CMR INSTITUTE OF TECHNOLOGY

USN

Internal Assessment Test I – March 2023

Sub:	**Computer Networks**							**Sub Code:**	**22MCA14**
Date:	**14/03/2023**	**Duration:**	**90 min's**	**Max Marks:**	**50**	**Sem:**	**I**	**Branch:**	**MCA**

Note : Answer FIVE FULL Questions, choosing ONE full question from each Module

	PART I	MARKS	OBE	
			CO	RBT
1	a) What is data communication? Explain with neat sketch three types of communications between the devices considering data flow. b) Explain the fundamental characteristics and components of a data communication system. **OR**	[5] [5]	CO1	L1
2	a) Define protocol. List and explain key elements of a protocol. b) What are the different types/categories of the networks? Explain in detail. And differentiate them.	[4] [6]	CO1	L2
3	**PART II** a) What is network topology? Explain the different network topologies with advantages and disadvantages. **OR**	[10]	CO1	L2
4	a) Analyze the principle behind protocol layering. Explain OSI reference model with neat diagram	[10]	CO1	L3
5	**PART III** a) List and explain different addresses in TCP/IP. b) List out functionalities of physical layer, data link layer and network layer **OR**	[5] [5]	CO1	L3
6	a) With a neat diagram explain the TCP/IP protocol suite mentioning the different layers and their functionalities in TCP/IP. Why is TCP/IP called a defacto standard.	[10]	CO1	L3
7	PART IV a) Explain Stop and Wait ARQ protocol with neat diagram. b) Explain the History of Internet **OR**	[5] [5]	CO4 CO1	L4
8	a) What is framing. b) Explain different types of framing. c) Explain bit and character stuffing with example.	[2] [4] [4]	CO4	L2
9	PARTV a) Explain Flow control and Error control. b) Explain Stop and Wait protocol with neat diagram. **OR**	[4] [6]	C04	L2
10	a) Assume five devices are connected in a mesh topology. How many duplex links are needed? How many ports are needed for each? b) Explain simplest protocol with neat diagram.	[4] [6]	CO4	L2

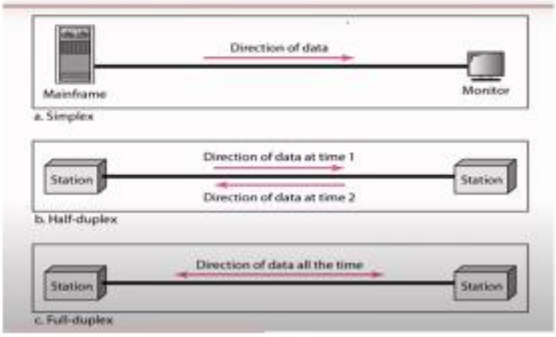
1-1 DATA COMMUNICATIONS

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

Data Flow [Transmission Mode]:

Communication between two devices can be

1. **Simplex**
2. **Half Duplex**
3. **Full Duplex**


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Direction of data at time 2
Station
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

Simplex

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive.

Half-Duplex

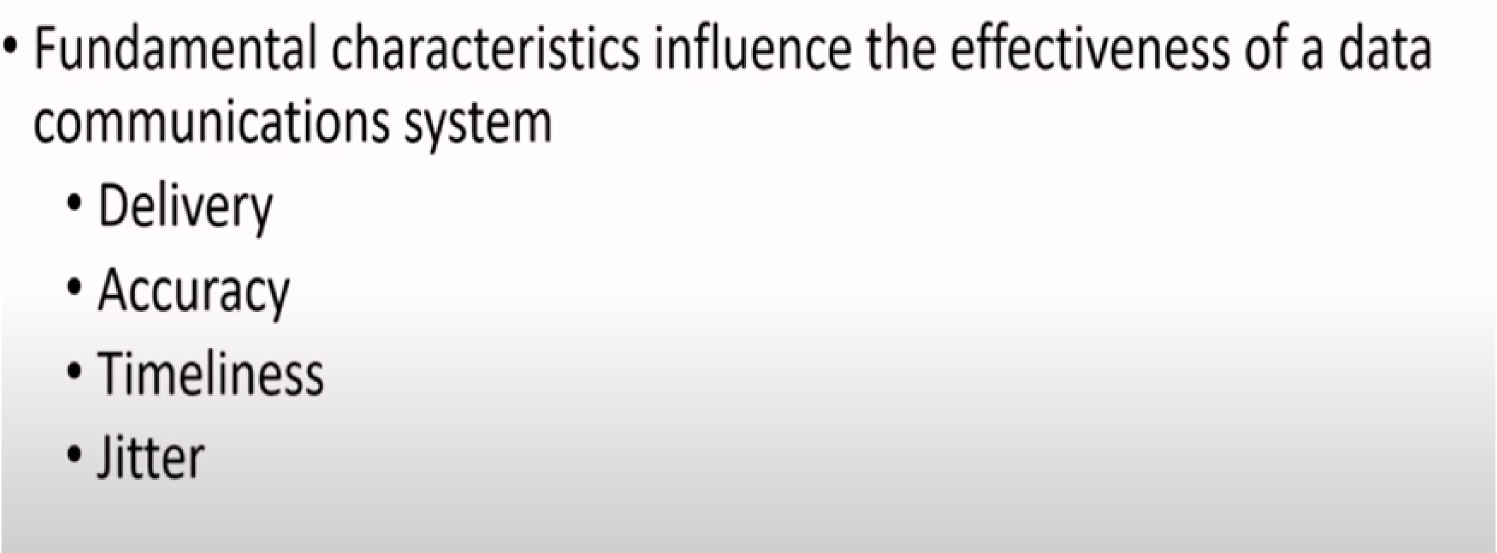
In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa.

Full-Duplex

In full-duplex mode (also called duplex), both stations can transmit and receive simultaneously

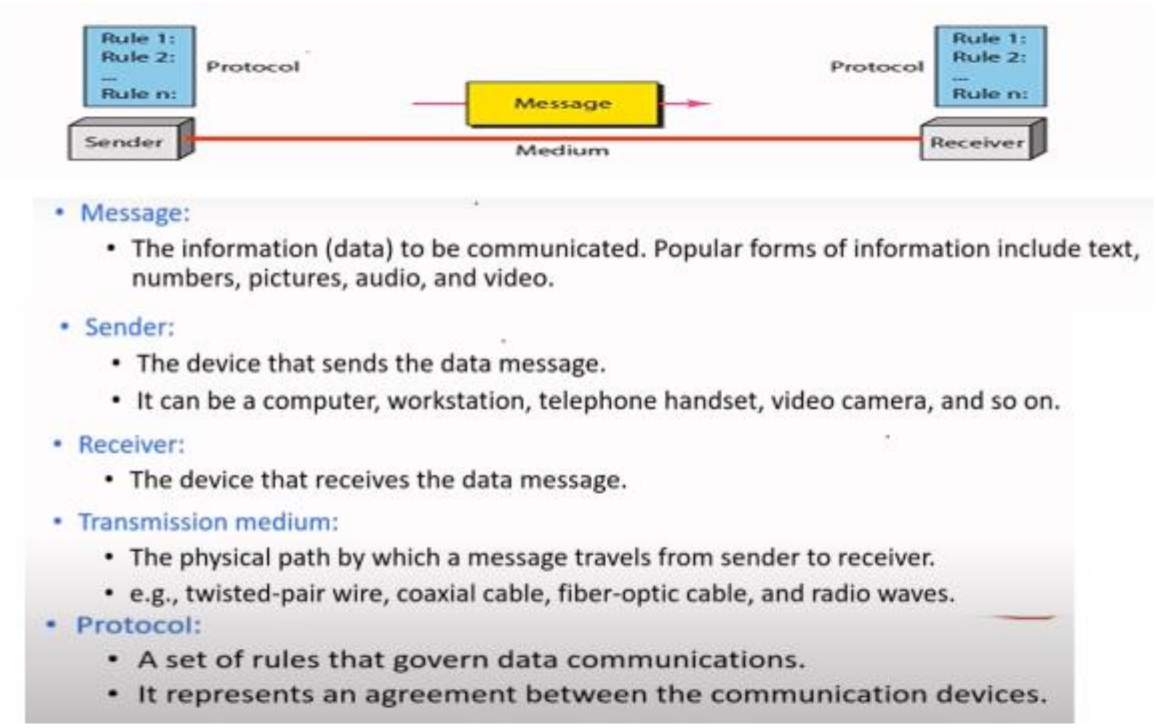
The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.



- Fundamental characteristics influence the effectiveness of a data communications system
  - Delivery
  - Accuracy
  - Timeliness
  - Jitter

Components of Data Communications:



- Message:
  - The information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- Sender:
  - The device that sends the data message.
  - It can be a computer, workstation, telephone handset, video camera, and so on.
- Receiver:
  - The device that receives the data message.
- Transmission medium:
  - The physical path by which a message travels from sender to receiver.
  - e.g., twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- Protocol:
  - A set of rules that govern data communications.
  - It represents an agreement between the communication devices.

2a)

<u>Protocol:</u>

- A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated.
- The key elements of a protocol are syntax, semantics, and timing.
- Syntax :
  - The term syntax refers to the structure or format of the data, meaning the order in which they are presented. How to read the bits.
    - Eg: a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

- Semantics:
    - semantics interprets the meaning of each section of bits.
    - what action is to be taken based on that interpretation.

For example, does an address identify the route to be taken or the final destination of the message?

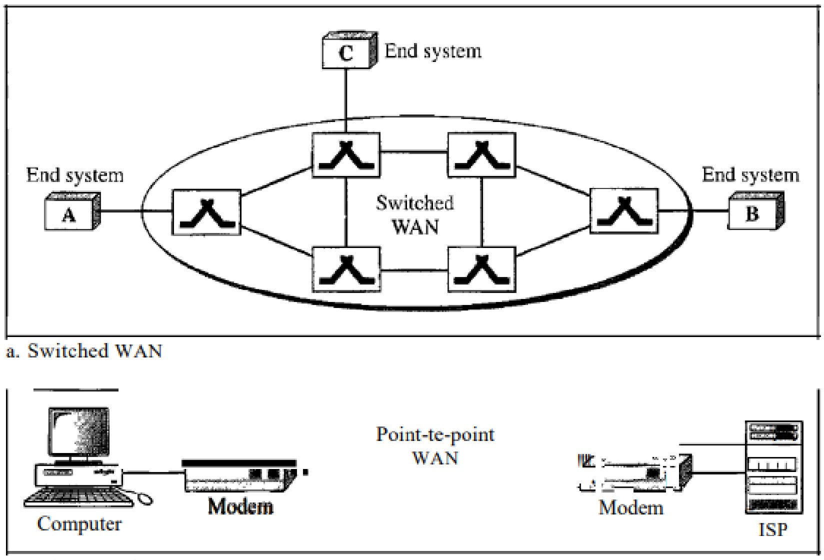
- Timing:
    - Timing refers to two characteristics: when data should be sent and how fast they can be sent.
    - For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

2b)

Categories of Networks :

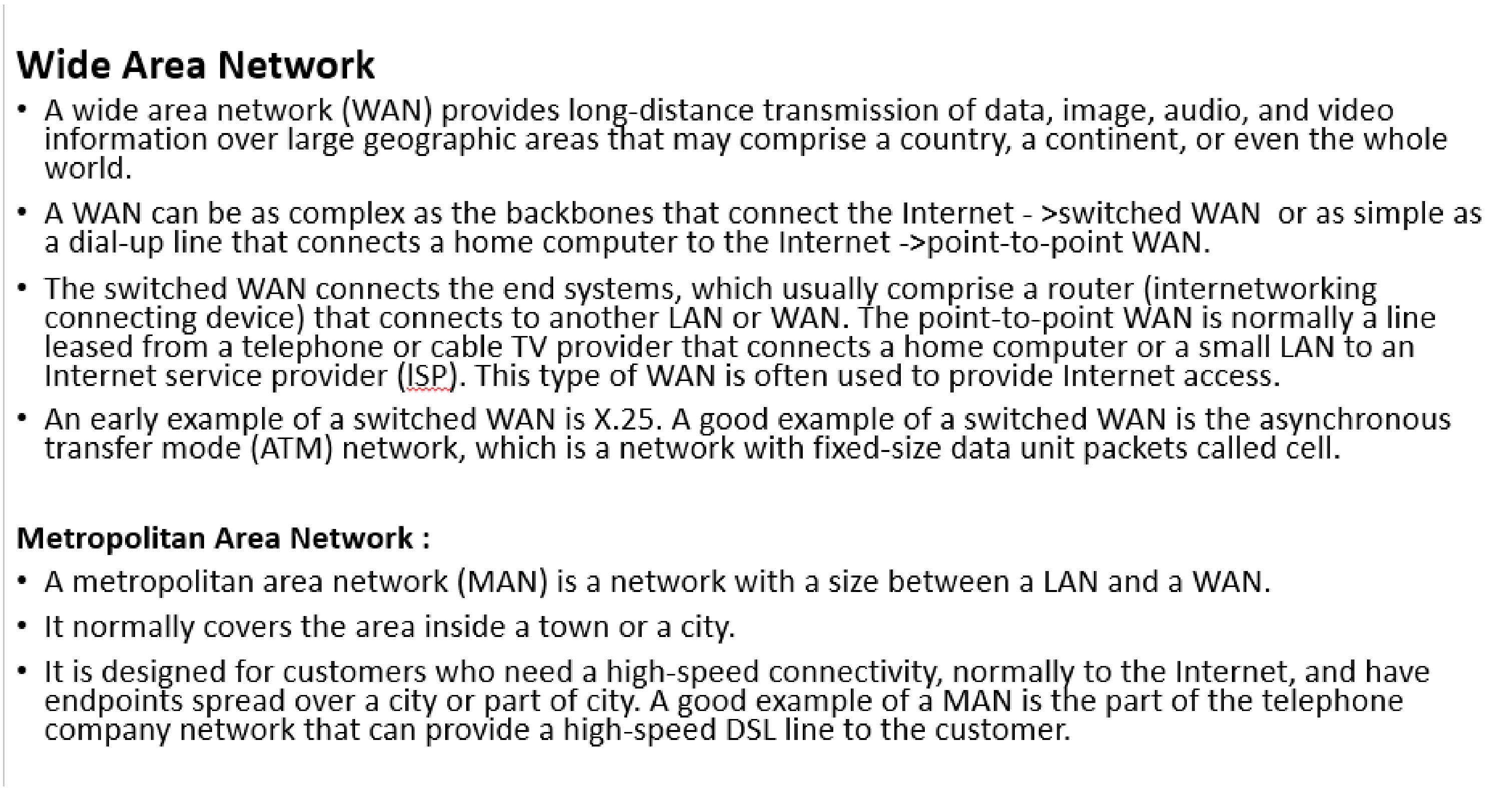
- The category into which a network falls is determined by its size.
    - A LAN normally covers an area less than 2 mi;
    - A WAN can be worldwide.
    - Networks of a size in between are normally referred to as **metropolitan area networks** and span tens of miles.
- **Local Area Network :**
    - A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.
    - Depending on the needs of an organization and the type of technology used, a LAN can be
        - as simple as two PCs and a printer in someone's home office; or
        - it can extend throughout a company and include audio and video peripherals.
    - Currently, LAN size is limited to a few kilometres.
    - LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data.
    - In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.

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



a. Switched WAN

b. Point-to-point WAN



Wide Area Network

- A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world.
- A WAN can be as complex as the backbones that connect the Internet - >switched WAN or as simple as a dial-up line that connects a home computer to the Internet ->point-to-point WAN.
- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (ISP). This type of WAN is often used to provide Internet access.
- An early example of a switched WAN is X.25. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cell.

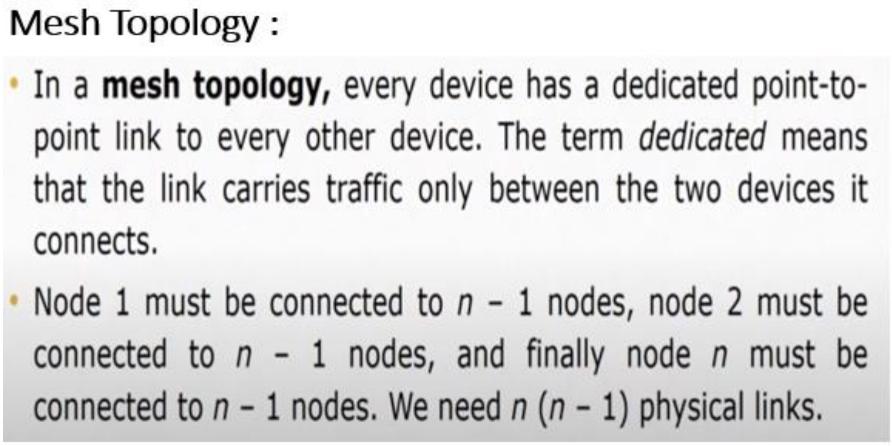
Metropolitan Area Network :

- A metropolitan area network (MAN) is a network with a size between a LAN and a WAN.
- It normally covers the area inside a town or a city.
- It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer.

3)

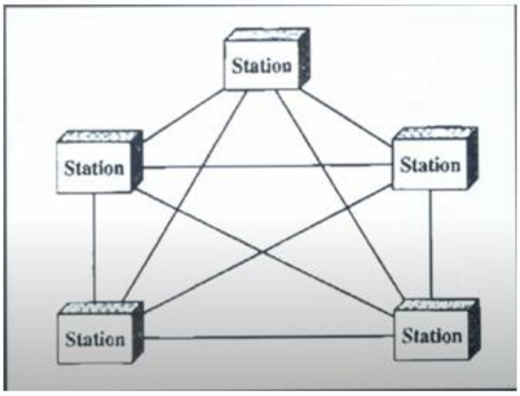
Physical Topology :

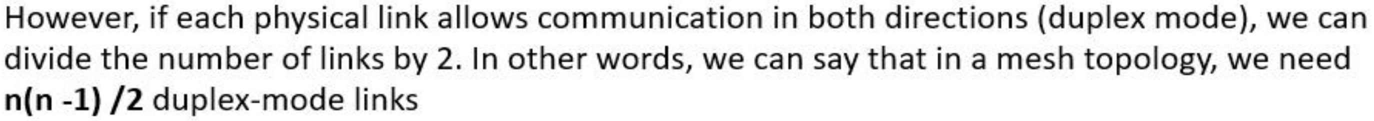
- The term physical topology refers to the way in which a network is laid out physically
- Two or more devices connect to a link, two or more links form a topology.
- The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are four basic topologies possible:
  - Mesh
  - Star
  - Bus
  - Ring



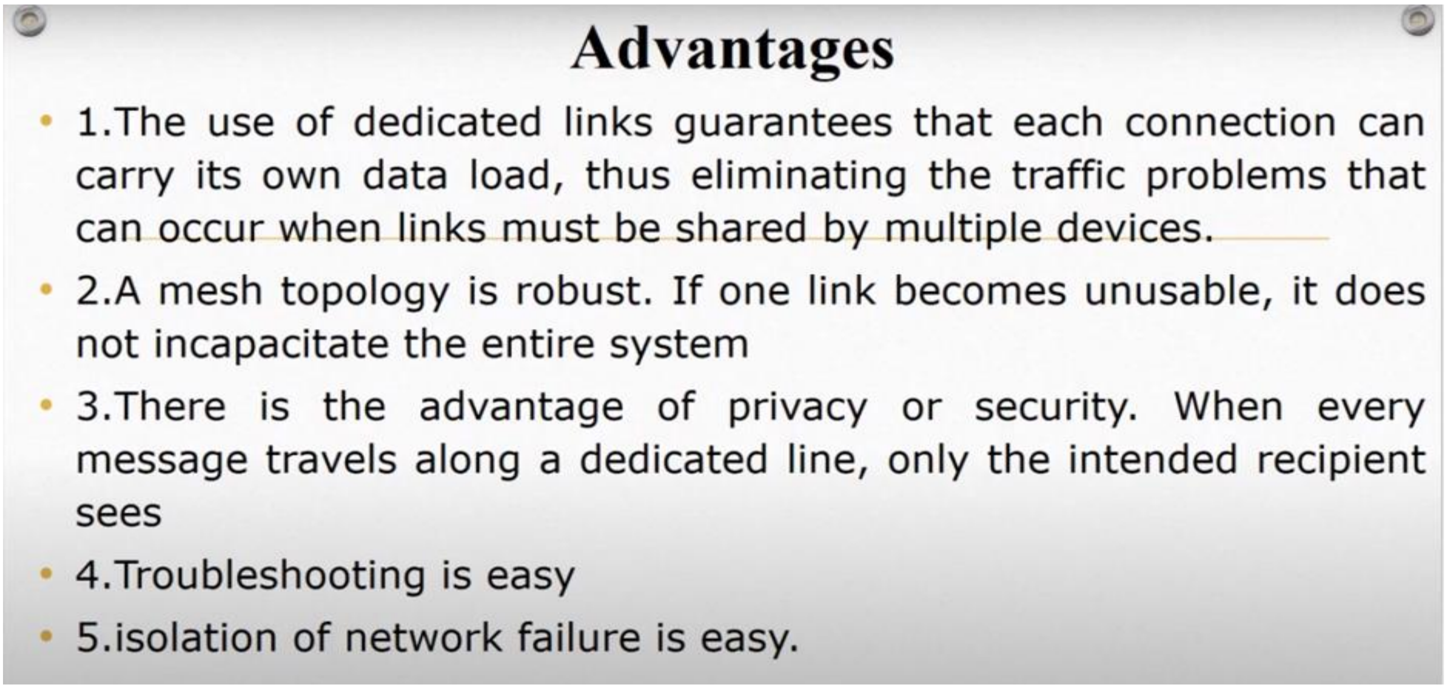
Mesh Topology :

- In a **mesh topology,** every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects.
- Node 1 must be connected to $n - 1$ nodes, node 2 must be connected to $n - 1$ nodes, and finally node n must be connected to $n - 1$ nodes. We need $n(n - 1)$ physical links.





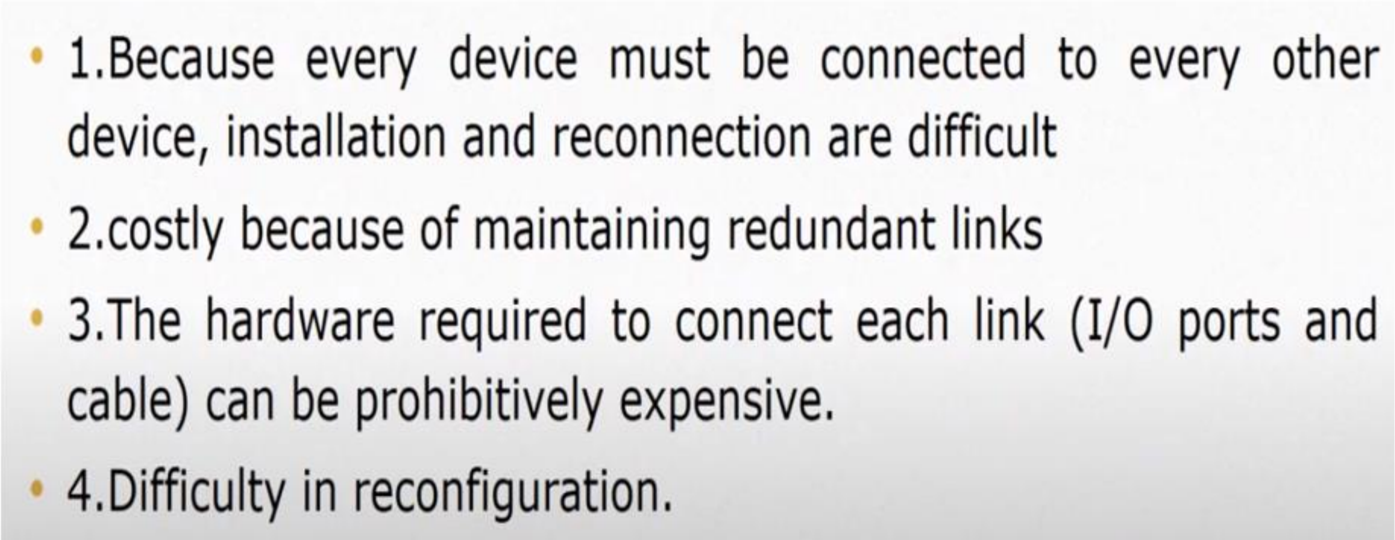
However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need **n(n -1) /2** duplex-mode links



Advantages

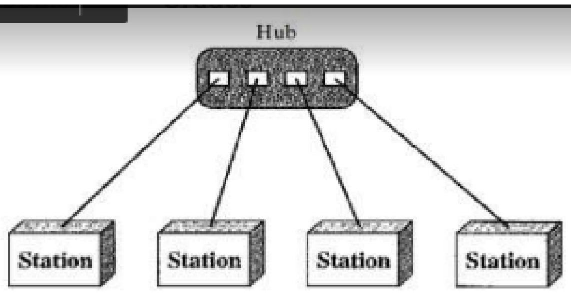
- 1.The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- 2.A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system
- 3.There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees
- 4.Troubleshooting is easy
- 5.isolation of network failure is easy.

Disadvantages:



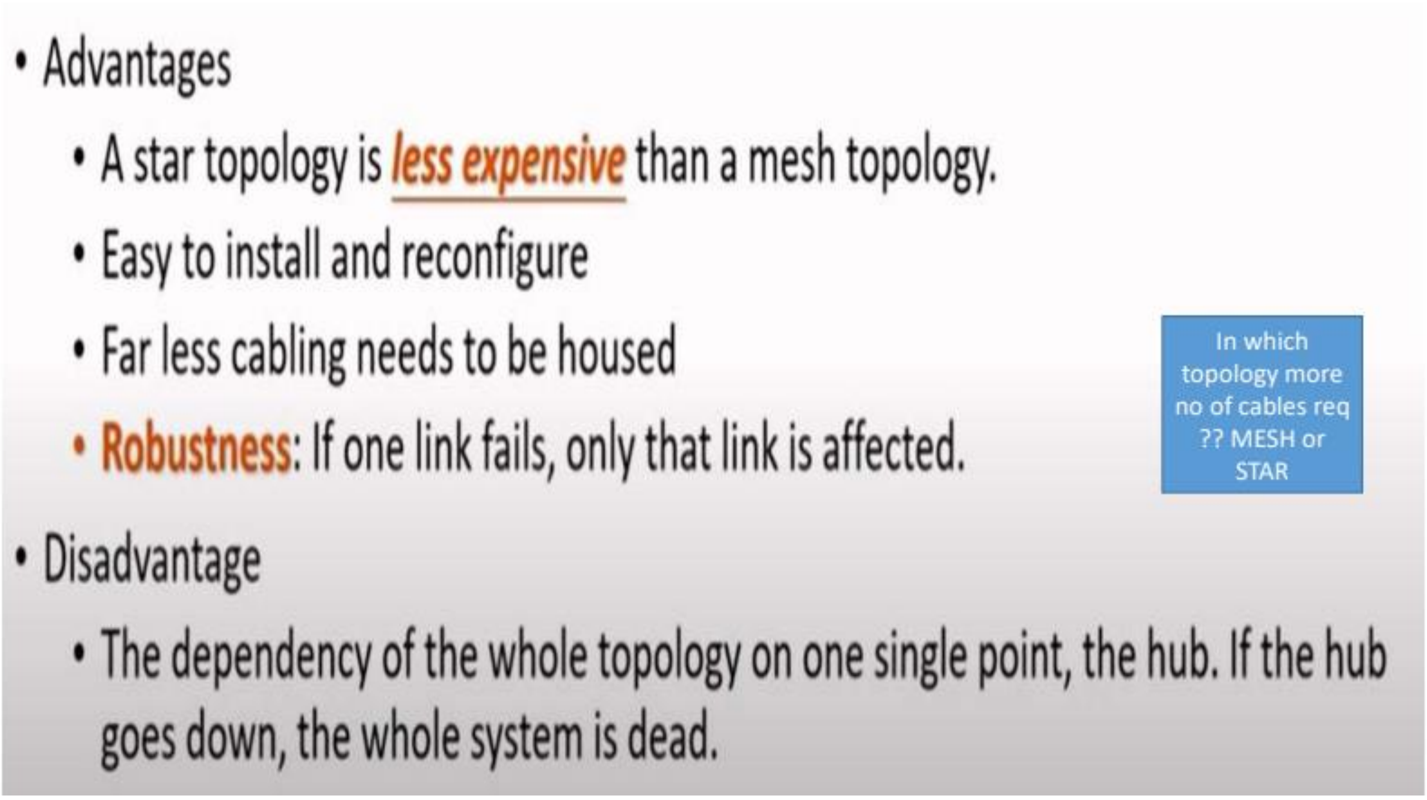
- 1.Because every device must be connected to every other device, installation and reconnection are difficult
- 2.costly because of maintaining redundant links
- 3.The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
- 4.Difficulty in reconfiguration.

Star Topology:



In a star topology :

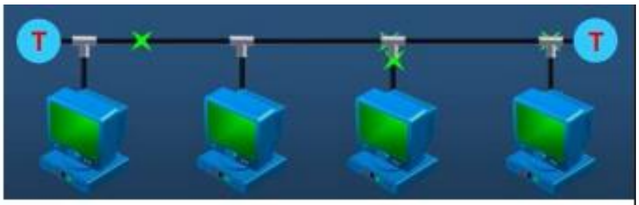
- Each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

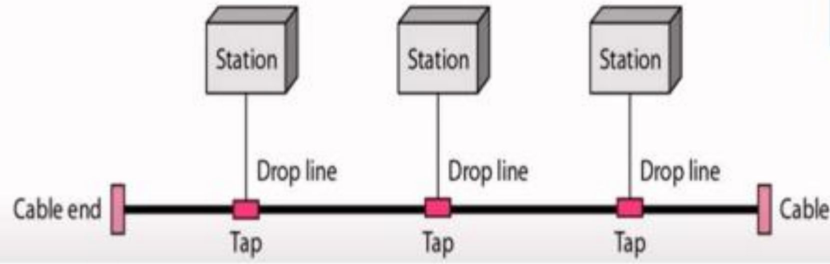


- Advantages
  - A star topology is ***less expensive*** than a mesh topology.
  - Easy to install and reconfigure
  - Far less cabling needs to be housed
  - **Robustness**: If one link fails, only that link is affected.
- Disadvantage
  - The dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

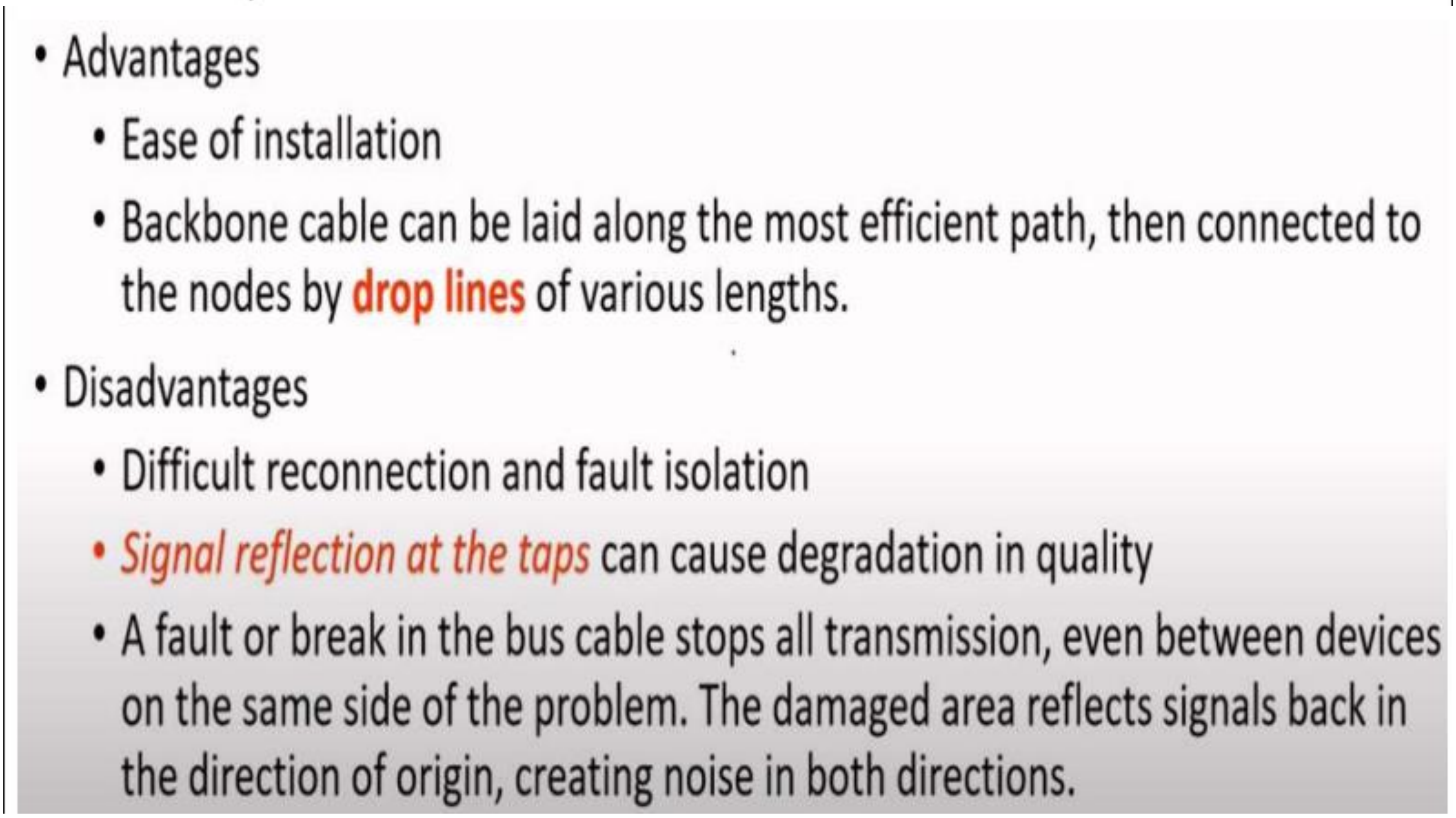
In which topology more no of cables req ?? MESH or STAR

Bus Topology:





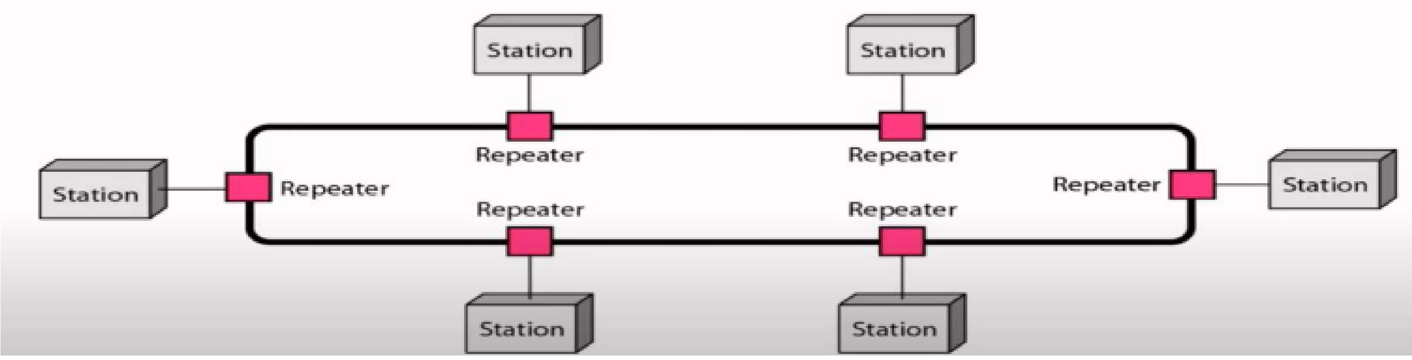
- The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint.
- One long cable acts as a backbone to link all the devices in a network
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.
- As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

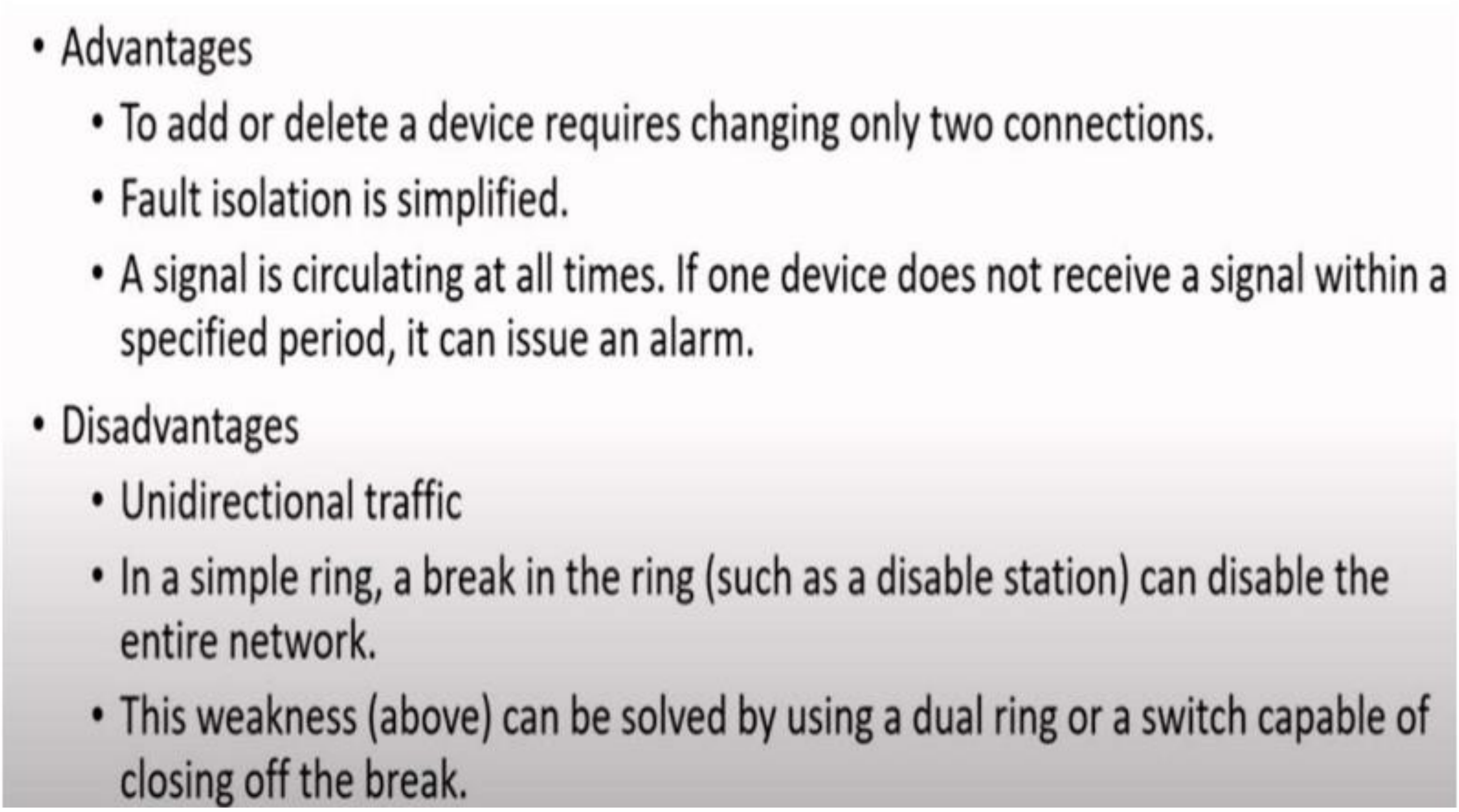


- Advantages
  - Ease of installation
  - Backbone cable can be laid along the most efficient path, then connected to the nodes by **drop lines** of various lengths.
- Disadvantages
  - Difficult reconnection and fault isolation
  - *Signal reflection at the taps* can cause degradation in quality
  - A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

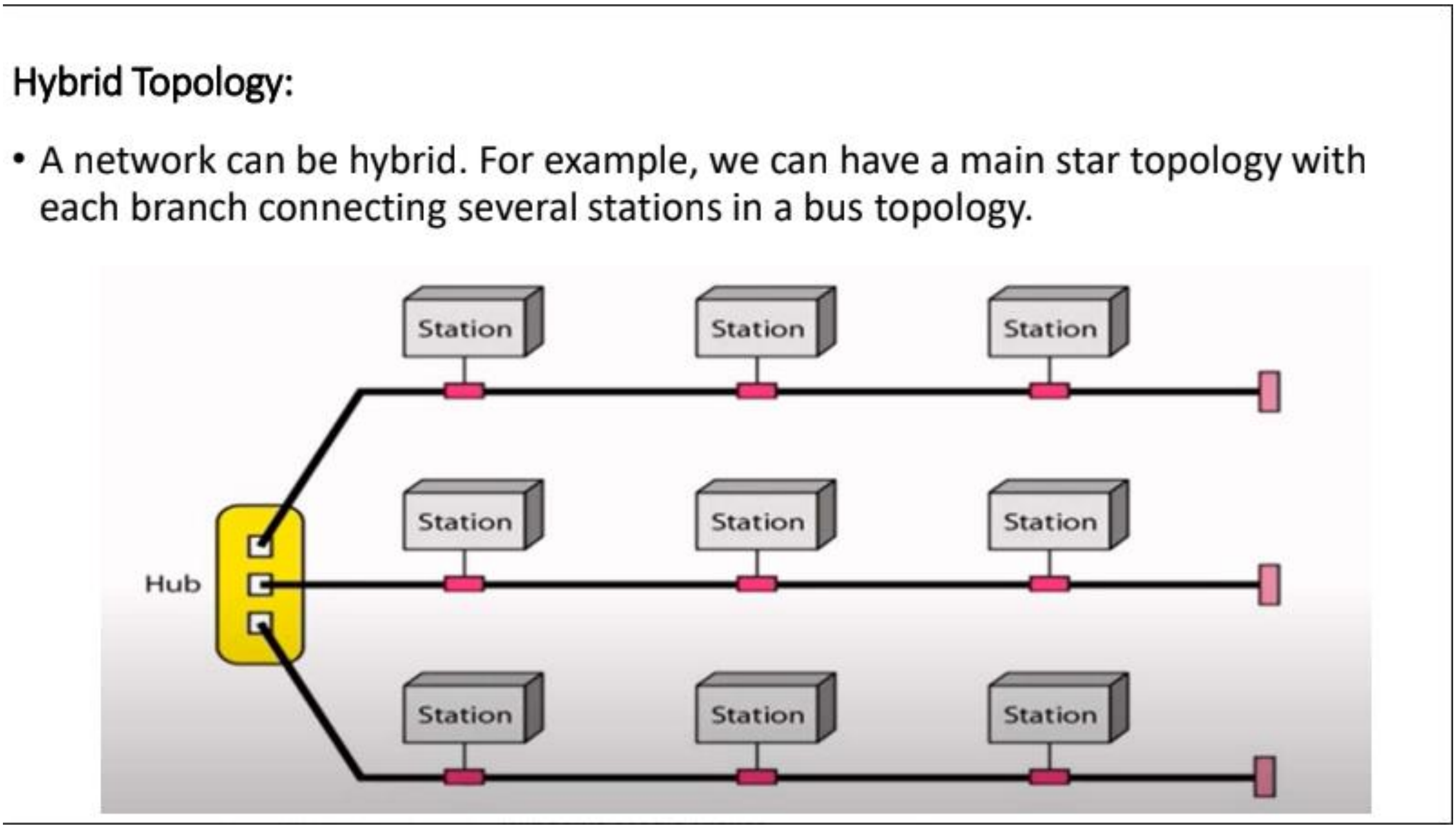
Ring Topology:

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.





- Advantages
  - To add or delete a device requires changing only two connections.
  - Fault isolation is simplified.
  - A signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm.
- Disadvantages
  - Unidirectional traffic
  - In a simple ring, a break in the ring (such as a disable station) can disable the entire network.
  - This weakness (above) can be solved by using a dual ring or a switch capable of closing off the break.



Hybrid Topology:

- A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology.

4)
OPEN SYSTEMS INTER CONNECTION
REFERENCE MODEL (OSIRM)
Introduction to OSI Model & its layers

The Open Systems Interconnection (OSI) Model was developed by International Organization for Standardization (ISO).

ISO is the organization, OSI is the model

It was developed to allow systems with different platforms to communicate with each other. Platform could mean hardware, software or operating system.

It is a network model that defines the protocols for network communications.

It is a hierarchical model that groups its processes into layers. It has 7 layers as follows: (Top to Bottom)

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data Link Layer
7. Physical Layer

Each layer has specific duties to perform and has to cooperate with the layers above and below it.

Layered Architecture of OSI Model

The OSI model has 7 layers each with its own dedicated task.
A message sent from Device A to Device B passes has to pass through all layers at A from top to bottom then all layers at B from bottom to top as shown in the figure below.At Device A, the message is sent from the top layer i.e Application Layer Athen all the layers till it reaches its physical layer and then it is transmitted through the transmission medium. At Device B, the message received by the physical layer passes through all its other layers and moves upwards till it reaches its Application Layer.

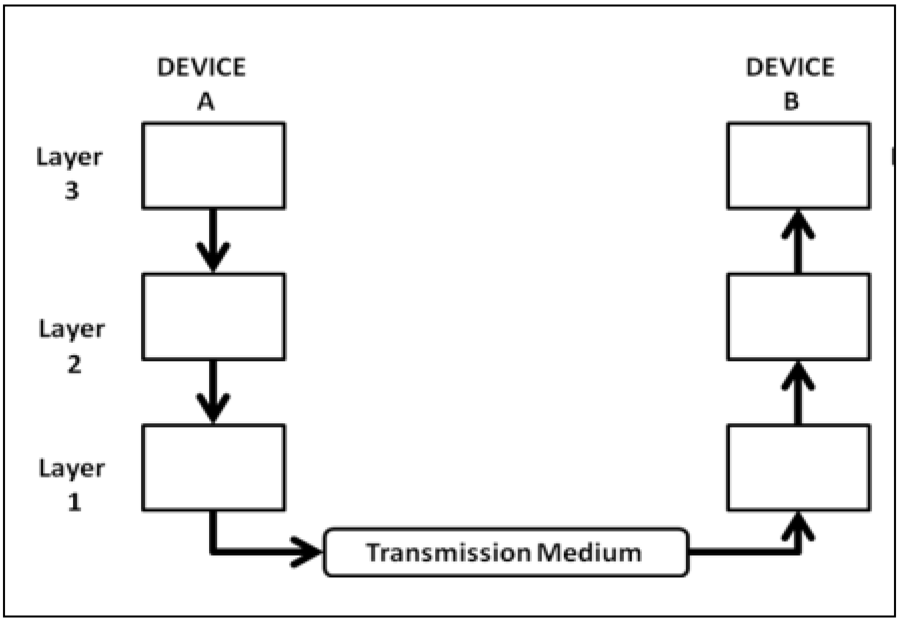


Fig: Flow of Data from Device A to Device B through various layers

As the message travels from device A to device B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model as shown below

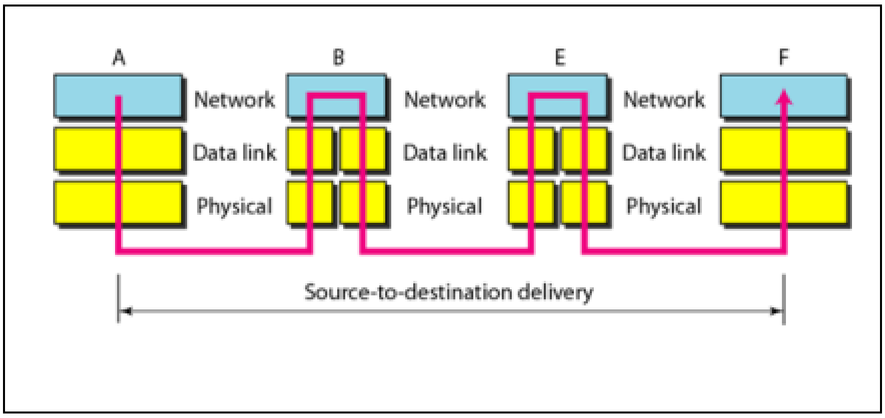


Fig: Data Transfer through Intermediate nodes

- The Data Link layer determines the next node where the message is supposed to be forwarded and the network layer determines the final recipient.

4.3.3 Communication & Interfaces

- For communication to occur, each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. Each layer in the receiving device removes the information added at the corresponding layer and sends the obtained data to the layer above it.

- Every Layer has its own dedicated function or services and is different from the function of the other layers.

- On every sending device, each layer calls upon the service offered by the layer below it.

- On every receiving device, each layer calls upon the service offered by the layer above it.

- Between two devices, the layers at corresponding levels communicate with each other .i.e layer 2 at receiving end can communicate and understand data from layer 2 of sending end. This is called peer –to – peer communication.

- For this communication to be possible between every two adjacent layers there is an interface. An interface defines the service that a layer must provide. Every layer has an interface to the layer above and below it as shown in the figure below

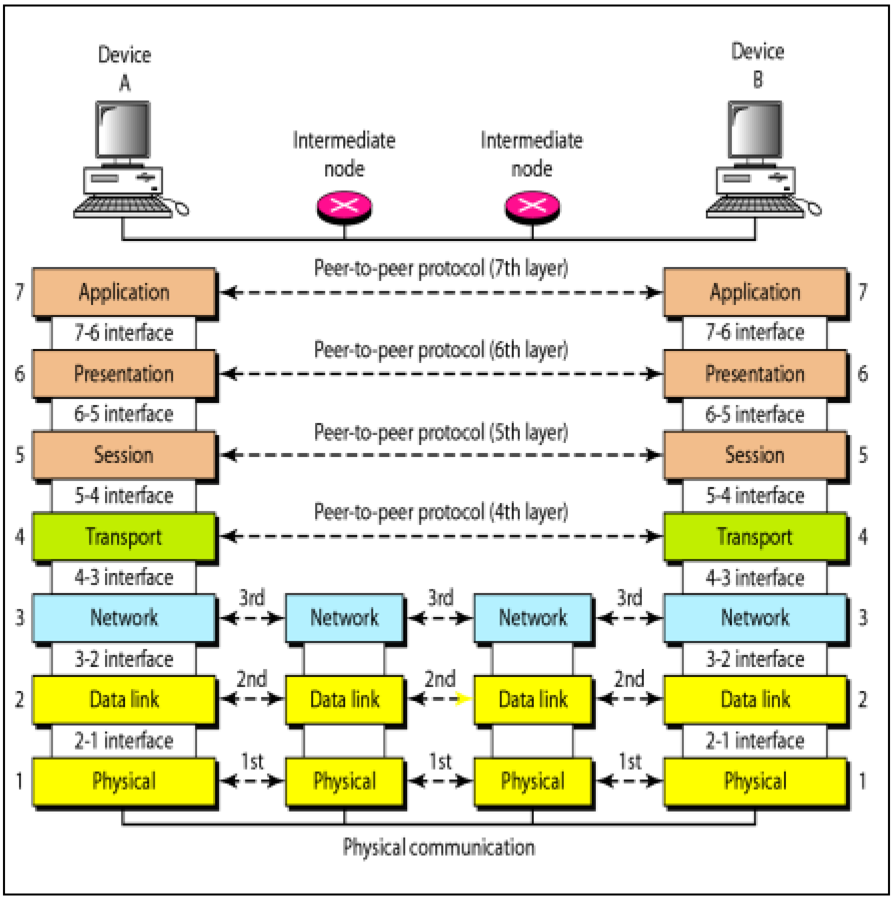


Fig: Communication & Interfaces in the OSI model

Encapsulation of Data

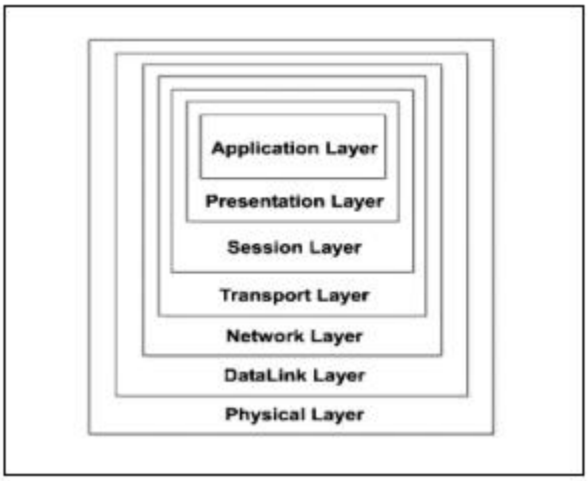


Fig: Encapsulation

- As shown in the figure above the data at layer 7 i.e the Application layer along with the header added at layer 7 is given to layer 6, the Presentation layer. This layer adds Its header and passed the whole package to the layer below.

- The corresponding layers at the receiving side removes the corresponding header added at that layer and sends the remaining data to the above layer.

- The above process is called encapsulation

5)

The TCP/IP protocol suited involves 4 different types of addressing:

1. Physical Address
2. Logical Address
3. Port Address
4. Specific Address

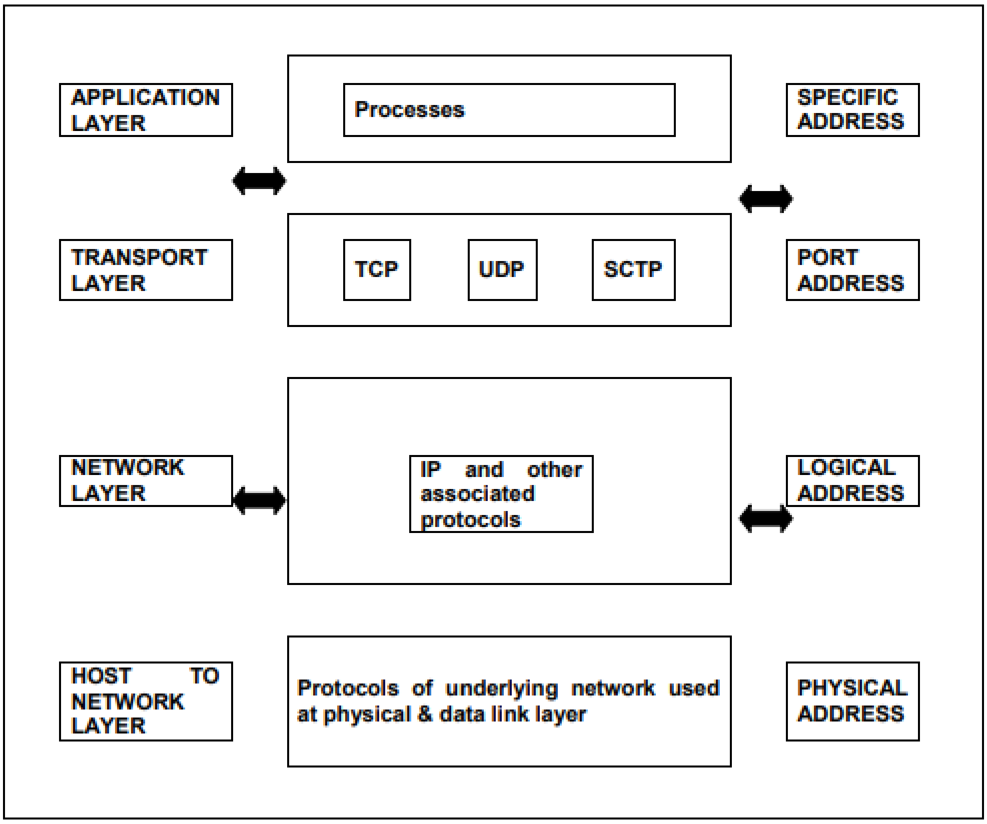


Fig: Addressing in TCP/IP model

Each of these addresses are described below:

1. Physical Address

i. Physical Address is the lowest level of addressing, alsoknown as link address.

ii. It is local to the network to which the device is connected and unique inside it.

iii. The physical address is usually included in the frame and is used at the data link layer.

iv. MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.

v. The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address.

2. Logical Address

i. Logical Addresses are used for universal communication.

ii. Most of the times the data has to pass through different networks; since physical addresses are local to the network there is a possibility that they may be duplicated across multiples networks also the type of physical address being
used may change with the type of network encountered. For ex: Ethernet to wireless to fiber optic. Hence physical addresses are inadequate for source to destination delivery of data in an internetwork environment.

iii. Logical Address is also called as IP Address (Internet Protocol address).
iv. At the network layer, device i.e. computers and routers are identified universally by their IP Address.
v. IP addresses are universally unique.
vi. Currently there are two versions of IP addresses being used:
a. IPv4: 32 bit address, capable of supporting 232 nodes
b. IPv6: 128 bit address, capable of supporting 2128 nodes
3. Port Address
VIII.A logical address facilitates the transmission of data from source to destination device. But the source and the destination both may be having multiple processes communicating with each other.
Ex. Users A & B are chatting with each other using Google Talk, Users B & C are exchanging emails using Hotmail. The IP address will enable transmitting data from A to B, but still the data needs to be delivered to the correct process. The data from A cannot be given to B on yahoo messenger since A & B are communicating using Google Talk.
IX. Since the responsibility of the IP address is over here there is a need of addressing that helps identify the source and destination processes. In other words, data needs to be delivered not only on the correct device but also on the correct process on the correct device.
X. A Port Address is the name or label given to a process. It is a 16 bit address.
XI. Ex. TELNET uses port address 23, HTTP uses port address 80
4. Specific Address
i. Port addresses address facilitates the transmission of data from process to process but still there may be a problem with data delivery.
For Ex: Consider users A, B & C chatting with each other using Google Talk. Every user has two windows open, user A has two chat windows for B & C, user B has two chat windows for A & C and so on for user C Now a port address will enable delivery of data from user A to the correct process (in this case Google Talk) on user B
but now there are two windows of Google Talk for user A & C available on B where the data can be delivered.
ii. Again the responsibility of the port address is over here and there is a need of addressing that helps identify the different instances of the same process.
iii. Such address are user friendly addresses and are called specific addresses.
iv. Other Examples: Multiple Tabs or windows of a web browser work under the same process that is HTTP but are identified using Uniform Resource Locators (URL), Email addresses.

6)

- It is also called as the TCP/IP protocol suite. It is a collection of protocols.
- IT is a hierarchical model, ie. There are multiple layers and higher layer protocols are supported by lower layer protocols.
- It existed even before the OSI model was developed.
- Originally had four layers (bottom to top):
    1. Host to Network Layer
    2. Internet Layer
    3. Transport Layer
    4. Application Layer
- The figure for TCP/IP model is as follows:

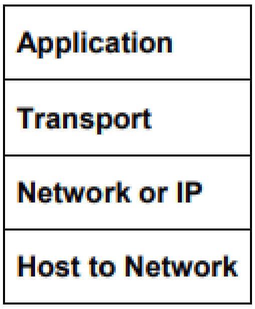
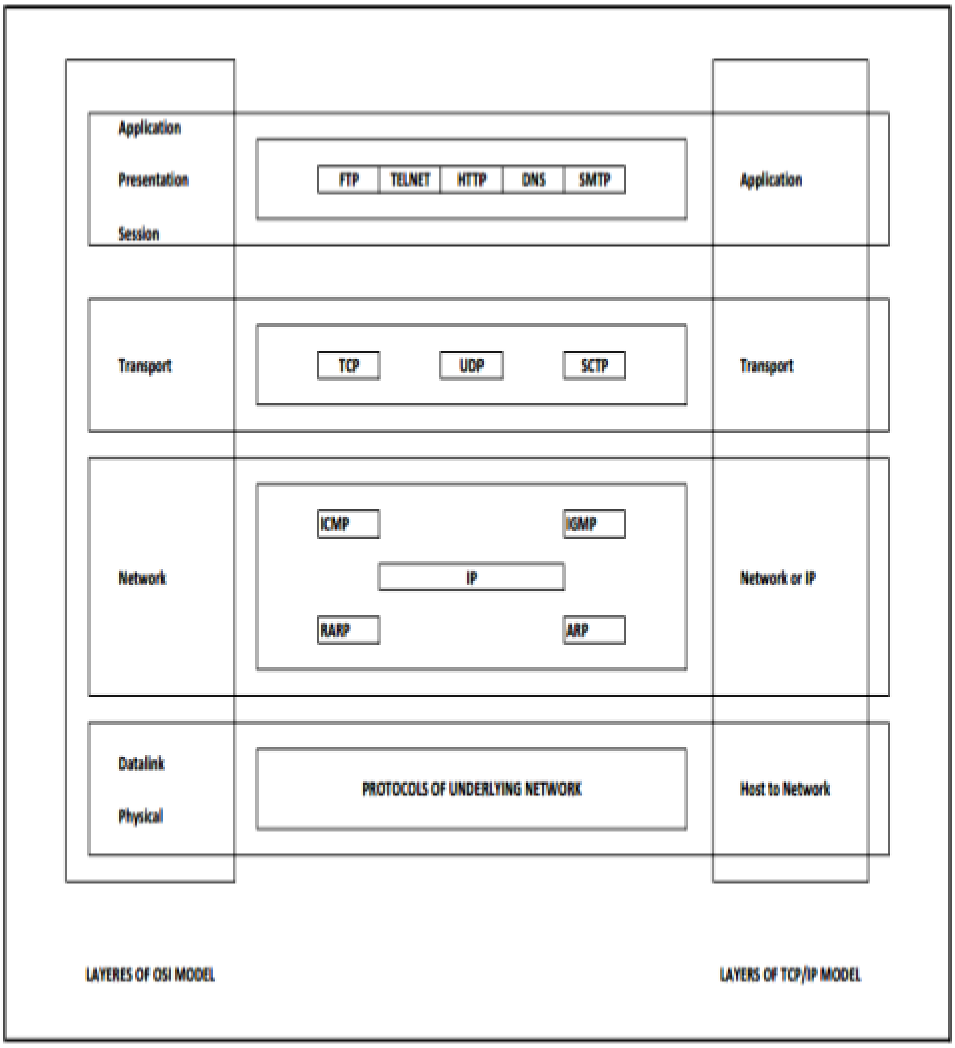


Fig: Layers of TCP/IP Reference Model

- The structure TCP/IP model is very similar to the structure of the OSI reference model. The OSI model has seven layers where the TCP/IP model has four layers.



Functions of the Layers of TCP/IP model:

A. Host to Network Layer

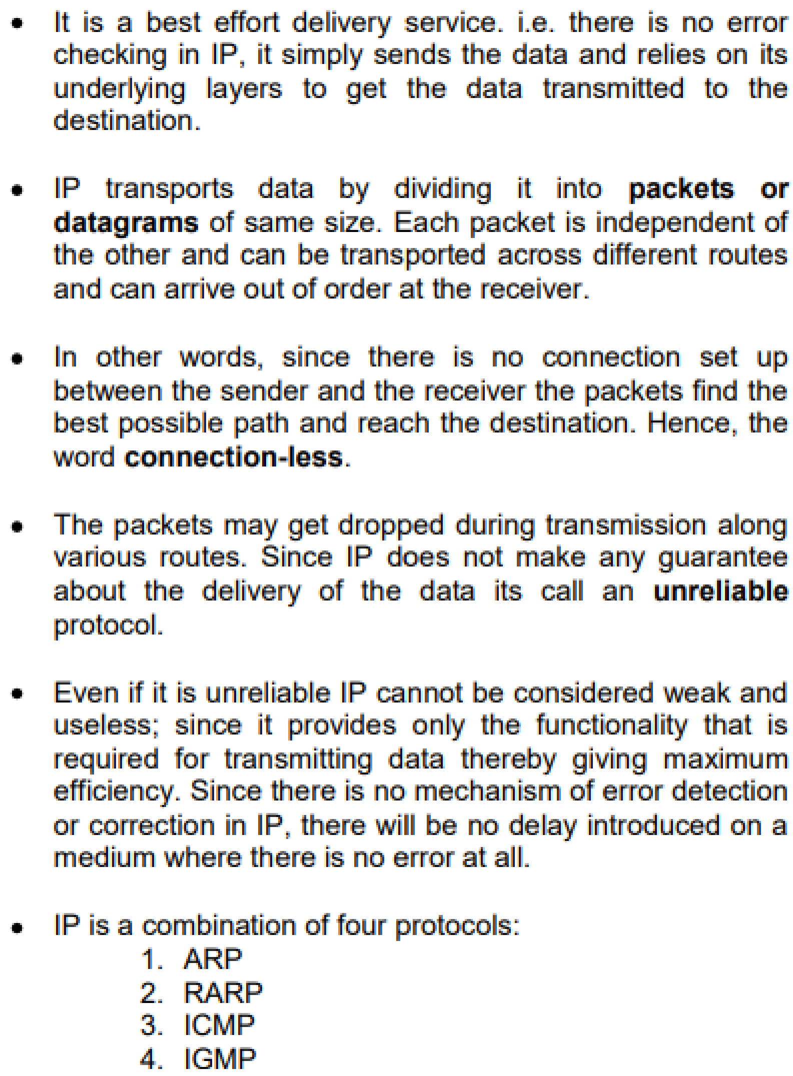
This layer is a combination of protocols at the physical and data link layers.

It supports all standard protocols used at these layers.

B. Network Layer or IP

- Also called as the Internetwork Layer (IP). It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data.

- The Internetworking Protocol (IP) is an **connection-less & unreliable protocol.**



- It is a best effort delivery service. i.e. there is no error checking in IP, it simply sends the data and relies on its underlying layers to get the data transmitted to the destination.

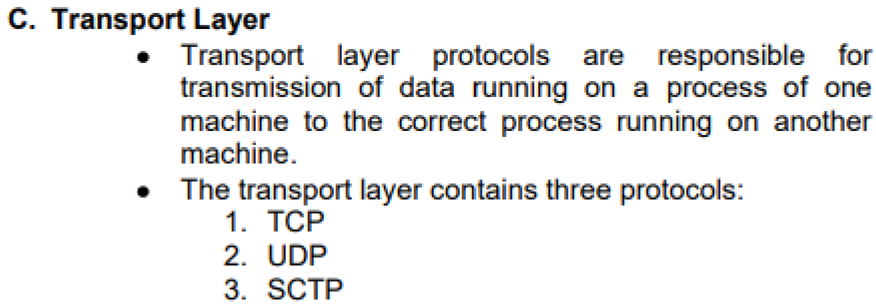
- IP transports data by dividing it into **packets or datagrams** of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver.

- In other words, since there is no connection set up between the sender and the receiver the packets find the best possible path and reach the destination. Hence, the word **connection-less**.

- The packets may get dropped during transmission along various routes. Since IP does not make any guarantee about the delivery of the data its call an **unreliable** protocol.

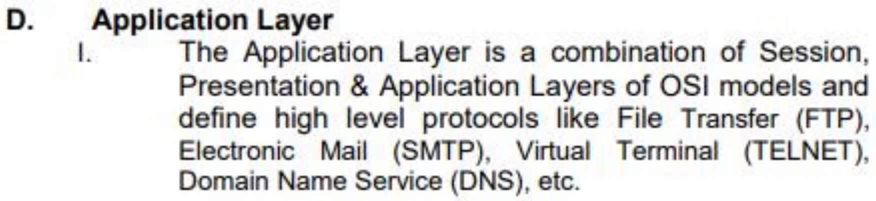
- Even if it is unreliable IP cannot be considered weak and useless; since it provides only the functionality that is required for transmitting data thereby giving maximum efficiency. Since there is no mechanism of error detection or correction in IP, there will be no delay introduced on a medium where there is no error at all.

- IP is a combination of four protocols:
    1. ARP
    2. RARP
    3. ICMP
    4. IGMP



C. Transport Layer

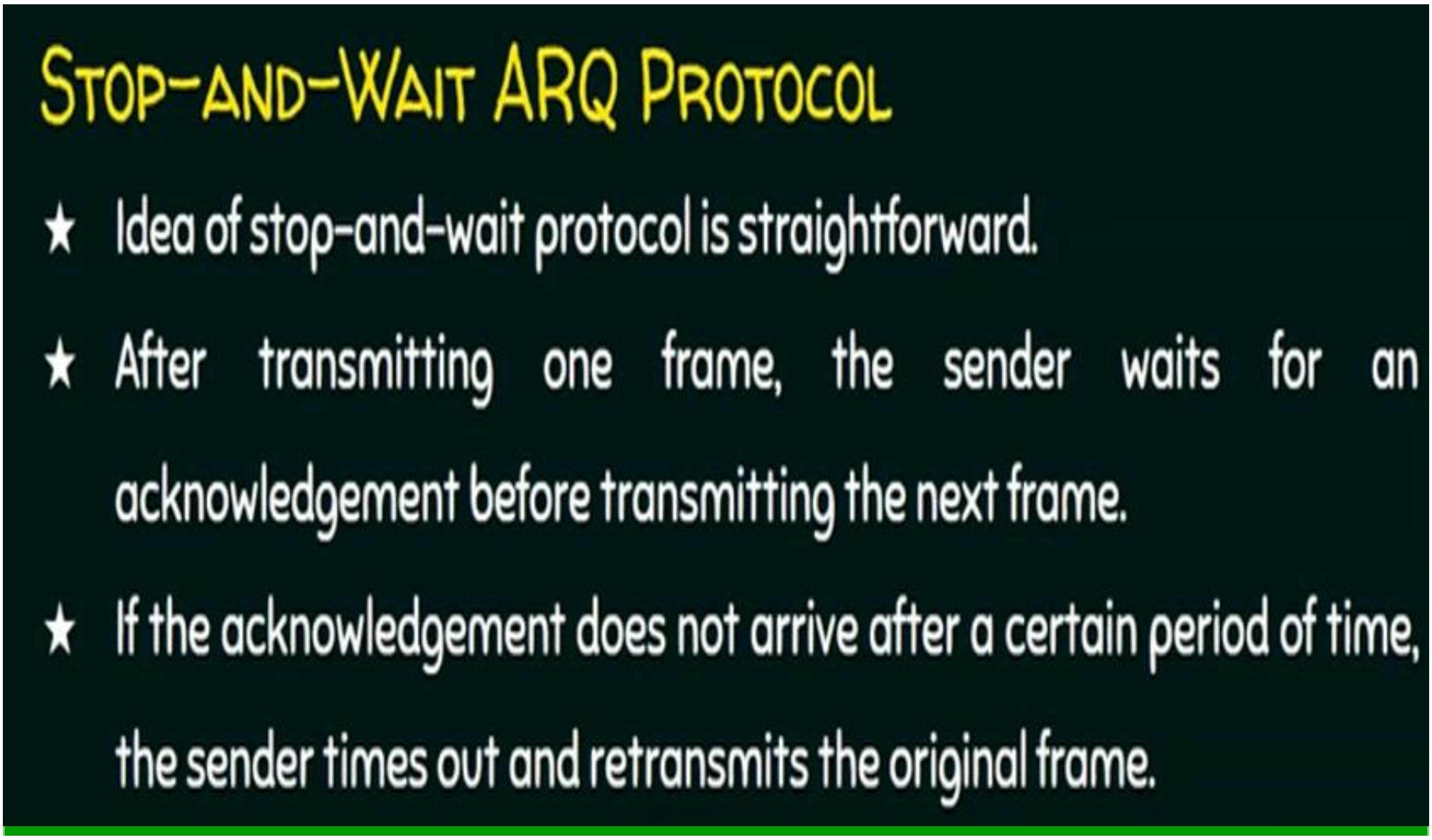
- Transport layer protocols are responsible for transmission of data running on a process of one machine to the correct process running on another machine.
- The transport layer contains three protocols:
    1. TCP
    2. UDP
    3. SCTP



D. Application Layer

I. The Application Layer is a combination of Session, Presentation & Application Layers of OSI models and define high level protocols like File Transfer (FTP), Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), etc.

7)



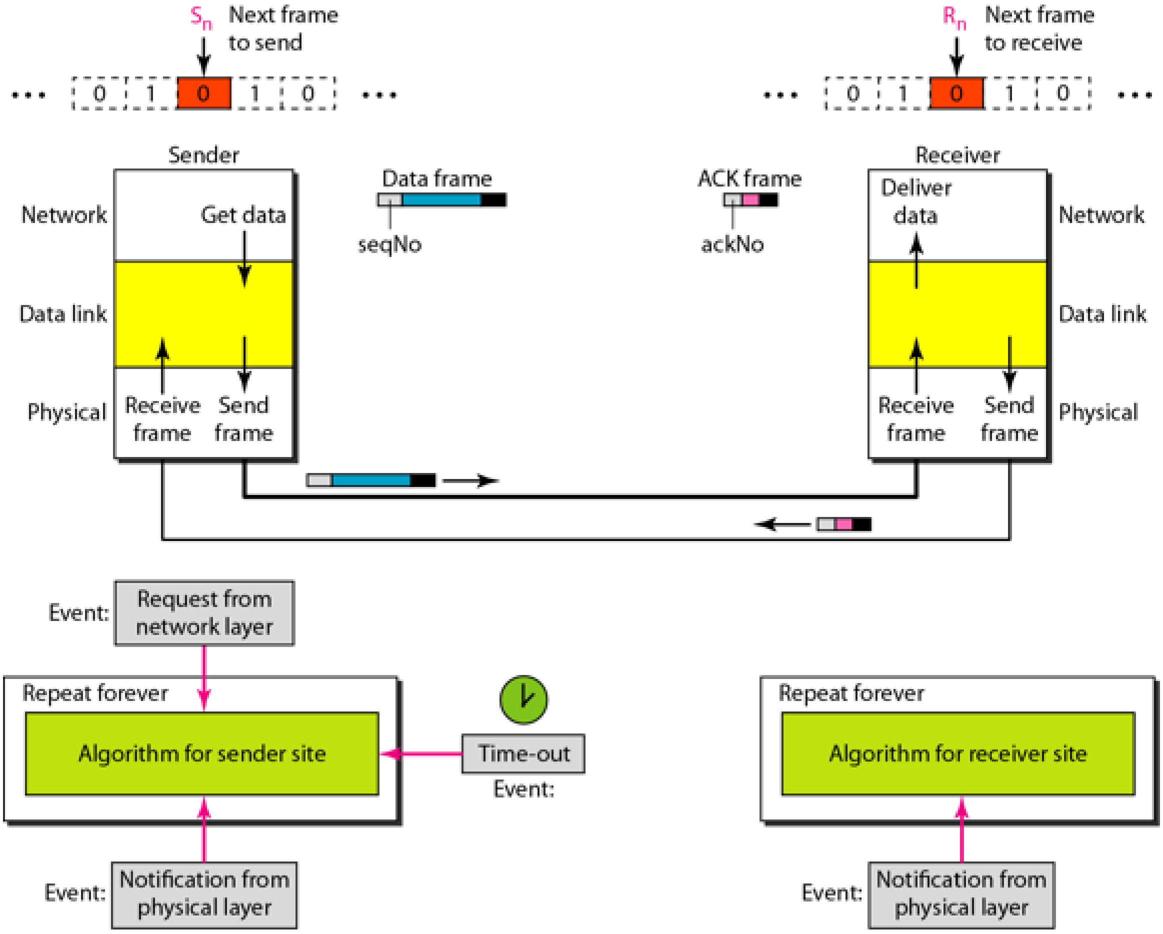
Stop-and-Wait ARQ Protocol

- ★ Idea of stop-and-wait protocol is straightforward.
- ★ After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.
- ★ If the acknowledgement does not arrive after a certain period of time, the sender times out and retransmits the original frame.

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

In Stop-and-Wait ARQ, we use sequence numbers to number the frames.
The sequence numbers are based on modulo-2 arithmetic.

In Stop-and-Wait ARQ, the acknowledgment number always announces in modulo-2 arithmetic the sequence number of the next frame expected.



The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame.

A data frames uses a seqNo (sequence number); an ACK frame uses an ackNo (acknowledgment number).

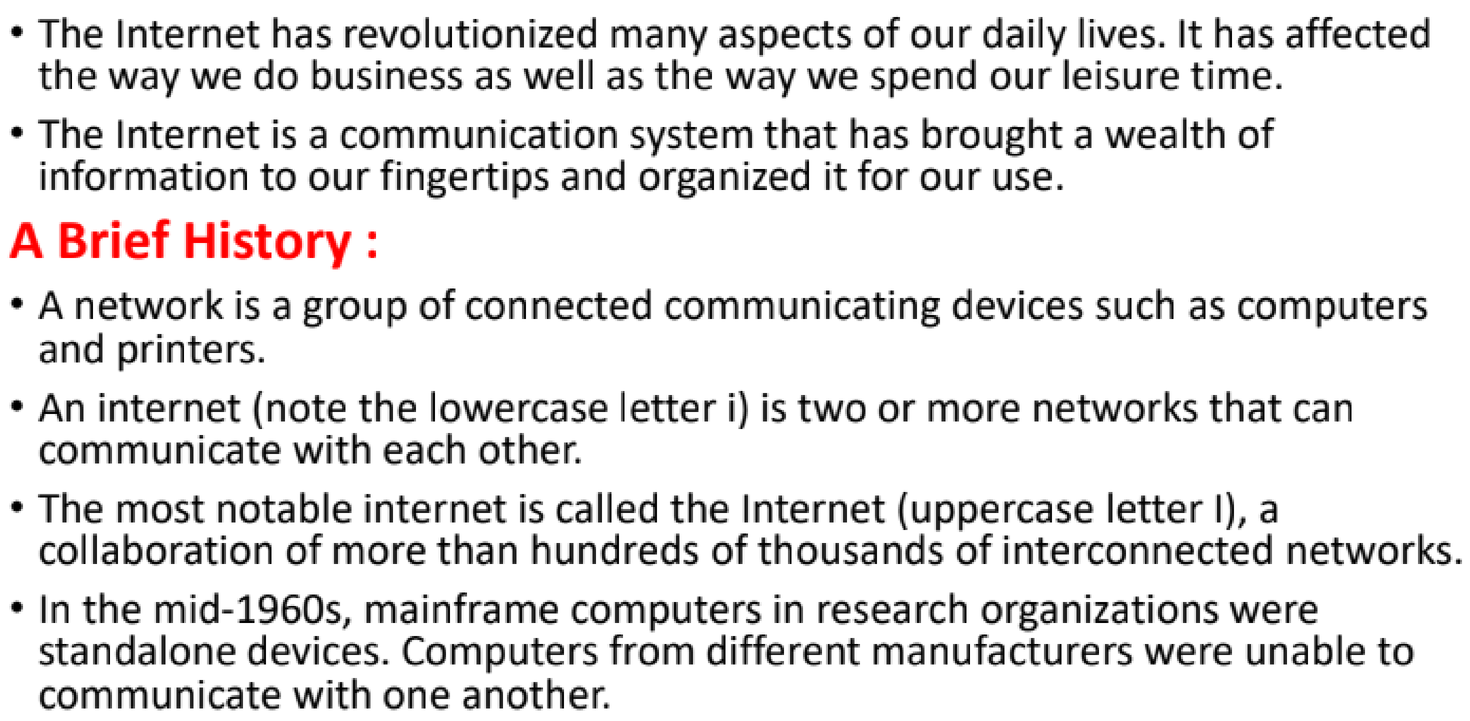
The sender has a control variable, which we call Sn (sender, next frame to send), that holds the sequence number for the next frame to be sent (0 or 1).

The receiver has a control variable, which we call Rn (receiver, next frame expected), that holds the number of the next frame expected.

When a frame is sent, the value of Sn is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa.

When a frame is received, the value of Rn is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa.

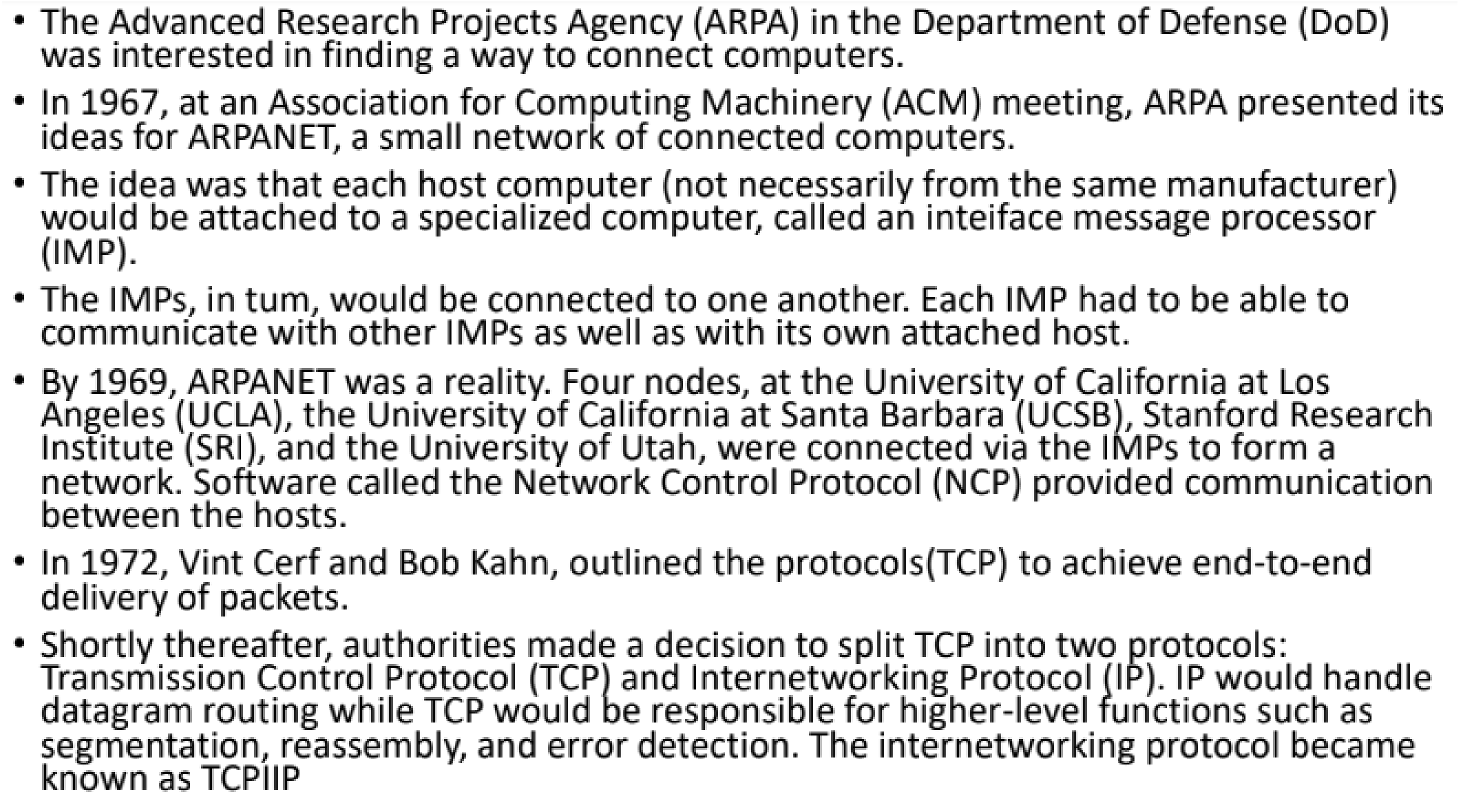
7b)



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

A Brief History :

- A network is a group of connected communicating devices such as computers and printers.
- An internet (note the lowercase letter i) is two or more networks that can communicate with each other.
- The most notable internet is called the Internet (uppercase letter I), a collaboration of more than hundreds of thousands of interconnected networks.
- In the mid-1960s, mainframe computers in research organizations were standalone devices. Computers from different manufacturers were unable to communicate with one another.



- The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers.
- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.
- The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an inteiface message processor (IMP).
- The IMPs, in tum, would be connected to one another. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.
- By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network. Software called the Network Control Protocol (NCP) provided communication between the hosts.
- In 1972, Vint Cerf and Bob Kahn, outlined the protocols(TCP) to achieve end-to-end delivery of packets.
- Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher-level functions such as segmentation, reassembly, and error detection. The internetworking protocol became known as TCPIIP

8)

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing. The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.

Fixed-Size Framing:

- In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter.

Variable-Size Framing

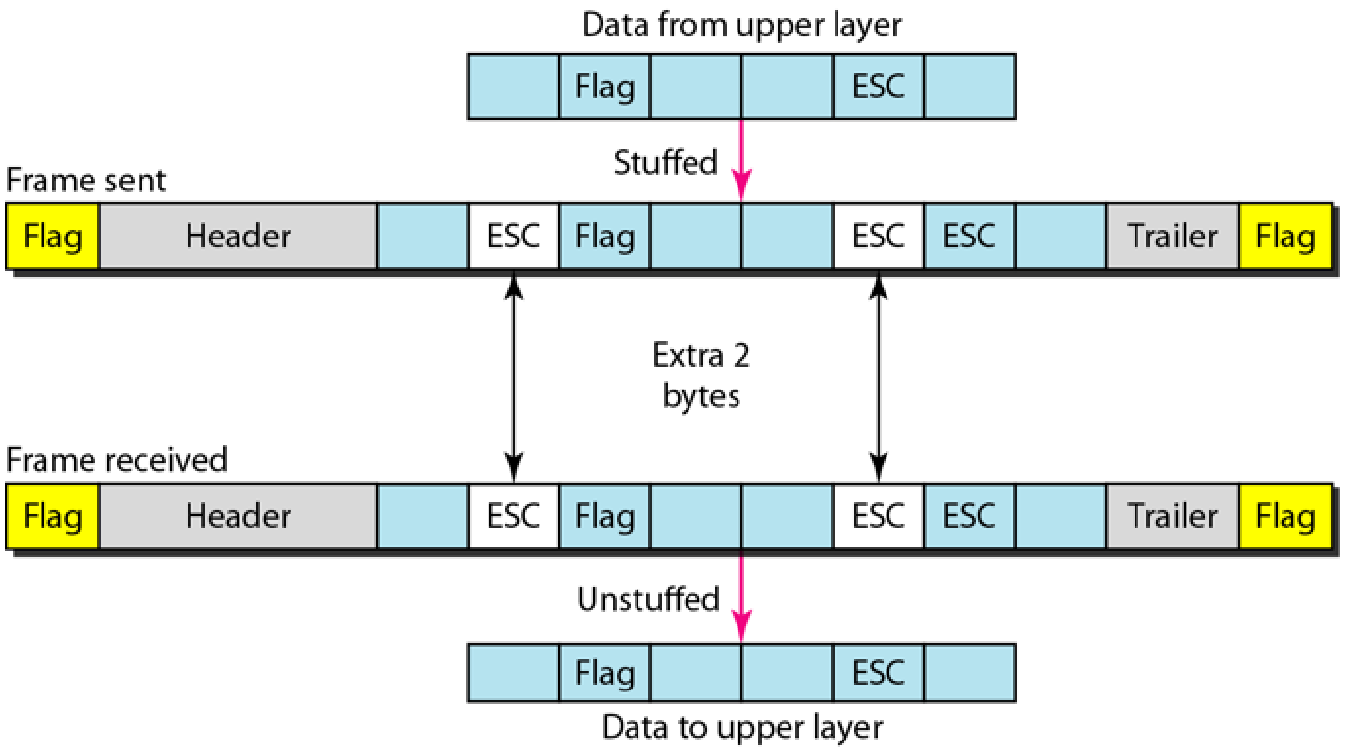
In variable-size framing, we need a way to define the end of the frame and the beginning of the next.

two approaches were used for this purpose:

a character-oriented approach

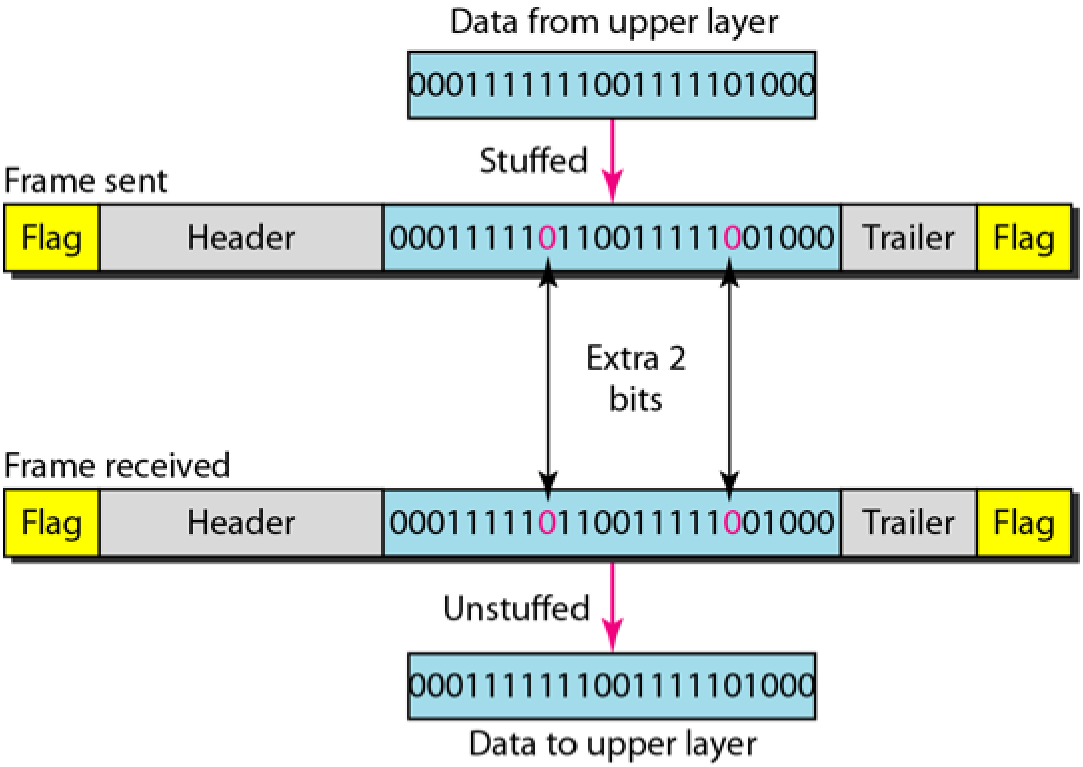
a bit-oriented approach.

Figure 11.2 *Byte stuffing and unstuffing*

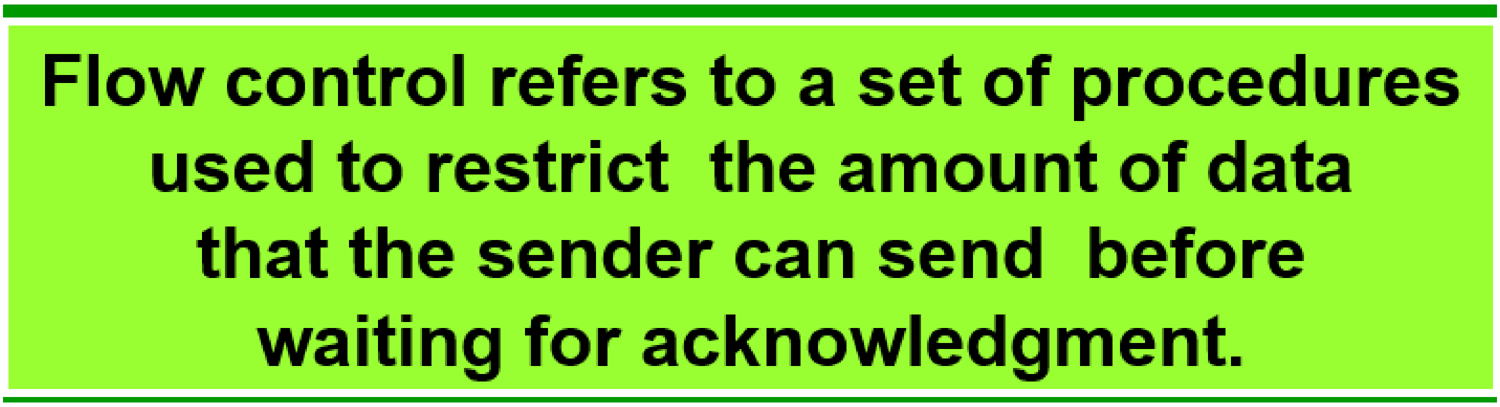


Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text.

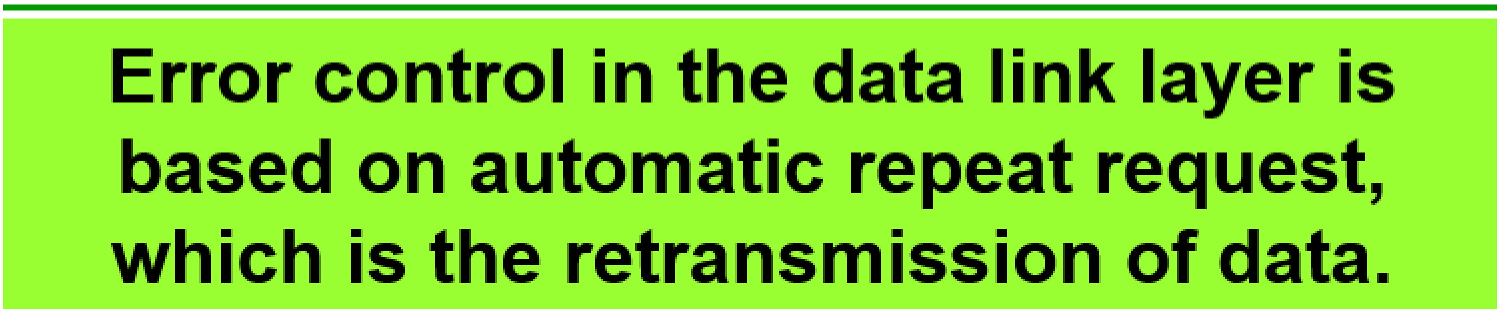
Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.



9)



Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.



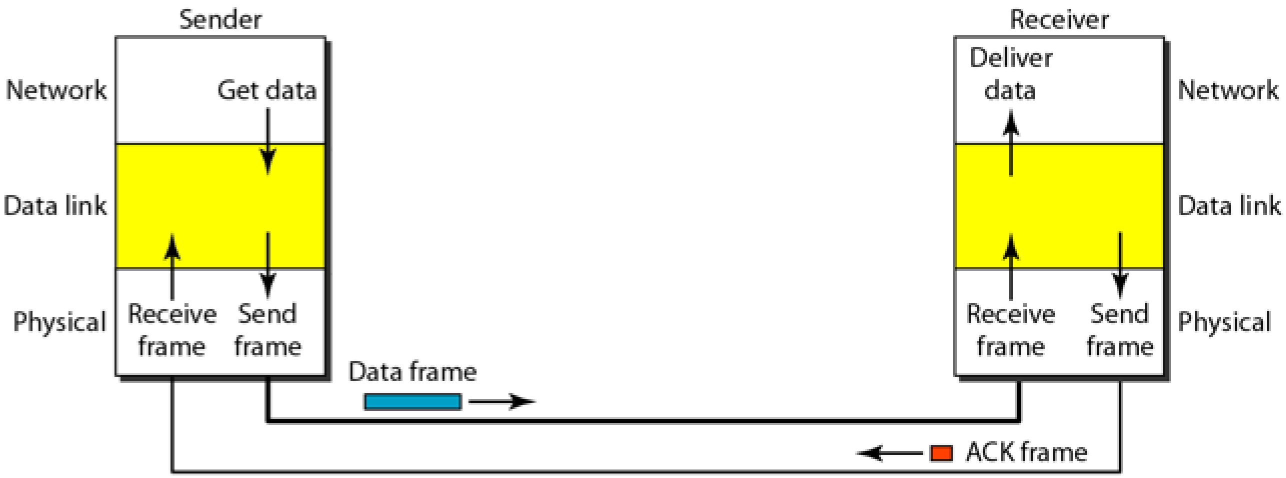
Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

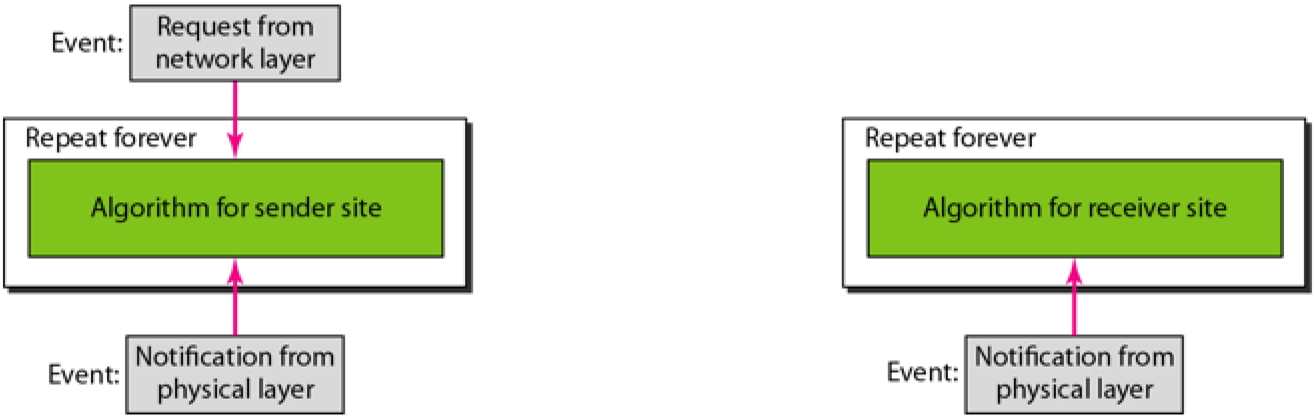
9 b)

Introduction :

- Stop-and-wait Protocol is used in the data link layer for the transmission in the noiseless channels.
- Suppose there is a scenario in which the data frames arrive at the receiver's site faster than they can be processed means the rate of transmission is more than the processing rate of the frames. Also, it is normal that the receiver does not have enough space, and the data is also coming from multiple sources. Then due to all these, there may occur discarding of frames.

- In order to prevent the receiver from overwhelming, there is a need to tell the sender to slow down the transmission of frames. We can make use of feedback from the receiver to the sender. Ie concept of the Stop-and-wait protocol.
- The sender sends one frame, then stops until it receives the confirmation from the receiver, after receiving the confirmation sender sends the next frame.
- stop-and-wait is one of the flow control protocol which makes the use of flow control service provided by the data link layer.
- For every sent frame, the acknowledgment is needed




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

- Datalink layer at the sender side waits for its network layer in order to send the data packet. the data link layer makes the frame out of the data provided by the network layer and then sends it to the physical layer. After sending the data it will then wait for the acknowledgment before sending the next frame.
- The data link layer on the receiver side waits for the frame to arrive. When the frame arrives then the receiver processes the frame and then delivers it to the network layer. After that, it will send the acknowledgment or we can say that ACK frame back to the sender.

10a)
Links : 10
Ports : 4
10b)

The data link layer at the sender side mainly gets the data from the network layer and then makes the frame out of data and sends it. On the Receiver site, the data link layer receives the frame from the physical layer and then extracts the data from the frame, and then delivers the data to its network layer.

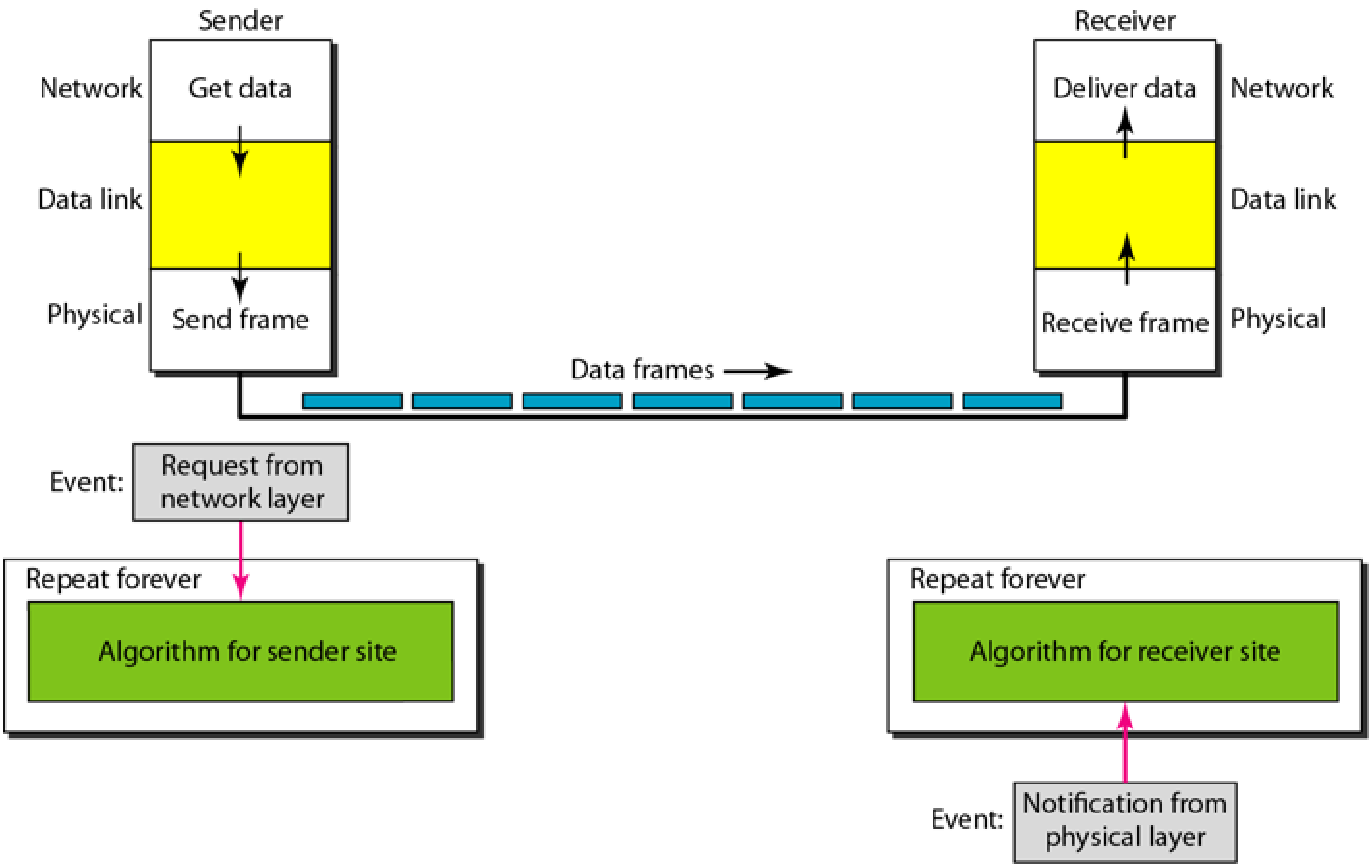
Procedure :

There is no frame send by the data link layer of the sender site until its network layer has a data packet to send.

Similarly, the receiver site cannot deliver a data packet to its network layer until a frame arrives.

The procedure at the sender site runs constantly; there is no action until there is a request from the network layer.

Also, the procedure at the receiver site runs constantly; there is no action until there is a notification from the physical layer.


Sender
Network
Get data
Data link
Physical
Send frame
Receiver
Deliver data
Network
Data link
Receive frame
Physical
Data frames
Event:
Request from network layer
Repeat forever
Algorithm for sender site
Repeat forever
Algorithm for receiver site
Event:
Notification from physical layer