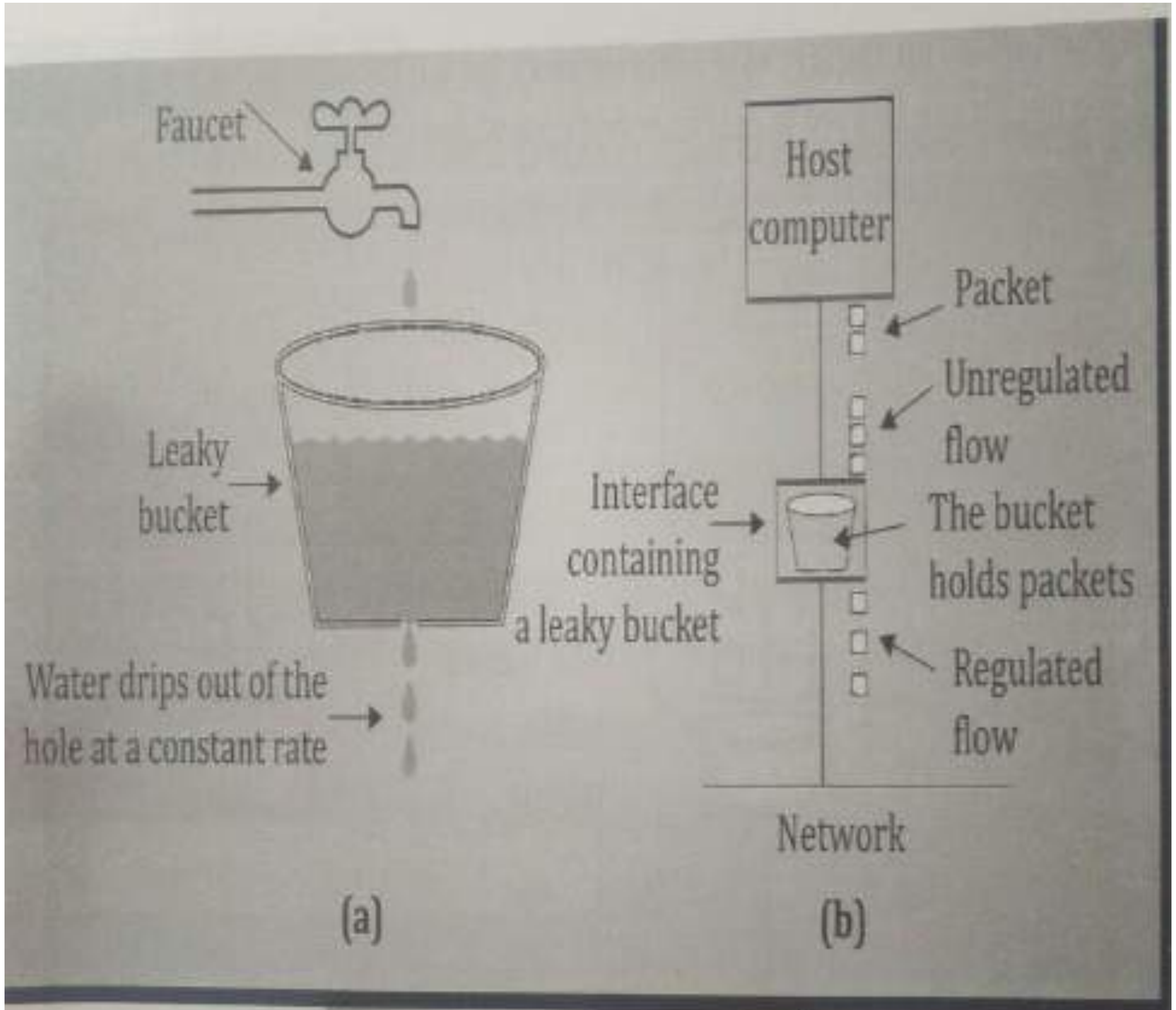


Figure 12.19 Leaky Bucket

TOKEN BUCKET ALGORITHM / TRAFFIC SHAPING

Regulates packet that are not conforming.

Packets that are conforming are passed through channel without further delay.

Tokens are generated periodically at constant rate & stored in Token Bucket.

If token bucket is full, additional tokens are discarded.

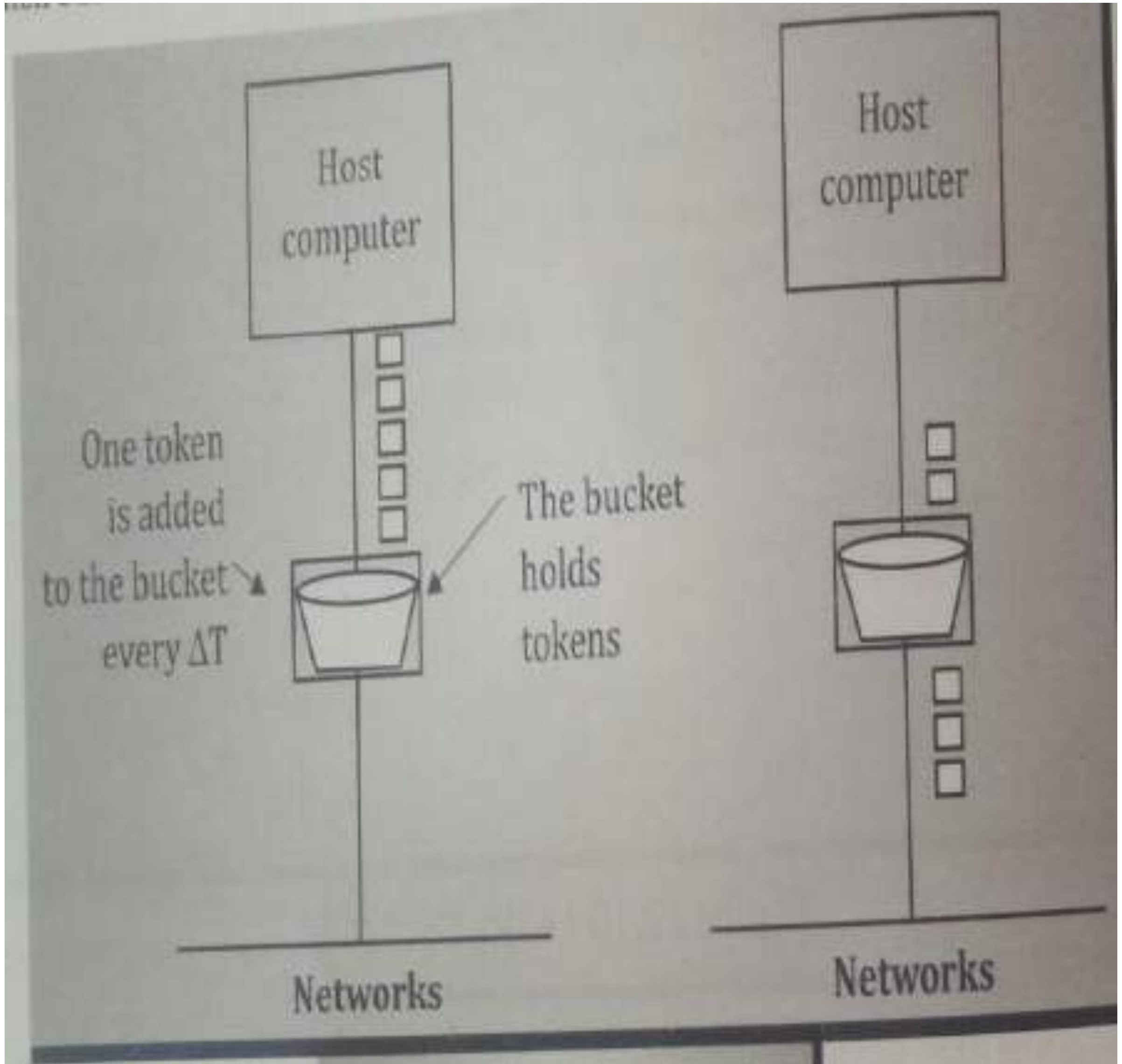


Figure 12.20 Token Bucket

CLOSED LOOP CONTROL

Performs no reservation.

Performs based on feedback.

Parameters are buffer content and link utilization.

Regulates packet flow rate.

Two types:

1) End to End v/s Hop by Hop

2) Implicit v/s Feedback

FEEDBACK: EXPLICIT OR IMPLICIT

Explicit Feedback

- ECN: Explicit Congestion Notification field in TCP and IP header indicating congestion.
- Turned on indicating Possibility of Congestion
- ICMP: Internet Control Message Protocol

Implicit Feedback

- Older TCP implementation had no field to indicate congestion.
- Retransmission, RTT and Dropping events indicate congestion.

REPEATER

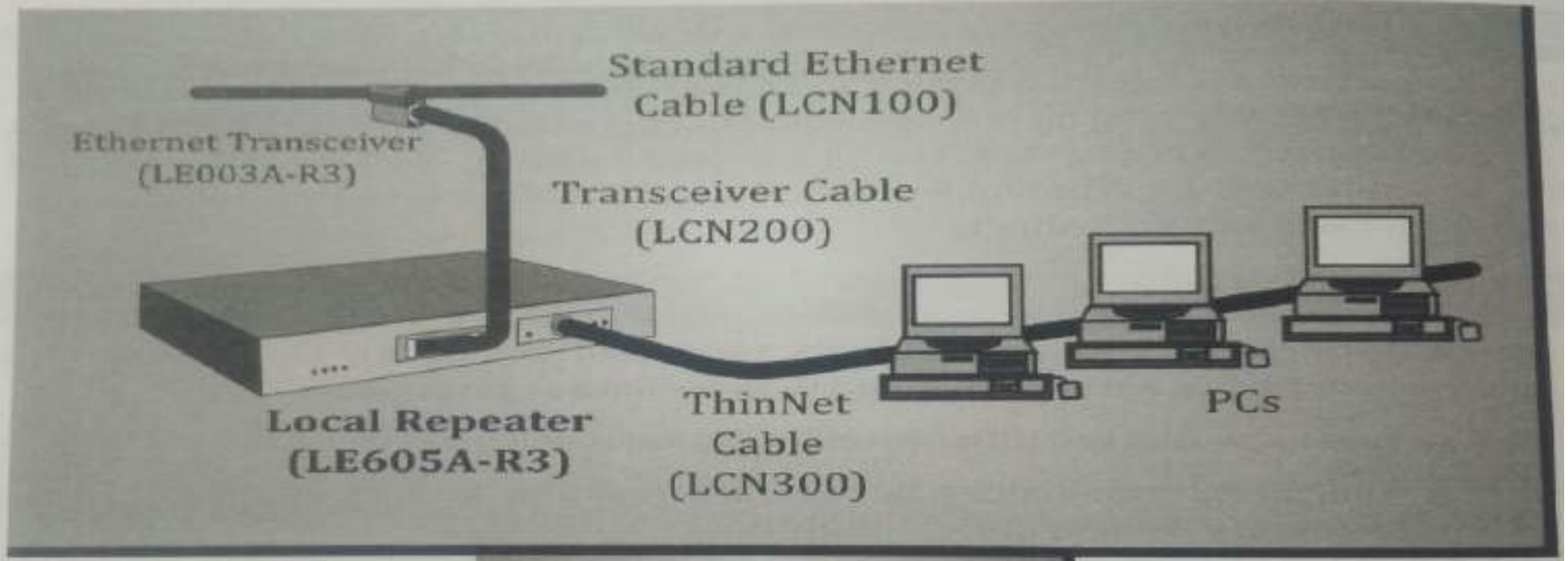


Figure12.21 Repeater

GATEWAY

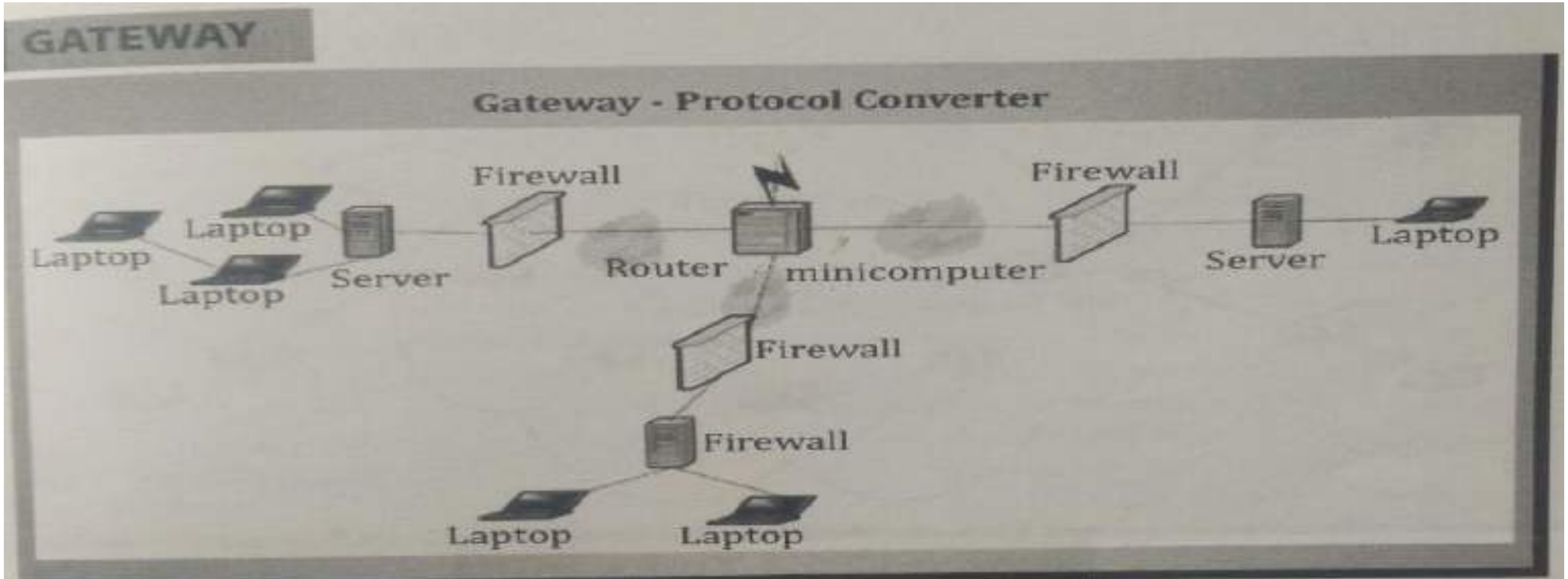


Figure 12.22 Gateway

TUNNELING

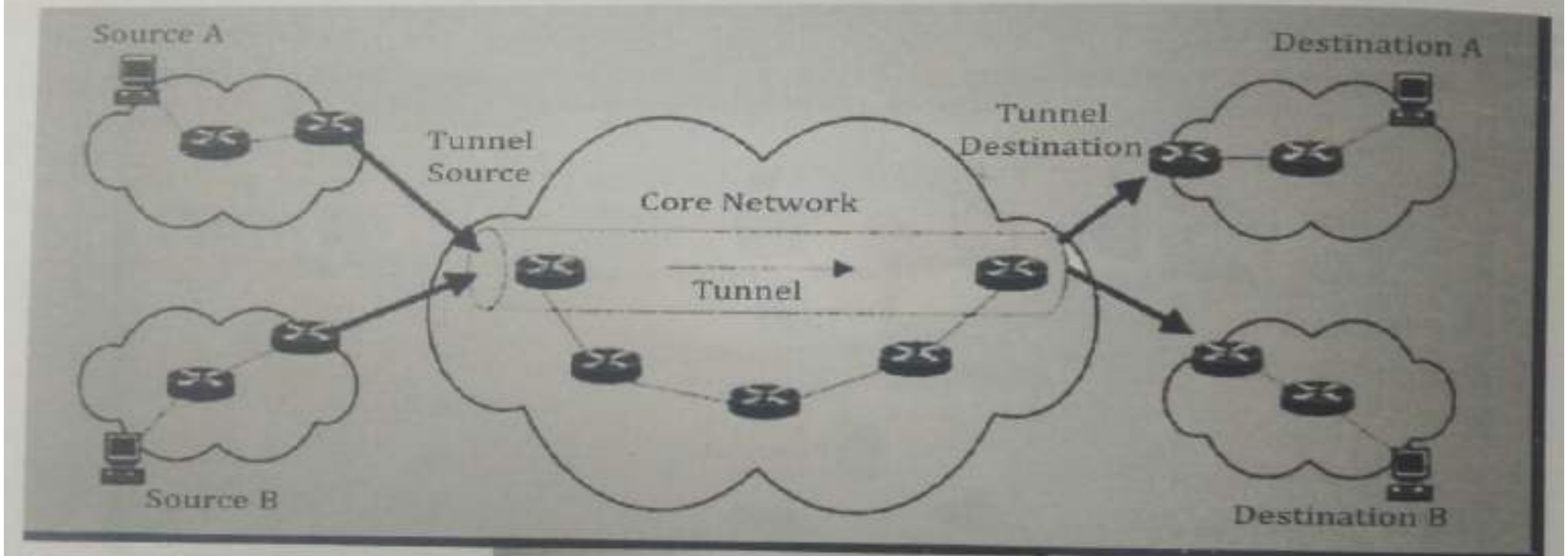


Figure 12.23 Tunneling

FRAGMENTATION

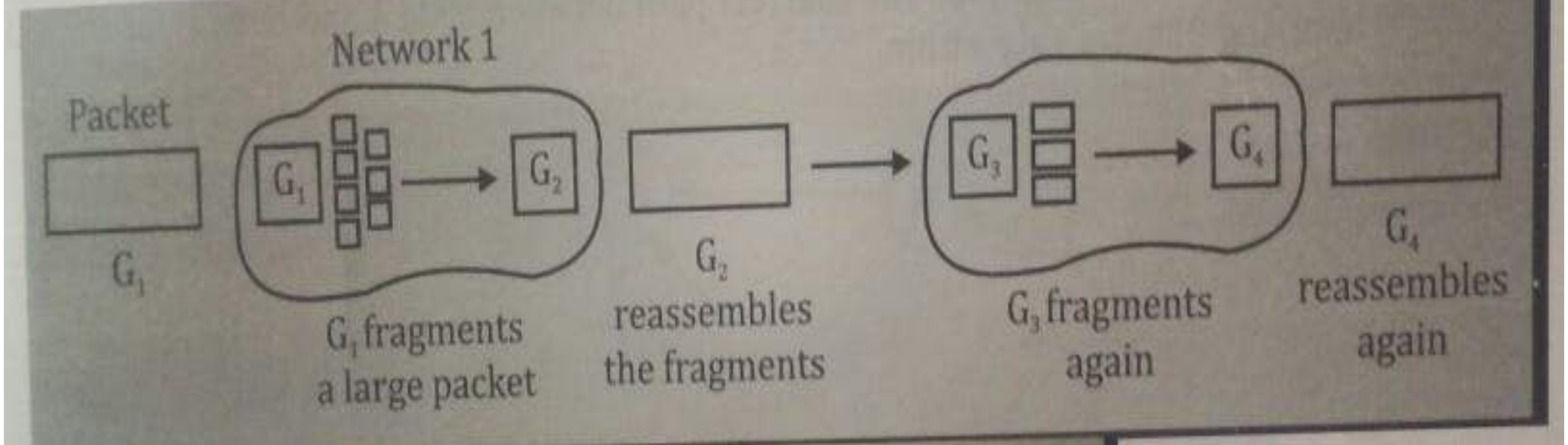


Figure 12.24 Fragmentation

HOW NETWORKS DIFFER FROM EACH OTHER?

12.13.1 How Networks Differ?

Networks vary in physical and data link layer by modulation techniques and frame format.

Some of the difference in the network implemented in in network layer is as follows.

S.No	Parameter	Some Possibilities
1.	Service offered	Connection orient ed versus connection less
2.	Protocols	IP, IPX, SNA, ATM, MPLS etc.
3.	Addressing	Flat versus hierarchical
4.	Multicasting	Present or Absent
5.	Packet Size	Every network has its own maximum
6.	Quality Service	Present or Absent
7.	Error Handling	Reliable, ordered and ordered delivery
8.	Flow Control	Sliding window, rate control
9.	Congestion control	Leaky bucket, RED, Token bucket choke etc.
10.	Security	Encryption
11.	Parameters	Different timeouts, flow specification etc
12.	Accounting	By connect time, by packet, by byte

COMPARISON, ANSWER OF ASSIGNMENT

10.4.4 Comparisons Of Scheduling Approaches

SCHEDULING APPROACHES	Description
Reservation	• Stations submit a request for the next round of data transmission. • Requires a lot of overhead information.
Polling	• Centralized controller repeatedly polls stations and allows each to transmit one protocol. • Uses dynamic form of time-division multiplexing • Provides fairness through regular access opportunities • Can provide bounds on access delay
Token Passing	• Stations circulates a token, each time it receives a token it transmit one packet. • Dynamic form of time-division multiplexing when users transmit in round-robin scheme • Requires token management system for efficient performance.

COMPARISON, ANSWER OF ASSIGNMENT

10.5 Comparisons Of Random Access And Scheduling Mac Control

	Random access approach	Scheduling approach
1.	In random or contention methods, no station is superior to another station and none is assigned the control over another.	In scheduled or controlled access, the stations consult one another to find which station has the right to send. A station cannot send unless it has been authorized by another station.
2.	Random access provides chaotic, uncoordinated, and unordered access.	Scheduling approach provides orderly access to the medium
3.	When bandwidth is plentiful, random access systems can provide very small delays as long as the systems are operated with light load.	The scheduling approach has less variability in the delays encountered by packets. Therefore they are used for supporting applications with stringent delay requirements.
4.	Popular random access methods are :-ALOHA, CSMA, CSMA/CD.	Popular scheduling access methods are :- Reservation, Polling, Token Passing.
5.	Relatively simple.	Sophisticated.
6.	Channel bandwidth is used to alert stations during collisions	Channel bandwidth carries explicit information that allows station to schedule their transmissions.
7.	More collision	Avoids collision

SYLLABUS OVER.
BEST WISHES FOR YOUR EXAMS.

IT WAS GREAT TIME TEACHING YOU ALL. THANK YOU FOR EVERYTHING. BLESSINGS.