

CHAPTER 1

INTRODUCTION TO COMPUTER NETWORKS

4 hours

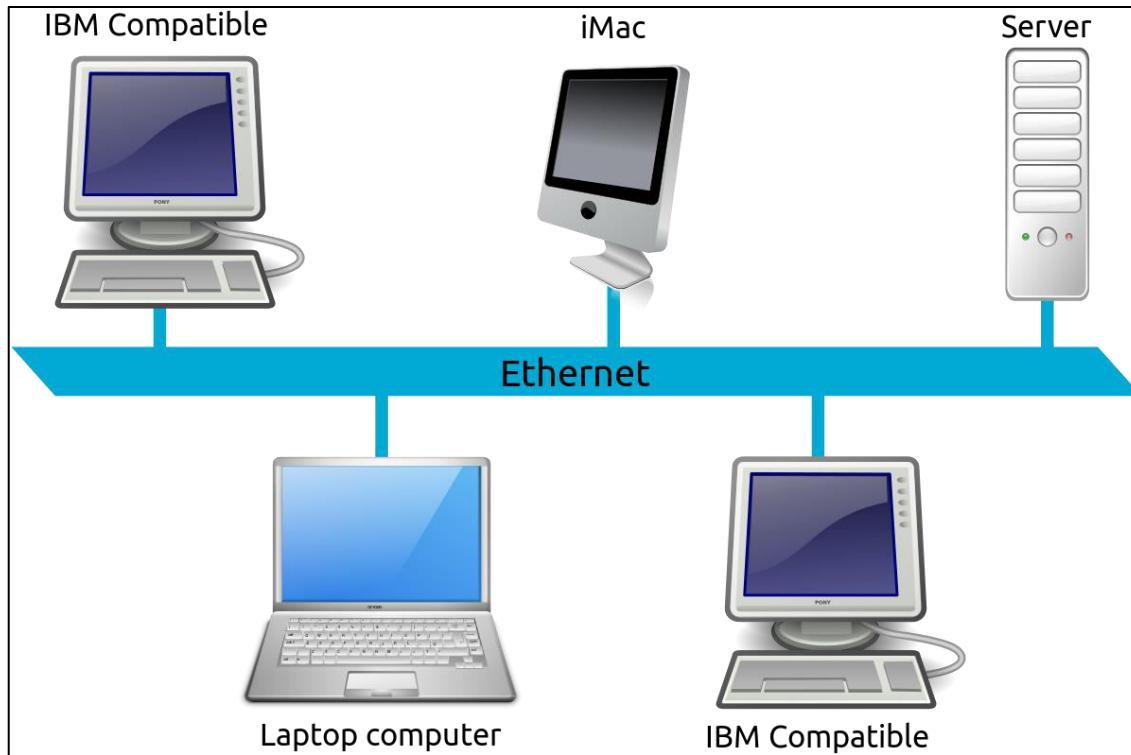
~ 7-8 marks

Overview

- Features, advantages and disadvantages of computer network
- Classification structure of networks
- Networking Topologies
- Network architectures (Client-Server and Peer-to-Peer)
- OSI model
- Connection-oriented and connection-less services
- Networking applications: ARPANET

What is computer network?

- A “network” is an interconnection of units.
- Computer network is a system of interconnected computer systems through some link for the purpose of sharing information.
 - The link for interconnection may be copper wire, fiber optics, microwave, satellite, wireless, etc.
- Computers connected to a network can communicate with each other by sending messages and/or sharing resources.



Components of a computer network

1. End devices
 - PC, mobile, laptops, smart devices
2. Communicating device / Networking devices
 - Router, switch, hub, repeaters
3. Communicating medium
 - Physical wires (STP, UTP, coaxial, optical fiber)
 - Wireless technology(microwaves, infrared, satellite, wi-fi)

Why Computer Networks are required?

- Sharing hardware resources
- Sharing software resources
- Communication purpose
- Sharing information over geographically distant regions
- Educational purpose
- Multimedia (File transfer, gaming, chats, internet)
- Global marketing (e-Commerce)

Advantages of computer networks

- Efficient data sharing or access between different units
- Since the same data can be used by many entities, data can be maintained in a central place
- Increased speed of data access
- Improved data security
- Centralized software structure
- Effective way of communication
- Remote access and communication is possible
- Good platform for establishing and expanding modern business empire

Disadvantages

- Security is always an issue
- Cost of installing network
- management of Network requires expertise
- Costly maintenance
- Units within a network always have a chance of breakdown, hence risk of network failure is persistent.
- Chances of computer crime (Data loss / leakage / cyber crimes)

Application area for networks

- Internet access (www.setopati.com)
- E-mail ([Gmail](#), [Hotmail](#))
- Long distance communication through video conferencing ([Viber](#)/[skype](#))
- E-commerce ([Amazon.com](#))
- Collaboration among various institutions that are geographically distant ([GitHub](#)/
[Slack](#), [TeamViewer](#))
- Banking and Finance ([NMB online banking](#))
- VPN ([India accessing TikTok](#))
- Online gaming ([Mario online](#))
- Resource sharing in home and offices ([Printers](#), [Access Points](#), [Software Systems](#))

1.2 Network structure and topologies

- Network structures define “how we interpret a network”
- Network structure pertains anything from design of network to all the way through implementation and use
- Network structure has different definition for different people.
 - In the perspective of people who use or implement the network, a network structure is a collection of wires, computers, and other related components.
 - However, for business oriented people, a network structure is the design that helps to achieve required goal. It can be scalable and satisfying the growing market structure.
- A network structure is generally designed by a network architect and implemented by network engineers.

Network Structure Classification

Based on Transmission Media.
(*Wired / Wireless*)

Based on Network Size
(*LAN / MAN / WAN*)

Based on Managing style
(*Client-Server / Peer-to-Peer*)

Based on Topology
(*Bus / Ring / Star / Mesh*)

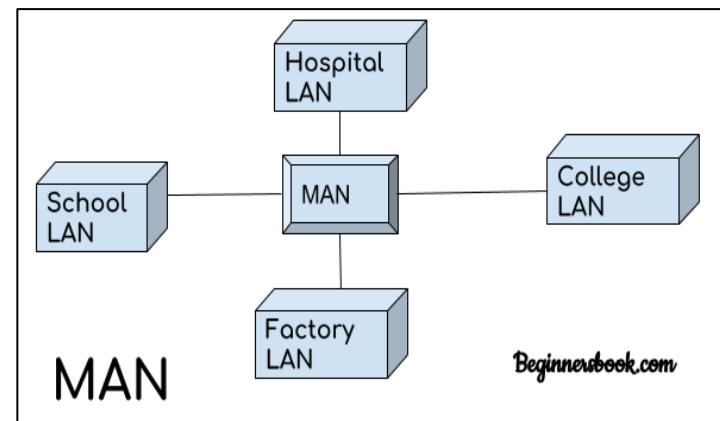
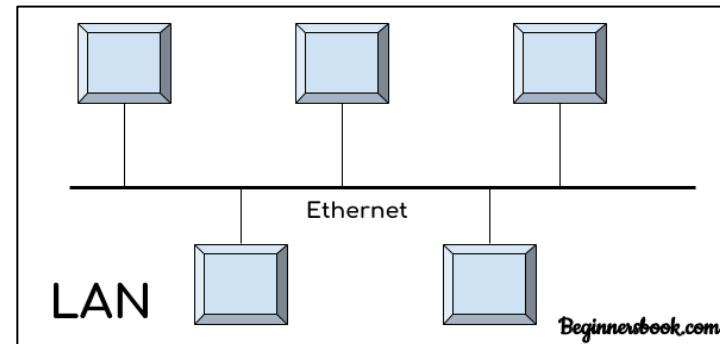
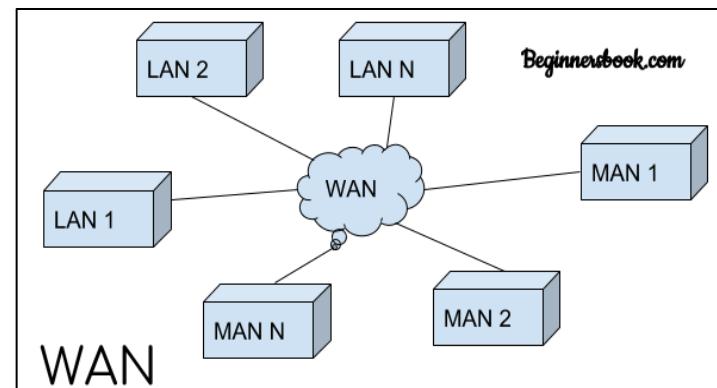
A. Classification on transmission media

1. Wired connection
 - Some network structure are connected through physical wires
 - These connections are based on desired speed, distance of transmission, and cost.
 - While these are cheaper to implement, their repairing and maintenance are tedious.
 - E.g. coaxial cable, optical fiber

2. Wireless connection
 - Some network structure are connected through wireless technology
 - Generally a central device works as a access point/hot spot.
 - In other cases various devices work as repeater/signal regenerating units for long distance communication.
 - As the scale of business expand, this mechanism becomes costlier.
 - E.g. Wi-Fi, Satellite, Microwave

B. Based on network size

1. LAN – local area network
 - Connection within an office building or complex
2. MAN – metropolitan area network
 - Connection covering multiple areas or cities
3. WAN – wide area network
 - Connection that covers cities, states , countries



S.n.	Parameters	LAN	MAN	WAN
1	Definition	Local Area Network	Metropolitan Area Network	Wide Area Network
2	Type of network ownership	Private	Public or private	Public or private
3	Area coverage	Small (Building)	Moderate (City)	Large (Countries)
4	N/w design & maintenance	Easy	Difficult	Difficult
5	Communication medium	Mostly coaxial or fiber, wireless	PSTN, coaxial and fiber, wireless	PSTN, satellite
6	Data transmission rate	High	Moderate	Low
7	Data propagation delay	Low	Moderate	High
8	Is network congestion possible?	No	Yes	Yes
9	Expertise for implementation or maintenance	Working knowledge is enough	Needs good knowledge for implementation	Needs experts for design, implementation & maintenance

Other networking schemes

1. HAN (Home Area Network)

- A type of LAN
- All of the end devices are generally used within a home.
 - E.g. computers, mobile phones, TVs, gaming consoles, smart watches
- End devices are connected to the router for network access.

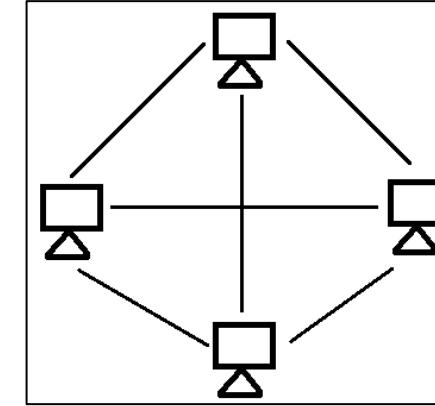
2. PAN (Private Area Network / Personal Area Network)

- These cover smaller area than LAN, usually a small room.
- Two devices that need to communicate need to be around a very limited range.
- E.g. Wi-Fi, Bluetooth, Infrared

C. Classification on managing style

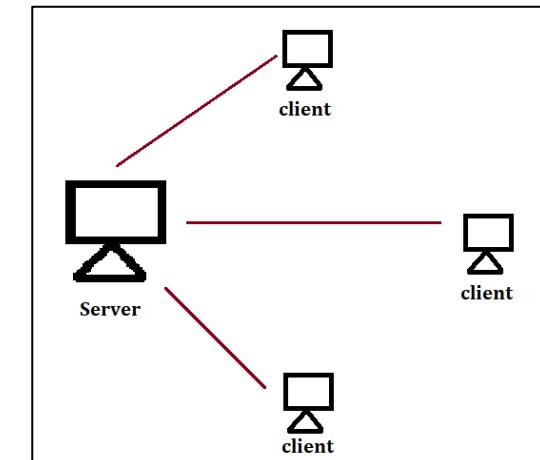
1. Peer-to-peer

- All connected end devices have equal capabilities
- All devices connected to each other without any hierarchy
- If a device fails, impact on network is not so significant



2. Client-server

- A server is a powerful computer that gives services to small powered computers called the clients.
- Each client must first interact with server for transmission of data.
- If server fails, network is highly affected



Client-server Architecture	Peer-to-peer Architecture
This architecture focuses on information handling and sharing	This architecture focuses on connectivity
Clients and servers have different specifications	All peers have non-differentiated specifications
Data storage is mainly done in server	Each peer is capable of independent storage
Server responds to the client requests	Each peer can request and respond freely.
Network fails if server crashes	Network can still survive if a peer crashes
Costlier arrangement	Cheaper arrangement than C-S architecture
Can be used in smaller and larger networks	Used for smaller networks (<10 computers)

D. Based on Network Topologies

- Bus
- Ring
- Star
- Mesh
- Hybrid

Bus topology

- All computers connected to a single cable (bus)
- One computer transmits message, other computers listen.
Only the correct recipient computer accepts the message
- Remarks

Easy installation

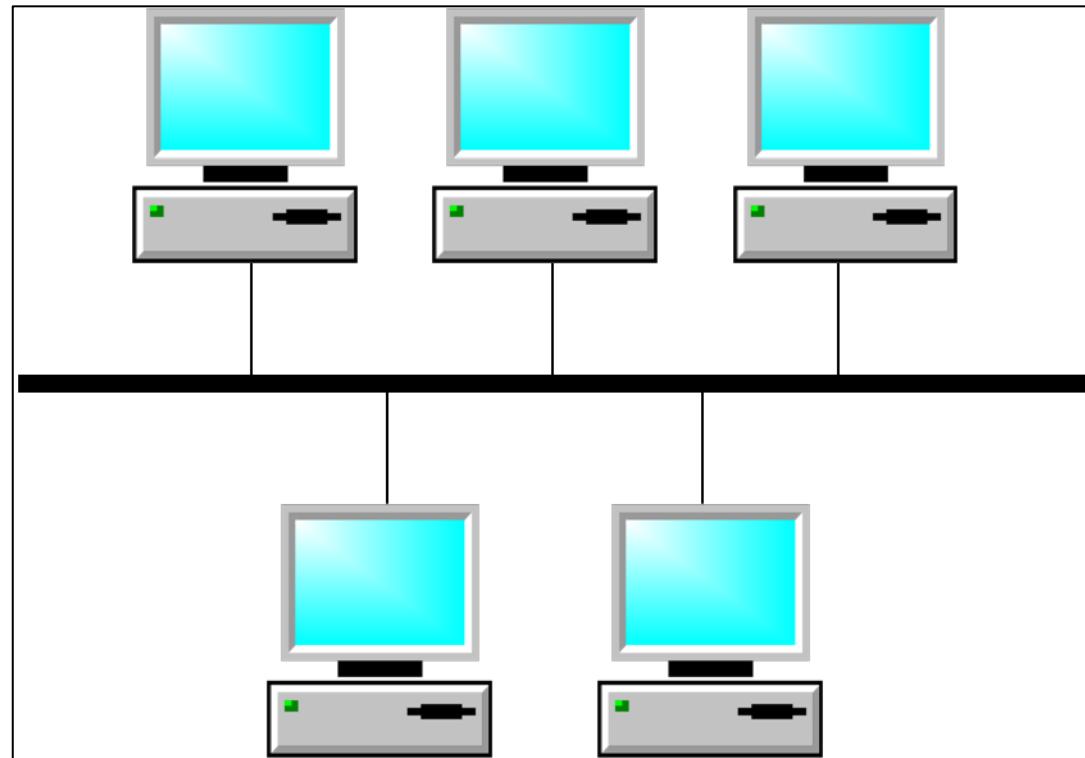
Cheap in cost.

Very useful for small networks

Data Bandwidth is wasted

Failure of cable brings whole network down

Expansion of network is difficult
(can be done using repeaters though)



RING topology

- Each computer connected to another computer to form a ring-like structure.
- Messages flow around in a specific direction.
- Use of *tokens* to indicate which computer wishes to send message to whom.

Fair share of network among computers

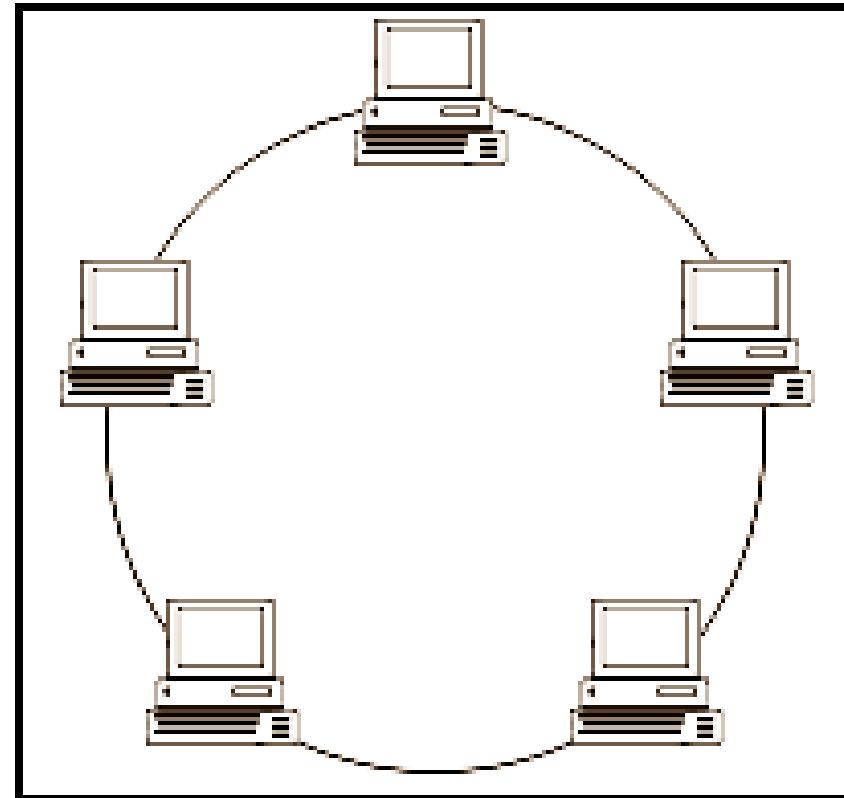
QoS can be achieved.

Each computer act as repeater for transmission

Adding new device is difficult

If a computer breaks, network is affected.

Difficulty in troubleshooting.



STAR topology

- All computers connected to a central device (Hub)
- One computer transmits message to hub,. The hub then broadcasts msg to other computers.
- Remarks

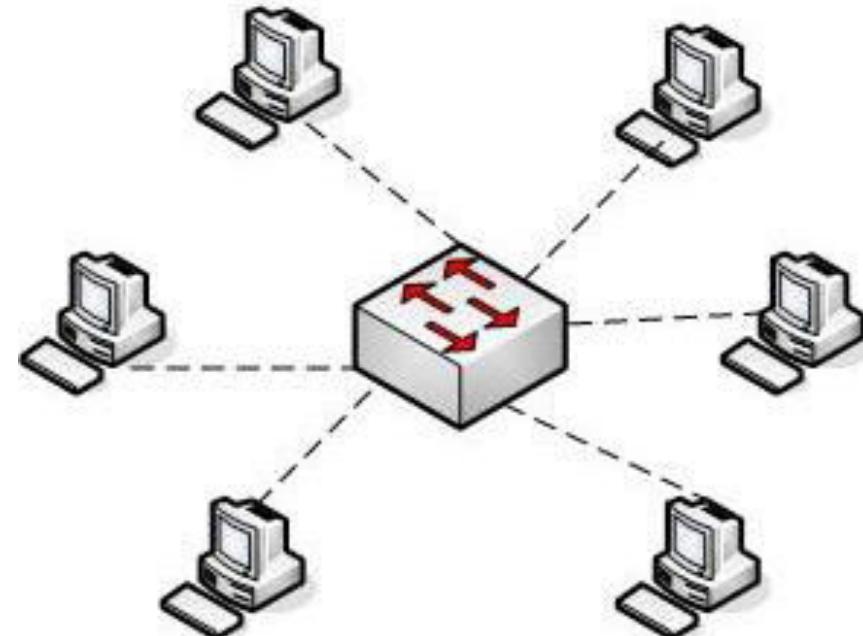
Good utilization of bandwidth

Devices can be easily added

Troubleshooting a node is easy

Network fails if hub crashes.

Cabling cost increases.



TREE topology

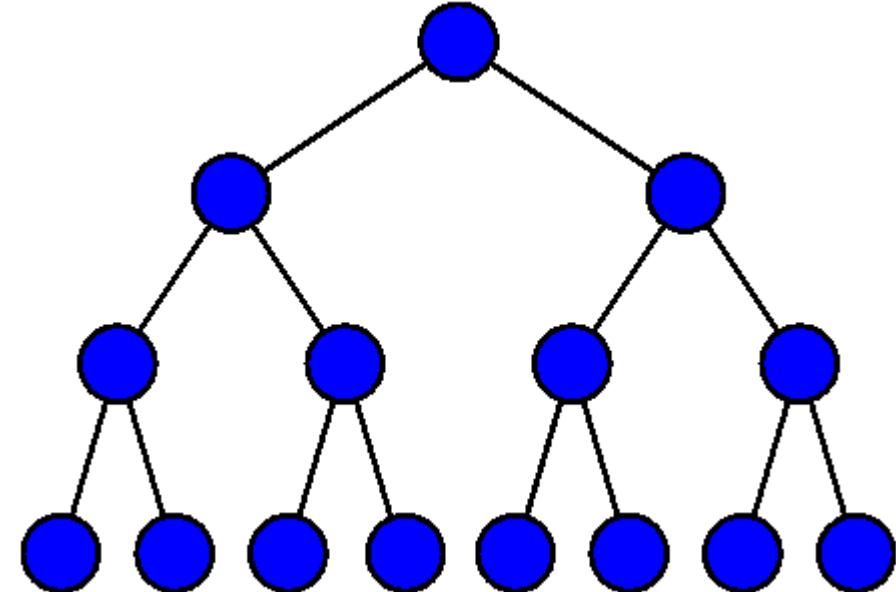
- Variation of star topology
- Computers are connected to secondary hubs, which are connected to a root hub (central)
- Remarks

Allows more device to attach to a hub

Computers can enjoy different priority facilities for communication

If central hub fails, system breaks down

Cabling cost increases



MESH topology

- Each computers connected to every other device
- A dedicated link established among each computer

- Remarks

No data traffic problem

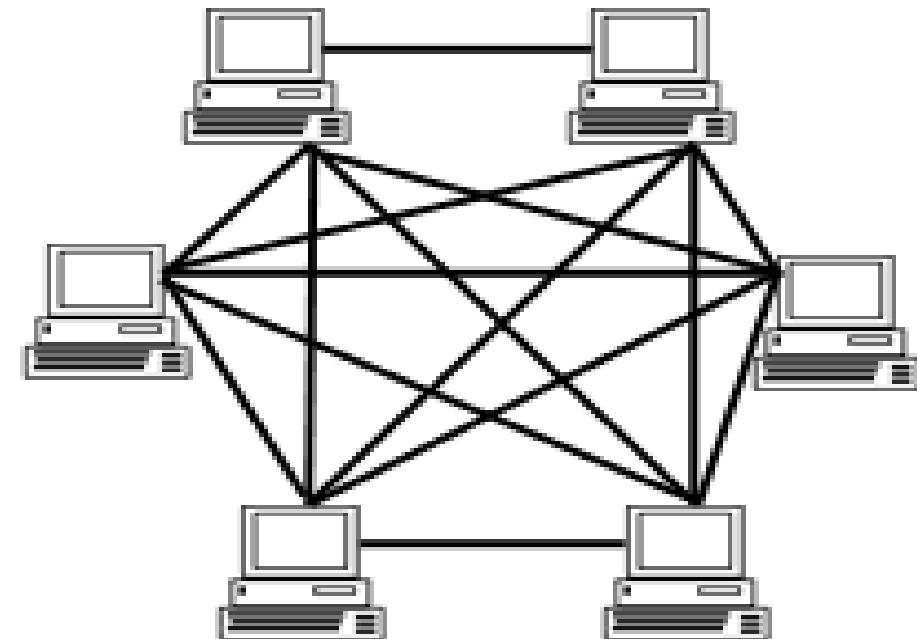
Failure of single computer doesn't affect n/w

Fault detection is easy

Adding new device is difficult

Expensive, since cabling cost increases

Mesh Topology



HYBRID topology

- Combination of two or more topologies
- Usually implemented for WANs or MANs (practical networking)

- Remarks

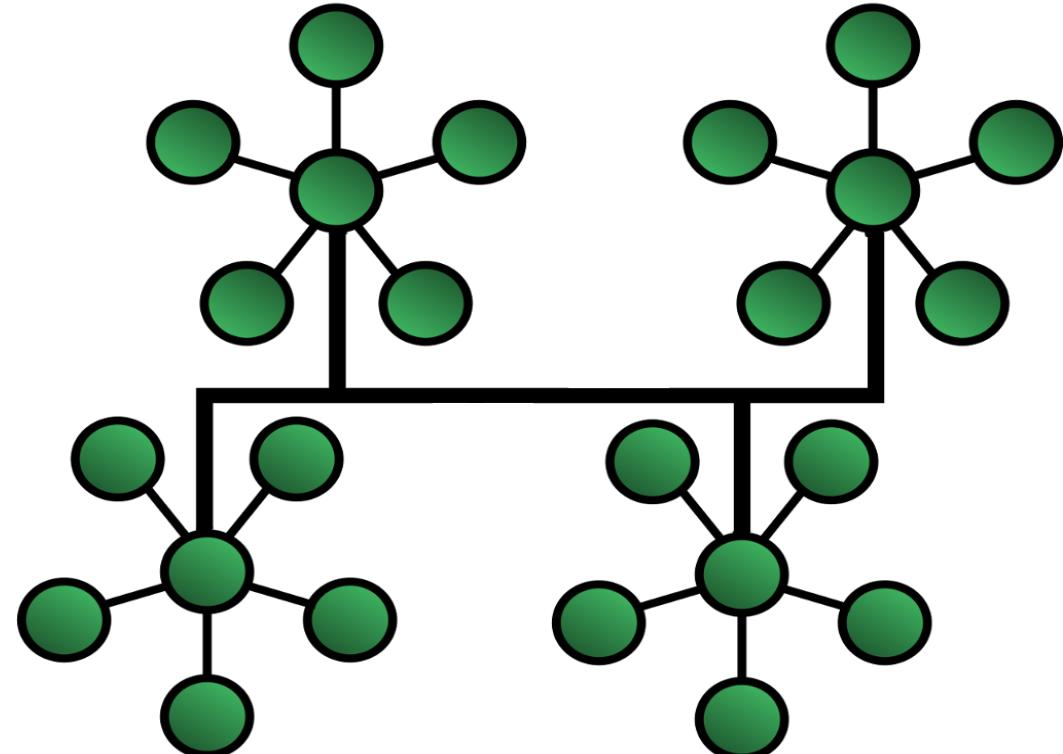
Can contain huge amount of nodes

Very useful for large scale networks

Cost issue

Dependent on requirement & demands

Expansion of network is difficult
(can be done using repeaters though)

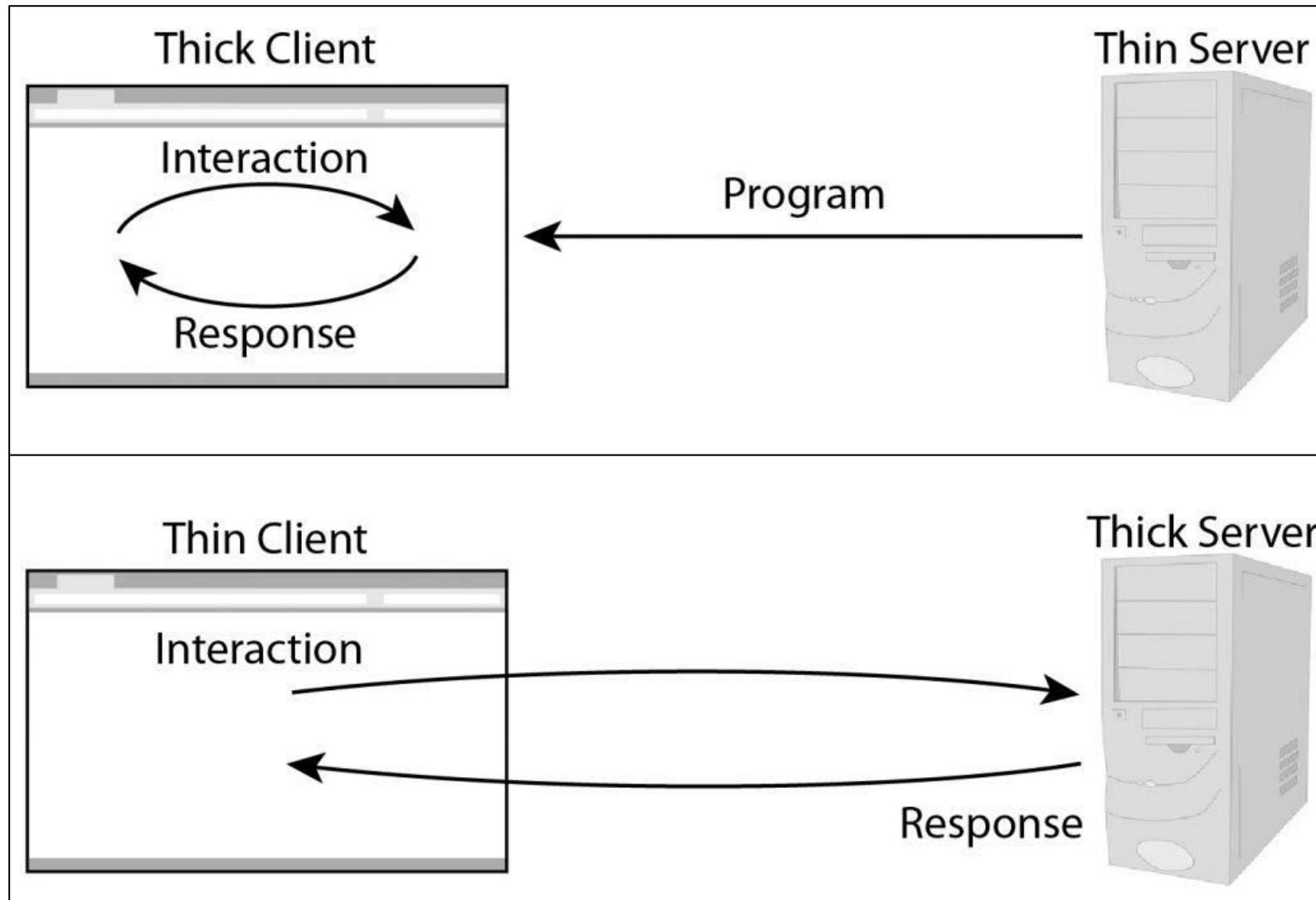


Parameters	Bus	Ring	Star	Mesh
Network Performance	Small	Small or Large	Small	Small
Cable Length Requirement	Less	Neither less nor	More	More
Traffic	Less	High	Medium	No
Dataflow Efficiency	More	Neither less nor more	More	More
Failure	Easy to solve	Difficult to solve	Easy to solve except hub/switch fails	Easy to solve
Cost	Low	High	High	High

If you want to learn about the topologies in easier language, visit the following site:
<https://www.geeksforgeeks.org/types-of-network-topology>

1.3 Network architecture and OSI model

- How network entities are placed and how interactions occur
- Architecture is divided into 2 types:
 - Peer to peer architecture
 - Client server architecture
- Variation of these architectures are also seen in networking world
 - Thin client architecture – A **thin client** runs from resources stored on a central server instead of a localized hard drive.
 - Fat client architecture – A fat client (also called **thick client**) computer provides **rich** functionality independent of the central server.



OSI model

- Open system Interconnection
- A model that is made to ensure that nationwide and worldwide data communication systems are uniform and compatible to each other.
- All the standards made by international group has been developed by looking into the framework prescribed by the OSI model.
- It defines the concept of layered network architecture.
 - It addresses well defined layers that describe what happens in each stage in the processing of data for transmission.

Benefits/importance of OSI

- It breaks the network communication into smaller, more manageable parts
- It standardizes network components to allow multiple vendor development and support
- It allows different types of network hardware and software to communicate with each other.
- It prevents changes in one layer from affecting in other layer
- Dividing a huge process into well defined sub-layers makes it easier to understand the data transmission process

OSI model layers

- Application layer
- Presentation layer
- Session layer
- Transport layer
- Network layer
- Data link layer
- Physical layer

➔ All People Seem To Need Different Pizza

1. Application layer

- Application software issue communication service request such as database access, email and file transfer
- This later provides file transfer access and management services on a remote computer
- Provides basis for email forwarding, database access.

2. Presentation layer

- It handles syntax and semantics of information exchanged between 2 systems
- It translates data into various format as recognized by network and computer (ASCII)
- It is responsible for protocol conversion, encryption & decryption, data compression etc.

3. Session layer

- It is responsible for establishment, maintenance and synchronization of interaction session between communicating systems
- It allows 2 systems to open a dialogue
- The transmission data stream is synchronized

4. Transport layer

- It is responsible for source to destination delivery of entire message
- It ensures that the whole message is sent or arrived intact and in order
- Division of message into packets
- It performs segmentation of message with sequence number
- Provides flow and error control services on both ends

5. Network layer

- It delivers packets from source to destination
- It translates logical network address into physical machine address
- It determines Quality of Service by determining the priority of message and determining the optimal route for its destination.
- If a packet is larger, it is broken into smaller packets

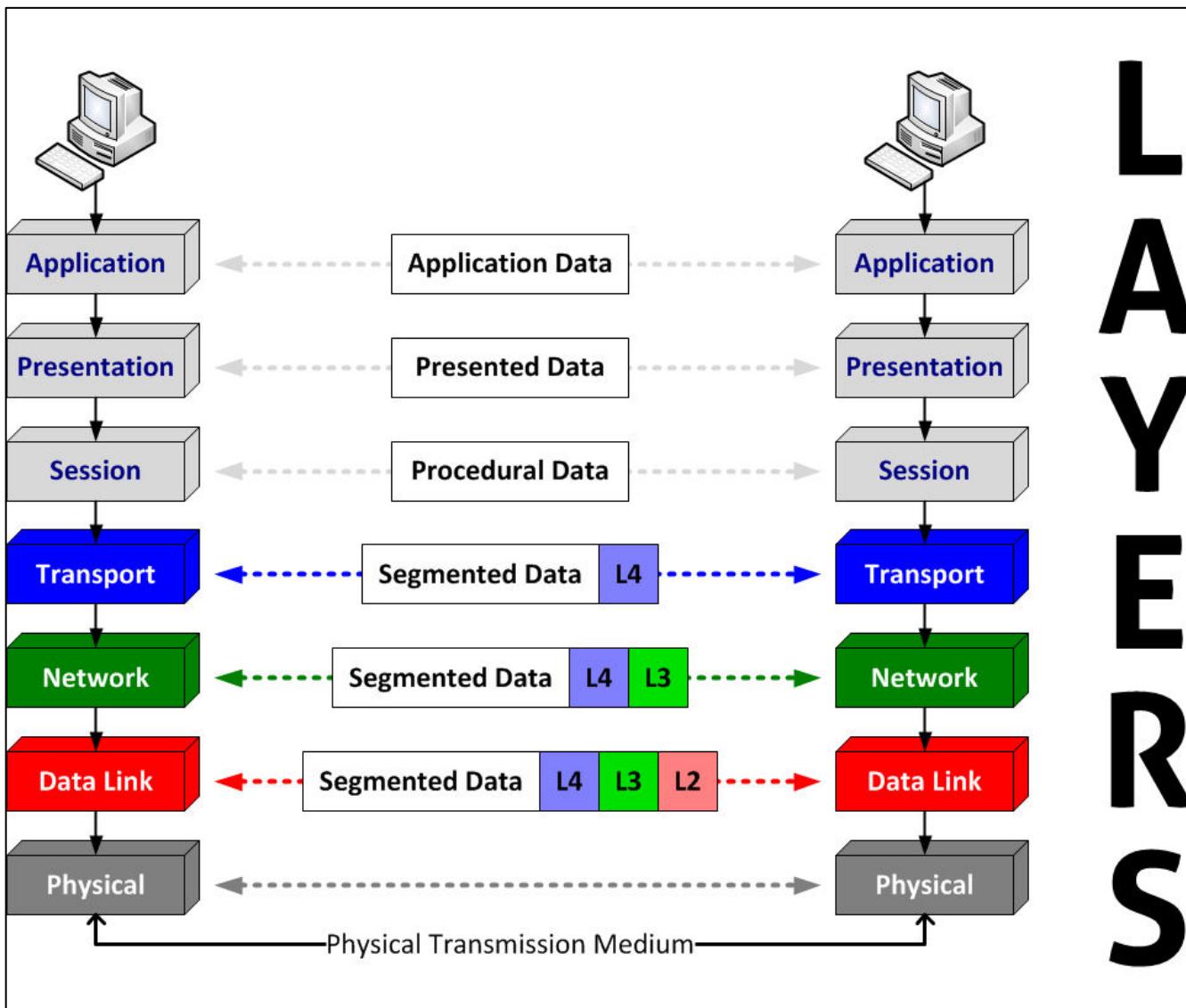
6. Data link layer

- It accepts packets from network layer, forms frame, and transmits frames to physical layer
- It makes header values to frame to define the sender and receiver
- It imposes flow control mechanism
- Node-to-node delivery of data
- It consists of MAC address (Media Access Control) to establish logical link between 2 computers

7. Physical layer

- Physical mechanism by which data are passed from one point to another
- Information are sent on bit by bit process
- It deals with physical connection to the network and with transmission and reception of signals.
- Data being sent or received are defined in terms of physical/mechanical components, that can be defined as 1 and 0 representations.
 - Some times how many pins will a network have, how data will be synchronized, what are the electrical details, etc are also described.

L
A
Y
E
R
S



1.4 Connection oriented & connection-less architecture

- Connection oriented service is the one where continuous support for connection is required
- Similar to a telephone system, where one needs to establish connection, use it, and then release it
- Data are continuously sent
- Connectionless service do not require consistent connection
- Similar to a postal service, data are injected into network and then their order are later arranged.
- The order of message arrival can be different

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

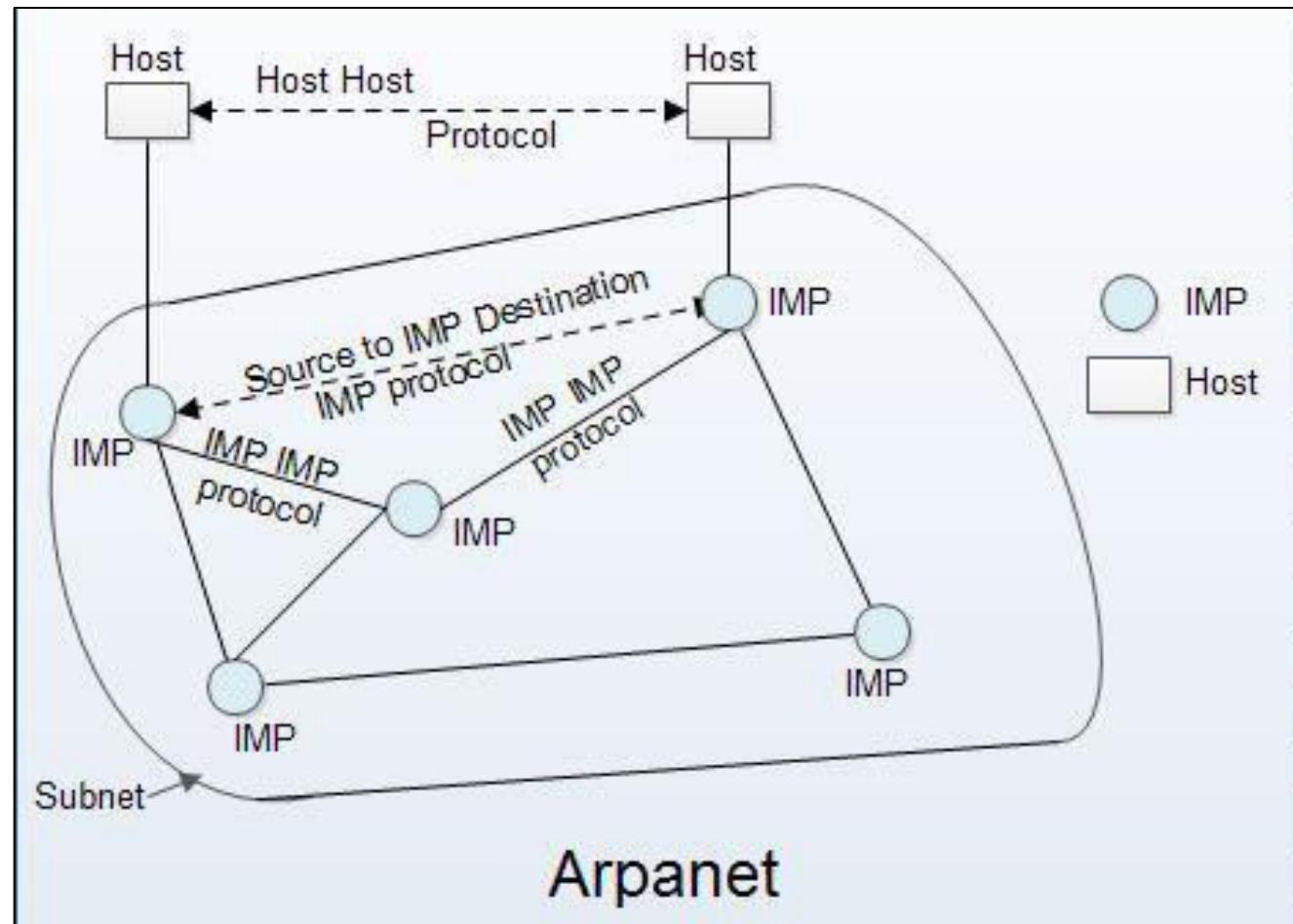
1.5 Private networks example: ARPANET

- ARPANET stands for Advanced Research Projects Agency NETwork.
- It is a WAN technology developed by **Do**f **D**efence (DoD) to service the military operations.
- Before ARPANET, networks were basically the telephone networks that operated on circuit switching network (connection-oriented scenario).
 - These networks were too vulnerable since simple problem in line could terminate the entire connection
- ARPANET introduced the packet switching network technique (connection-less scenario) that uses subnet and host computers.
- It was also the first network ever to implement a protocol suite(TCP/IP).
- This was the breakthrough that paved path for modern day internet.

How does ARPANET work?

- ARPANET uses concept of packet switching that consists of subnet and host computers.
 - Subnet (subnetwork, a part of a large network) consist of mini-computers called the Interface Message Processors (IMPs). These subnet are used to interconnect the local resources.
 - Host computers are the computer systems that seek to access or send particular information at a particular time.
- ARPANET components are connected using physical wire.
- The host would send messages upto 8063 bits to its IMP, which would then break the message into packets and then forward them independently towards the destination.
- The subnet could store each packet and then forward it towards the destination via suitable route.

- Slowly more and more networks were added into ARPANET.
- As the network size increased, the need to monitor and guide the network was felt strongly.
 - The host management was getting tedious.
 - Thus the foundation of TCP/IP protocol suite was laid.
- Machines were organized into domains and the host names were given IP addresses. Both of these components were mapped using DNS(Domain Naming System)



Features of ARPANET

Advantages

- Service was so reliable that it could serve even in a nuclear attack!
- It could support email and other data communication services
- Better data transmission mechanism
- Secure defense against the communication problems of that time

Disadvantages

- As the number of LANs increased, management became difficult
- Implementation cost was higher
- While it itself was an advancement in technology, it could not cope up with other forms of advanced technologies.

End of chapter 1

Important questions (Assignment 1)

(Assume each questions of 10marks)

- Mention Features, pros and cons of computer network
- Explain in brief various network topologies
- Describe the kinds of network architecture (peer to peer, c-s architecture)
- Mention the features of OSI model. Explain in short the layers of OSI model.
- Compare between connection-oriented and connection-less services
- Write short notes on
 - ARPANET
 - Client-Server Architecture
 - OSI model



Chapter 2

Local Area Networks

4 hours

~ 6-8 marks

Chapter overview

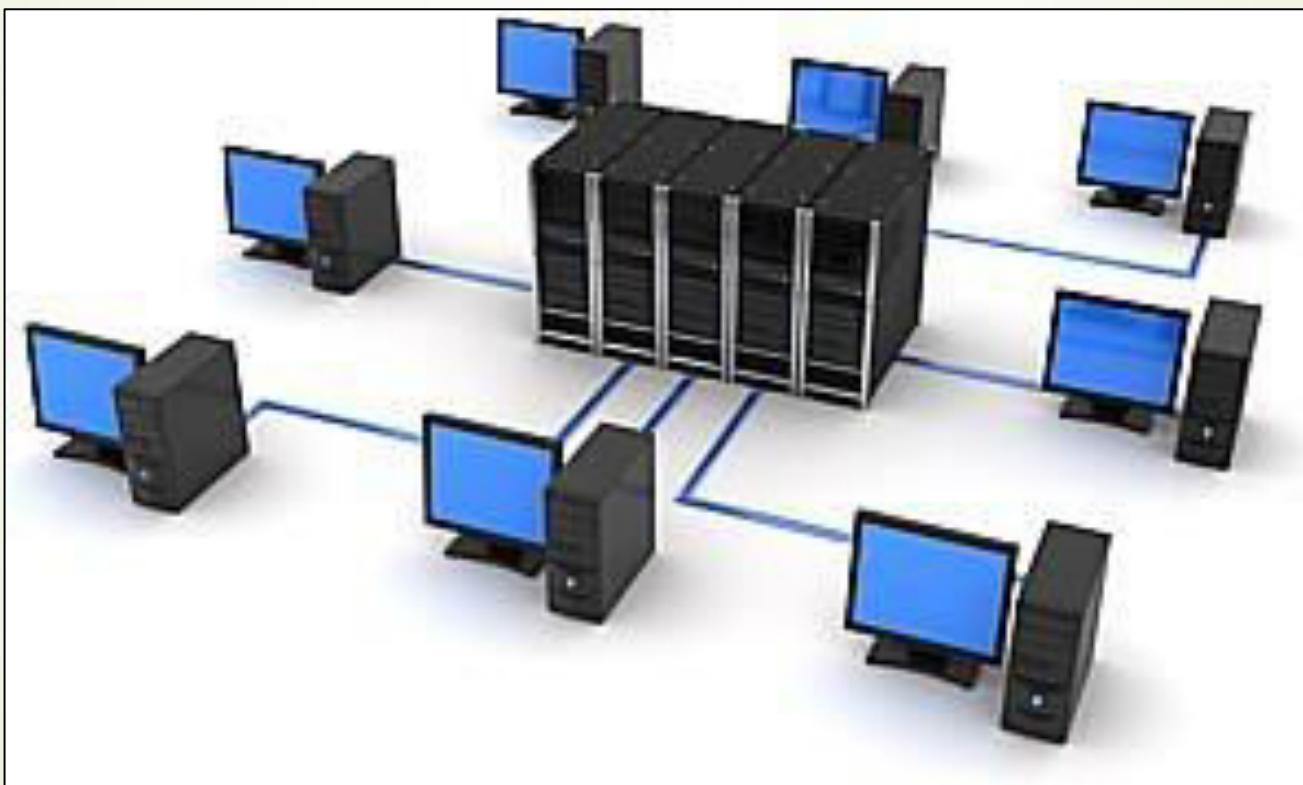
- Lan concepts
 - Network server & Workstation
- Network hardware
 - Cable types, Hub, RAID, Local and Network Printers
- LAN Schemes
 - CSMA/CD
 - IEEE 802.3 standards
 - Wireless LAN (WLAN) & 802.11x standards

2.1 Basic LAN concepts

Network Servers

- ❖ A server is a computer program that provides services to other computer programs (and their users) in the same or other computers.
- ❖ These computers have huge processing as well as storage capabilities.
- ❖ Servers are used to manage network resources.
 - For e.g., a user may setup a server to control access to a network, send/receive e-mail, manage print jobs, or host a website.
- ❖ **Network servers** are computers that are used as the central repository for data and various programs, and are shared by many users within the network.

5



Why network server is used?

- ❖ Most of the important/common files are stored in server, making it a central repository.
- ❖ Ease of access (connect to network, get permission from server, and you're good to go!)
- ❖ Other computers need not worry about management or organization of data.
- ❖ Collaboration works are heightened by the use of network server.
 - ❖ Multiple users can make changes to the same document.
- ❖ Network servers help to improve file management and security.

Role of network servers

1. Grant network permissions and log-ins for authorized users.
2. Allow access to/gateway to the Internet for a business or an organization.
3. Act as a centralized location to store files.
4. Grant and manage access to shared devices on the network like a printer or a scanner.
5. Perform works as a place to host a multi-user applications for the business.
 - ▶ E.g.: email servers, Wikipedia or webpage-type applications, CRM or financial packages.

Workstation

- ▶ A workstation is a user computer that is used in an organizational domain.
- ▶ It has better capabilities than a general Personal Computer.
 - ▶ E.g. better display, better RAM specs, and drive storage.
- ▶ It has multitasking ability so as to share network resources and work in collaborative environments.
- ▶ Workstations usually are built with an optimized design for complex data manipulation and visualization.
- ▶ While traditional workstations represented mainframe and mini computers, today micro computers with high performance and better data storage also fall under workstation.
- ▶ Workstations are used for graphics related works, telecommunication & networking, grid computing, etc.

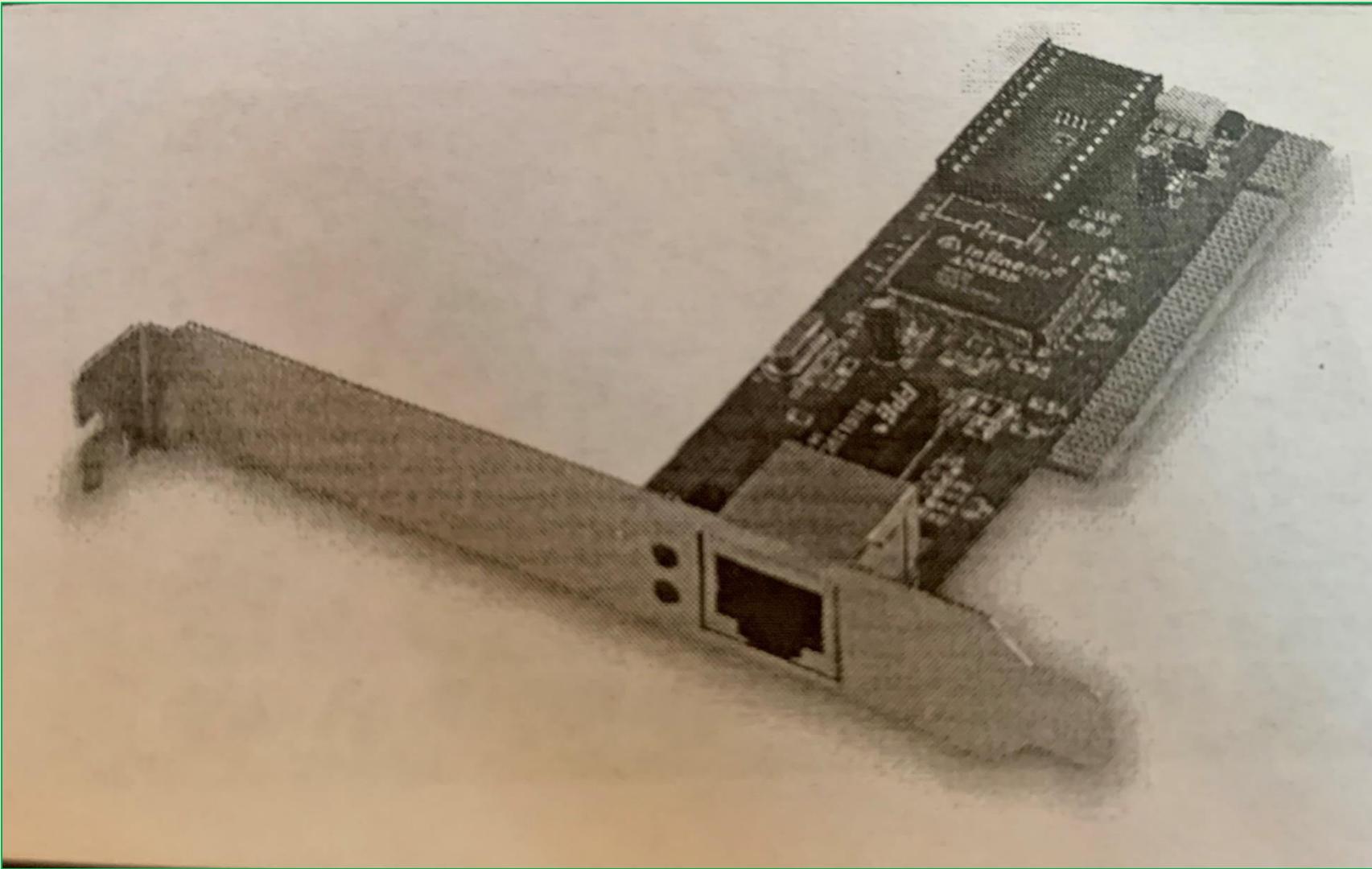
9



2.2 Network Hardware

NIC

- ▶ Network Interface Card
- ▶ A hardware that is designed to connect computers with other networking devices.
 - ▶ It typically supports network cables through which a computer is connected on the network
- ▶ This card is installed in an expansion slot in each computer or built into the system
- ▶ NIC coordinates the information between computer and network.
- ▶ Each NIC is assigned a unique MAC address, which is stored in its ROM.
- ▶ Functions of NIC are:
 1. To prepare data from computer for the network cable
 2. Send and receive data to/from another computer
 3. Control the flow of data between the computer and the cable system.



Networking Cables

- ▶ Cables are the transmission media through which data travels from a source to a destination.
- ▶ Also called as communication media
- ▶ Transmission cables are categorized as the guided media, because the signals have a direction to flow on.
 - ▶ Because of this feature, chances of data being lost is low as compared on unguided/wireless media.
- ▶ There are 3 types of wires being used for networking:
 - a) Twisted pair cable
 - b) Coaxial cable
 - c) Optical fiber cable

1. Twisted pair cable

- ▶ The oldest and still most common transmission media
- ▶ It contains a group of pair of cables, twisted with each other.
 - ▶ Tighter the twisting cables, higher the transmission rate
- ▶ It is used for various networking scenario, from telephone system to the Ethernet cable.
- ▶ Twisted pair can only run few meters without amplification, but for long distance, requires repeaters.
- ▶ Cheaper, lighter, thinner, and easier to install.
 - ▶ Hence it is an ideal choice in small offices or small networks.
- ▶ There are 2 kinds of twisted pair: shielded and unshielded.

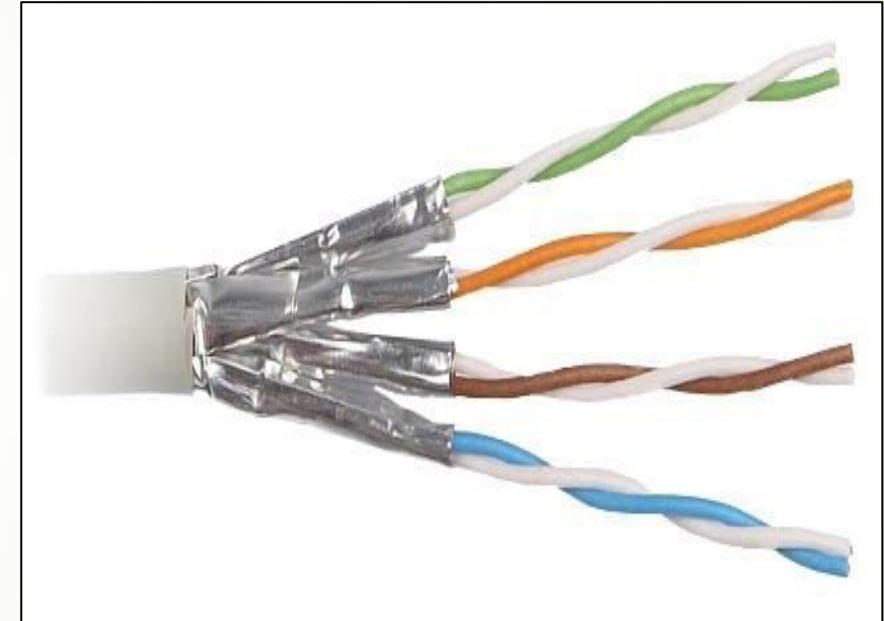
Unshielded Twisted Pair (UTP)

- ▶ Most common form of Twisted pair cable.
- ▶ Its twisted pair do not have extra protection contents as compared to its other variation (STP)
- ▶ It has 4 pairs of copper wires that are present inside a plastic sheath.
 - ▶ This sheath is the only protection mechanism to protect the wires.
- ▶ Cheaper in cost, but may experience crosstalk.
- ▶ Used as cable for modern Ethernet system as well as connecting medium for video applications such as security cameras.

Shielded Twisted Pair

- ▶ A shielded twisted pair contains an extra metal foil outside the plastic cover of each pair.
- ▶ It can carry data signal for longer distance
- ▶ Susceptibility to cross talks or EM interference is lower than UTP
- ▶ Expensive.
- ▶ Used by larger organization that can spend some extra amount for reliable wiring systems.
 - ▶ E.g. telephone wiring systems.

UTP and STP



Twisted Pair Analysis

Pros

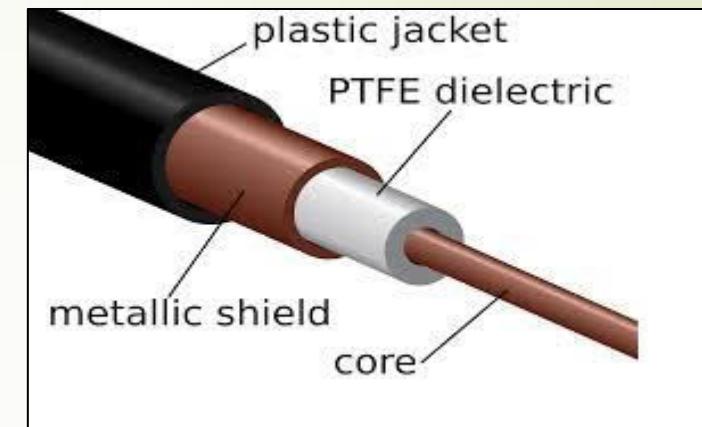
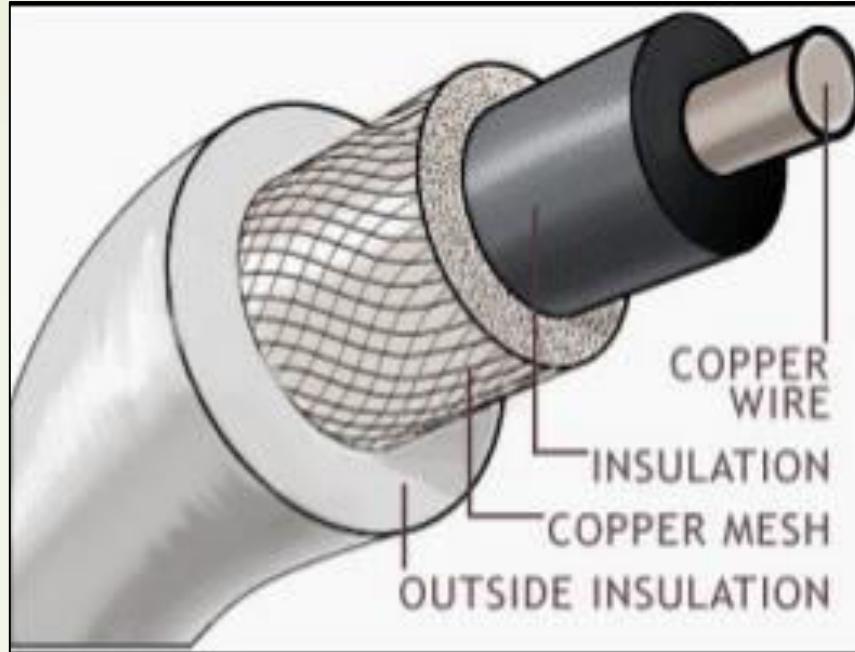
- ▶ Easy to install
- ▶ Cheap
- ▶ Works well for short distances
- ▶ Cost-performance ratio is satisfactory
- ▶ Has a wide application

Pros

- ▶ Low bandwidth
- ▶ Chance of crosstalk
- ▶ Susceptible to E-M Interference
- ▶ Low durability
- ▶ Signal gets attenuated at longer distance

2. Coaxial Cable

- ▶ A coaxial cable has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and the outer layers.
- ▶ A braided metal shield layer is present that helps to block any outside interference during transmission.
- ▶ Coaxial cable carries data signal of higher frequency and at faster speed than a twisted pair cable.
- ▶ Its common use is for the transmission of signals in cable television system and broadband internet system.
- ▶ It supports transmission of various signal at the same time.
 - ▶ Each channel travels along at a different frequency. Hence it doesn't interfere with other channels.



Coaxial cable Analysis

Pros

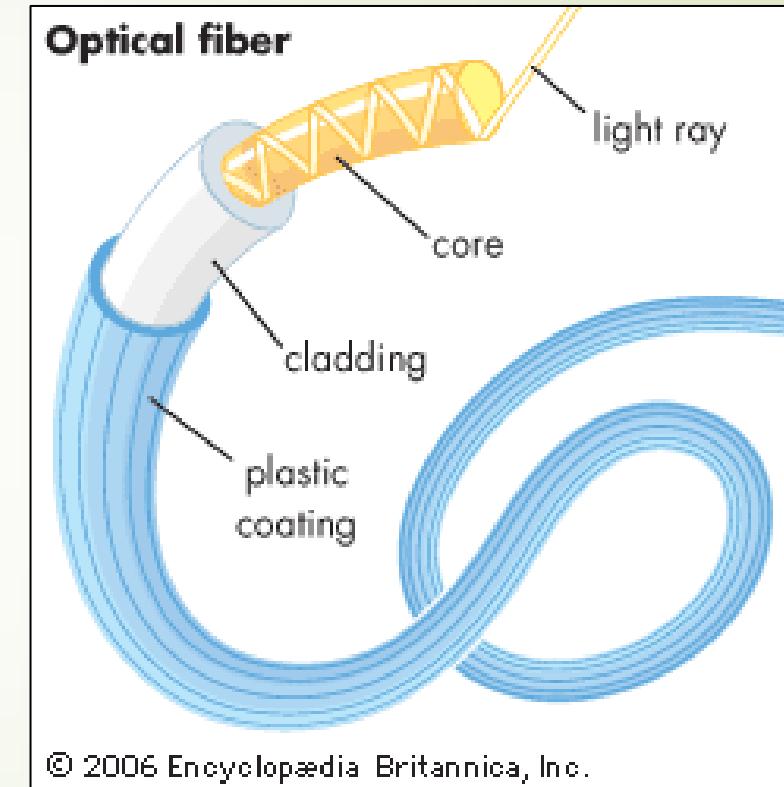
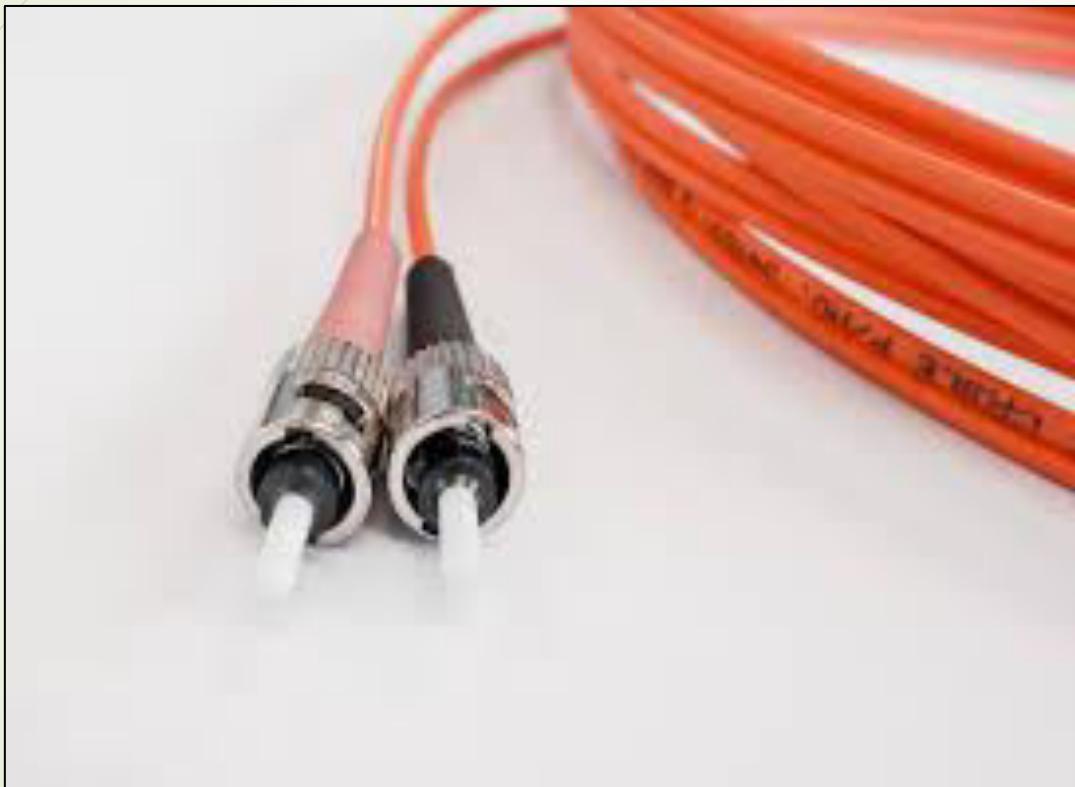
- ▶ Very durable
- ▶ Good bandwidth capacity
- ▶ Best performance for small distance transmission
- ▶ Can carry signals of different frequencies
- ▶ Higher Resistance towards cross-talks and interference

Cons

- ▶ It loses its performance on long distance
- ▶ Chance of signal leakage on connection
- ▶ Bulky dimension makes it difficult to manage

3. Optical Fiber Cable

- ▶ A fiber optic cable is made of glass or plastic and transmits signals in form of light.
- ▶ It contains single or multiple hairs like thin filaments of glass fibers wrapped by a protective jacket.
- ▶ Optical fiber can carry voice, video, and data. It has enormous bandwidth and can carry signals for very long distances.
- ▶ Since it works on principle of optical propagation (Total Internal Reflection), it is immune to electromagnetic interference.
- ▶ Extremely faster, and more secure than other cables



Fiber optic cable Analysis

Pros

- ▶ Better resistance to EMI
- ▶ Performs well on long distance transmission
- ▶ Better bandwidth support

Cons

- ▶ Expensive
- ▶ Difficult to install
- ▶ Needs special care for maintenance
- ▶ Can be damaged easily
- ▶ Light waves get dispersed and attenuated.
- ▶ Requires converter device for long distance transmission

Do-it-Yourself

- ▶ Perform a tabular comparison of various kinds of networking cables (based on cost, ease of implementation, supported distance, bandwidth, protection against interference, crosstalk scenario, application scope, etc.)

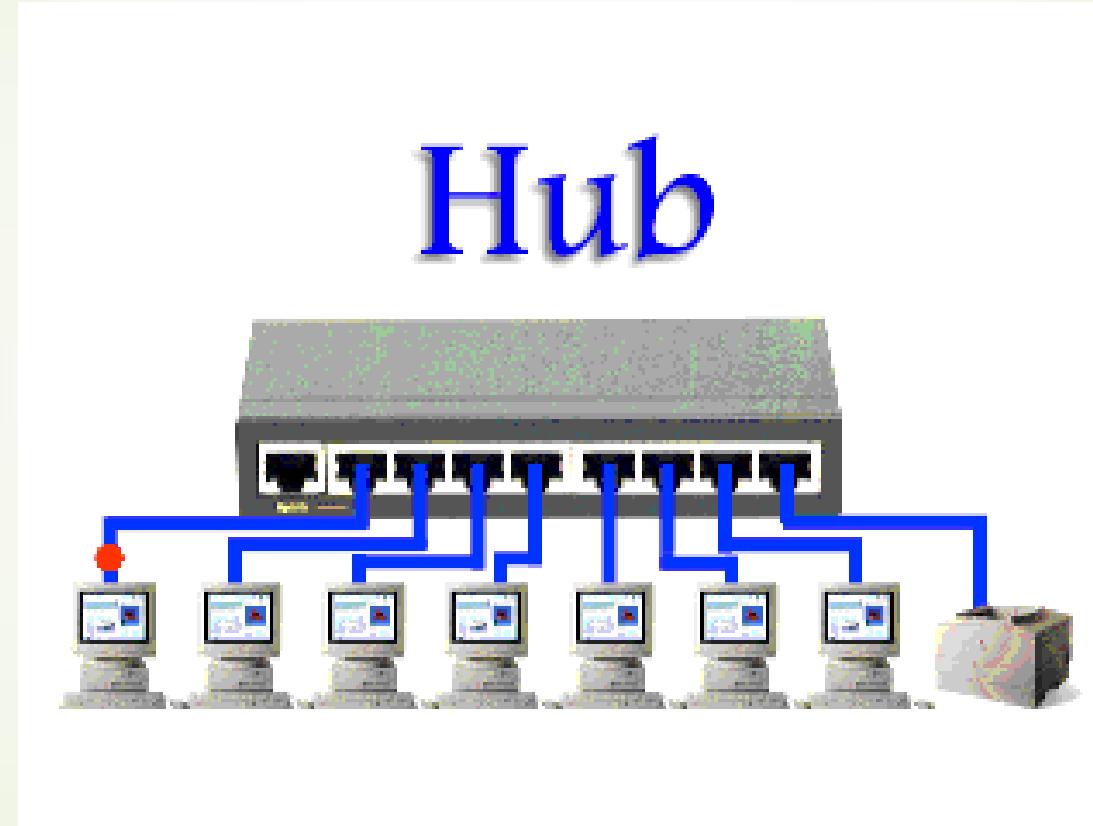


Hub

- ▶ A hub is a connectivity device with multiple ports for connecting computers.
- ▶ It is a central communicating device for star topology.
- ▶ It accepts data, amplifies them and broadcasts.
 - ▶ Any data entering a port is repeated to the output of every other port except the entry port itself.
 - ▶ Due to broadcasting, the data traffic increases.
- ▶ A hub can also split network segments and propagate signals through these segments.
 - ▶ Because of this feature, sometimes it is also called the multiport repeater.

- ▶ While a hub is easier to operate, it cannot filter network.
 - ▶ Hence there is a limitation on number of computers that can be connected or serviced.
- ▶ With reference to the OSI model, a network hub works on physical layer.
- ▶ Hubs are now obsolete, and are now replaced by network switches.

How hub works



30



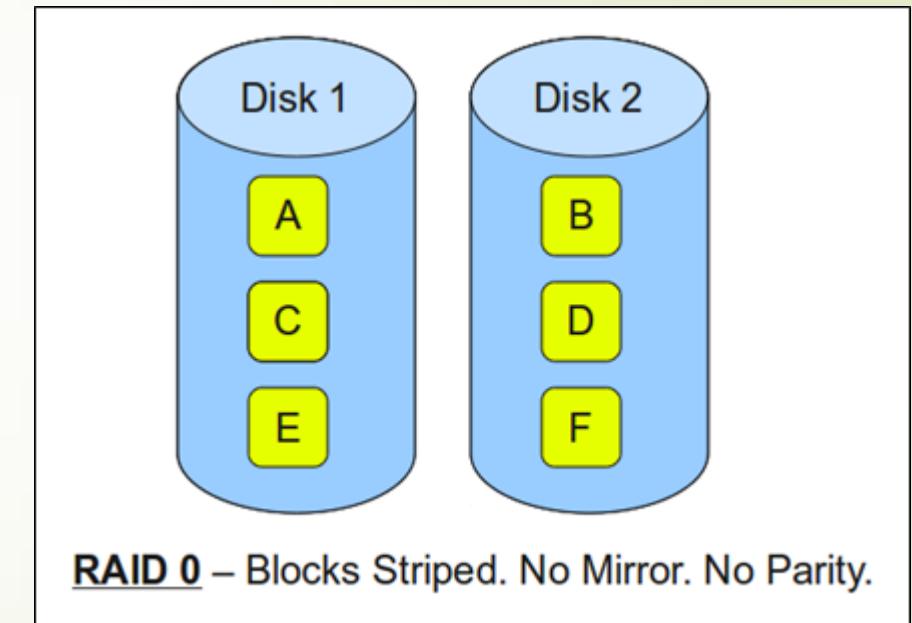
RAID

- ▶ Redundant Array of Independent Disks
- ▶ It is a way of logically putting multiple disks together to form a single array.
- ▶ A technique that makes use of a combination of multiple disks instead of using a single disk for increased performance, data redundancy, or both.
- ▶ Although data redundancy takes up more space, it improves disk reliability.
 - ▶ If same data is backed up on another disk, the load on single disk is reduced.
 - ▶ This means, failure of a single disk wont matter much.
- ▶ Here, data is distributed across the drives in one of several ways, referred to as **RAID levels**, depending on the required level of redundancy and performance.
- ▶ Each RAID level provides a difference balance among various desired attributes: Reliability, Availability, Performance, Capacity, etc.

RAID Levels

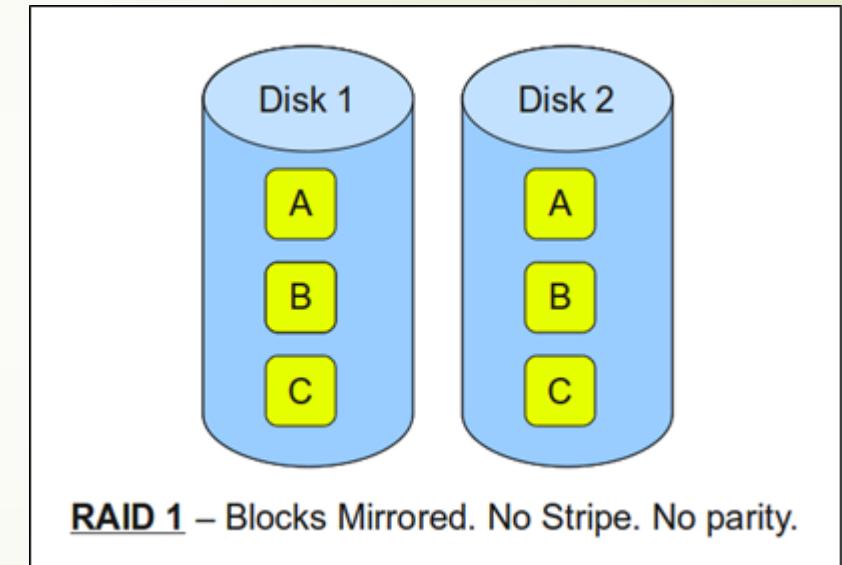
RAID-0 (Striping)

- ▶ Here, blocks are “striped” across disks.
 - ▶ E.g. A,C,E form a strip.
- ▶ Instead of disk working on just one block, a disk can work on multiple blocks at a time.
- ▶ Since most blocks don’t contain any duplicated data, damage of a disk means that data is lost forever.
- ▶ Good thing is, all the disk space is well utilized.



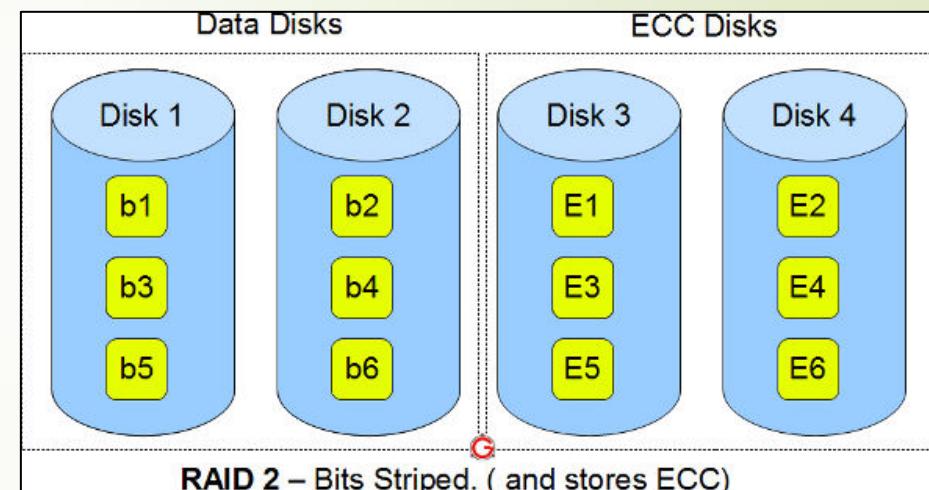
RAID-1 (Mirroring)

- More than one copy of each block is stored on a separate disk.
- Since there are redundant blocks across more than 1 disk, RAID-1 can tolerate some levels of disk failure.
- Only half of the space is being used to store the real data. Hence disk space utility is halved than RAID-0.
- Faster Reading, but slower writing.



RAID-2 (Bit level striping)

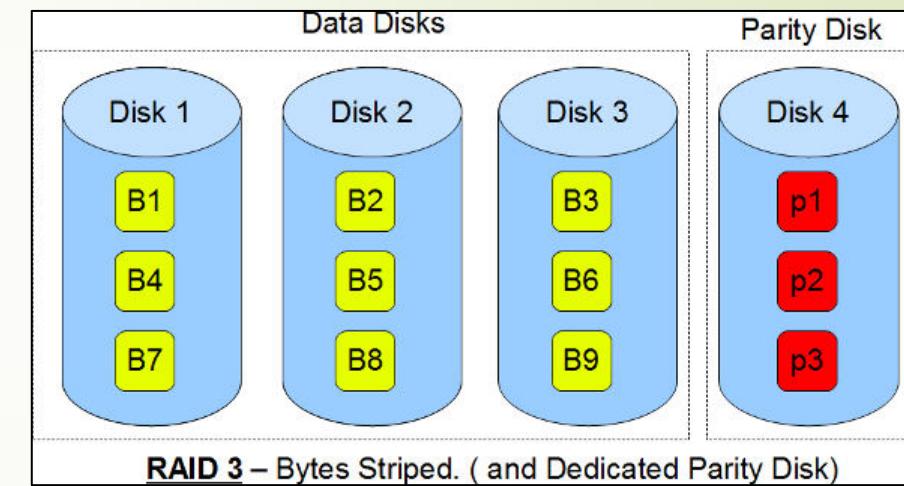
- Here all data are striped into bit level (not block)
- It maintains a separate set of disks for Error Correction Code (ECC).
- When data is written into disks , the ECC code is calculated and then the data bits are striped across the data disks.
- When data is read from the disk, the corresponding ECC is also read to check if the data is consistent or not.
- Allows data reconstruction in case of failure.
- This level uses more disk. Hence it is expensive and complex for implementation.
 - Not used anymore



No. of data disk = no. of ECC disk

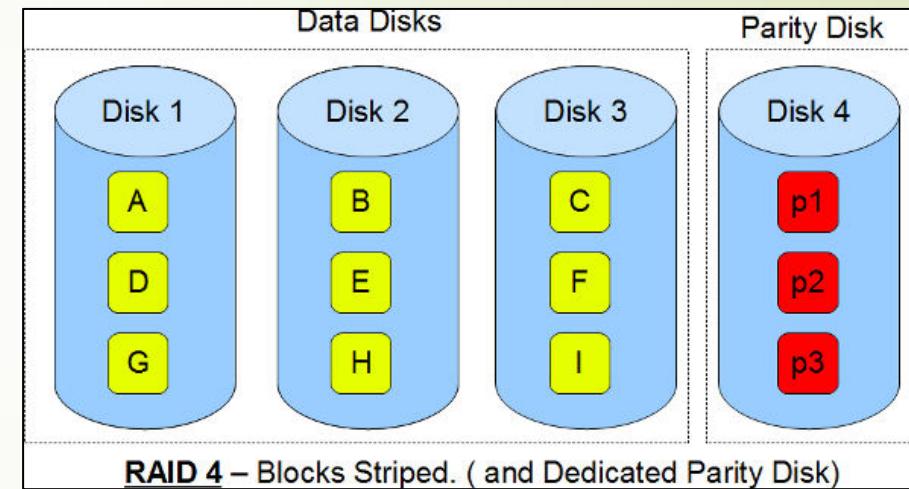
RAID-3 (Byte striping with dedicated Parity Check)

- ▶ Here all data are striped into byte level (not block)
- ▶ Uses multiple data disks, and a separate disk for parity checks.
- ▶ The multiple data disk spin in sync to get the data
- ▶ The parity disk stores parity value for each row of data on disks.
- ▶ In case of failure, it allows to recover data by an appropriate calculation of remaining bytes with parity bytes corresponding to them



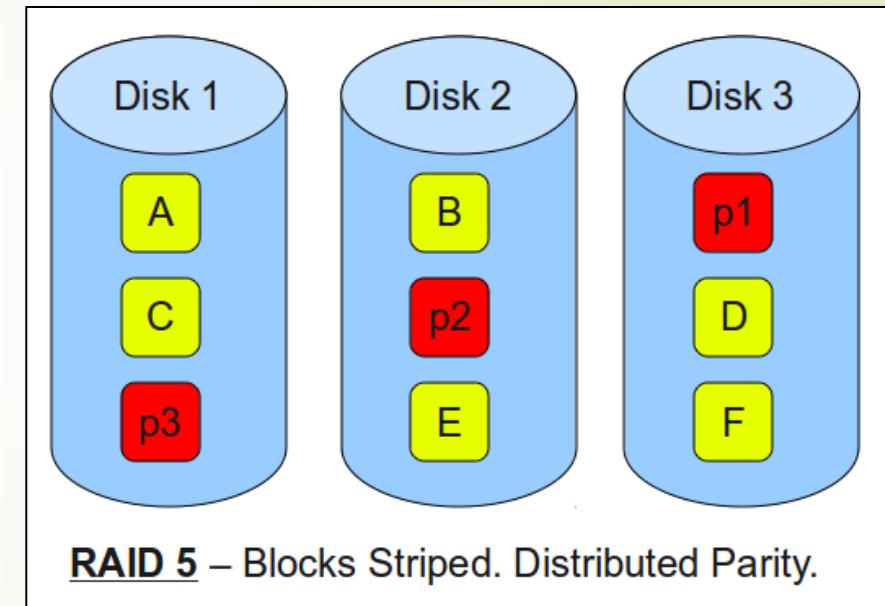
RAID-4 (Block striping with dedicated Parity Check)

- ▶ Block striped working nature.
- ▶ Uses multiple data disks, and a separate disk for parity check.
- ▶ Min. of 3 disks is reqd. in this level (2 for data, 1 for parity)
- ▶ Just like in RAID-3, it works with parity bits.
 - ▶ But here it works on block level
- ▶ Allows re-construction of blocks if disk gets damaged.
- ▶ Requires hardware support for checking parity bits.
- ▶ Not used anymore.



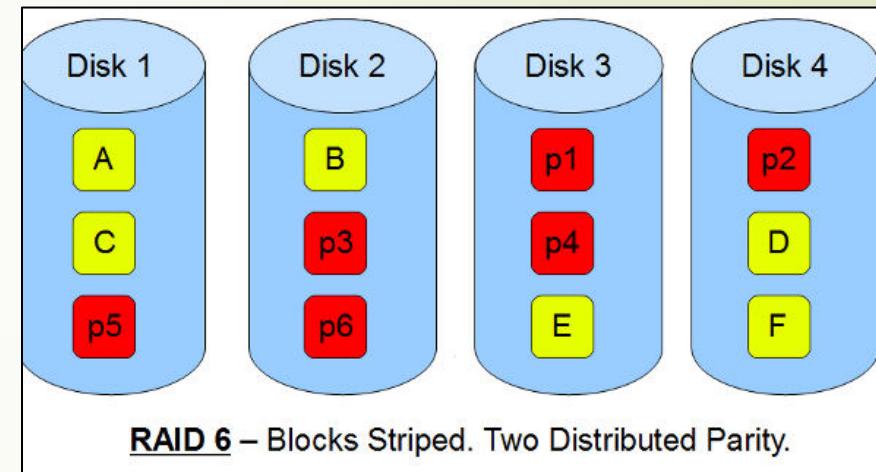
RAID-5 (Block Striping with Distributed Parity)

- ▶ Here, blocks are “striped” across disks.
- ▶ Instead of a dedicated parity disk, the parity values are also written in the data disk.
 - ▶ Each parity value corresponds to row-wise values of data blocks
- ▶ Good performance and good redundancy
- ▶ Data recovery is limited to 1 disk.
 - ▶ If multiple disks fail, reconstruction fails.



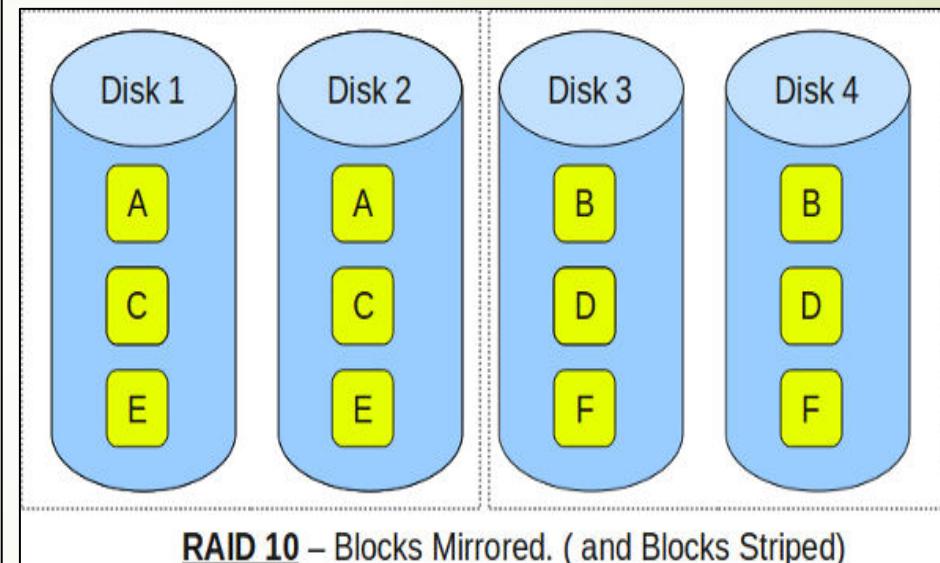
RAID-6 (Striping with double parity)

- ▶ Block level striping with 2 parity values.
- ▶ For each data block, two parity values are created.
- ▶ It can handle simultaneous failure of 2 disks
- ▶ Complex to implement, but has a better reliability than RAID-5



RAID-10 (Striping and mirroring)

- ▶ Also called “the striping of mirrors”
- ▶ Minimum 4 disks are required.
- ▶ Excellent redundancy and reliability
- ▶ Best level to implement if money is not the problem.
 - ▶ Which usually is!



2.3 LAN Standards (Ethernet and Wireless)

CSMA/CD

- ▶ It stands for Carrier Sense Multiple Access / Collision Detection
- ▶ CSMA protocol operates on the principle of carrier sensing.
 - ▶ Here, a station listens to see the presence of transmission(carrier) on the cable and decides to act accordingly.
- ▶ It is a MAC protocol in which a node(computer) verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electric data bus or an electromagnetic spectrum.
- ▶ In a non-dedicated link where multiple systems share the transmission channel, more than one computer may access the channel simultaneously.
 - ▶ In this case collision occurs, and the transmission cannot be finished
 - ▶ E.g. when a teacher asks a question, and all students start answering.

- ▶ Because collisions can occur anytime in a non-dedicated transmission channels, there must be some protocol for sharing information.
 - ▶ CSMA/CD falls under random distribution /access protocol
- ▶ In CSMA/CD, a station monitors the medium after it sends a frame to see if the transmission was successful.
 - ▶ If successful, the station is finished.
 - ▶ If not, the frame is sent again.

Environment for transmission in CSMA

There are 3 scenario for transmission of signal under CSMA:

1. Non-persistent CSMA

- Here, if a station wants to transmit a frame, and it finds that the channel is busy, then it has to wait for certain time.
- After this time, it again checks the status of the channel. If it is free, station transmits.

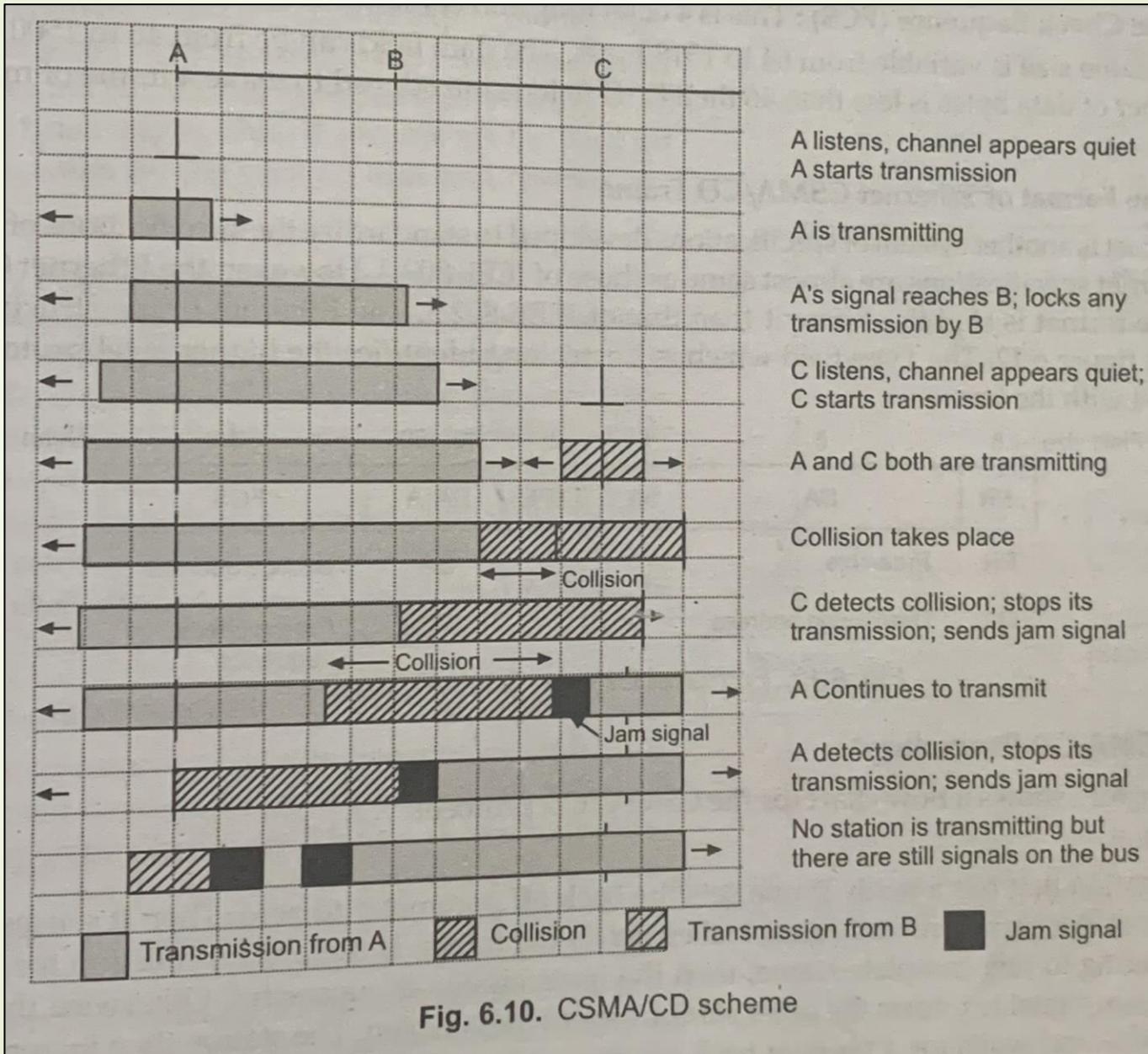
2. 1-persistent CSMA

- Here, the station that wants to transmit continues to monitor the channel
- In any moment where the channel is idle, the station starts transmitting immediately
- If two stations transmit simultaneously, a collision takes place.

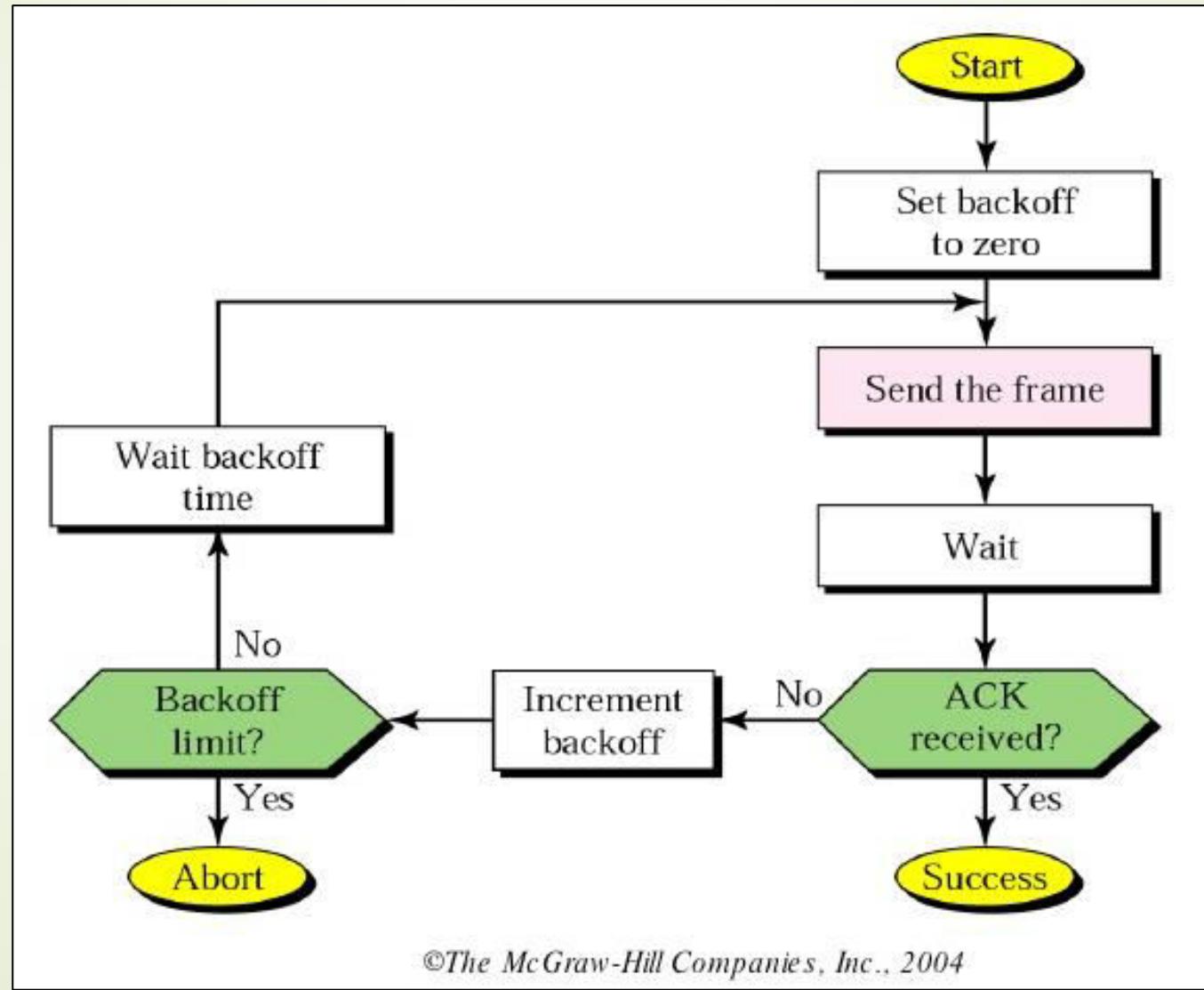
3. p-persistent CSMA

- ▶ Here, the possibility of such collisions and re-transmissions is reduced.
- ▶ If a station wants to transmit, it checks availability of channel.
 - ▶ If channel is busy, it waits till the end of current transmission.
 - ▶ All the waiting stations are allocated a probability **p**.
 - ▶ After the channel is free, it transmits the message
 - ▶ The probability **p** determines whose message is transmitted
- ▶ For e.g. there are 6 computers waiting for a free channel. Then $p=1/6$.
 - ▶ Whenever the channel is free, 1 out of those 6 computers will get the chance to transmit its message.

What happens in CSMA



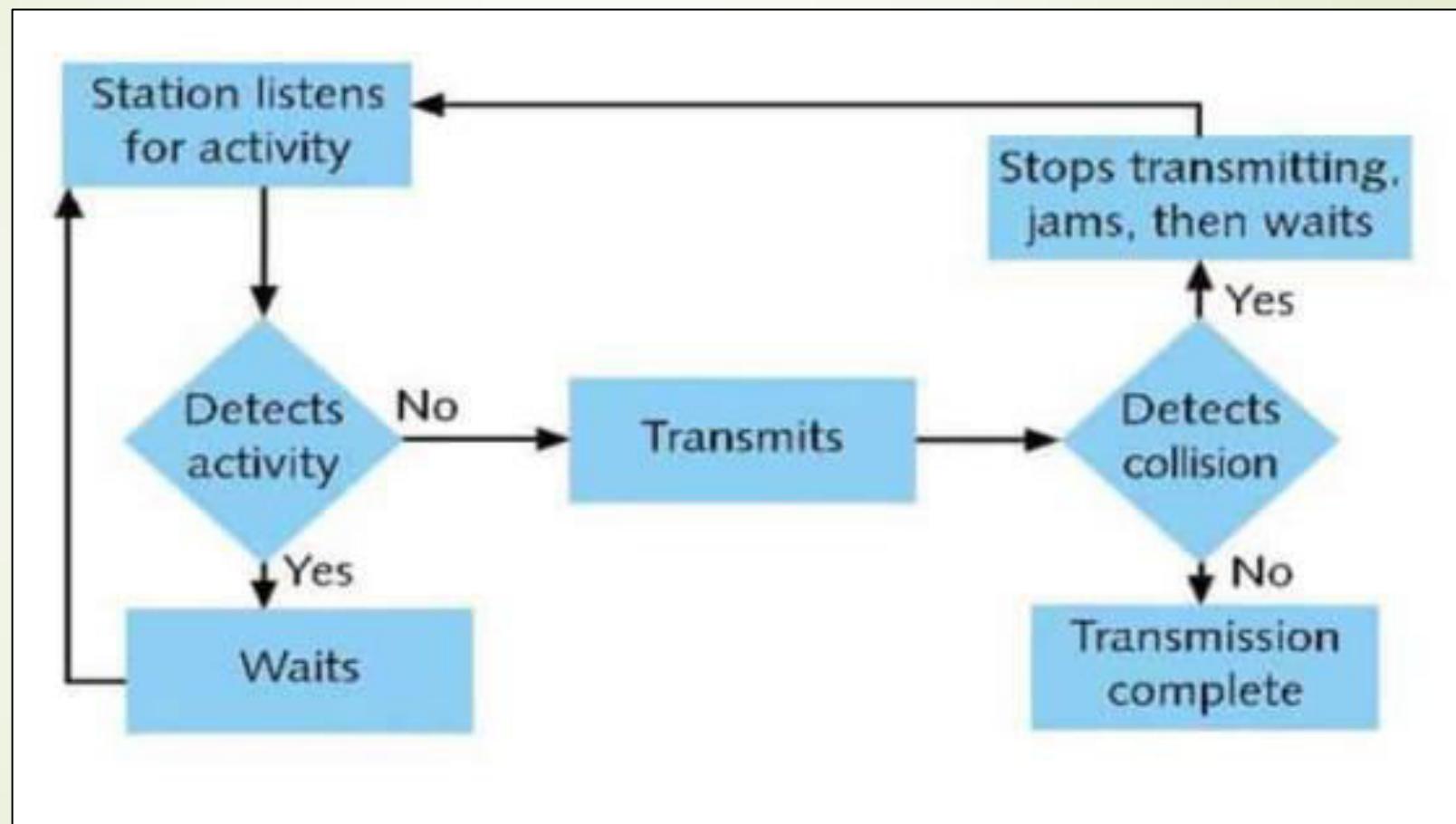
How does CSMA/CD work?



Explanation:

- ▶ The station that has a ready frame sets the back off parameter to 0.
 - ▶ Back off parameter is the time value reqd. to wait because of the collision detected currently on the channel.
- ▶ Then it senses the line using one of the persistent strategies.
- ▶ It then sends a frame.
- ▶ If there is no collision for a period corresponding to one complete frame, then the transmission is successful.
 - ▶ Else, the station has to send a “jam” signal to inform other stations about collision.
- ▶ The station then increments the back off time and waits for a random back off time, and then sends frame again
- ▶ If back-off time has reached its limit, then the station aborts the transmission.

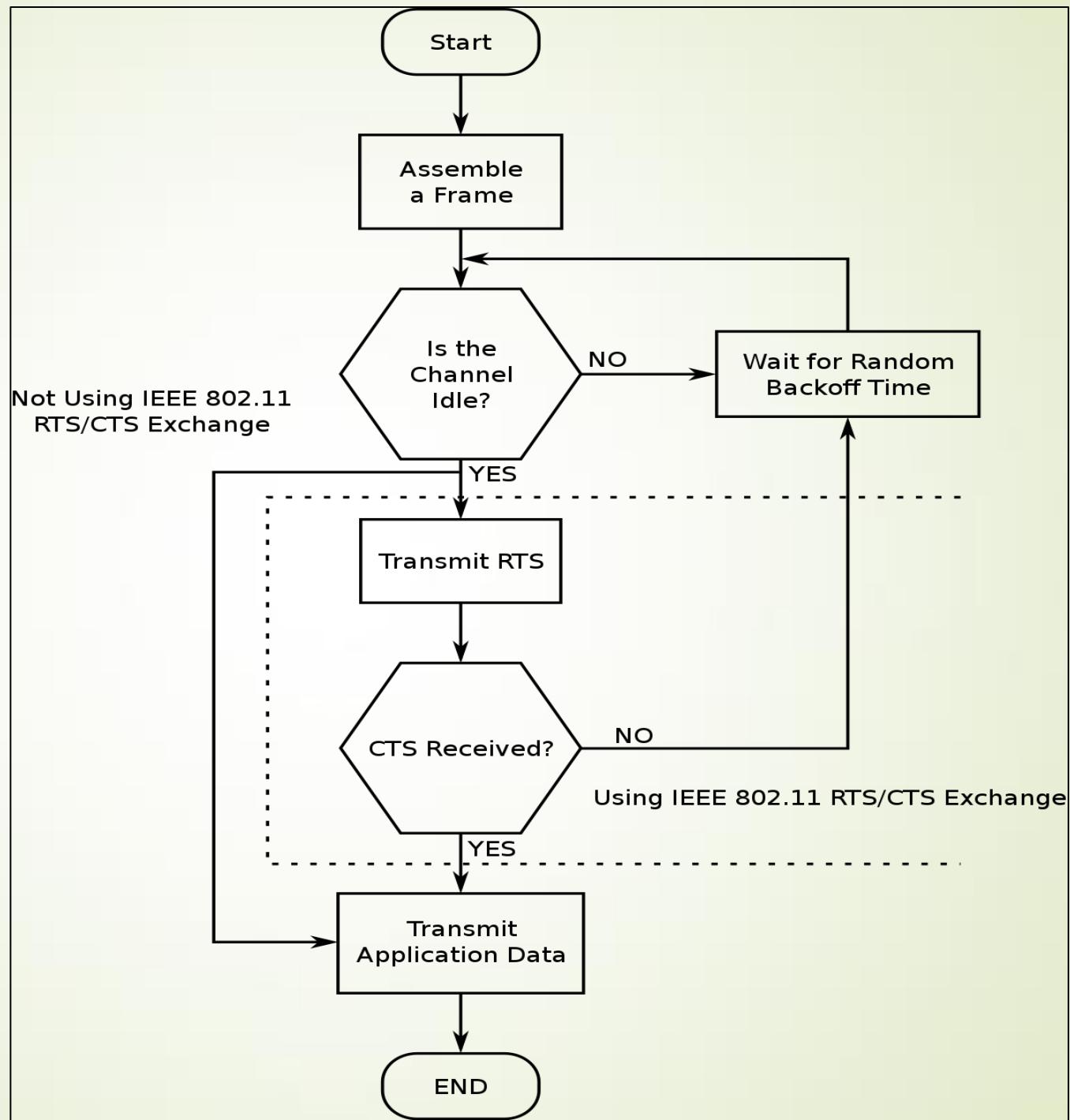
How stations work in CSMA/CD?





What is CSMA/CA

- ▶ Collision Avoidance (CSMA/CA) avoids collisions by listening for a transmission signal before sending data.
- ▶ If a signal is detected, the sender starts a counter with a random value and then waits.
 - ▶ Once this counter runs down, the sender will try again.
 - ▶ This process repeats until the sender can send the data.
- ▶ The part where the transmission waits to send is Collision Avoidance in action.



CSMA/CA vs CSMA/CD

Table 2. The difference between CD and CA

	Definition	Media	Detection way	Utilization rate
Collision detection	Carrier sense multi-access with impact detection, detecting collisions, avoiding conflicts	Bus Ethernet	Detected by voltage changes in the cable (when the data collides, the voltage in the cable changes)	Protocol channel utilization is high
Collision avoidance	Carrier sense multiple access with collision avoidance, while transmitting packets can not detect the presence or absence of conflicts on the channel, only try to "avoid"	Wireless LAN	Energy detection (ED), carrier detection (CS), energy carrier hybrid detection - three ways to detect channel idleness	Low protocol channel utilization

S.NO	CSMA/CD	CSMA/CA
1.	CSMA / CD is effective after a collision.	Whereas CSMA / CA is effective before a collision.
2.	CSMA / CD is used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3.	It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4.	CSMA / CD resends the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5.	CSMA / CD is used in 802.3 standard.	While CSMA / CA is used in 802.11 standard.
6.	It is more efficient than simple CSMA(Carrier Sense Multiple Access).	While it is similar to simple CSMA(Carrier Sense Multiple Access).

CSMA/CD vs CSMA/CA (without RTS/CTS)

CD Collision Detect

wired – listen and talk

1. Listen for others
2. Busy? goto 1.
3. Send message (and listen)
4. Collision?
 - a. JAM
 - b. increase your BEB
 - c. sleep
 - d. goto 1.

CA Collision Avoidance

wireless – talk OR listen

1. Listen for others
2. Busy?
 - a. increase your BEB
 - b. sleep
 - c. goto 1.
3. Send message
4. Wait for ACK (*MAC ACK*)
5. Got No ACK from MAC?
 - a. increase your BEB
 - b. sleep
 - c. goto 1.

CSMA/CD

VS

CSMA/CA

The collision detection methodology is what it is

It's found in 802.3 Ethernet network cables

It is compatible with wired networks

It is effective after a network's collision detection

It is a collision avoidance protocol

It is used in the Ethernet 802.11 network

It is compatible with wireless networks

It is useful prior to collision detection on a network

IEEE 802.3

- IEEE stands for Institute of Electrical and Electronics Engineers.
 - It is a technical professional organization that defines standards for various range of technologies. It works on advancement of technologies for betterment of humanity.
- 802.3 is a working group and a collection of IEEE standards produced by the working group defining the physical layer and data link layer's media access control (MAC) of wired Ethernet.
- This is generally a local area network (LAN) technology with some wide area network (WAN) applications.
- Through the use of this 802.3 protocol, physical connections are made between nodes and/or infrastructure devices (hubs, switches, routers) by various types of copper or fiber cable.

- ▶ 802.3 also defines LAN access method using CSMA/CD.
- ▶ OSI model, which was standardized only after introduction of these standards, was predicted using these very standards.

Various networking standards defined by IEEE

Standards	Related to	Explanation
802.1	Internetworking & management	Routing, bridging & internetwork communications
802.2	Logical Link Control (LLC)	Error control & flow control schemes
802.3	Ethernet LAN	Ethernet wire, CSMA/CD, Ethernet interfaces
802.4	Token Bus LAN	Token bus medium and interfaces
802.5	Token ring LAN	Token ring medium and interfaces
802.6	MAN management	MAN technologies, addressing, and interfaces
.....
802.10	Network security	Network access controls, certification, encryption
802.11	Wireless LAN working group	Wireless networking mechanism
.....

802.3 standard: Ethernet

- ▶ Ethernet is the most successful local area network protocol technology.
- ▶ It is a multi-access network, meaning that a set of nodes send and receive frames over a shared link.
 - ▶ Hence, Ethernet can be viewed as a bus that has various stations(computers) attached to it.
- ▶ It is the working example of CSMA/CD.
- ▶ The transmission rate for Ethernet has changed over the years.
 - ▶ In early years, 10-Mbps Ethernet was considered great
 - ▶ Now it can support 100Mbps (**Fast Ethernet**), 1000Mbps (**Gigabit Ethernet**) versions.

802.3 cabling

There are 4 types of cables being used for Ethernet:

1. 10 Base 5
2. 10 Base 2
3. 10 Base T
4. 10 Base F

Here, 10 represents Transmission rate in Mbps, Base represents Baseband signaling, and 5 means the wire supports maximum segment of (5*100) meters.

Name	Cable	MAX Segment	Nodes/seg.	Advantages
10Base5	Thick coaxial	500 meters	100	Good for Backbones.
10Base2	Thin coaxial	200 meters	30	Cheapest System.
10Base-T	Twisted pair	100 meters	1024	Easy Maintenance.
10Base-F	Fiber Optics	2000 meters	1024	Best between Buildings.

Wireless LAN

- ▶ WLAN technology uses radio frequency to transmit and receive data over air.
- ▶ It provides all the features and benefits of traditional LANs but without the limitations of a cable.
- ▶ It is a data communication system providing wireless peer-to-peer and point-to-point connectivity within a building or a complex.
- ▶ WLANs perform same task as the traditional Ethernet technology, but instead of cables, they use electro magnetic waves for file transfer, peripheral sharing, email, database access and other similar operations.
- ▶ WLAN is supported by 802.11 standard.

Differentiating Ethernet with wireless network

Ethernet	Wireless network
Follows IEEE 802.3 standard	Follows IEEE 802.11 standard
Uses coaxial cable for communication	Uses radio wave for communication
Uses MAC	Uses MAC Sublayers
Uses CSMA/CD	Uses CSMA/CA
High efficiency	Low efficiency
Long range support is possible	For short ranges only
Addressing is simpler	Complicated addressing
E.g. Star topology using Ethernet	E.g. Wi-Fi

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m
802.11 b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m
802.11 a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m
802.11 g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m
802.11 n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m
802.11 ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km

Short forms:

- ▶ **DSSS** → Direct Sequence Spread Spectrum
- ▶ **FHSS** → Frequency hopping Spread Spectrum
- ▶ **OFDM** → Orthogonal Frequency Division Multiplexing
- ▶ **CCK** → Complementary Code Keying
- ▶ **SC** → Single Carrier

IEEE 802.11 PHY Standards

Release date	Standard	Frequency Band	Bandwidth	Transmission Scheme	Max Modulation	MIMO	Max Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	QPSK	N/A	2 Mb/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	QPSK	N/A	11 Mb/s
1999	802.11a	5 GHz	20 MHz	OFDM	64QAM	N/A	54 Mb/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, OFDM	64QAM	N/A	54 Mb/s
2009	802.11n	2.4 GHz 5 GHz	20 MHz 40 MHz	OFDM	64QAM	4x4	600 Mb/s
2013	802.11ac	5 GHz	20 MHz 40 MHz 80 MHz 160 MHz	OFDM	256QAM	8x8	6.93 Gb/s
2018	802.11ad	60 GHz	2160 MHz	SC, OFDM	256QAM	Beamforming	6.93 Gb/s



End of chapter 2

Important questions (5-6 marks)

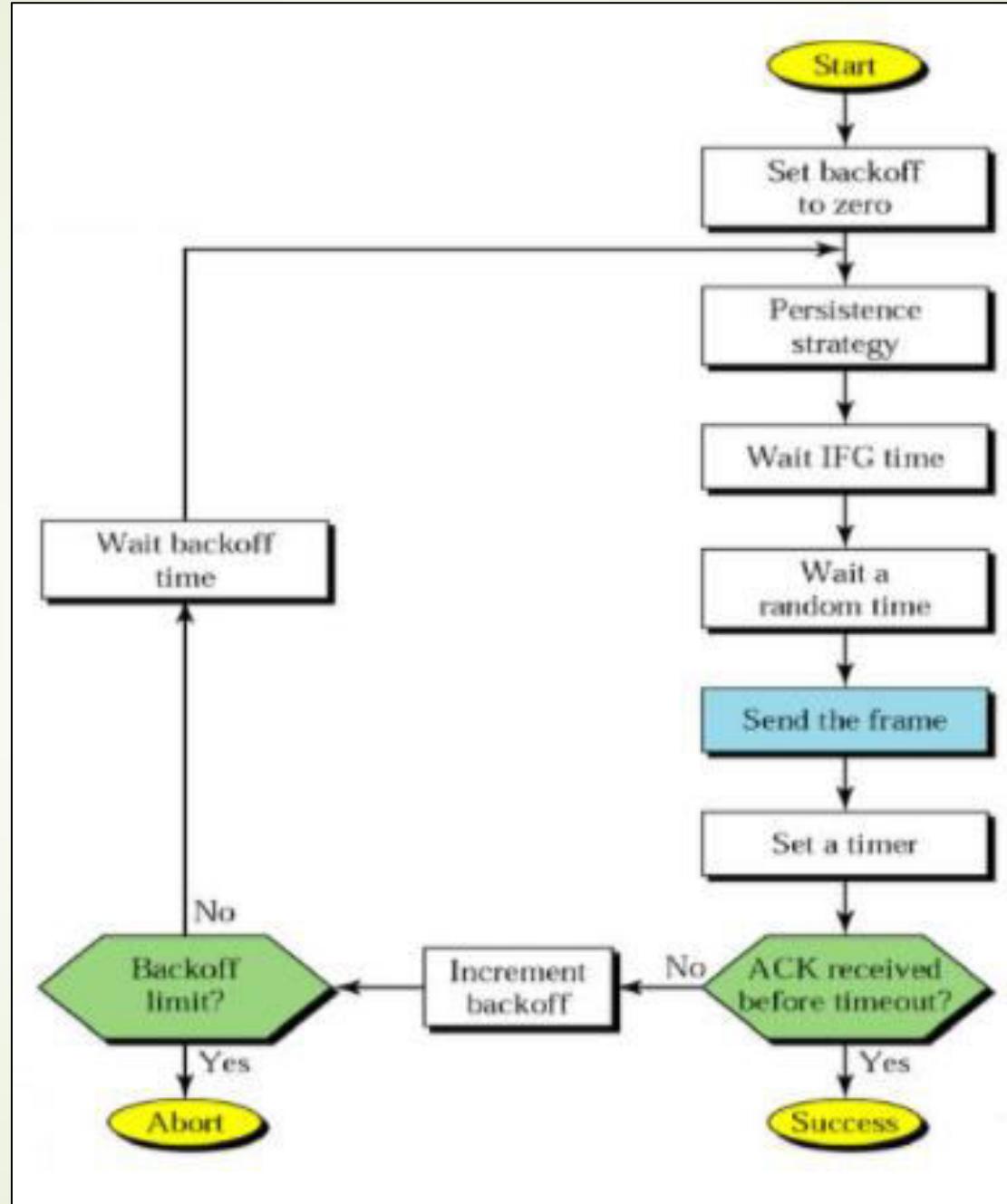
1. Comparison of networking cables
2. What is RAID? Explain in brief various levels of RAID scheme.
3. What is CSMA/CD? Explain working mechanism of CSMA/CD.
4. Write short notes on
 - a) IEEE 802.3 standard
 - b) Wireless LAN vs wired LAN
 - c) Hub

Extra contents

CSMA/CA

- ▶ Carrier Sense Multiple Access/ Collision Avoidance
- ▶ In contrast to CSMA/CD that deals with collisions after their occurrence, CSMA/CA prevents collisions prior to their origin.
- ▶ Here, whenever the channel is found idle, the station doesn't transmit immediately. It waits for a period of time called the Inter Frame Space (IFS)
 - ▶ The purpose of IFS is to allow the transmitted signal to reach other stations.
- ▶ Used in wireless network transmission.

- ▶ When channel is sensed to be idle, it may be possible that some distant stations may have started transmitting, and their signals might not have reached other stations.
 - ▶ The station that is about to send its frame looks and waits for IFS to end.
 - ▶ After it has ended, it can send the frame.
- ▶ When a sender is about to send the frame, it sets a timer.
 - ▶ As soon as the transmission starts, the station waits for an acknowledgement signal before the timer expire.
 - ▶ If ACK signal is received, message is successfully sent.
 - ▶ If timer expires first, Then back-off timer is increased and the station has to wait for resend.



CHAPTER 3

THE PHYSICAL LAYER

5 hours

~ 8 marks

Chapter overview

- ❖ Transmission media
 - twisted pair, coaxial cable, optical fiber, line of sight, satellite
- ❖ Analog transmission
 - Telephone, Modem, RS 232
- ❖ Digital transmission
 - Digital encoding, PCM
- ❖ Channel switching & multiplexing techniques
 - Multiplexing, circuit switching and packet switching

3.1 Transmission media

- The communication medium through which data propagates from source to destination.
- Also called the communication media.
- Media can be guided(wired) or unguided(wireless)
 - Guided medium are reliable, but do not cover large area like wireless can
 - Unguided medium have large area of coverage, but are expensive

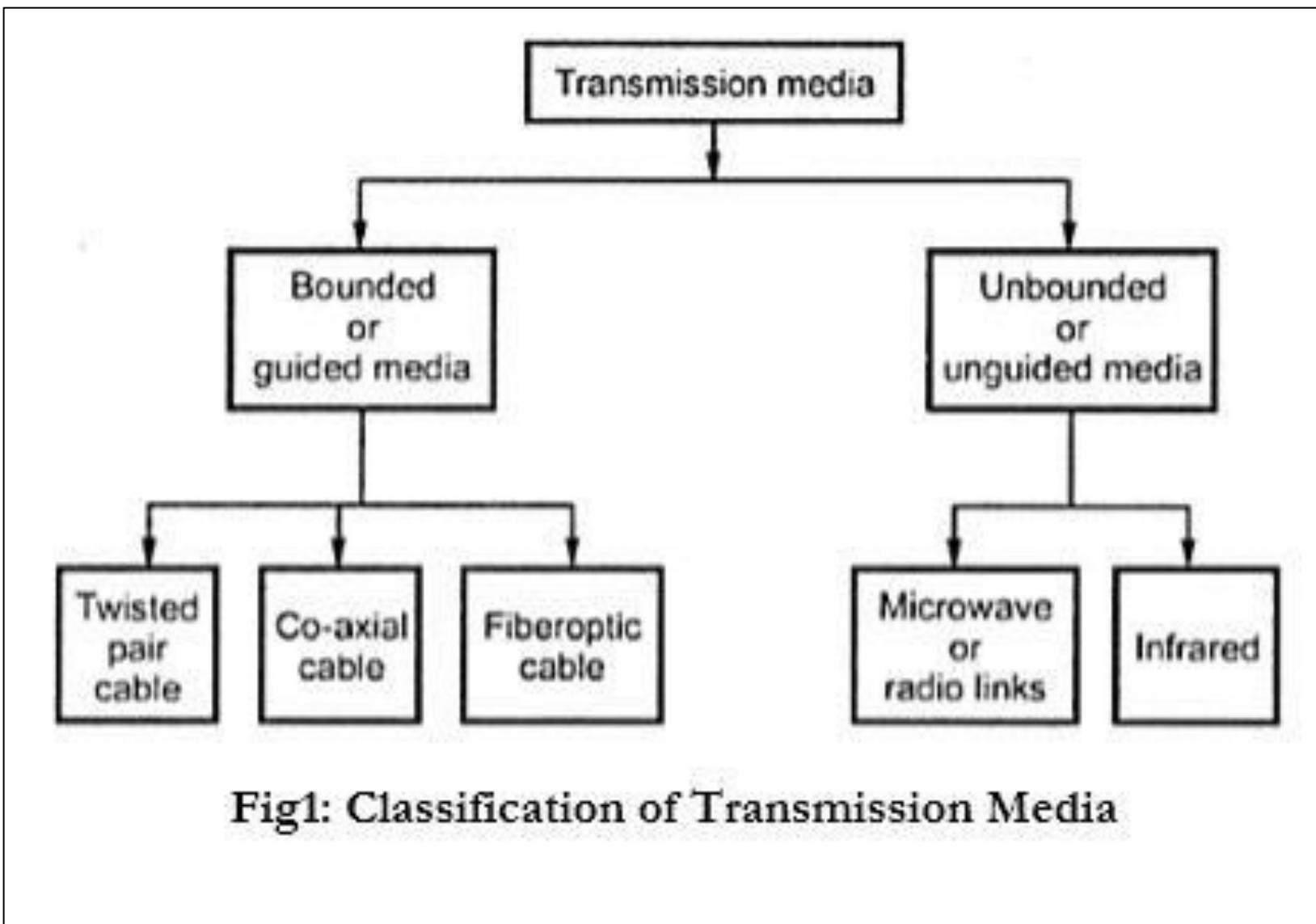


Fig1: Classification of Transmission Media

Guided media

- It is also referred to as Wired or Bounded transmission media.
- Signals being transmitted are directed and confined in a narrow pathway by using physical links.
- Features:
 - High Speed
 - Secure
 - Used for comparatively shorter distances
- There are 3 kinds of guided media:
 - Twisted pair cable
 - Coaxial cable
 - Optical fiber cable

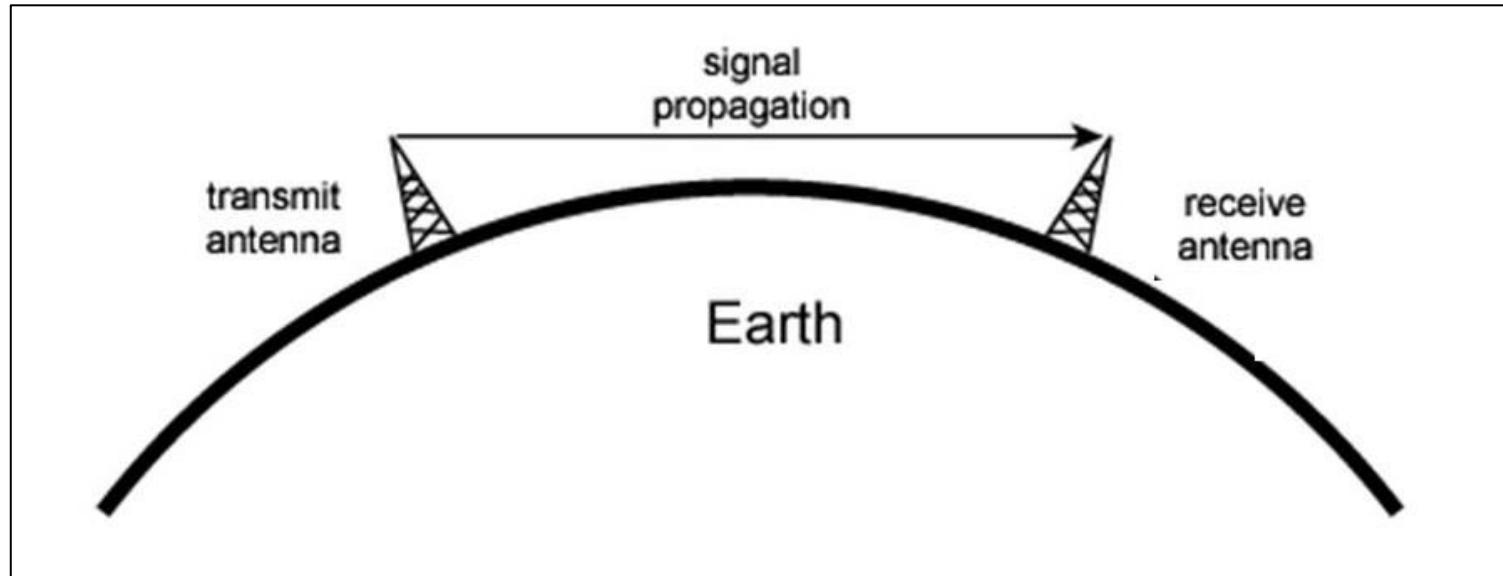
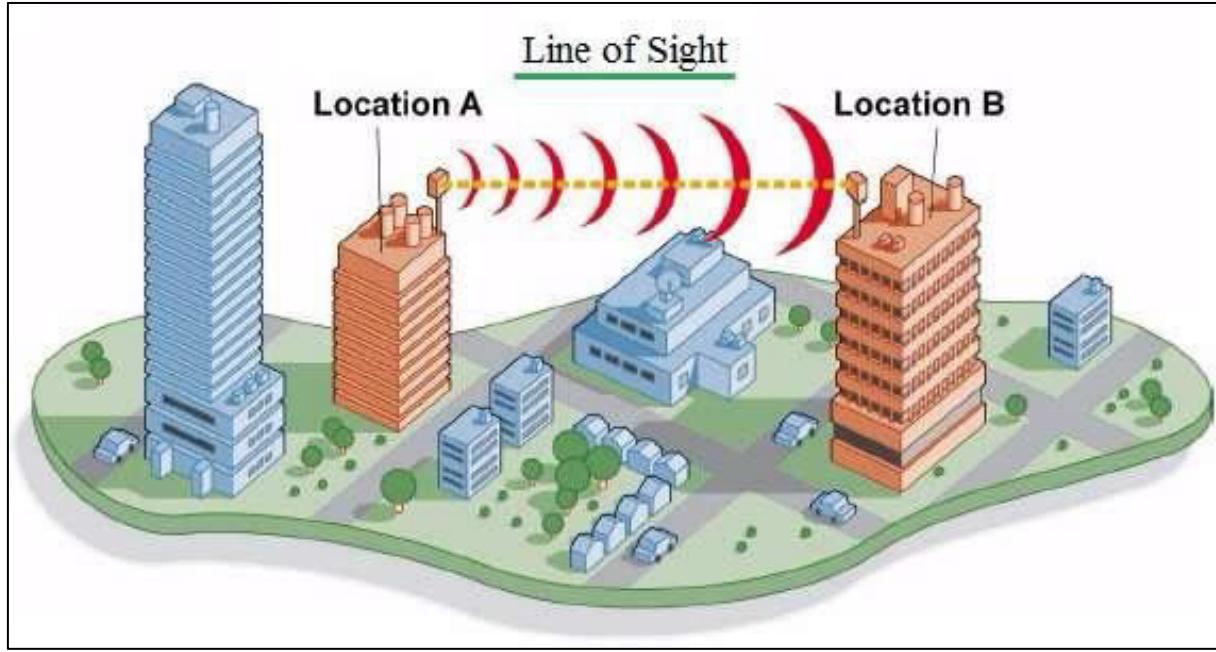
- Guided media have been explained in chapter 2

Unguided media

- It is also referred to as Wireless or Unbounded transmission media.
- No physical medium is required for the transmission of electromagnetic signals.
- Features:
 - The signal is broadcasted through air
 - Less Secure
 - Used for larger distances
- There are 3 types of unguided media signals:
 - Radiowaves → FM, cordless phone, satellite
 - Microwaves → cellular communication, television channel distribution
 - Infrared → Bluetooth, infrared

Line of sight

- A type of signal propagation mechanism where transmission and reception of data is only possible when transmitting and receiving stations are in view of each other without any sort of an obstacle between them.
- Here, radio waves of VHF (Very high frequency) mode travel in straight path between the receiver and transmitter antenna.
- Since the earth is round in shape, direct LoS communication is limited to approximately 75km (without use of routers)
- E.g. This mechanism is used in FM Radio, Microwave and satellite transmissions



Pros

- Long area coverage
- High bandwidth
- Relatively inexpensive (that satellite)

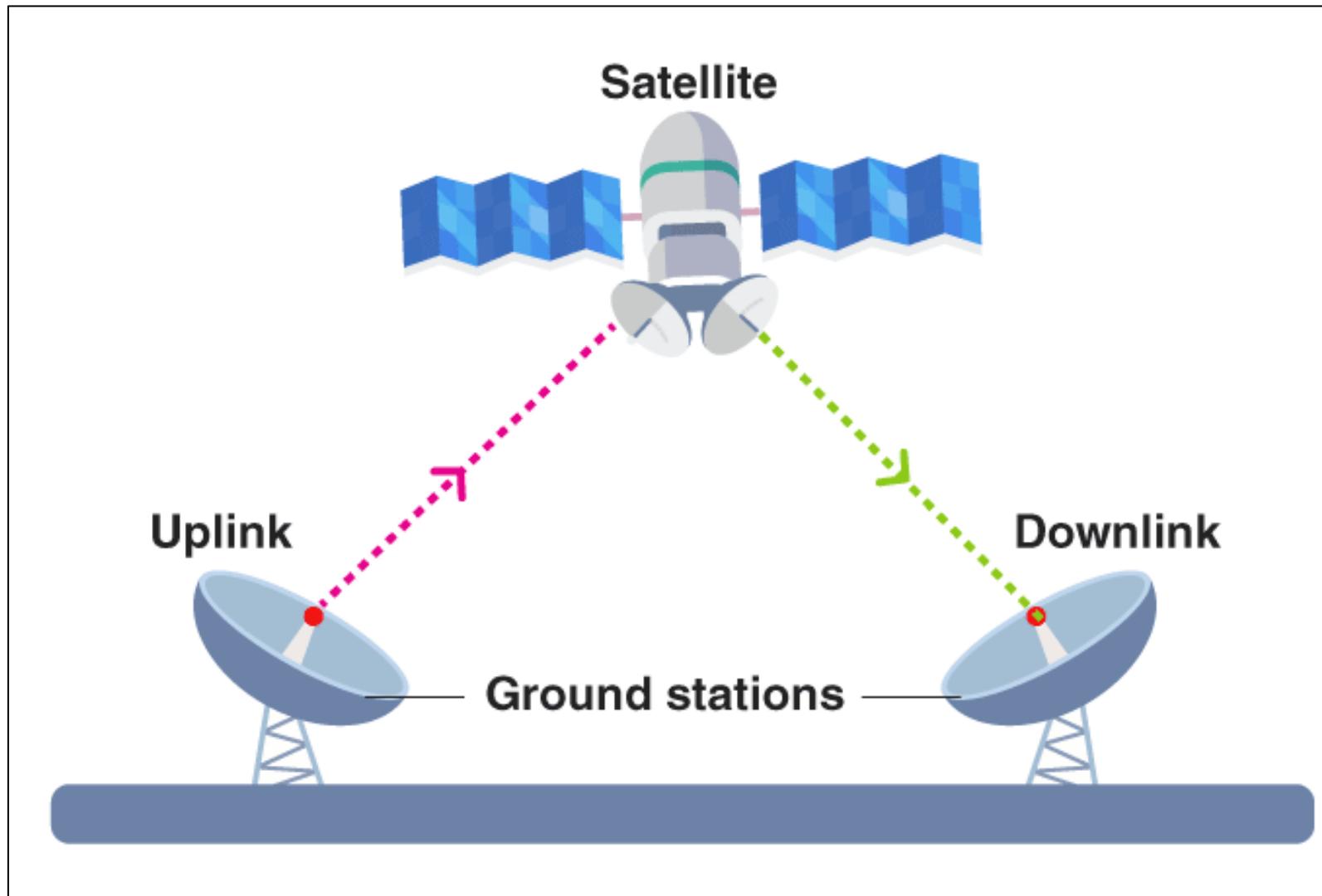
Cons

- Require unobstructed LoS
- Environmental interference possibility
- Free Space Loss (Signals disperse along long distance)
- Atmospheric Absorption (Water vapour and air molecules absorb radio signals)

- LoS propagation signals are affected by Electro-Magnetic Interference
 - Since the waves have free propagation path, they can also be jammed or eaves dropped

Satellite Communication

- A satellite is a repeater on space.
 - It receives one frequency, amplifies or repeats the signal and then transmits the signal on another frequency
- A communication satellite is an artificial satellite that amplifies and relays the radio telecommunication signals via a transponder.
 - It creates a communication channel between a source transmitter and a receiver at different locations on the earth.
- Satellite communications play a vital role in the global telecommunications system.
 - Approximately 2,000 artificial satellites orbiting Earth relay analog and digital signals carrying voice, video, and data to and from one or many locations worldwide.



- Satellite communication has two main components:
 - the ground segment, which consists of fixed or mobile transmission, reception, and ancillary equipment.
 - the space segment, which primarily is the satellite itself.
- A typical satellite link involves the transmission or “**uplink**” of a signal from an Earth station to a satellite.
 - The satellite then receives and amplifies the signal
 - Satellite retransmits the signal back to Earth (which is called the “**downlink**”), where it is received and re-amplified by Earth stations and terminals.
- The function of receiving, processing, and transmitting of the signals is performed by a component of the satellite called the **transponder**.
- Satellite communication can be point-to-point link between two stations (Remote Telecommunication) , or can be a broadcasting link to multiple receivers (Dish TV connections)

Pros

- Reduction of size of antennas (client side)
- High bandwidth
- Global reach
- Has variety of useful application
- Uniform service to everyone

Cons

- Costly implementation
- Hard to maintain
- Signal propagation takes considerable time, producing delays
- Weather conditions can affect signal propagations

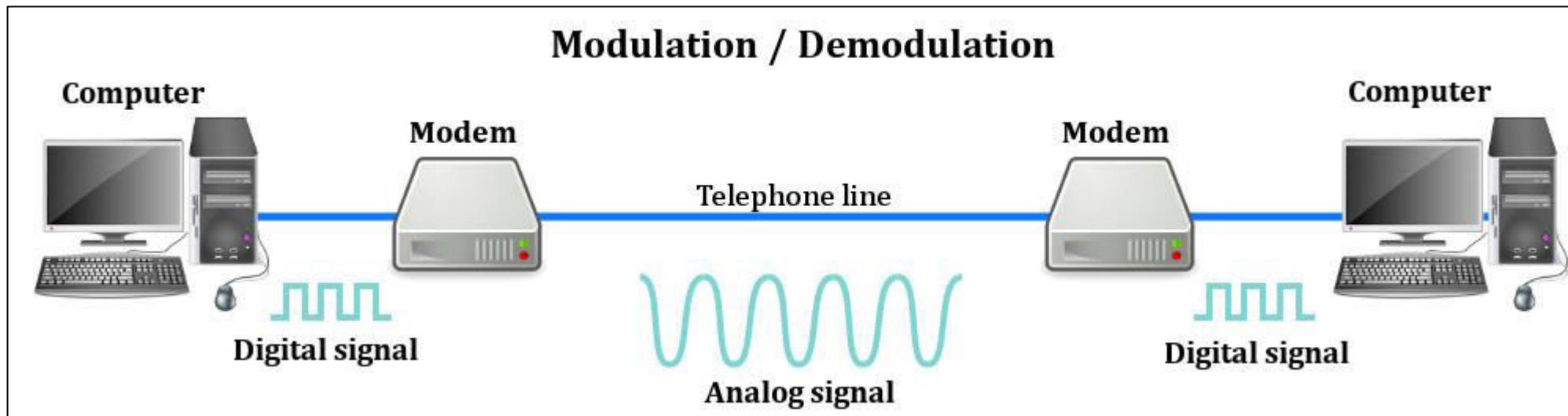
3.2 Analog communication

MODEM

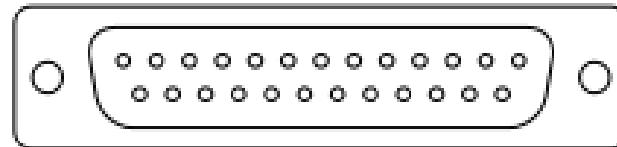
- It stands for MODulator DEModulator.
- It is a hardware component/device which can connect computer and other devices such as router and switch to internet.
- Modems converts or modulates the analog signals coming from telephone wire into digital form i.e. in form of 0's and 1's.
- The first modems were “dial-up” which means user had to dial a phone number to connect computer to ISP. Their maximum data transfer rate is almost 56 kbps.
 - Modern modems are DSL or cable modems. They have high data transfer rate and wider frequency range as compared to dial-up modems.

How MODEM work?

- Computer can exchange information over telephone lines by using two modems- one on each side.
- A calling computer (or a terminal) or an originator, contacts the receiving computer (also known as answering) through a telephone number, and a communication link is established after control signals have been exchanged between computers and modems.
- Communication using modem happens as follows:
 1. The calling computer first sends its request in a digital format.
 2. MODEM converts this digital signal into analog form (**MODULATION**).
 3. This analog wave is transmitted via telephone circuit
 4. In the receiving zone, receiver-end MODEM converts the received analog signal to digital signal (**DEMODULATION**)
 5. Receiver computer then reads the digital signal.



RS232



- Standard protocol for serial communication
 - Serial communication is the process of sending data one bit at a time, sequentially, over a communication channel or computer bus.
 - This is in contrast to parallel communication, where several bits are sent as a whole, on a link with several parallel channels.
- It is used for connecting computer and its peripheral devices to allow serial data exchange between them.
- A serial port complying with the RS-232 standard was once a standard feature of many types of computers. Personal computers used them for connections not only to modems, but also to printers, computer mice, data storage, uninterruptible power supplies, and other peripheral devices.

- RS232 has lower transmission speed, short maximum cable length, large voltage swing, large standard connectors, no multipoint capability and limited multidrop capability as compared to Ethernet, or other counterparts.
- It formally defines signals connecting between a DTE (data terminal equipment) such as a computer terminal, and a DCE (data circuit-terminating equipment or data communication equipment), such as a modem



- In modern personal computers, USB has displaced RS-232 from most of its peripheral interface roles.

3.3 Digital Transmission: PCM and Encoding

Digital Transmission: Background

- Communication mechanism where waves are transmitted in form of digital signals.
- In analog system, waves are represented in form of continuous, time-varying signals.
 - Telephone systems, speakers carry analog signals
- In digital transmission, the analog signals are first converted from an analog format to a quantized, discrete time format.
 - Digital signals can be carried over the optical fiber, coaxial and microwave systems.
- Digital systems are noise-immune during transmission and R/W cycle.
 - They are less-likely to get affected by the noise.
- Digital transmission systems consist of more bandwidth to carry information than traditional analog systems

Digital Transmission

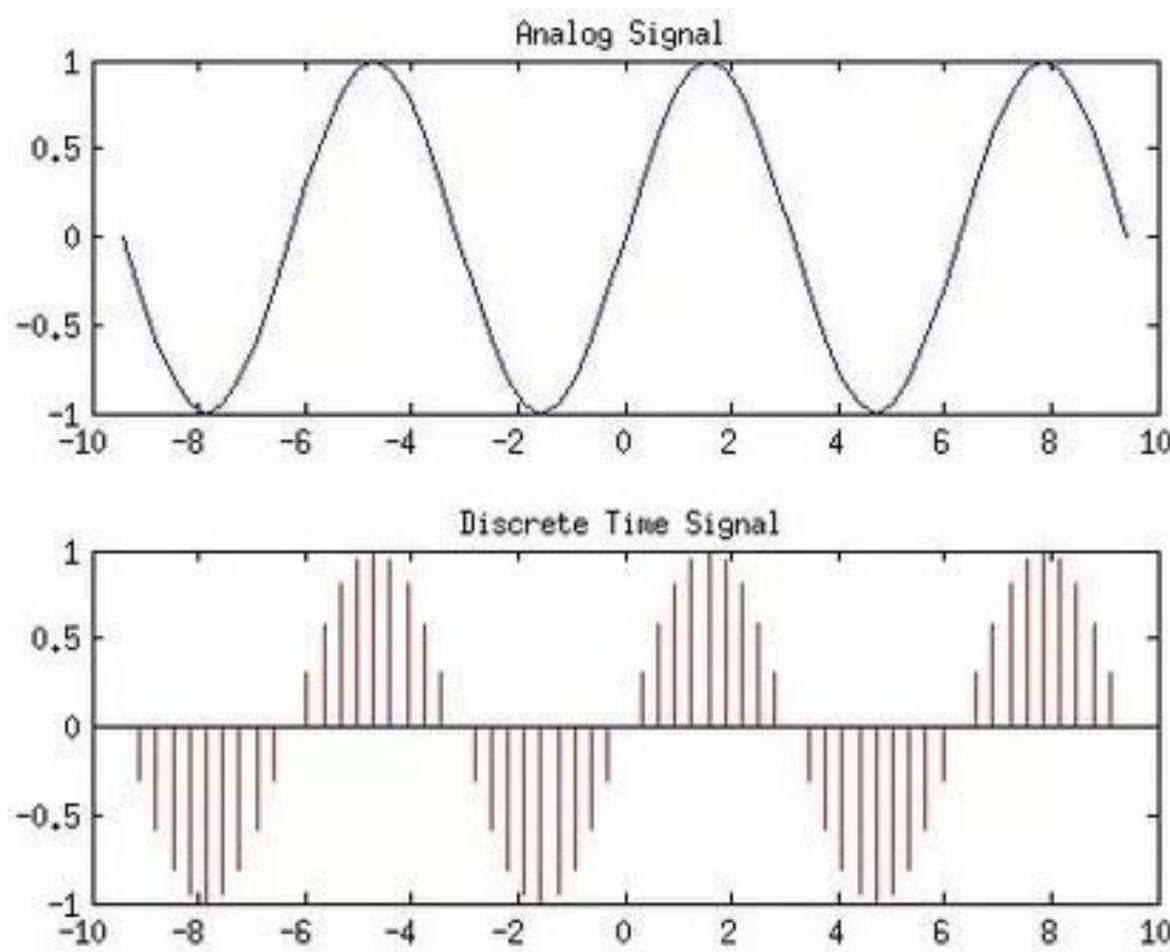
- Method to digitally represent the sampled analog signals.
- In a digital transmission, analog message is sampled, converted into a fixed length (quantization), and then serialized into binary number for transmission.
- In digital transmission, more focus is placed on ADC (Analog-to-Digital Conversion).
The phases on ADC are:
 1. Sampling
 2. Quantization
 3. Encoding

PCM

- Pulse coded modulation.
- A method used to digitally represent sampled analog signal.
- It is the standard form of digital audio in computers, CDs, digital telephony, and other digital audio applications.
- Most common technique to change an analog signal to digital data.
- A PCM encoder, just like a traditional ADC, consists of 3 major processes:
 - Sampling
 - Quantization
 - Encoding

A. Sampling

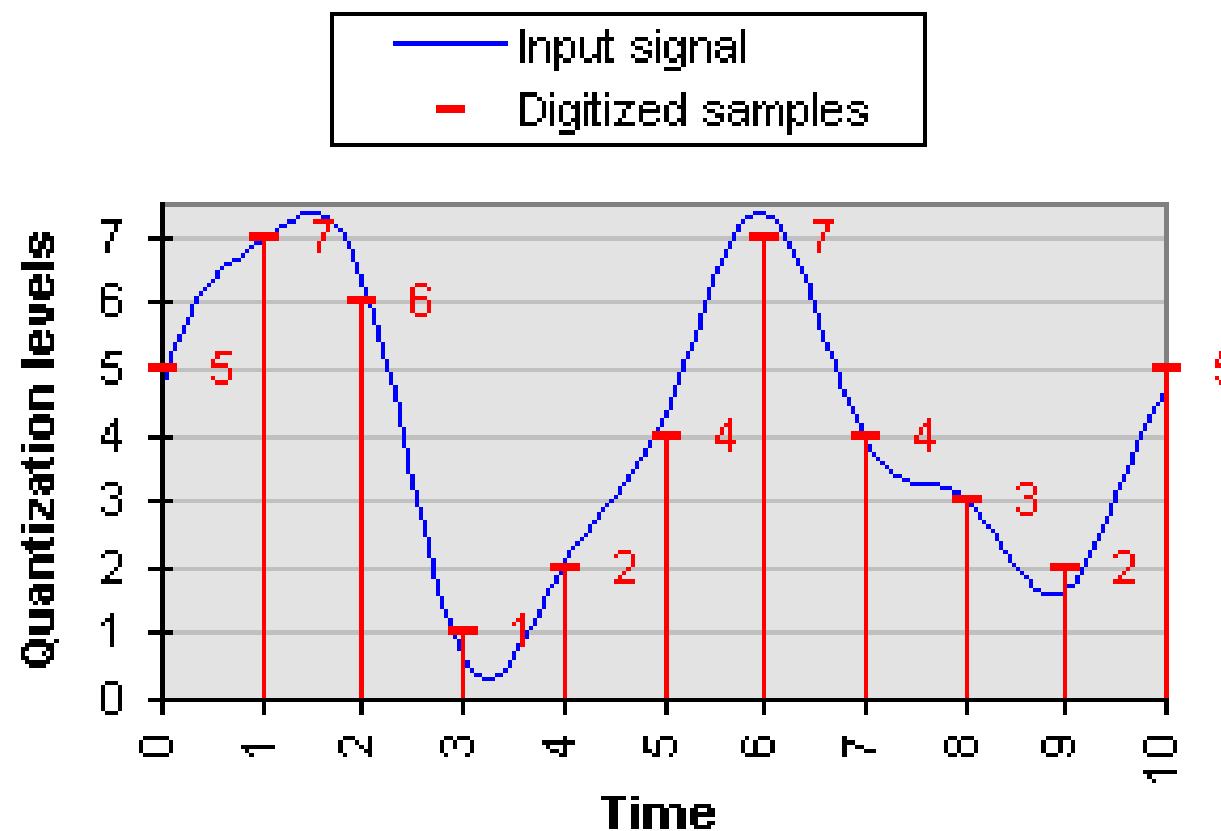
- Sampling is a process of measuring the amplitude of a continuous-time signal at discrete instants, converting the continuous signal into a discrete signal.
- The amplitude of analog wave in repeated interval.
 - Here, each measure instance is a sample
- A PCM sampler will convert continuous-time, continuous-amplitude input signal (analog signal) into discrete-time, continuous amplitude signal (PAM pulses)



B. Quantization

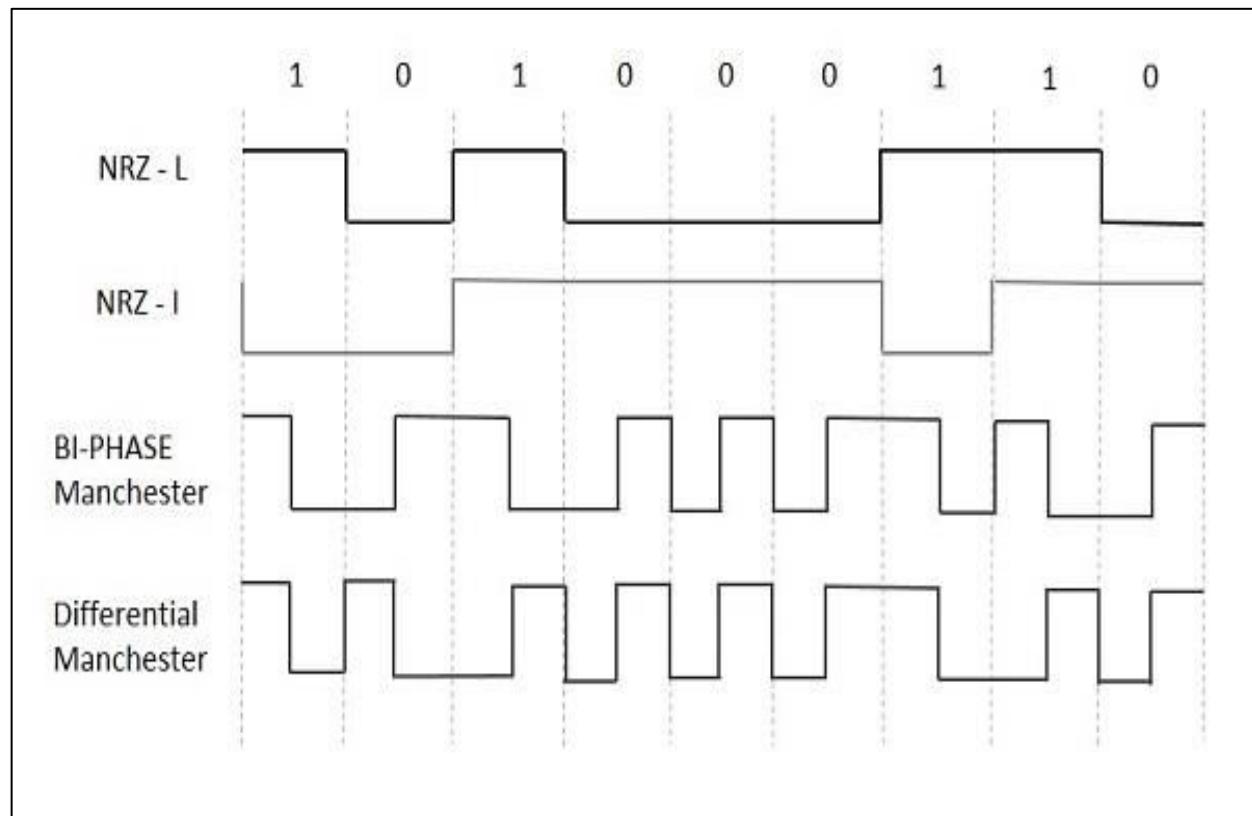
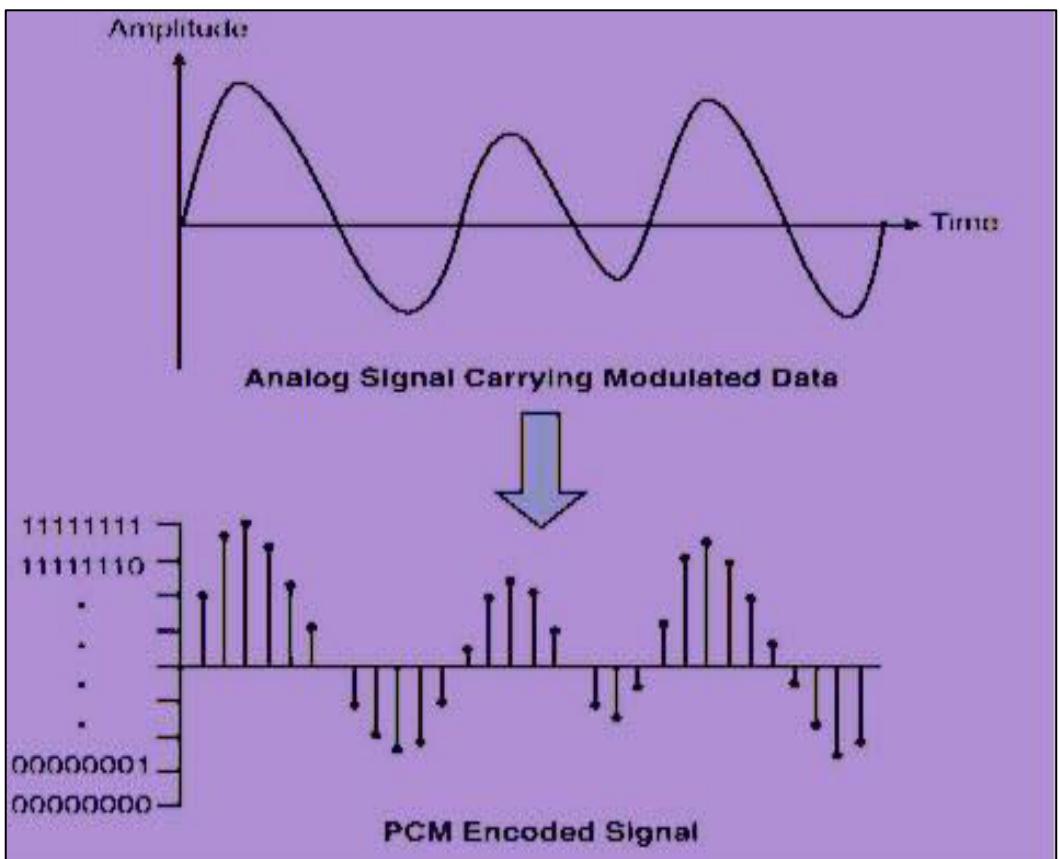
- It is the process of counting the value of samples to a fixed value.
- The result of sampling is a series of pulses with amplitude values between the maximum and minimum amplitudes of the signal.
 - These values are then counted to obtain a fixed value of amplitude.
- In quantization, an analog sample with an amplitude that converted into a digital sample with an amplitude that takes one of a specifically defined set of quantization values.
- Quantization is done by dividing the range of possible values of the analog samples into some different levels and assigning the center value of each level to any sample in the quantization interval.
- Quantization approximates the analog sample values with the nearest quantization values. So almost all the quantized samples will differ from the original samples by a small amount.

Quantizing and Digitizing a Signal

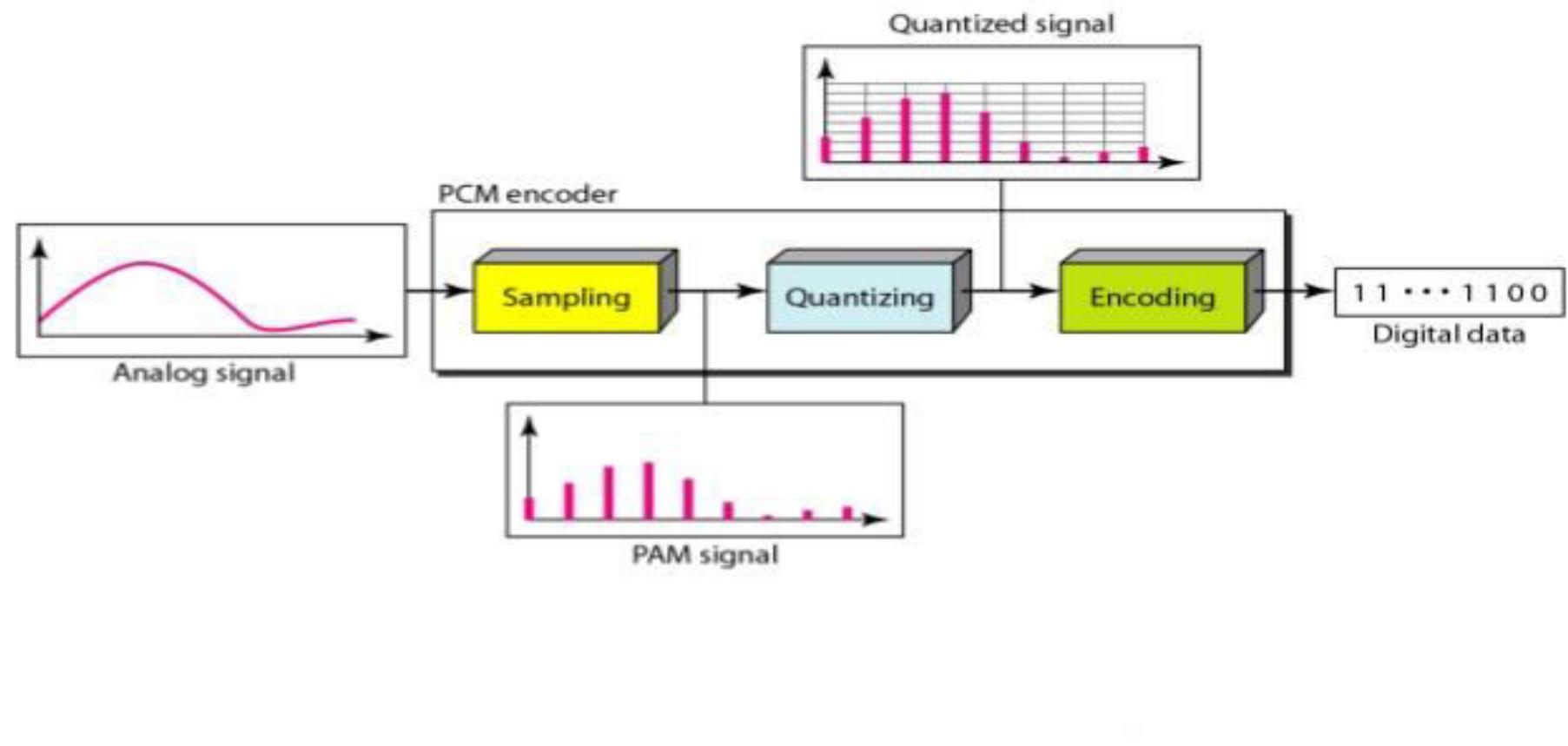


C. Encoding

- Here, each quantized sample is encoded into an 8-bit code-word that is represented into 0s and 1s.
- After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n bit code.
- An encoder designates each quantized level by a binary code.



BLOCK DIAGRAM OF PCM



Line encoding methods

1. Unipolar

- 1 → high voltage (above axis)
- 0 → no voltage (on the axis)

2. Polar

- 1 → logic high level(below axis)
- 0 → logic low level (above axis)

3. Bipolar

- 1 → high voltage (above or below axis, alternates with each 1 detected)
- 0 → low voltage (on the axis)

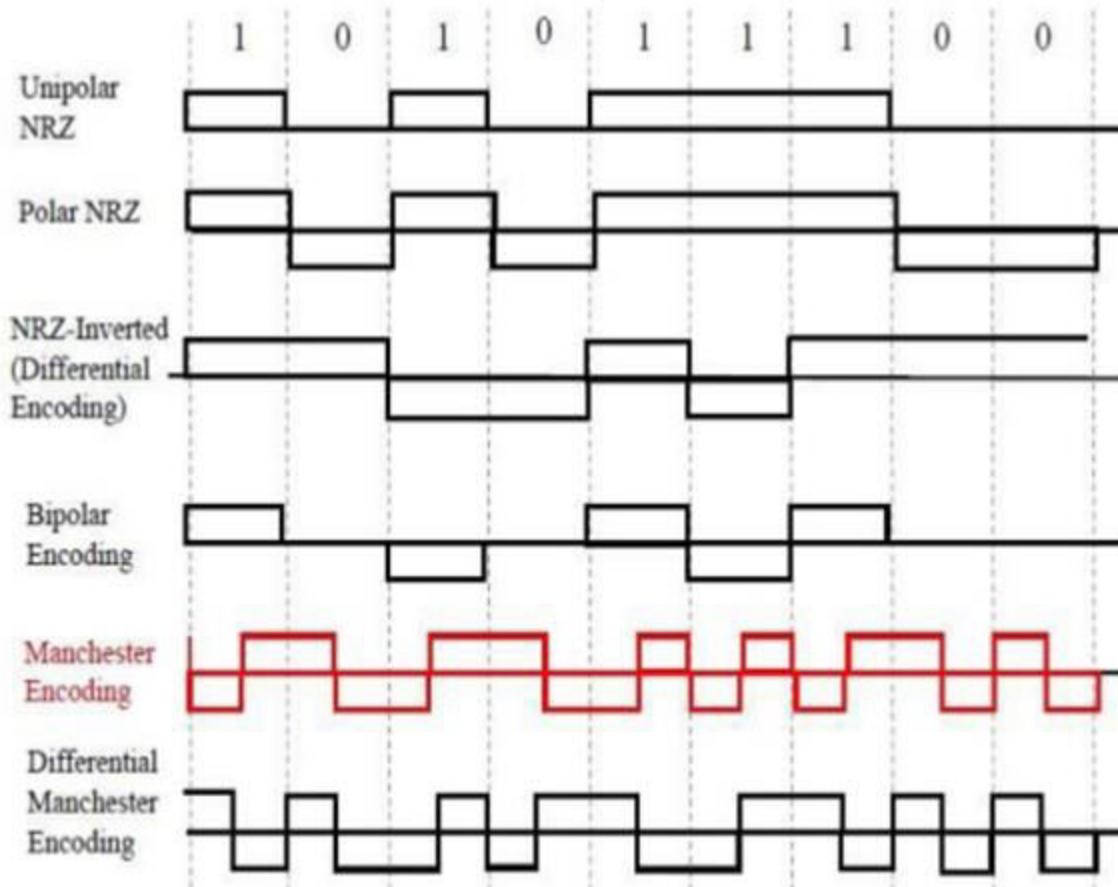
4. Manchester

- 1 → ½ of high to ½ of low
- 0 → opposite to 1

Other encoding techniques

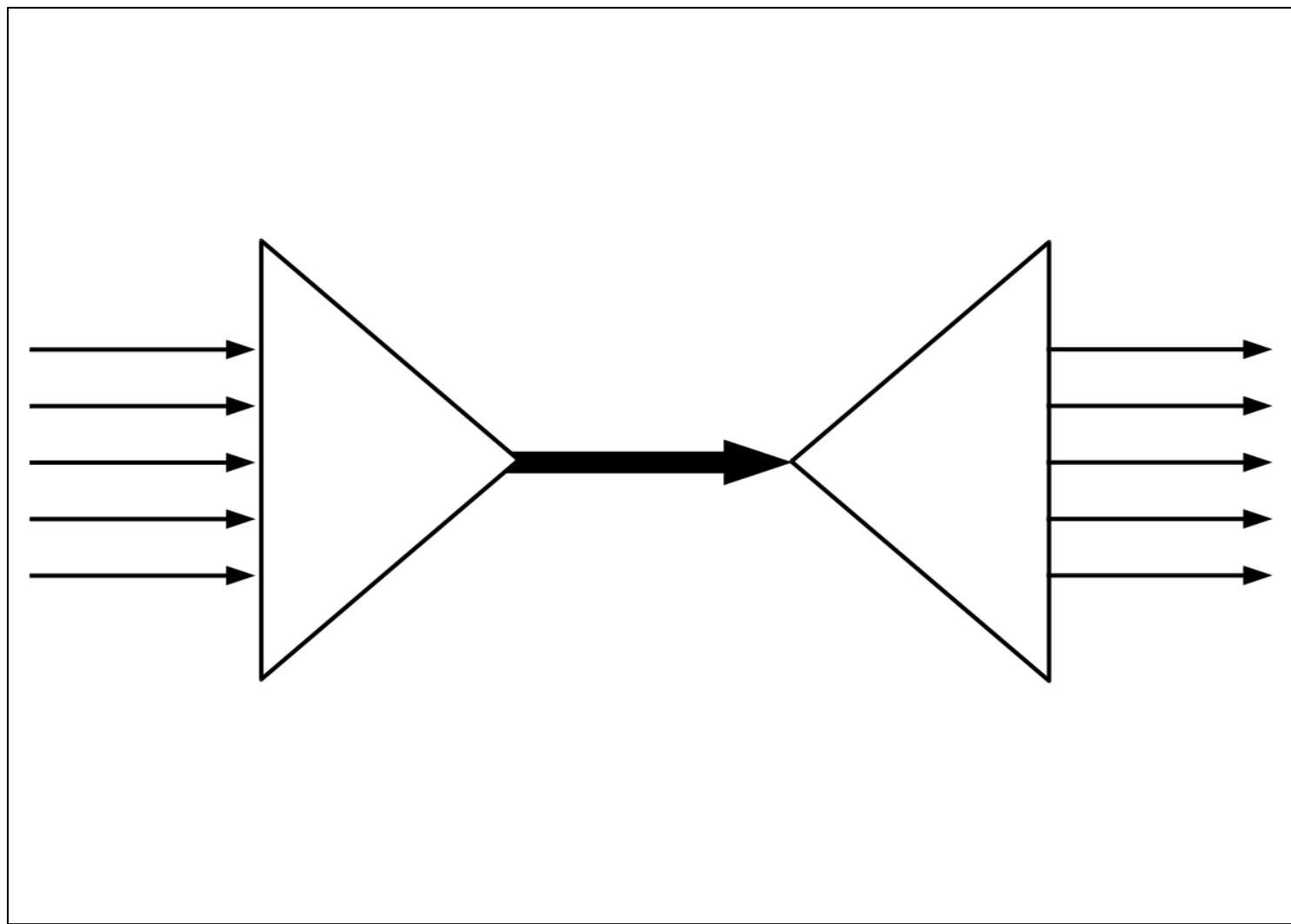
- Non Return to Zero Inverted (NRZ-I)
 - 1 → high voltage (above or below axis until another 1 is detected)
 - 0 → low voltage (follows the signal of 1)

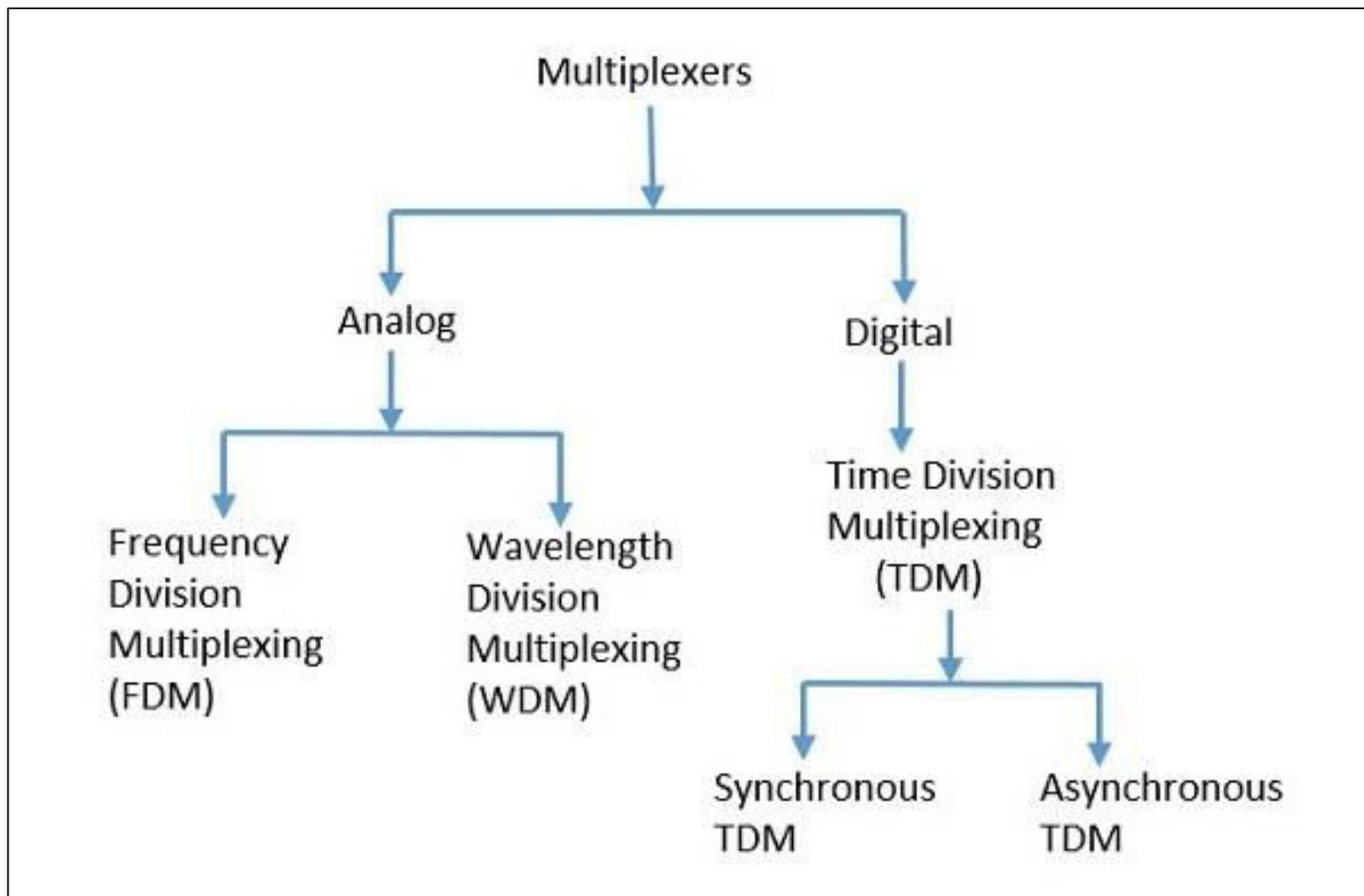
encoding schemes



Multiplexing

- A technique of simultaneously transmitting two or more individual signals over a single communication channel
- Due to multiplexing, it is possible to increase the no of signals in the telephony or satellite communication,
- The multiplexing device combines all the input signals to a single composite signal and transmits it over the communication medium.
- There are various kinds of multiplexing techniques:
 - Frequency division
 - Time division
 - Wavelength division

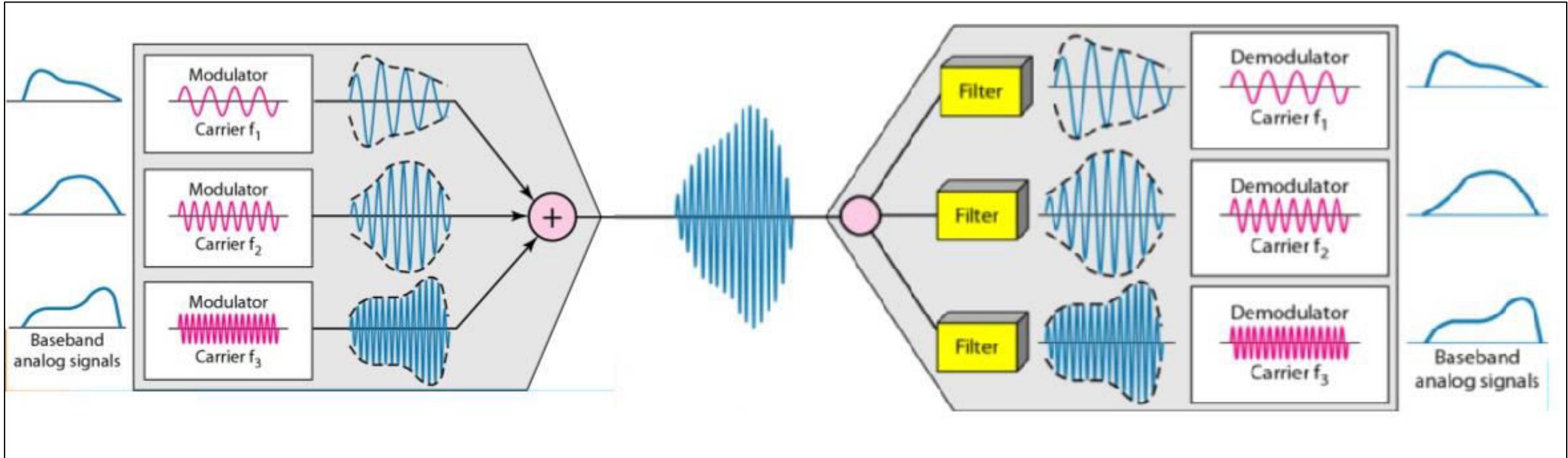


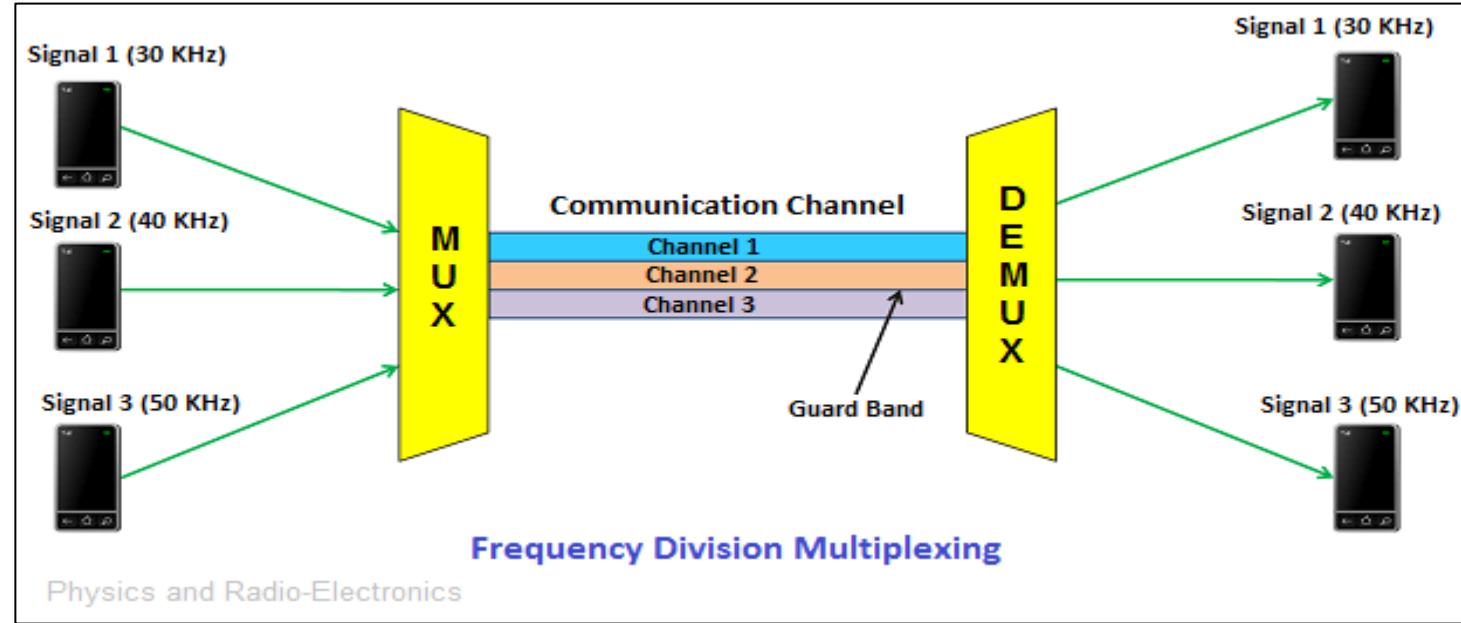


Frequency Division Multiplexing

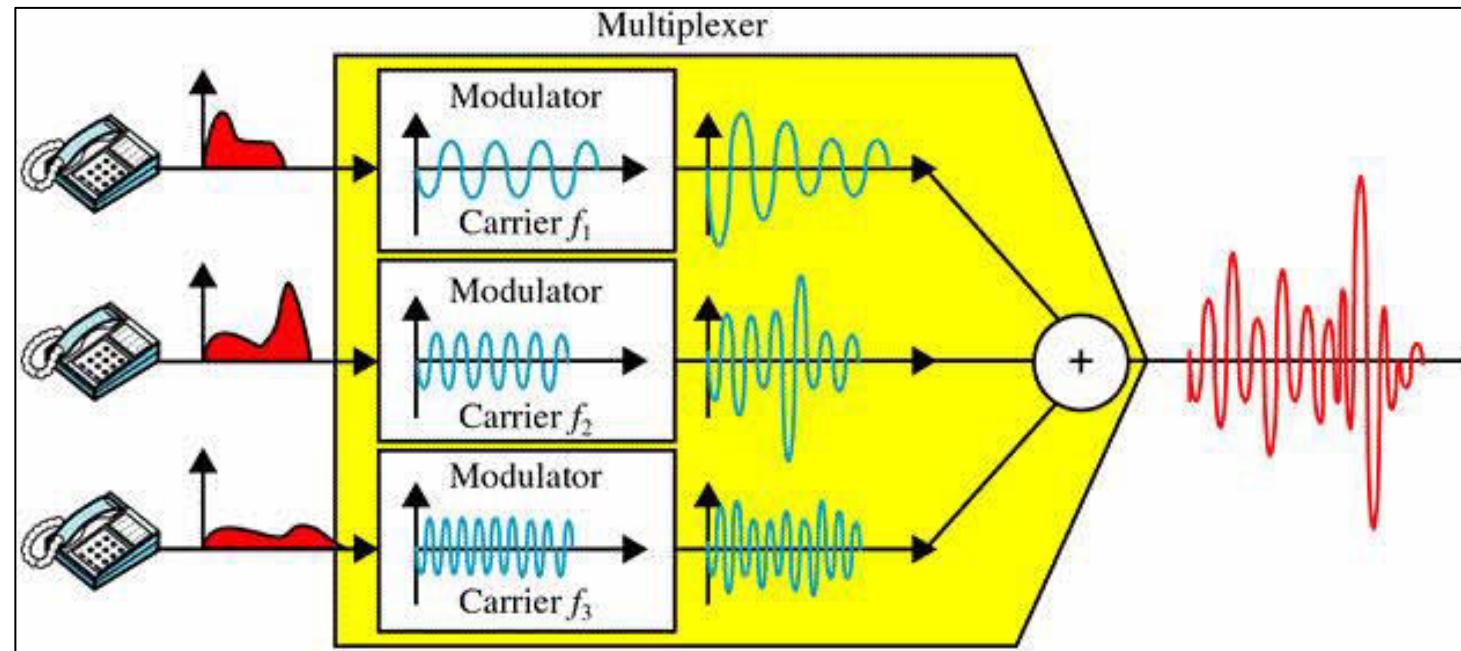
- Most used technique in analog signal multiplexing.
- It uses various frequencies to combine streams of data, for sending them on a communication medium, as a single stream.
- Bandwidth of a link should be greater than the combined bandwidth of various channel.
- Channels are generally separated by strips of unused bandwidth to prevent overlapping.

- In this a number of signals are transmitted at the same time, and each source transfers its signals in the allotted frequency range. There is a suitable frequency gap between the 2 adjacent signals to avoid over-lapping.
- A number of signals are sent simultaneously on the same time allocating separate frequency band or channel to each signal.
- Therefore to avoid interference between two successive channels **Guard bands** are used.
- E.g.
 1. A traditional television transmitter sends a no. of channels through a single cable uses FDM
 2. FM and AM radio broadcasting





Physics and Radio-Electronics



Pros

- Supports large no. of signals
- Demodulation is easy
- Doesn't need any synchronization between its receiver and transmitter

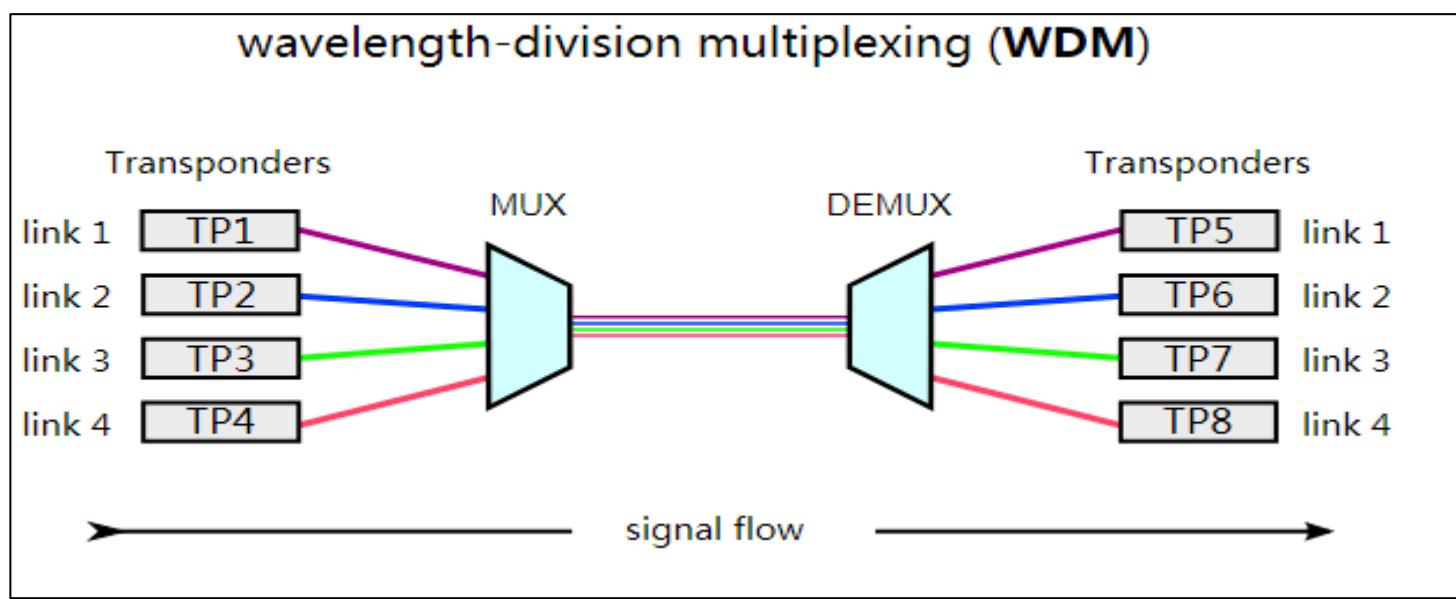
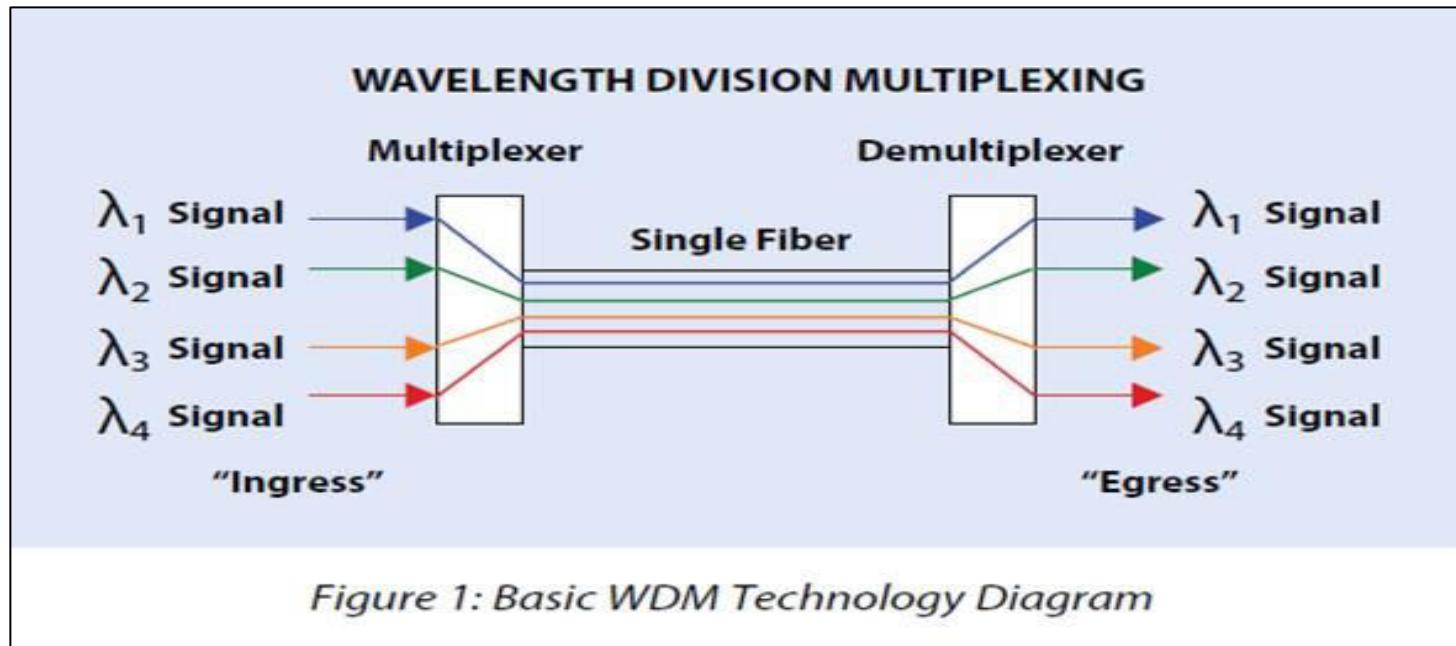
Cons

- Requires very large communication
- Requires large no. of modulators and filters
- FDM suffers from crosstalk

Wavelength Division Multiplexing

- An analog multiplexing technique to combine optical signals
- Multiple beams of light having different wavelength are multiplexed into a single transmission channel.
- This multiplexing method is implemented using fiber cables since they use optical propagation technique.
 - WDM uses light splitting property to send signals of different colors down a fiber simultaneously.
- In MUX section, multiple optical signals of different wavelengths are combined to form a single optical signal.
 - In DEMUX section, a single optical signal is refracted to separate multiple optical signals of differing wavelengths.

- The working mechanism is same as that of FDM.
 - In FDM, we talk about multiplexing of signals having varying frequencies
 - In WDM, we talk about multiplexing of signals having varying wavelengths generated from different sources.
- The combining and splitting of light waves is done by using a prism.
 - Prism bends the beam of light based on the angle of incidence and the frequency of the light wave.
- E.g. use of optical fibers in
 1. FTTH (Fiber To The Home)
 2. Telephony system
 3. Backbone Optical fiber transmission



Pros

- Supports many channels
- Long route communication
- Crosstalk is prevented

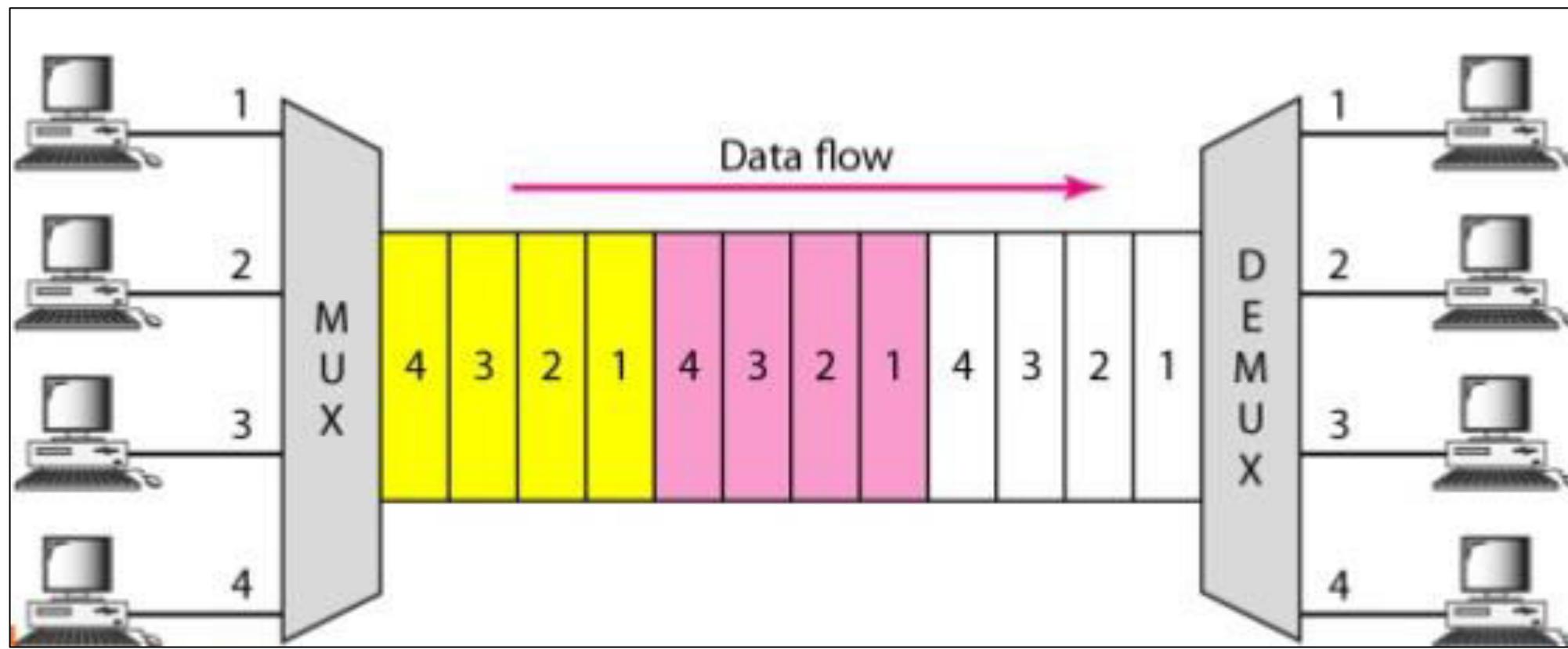
Cons

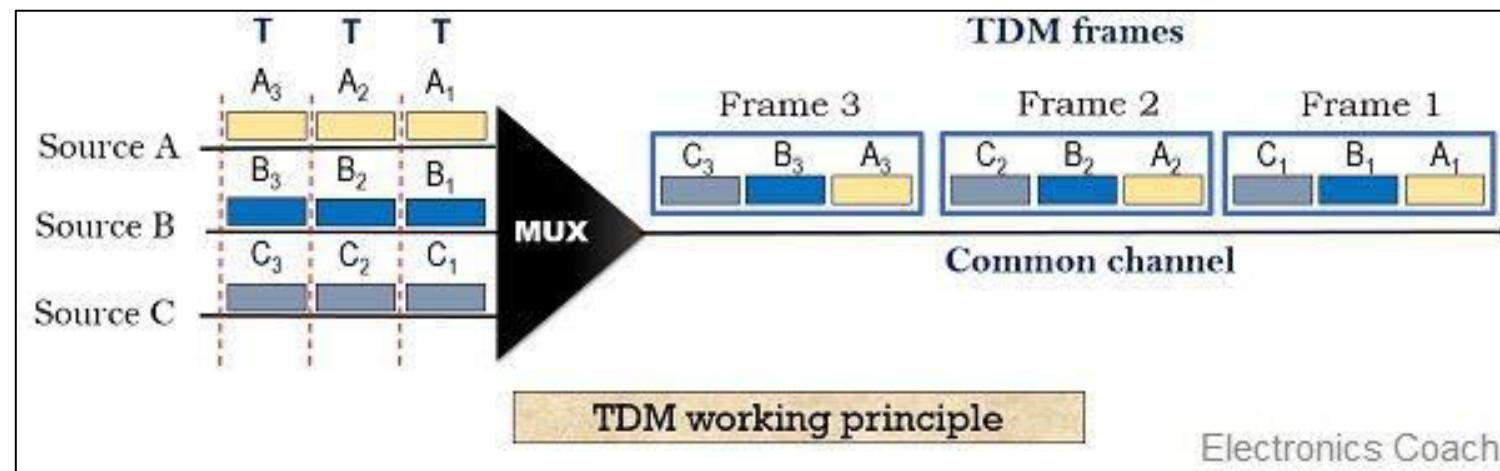
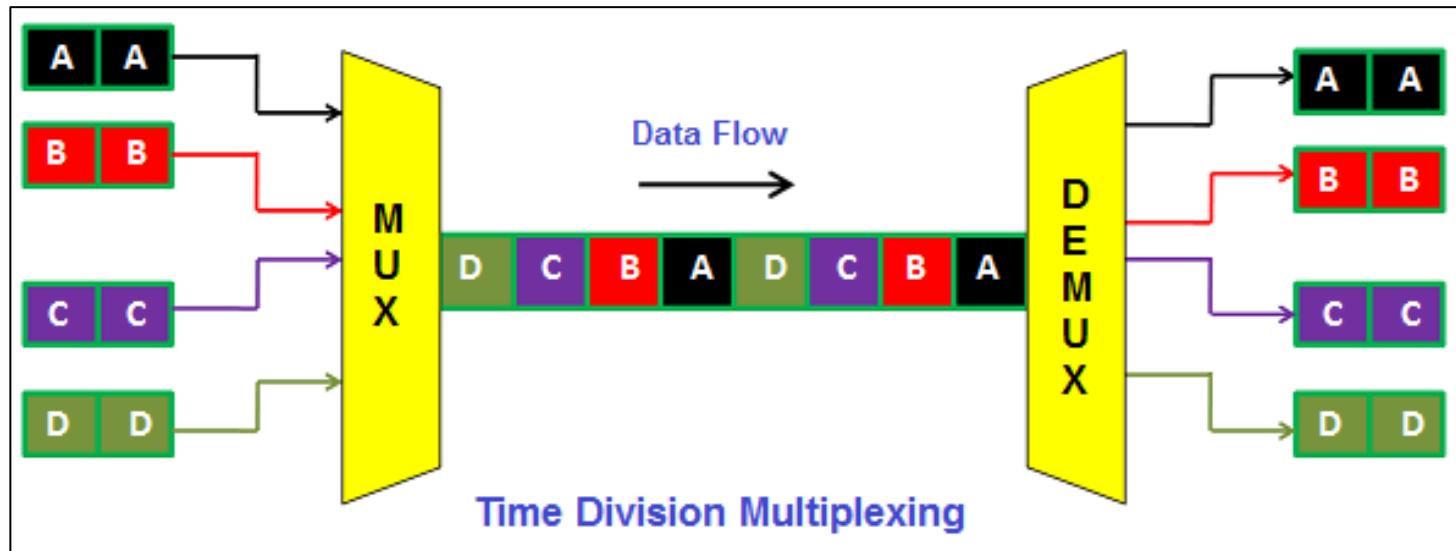
- Frequency must be distinct for each channel
- Expensive implementation
- Demodulation is complex

Time Division Multiplexing

- It is usually used with digital signals or the analog signals carrying digital data.
- Here, data from various sources are carried in the repetitive frames
- Each frame consists of a set of time slots
- Each source is assigned one or more time slots per frame.

- Instead of sharing a portion of the bandwidth, time is shared.
- Digital data from different sources are combined into one timeshared link.
- There are synchronous and asynchronous TDM modes.
 - In synchronous TDM, time slots are pre-assigned and fixed. Even if a source has no data to transmit, the slot that it is allocated to is sent empty
 - In asynchronous TDM, the slots are allocated dynamically depending on the speed or requirement.
- E.g.
 1. Digital telephony
 2. Data communication





Pros

- Efficiency of transmission
- Adapts multimedia transmission (Voice + data)
- High transmission rate
- Circuitry is not so complex
- Throughput is high even for many users

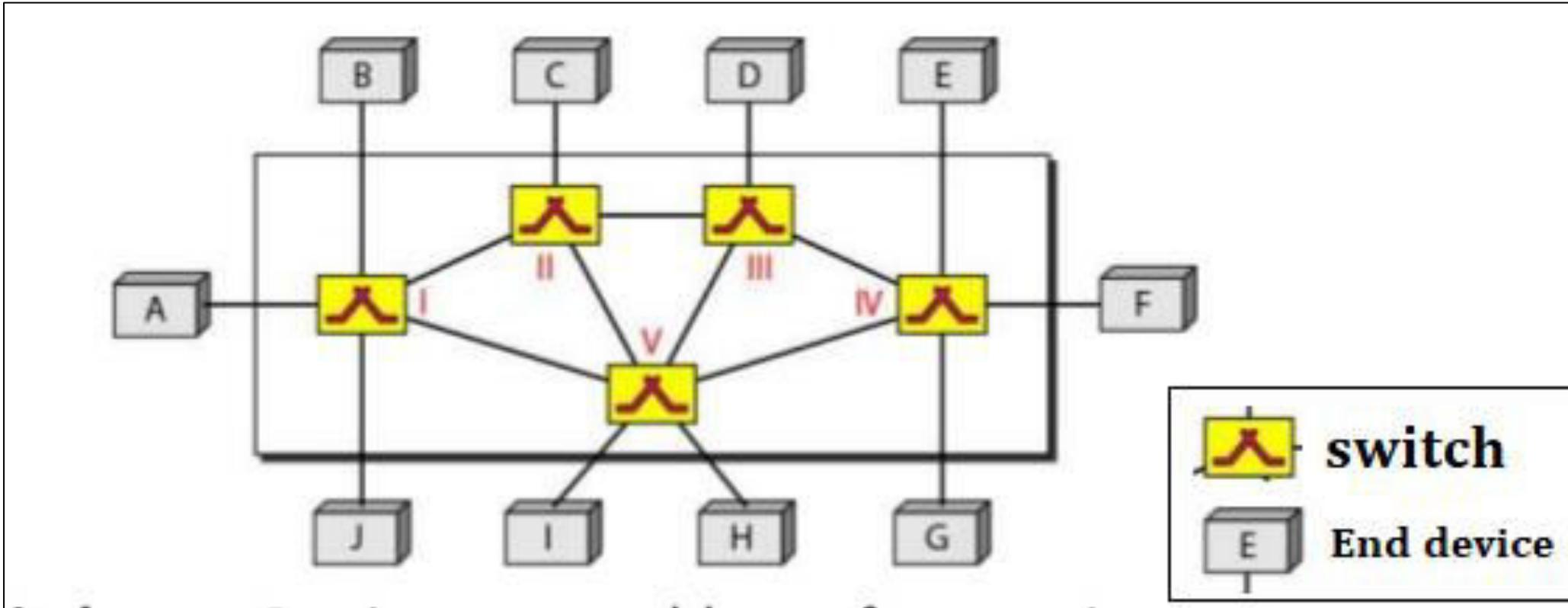
Cons

- Since all user get only a predefined time slot, some user that are roaming from one cell to another (i.e. suddenly appear into a source channel) might not get any time slot at all.
- Synchronization is essential for proper operation.
- Probability of error on bit rate transmission

Switching networks: Packet and Circuit Switching

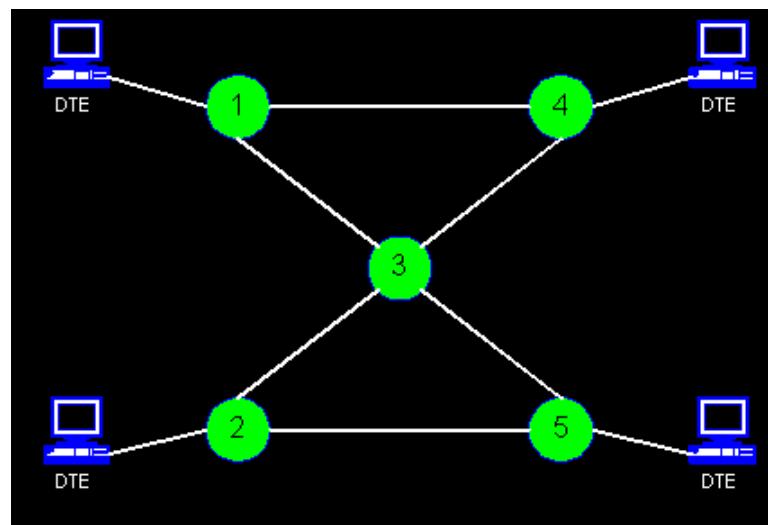
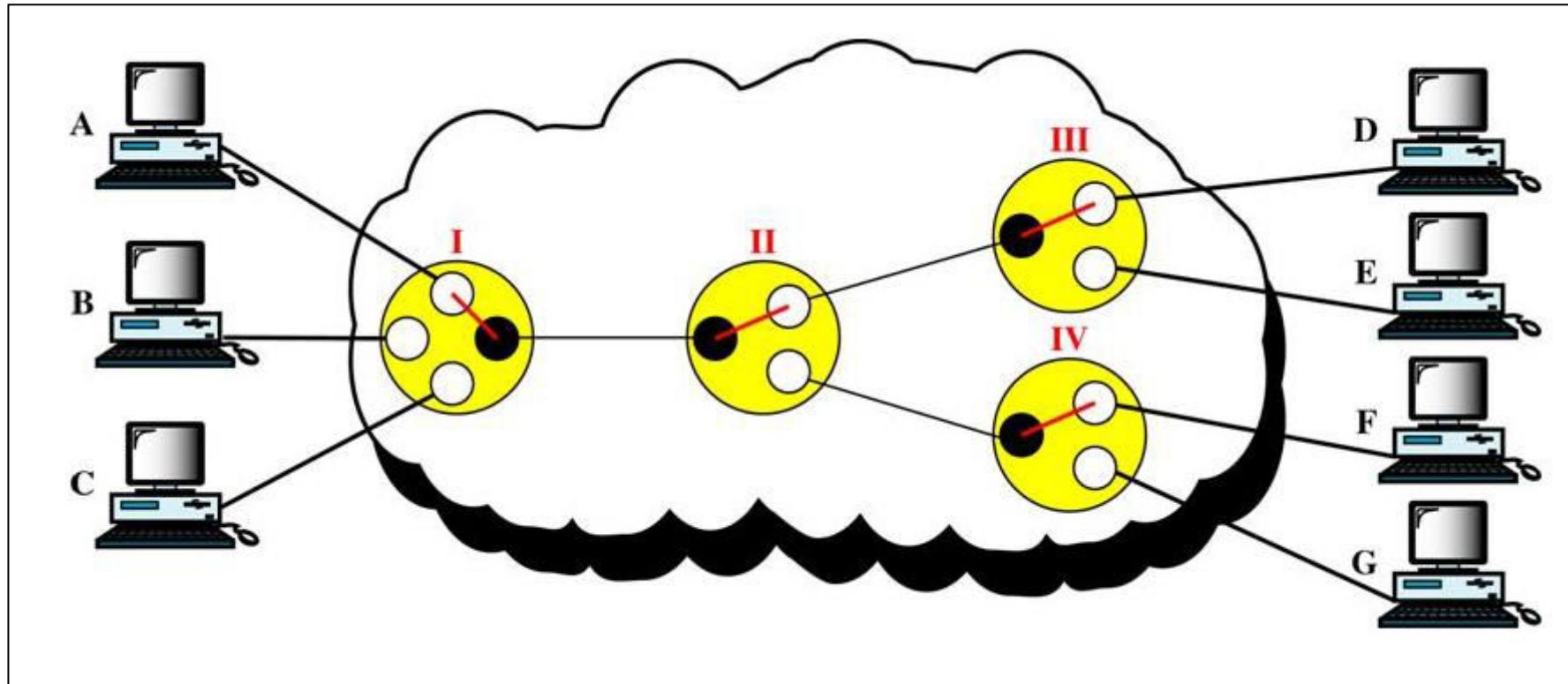
Switching Networks

- To connect multiple devices, one could either establish point-to-point connection, or connect all device to a central device through star topology.
 - Both of these methods are impractical for very large networks
- A better solution is switching.
 - A switch creates temporary connection between devices.
- In practical use, the transmission of data beyond a local area is achieved by using a network of intermediate switching nodes. The devices connected to it are called stations.
 - Stations can be computers, telephones etc.
- Hence, switching networks are the series of interlinked nodes, called switches. These switches are capable of creating temporary connections between two or more devices linked to them. These switches are either end-systems, or can be used for routing.



Circuit Switching Networks

- It is used in public telephone network.
- It was developed to handle voice traffic
 - Now it also handles digital data traffic
- It uses circuit switch, a dedicated path is established between two stations for communication.
 - Through this path, a 2-way, real-time transmission of voice signals across a network is achieved.
- These networks are connection-oriented, because they require the setting up of connection before the actual transfer of information can take place.



- The dedicated path is maintained for the duration of conversation. After the flow of information stops (call is dropped), the link is released.
- Circuit switched networks operate in 3 phases
 - Set-up phase [Connection Establish]
 - Data transfer phase
 - Tear down phase / Disconnection phase [Circuit is released]

Pros

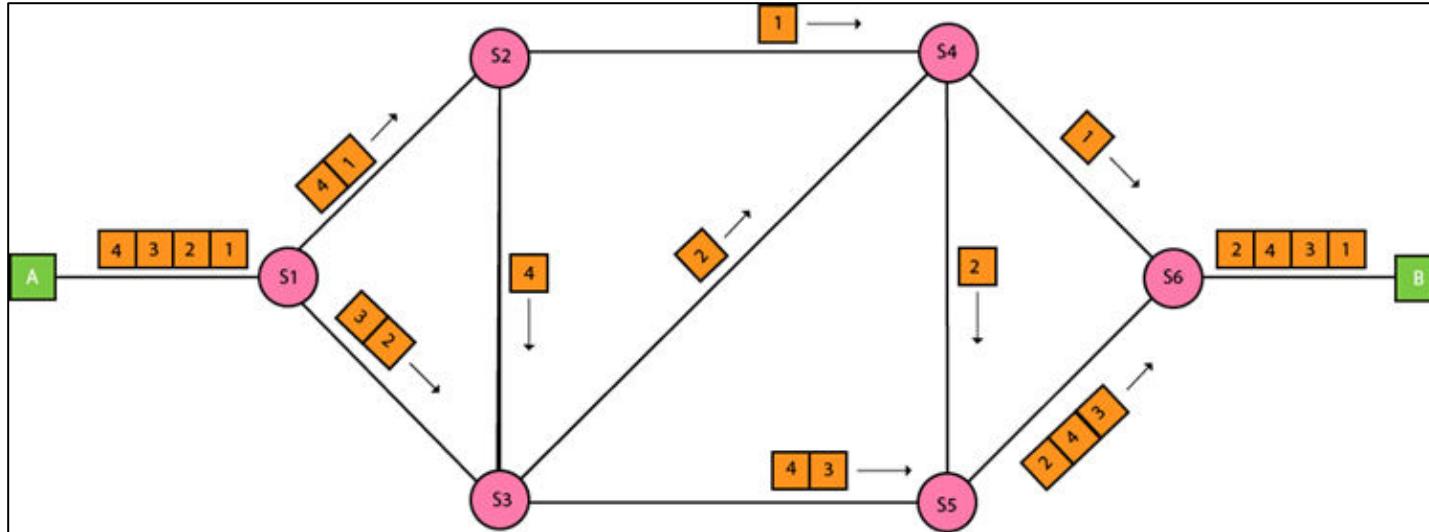
- Dedicated transmission channel
- Provides guaranteed data rate
- No delay in data flow

Cons

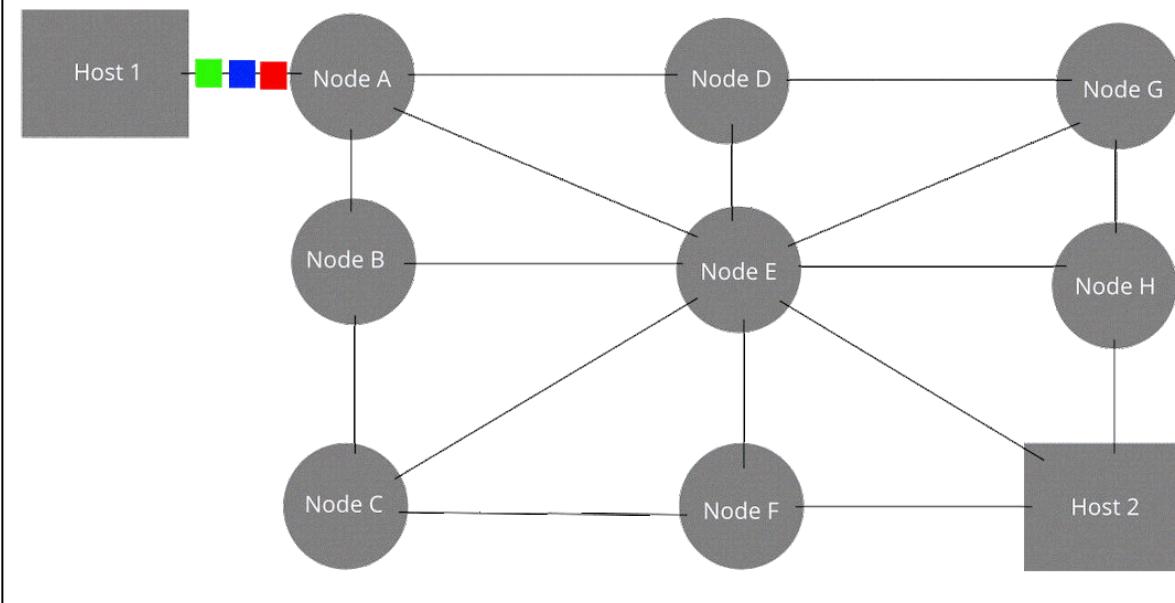
- Requires more bandwidth
- Takes some time to establish connection
- Since the channel is dedicated, the channel is working even if no data is being sent.

Packet Switching Networks

- In packet switching networks, messages are broken into packets, each of which includes a header with source, destination, and intermediate node address info.
- Individual packets may follow different routes to reach the destination
- The packet length is restricted to allow the switching devices to store packet data in memory
- It is a connection-less circuit, where packets can move from various routes and can be received in different order at the receiver's end.
- Each switch that acts as an intermediate route, maintains a routing table.



The original message is Green, Blue, Red.



- Packet-switching technologies are part of the basis for most modern Wide Area Network (WAN) protocols, including Frame Relay, X.25, and TCP/IP.
- packet switching networks are both effective and more efficient for data that can tolerate some transmission delays, such as site data and e-mail messages.

Pros

- Doesn't require intermediate storage
- Communication continues even if a switching node fails
- Multiple users can simultaneously use the channel.
- Ensures better bandwidth

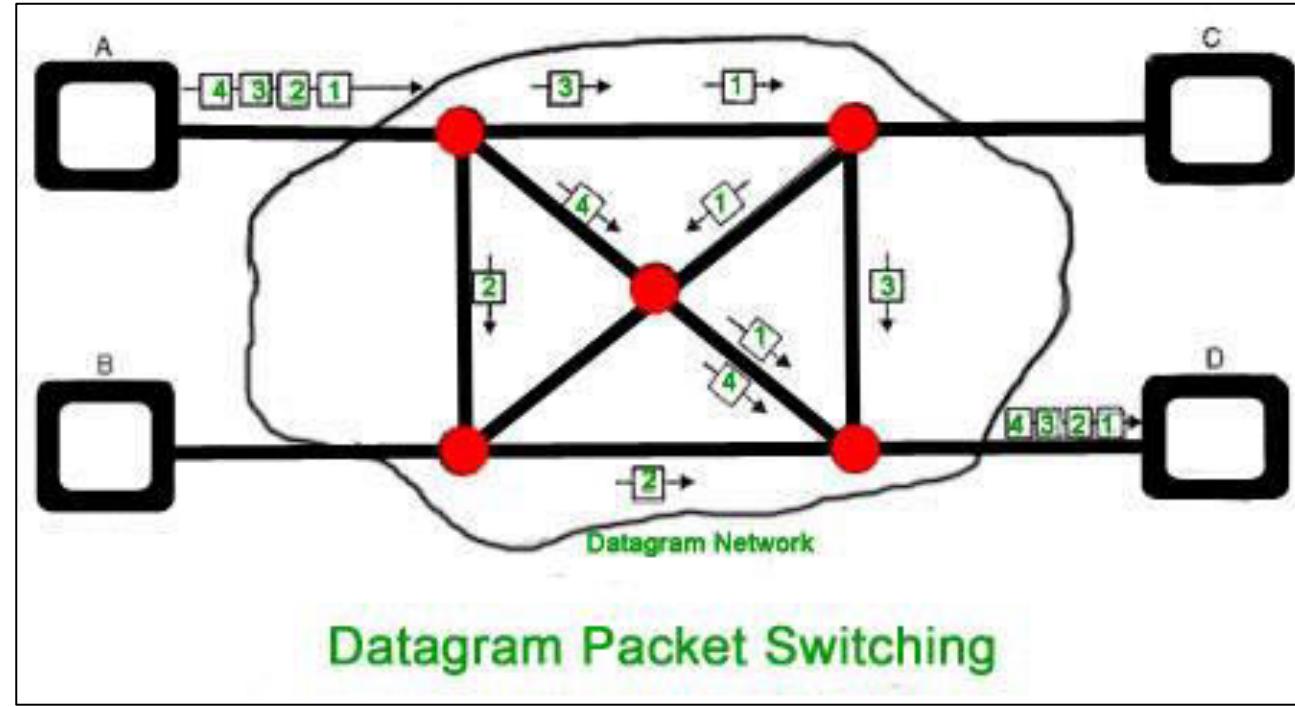
Cons

- Not suitable for real-time data transmission.
- Higher installation costs
- Require complex protocols for delivery.
- Packet delivery errors and losses can occur.

- There are two methods for packet switching
 - Datagram packet switching
 - Virtual circuit packet switching

Datagram Packet Switching Networks

- Here each message is divided into a stream of packets
- Each packet is treated as an independent unit with its own control instructions
- The switching devices route each packet independently through the network.
- Before transmission starts, the sequence of packets and their destinations are established by the exchange of control information before the sending terminal, the network, and the receiving terminal.
- The resources are allocated on demand and on the first-come-first-serve basis
- The packets may arrive out of order at the destination
- Some delay may be experienced, since each packets follow different paths.
 - Some packets may also be lost due to lack of resources
- The networking nodes here are routers.
 - The packets are called the Datagram



Pros

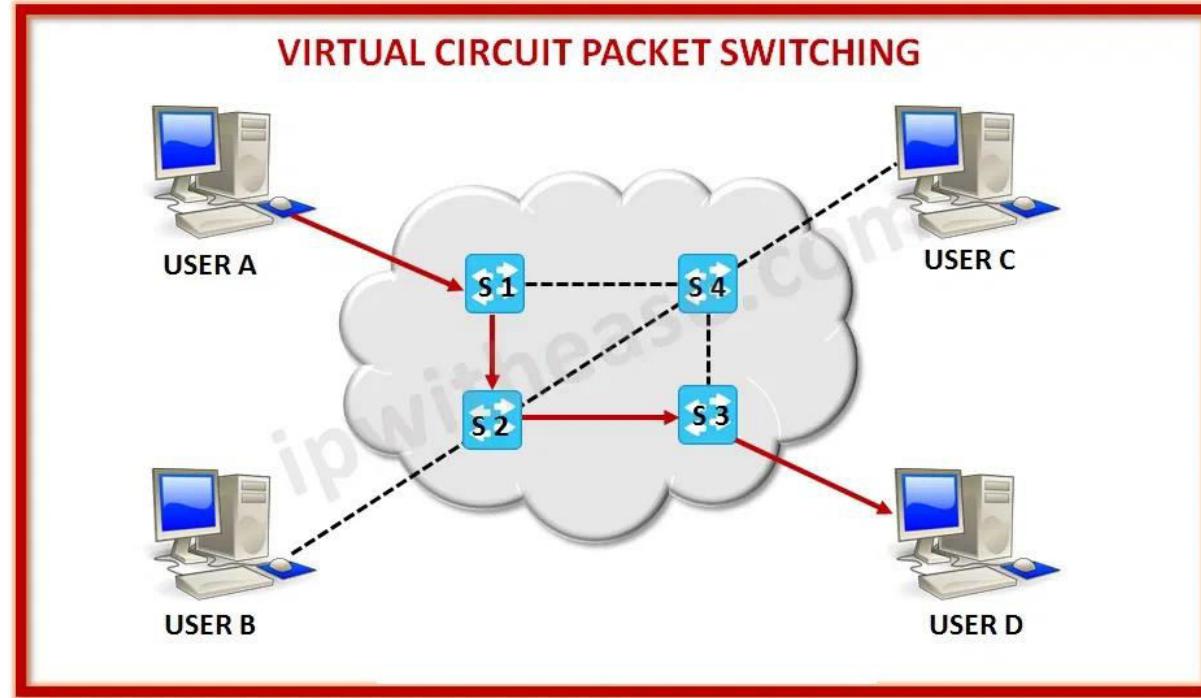
- Greater utilization of channel
- Priority levels can be implemented
- Feature of retransmission for lost data
- New calls can be added without affecting already-added users

Cons

- Not so good for real time operations
- Delay during transmission, processing, or queuing can be experienced
- More processing is required at the node.

VC Packet Switching Networks

- It establishes logical connection between sending and receiving devices, hence called the virtual circuit.
- Sender and receiver agree on communication parameters, such as message size and network path.
- After establishing virtual circuit, all packets travel through this logical connection.
- This network has characteristics of both circuit switching and a datagram network.
 - It has set up and tear down phase, just like circuit switching
 - It sends data in form of packets, just like datagram networks
- Just like in circuit switching, packets in VC switching networks follow the same path established during the setup phase



Pros

- Reserves bandwidth for connection during setup
- Fast processing and forwarding of packets
- Sequencing and error control is maintained

Cons

- If fault occurs in the selected node, all affected connections must be established again
- If a switch is not able to handle network traffic, the connection cannot be setup
- Dynamic routing tables are complex to maintain

End of chapter 3

Related questions from this chapter (6-10 marks)

1. What is PCM? Why is it needed? Explain the phases of PCM.
2. What is multiplexing. Mention pros and cons of multiplexing. Explain in detail the types of multiplexing that are commonly used in networking.
3. What is a switching network? Describe in brief the types of switching networks.
4. What is an X.25 network? Describe its working mechanism.
5. Differentiate circuit switching and packet switching networks.
6. Differentiate virtual circuit and datagram packet switching networks.
7. Write short notes on following
 - Guided media
 - Line of Sight
 - Satellite communication
 - Modem

CHAPTER 4

THE DATA LINK LAYER

5 hours

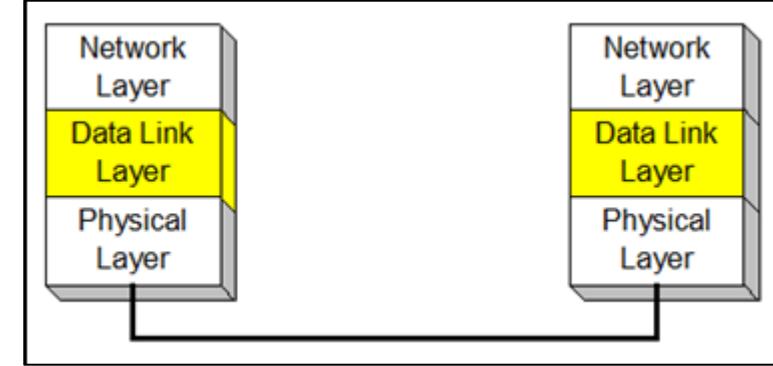
~ 8 marks

Chapter overview

- ❖ Error Detection and control mechanisms
 - CRC, Checksums, Hamming Codes
- ❖ Sliding window protocols
 - One bit sliding, Go Back N, Selective Repeat
- ❖ IEEE standard 802 for LAN: 802.3 , 802.4, 802.5
- ❖ FDDI (Fiber Distributed Data Interface) Network
- ❖ Satellite Networks
 - SPADE, ALOHA

Background

- OSI layer has 7 layers
 - ❖ Data link layer lies on the 2nd position from below
- Data link layer plays crucial role for achieving reliable and efficient communication between two communicating machines.
 - ❖ It is concerned with sending data to the next immediate neighbor
- DLL basically deals with frame formation, flow control, error control, addressing and link management.
- 3 main task in DLL is:
 - ❖ Framing: converting streams of data into a packaged format
 - ❖ Error handling steps for accurate transmission of message
 - ❖ Flow control to ensure that communication is stable



4.1 Error Detection and Correction mechanisms

- When digital signals are transmitted over a channel, the signal might get contaminated due to the presence of noise.
 - ❖ This noise can introduce error in the binary bits.
 - ❖ So, a 1 may become a 0 and vice versa
- Errors can occur on a single bit of data, or can occur on one or more bits.
 - ❖ If $100110 \rightarrow 100100$, then it is a single bit error
 - ❖ If $01110011 \rightarrow 01011001$, then it is a burst error
- In the DLL, errors should be detected and if possible, corrected.
 - ❖ Errors are inevitable. Idea is to communicate correctly despite having errors.

- Error detection methods are:
 1. **Parity Checks**
 - Addition of one extra bit to each word being transmitted
 - Odd Parity is set so that no. of 1 bits in the entire word is odd.
 - Even parity is set so that no. of 1 bits in the entire word is even.
 2. **Checksum error detection**
 - As each word is transmitted, it is added to the previously sent word.
 - The sum up to that time is sent as well.
 - The sum of corresponding words as well as the check sum value determines if there is error during reception or not.
 3. **Cyclic Redundancy Check (CRC)**
 - A polynomial code generated and sent along the message.
 - CRC checker divides the combination of message and CRC value. If the remainder is 0, then code is error-free.

4.1 (a) Cyclic Redundancy Check (CRC)

- CRC is an error detection code normally used in digital networks and storage devices to detect the accidental changes to the raw data.
- Block of data entering the system gets a short checked value attached based on a polynomial division of their contents
- CRC are called so because the check value is a redundancy without adding information and the algorithm is based on cyclic code
- It is easy to analyze
- An efficient method for error analysis.
- CRC uses **Generator Polynomial** which is available on both sender and receiver side.

On sender's side

- Message is listed in binary form.
 - E.g. $M(x) = 10111$
- A divisor value is either given, or is generated from a polynomial expression.
 - If the polynomial is x^3+x+1 , then the divisor value is 1011
- If the no. of bits in the divisor value is n , then append $(n-1)$ no. of zero to the message $M(x)$.
 - E.g. here divisor value bits=4. So, 3 zero are appended to $M(x)$.
- Divide the newly appended $M(x)$ with the divisor.
 - In this division, XOR operation is used instead of basic subtraction.
- Remainder to this division is our CRC value.
 - (it will also have one bit less than divisor)
- Replace the previously appended no. of zeros with the CRC value.

On receiver's side

- Receiver receives codeword consisting of data and the CRC.
- Receiver divides it by the divisor value.
- If the codeword is exactly divisible by the divisor, then received codeword is error-free.
- If the codeword produces a remainder, then the received codeword consists of errors.

E.g. Codeword → 1100 1001 01011

Divisor → 10101

Is this codeword free of errors?

$$\begin{array}{r} 11 \\ \hline 10101) 1100100101011 \\ \oplus \quad 10101 \\ \hline 01100\textcolor{red}{0} \\ \oplus \quad 10101 \\ \hline 01101\textcolor{red}{0} \end{array}$$

And the sequence continues....

At last, Quotient → 1111100001 and Remainder → 1110

Since there is a remainder, the codeword consists of errors

	1	1	1	1	1	0	0	0	1		
—	—	—	—	—	—	—	—	—	—		
	1	1	0	0	1	0	0	1	0	1	1
	1	0	1	0	1						
—	—	—	—	—	—	—	—	—	—	—	—
	1	1	0	0	0	0	1	0	1	0	1
	1	0	1	0	1						
—	—	—	—	—	—	—	—	—	—	—	—
	1	1	0	1	0	1	0	1	1		
	1	0	1	0	1						
—	—	—	—	—	—	—	—	—	—	—	—
	1	1	1	1	1	0	1	1			
	1	0	1	0	1						
—	—	—	—	—	—	—	—	—	—	—	—
	0	0	0	1	1	0	1	1			
	0	0	0	0	0						
—	—	—	—	—	—	—	—	—	—	—	—
	0	0	1	1	0	1	1				
	0	0	0	0	0						
—	—	—	—	—	—	—	—	—	—	—	—
	0	1	1	0	1	1					
	0	0	0	0	0						
—	—	—	—	—	—	—	—	—	—	—	—
	1	1	0	1	1						
	1	0	1	0	1						
—	—	—	—	—	—	—	—	—	—	—	—
	1	1	1	0							

E.g. generate CRC code for Message → 1100 10101
consider Divisor → 10101

- Divisor bits=5
- So no. of zeros to append = 4
- So, the appended message value becomes → 1100 10101 0000
- Dividing this appended value by the given divisor we get
 - Remainder → 1011
- Replacing the added zeros with this remainder, we get
 - 1100 10101 1011
- This is our required CRC code

	11110111

	1100101010000
	10101

	110001010000
	10101

	11011010000
	10101

	1110010000
	10101

	100110000
	10101

	01100000
	00000

	11000000
	<u>10101</u>
	110100
	10101

	11110
	10101

	1011

E.g. $M(x) \rightarrow 1010011110$

Generator polynomial= x^3+x+1

Calculate CRC codeword for above transmission.

Soln:

- Divisor $\rightarrow 1011$
- Appended $M(x) \rightarrow 1010011110\ 000$
- Remainder after divisor divides appended $M(x) \rightarrow 001$
- So, CRC code $\rightarrow 10100\ 11110\ 001$

4.1 (b) CheckSum

- Here the transmitted message is accompanied by a numerical value based on the number of bits in the message
- The receiver station applies formula to the message and checks to make sure if the accompanying value is same or not.
- E.g. for set of number (1,2,4,5,6), the sender sends (1,2,4,5,6,18) in the channel, where 18 is the sum of original 5 numbers
- The receiver receives all the numbers and then adds 5 numbers to see if the sum matches with last received no., i.e. the sum

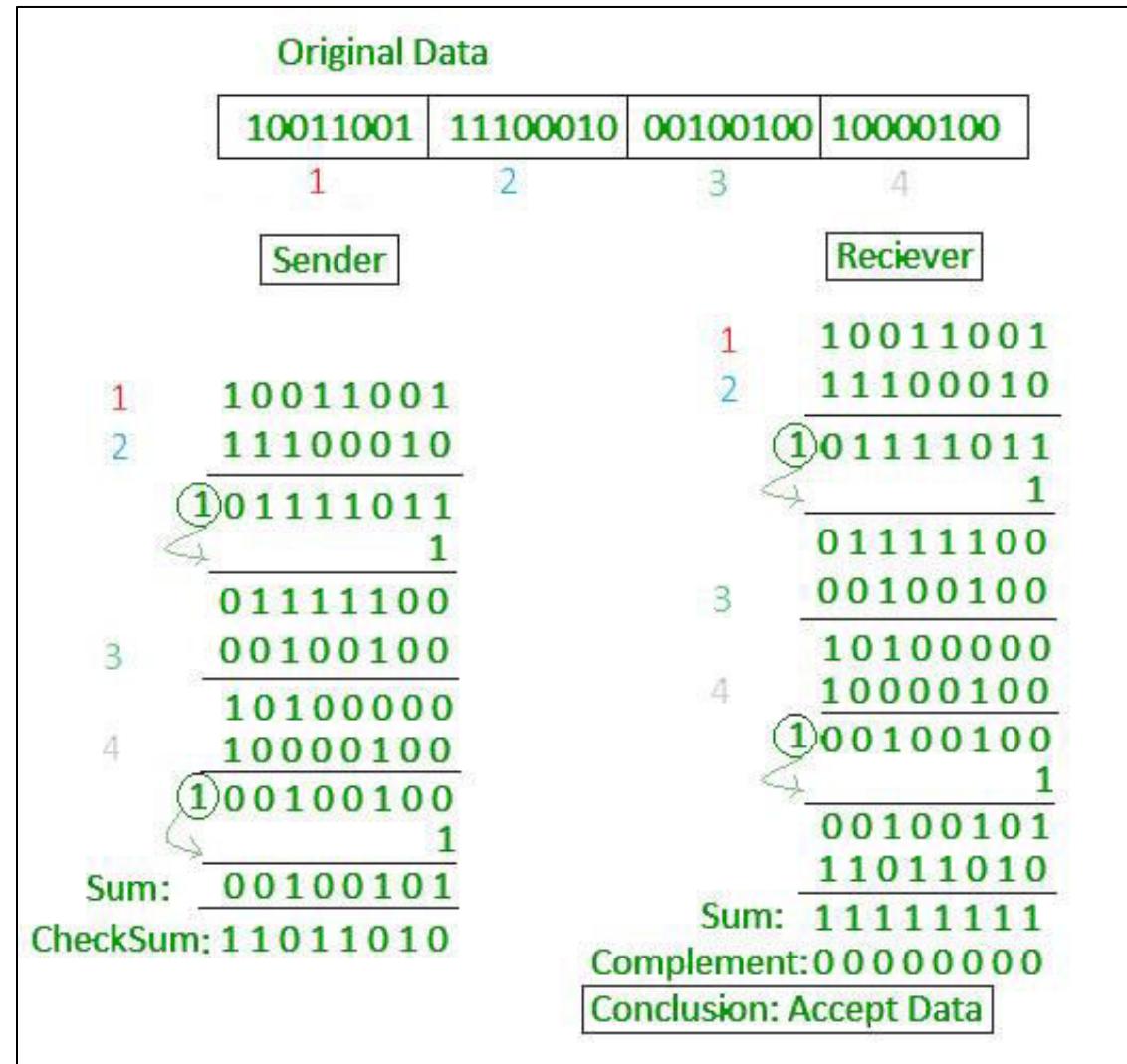
At the sender's side

- Divide message into 16-bit words
- Value of checksum word is initially set to 0
 - Any carry over occurring on the MSB after each addition operation are added to the sum during each iteration of addition.
 - The carry occurring at the last iteration is discarded.
- This sum is complemented to obtain the final checksum.

At the receiver's side

- Received message is divided into 16 bit words
- All words, including the checksum, are added using 1's compliment addition.
- This sum is complemented [1's].
 - If the compliment yields all zeros, message is accepted.

E.g. for $m=10011001, 11100010, 00100100, 10000100$, calculate the checksum



E.g. for $m =$
11001100,
10101010,
11110000,
11000011,
 calculate the
 checksum

Sender's End	Receiver's End
Frame 1: 11001100	Frame 1: 11001100
Frame 2: + 10101010	Frame 2: + 10101010
Partial Sum: 1 01110110	Partial Sum: 1 01110110
+ 1	+ 1
01110111	01110111
Frame 3: + 11110000	Frame 3: + 11110000
Partial Sum: 1 01100111	Partial Sum: 1 01100111
+ 1	+ 1
01101000	01101000
Frame 4: + 11000011	Frame 4: + 11000011
Partial Sum: 1 00101011	Partial Sum: 1 00101011
+ 1	+ 1
00101100	00101100
Sum: 00101100	Checksum: 11010011
Checksum: 11010011	Sum: 11111111
	Complement: 00000000
	Hence accept frames.

4.1 (c) Hamming Codes

- Hamming code is a block code that is capable of detecting up to two simultaneous bit errors and correcting single-bit errors.
- The message is divided into fixed-sized blocks of bits, to which redundant bits are added for error detection or correction.
- In this coding method, the source encodes the message by inserting redundant bits within the message. These redundant bits are extra bits that are generated and inserted at specific positions in the message itself to enable error detection and correction.
- When the destination receives this message, it performs recalculations to detect errors and find the bit position that has error.

Hamming code mechanism

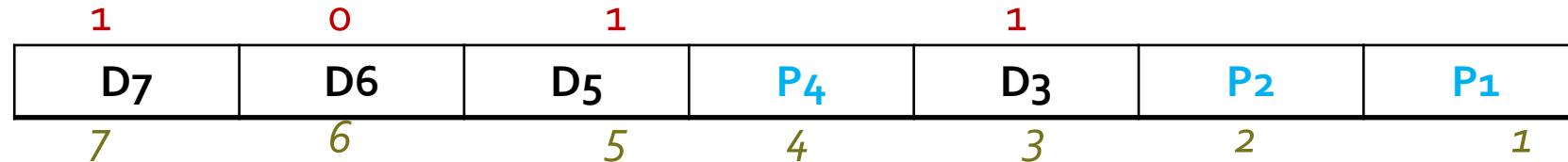
- Generally made out of 7-bit.
 - But can be adjusted to any no. of bit
- Data bits are placed in specific positions. Based on the no. of bit chosen, the empty spaces are filled with parity bits.
 - For 7bit code, there are 3 parity bits
 - For 15 bit code, there are 4 parity bits
- Parity bits are always inserted in 2^n bit locations, i.e. 1st, 2nd, 4th, 8th, etc.
- E.g. for 1011 message, the codeword will be [1 0 1 P₄ 1 P₂ P₁]

How to calculate parity bit values?

- $P_1 \rightarrow 1, 3, 5, 7, 9, 11, 13, 15, \dots$
 - $P_2 \rightarrow 2, 3, 6, 7, 10, 11, 14, 15, \dots$
 - $P_3 \rightarrow 4, 5, 6, 7, 12, 13, 14, 15, \dots$
 - $P_4 \rightarrow 8, 9, 10, 11, 12, 13, 14, 15, \dots$
-
- P_1 is adjusted to 0 or 1 so as to establish even parities over bits 1, 3, 5, 7
 - P_2 is adjusted to 0 or 1 so as to establish even parities over bits 2, 3, 6, 7
 - P_3 is adjusted to 0 or 1 so as to establish even parities over bits 4, 5, 6, 7

E.g. generate 7bit hamming code for **1011**.
Consider even parity code for data.

- Since word is **1011**, the hamming code will have following format



- For **P₁**, we look at **1,3,5,7** position values.
 - Here D₃D₅D₇ values are **111**. So P₁=1 to set even parity
- For **P₂**, we look at **2,3,6,7** position values
 - Here D₃D₆D₇ values are **101**. So P₂=0 to set even parity
- For **P₄**, we look at **4,5,6,7** position values
 - Here D₅D₆D₇=**101**. So P₄=0 to set even parity
- So our codeword is **1010101**

Detection and correction of errors

- When hamming code is transmitted, at receiver end, it is decoded to get the data back.
- Receiver checks even parity on the bits $(1,3,5,7)$, $(2,3,6,7)$ and $(4,5,6,7)$.
 - If these combinations have even parities then the received codeword is correct.
- If any combination contains odd parity value, then the value of the corresponding parity bit is set to the error word.
 - E.g. if $2,3,6,7$ yield odd parity value, then P_2 is set to 1 on the error word.
 - If the parity seems even value, then P_2 is set to 0 on the error word
- Error word is then written as the combination of parity bits set on the previous process
 - E.g. if $P_1=1$, $P_2=1$, $P_4=0$, then error word = 011.

Detection and correction of errors

- By treating the values on the error word as the binary values, we determine the decimal value of the number as seen on the error world.
 - E.g. If $P_4 P_2 P_1 \rightarrow 101$, then $E = (101)_2 \rightarrow (5)_{10}$
- This decimal equivalent value gives us the location of bit that needs to be changed to correct the codeword.
 - E.g. from above calculation, we can see that the 5th position value needs to be changed.
 - So if $D_5 \rightarrow 1$, then we change it to 0 now.

E.g. a 7-bit code is received as 1110101. Is the code correct?

- Here,
 - 1,3,5,7 → even no. of 1s → no error → set $P_1=0$
 - 2,3,6,7 → odd no. of 1s → error → set $P_2=1$
 - 4,5,6,7 → odd no. of 1s → error → set $P_4=1$
- Hence, for error word, $E = (P_4 P_2 P_1) = (110)_2 \rightarrow (6)_{10}$
- Hence we invert the 6th position value to correct the code
- Hence the corrected code is 1010101.

Error detection and correction

- During transmission of message frames, messages that are received may have been affected by noise to produce errors.
- Such errors must be detected and corrected as much as possible.
- There are 2 basic systems for correction:
 - Forward Error Correction (FEC) – Here the receiver search for most likely correct codeword. Valid keyword having the minimum distance (having least no. of differences in the arrangement of numbers) is selected as the most likely correct version.
E.g. Hamming Codes, CRC
 - Automatic Repeat Requests (ARQ) – Here, when an error is detected, a request is made for the retransmission of that signal.

Error Detection Mechanism

1. Parity Checking
2. Checksum
3. CRC

Error Correction Mechanism

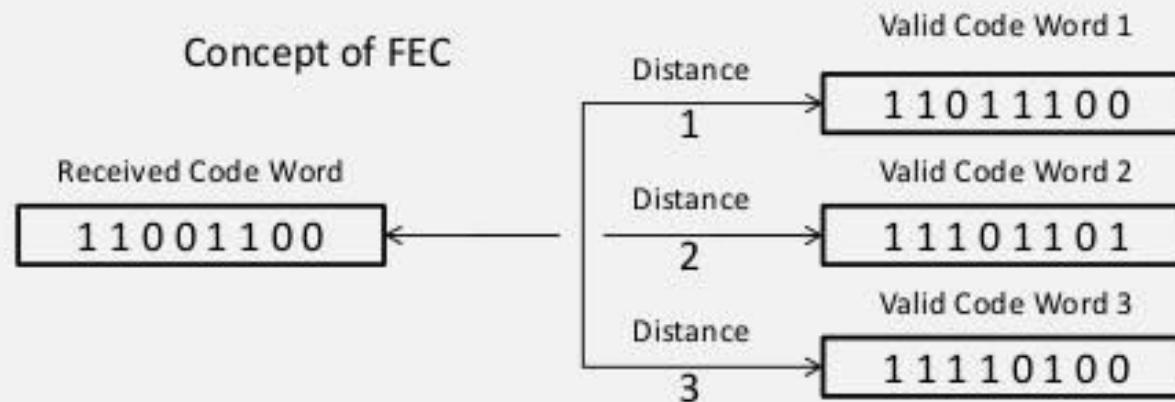
1. Forward Error Correction (FEC)
 - using hamming codes
 - using cyclic codes
2. ARQ technique

FEC (Forward Error Correction)

In FEC the receiver searches for the most likely correct code word.

When an error is detected, the distance between the received invalid code word & all the possible valid code words is measured.

The nearest valid code word (the one having minimum distance) is the most likely correct version of the received code word as shown in given figure.



In given figure, The valid code word 1 has the minimum distance (1), hence it is the most likely correct code word.

ARQ Technique (Retransmission)

There are two basic systems of error detection & correction they are

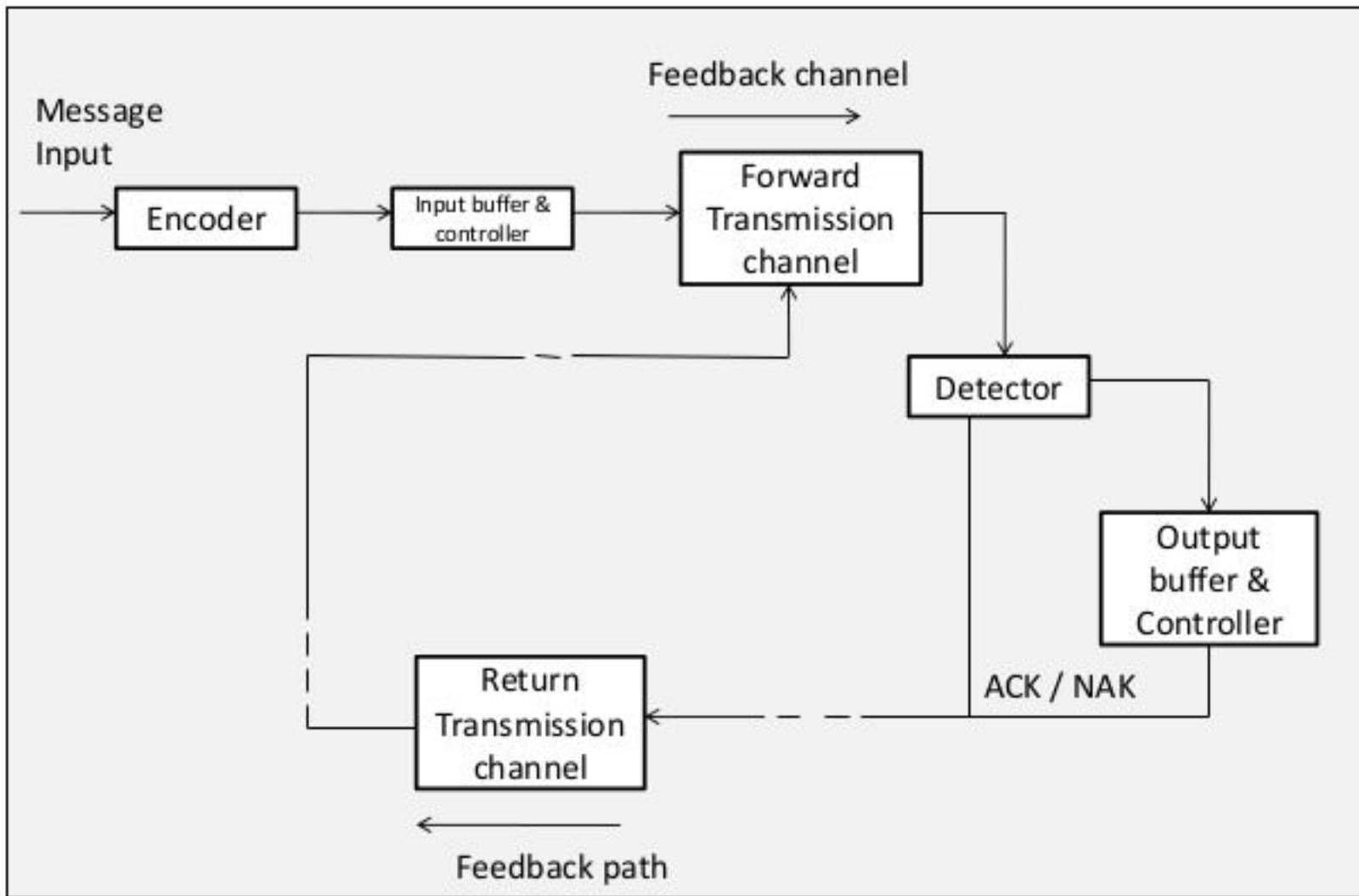
- Automatic repeat request (ARQ).
- Forward error correction (FEC).

In ARQ system when error is detected, a request is made for the retransmission of that signal.

The points differs ARQ & FEC are:-

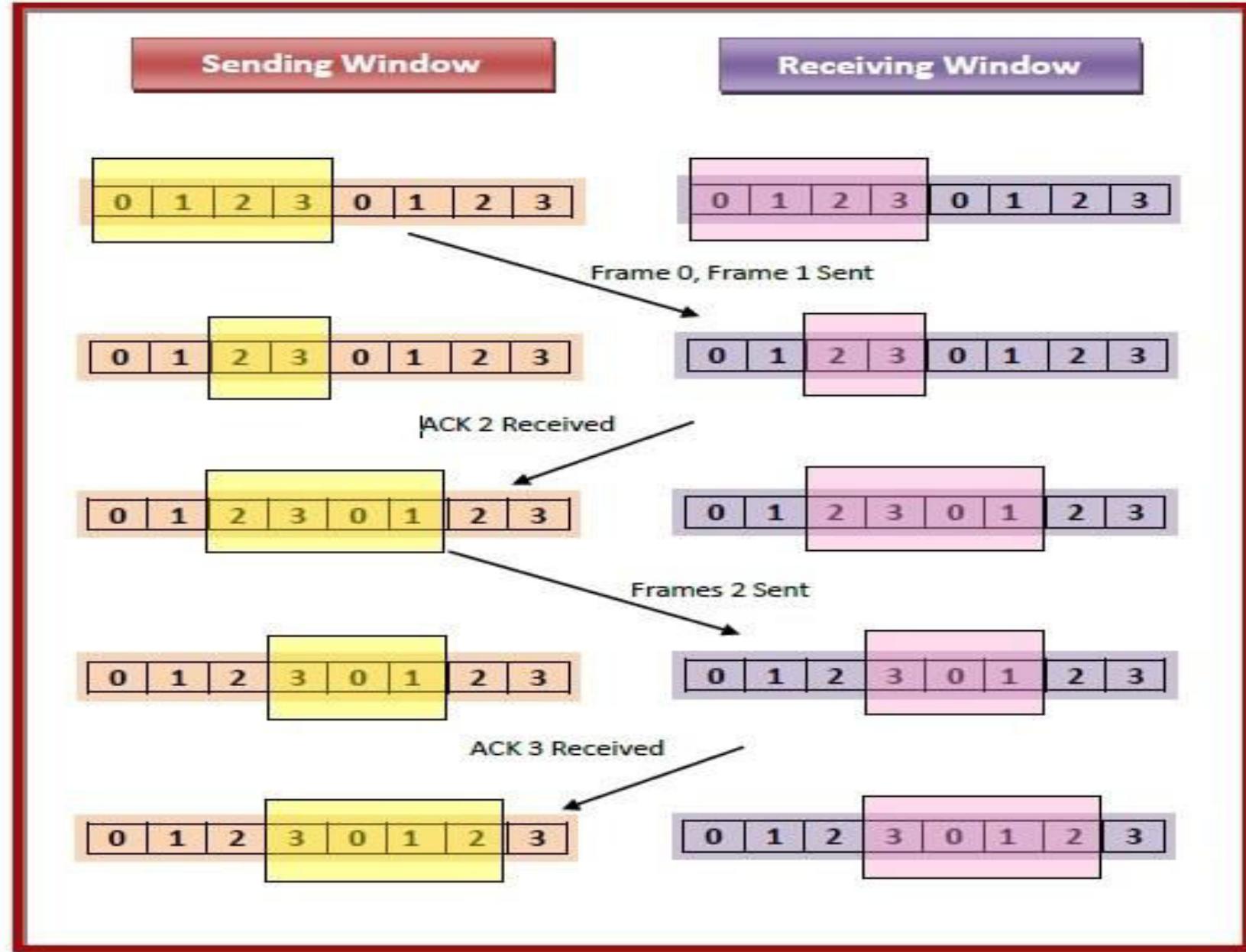
- In ARQ system less number of check bits (parity bits) are required to be sent. This will increase the (k/n) ratio for an (n,k) block code if transmitted using the ARQ system.
- A return transmission path & additional hardware in order to implement repeat transmission of codeword's will be needed.
- The bit rate of forward transmission must make allowance for the backward repeat transmission.

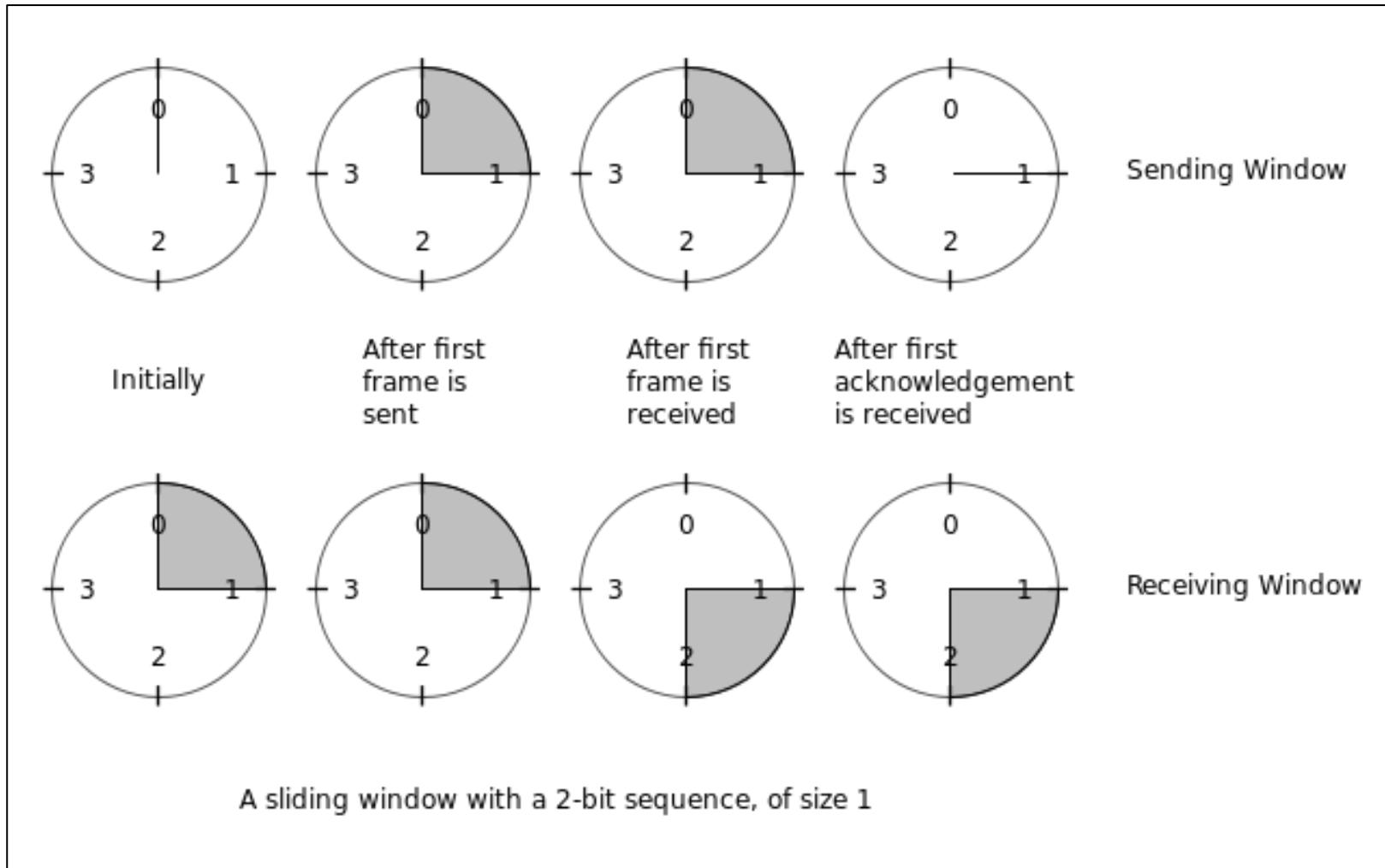
Block Diagram of the basic ARQ System



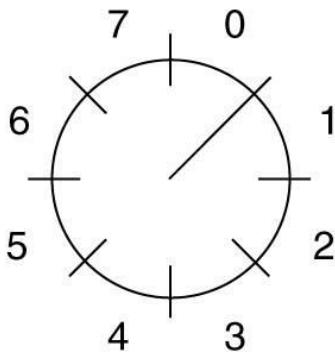
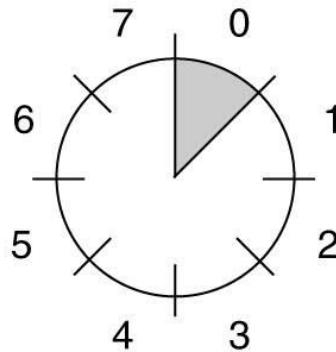
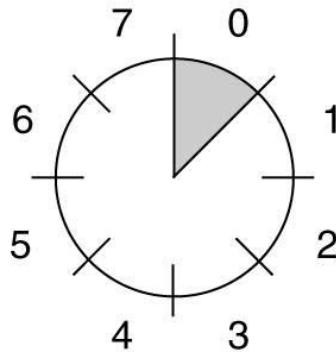
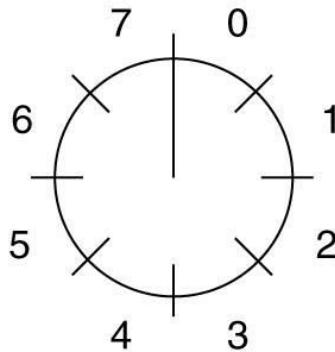
4.2 Sliding Window Protocols

- A part of ARQ technique
- Sliding window are the imaginary boxes at the transmitter and the receiver.
- This window holds the frames at either end and provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgement.
- At any instant of time, the sender maintains a set of sequence numbers corresponding to the frames permitted to send.
 - These frames which are being permitted to send are said to be falling in the ***sending window***.
 - The receiver also maintains a ***receiver window***. It corresponds to the set of frames permitted to accept.
- The sender's and receiver's window need not be of same size.
- The sequence numbers within the sender's window represents the number of frames sent but not yet acknowledged.
 - The frames that are unacknowledged can be either damaged or lost during transmission.
 - Hence all the frames are stored in memory in case of scenario for retransmission.

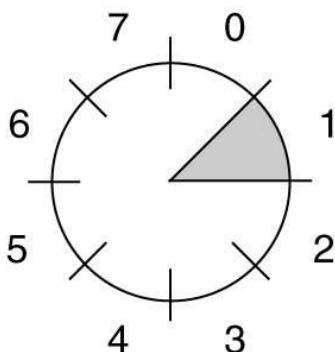
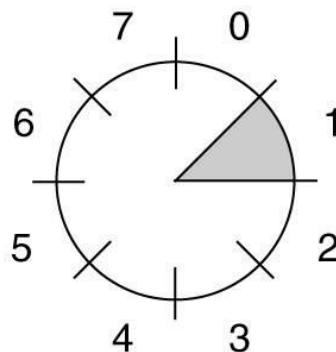
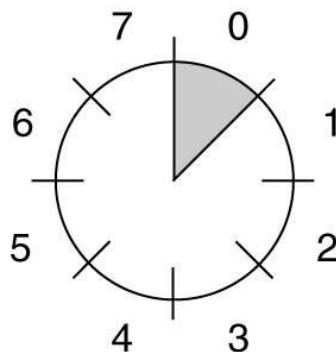
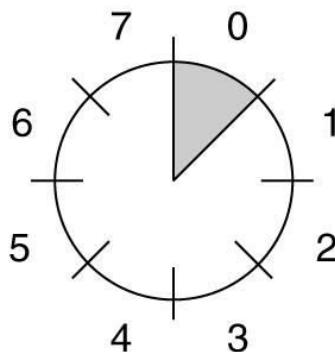




Sender



Receiver



(a)

(b)

(c)

(d)

Sliding Window Protocols

There are 3 protocols[mechanism] used in sliding window:

1. **1-bit sliding window**

- Sending one frame at a time and wait for its acknowledgement before sending another frame.
- Also called stop-and-wait protocol.

2. **Go back N protocol**

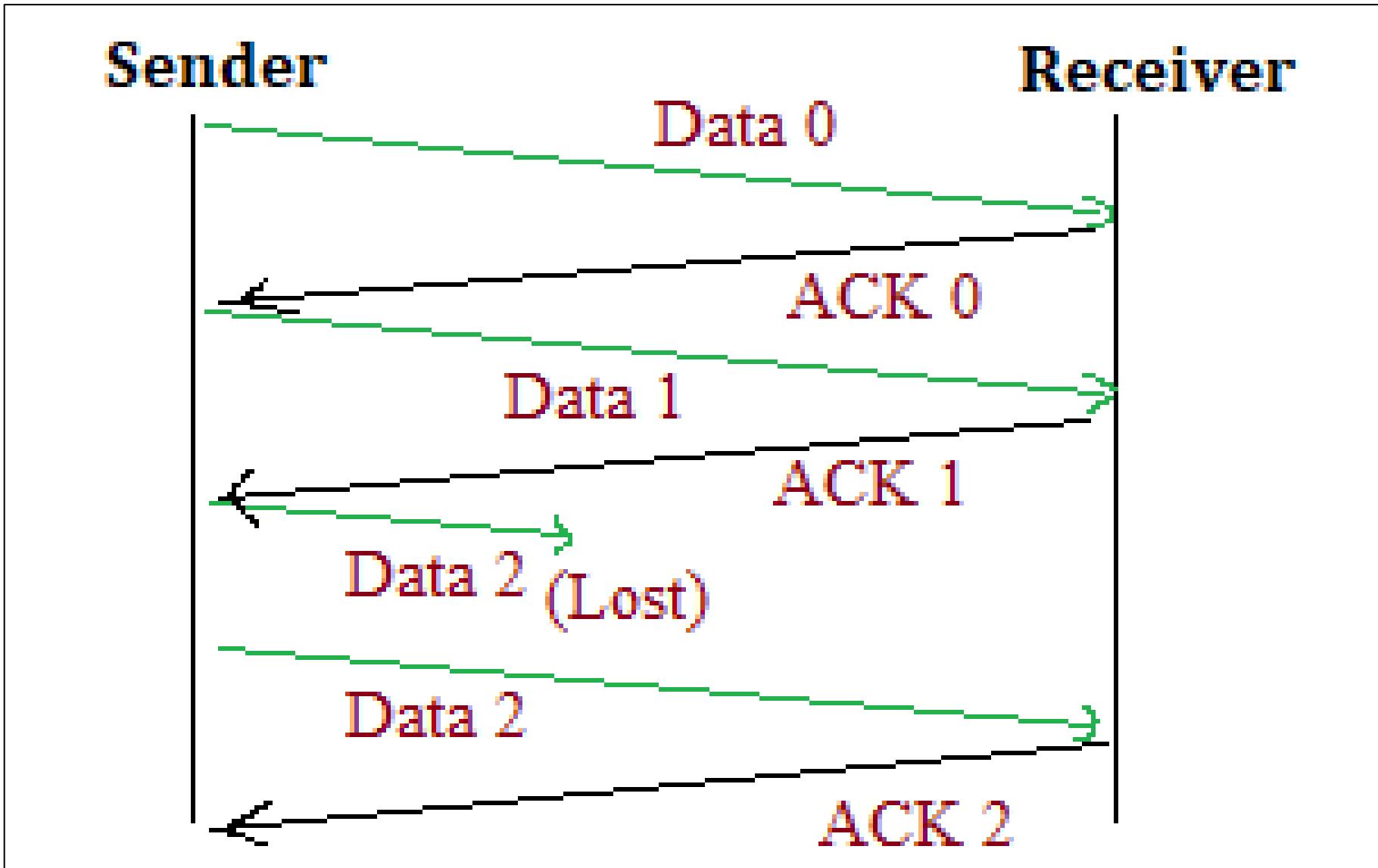
- During transmission, if one frame is damaged or lost, all frames are sent since the last acknowledged frame.
- Here, the sender doesn't wait for ACK signal for transmission of next frame. It sends the frames continuously as long as it doesn't receive a NAK signal.

3. **Selective Repeat ARQ**

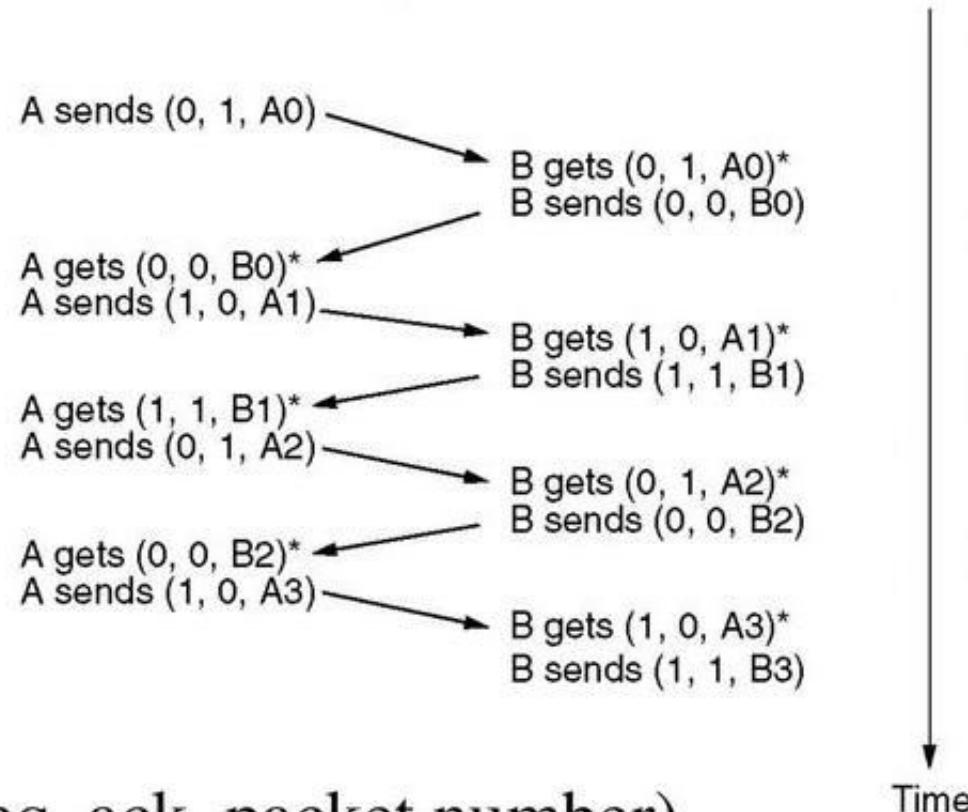
- In case of retransmission, sender can send particular frames that were lost or damaged.
- Most efficient but complex protocol

4.2 (a) One bit sliding

- Also known as a one-bit protocol since the maximum window size is 1.
 - That means, only one frame can be sent or received at one instant of time.
- It uses stop-and-wait technique.
 - This means, the sender sends one frame and waits to get its acknowledgement
 - Only after receiving the acknowledgement, it transmits next frames
- Operations occurring:
 - DLL from sending machine fetches the first packet from the Network Layer
 - DLL builds a frame for it and sends it to receiver [sends towards its physical layer]
 - Receiver machine's DLL looks at the frame for any possible duplication or error
 - If the frame is valid correct, receiver machine's DLL sends an ACK signal
 - If a frame is damaged, receiver machine can send a NAK signal for retransmission of that frame.
 - If no ACK is received, sender machine resends the frame.
 - Receiver machine's DLL passes the frame to its network layers



A One-Bit Sliding Window Protocol

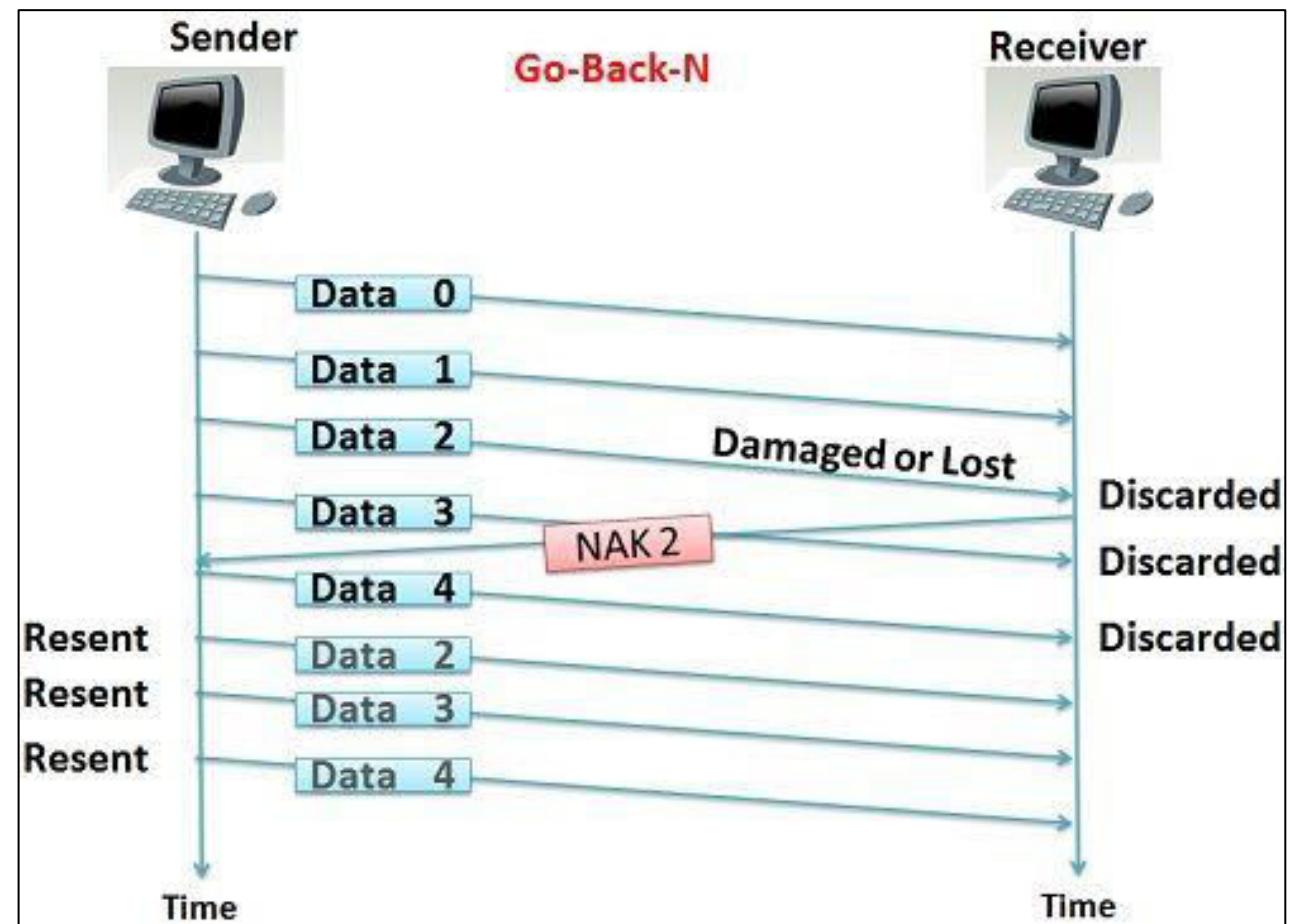
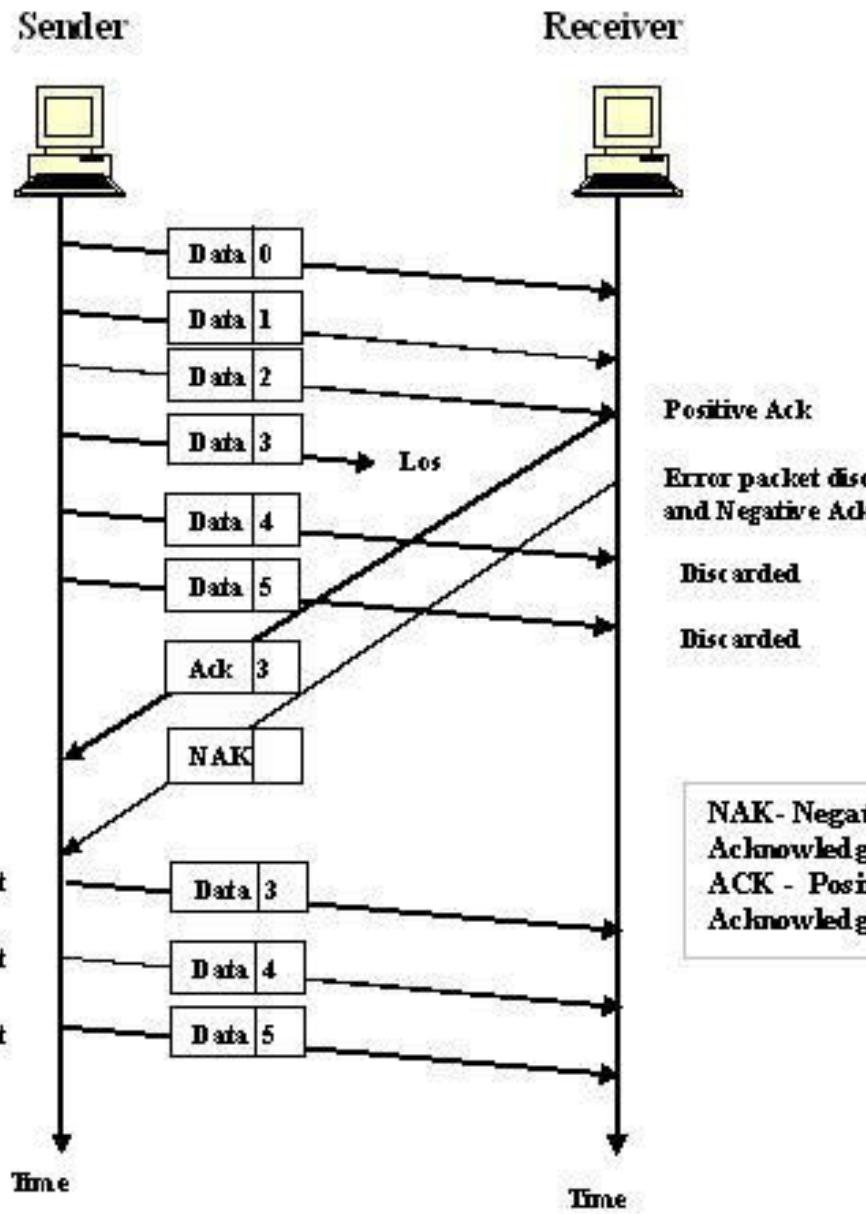


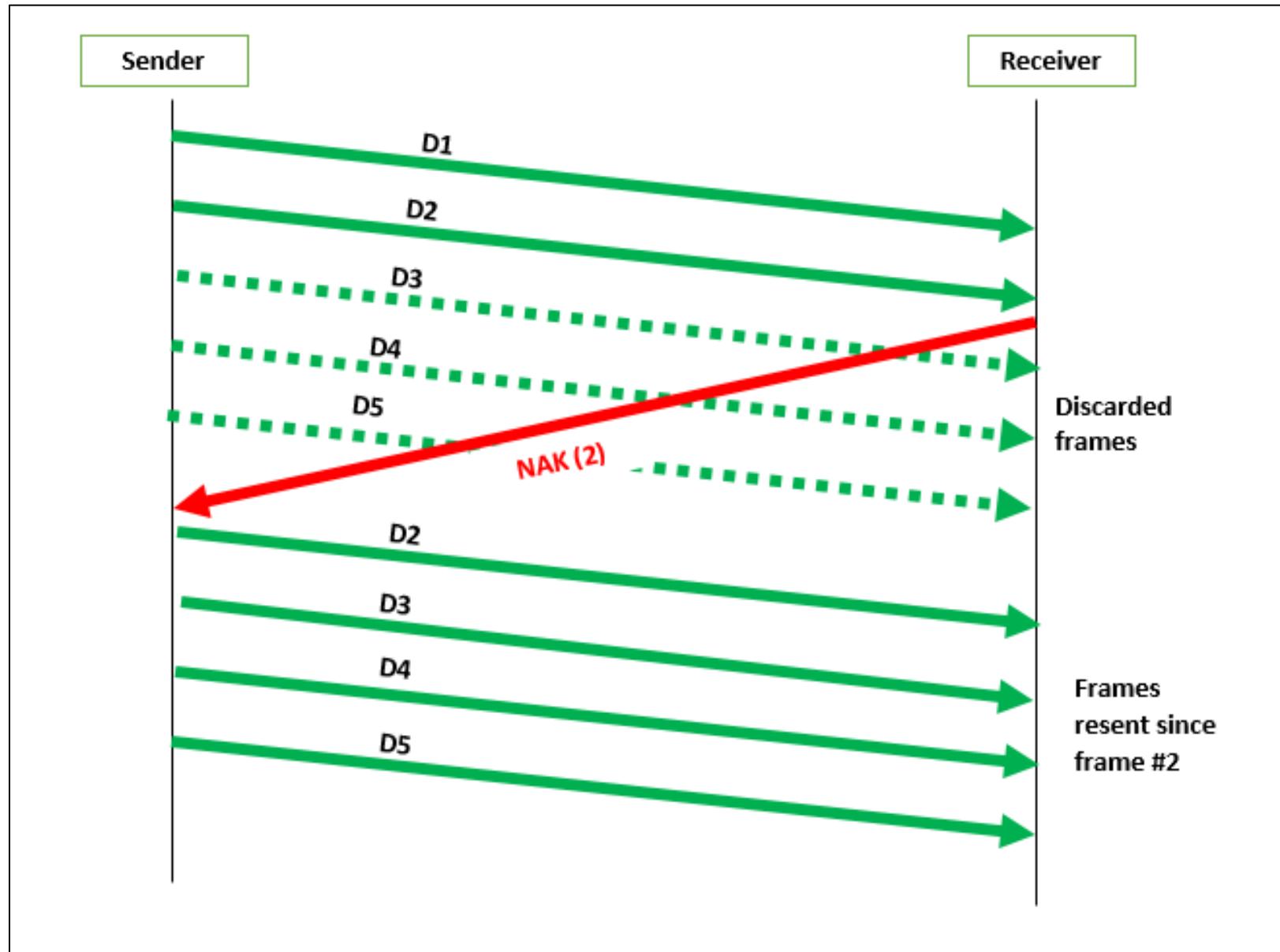
The notation is (seq, ack, packet number).

* indicates where a network layer accepts a packet.

4.2 (b) Go back N

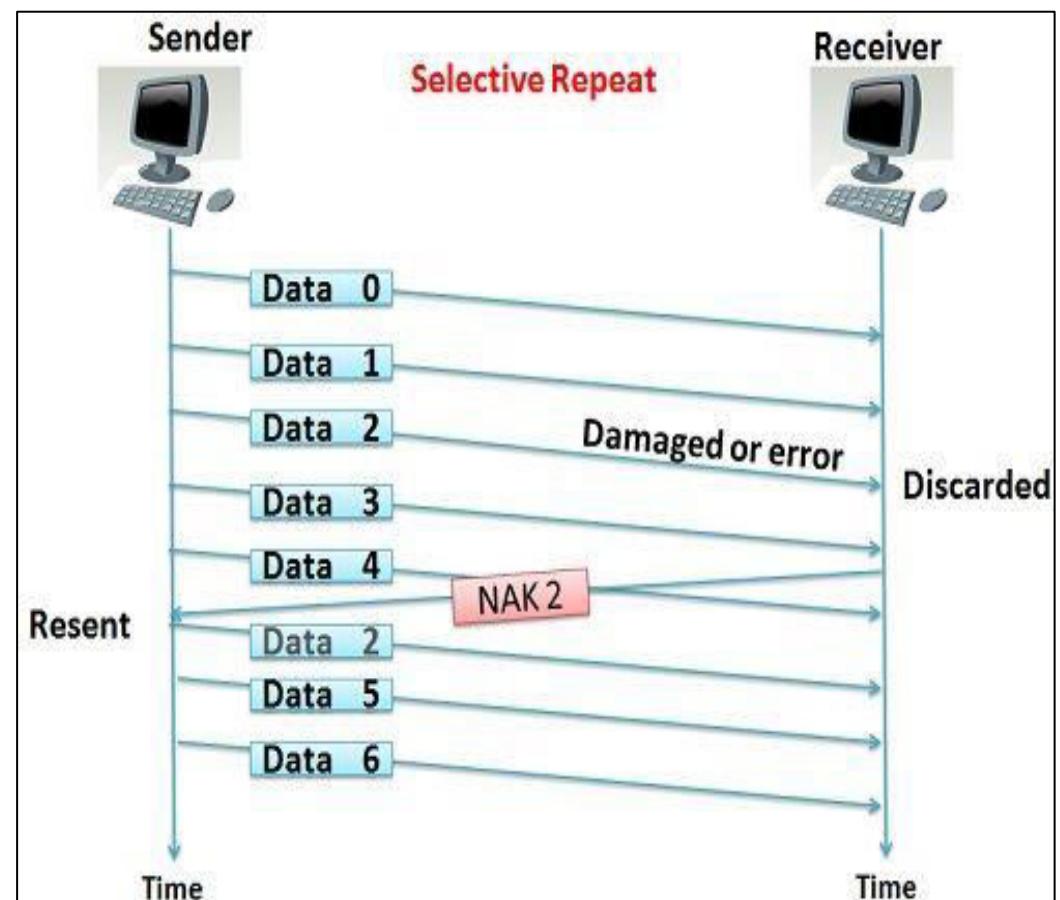
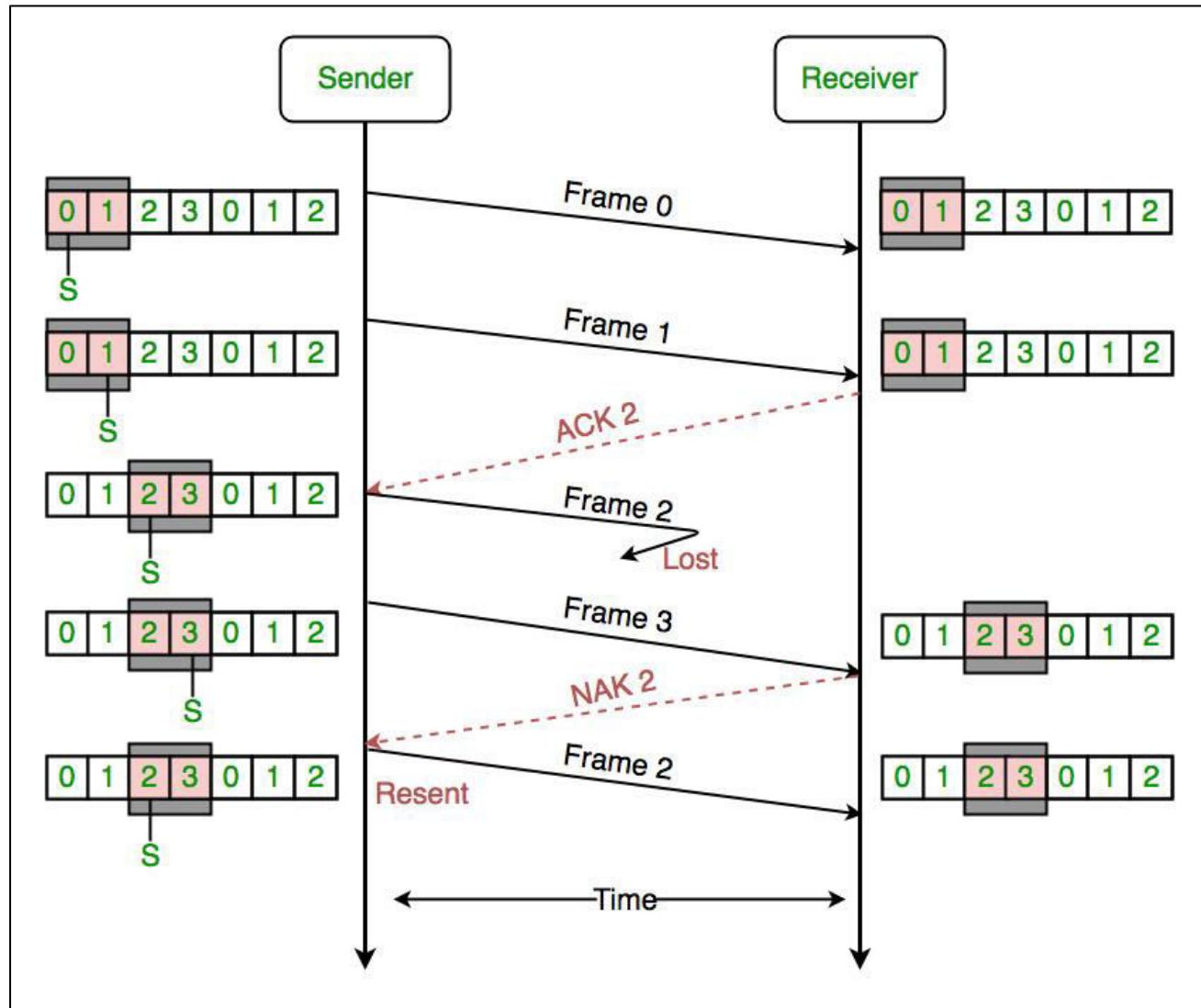
- A modification of stop and wait protocol.
 - The time between a received frame and its corresponding ACK signal was considered to be negligible. But this is not always the case (E.g. satellite communication has propagation delay)
- Here, the transmitter continues sending enough frames so that the channel is kept busy while the transmitter is waiting for ACK signals.
- In this method, if one frame is lost or damaged, the sender has to send all the frames since the last acknowledged frame number.
 - If a frame is damaged, receiver sends a NAK signal to the sender.
 - Sender then resends all the frames starting from that particular frame till the last of the windows or till further NAK signals are encounteredm

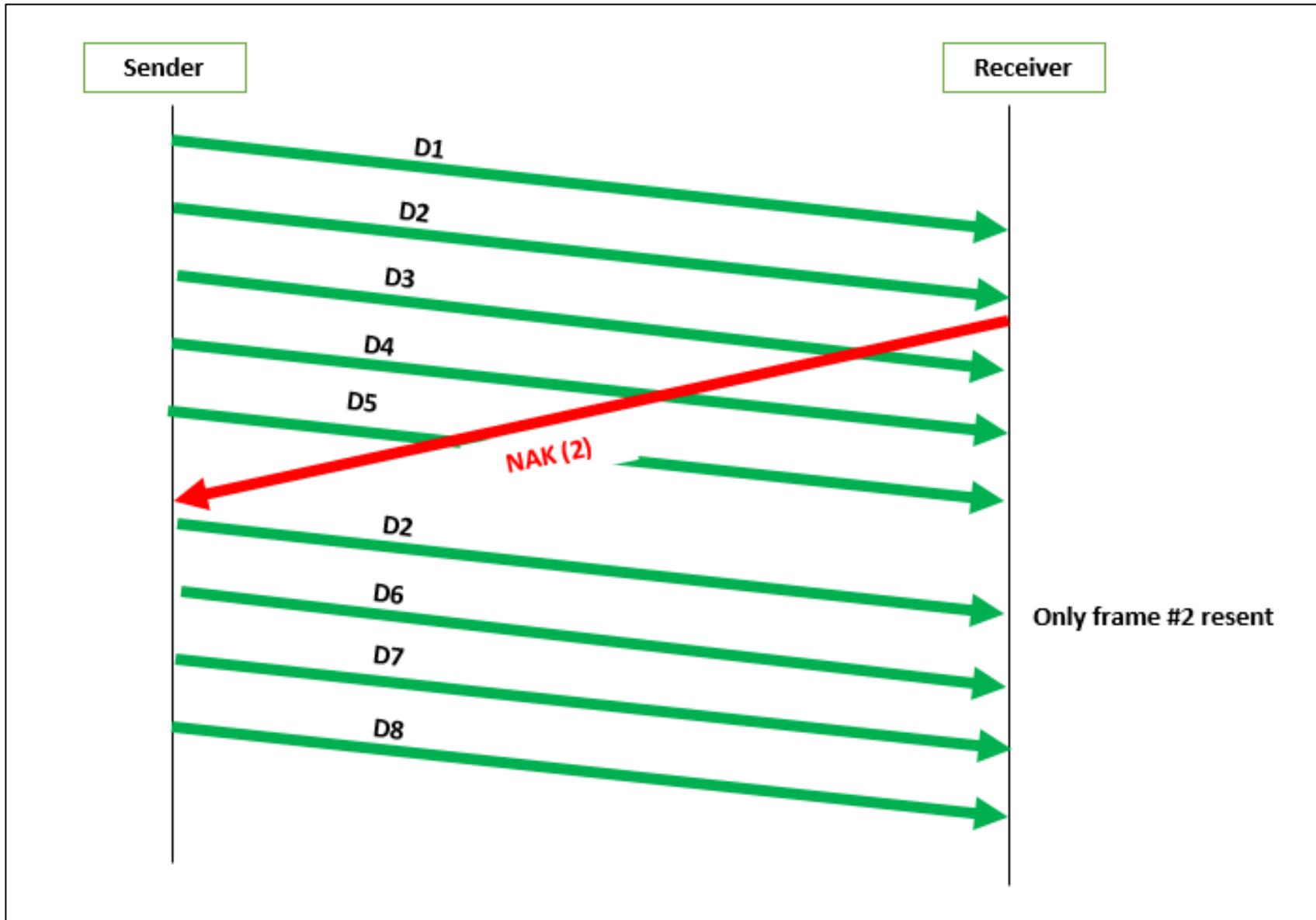




4.2 (c) Selective Repeat

- Here, only selective lost or damaged frames are retransmitted.
- Whenever receiver doesn't receive a frame or obtains a damaged frame, it sends a NAK signal to the sender.
- When sender receives the NAK signal, it resends the requested frame.
- All other frames that were previously sent to the receiver are accepted by the receiver.
 - This is in contrast to the go-back-N protocol where all other frames would be discarded.
- Since the frames can be received without a proper sequence due to retransmission, receiver machine should maintain the sequential ordering of the frames.
- The most efficient but the most complex protocol.





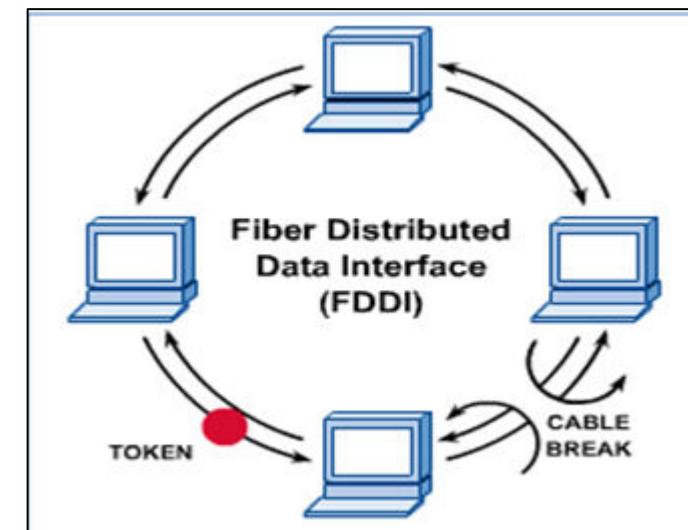
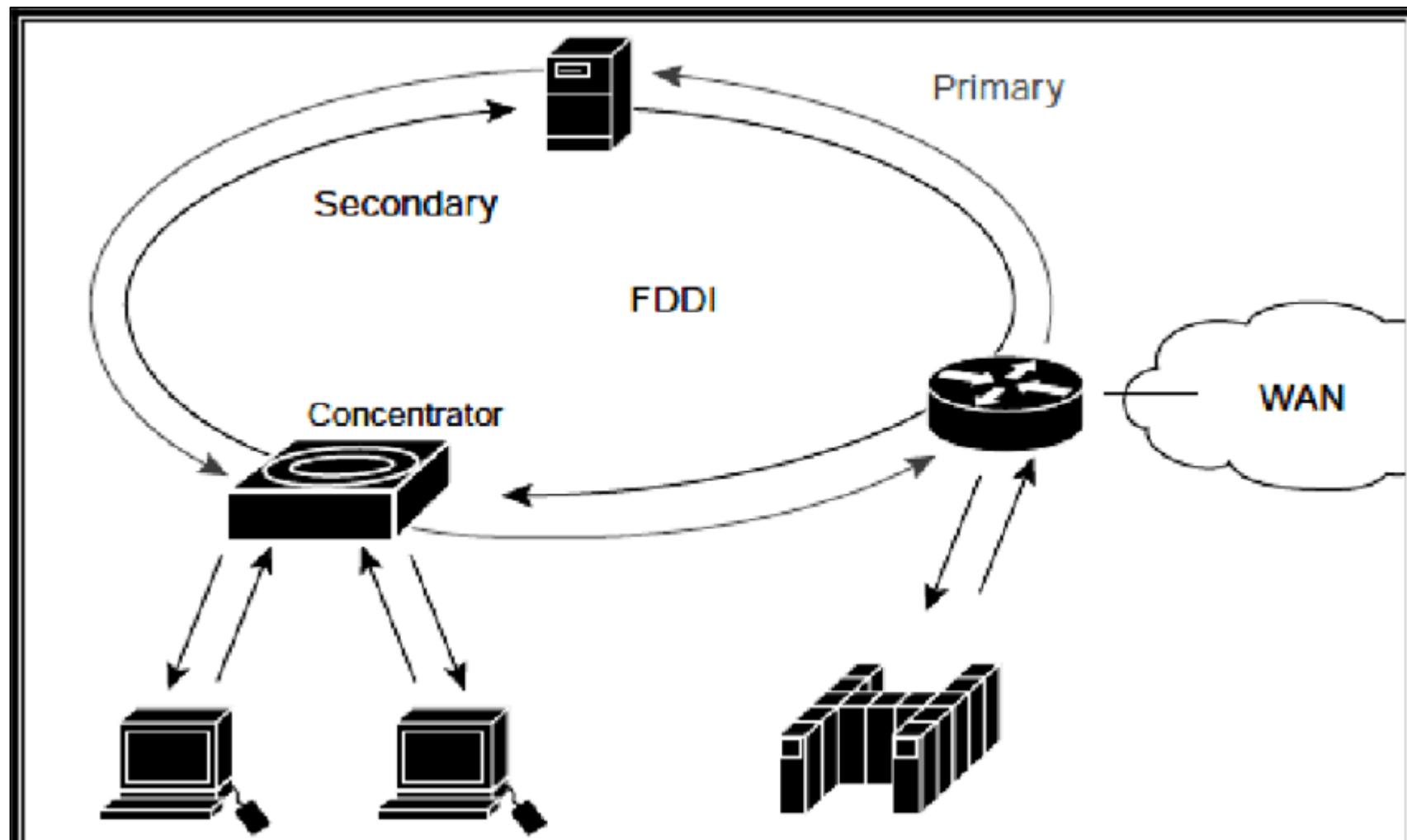
4.3 various IEEE 802.x LAN standards

S. N.	Features	802.3	802.4	802.5
1	Network Type	Ethernet	Token Bus	Token Ring
2	Physical Topology	Linear	Linear	Ring
3	Logical Topology	-	Ring	Ring
4	How do nodes communicate	Random Communication	Require Token	Require Token
5	Delay before transmission?	None	Depends on distance between stations	Depends on distance between stations
6	Cables used	TP, Coaxial, Fiber	Co-axial	TP and Fiber
7	Cable length support	50 - 2000m	200 - 500m	50 - 1000m
8	Adding new stations	Can add almost anywhere	Scheduling algorithm required	Scheduling algorithm required
9	Transmission affected during heavy load?	Highly affected	Provides fair access to all stations	Provides fair access to all stations

4.4 FDDI (Fiber Distributed Data Interface)

- Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables.
- A high performance Fiber Optic token ring network system
- FDDI arrangement consists of 2 fiber rings
 - One ring(Primary) transmits data and token from one node to other nodes within the network
 - Other ring(Secondary) works as a backup system if the primary ring fails.
 - If either one breaks, the other one can be used as backup
 - If both break at the same point, then the two rings can be joined to form a single ring
- Since the network system is based on token ring pattern, a station must first capture the token. Then it transmits a frame and remove it when it comes around again.
- FDDI specifies protocols for physical and data link layer.

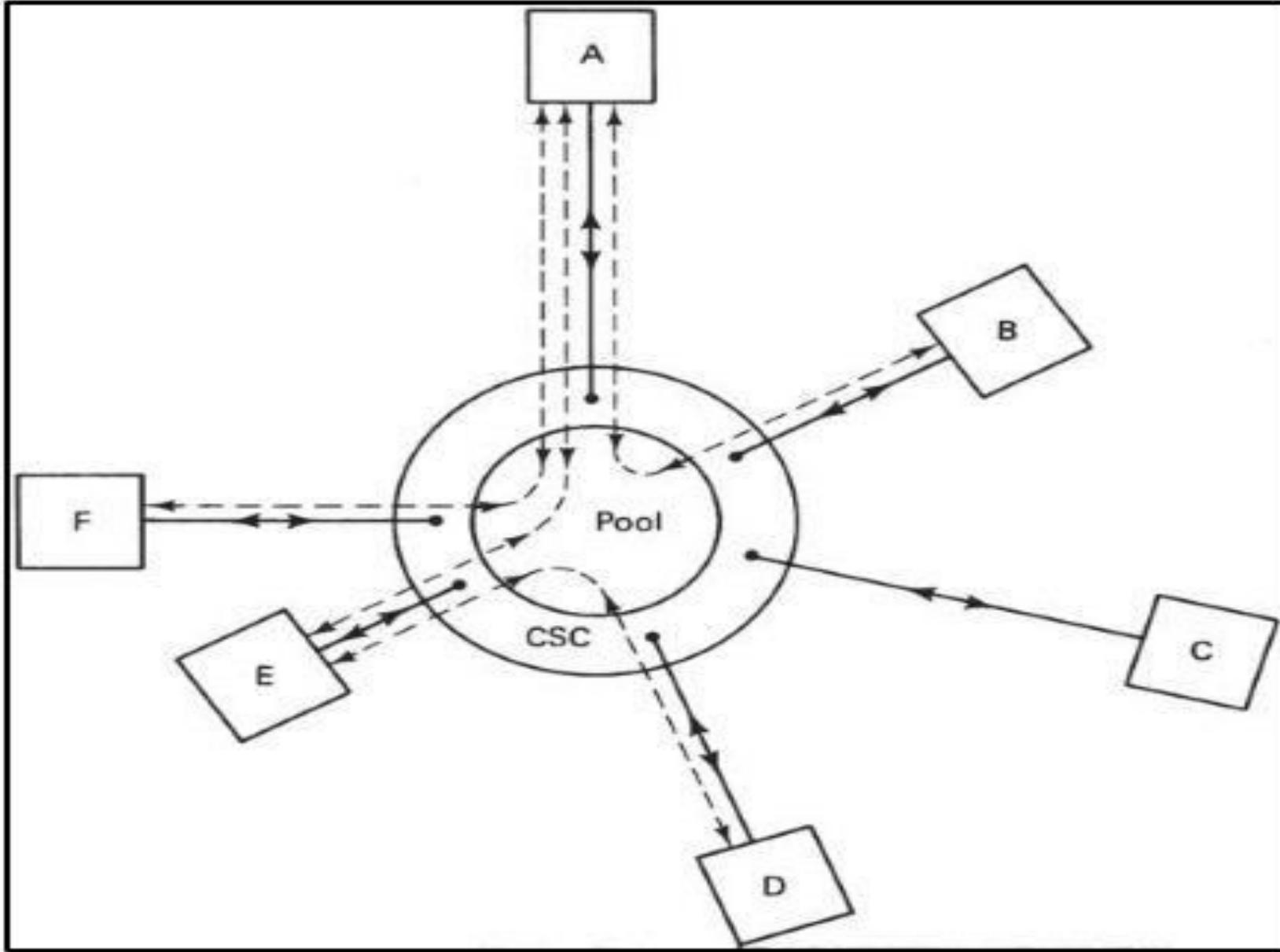
- FDDI defines data traffic as 2 classes: synchronous and asynchronous.
 - In synchronous communication, the traffic is delay sensitive. E.g. audio-video messages
 - In asynchronous, time or reception is not so important.
- When a node receives a token, it is allowed to send synchronous data without regard for whether the token is late or early.
 - In contrast, a node can send asynchronous data only when the token is early.
- Unlike 802.5 where a station may not generate a new token until its frame has gone all around and come back, FDDI can generate a new frame during the transmission of another frame.
- FDDI's applications include direct connection in workstation and servers within workgroups, and as a high speed backbone to connect other networks in a building or in a city.(i.e. it is used as the backbone for WAN)



4.5 Satellite Networks

SPADE

- It stands for Single channel per carrier Pulse Code modulated multiple Access Demand assignment Equipment.
- It was developed by Comsat for use on the INTELSAT satellite
- This system is extensively used with digital signals
- It is basically a pooling-waiting system where different Earth stations are eternally connected to a center pool which connects two respective stations on demand in an assignment-to-assignment basis.
- The distributed demand assignment facility requires use of a Common Signaling Channel (CSC).



Working Mechanism of SPADE

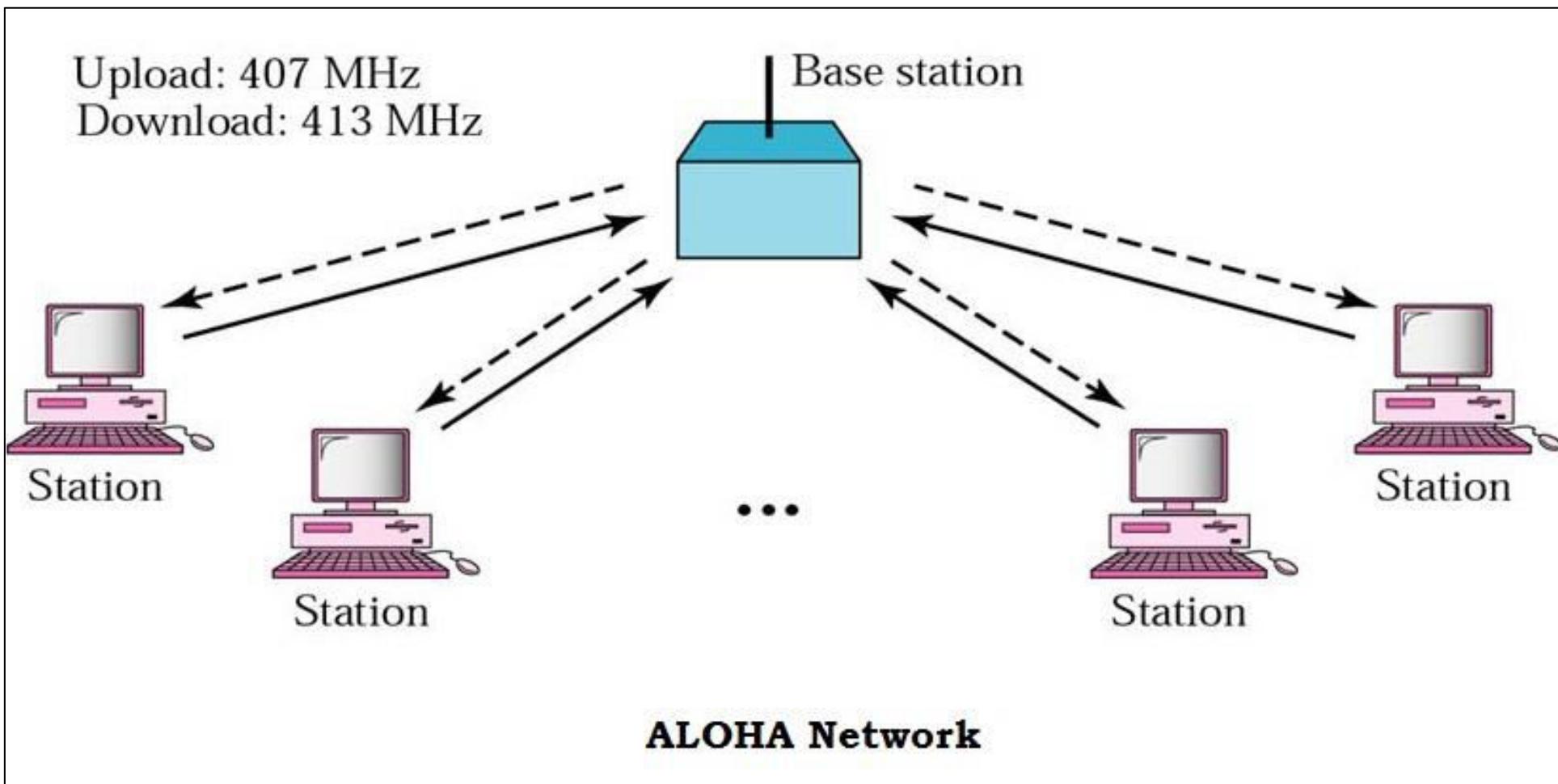
- All the Earth stations are permanently connected through the CSC.
- Each earth station has the facility for generating any one of the 794 carrier frequencies using frequency synthesizers.
 - Furthermore, each earth station has a memory containing a list of the frequencies currently available, and this list is continuously updated through the CSC.
- E.g. station C wants to call station F.
 1. C selects a frequency pair at random from those currently available on the list. C also signals F about this frequency information through CSC.
 2. Station F acknowledges that it can complete the circuit.
 3. Once the circuit is established, other Earth stations are instructed, through CSC, to remove this frequency pair from their list
 4. Since satellite communication has propagation delay, the frequency pair chosen by C might be busy due to use by other stations. If this case occurs, C receives busy information from CSC update list, and then will choose another pair immediately.
 5. Once a call has been completed and the circuit has been disconnected, the two frequencies are returned to the pool, the information again transmitted to all the Earth stations by CSC.

ALOHA

- ALOHA originally stood for Additive Links On-line Hawaii Area
- ALOHA, also called the ALOHA method, refers to a simple communications scheme in which each source (transmitter) in a network sends data whenever there is a frame to send.
 - If the frame successfully reaches the destination (receiver), the next frame is sent.
 - If the frame fails to be received at the destination, it is sent again.
- This protocol was originally developed at the University of Hawaii for use with satellite communication systems in the Pacific.
 - It provided the first public demonstration of a wireless packet data network
 - It was used for ground based radio broadcasting.
- When two or more stations try to send messages across the network simultaneously, contention is said to have occurred.
 - A contention-based protocol defines what happens when contention occurs.
 - **ALOHA is a contention-based protocol.**

ALOHA

- ALOHA allows many users to use the same radio channel without pre-coordination.
- It establishes rules by which a transmitter provides reasonable opportunities for other transmitters to operate.
- It also defines procedures for initiating new transmissions processes through determination of channel state (available or unavailable), and procedures for managing transmissions in the event of a busy channel.
- It was traditionally employed as Ethernet cable based network and then/now employed as satellite network.
- ALOHA was applied in SMS texting in 2G mobile phones and its versions were applied as GPRS in 2.5G & 3G mobile phones.
- Unlike the ARPANET where each node could only talk to 1 node directly, in ALOHA network, all client nodes can communicate with the hub on the same frequency.



ALOHA

- ALOHA network allowed each client to send its data without controlling when it was sent, with an acknowledgement/re-transmission scheme used to deal with collisions.
 - This approach reduced the complexity of the protocol and network hardware since nodes do not need to negotiate “who” is allowed to speak (unlike token bus or token ring systems)
- There are 2 types of ALOHA:
 - a) Pure ALOHA
 - b) Slotted ALOHA

Pure ALOHA

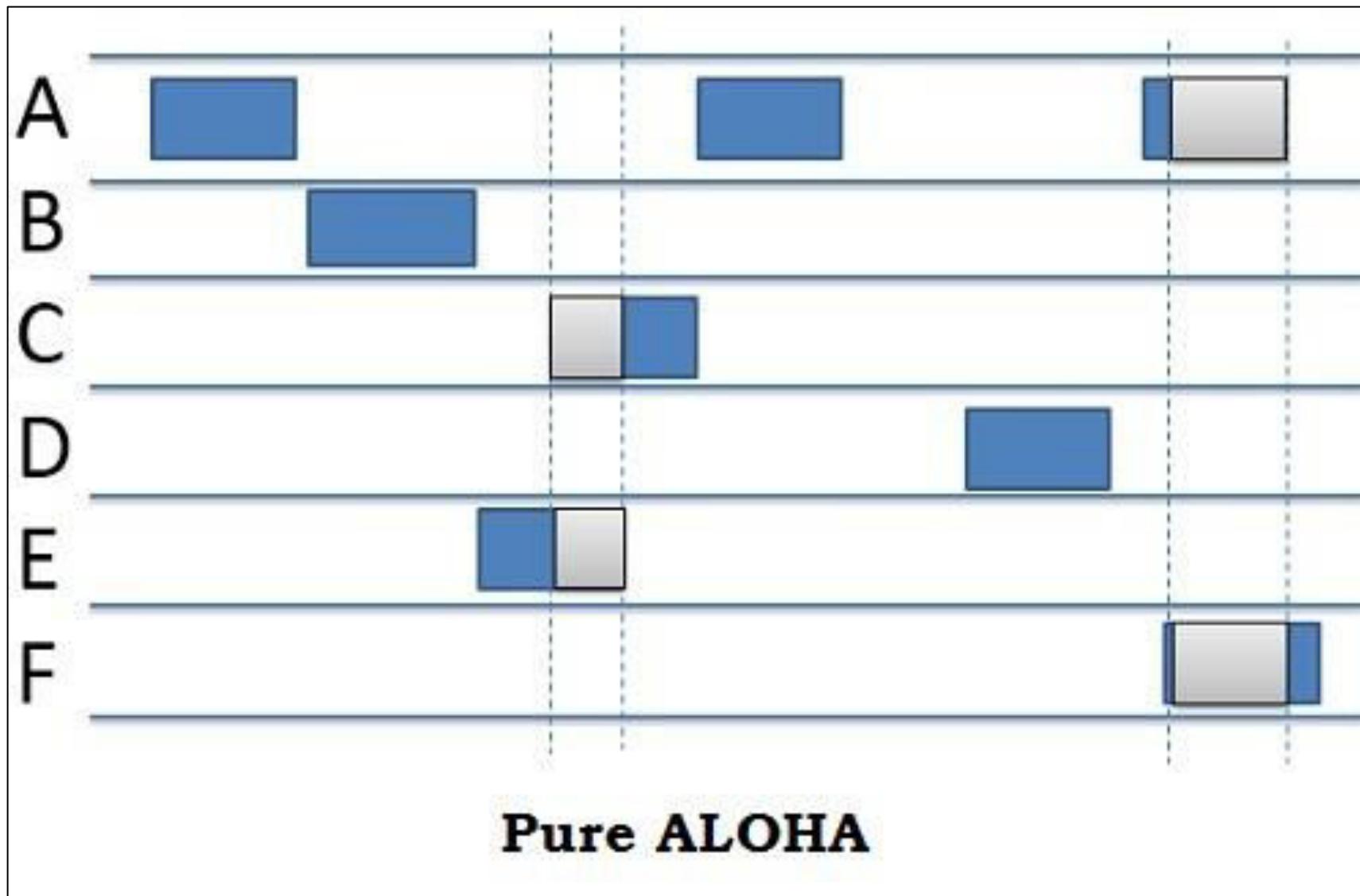
- If station 1 has data to send, it sends the data.
 - It doesn't pre-check whether the channel is busy before transmitting.
- If station 1 is transmitting data, and it receives any data from another station during that process, then a collision message is circulated.
- All the transmitting stations will then try to resend "later"
- Time gap for retransmission is specified.

Advantage

- Easy to understand

Disadvantage

- Transmission time is wasted
- Data can lost during "wait" time.
- Not useful for busy channels with real-time data requirements.



Slotted ALOHA

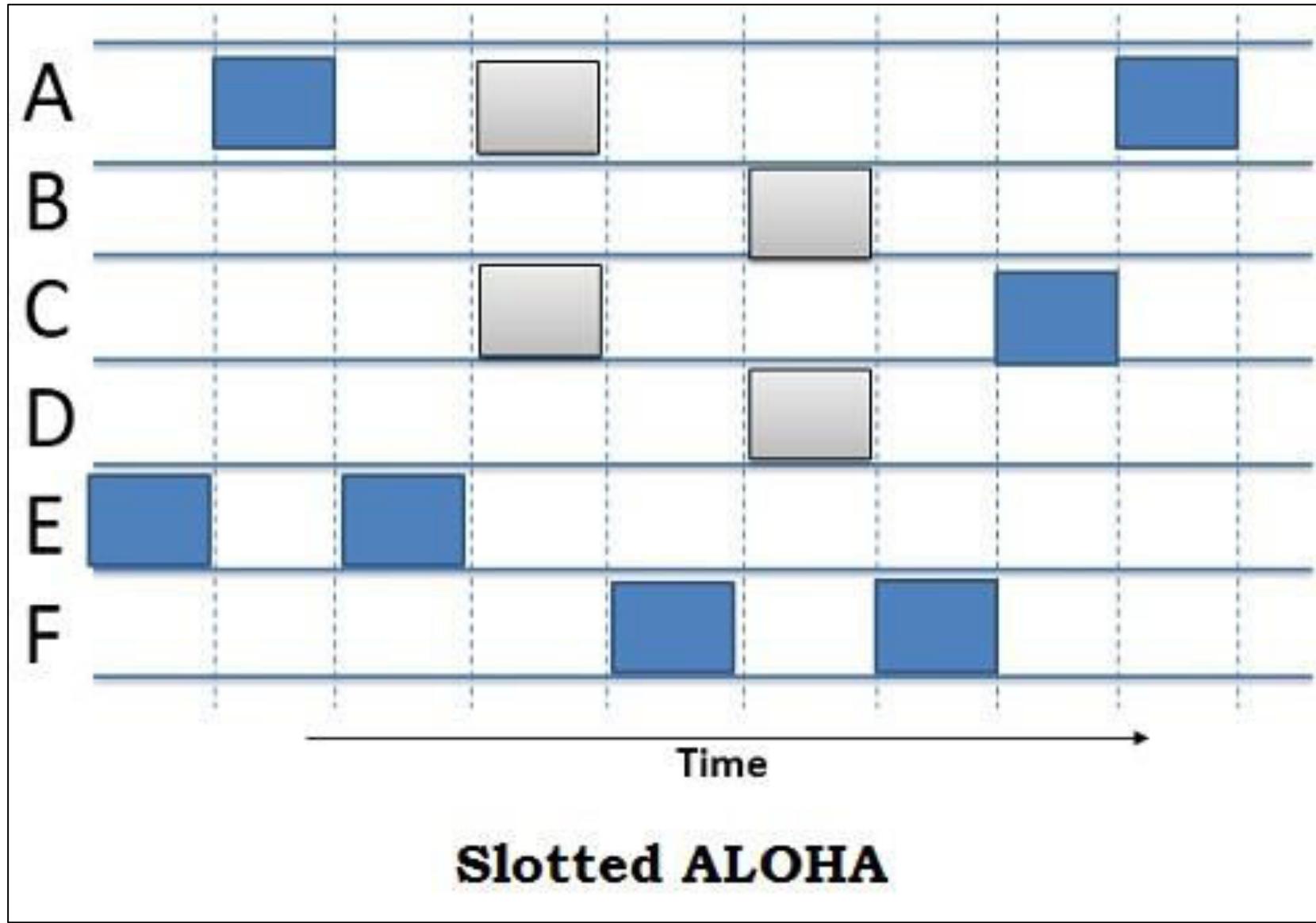
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- It uses discrete time system.
 - This increases max throughput.
- Station can start a transmission only at the beginning of a time slot, and thus collision are reduced. (almost 50% collision)
- Even if station is ready to send in middle of a slot, it must wait until the beginning of the next one.

Advantage

- More efficient than pure ALOHA

Disadvantage

- As the networks become complex, more communications occur. Hence chances of simultaneous transmissions are possible, resulting in contention
(This is why CSMA/CD is introduced)



End of chapter 4

Important Questions

1. What is CRC? Explain working scenario of CRC.
2. Explain how Checksum detects the error in transmission of frames.
3. How are hamming codes created? Explain how hamming codes can detect and correct transmission errors.
4. Sliding window protocols
5. Write short notes on
 - a) ALOHA
 - b) SPADE
 - c) FDDI

Computer Networks

Chapter 5
Internetworking
(9 hours \approx 16-18 marks)

Pros and cons of this chapter

A. Pros

- Easy to understand
- Easy to grab marks (“What are the...” questions are rarely asked)
- If u memorize points, you can get creative in description

B. Cons

- Points memorizing can be hectic
- Too much to manage
- Uncertainty to pin-point sure-shot questions (can't say which topic will be asked in exam with certainty)

Chapter Outlines

5.1 Routing Algorithms

- a) Adaptive Algorithms
- b) Non-Adaptive Algorithms (Shortest Path, Flooding, Distance Vector, Link State)

5.2 Congestion Control Algorithms

- a) Congestion Prevention Policies
- b) Congestion control in Datagram subnet (Warning bit, Packet choke, Hop-by-Hop choke, Load Shedding, Jitter control)
- c) Traffic shaping algorithms (Leaky bucket, Token bucket algorithm)

5.3 Bridges, Routers, Gateways

Routing Background

- Routing is the process of transferring packets received from the Data link layer of the source network to the Data link layer of the destination network.
- Routing involves making decisions at each intermediate node on where to send the packets next, so that they eventually reach the destination.
- The node that makes these routing choices is called the Router, and the mechanism by which routing is done is directed by certain procedure or algorithm, known as routing algorithm.

- A routing algorithm is responsible for deciding which output line must an incoming packet be transmitted on.
- If the network uses Datagrams, the decision are made for every arriving packet.
 - If the network uses Virtual Circuit, the decision are made only before VC is set up.
- Routing algorithms are selected keeping following desirable features:
 - Simplicity (simple routing reduces complexity and routing overhead)
 - Correctness (correct routing helps packet to reach destination)
 - Robustness (robust routing can handle h/w or s/w changes or even failures)
 - Stability (algorithm must be stable under all possible circumstances)
 - Fairness (every node in the network must have fair chance of transmission)
 - Optimality (best throughput and minimal packet delays must be balanced)

Routing Algorithm Types

1. Adaptive Algorithms

- Uses dynamic information as current topology, load, delay to select routes.
- They get routing information from adjacent routers or from all routers.
- The optimization parameters are distance, number of hops, estimated transit time, etc.
- Types:
 - Isolated (routers don't exchange information with each other)
 - Centralized (a centralized node has global info & makes all routing decision)
 - Distributed (combination of local and global information)

a) Isolated Adaptive Routing

- Here the node decides the routing without seeking information from other nodes.
 - Because the sending node doesn't have enough information about a particular link, the route may be congested.

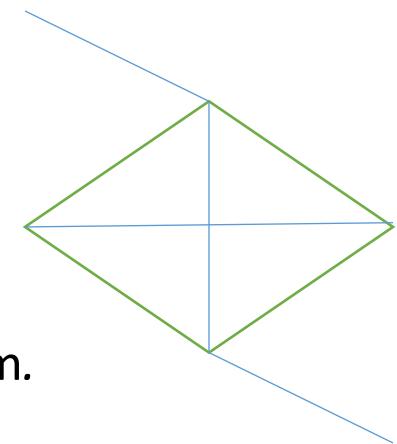
- Some algorithms that follow isolated routing mechanism:

1. Hot Potato Routing:

1. packet is continuously forwarded to adjacent nodes
2. Contrast to "*store & forward*" technique as it has no buffer mechanism.

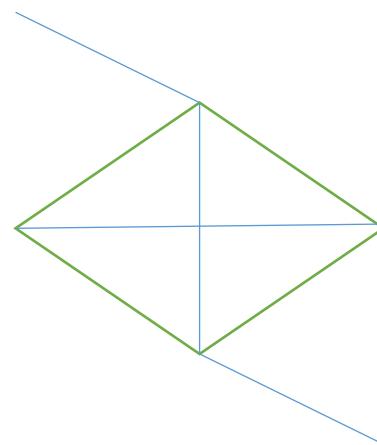
2. Backward Lean Routing:

1. Routing table at each node is updated by the information from incoming packets.



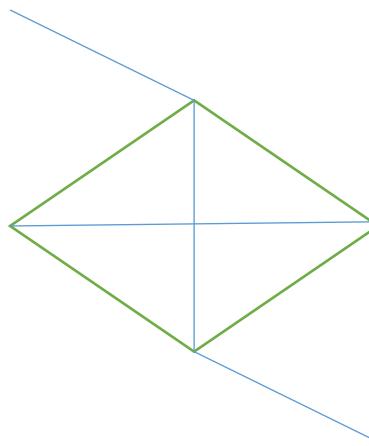
b) Centralized Adaptive Routing

- Here a central node gets entire information of the network topology.
- Based on traffic, no. of nodes, & the topology, it then decides the routing.
- The routing information is then transmitted to the respective routers.



c) Distributed Adaptive Routing

- Here the node receives information from its neighboring nodes and then decides about which way to send the packet.
- Packets can be delayed if there is some changes occurring between node receiving information and node sending the packet.

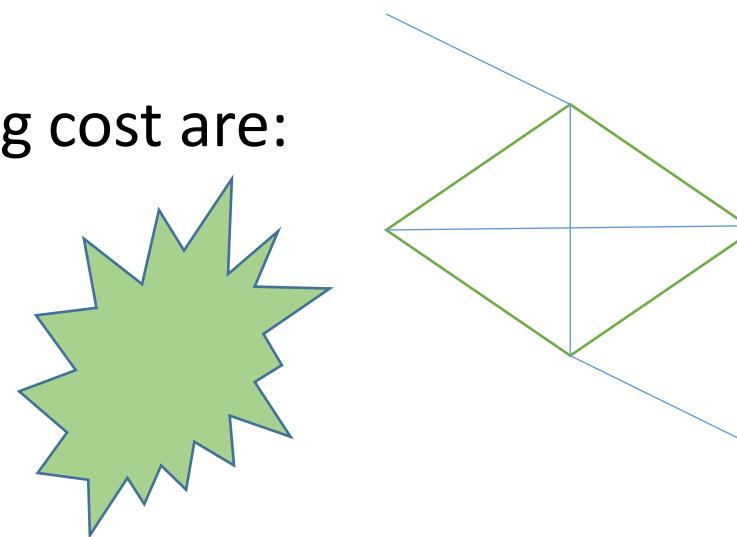


2. Non-Adaptive Routing Algorithms

- Also called static routing, since the route from one node to another is computed in advance.
- The advance computation is then downloaded by routers when the network is established.
- These algorithms do not base their routing decisions based on measurements or estimates of current traffic or topology.
- Classifications:
 1. Shortest Path Routing
 2. Flooding
 3. Distance Vector Routing
 4. Link Static Routing

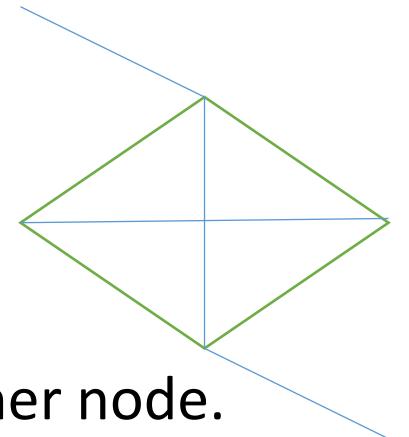
1. Shortest Path Routing

- Here the path taken from the sending computer to the recipient computer is minimized.
 - The path can be measured in terms of physical distance, or in terms of number of hops.
- A network is represented as a graph, where the terminals are nodes and the links are edges.
 - A length which represents cost of using that link is associated with each edge.
 - Lower the cost, more suitable is the link.
- Some important attributes for determining cost are:
 - ✓ Min. number of hops
 - ✓ Transmission and propagation delays
 - ✓ Queuing delays



2. Flooding

- Every incoming packet is sent on every outgoing lines except on the one on which it arrived.
- Because all outgoing lines for a node are used, the packets may go in a loop. (for E.g. 1→2→3→5→1)
- To overcome repetition, some techniques are adapted :
 - ✓ Implementing Sequence numbers in packets
 - ✓ Establish a hop counter and update it whenever it jumps to another node.
 - ✓ Maintain a spanning tree routed at the source to the destination.



3. Distance Vector Routing

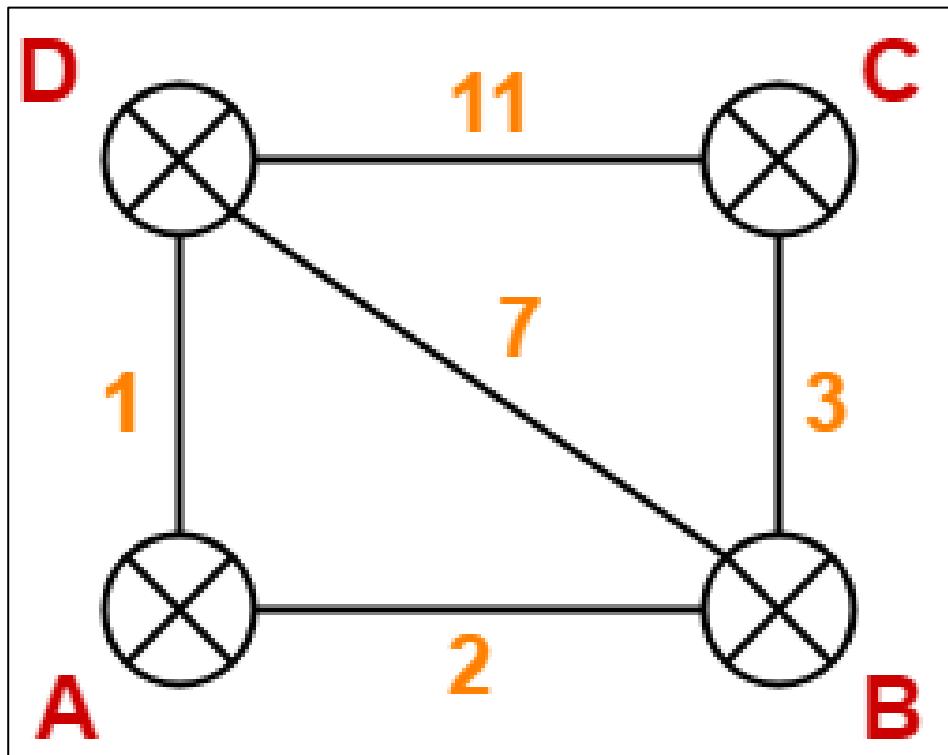
- The **distance vector** is a component that is determined by each router as the distance between itself and each possible destination.
- This routing was originally used as ARPANET routing algorithm.
 - It is also used in the Internet under the name RIP (Routing Info Protocol).
- Key features of distance vector routing:
 - ✓ The routers share the knowledge of entire autonomous system.
 - ✓ Information is shared only with the neighbors
 - ✓ Sharing of information occurs at fixed regular intervals

Mechanism...

- The distance vector is computed as the distance between a router and all of its intermediate router neighbors, and adding each neighboring router's computations for the distances between that neighbor and all of its intermediate neighbors.
- Each router gets information of its neighbors.
 - So each router maintain / update the routing table and sends the updated table to its own neighbors.

Example

- Compute Vector distance for each components shown below:



Stage 1:

Each router prepares its routing table using its local knowledge.

<u>At Router A-</u>		
Destination	Distance	Next Hop
A	0	A
B	2	B
C	∞	-
D	1	D

<u>At Router B-</u>		
Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	7	D

<u>At Router C-</u>		
Destination	Distance	Next Hop
A	∞	-
B	3	B
C	0	C
D	11	D

<u>At Router D-</u>		
Destination	Distance	Next Hop
A	1	A
B	7	B
C	11	C
D	0	D

Stage 2:

- Each router exchanges its distance vector obtained in Step-01 with its neighbors.
- After exchanging the distance vectors, each router prepares a new routing table based on shortest distance required to reach each node.

1. Cost of reaching B from A

$$= \min \{ 2+0, 1+7 \} = 2 \text{ via B.}$$

2. Cost of reaching C from A

$$= \min \{ 2+3, 1+11 \} = 5 \text{ via B.}$$

3. Cost of reaching D from A

$$= \min \{ 2+7, 1+0 \} = 1 \text{ via D.}$$

At Router A-

From B

2
0
3
7

From D

1
7
11
0

Cost(A→B) = 2

Cost(A→D) = 1

Destination	Distance	Next hop
A	0	A
B		
C		
D		

New Routing Table at Router A

Thus, the new routing table at router A is-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	5	B
D	1	D

From A

0
2
∞
1

From C

∞
3
0
11

From D

1
7
11
0

Destination	Distance	Next hop
A		
B	0	B
C		
D		

$$\text{Cost (B} \rightarrow \text{A)} = 2$$

$$\text{Cost (B} \rightarrow \text{C)} = 3$$

$$\text{Cost (B} \rightarrow \text{D)} = 7$$

New Routing Table at Router B

- Cost of reaching destination A from router B = $\min \{ 2+0, 3+\infty, 7+1 \} = 2$ via A.
- Cost of reaching destination C from router B = $\min \{ 2+\infty, 3+0, 7+11 \} = 3$ via C.
- Cost of reaching destination D from router B = $\min \{ 2+1, 3+11, 7+0 \} = 3$ via A.

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	3	A

For B

From B

2
0
3
7

From D

1
7
11
0

Cost (C→B) = 3

Cost (C→D) = 11

Destination	Distance	Next hop
A		
B		
C	0	C
D		

New Routing Table at Router C

- Cost of reaching destination A from router C = $\min \{ 3+2, 11+1 \} = 5$ via B.
- Cost of reaching destination B from router C = $\min \{ 3+0, 11+7 \} = 3$ via B.
- Cost of reaching destination D from router C = $\min \{ 3+7, 11+0 \} = 10$ via B.

Destination	Distance	Next Hop
A	5	B
B	3	B
C	0	C
D	10	B

For C

From A

0
2
∞
1

From B

2
0
3
7

From C

∞
3
0
11

$$\text{Cost } (D \rightarrow A) = 1$$

$$\text{Cost } (D \rightarrow B) = 7$$

$$\text{Cost } (D \rightarrow C) = 11$$

Destination	Distance	Next hop
A		
B		
C		
D	0	D

New Routing Table at Router D

- Cost of reaching destination A from router D = $\min \{ 1+0 , 7+2 , 11+\infty \} = 1$ via A.
- Cost of reaching destination B from router D = $\min \{ 1+2 , 7+0 , 11+3 \} = 3$ via A.
- Cost of reaching destination C from router D = $\min \{ 1+\infty , 7+3 , 11+0 \} = 10$ via B.

Destination	Distance	Next Hop
A	1	A
B	3	A
C	10	B
D	0	D

For D

Stage 3:

- Each router exchanges its distance vector obtained in Step-02 with its neighboring routers.
 - After exchanging the distance vectors, each router prepares a new routing table.
- ❖ This stages repeat till all the routing table is filled with shortest routes between the nodes.
- ❖ Generally the stages iterate for $(n-1)$ times where n is the number of nodes in the graph.

4. Link State Routing

- Here, unlike vector routing, each router shares its knowledge of its neighborhood with every other router in the internetwork.
- Key features of link state routing:
 - ✓ A router sends entire routing table of the network.
 - ✓ Each router sends this info to all other router through Flooding technique.
 - ✓ Follows lowest cost mechanism.
 - ✓ In vector routing, cost is the hop count.
 - ✓ In link state, cost is based on security, traffic, state of link etc.

- Cost is applied as a packet leaves the router.
- When a router floods the network with the information about its neighborhood, it is said to be advertising.
 - The basis of this advertising is a short packet called a Link State Packet (LSP).
- A link state packet contains 4 fields: Advertiser ID, destination N/W ID, the cost, Neighbor ID.

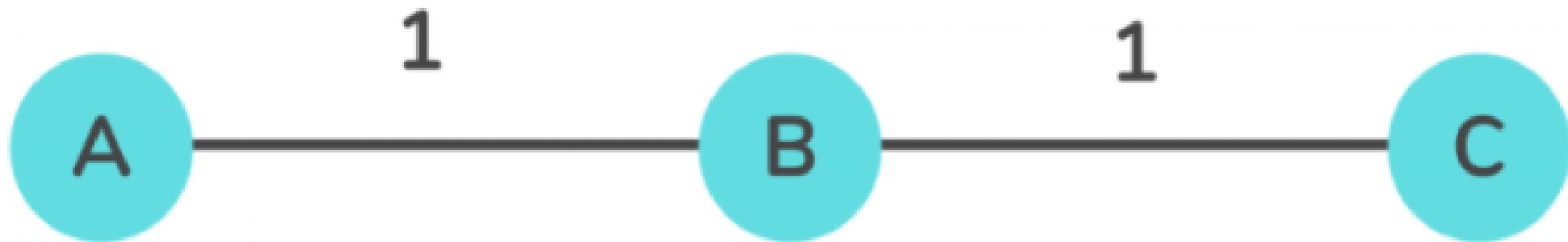
Advertiser (Host ID)	Destination ID	Cost	Neighbor

- Related example:
 - <https://www.javatpoint.com/link-state-routing-algorithm>

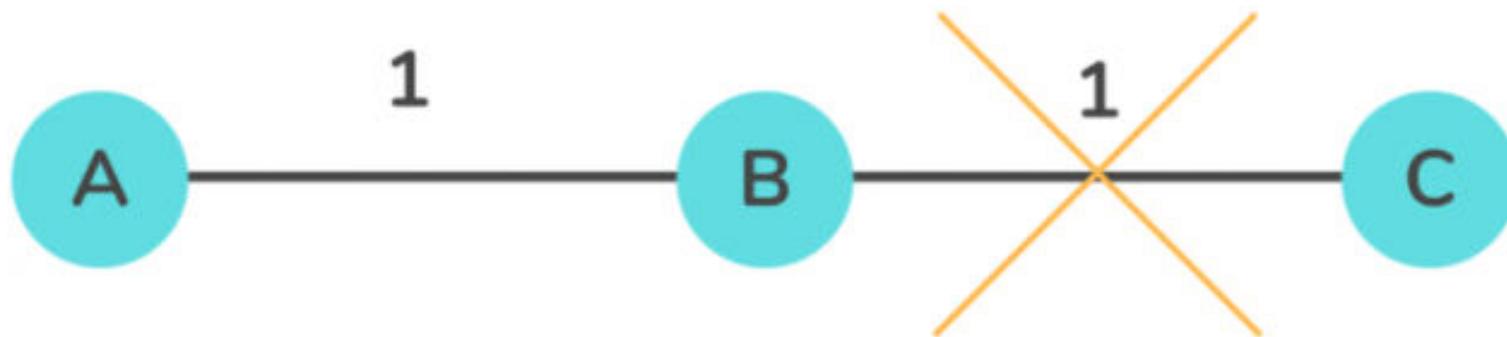
BASIS FOR COMPARISON	DISTANCE VECTOR ROUTING	LINK STATE ROUTING
Algorithm	Bellman ford	Dijkstra
Network view	Topology information from the neighbour point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops	Based on the cost
Updates	Full routing table	Link state updates
Updates frequency	Periodic updates	Triggered updates
CPU and memory	Low utilisation	Intensive
Simplicity	High simplicity	Requires a trained network administrator
Convergence time	Moderate	Fast
Updates	On broadcast	On multicast
Hierarchical structure	No	Yes
Intermediate Nodes	No	Yes

What is count to infinity problem?

- The Count to Infinity problem arises from the routing loop in this Distance Vector Routing(DVR) network.
 - Such Routing Loops usually occurs when 2 routers send an update together at the same time or when an interface goes down.
- If a node tells 2nd node that there is a path connecting to the third node via 1st node, then the 2nd node might not know if it is a part of that path already.



Consider the above diagram, for this setup, the Bellman-Ford algorithm will work such that for each router, they will have entries for each other. Router A will infer that it can reach B at a cost of 2 units, and B will infer that it can reach C at a cost of 1 unit.



Consider the case in the above diagram, where the connection between B and C gets disconnected. In this case, B will know that it cannot get to C at a cost of 1 anymore and update its table accordingly. However, it can be possible that A sends some information to B that it is possible to reach C from A at a cost of 2. Then, since B can reach A at a cost of 1, B will erroneously update its table that it can reach C via A at a cost of $1 + 2 = 3$ units. A will then receive updates from B and update its costs to 4, and so on. Thus, the process enters into a loop of bad feedback and the cost shoots towards infinity. This entire situation is called the Count to Infinity problem.

5.2 Congestion Control Policies

Background

- When too many packets are present in the subnet, performance degrades. It may also result in loss of packets.
 - This situation is called **congestion**.
- Congestion can occur if the load on network (the no. of packets sent to a network) is greater than the capacity of network (no. of packets the network can handle at a given time)
- Congestion control mechanisms and techniques are implemented to control the congestion and keep the network load below the capacity.

- Congestion control can be addressed in both network level and the transport level.
- Congestion control consist of following possible approaches:
 1. Packet dropping
 - If the buffer becomes full, router can drop the waiting packets.
 2. Packet scheduling
 - Schedule traffic so as to isolate users that are transmitting at higher rate
 3. Traffic control policy
 - Allow connection-oriented network transmission only if network can handle them.
 4. Rate Control
 - Control the source rate explicitly based on feedback from either network or receiver.

5.2 a Congestion prevention policies

- Attempt to solve congestion problem by ensuring it doesn't occur in the first place.
 - Once the system is up and running, midcourse connections are not made.
- Also called open loop congestion control policies.
- Tools for open loop control include **deciding when to accept new traffic, when to discard packets, and making scheduling decisions.**

- Various open loop congestion controls are:
 - a) Retransmission policy
 - Better retransmit than to create congestion in the network.
 - b) Window policy
 - a) Better use selective window rather than Go back N.
 - c) Acknowledgement policy
 - a) If receiver need not acknowledge every packet it receives, it may prevent congestion.
 - d) Discarding policy
 - a) A router should discard packets that may result in congestion.

Layer	Policies
Transport	Retransmission Policy
	Out-of-order Caching Policy
	Acknowledgement Policy
	Time-out determination Policy
Network	VC vs datagram inside subnet
	Packet queuing and service policy
	Packet Discard Policy
Data Link	Routing Algorithm
	Packet Lifetime Management

5.2 b Congestion control in Datagram network

1. Warning bit

- When the router detects congestion occurring, it warns the source host by sending a warning bit as signal.
- When the source receives warning bit, it has to reduce its traffic being sent for some time.

2. Packet choke

- Whenever a utilization line for a router goes above threshold, the output line enters a “warning” state.
- The router sends a choke packet to the source host, giving it a signal with a special header.
- When the host gets the choke packet, it must reduce the traffic being sent to a specified value by certain percent.
- Causes the source host to have unnecessary load.
- Host may or may not reduce the traffic outflow towards the router.

3. Hop-by-Hop choke

- Choke packet is not very effective for high speed networks or long distance networks, because the host reaction might be slow.
- An alternative approach is to have the choke packet take effect at every hop it passes through.

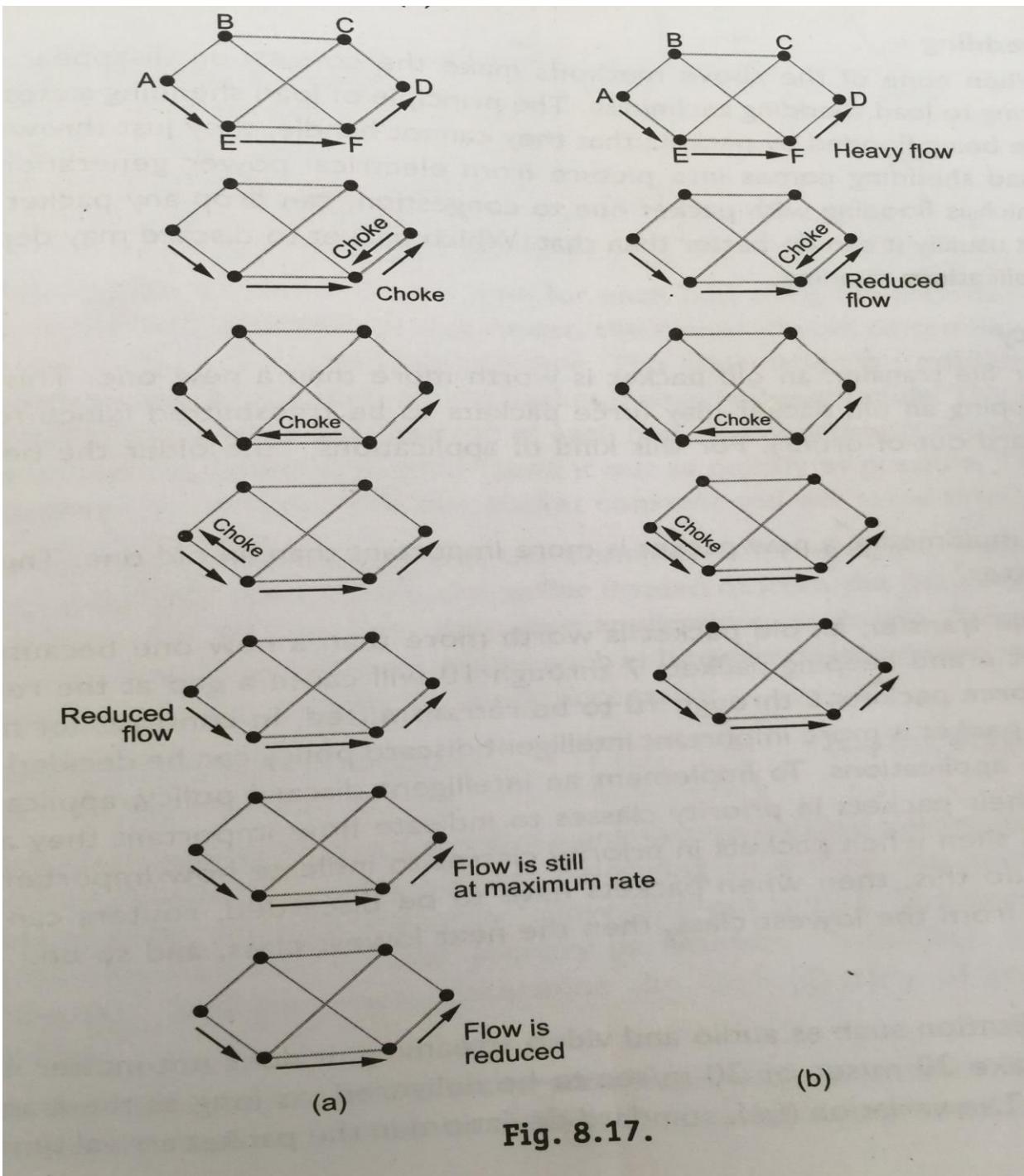


Fig. 8.17.

4. Load Shedding

- Analogue to electrical power generation.
- When the routers are flooded by packets that they cannot handle, they just throw them away.
- The router which is being flooded can drop any packet at random.
 - However, for effectiveness, router discards packets depending on the applications running.

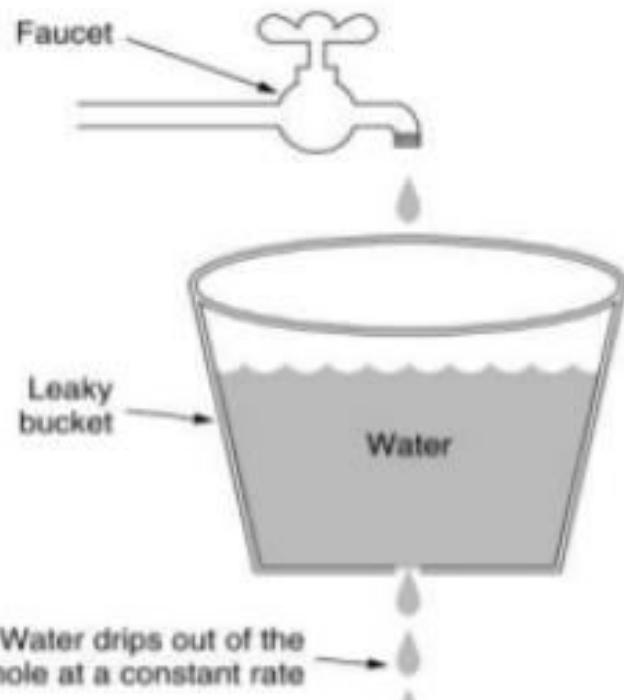
5. Jitter control

- For Audio/Video files, the transit time matters more than the packet transmission time.
- The variation in packet arrival time is called jitter.
- When a packet arrives at router, the router checks how much the packet is behind or ahead of its schedule.
 - This information is stored in the packet and is updated at each hop.
- In some applications, such as VoD, buffering at the receiver and then fetching data for display from the buffer instead of from the network in real time can eliminate jitter.
 - However, applications requiring real-time interaction such as video conferencing or Internet Telephony, buffer management is ineffective.

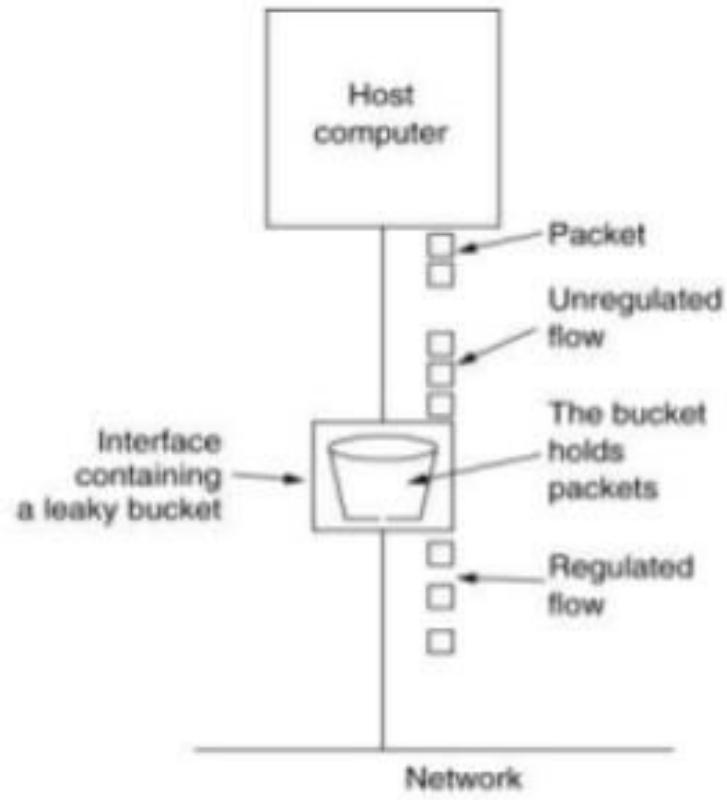
5.2 c Traffic shaping algorithms

- Traffic shaping is the mechanism to control the amount and rate of the traffic sent to the network.
- It smoothens the traffic on server side by implementing open loop control.
- It manages congestion by forcing the packet transmission rate to be more predictable.
- There are 2 traffic shaping algorithms:
 1. Leaky Bucket
 2. Token Bucket

The Leaky Bucket Algorithm



(a)



(b)

(a) A leaky bucket with water.

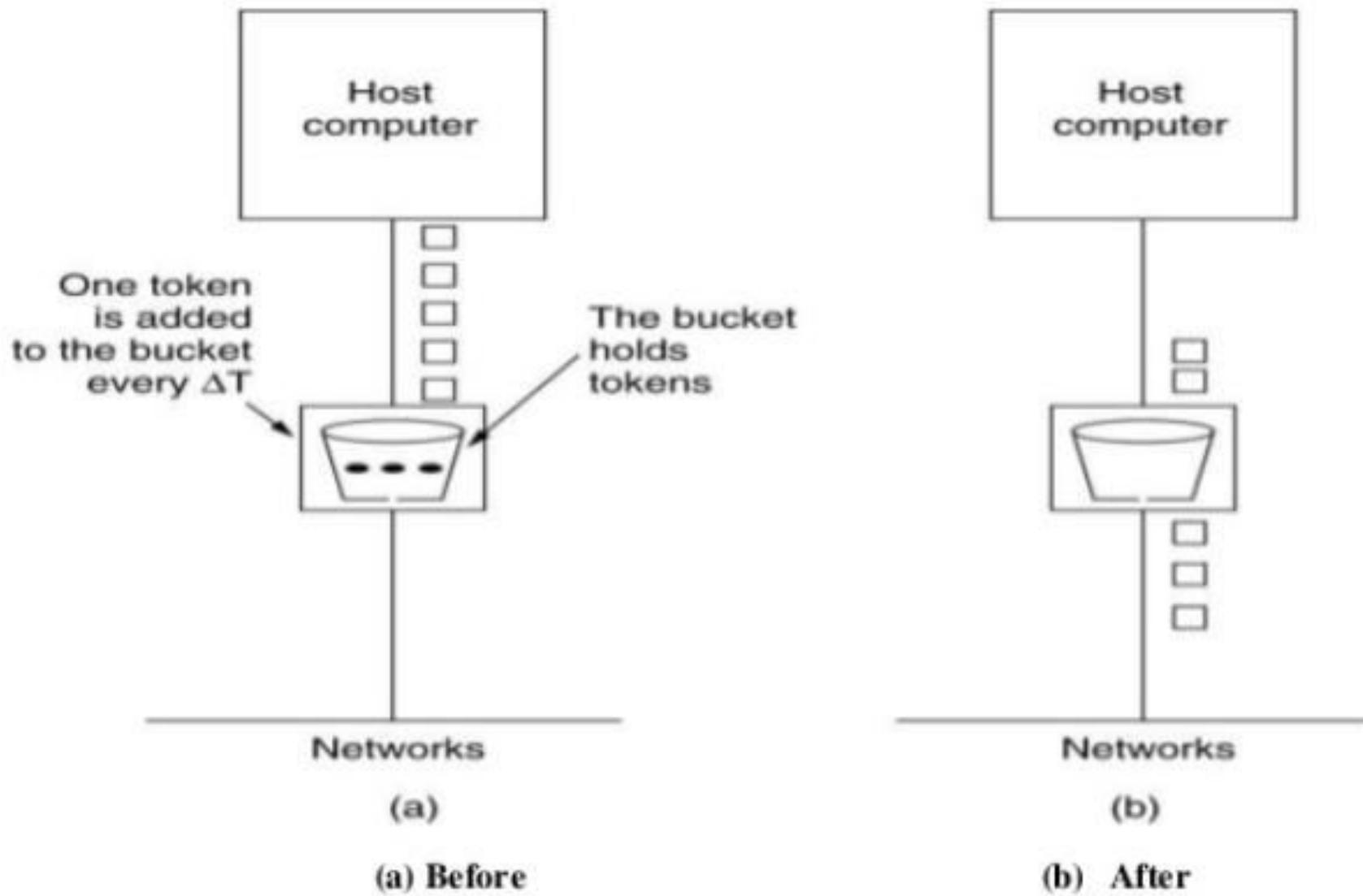
(b) a leaky bucket with packets.

1. Leaky Bucket Algorithm

- Consider a bucket with a small hole at the bottom.
- Whatever may be the rate of water pouring into the bucket, the rate at which the water comes out from that small hole is constant.
- Once the bucket is full, any additional water entering it spills over the sides and is lost (i.e. it doesn't appear in the output stream flowing through the hole underneath).
- The nature of inflow can be bursty or a continuous stream.
- Same idea is applied to the packet via router.

- When the host has to send a packet, the packet is thrown into a bucket.
 - The bucket leaks at a constant rate, i.e. the network interface transmits packets at a constant rate
 - Bursty traffic is converted into a uniform traffic by the leaky bucket.
-
- Router implements this algorithm in form of a finite queue that outputs in a finite rate.
 - When a packet arrives, it is queued up.
 - If the queue is full, the packet is discarded.

Token Bucket Algorithm



2. Token Bucket Algorithm

- Here the bucket holds token, generated at regular intervals.
- The bucket can hold at most b tokens. If a token arrives when the bucket is fully, it is discarded.
- When a packet of n bytes arrives, n tokens are removed from the bucket, and the packet is sent to the network.
- If fewer than n token are available, no tokens are removed from the bucket and the packet is considered to be non-conformant.
 - Non-conformant packets can either be dropped, or kept on hold till sufficient tokens have been generated.

Token Bucket Vs Leaky Bucket

TABLE 4

Token Bucket	Leaky Bucket
<ul style="list-style-type: none">– The algorithm for traffic shaping quite different.	<ul style="list-style-type: none">– In this there is trade off between memory and bandwidth and packet life time.
<ul style="list-style-type: none">– It allows saving up to maximum size of 'n' i.e. burst can be sent of size 'n' at once	<ul style="list-style-type: none">– It has constant traffic depending on the leakage.
<ul style="list-style-type: none">– Token bucket discarded token when bucket fills up.	<ul style="list-style-type: none">– This discards the packets when bucket fills up.
<ul style="list-style-type: none">– The implementation consists of just counting token. The counter is incremented by one for every DT and decremented by one whenever a packet is sent. When packet hit zero no packet may be sent	<ul style="list-style-type: none">– The implementation of this is because routers, buffer, bandwidth discard packets whenever more links want service to only one output link. When the bucket is empty, no packet is sent.

Difference between Leaky and Token buckets –

LEAKY BUCKET	TOKEN BUCKET
When the host has to send a packet , packet is thrown in bucket.	In this leaky bucket holds tokens generated at regular intervals of time.
Bucket leaks at constant rate	Bucket has maximum capacity.
Bursty traffic is converted into uniform traffic by leaky bucket.	If there is a ready packet , a token is removed from Bucket and packet is send.
In practice bucket is a finite queue outputs at finite rate	If there is a no token in bucket, packet can not be send.

Some advantage of token Bucket over leaky bucket –

- If bucket is full in token Bucket , token are discard not packets. While in leaky bucket, packets are discarded.
- Token Bucket can send Large bursts can faster rate while leaky bucket always sends packets at constant rate.

DIFFERENCE BETWEEN LEAKY BUCKET AND TOKEN BUCKET ALGORITHM

TOKEN BUCKET	LEAKY BUCKET
Token dependent.	Token independent.
If bucket is full token are discarded, but not the packet.	If bucket is full packet or data is discarded.
Packets can only transmitted when there are enough token	Packets are transmitted continuously.
It allows large bursts to be sent faster rate after that constant rate	It sends the packet at constant rate
It saves token to send large bursts.	It does not save token.

5.3 Bridges, Routers, & Gateways

Background for device operations on OSI layers

1. Below physical layer - passive hub
2. Physical layer – Repeater , Active Hub
3. Physical and Data Link Layer – Bridge, 2-layer switch
4. Physical, data link, network layer – Router, 3-Layer switch
5. All 5 layers - Gateway

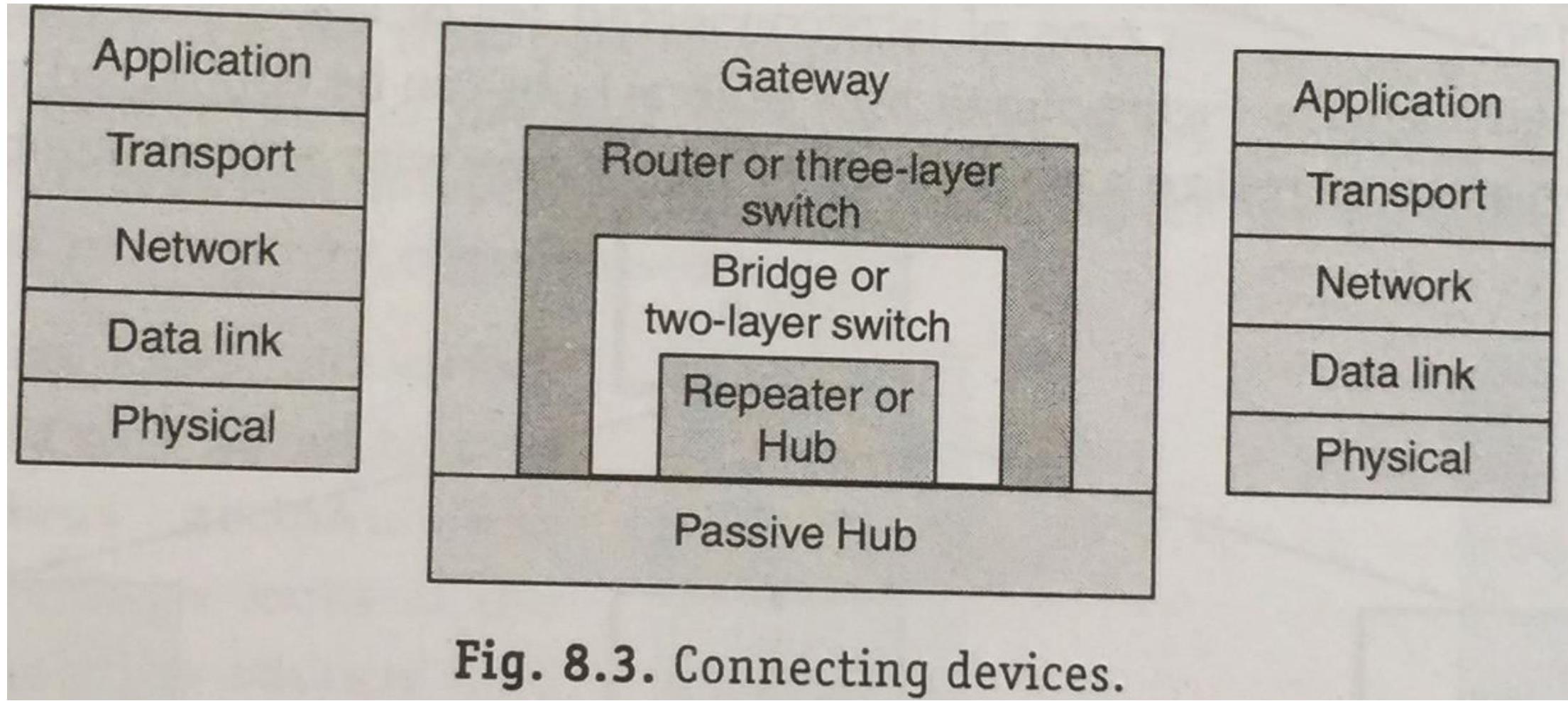


Fig. 8.3. Connecting devices.

Bridges

- Device that pass packets from one network to another.
- Operate at data link layer
- Serves both as a medium and a filter.
- Allows packets from a node on one network to be sent to a node on another network.
- Bridges looks into various fields of a frame to take various actions (forwarding, error check)
- Offers a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage.

- A bridge must contain addressing and routing capability.
- Two routing algorithms has been proposed for a bridged LAN environment.
 - ❖ 802.1 Transparent Bridge
 - ❖ 802.5 Token ring

Routers

- Router can be used to link two dissimilar LANs
- A router isolates LANS into subnets to manage and control network traffic.
 - However, unlike bridges it is not transparent to end stations.
- It determines a path to a destination for a packet, and then starts the packet on its way.
- To determine a path, router communicates with other routers in the larger network.
- Routers operate at the network layer.

- A router has 4 basic components:
 1. Input port
 - Performs physical to data-link layer functions by holding packets before forwarding
 2. Output port
 - Forwards packets to the switching fabric
 3. Routing processor
 - Routing table maintenance
 4. Switching fabric
 - Moves input queue to the output queue through some mechanisms

Gateways

- Gateway moves packets between two different computer environment, such as a LAN and a mainframe environment.
- Gateways operate at session layer and above.
- Gateways connect dissimilar network, perform compression or expansion, encryption or decryption, and so on.
- The application level gateways can look into the content application layer packets such as email before forwarding it to the other side.
- It is best used in firewalls.

Related Questions:

1. Explain Leaky Bucket algorithm and compare it with token bucket algorithm.
2. Briefly describe Hub, Switch, and Router.
3. What are the routing algorithms? Briefly explain about distance vector and link state routings with suitable example.
4. Discuss jitter control.
5. Discuss importance of gateways and bridges.
6. What are the main differences between distance vector routing and link state routing? Explain with an example how distance vector is used to route packet. What is count-to-infinity problem?
7. How does congestion happen over the network? Explain with suitable diagram the concept of token bucket algorithm.

8. What is non-adaptive algorithm? Explain various types of adaptive routing algorithms.
9. Write short notes on Bridge.
10. Explain link state routing algorithm.

Computer Networks

Chapter 6
Overview of TCP/IP
(10 hours ≈ 15-20 marks)

Chapter Outlines

- | | |
|---|---|
| <ul style="list-style-type: none">1. TCP/IP and the Internet<ul style="list-style-type: none">• TCP/IP features• Protocol Standards2. A data communication model3. TCP/IP protocol Architecture4. Network Access Layer5. Internet Layer<ul style="list-style-type: none">• Internet Protocol• Datagram• Routing• Fragmenting• Passing datagrams to transport layer | <ul style="list-style-type: none">6. ICMP<ul style="list-style-type: none">• Flow control• Detecting unreachable destinations• Redirecting routes• Checking remote hosts7. Transport Layer<ul style="list-style-type: none">• UDP• TCP8. Application Layer<ul style="list-style-type: none">• HTTP, FTP, SMTP, POP3, IMAP |
|---|---|

6.1 TCP/IP and the Internet

6.1.1 TCP/IP features

- TCP/IP (Transmission Control Protocol/Internet Protocol), is a suite of communication protocols used to interconnect network devices on the private network or the internet.
- it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.
- It specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination.

- The two main protocols in the TCP/IP suite serve specific functions:
 - a) **TCP**
 - defines how applications can create channels of communication across a network.
 - manages how a message is assembled into smaller packets, transmitted over the internet, and reassembled in the right order at the destination address.
 - b) **IP**
 - defines how to address and route each packet to make sure it reaches the right destination.
 - Each gateway computer on the network checks this IP address to determine where to forward the message.
- TCP/IP uses the client/server model of communication in which a user or machine (a client) is provided a service (like sending a webpage) by another computer (a server) in the network.

TCP/IP features

1. Open Protocol standards.
2. A common addressing scheme that allows any TCP/IP device to uniquely address any other device in the entire network, even if the network is as large as the worldwide Internet.
3. Hardware Independence
 - Protocols can be used on Mac, PC, mainframe or any other computer
4. Software Independence
 - All kinds of applications and OS support TCP/IP
5. High level of failure recovery
 - TCP/IP helps to renew network performance
6. The ability to handle a big range of transfer errors
 - Protocols can determine data transmission errors and perform recovery.

6.1.2 Protocol Standards

- When computers communicate, it is necessary to define a set of rules to govern their communications.
 - In data communications, these sets of rules are also called protocols.
- TCP/IP creates a heterogeneous network with open protocols that are independent of operating system and architectural differences.
- TCP/IP protocols are available to everyone and are developed and changed by consensus, not by the fiat of one manufacturer.
 - Everyone is free to develop products to meet these open protocol specifications.

- Internet standards are developed by the Internet Engineering Task Force (IETF) in open, public meetings.
 - The protocols developed in this process are published as Requests for Comments (RFCs)
- RFCs contain a wide range of interesting and useful information, and are not limited to the formal specification of data communications protocols
- Currently there are more than 3000 RFCs.
- There are three basic types of RFCs:
 - standards (STNDs)
 - best current practices (BCPs)
 - and informational (FYIs).

a. Standards

- RFCs that define official protocol standards
- These standards are given an STND number in addition to an RFC number
- Standards pass through 3 maturity levels:
 Proposed, Draft, Internet
- There are two kinds of standards:
 - Technical Specification (TS) --- defines a protocol
 - Applicability Statement (AS) --- defines when the protocol is to be used

b. Best Current Practices (BCPs)

- These RFCs formally document techniques and procedures.
- Some document the way the governing organization conducts itself, while some provide guidelines for the operation of a network or service.
- BCPs that provide operational guidelines are often of great interest to network administrators.

c. Informational RFCs (FYI)

- FYI documents provide introductory and background material about the Internet and TCP/IP networks.
- FYI documents are not included in the Internet standards process.
- A FYI document is given a FYI number in addition to an RFC number

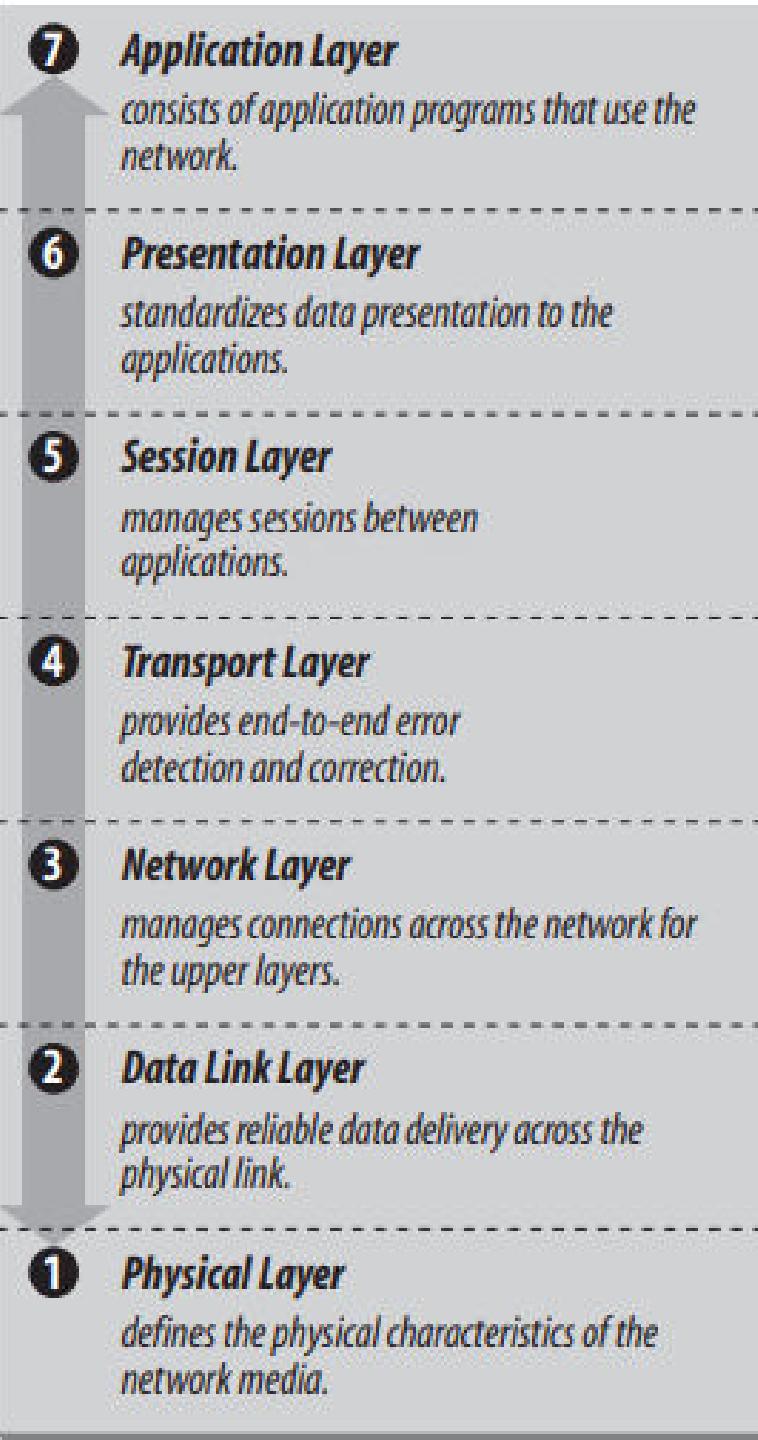
6.2 A data communication model

- A common frame of reference is necessary for understanding data communications terminology so that term ambiguity doesn't come into play.
- An architectural model developed by the International Standards Organization (ISO) is frequently used to describe the structure and function of data communications protocols.
 - The model is called Open Systems Interconnect (OSI) model.
- The terms defined by this model are well understood and widely used in the data communications community

- The OSI Reference Model contains seven layers that define the functions of data communications protocols.
- Each layer of the OSI model represents a function performed when data is transferred between cooperating applications across an intervening network.
- In OSI model, the protocols are like a pile of building blocks stacked one upon another.
 - Because of this appearance, the structure is often called a stack or protocol stack.

- A layer does not define a single protocol—it defines a data communications function that may be performed by any number of protocols.
 - Therefore, each layer may contain multiple protocols, each providing a service suitable to the function of that layer.
- Every protocol communicates with its peers.
 - A peer is an implementation of the same protocol in the equivalent layer on a remote system.
 - E.g. the local File Transfer Protocol is the peer of a remote File Transfer Protocol.
- In the abstract, each protocol is concerned only with communicating to its peers; it does not care about the layers above or below it.

OSI Model



Description about each layers:

Refer to chapter 1 notes.

6.3 TCP/IP protocol Architecture

- TCP/IP is generally viewed as being composed of fewer layers than the seven used in the OSI model.
- Most descriptions of TCP/IP define three to five functional levels in the protocol architecture.
- While some research papers define TCP/IP in terms of 5 layers (**A,T,N,D,P**), the standard model describes model as 4-leveled:
 1. **Application** (*combines Application, Presentation and Session layer from OSI model*)
 2. **Transport**
 3. **Internet** (*Also the Network layer*)
 4. **Network Interface** (*Combines Data Link and Physical layer from OSI model*)

4

Application Layer

consists of applications and processes that use the network.

3

Host-to-Host Transport Layer

provides end-to-end data delivery services.

2

Internet Layer

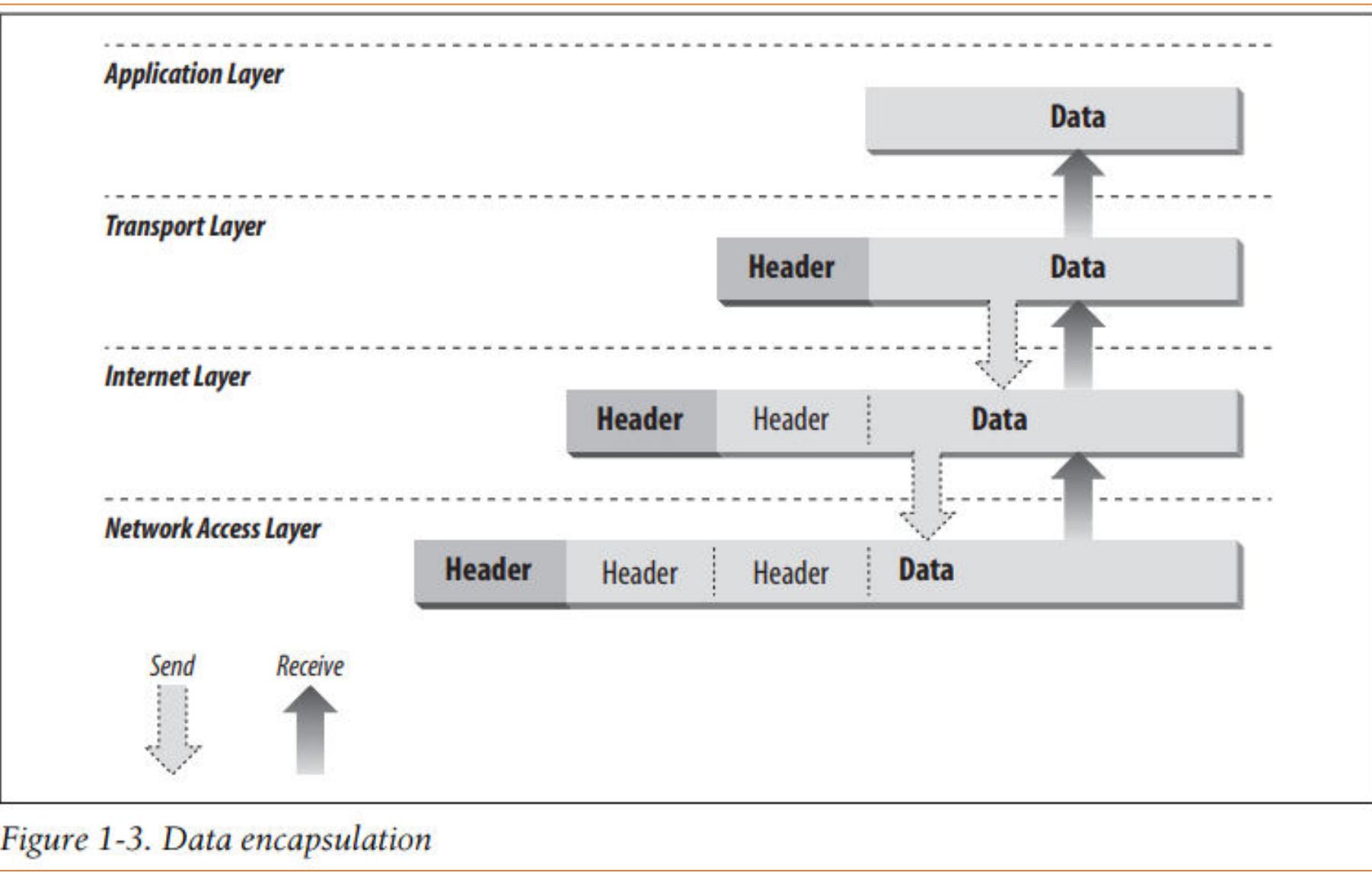
defines the datagram and handles the routing of data.

1

Network Access Layer

consists of routines for accessing physical networks.

- As in the OSI model, data is passed down the stack when it is being sent to the network, and up the stack when it is being received from the network.
- The four-layered structure of TCP/IP is seen in the way data is handled as it passes down the protocol stack from the Application Layer to the underlying physical network.
- Each layer in the stack adds control information to ensure proper delivery.
 - This control information is called a header because it is placed in front of the data to be transmitted



- Each layer treats all the information it receives from the layer above as data, and places its own header in front of that information.
 - The addition of delivery information at every layer is called *encapsulation*.
- When data is received, the opposite happens.
 - Each layer strips off its header before passing the data on to the layer above
- As information flows back up the stack, information received from a lower layer is interpreted as both a header and data.
- Each layer has its own independent data structures and its own terminology to describe that structure.

TCP/IP Model Layers

1. Network Interface Layer

- This layer acts as an interface between hosts and transmission links and used for transmitting datagrams.
- It also specifies what operation must be performed by links like serial link and classic Ethernet to fulfil the requirements of the connectionless internet layer.

2. Internet Layer

- This layer transmits an independent packet into any network which travels to the destination.
- It includes the IP (Internet Protocol), ICMP (Internet Control Message Protocol) and ARP (Address Resolution Protocol) as the standard packet format for the layer.

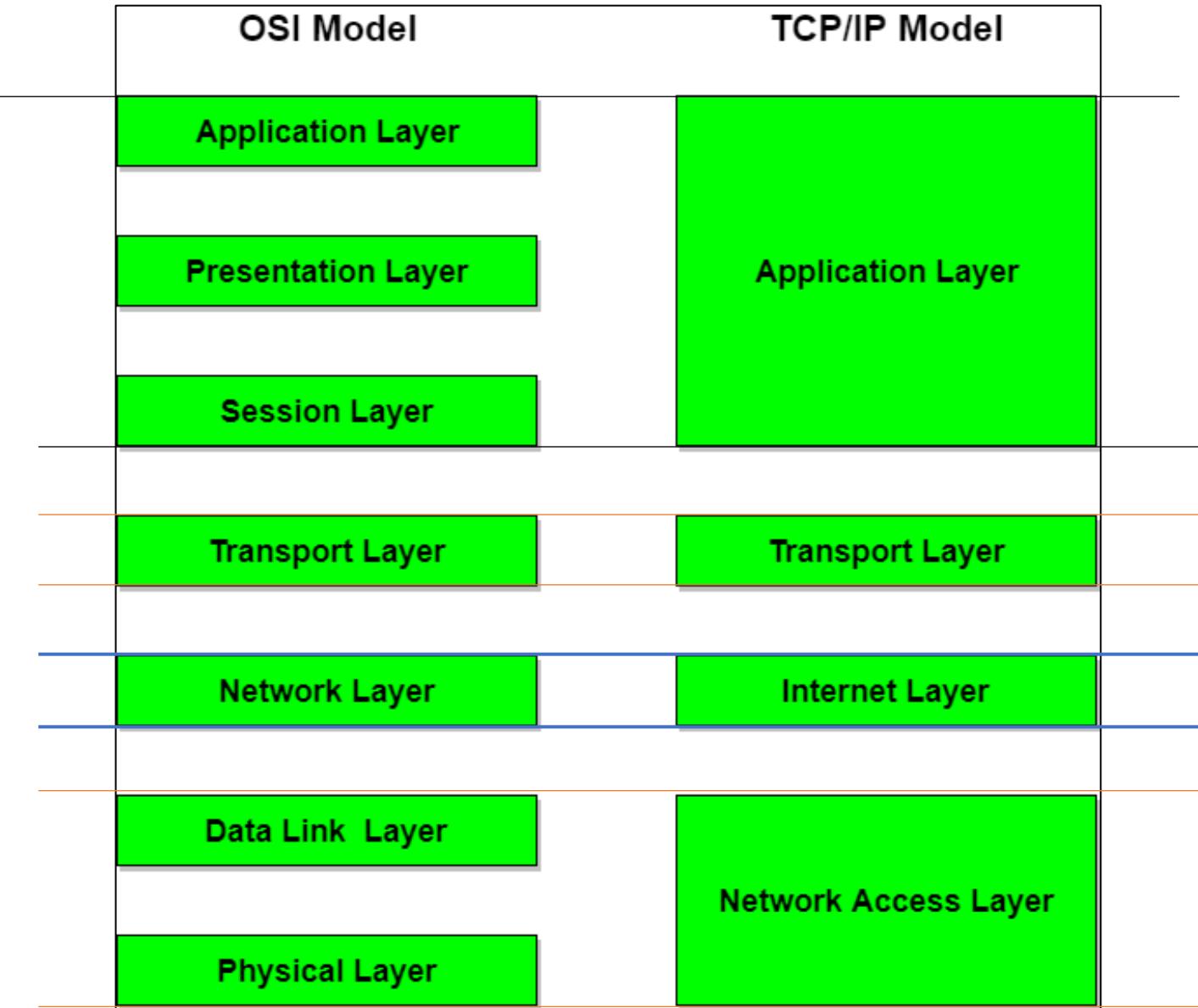
3. Transport Layer

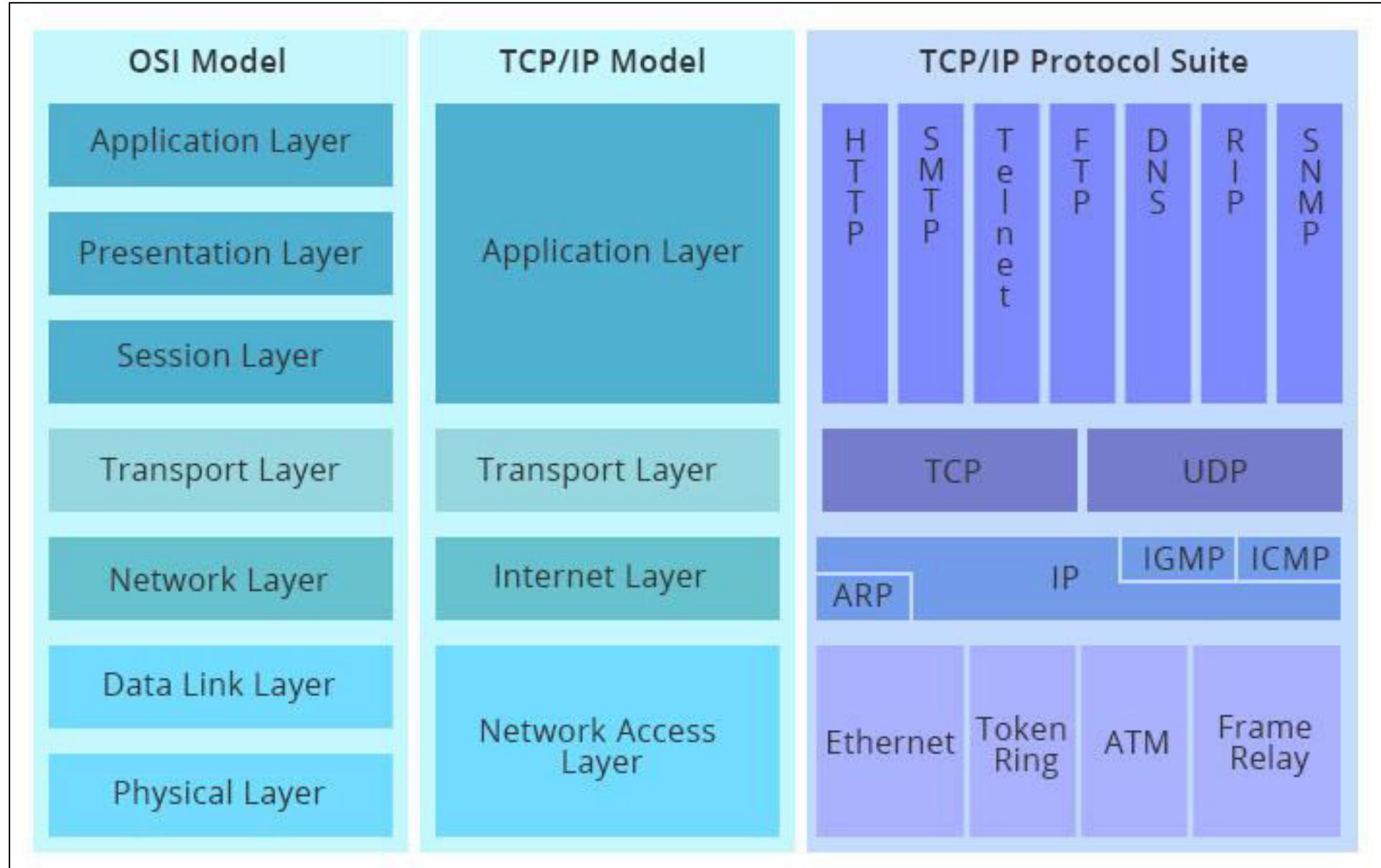
- It enables a fault-free end-to-end delivery of the data between the source and destination hosts in the form of datagrams.
- The protocols defined by this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

4. Application Layer

- This layer permits users to access the services of global or private internet.
- The various protocols described in this layer are virtual terminal (TELNET), electronic mail (SMTP) and file transfer (FTP).
- Some additional protocols like DNS (Domain Name System), HTTP (Hypertext Transfer Protocol) and RTP (Real-time Transport Protocol).
- The working of this layer is a combination of application, presentation and session layer of the OSI model.

OSI model vs TCP/IP model





BASIS FOR COMPARISON	TCP/IP MODEL	OSI MODEL
Expands To	Transmission Control Protocol/ Internet Protocol	Open system Interconnect
Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.
Number Of Layers	4 Layers	7 Layers
Developed by	Department of Defense (DoD)	ISO (International Standard Organization)
Tangible	Yes	No
Usage	Mostly used	Never used
Obeys	Horizontal approach	Vertical approach

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. Transport Layer is Connection Oriented.	5. Transport Layer is both Connection Oriented and Connection less.
6. Network Layer is both Connection Oriented and Connection less.	6. Network Layer is Connection less.
7. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	7. TCP/IP model is, in a way implementation of the OSI model.
8. Network layer of OSI model provides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
9. OSI model has a problem of fitting the protocols into the model.	9. TCP/IP model does not fit any protocol
10. Protocols are hidden in OSI model and are easily replaced as the technology changes.	10. In TCP/IP replacing protocol is not easy.

6.4 Network Access layer (or Network Interface Layer)

- This layer defines how to use the network to transmit an IP datagram
- The protocols in this layer provide the means for the system to deliver data to the other devices on a directly attached network.
- Unlike higher-level protocols, Network Access Layer protocols must know the details of the underlying network (its packet structure, addressing, etc.) to correctly format the data being transmitted to comply with the network constraints
- The TCP/IP Network Access Layer can encompass the functions of all three lower layers of the OSI Reference Model (Network, Data Link, and Physical).

- Functions performed at this level include encapsulation of IP datagrams into the frames transmitted by the network, and mapping of IP addresses to the physical addresses used by the network.
- Two RFCs that define Network Access Layer protocols are:
 1. RFC 826, Address Resolution Protocol (ARP)
 - It maps IP addresses to Ethernet addresses
 2. RFC 894, A Standard for the Transmission of IP Datagrams over Ethernet Networks
 - It specifies how IP datagrams are encapsulated for transmission over Ethernet networks
- As implemented in Unix, protocols in this layer often appear as a combination of device drivers and related programs

6.5 Internet Layer

- The layer above the Network Access Layer in the protocol hierarchy.
- The Internet Protocol (IP) is the most important protocol in this layer.
- IP protocol helps to exchange data with remote systems.
- IP provides the basic packet delivery service on which TCP/IP networks are built.
- All protocols, in the layers above and below IP, use the Internet Protocol to deliver data.
- All incoming and outgoing TCP/IP data flows through IP, regardless of its final destination.
- The release of IP used in the current Internet is IP version 4 (IPv4), which is defined in RFC 791.
 - There are more recent versions of IP (i.e. IPv6) that have completely different address structure than IPv4.

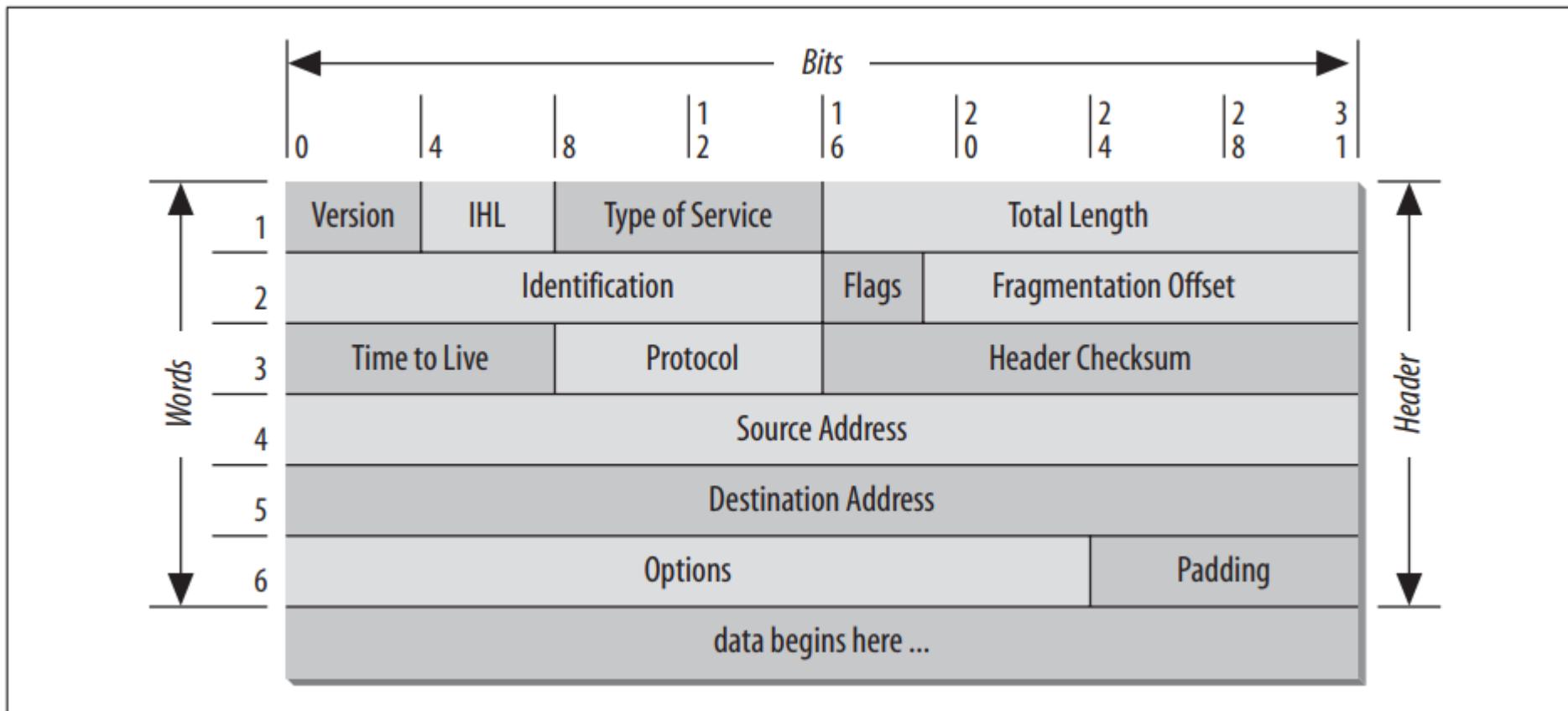
6.5.1 Internet Protocol

- IP defines the datagram, which is the basic unit of transmission in the Internet.
- It defines the Internet addressing scheme.
- It helps moving data between the Network Access Layer and the Transport Layer.
- Responsible for routing datagrams to remote hosts.
- It performs fragmentation and re-assembly of datagrams

- Internet Protocol is a *connectionless protocol*.
 - This means, it does not exchange control information(called a *handshake*) to establish an end-to-end connection before transmitting data.
 - The Internet Protocol relies on protocols in other layers to establish the connection if they require connection-oriented service.
- The Internet Protocol(IP) is sometimes called an *unreliable protocol* because it contains no error detection and recovery code.
- It is not implied that IP cannot be relied on.
 - IP can be relied upon to accurately deliver your data to the connected network, but it doesn't check whether that data was correctly received.
 - Protocols in other layers of the TCP/IP architecture provide this checking when it is required

6.5.2 Datagram

- A packet-switching network uses the addressing information in the packets to switch packets from one physical network to another, moving them toward their final destination.
 - TCP/IP is a packet-switching network that was built to transmit data over ARPAnet.
- The datagram is the packet format defined by the Internet Protocol.
- IP datagram consists of data and header.
 - The 1st 5 or 6 32-bit words of datagram are control information called *header*.



- By default, the header is five words long; the sixth word is optional.
 - Because the header's length is variable, it includes a field called Internet Header Length (IHL) that indicates the header's length in words.
- The Internet Protocol delivers the datagram by checking the *Destination Address* in word 5 of the header.
 - The Destination Address is a standard 32-bit IP address that identifies the destination network and the specific host on that network.
- If the Destination Address is the address of a host on the local network, the packet is delivered directly to the destination.
 - If the Destination Address is not on the local network, the packet is passed to a gateway for delivery
- Deciding which gateway to use is called *routing*.
 - IP makes the routing decision for each individual packet

6.5.3 Routing Datagrams

- In TCP/IP terminology, there are 2 types of network devices: *gateways* and *hosts*.
- The hosts (or end systems) process packets through all four protocol layers, while the gateways (or intermediate systems) process the packets only up to the Internet Layer where the routing decisions are made.
- Systems can deliver packets only to other devices attached to the same physical network.
- the underlying physical networks a datagram travels through may be different and even incompatible.

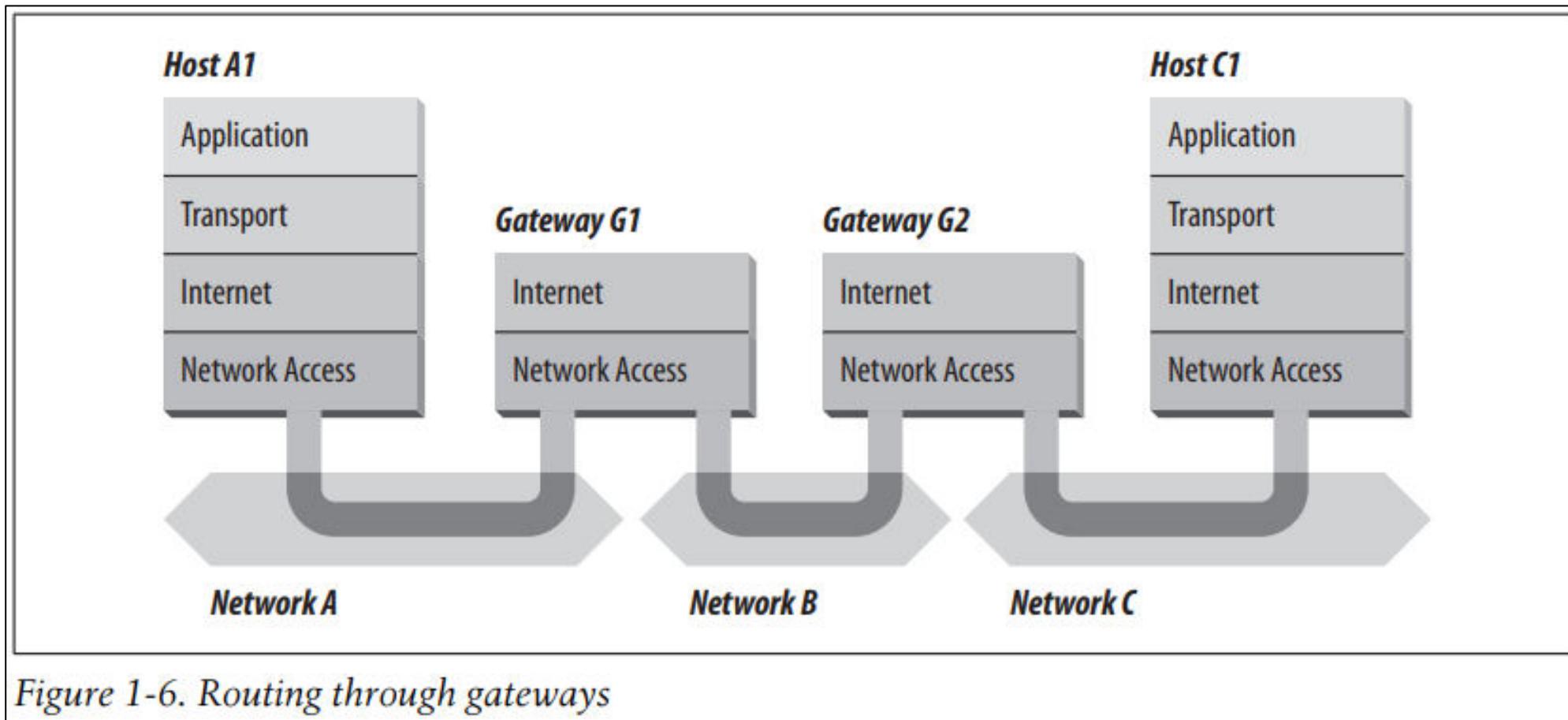
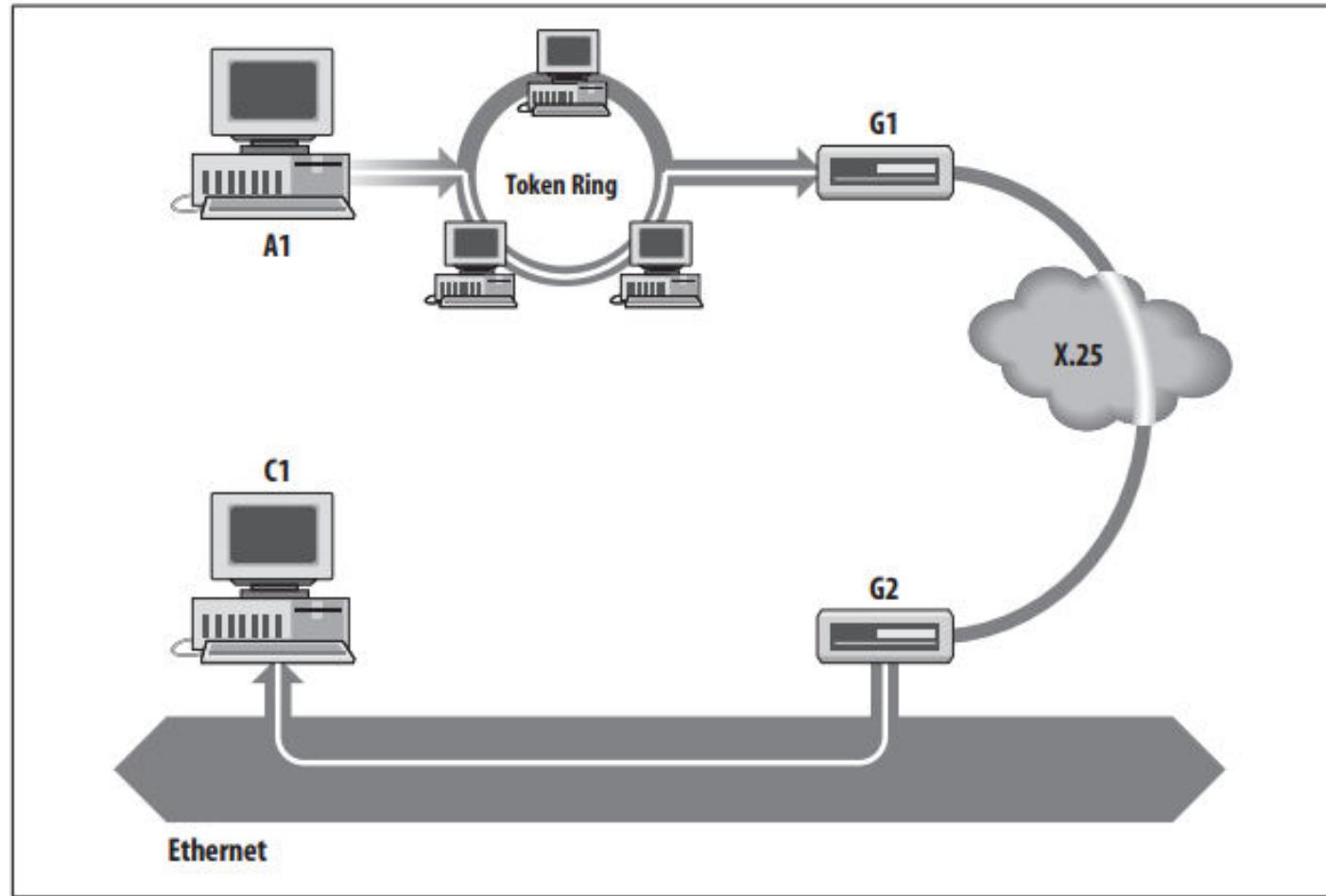


Figure 1-6. Routing through gateways

Routing (a)

- Packets from A1 destined for host C1 are forwarded through gateways G1 and G2.
- Host A1 first delivers the packet to gateway G1, with which it shares network A.
- Gateway G1 delivers the packet to G2 over network B. Gateway G2 then delivers the packet directly to host C1 because they are both attached to network C.
- Host A1 has no knowledge of any gateways beyond gateway G1.
- It sends packets destined for both networks C and B to that local gateway and then relies on that gateway to properly forward the packets along the path to their destinations.
- Likewise, host C1 sends its packets to G2 to reach a host on network A, as well as any host on network B.



Routing (b)

- Host A1 on the token ring network routes the datagram through gateway G1 to reach host C1 on the Ethernet.
- Gateway G1 forwards the data through the X.25 network to gateway G2 for delivery to C1.
- The datagram traverses three physically different networks, but eventually arrives intact at C1.

6.5.4 Fragmenting Datagrams

- when a gateway interconnects dissimilar physical networks, a datagram received from one network may be too large to be transmitted in a single packet on another network.
- As a datagram is routed through different networks, it may be necessary for the IP module in a gateway to divide the datagram into smaller pieces.
- Each type of network has a maximum transmission unit (MTU), which is the largest packet that it can transfer.
 - If the datagram received from one network is longer than the other network's MTU, the datagram must be divided into smaller fragments for transmission.
 - This process is called fragmentation.

- The format of each fragment is the same as the format of any normal datagram.
 1. Header word 2 contains information that identifies each datagram fragment and provides information about how to re-assemble the fragments back into the original datagram.
 2. The Identification field identifies what datagram the fragment belongs to, and the Fragmentation Offset field tells what piece of the datagram this fragment is.
 3. The Flags field has a “More Fragments” bit that tells IP if it has assembled all of the datagram fragments.

6.5.5 Passing datagrams to Network Layer

- When IP receives a datagram that is addressed to the local host, it must pass the data portion of the datagram to the correct Transport Layer protocol.
- This is done by using the protocol number from word 3 of the datagram header.
 - Each Transport Layer protocol has a unique protocol number that identifies it to IP.

6.6 Internet Control Message Protocol

ICMP : Background

- ICMP is an integral part of IP that is defined in RFC792.
- This protocol is part of the Internet Layer and uses the IP datagram delivery facility to send its messages.
- ICMP sends messages that perform the flow control, error reporting, and informational functions for TCP/IP.

6.6.1 Flow control

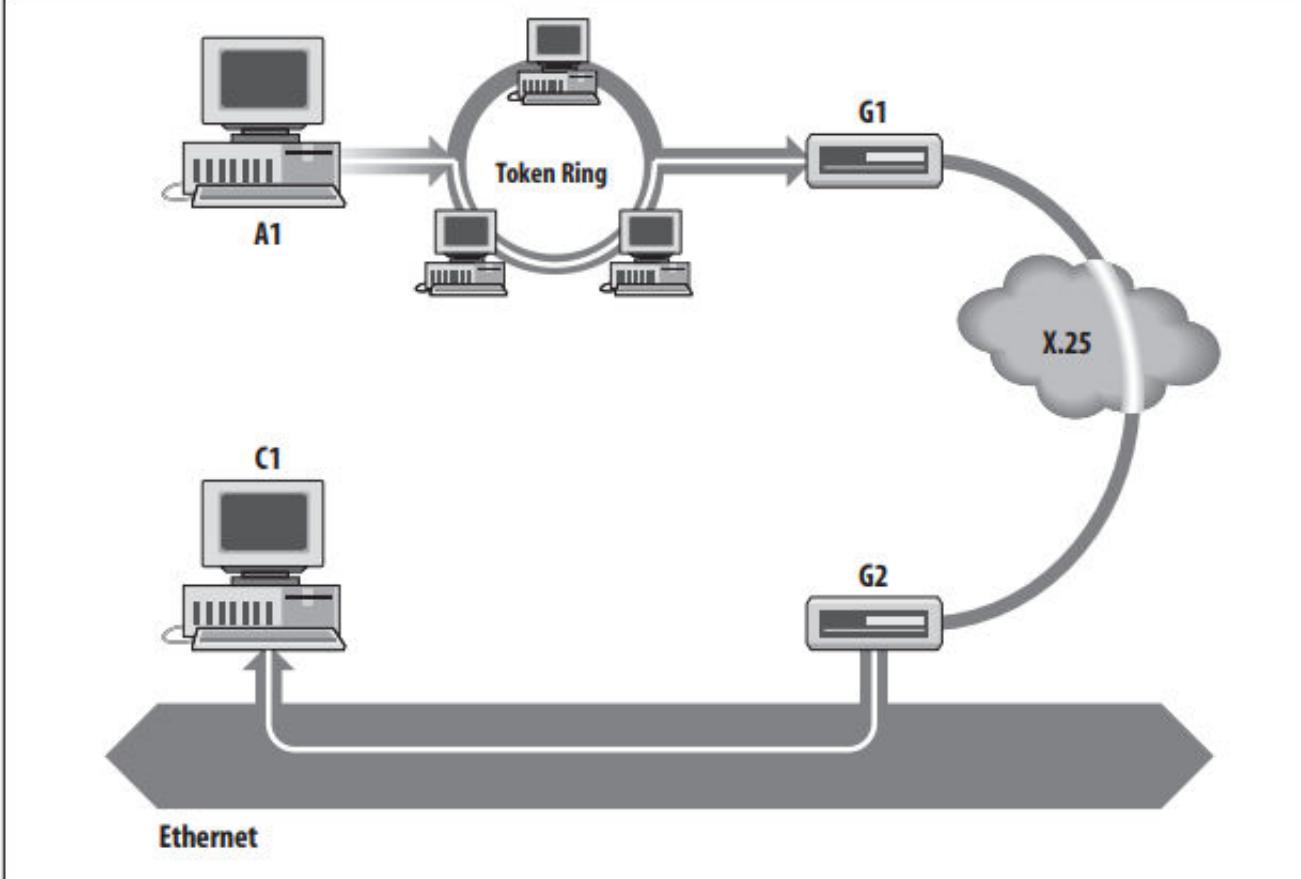
- When datagrams arrive too fast for processing, the destination host or an intermediate gateway sends an ICMP Source Quench Message back to the sender.
 - This tells the source to stop sending datagrams temporarily.

6.6.2 Detecting unreachable destinations

- When a destination is unreachable, the system detecting the problem sends a “Destination Unreachable” Message to the datagram’s source.
- If the unreachable destination is a network or host, the message is sent by an intermediate gateway.
- But if the destination is an unreachable port, the destination host sends the message.

6.6.3 Redirecting routes

- A gateway sends the ICMP Redirect Message to tell a host to use another gateway, presumably because the other gateway is a better choice.
 - This message can be used only when the source host is on the same network as both gateways.
- E.g. on next page



- If a host on the X.25 network sent a datagram to G1, it would be possible for G1 to redirect that host to G2 because the host, G1, and G2 are all attached to the same network.
- On the other hand, if a host on the token ring network sent a datagram to G1, the host could not be redirected to use G2. This is because G2 is not attached to the token ring.

6.6.4 Checking remote hosts

- A host can send the ICMP Echo Message to see if a remote system's Internet Protocol is up and operational.
- When a system receives an echo message, it replies and sends the data from the packet back to the source host.
- The *ping* command uses this message.

6.7 Transport Layer

Background

- The protocol layer just above the Internet Layer
- Also called Host-to-Host Transport Layer,
- Both protocols deliver data between the Application Layer and the Internet Layer.
- The two most important protocols in the Transport Layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
 - TCP provides reliable data delivery service with end-to-end error detection and correction.
 - UDP provides low-overhead, connectionless datagram delivery service.
- Applications programmers can choose whichever service is more appropriate for their specific applications

6.7.1 User Datagram Protocol (UDP)

- The User Datagram Protocol gives application programs direct access to a datagram delivery service, like the delivery service that IP provides.
 - This allows applications to exchange messages over the network with a minimum of protocol overhead.
- UDP is an unreliable, connectionless datagram protocol
 - This is because, there are no techniques in the protocol for verifying that the data reached the other end of the network correctly.
- Within the same computer, UDP will however deliver data correctly.
- UDP uses 16-bit Source Port and Destination Port numbers in word 1 of the message header to deliver data to the correct applications process.

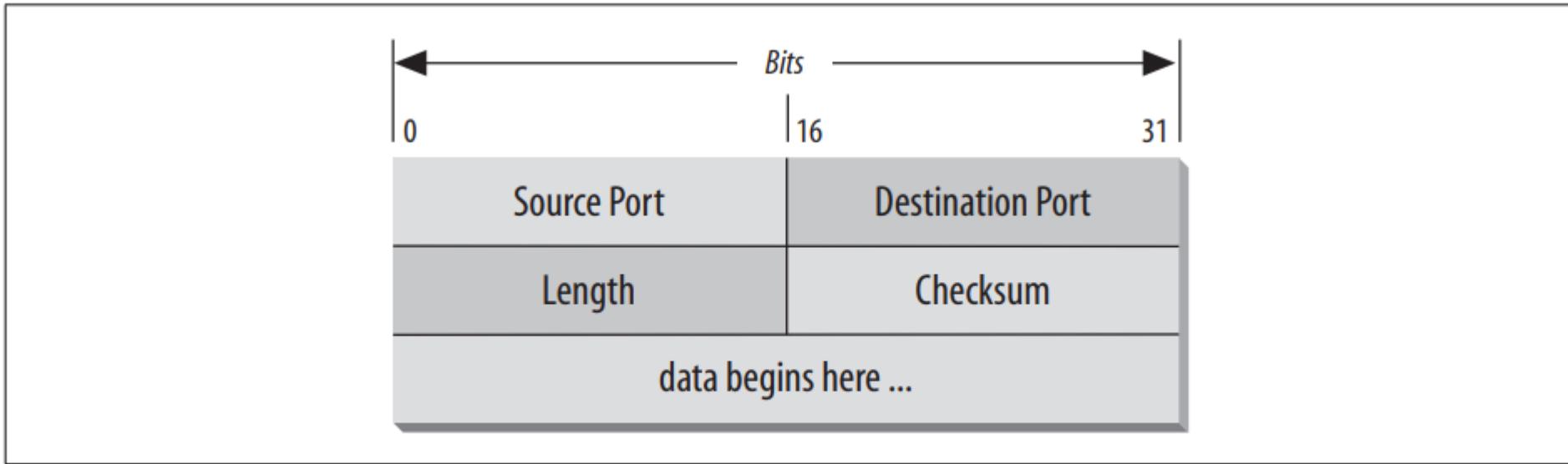


Figure 1-8. UDP message format

Why UDP?

- UDP is the most efficient choice for a Transport Layer protocol if the amount of data being transmitted is small.
 - This is because the overhead of creating connections and ensuring reliable delivery may be greater than the work of re-transmitting the entire data set.
- Applications that fit a query-response model are good candidates for UDP.

6.7.2 Transmission Control Protocol (TCP)

- Applications that require the transport protocol to provide reliable data delivery use TCP because it verifies that data is delivered across the network accurately and in the proper sequence.
- TCP is a *reliable*, *connection-oriented*, *byte-stream* protocol.
- TCP provides reliability with a mechanism called Positive Acknowledgment with Retransmission (PAR).
 - System using PAR sends the data again unless it hears from the remote system that the data arrived OK.

- The unit of data exchanged between cooperating TCP modules is called a *segment*.
- Each segment contains a checksum that the recipient uses to verify that the data is undamaged.
 - If the data segment is received undamaged, the receiver sends a positive acknowledgment back to the sender.
 - If the data segment is damaged, the receiver discards it.
- After an appropriate timeout period, the sending TCP module re-transmits any segment for which no positive acknowledgment has been received.

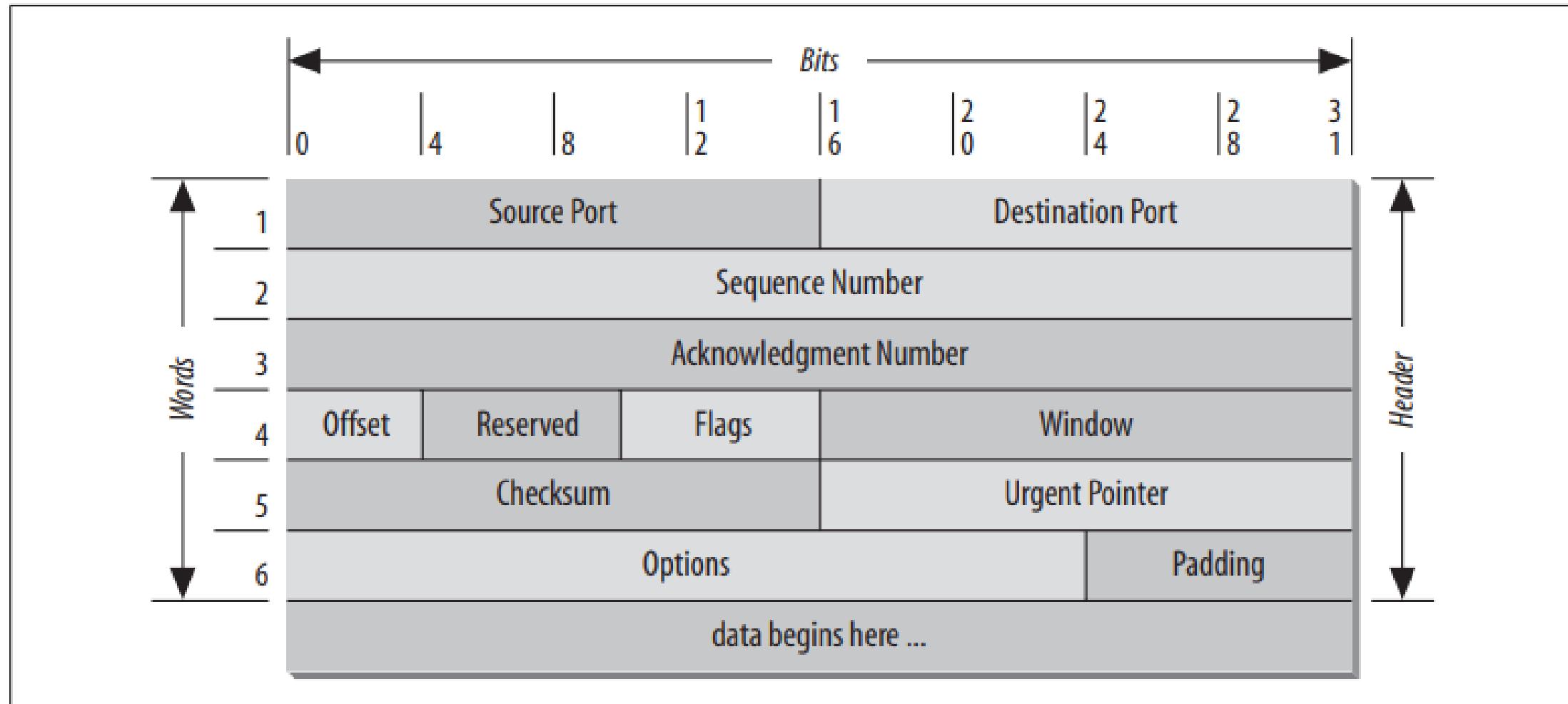


Figure 1-9. TCP segment format

- TCP is connection-oriented, as it establishes a logical end-to-end connection between the two communicating hosts.
- Control information, called a *handshake*, is exchanged between the two endpoints to establish a dialogue before data is transmitted.
- The type of handshake used by TCP is called a *3-way handshake* because three segments are exchanged before establishing connection.
 - Tx sends synchronize signal SYN to Rx.
 - Rx sends acknowledgement signal ACK along with SYN signal bits to Tx.
 - Tx sends acknowledgement signal ACK along with data bits to Rx.

- TCP views data as continuous stream of bytes, not as independent packets.
 - Therefore, TCP takes care to maintain the sequence in which bytes are sent and received.
 - The Sequence Number and Acknowledgment Number fields in the TCP segment header keep track of the bytes.

Differentiating TCP and UDP

- UDP is faster, simpler and efficient and hence generally used for sending audio, video files.
 - Used for music streaming, VoIP
- TCP, on the other hand, is robust, reliable and guarantees the delivery of packets in the same order.
 - Used for emails, web browsers

Differences between UDP and TCP

1. TCP is Connection-oriented whereas, UDP is Connectionless protocol.
2. TCP is highly reliable for transferring useful data as it takes the acknowledgement of information sent. Also, resends the lost packets if any. Whereas in the case of UDP if the packet is lost it won't request for retransmission and the destination computer receives corrupt data. So, UDP is an unreliable protocol.
3. TCP is slower as compared to UDP since TCP establishes the connection before transmitting data, and ensures the proper delivery of packets. On the other hand, UDP does not acknowledge whether the data transmitted is received or not.
4. Header size of UDP is 8 bytes, and that of TCP is more than double. TCP header size is 20 bytes since, and TCP header contains options, padding, checksum, flags, data offset, acknowledgement number, sequence number, source and destination ports, etc.
5. Both TCP and UDP can check for errors, but only TCP can correct the error since it has both congestion and flow control.

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP header size is 20 bytes.	UDP Header size is 8 bytes.
TCP is heavy-weight.	UDP is lightweight.
TCP is used by HTTP, HTTPS, FTP, SMTP and Telnet	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

6.8 Application Layer

Introduction

- The top of the TCP/IP protocol architecture.
- This layer includes all processes that use the Transport Layer protocols to deliver data.
- There are many applications protocols.
 - Most provide user services, and new services are always being added to this layer
- Some of the widely used application protocols are *Telnet*, *FTP*, *HTTP*, *SMTP* etc.

Some Application Protocols

1. HTTP

- Hypertext Transfer Protocol
- It delivers web pages over the network

2. FTP

- File Transfer Protocol
- Used for interactive file transfer.

3. SMTP

- Simple Mail Transfer Protocol
- It delivers electronic mail.
- message transfer agent

4. POP3

- Post Office Protocol 3
- used by e-mail clients to retrieve e-mail from a mail server.
- message access agent

5. IMAP

- Internet Message Access Protocol
- Used email clients to retrieve email messages from a mail server over a TCP/IP connection
- While POP3 downloads email from a server to a single device **and** deletes it from the server, IMAP ensures that emails are synced across multiple devices.

6. DNS

- Domain Name System
- It maps IP addresses to the names assigned to network devices.

7. Telnet

- a network text-only protocol that provides bidirectional interactive communications facility using virtual terminal connection.
- Allows connection to remote computers (called hosts) over a TCP/IP network (such as the internet)

End of chapter

Related Questions:

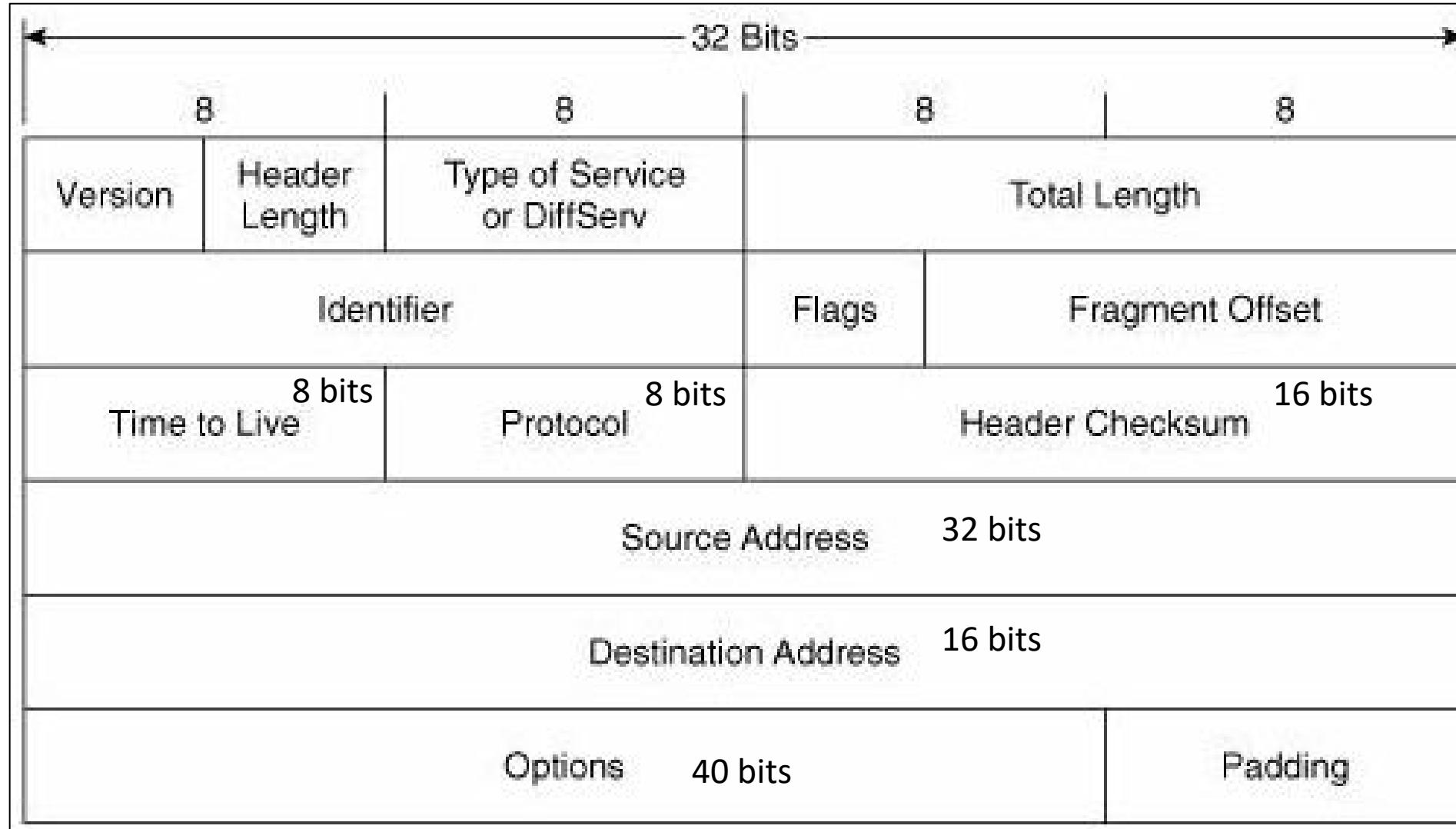
1. TCP/IP architecture showing layers and protocols
2. OSI vs TCP/IP
3. TCP vs UDP
4. Write short notes on:
 - a) ICMP
 - b) IPv4
 - c) IPv6

Extra Questions

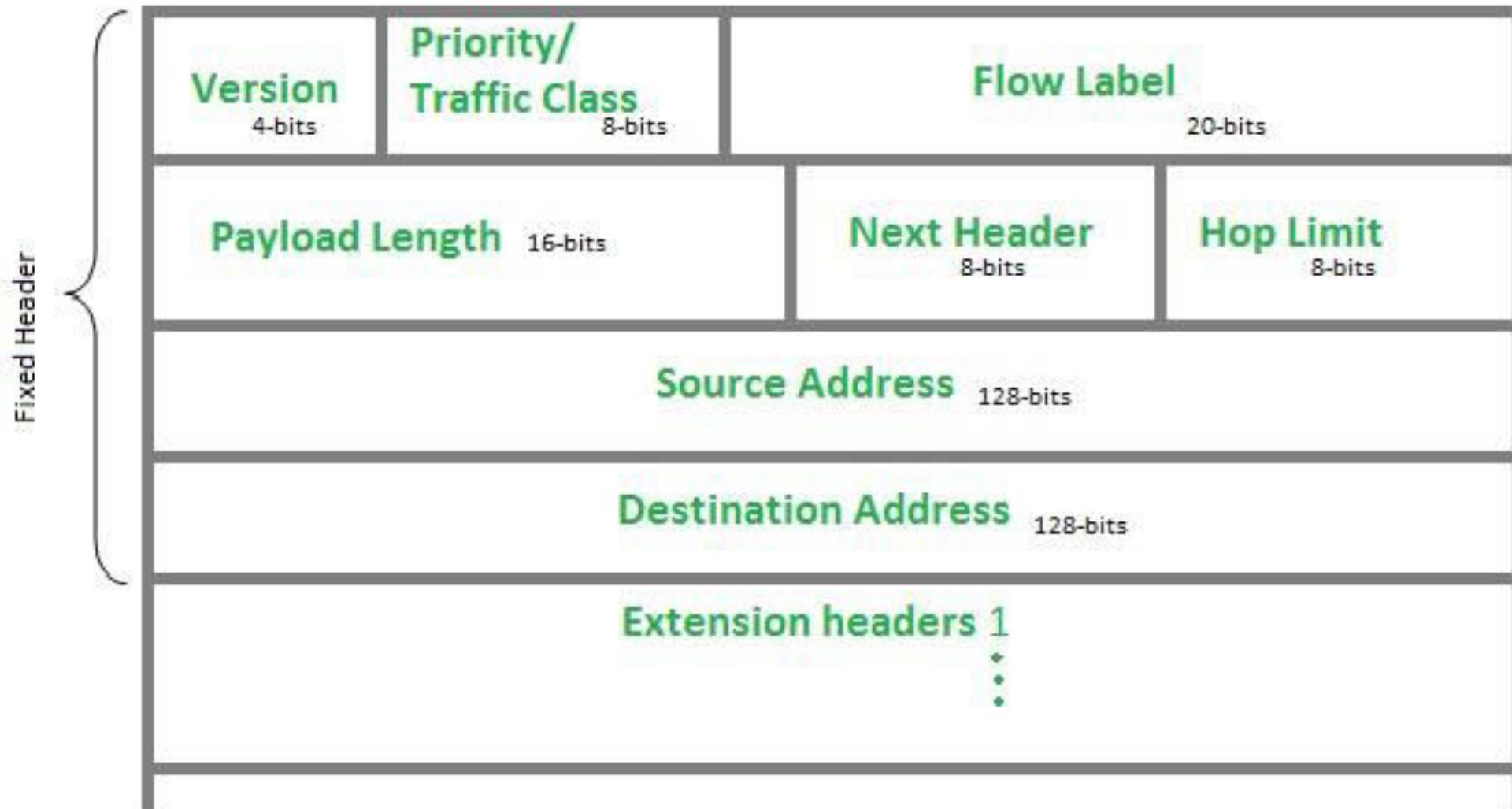
- IPv4 vs IPv6
- Header format for ipv4 and ipv6

Extra topics - Answers

- IPv4 header format



- IPv6 header format



Differences between IPv4 and IPv6

1. IPv4 has 32-bit address length whereas IPv6 has 128-bit address length.
 2. IPv4 addresses represent the binary numbers in decimals. On the other hand, IPv6 addresses express binary numbers in hexadecimal.
 3. while IPv4 requires an intermediate router to fragment any datagram that is too large, IPv6 uses end-to-end fragmentation.
 4. Header length of IPv4 is 20 bytes. In contrast, header length of IPv6 is 40 bytes.
- Write detailed differences from:
<https://techdifferences.com/difference-between-ipv4-and-ipv6.html>

IPv4 vs IPv6

IPv4	IPv6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address space for IPv4 is lower as compared to IPv6 (2^{32} address spaces)	Address space of IPv6 is quite large (around 2^{128} address spaces)
Checksum field is available in IPv4 headers	Checksum field is not available
Ipv4 addresses will be exhausted someday	There are enough ipv6 addresses to allocated one value to every computing devices.

Computer Networks

Chapter 7 Delivering the data

(4 Hours \approx 7-8 marks)

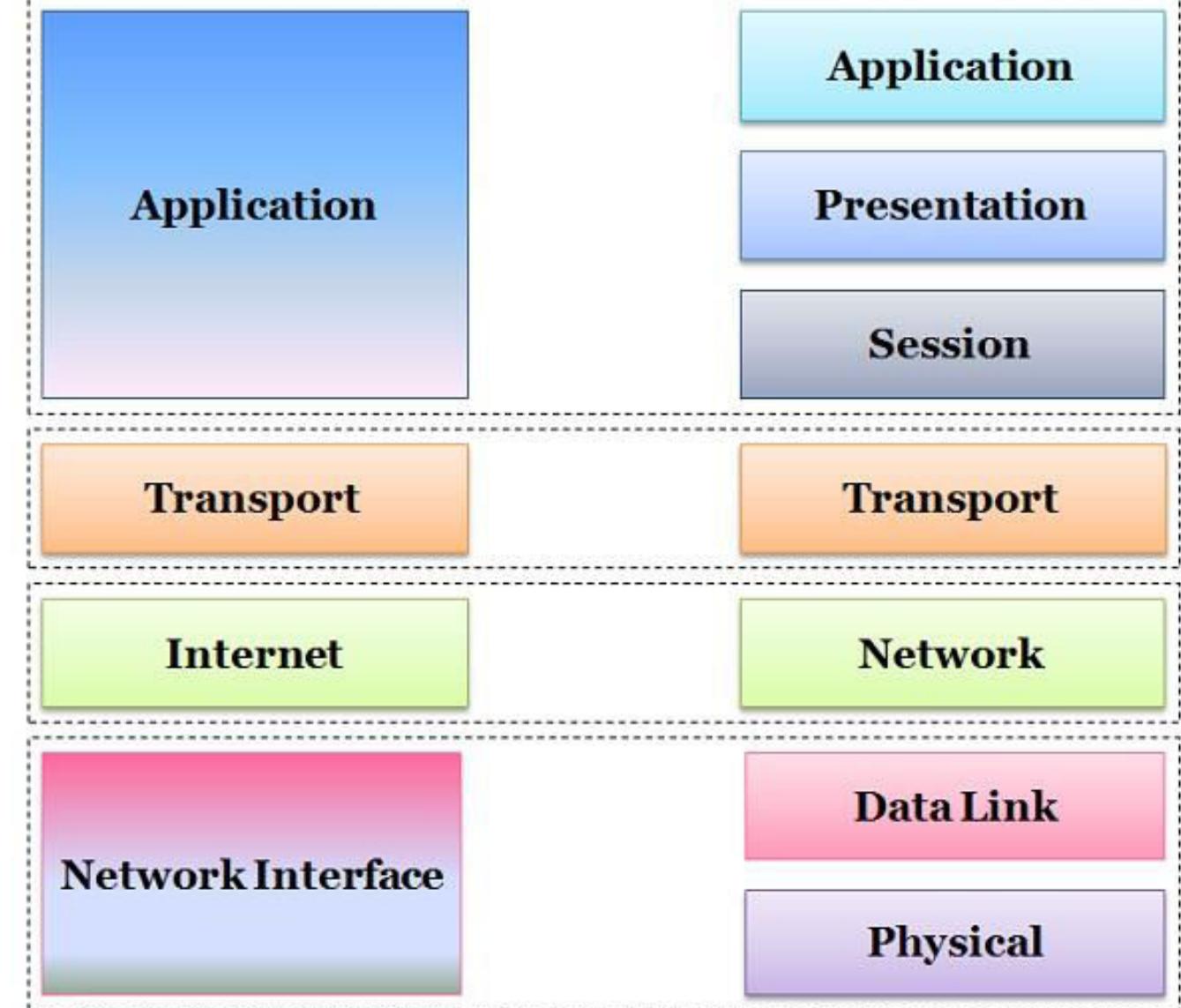
Background

❖ TCP/IP model

- OSI is a conceptual model which is not practically used for communication.
 - Whereas, TCP/IP is used for establishing a connection and communicating through the network.
- TCP/IP Model is reliable over OSI Model, TCP/IP is used for end to end connection so as to transmit the data over the internet.
- Unlike OSI Model, TCP/IP consists of four layers each having its own protocols. Internet Protocols are the set of rules defined for communication over the network.

TCP/IP MODEL Vs OSI MODEL

1. Application layer
 - This layer permits users to access the services of global or private internet.
 - E.g. TELNET, SMTP, HTTP, FTP, DNS
2. Transport layer
 - It enables a fault-free end-to-end delivery of the data between the source and destination hosts in the form of datagrams.
 - E.g. TCP, UDP
3. Internet layer
 - This layer transmits an independent packet into any network destination .
 - E.g. IP, ICMP, ARP
4. Network layer
 - It acts as an interface between hosts and transmission links and used for transmitting datagrams.



Chapter Outlines

1. Addressing, routing, and multiplexing
2. The IP address
3. Address Depletion (Reduce)
4. Subnets
5. Address Resolution
6. Ports and Sockets

7.1 Addressing, routing, and multiplexing

- To deliver data between two Internet hosts, it is necessary to move the data across the network to the correct host, and within that host to the correct user or process.
- TCP/IP uses three schemes to accomplish these tasks:
 1. **Addressing**
 - IP addresses, which uniquely identify every host on the Internet, deliver data to the correct host.
 2. **Routing**
 - Gateways deliver data to the correct network.
 3. **Multiplexing**
 - Protocol and port numbers deliver data to the correct software module within the host.
- Each of these functions - **addressing** between hosts, **routing** between networks, and **multiplexing** between layers - is necessary to send data between two cooperating applications across the Internet.

7.2 The IP Address

- An IP address is a 32-bit value that uniquely identifies every device attached to a TCP/IP network.
- IP addresses are usually written as four decimal numbers separated by dots (periods) in a format called dotted decimal notation.
 - Each decimal number represents an 8-bit byte of the 32-bit address.
 - Each of the four numbers lie in the range (0-255)
 - E.g. 192.168.10.10, 172.16.12.0
- IP addresses are assigned to network interfaces, not to computer systems.

- Systems can be addressed in three different ways:
 1. Unicast Address
 - Address for individual systems.
 - A unicast packet is addressed to one individual host.
 2. Multicast Address
 - Address for group of systems.
 - A router routes copies of the packet to each member of the multicast group.
 - Not all routers readily support multicast address.
 3. Broadcast Address
 - Address for all systems on a network.
 - Broadcast address depends on the broadcast capabilities of the underlying physical network.

- Some IP addresses (host addresses) are reserved for special uses.
 - On all networks, host numbers **0** and **255** are reserved.
 - N/w addresses with a first byte value greater than **223** cannot be assigned to a physical network as they are reserved for special use.
 - Other n/w addresses are **0.0.0.0** (default route) and **127.0.0.1** (loopback address)
- An IP address with all host bits set to **1**(binary) is a broadcast address.
 - E.g. broadcast address for **172.16** network is **172.16.255.255**
- An IP address with all host bits set to 0 identifies the network itself.
 - E.g. **10.0.0.0** refers to network **10**, and **172.16.0.0** refers to network **172.16**
- Addresses in these forms are used in routing tables to refer to the entire n/w.

Address structure

- An IP address contains of Network part (N) and a Host part (H).
- The number of address bits used to identify the network and host number vary according to the prefix length of the address.
 - The prefix length is determined by the address mask.
- If a bit is on in the mask, that equivalent bit in the address is interpreted as a network bit; if a bit in the mask is off, the bit belongs to the host part.
 - For example, if address **172.22.12.4** is given the network mask **255.255.255.0**, which has **24** bits on and **8** bits off, the first **24** bits are the network number and the last **8** bits are the host address.
- Instead of writing network **172.31.26.32** with a mask of **255.255.255.224**, we can write **172.31.26.32/27**.
 - The format of this notation is *address/prefix-length*, where *prefix-length* is the number of bits in the network portion of the address.

- ❖ Because the prefix shows the length of the network address, the number of host addresses available to an organization (the host portion of the address) is determined by subtracting the prefix from the total number of bits in an address, which is 32.
 - ❖ Thus a prefix of **20** (E.g. **192.168.16.0/20**) leaves **12** bits that are available to be locally assigned. This is called a “**12-bit block**” of addresses.
 - This means, an organization with given IP address encompasses 4,096 addresses from 192.168.16.0 to 192.168.31.255.
 - ❖ A prefix of **24** (E.g. **192.168.32.0/24**) creates an “**8-bit block**.”
 - This means, it includes the 256 addresses from 192.168.32.0 to 192.168.32.255.
- ❖ Each of these address blocks appears to the outside world to be a single “network” address.

7.3 Address Depletion (Reduce)

- IPv4, the current IP address system, is limited to approximately 4 billion possible addresses, a threshold that is quickly approaching as a countless new devices connect to the internet.
- When no IPv4 addresses are left, new devices or websites will be unable to access the internet.
- While temporary solutions such as IP sharing for business and home networks slow this depletion, they will not prevent the ultimate depletion of IPv4 addresses.

Cause for IPv4 address exhaustion

1. Digital Networking Devices (Mobile devices)

- Use of mobile phones for digital communication increased the demand on limited supply of addresses.

2. Always-on connections (Broadband connection networks)

- Unlike dial-up modems that would share the IP pool, current broadband networks are always active and uptake addresses assigned by ISPs.

3. Huge Spike in Internet Demography

- While only a small portion had access to internet in early 90s, almost half of the total population enjoyed internet facilities 15 years later.

4. Inefficient address use

- Companies that obtained IP addresses in 1980s were often allocated far more addresses than they actually required.

Mitigation against depletion

1. Use of NAT (Network Address Translation)
 - It allows a private network to use one public IP address and permits private addresses in the private network.
2. Use of private network addressing.
3. Name based virtual hosting of web site.
4. Network renumbering and subnetting.

7.4 Subnets

- In subnetting, a network is divided into several smaller subnetworks with each subnetwork (or subnet) having its own subnetwork address.
- Subnetting allows decentralized management of host addressing.
 - With the standard addressing scheme, a central administrator is responsible for managing host addresses for the entire network.
 - By subnetting, the administrator can delegate address assignment to smaller organizations within the overall organization— which may be a political expedient, if not a technical requirement.
- The structure of an IP address can be locally modified by using host address bits as additional network address bits.
 - Essentially, the “dividing line” between network address bits and host address bits is moved, creating additional networks but reducing the maximum number of hosts that can belong to each network.
 - These newly designated network bits define an address block within the larger address block, which is called a subnet.

- Subnetting allows the network to be split into several parts for internal use but still act like a single network to the outside world.
- Each subnet addresses have unique address.
- Unlike 2 level hierarchy (Net ID, Host ID) in traditional IP allocation, Subnetting supports 3 level addressing:
 - a) Site ID
 - b) Subnet ID
 - c) Host ID

Subnet Masks

- The network mask is used to find the first address in the block or the network address.
 - However, when a mask is subnetted, the situation is different.
- To implement subnetting, the main router needs a subnet mask that indicates the split between (network + subnet number) and host.
- Subnet masks can also be written in dotted decimal notation.
 - Here subnet masks are represented by addition of a slash followed by no. of bits in the network+subnet part.
 - E.g. subnet mask can be written as 255.255.252.0 or denoted by /22 to indicate that the subnet mask is of 22 bits.

How to find subnet address

1. Straight method

- Use binary notation for both the address and the mask.
- Apply AND operation to find the subnet address.

E.g. What is the subnetwork address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0?

	Binary Form	Decimal Form
Given IP address	11001000 00101101 00100010 00111000	200.45.34.56
Subnet Mask	11111111 11111111 11110010 00000000	255.255.240.0
-----	Logical AND	-----
Subnet Address	11001000 00101101 00100010 00000000	200.45.32.0

2. Shortcut method

- Useful when subnet mask has a run of 1s followed by run of 0s (contiguous mask).
 - If the byte in the mask is 0, the subnet address byte is 0.
 - If the byte in the mask is 255, copy the address byte in subnet address byte.
 - If the byte in the mask is between 0 & 255, binary ADD address and mask.

E.g. What is the subnetwork address if the destination address is 19.30.84.5 and the subnet mask is 255.255.192.0?

Address :	192.30.84.5	11000000 00011110 01010100 00000101		
Subnet Mask :	255.255.192.0	11111111 11111111 11000000 00000000		
	255	255	192	0
<Actions>	Copy Address Byte	Copy Address Byte	AND 84 with 192	Place 0 on address
	192	30	(01000000) 64	0

Designing subnet masks

a) Number of subnetworks

- Count number of extra 1s that are added to the default mask to make subnet mask.
- Calculate 2^n where n is the number of extra 1s.
- E.g. if default mask is 255.255.0.0 and subnet mask is 255.255.254.0, then the number of extra 1s in subnet mask (wrt default mask) is 3.
 - Hence, total number of subnetworks possible = $2^3 = 8$

Default mask: 255.255.0.0	11111111	11111111	00000000	00000000
Subnet Mask : 255.255.254.0	11111111	11111111	11100000	00000000

b) Number of addresses per subnetwork

- Count the number of 0s in the subnet mask.
- Calculate 2^n where n is the number of 0s.
- E.g. if subnet mask is 255.255.254.0, then the number of 0s in subnet mask is 13.
 - Hence, total number of subnetworks possible = $2^{13} = 8192$
- The first address in each subnet (i.e. host ID with all 0s) is the subnetwork address.
- The last address in each subnet (i.e. host ID with all 1s) is reserved for limited broadcast.

Subnet Mask : 255.255.254.0 11111111 11111111 11100000 00000000

Here, No. of 0 is 13.

c) Range of address in each subnet

- Method 1:
 - Find the first address in the block.
 - Add the no. of addresses in each subnet to get last address.
 - Add 1 to this address to find first address of the next block.
 - Repeat the process to calculate each subnet range.
- Method 2:
 - Calculate 2^n where n is the number of 0s.
 - Start last address in the last subnet.
 - Apply mask to obtain first address in this subnet.
 - Subtract 1 from this to obtain the last address of the subnet before the last.
- The numbers of addresses in each subnet is $2^{(\text{number of 0s})}$.

Example:

IP address: 190.100.0.0

Divide this address into 64 customer each needing 256 addresses

- Customer need 256 address.
 - $2^n=256 \rightarrow$ hence the suffix length is 8.
 - Hence the prefix length is $32-8=24$
- Hence, 1st customer \rightarrow 192.100.0.0/24 to 192.100.0.255/24
2nd customer \rightarrow 192.100.1.0/24 to 192.100.1.255/24
3rd customer \rightarrow 192.100.2.0/24 to 192.100.2.255/24
.....
64th customer \rightarrow 192.100.63.0/24 to 192.100.63.255/24
- Total number of IP assigned = 64 customers * 256 addresses = 16,384

Example:

IP address: 190.100.64.0

Divide this address into 128 customer each needing 128 addresses

- Customer need 128 address.
 - $2^n=128 \rightarrow$ hence the suffix length is 7.
 - Hence the prefix length is $32-7=25$
- Hence, 1st customer → 192.100.64.0/25 to 192.100.64.127/25
2nd customer → 192.100.64.128/25 to 192.100.64.255/25
3rd customer → 192.100.65.0/25 to 192.100.65.127/25
.....
128th customer → 192.100.127.128/25 to 192.100.127.255/25
- Total number of IP assigned = 128 customers * 128 addresses = 16,384

Q. A network has subnet mask of 255.255.240.0
What is the max number of hosts it can handle?

❖ Here,

255.255.240.0 → 11111111 11111111 11110000 00000000
→ 20 bit 1s, 12 bit 0s

So, Host bits = 12

So, number of hosts = $2^{12} = 4096$

Classes of IP Addresses

1. Class A (0-127):

- The first 8 bits identify the network, and the last 24 bits identify the host.
- If the first bit of an IP address is 0, the default mask is 8 bits long (prefix 8).

2. Class B (128-191):

- 16 bits identify the network, and 16 bits identify the host.
- If the first 2 bits of an IP address are 1 0, the default mask is 16 bits long (prefix 16).

3. Class C (192-223):

- The first 24 bits identify the network, and the last 8 bits identify the host.
- If the first 3 bits of an IP address are 1 1 0, the default mask is 24 bits long (prefix 24).

4. Class D(224-239):

- This is a multicast address that address group of computers all at one time.
- The default mask is 32 bits long (prefix 32).

5. Class E(240 onwards):

- Reserved for future use

A. Take an address 10.104.0.19

- Here, 1st bit of this address is 0 (since 10= 00001010).
- So this is Class A network address with 8Network bit and 24 host bit
- It is interpreted as host 104.0.19 on network 10.

B. The 2nd address is 172.16.12.1

- Here, two higher order bits are 1 0 (since 172=10101100).
- So this is Class B network address with 16Network bit and 16 host bit
- It is interpreted as host 12.1 on network 172.16

C. The 3rd address is 192.168.16.1

- Here, 3 higher order bits are 1 1 0 (since 192=11000000).
- So this is Class C network address with 32Network bit and 8 host bit
- It is interpreted as host 1 on network 192.168.16

7.5 Address Resolution

- The physical networks underlying the TCP/IP network do not understand IP addressing.
 - Physical networks have their own addressing schemes, and there are as many different addressing schemes as there are different types of physical networks.
- One task of the network access protocols is to map IP addresses to physical network addresses.
 - The most common example of this Network Access Layer function is the translation of IP addresses to Ethernet addresses.
 - The protocol that performs this function is Address Resolution Protocol (ARP)

- The ARP software maintains a table of translations between IP addresses and Ethernet addresses.
 - This table is built dynamically.
- When ARP receives a request to translate an IP address, it checks for the address in its table.
 - If the address is found, it returns the Ethernet address to the requesting software.
 - If the address is not found, ARP broadcasts a packet to every host on the Ethernet.
- The packet contains the IP address for which an Ethernet address is sought.
 - If a receiving host identifies the IP address as its own, it responds by sending its Ethernet address back to the requesting host. The response is then cached in the ARP table.

7.6 Ports and Sockets

- As the data moves up or down the TCP/IP layers, a mechanism is needed to deliver it to the correct protocols in each layer.
- Data arriving from the network must be de-multiplexed: divided for delivery to multiple processes. To accomplish this task, IP uses **protocol numbers** to identify transport protocols, and the transport protocols use **port numbers** to identify applications.

Ports

- After IP passes incoming data to the transport protocol, the transport protocol passes the data to the correct application process.
 - Application processes (also called network services) are identified by port numbers, which are 16-bit values.
- The source port number identifies the process that sent the data and the destination port number identifies the process that will receive the data.
 - Both of these are contained in the first header word of each TCP segment and UDP packet.
- Each data packet comes with a port number associated with it.
 - This enables the protocols to decide that what are the requirements of the data packets and to which port are they supposed to be directed.
 - The existence of ports is crucial to make sure that data packets reach their desired destinations accurately.

Some commonly used ports

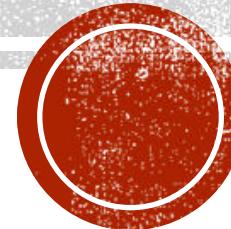
Service Name	Full Form	Port Number
SMTP	Simple Mail Transfer Protocol	25
HTTP	HyperText Transfer Protocol	80
HTTPS	HyperText Transfer Protocol (Secure)	443
FTP	File Transfer Protocol	20,21
Telnet	Telnet (Remote Connection Terminal)	23
DNS	Domain Name System	53

Sockets

- The combination of an IP address and a port number is called a socket.
- A socket uniquely identifies a single network process within the entire Internet.
- A pair of sockets, one socket for the receiving host and one for the sending host, define the connection for connection-oriented protocols such as TCP.
- Socket = IP + Port No. Added to IP
 - E.g. The socket for the source side = 172.16.12.2.3382
(IP address 172.16.12.2 plus port number 3382)

CHAPTER 8

SECURE COMMUNICATION



4 Hours

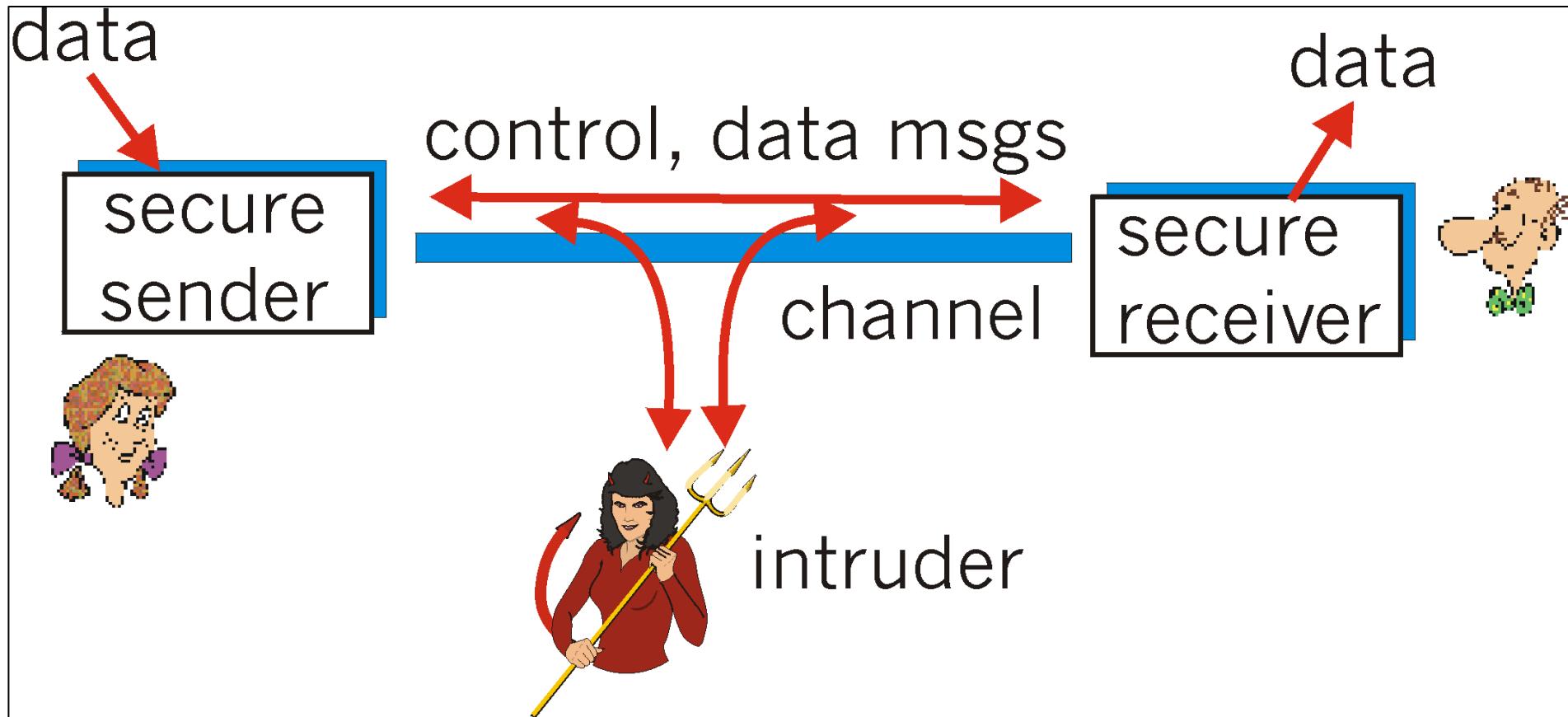
~7-8 marks

CHAPTER OUTLINE

- Definition & Parameters of secure communication
- Cryptography (Substitution and Transposition cipher)
- Firewall
- Concept of Digital Signature

SECURE COMMUNICATION

- Secure communication is the scenario where transmission of messages take place without interference of any third party who want to listen or use the message for destructive purpose.
- When two entities are communicating and they do not want any kind of interception with the message, they need to implement some technique for protection of information.
- In real world, no communication can be guaranteed 100% secure, because technologies and their compromise are being developed gradually.



SECURE COMMUNICATION PARAMETERS

Secure communication must have 3 important properties:

1. Confidentiality (Secrecy)

- Information must not be disclosed to unauthorized individuals, entities and process.
- Only the sender and receiver should understand the message content.

2. Integrity (Message Integrity)

- Receiver should be able to check if the message has been altered or not.
- It ensures the accuracy and completeness of information and processing methods.

3. Availability

- Receiver should be able to access services provided by the sender.
- Authorized users should have access to information and associated assets when required.

SECURE COMMUNICATION PARAMETERS

Other properties:

4. Authentication

- Are the communicating entities verified?
- Is the source or destination trusted?

5. Accountability

- Authorization of concerned parties
- Who has the access to which file and what he/she can do with it

6. Non-Repudiation

- One party cannot deny receiving a message. Likewise, one party cannot deny that the message has been sent on their behalf.

8.1 CRYPTOGRAPHY CONCEPTS

WHAT IS CRYPTOGRAPHY

- Cryptography comes from kryptos which means “secret” or “hidden”.
- Cryptography is the study of various ways to disguise messages in order to avoid the interception from an unauthorized interceptor.
- It is the art of hiding information so that message is unreadable when a 3rd party is able to intercept the transmission of message.
- It is a complex field which requires knowledge of mathematics, electronics, and engineering.

TERMINOLOGIES IN CRYPTOGRAPHY

1. Plaintext

- The original text message produced by the sender

2. Ciphertext

- Plaintext transformed into unintelligible (cannot be understood readily) string of characters.

3. Encryption

- The process/program that converts a plaintext into a ciphertext
- Also known as enciphering or encoding.

4. Decryption

- The process/program that converts a ciphertext into a plaintext.
- Also known as deciphering or decoding.
- Reverse process to encryption.

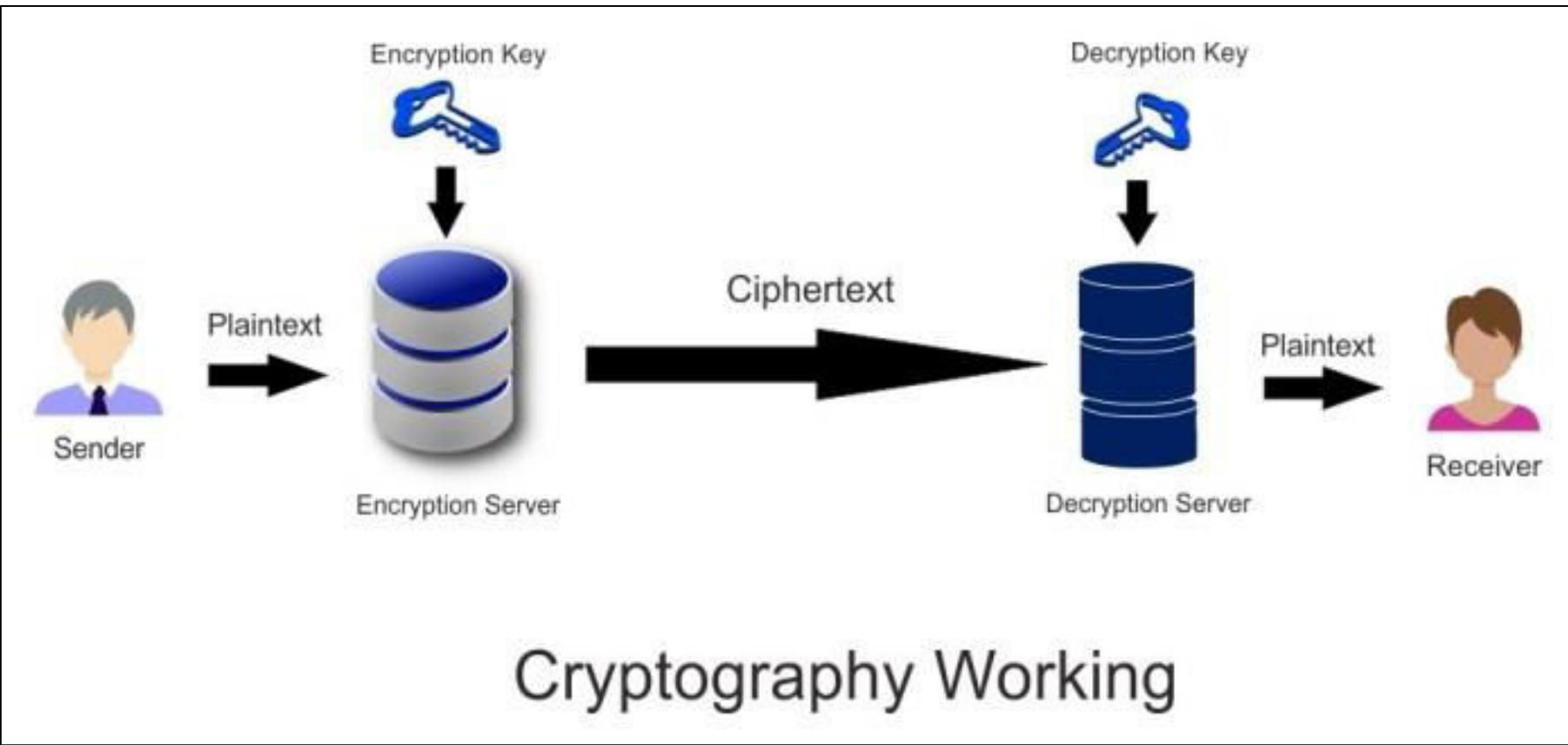
TERMINOLOGIES IN CRYPTOGRAPHY

5. Key

- A value or number that is used for encryption or decryption process.
- Keys are generally assumed to be known to the sender and receiver only.
- Without the knowledge of key, the interceptor cannot really know what the actual message is.

6. Cipher

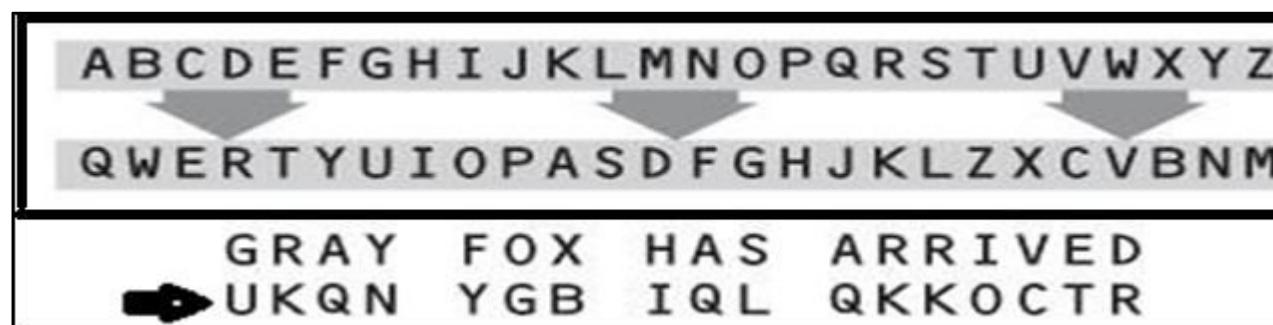
- The encryption and decryption algorithms together are referred to as ciphers.
- This term is also used to refer to different categories of algorithms in cryptography.



BASIC CRYPTOGRAPHY TECHNIQUES

SUBSTITUTION CIPHER

- Here, one letter of plaintext is substituted by another letter to form a ciphertext.
- Since the general components of plaintext are alphanumeric values, each of these plaintext values can be replaced with another alphanumeric value.
 - This means, each alphabet in plaintext is replaced by another alphabet.
 - This means, each digit in plaintext is replaced by another digit.
- Based on the number of transformation, substitution cipher can be of 2 types
 - a) Mono-alphabetic → one single alphabet replaces one plaintext alphabet
 - b) Poly-alphabetic → more than one alphabets replace one plaintext alphabet



MONO-ALPHABETIC SUBSTITUTION CIPHER

- Here, a character in the plaintext is always substituted by a single character in the ciphertext.
- The conversion is always same, regardless of the position of alphabet in the text.
 - E.g. If A → F, then all the A's in "Hari ate Ramen" will be replaced by F to form ciphertext.
- In mono-alphabetic substitution cipher, key denotes a number. Through this number, we shift certain positions in alphabet list to acquire the required ciphertext.
- In an old method of substitution cipher, also called the Caesar cipher, the key was set to be 3.
 - This means, alphabets and digits were shifted down by 3.

MONO-ALPHABETIC SUBSTITUTION CIPHER

- For encryption process, each alphabet in plaintext is substituted by the alphabet that is k^{th} position ahead from current alphabet.
 - For decryption process, each alphabet in ciphertext is substituted by the alphabet that is k^{th} position behind from current alphabet.
- E.g. if $k=3$ (shift by 3 positions)

A → D

B → E

C → F

and so on.

So, “Gold is on the truck” text with $k=3$ becomes

Jrog lv rq wkh wuxfn

MONO-ALPHABETIC SUBSTITUTION CIPHER

- For decryption of the same question, we shift the ciphertext by 3 positions backward.
- E.g. if $k=3$ (shift by 3 positions)

D → A

E → B

F → C

and so on.

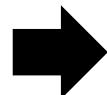
- If current alphabet list finishes, a new set of alphabet list can be used.
 - E.g. if U→Y, V→Z, then W→A, X→B and so on
 - The main basis is that each alphabet must be mapped into another unique alphabet for substitution
- While the use key value is the most popular form of implementation, sometimes substitutions are also made at random for creating more confusion for the interceptor.
 - E.g. A→G, B→X, C→I , D→M, E→A

EXAMPLE

1. using K=3, convert the text “My Time Has Come”

Answer: → PB WLPH FRPH

2. using following substitution table, convert the text “odd semester starts next year”



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	I	K	B	P	H	Y	C	U	R	E	A	W	Q	X	Z	F	O	L	N	V	S	D	J	G	M

Answer: → XBB LPWPLNPO LNTONL QPJN GPTO

Pros:

- Easy to implement
- Quick computation

Cons:

- Repetitive occurrence of letter
- Space between two words is preserved in ciphertext

POLY-ALPHABETIC SUBSTITUTION CIPHER

- Here, each alphabet can be replaced by a group of characters
- Each plaintext character has one-to-many relationship with the ciphertext character.

POLY-ALPHABETIC CIPHER

For encryption

Find the first plaintext letter down the far left column, and encrypt this letter to the ciphertext letter in the first column.

You would then move to the next column, and so on.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
B	E	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
C	G	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
D	H	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
E	F	E	F	G	H		J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
F	F	G	H	I		K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
G	G	H		J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
H	H		J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
I		K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
L	L	M	N	O	F	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Plaintext: **johannes trithemius**

Ciphertext: **jpjdrsksz asetraxkj**

Pros:

- Relatively secure than mono alphabetic
- More efficient
- Grammar analysis is not possible

Cons:

- Complex implementation
- Computation takes time

TRANSPOSITION CIPHER

- A transposition is an encryption in which the letters of the message are rearranged .

- Encryption Mechanism:
 - a) Arrange the letters of plaintext in form of rows.
 - The length of rows is generally taken as 5 or as per length of a pre-determined keyword.
 - b) Add a bit of padding(random characters) to make the rows and columns a perfect square.
 - c) Now take the individual columns vertically to create the cipher text.

- Decryption mechanism:
 - a. Rearrange the letters into columns.
 - b. Read the text row-wise.

m	e	e	t	m
e	a	t	t	h
e	f	o	u	n
t	a	i	n	a
t	n	i	n	e

Plaintext: **meet me at the fountain at nine**

ciphertext: **meett eafan etoii ttunn mhnae**

a	t	m	i	d
n	i	g	h	t
y	o	u	w	i
l	l	f	i	n
d	m	e	i	n
t	h	e	p	a
r	k	x	x	x

ciphertext: **anyldtr tiolmhk mgufeex ihwiipx dtinnax**

Plaintext: **at midnight you will find me in the park**

REFINEMENT IN TRANSPOSITION CIPHER

- A certain keyword or numerical value can be assigned to determine number of columns required during transposition.
- These keywords or numbers can also be used to rearrange the order of columns for encryption or decryption, thus acting as key.



Keyword

T	O	M	A	T	O
5	3	2	1	6	4

THE TOMATO IS A
PLANT IN THE NIGHTSHADE
FAMILY

TINESAX EOAHTFX
HTLTHEY MAIIAIX TAPNGDL
OSTNHNMX

Pros

- Good use of permutation makes it harder to analyze
- Can be applied over same plaintext multiple times to produce more complex ciphertext.

Cons

- ❖ More laborious and error prone than other ciphers.
- ❖ Prone to frequency analysis.

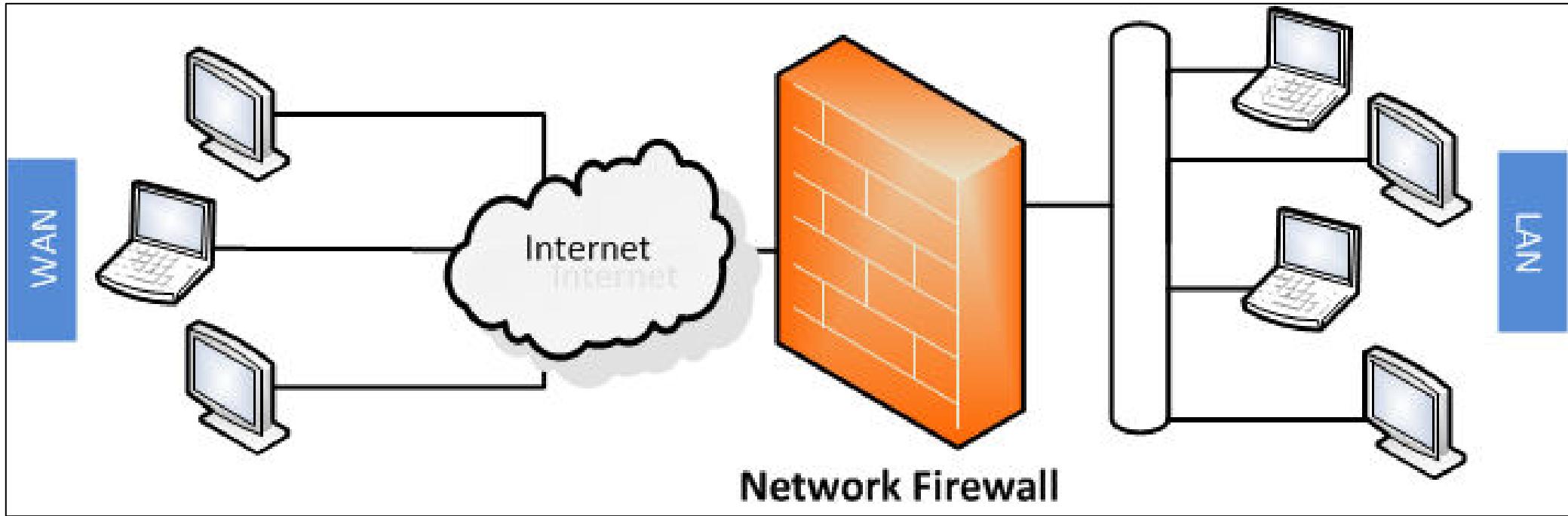
CLASSIFICATION OF CRYPTOGRAPHY TECHNIQUES

- Based on the type of key used, cryptography ciphers can be classified into 2 categories:
 - a) Symmetric cryptography
 - Same key/key value is used for encryption and decryption
 - E.g. traditional substitution cipher, DES
 - b) Asymmetric cryptography
 - different key/key value is used for encryption and decryption
 - E.g. RSA, Digital Signature

8.2 FIREWALL

WHAT IS FIREWALL?

- A firewall is a system (or group of systems) that enforces a security policy between a secure internal network and an untrusted network such as the internet.
- Firewalls tend to be seen as a protection between the internet and a private network
 - But in general speaking, firewall is considered to be a means to divide the world into two or more networks: one being secure, one being non-secure network.
- A firewall can be a PC, a router, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information or services from the outside.
- A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.



WHAT DOES FIREWALL CONTROL?

- **Service control**
 - Filtering traffic according to IP address
 - Interpreting service requests on proxy servers
- **Direction control**
 - Determining direction in which a particular service request can be initiated or allowed to flow.
- **User control**
 - Controlling outside access to a service through authentication mechanism
 - Creating access control list for service access requests made inside a private network
- **Behavioral control**
 - Controls how a particular service is used (e.g. spam email filters, filtering messages to servers)

COMPONENTS OF FIREWALL

- A firewall typically consists of one or more of the following:

- a) Packet filtering router
- b) Application level gateway
- c) Circuit level gateway

In order to build an effective firewall, these components are used together.

- ❖ Packet filtering router is responsible for forwarding packets according to the established rules. It makes decision for allowing or discarding the packets.
- ❖ Application level gateway (proxy) provides higher-level control on the traffic between two networks. For a client, proxy acts as a server and vice-versa.
- ❖ Circuit level gateway handles datagram packets on the basis of TCP/IP protocols. It is used to observe and filter out the outbound connections.

CATEGORY OF FIREWALL

- A firewall can be categorized on the basis of
 - a) Functionality: Packet filtering, Application Filtering, circuit filtering
 - b) Application scope: Network based or Host based
- ❖ Packet filtering firewall provides allowance or discarding of packets based on their source or destination addresses. These are easy to set up, but have limited capabilities.
- ❖ Application filtering firewall filters screen traffic involving specific applications or services. It is good system for sophisticated evaluation and authentication measure. But it is generally unaware of modern applications, hence not 100% effective.
- ❖ Circuit level firewall filters packets without source and destination address, observes the intermediate circuit for routing.

CATEGORY OF FIREWALL

- ❖ Network based firewall filters traffic between two or more network. It generally runs on network hardware.
- ❖ Host based firewall controls network traffic in and out of host machines. It generally runs on the host computers.

DIGITAL SIGNATURE

WHAT IS DIGITAL SIGNATURE

- A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

- A digital signature is a data structure that provides the proof of an origin, i.e. Authentication, integrity, and Non-repudiation

Authentication → only certain people can open/access it.

Integrity → message accuracy and consistency is assured.

Non-repudiation → sender cannot deny the fact of origin of message

- A digital signature is a form of standard electronic signature that takes the concept of traditional paper-based signing and turns it into an electronic “fingerprint”
 - This fingerprint, or coded message, is unique to both the document and the signer.

WHAT DOES DIGITAL SIGNATURE REPRESENT?

Digital signature must have following properties:

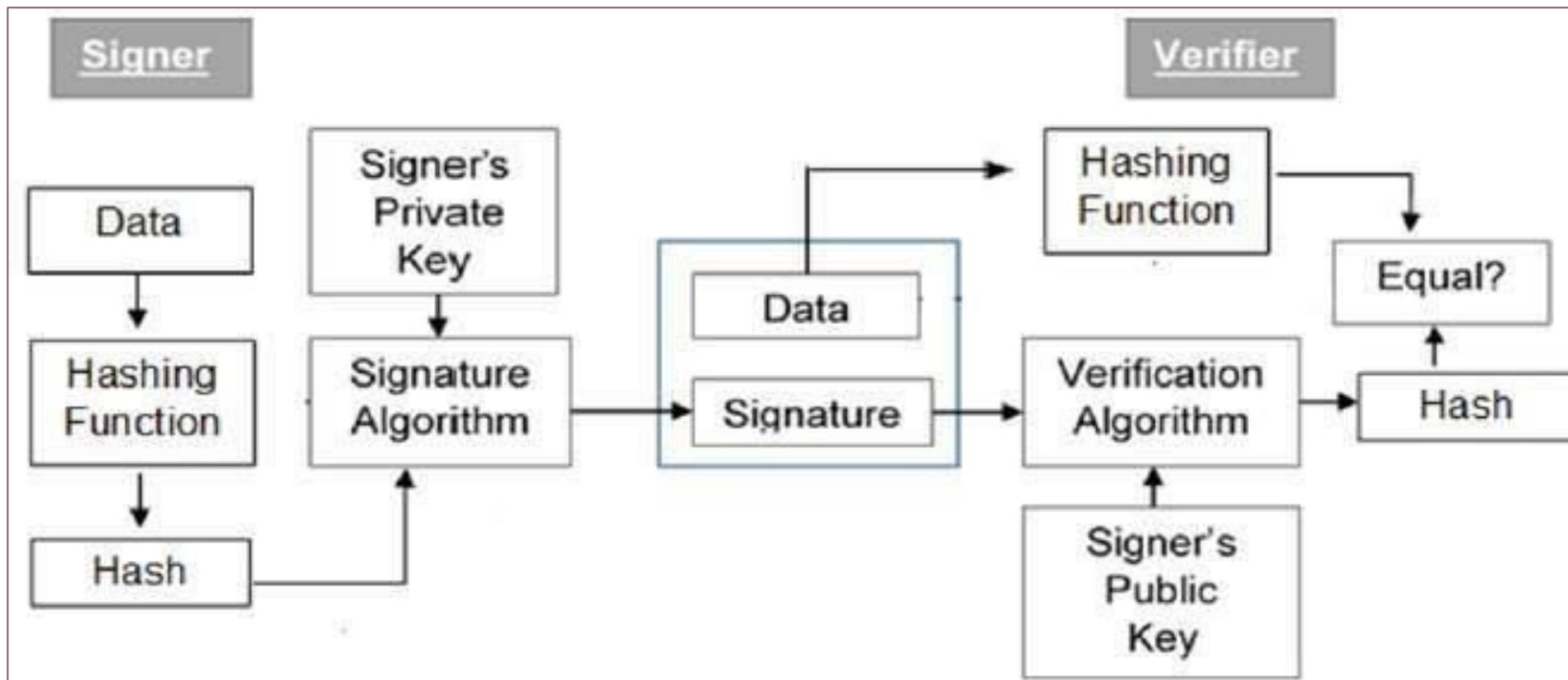
1. It must verify the author and the date time of the signature
2. It must authenticate the contents at the time of the signature
3. It must be verifiable by third parties, to resolve disputes.

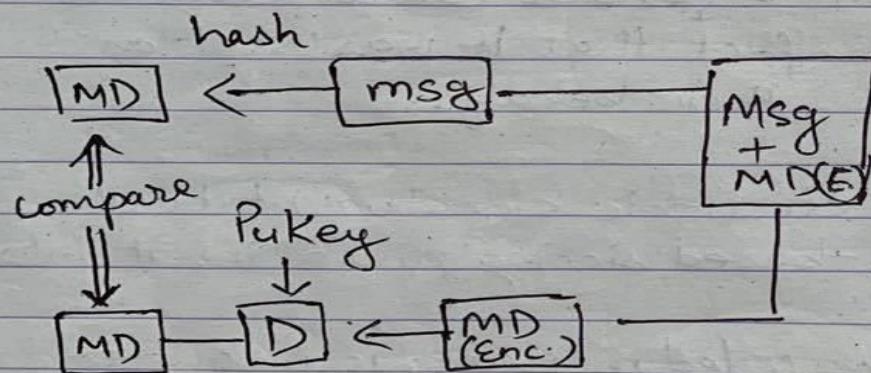
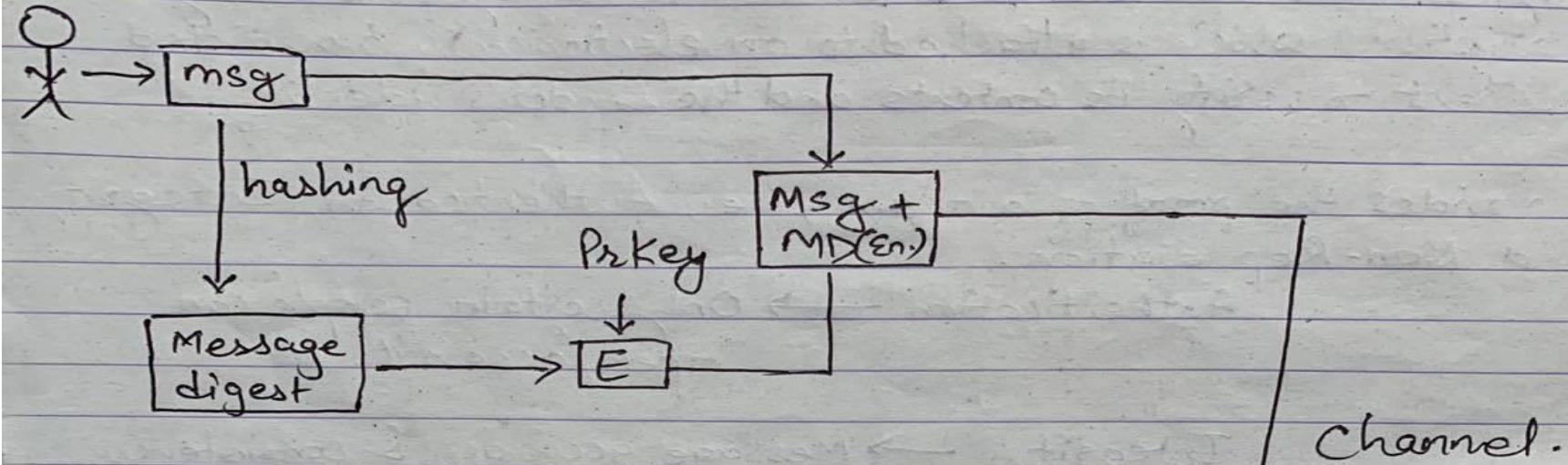
As a medium of secure communication, digital signature represents following elements:

- a) Confidentiality
- b) Integrity
- c) Authentication
- d) Non-repudiation

SECURE COMMUNICATION USING DIGITAL SIGNATURE

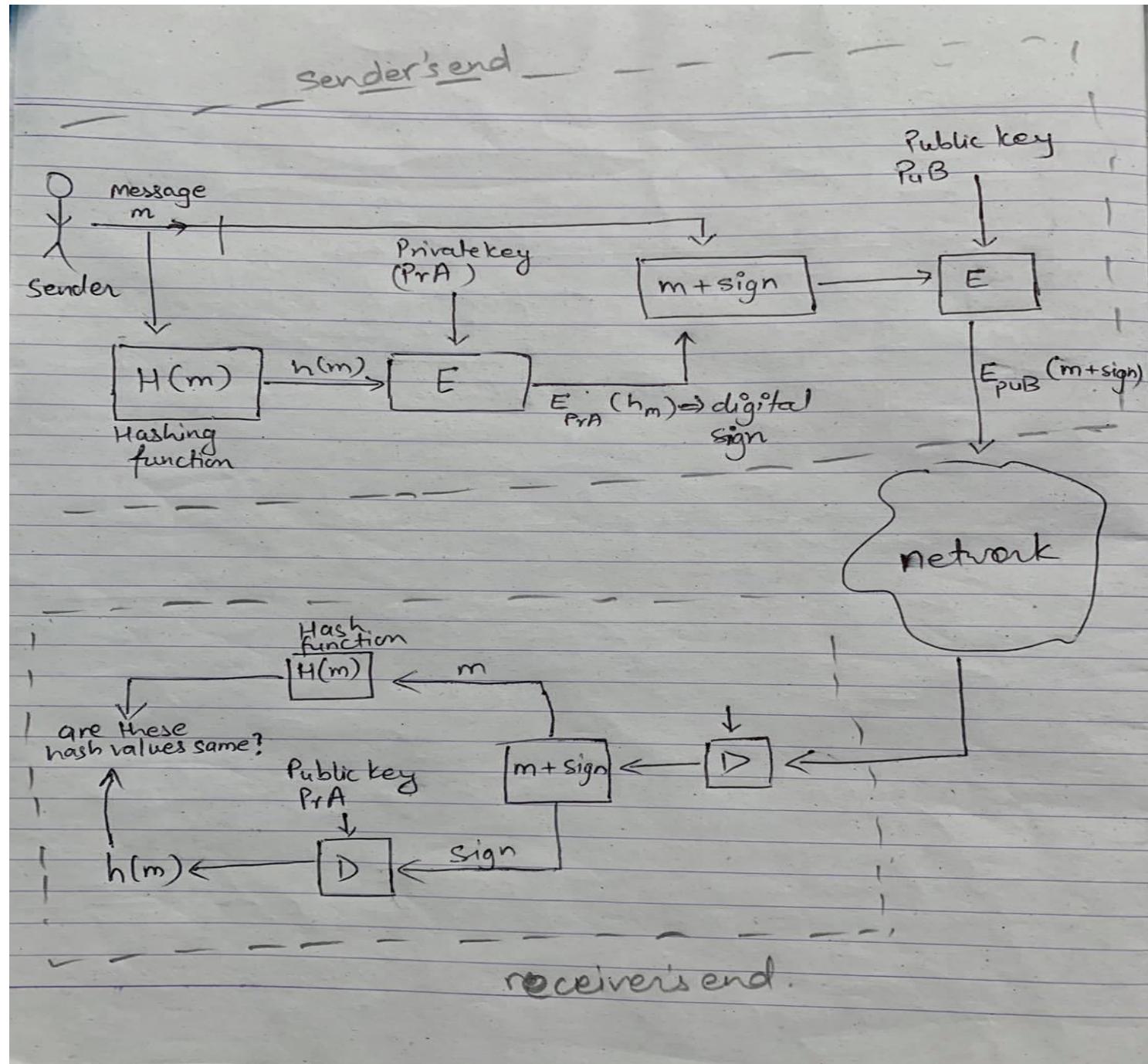
1. A (sender) has a message “M” to pass
2. A uses hash function to generate hash $h(M)$ of the message
3. A encrypts this hash value using his/her private key. This encrypted content $E_{prA}[h(M)]$ is now the digital signature for the sender.
4. A sends both the real message and the digital signature through the communication channel.
5. B (receiver) receives a combination of message M^* and an encrypted hash value.
6. B uses hash function to generate hash of the received message... i.e. $h(M^*)$
7. B decrypts the received encrypted hash value using the public key of A. The resulting value is the hash value of the original message M
8. B compares the hash value of $h(M)$ and $h(M^*)$. If both values are same, then message is unaltered, and is indeed sent by A.
 - ❖ If the hash values differ, either A didn't send it, or the message has been altered during the transmission.





MODIFICATION OF DIGITAL SIGNATURE

1. A (sender) has a message “M” to pass
2. A uses hash function to generate hash $h(M)$ of the message
3. A encrypts this hash value using his/her private key. This encrypted content $E_{prA}[h(M)]$ is now the digital signature for the sender.
4. A encrypts the combination of message and the digital signature with the receiver's public key or a shared key.
5. A sends the encrypted package through the communication channel.
6. B (receiver) receives the encrypted package through communication channel
7. B decrypts the package using his/her private key, or using shared key.
8. B obtains a combination of message M^* and an encrypted hash value.
9. B uses hash function to generate hash of the received message... i.e. $h(M^*)$
10. B decrypts the received encrypted hash value using the public key of A. The resulting value is the hash value of the original message M
11. B compares the hash value of $h(M)$ and $h(M^*)$. If both values are same, then message is unaltered, and is indeed sent by A.
 - ❖ If the hash values differ, either A didn't send it, or the message has been altered during the transmission.



END OF CHAPTER 8

IMPORTANT QUESTIONS

- Describe in brief the elements of secure communication
- Definition and terminology of cryptography
- Substitution cipher (numerical or example)
- Transposition cipher (numerical or example)
- Firewall functionality and types
- What element of secure communication does Digital signature ensure?
- Explain the mechanism of secure communication using digital signature.