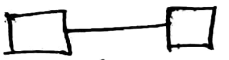
→ Data - An information. Unit-I Class 1 - 17/12/19
→ sharing of information. ⇒ Data communication. (Introduction)
→ local or remote
→ "telecommunication" ⇒ tele = far
→ Communicating devices ⇒ s/w + h/w.
→ Data communication system

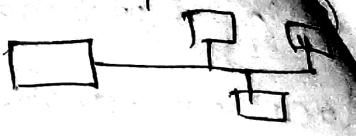
→ Data representation. ⇒ text, images, numbers, audio & video.
(Unicode - 32 bits ⇒ ASCII
→ Data flow ⇒ simplex, half-duplex, full-duplex.
↓ one direction. ↓ both direction → but one at a time. ↓ both direction. → at same time.
↓ ↓ ↓
Ex. keyboards, traditional monitors walkie-talkies Telephone network.
(Two diff transmission paths are used at each end one for sending one for receiving).
→ Network. ⇒ set of devices connected by communication links.
→ N/w criteria ⇒ ① Performance (throughput & delay)
↓
* Transit time
* Response time
② Reliability
③ Security

→ physical structures

① Type of connection ⇒ ① point to point ② multipoint



ex. remote control & television.



② Topology ⇒ the way in which n/w is formed.

① Mesh ② Star ③ Bus ④ Ring

① Each node is connected to other node. (point to point)

Advantages

→ Dedicated links (Reduce traffic problems)

→ Robust

→ privacy & security

Disadvantage

→ Complexity (cabling, I/O ports) → expensive.

Example

→ Telephone regional office

① each device has a dedicated point-to-point link to central controller.

② point to point

Advantage

→ less expensive

→ robustness

Disadvantage

→ central controller

Example

→ Local LAN's

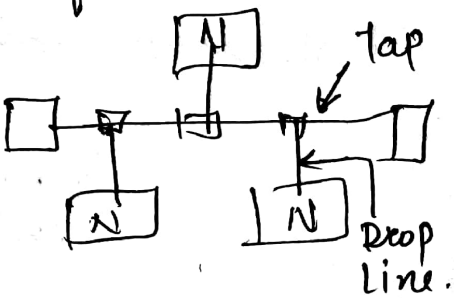
① multipoint

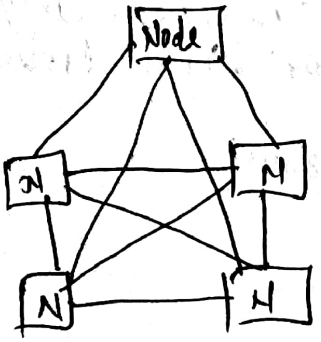
Advantages

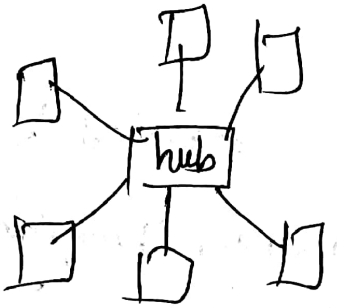
→ ease of installation.

Disadvantage

→ reconnection and fault isolation.







⑤ Hybrid

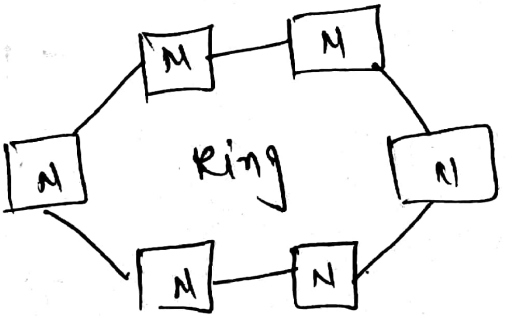
⇒ mixed topology.

④ Ring ⇒ ① dedicated point to point

Advantages → easy to install & reconfigure.

Example → Token ring

Disadvantage → if it is unidirectional.



③ Network models
→ OSI (open system interconnection)
→ Internet-model (TCP/IP protocol suite).

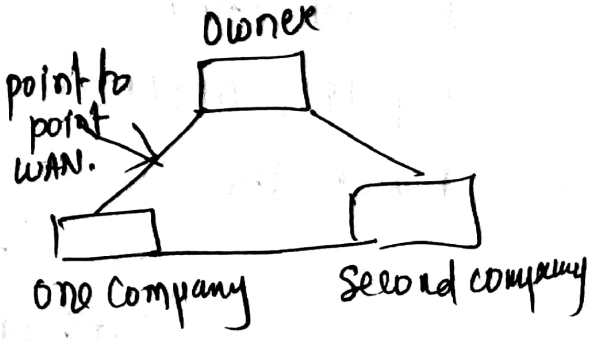
④ Types of Networks
→ LAN (few kilometers) → one transmission media → bus, ring, star (100 to 1000 mbps)
→ WAN (at long distance)

Switched WAN ↓
Connects end system to router that connects another LAN or WAN.
→ ex. X.25
Frame Relay
ATM

Point-to-point WAN ↓
a telephone or cable TV provider that connects a home computer or small LAN to ISP.
→ wireless WANs

→ MAN — size between LAN and WAN.
→ DSL Line ② Cable TV network

* Internetwork (Internet)
→ Two or more networks are connected.



Unit - I

Class 2 - 18

* The Internet

→ A communication system that has brought a wealth of info... to our fingertips and organized it for our use.

→ ① Internet ⇒ a collaboration of more than hundreads of thousands of interconnected networks.
(came into picture from 1969)

→ In 1960's, ARPA (Advanced Research Project Agency) in the DoD (Department of Defence) was interested in finding way to connect computers.

→ In 1967, at an ACM (Association for computing machinery), ARPANET was evolved. The idea was that each computer would attached to a specialized computer called IMP (interface message processor.) and then IMP's are connected to each other.

→ By 1969 ARPANET ~~becomes~~ was reality.

→ four nodes, University of California at Los Angeles (UCLA)
University of California at Santa Barbara (UCSB)
stanford research institute (SRI)
University of Utah were connected by IMP's.

→ NCP (Network control protocol) provided communication.

→ In 1972, Vint Cerf and Bob kahn collaborated on Internetting project.

→ In 1973, TCP (Transmission Control Protocol) were developed.

→ shortly, thereafter the protocol is splitted into two TCP and IP (Internetworking Protocol).

→ The networking protocol became known as TCP/IP.

The Internet today (Dia: 1:13 Hierarchical organization of the internet page-15)

→ It is made up of many wide and local area networks joined by connecting devices and switching stations.

→ Internet connections use the services of ISP's (Internet Service Providers)

→ The internet today is run by private companies, not the government.

* ISP (Internet Service Providers)

→ ① International ISP's

→ This are at the top of hierarchy that connects nations together

② National ISP's

→ This are backbone networks created and maintained by specialized companies.

→ To provide connectivity between end users these backbone networks are connected by complex switching stations called NAPs (Network access points).

→ Some national ISP's are connected to one another by private switching stations called peering points.

→ Operates at a rate of 600 mbps.

③ Regional ISP's

→ smaller ISP's that are connected to one or more national ISP's.

→ They are at the third level of the hierarchy with a smaller data rate.

④ Local ISP's

→ This provides direct service to end users.
→ Can be connected to regional ISP's or directly to national
→ Local ISP's can be a company that just provides internet services, a corporation that supplies services to its own employees. or nonprofit organizations. such as college or a university, that runs its own network.
→ Each local ISP's can be connected to a regional or national service provider.

* Protocols and standards

① Protocols

→ set of rules that govern data communications.
→ A protocol defines what is communicated, how it is communicated and when it is communicated.
→ For communication to occur, the two entities must agree on a protocol.
→ The key elements of protocol are as follows.
  * Syntax ⇒ Refers to structure or format of the data
    ex. a simple protocol might expect the first 8 bits of data to be the address of the sender, next 8 bits as receivers address, and remaining bits as message itself.

  * Semantics ⇒ Refers to the meaning of each section of bits.
    ⇒ How the particular pattern to be interpreted and what action to be taken
    ⇒ For ex. does an address identify the route to be taken for the final destination of the message.

Timing - It refers to two characteristics.
① When data should be sent.
② How fast they can be sent.

② Standards

→ Standard provides guidelines to manufactures, vendors, government agencies and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

→ Data communication standards falls in two categories.

① De-facto - standards that have been approved by organized body but have been adopted as standards through widespread use are de facto standards. This standards are often established originally by manufacturers.

② De-jure - Those standards that have been legislated by an officially recognized body are de-jure standards.

→ standards are developed through the cooperation of standards creation committees, forums and government regulatory agencies. Some of these are ISO, ITU-T, ANSI, IEEE, EIA, W3C, OMA are the standards creation committees.

ISO - International Organization for standardization.
ITU-T - International Telecommunication Union - Telecommunications
ANSI -
IEEE -
W3C -

→ forums → Telecommunications technology development is faster than the ability of standards committees to ratify standards. To speed up the process of standardization the forums are developed.

→ This forums works with universities and users to test, evaluate and standardize new technologies.

→ Some important forums are:

① Frame Relay Forum - This forum was formed to promote the acceptance and implementation of Frame Relay.

② ATM Forum - promotes the use of ATM technology.

③ Universal Plug and Play Forum - This forum supports and promotes simplifying the implementation of networks by creating zero-configuration networking devices.

→ Regulatory Agencies - All communication technology is subject to regulation by government agencies. The purpose of these agencies is to protect the public interest by regulating radio, television and wire/cable communications.

→ Federal Communications Commision (FCC) - The Federal communications commision has authority over interstate and international commerce as it relates to communications.

The OSI model – Layering Scenario. Class 3

→ OSI is an ISO (International standards Organication) standard that covers all aspects of network communications.

→ Open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

→ The OSI model is a layered framework consisting of seven separate but related layers each of which defines a part of the process of moving information across a network. (Fig 2.a seven layers of the OSI model page no: 30)

→ Each layer defines a family of functions distinct from those of the other layers.

→ Within a single machine, each layer calls upon the services of the layer just below it.

→ The processes on each machine that communicate at a given layer are called peer-to-peer processes.

→ The OSI model composed of seven ordered layers. physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6) and application (layer 7).

→ At the physical layer, communication is direct. At the higher layers, however, communication must move down through the layers. and then back up through the layers.

→ Each layer in the sending device add its own information to the message it receives from the layers just above it and passes the whole data to the layer just below it.

→ At the receiving machine, the message is unwrapped layer.

→ The passing of the data and network information is made possible by an interface between each pair of adjacent layers.

→ The seven layers grouped as three subgroups : layer 1, 2 and 3 - physical, data link and network - are the network support layers, they deal with the physical aspects of moving data from one device to another.

→ Layers 5, 6 and 7 – session, presentation and application thought of as the user support layers.

→ Layer 4, the transport layer, links the two subgroups.

→ Upper OSI layers are implemented in software, lower layers are a combination of hardware and software. except physical layer, which is mostly hardware.

→ The communication process starts at layer 7 then moves from layer to layer in descending, sequential order.

→ At each layer, a header and trailer can be added to the data unit, the formatted data unit passes through application layer to physical layer.

→ Then it is exchanged through transmission media.

→ Upon reaching destination data passes from physical layer to application layer and each time header is droped and the information is passed to upper layers. (Fig 2.3, 2.4 page no. 31, 32)

- Layer's in OSI Model

① **Physical Layer** (Fig. 2.5 physical Layer) page no. 33

→ This layer deals with the functions required to convey a bit stream over physical medium.
→ physical characteristics of interfaces and medium.
→ Representation of bits. ⇒ bits are encoded into signals.
→ Data rate ⇒ the number of bits sent each second.
→ Synchronization of bits
→ Line configuration.
→ physical topology
→ Transmission mode.

② **Data link Layer** (Fig. 2.6 Data Link layer) page no. 34

→ This layer transforms the physical layer, a raw transmission facility, to a reliable link.
→ Framing – the stream of bits received from the network layer into data units called frames.
→ physical Addressing – Addresses at the lower layers will be decided.
→ Flow control – to avoid overwhelming the receiver.
→ Error control – detect duplicate frames, lost frames and retransmit frames
→ Access Control – Decides which device will have control of the link.

③ **Network Layer** (Fig. 2.8 Network layer page no. 36)

→ Is responsible for the source-to-destination delivery of a packet across multiple networks.
→ Logical Addressing →
→ Routing

④ Transport layer (Fig. 2.11 page no. 39)

→ Responsible for process to process delivery of the entire message.
→ service point addressing →
→ segmentation and reassembly
→ Connection control
→ Flow control
→ Error control

⑤ Session layer

→ This layer is a dialog controller. It establishes, maintains and synchronizes the interaction among communicating devices.
→ Dialog Control
→ Synchronization

⑥ Presentation layer

→ This layer is concerned with the syntax and semantics of the information exchanged between two systems.
→ Translation
→ Encryption
→ compression

⑦ Application layer (Fig. 2.14 Application layer page no. 41)

→ It provides user interfaces and support for services.
→ Network virtual terminal.
→ File transfer, access and management
→ Mail services
→ Directory services.

TCP/IP protocol suite (Fig. 2.16 TCP/IP and OSI model page no. 43)

→ TCP/IP protocol suite is made of five layers: physical, data-link, network, transport and application.

→ The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.

→ the three topmost layers in the OSI model, however are represented in TCP/IP by a single layer called the application layer.

→ (1) physical and Data Link layers.

→ At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all standard and proprietary protocols.

→ Network layer:

→ At the network layer, TCP/IP supports the internetworking protocol.

→ IP in turn, uses four supporting protocols ARP, RARP, ICMP & IGMP.

→ IP (Internetworking protocol) – is the transmission mechanism used by the TCP/IP protocol. It is unreliable & connectionless protocol.

→ IP transports data in packets called datagrams, each of which transported seperately.

→ ARP (Address Resolution Protocol) – is used to associate logical address to physical address.

→ RARP (Reverse Address Resolution Protocol) – allows a host to discover its Internet Address when it knows only its physical Address.

→ ICMP (Internet Control Message Protocol) - is a mechanism hosts and gateways to send notification of datagram proble back to the sendee.

→ IGMP (Internet group message Protocol) - is used to facilit the simultaneous transmission of a message to a group of recipients.

→ Transport layer

→ Transport layer represented by two protocols: TCP and UDP

→ SCTP has been devised to meet the needs of some newer applications.

→ UDP (User Datagram Protocol) - is the simplee process-to--process protocol.

→ TCP (Transmission Control Protocol) - provides full transport layer services. TCP is a reliable stream transport protocol.

→ SCTP - (Stream Control Transmission Protocol) provides support for newer applications such as voice over internet.

→ Application layer

→ The application layer is equivalent to the combination of session, presentation and application layers in the osi model.

3, 6

Physical layer

(Fig. 7.1 Transmission medium & physical layer) page no. 191).

Transmission Media

→ A transmission medium can be anything that can carry information from source to a destination.
ex. free space, metallic cable or fiber-optic cable.

→ In telecommunications, transmission media can be divided into two broad categories.

① Guided media – twisted pair cable, coaxial cable and fibre optic cable.

② Unguided media – free space.

(Fig. 7.2 classes of transmission media page. no. 192)

① Guided Media

(A) Twisted-Pair Cable (Fig. 7.3 page no. 193)

→ Twisted-pair cable uses metallic conductors that accept and transport signals in the form of electric current.

→ A twisted pair consists of two copper conductors each with its own plastic insulation, twisted together.

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

→ Twisting of the cable makes it probable that both wires are equally affected by external influences (noise or crosstalk). So the number of twists per unit of length has some effect on the equ quality of the cable.

→ There are two categories of twisted-pair cable.

ⓐ Unshielded

ⓑ shielded

→ the most common twisted-pair cable used in communic... is unshielded twisted-pair.

→ STP cable has a metal foil covering that encases e... pair of insulated conductors which improves the quality of cab...

→ Unshielded twisted-pair cable into seven categories, determine... by cable quality, with 1 as the lowest and 7 as the highest.

→ The most common UTP connector is RJ-45 (registered jack) which is a keyed connector, meaning the connector can be inserted in only one way.

→ The performance of cable is measured by comparing attenuation versus frequency and distance.
(Reduction in amplitude) (the rate over time).

→ Twisted pair cable are used in telephone lines to provide voice and data channels.

→ The DSL lines also uses this cable.

→ LAN such as 10Base-T and 100Base-T also uses this cable.
(10mbps) (100mbps)

(B) Coaxial Cable (Fig. 7.7 page. no. 196)

→ Coaxial cable carries signals of higher frequency than those in twisted pair cable.

→ Coax has a central core conductor of solid wire (copper) enclosed in an insulating sheath which in turn, encased in an outer conductor of metal foil.

→ The outer metallic wrapping serves both as a shield against noise and as the second conductor. This outer conductor is also enclosed in an insulating sheath and the whole cable is protected by plastic cover.

Coaxial cable are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire guage of the inner conductor, the thickness and type of the inner insulator, the construction of the shield and the size and type of the outer casing.

① RG-59 – 75Ω – Cable TV
② RG-58 – 50Ω – Thin Ethernet
③ RG-11 – 50Ω – Thick Ethernet

→ The most common type of connector used is BNC (Bayone-Neil-Concelman) connector. which has three types in that: the BNC connector, the BNC T connector, and the BNC terminator.

→ (a) BNC Connector is used to connect the end of the cable to a device.

→ (b) BNC T Connector used in ethernet networks to branch out to a connection to a computer or other device.

→ (c) BNC terminator is used at the end of the cable to prevent the reflection of the signal.

→ Although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

→ Coaxial cable was widely used in analog telephone networks but now it is used in digital telephone networks also with data up to 600mbps.

→ Traditional cable TV network also used coaxial cable.

→ Common application of coaxial cable is in traditional ethernet LAN's. ① 10Base2 (Thin Ethernet) – RG58 – BNC Connector – 10mbps – 185m
② 10 Base 5 (Thick Ethernet) – RG11 – 10mbps – 5000m

③ Fibre-Optic Cable (Fig. 7.11 & 7.12 page no. 199)

→ A fibre-optic cable is made of glass or plastic and tra... signals in the form of light.

→ Optical fibre uses reflection to guide light through a chann...

→ A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

→ There are two modes of light propogation. (Fig 7.13 page no. 200, 7.14 page no. 201)

Ⓐ Multimode – multiple beams from light source move through the core in different paths. multimode can be implemented in two forms: step-index or graded index.

→ In multimode step-index fiber, the density of the core remains constant from the center to the edges.

→ A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density, this alters the angle of the beam's motion which causes distortion of the signal as it passes through the fiber.

→ The multimode graded-index fiber decrease this distortion of the signal through the cable. In this density is highest at the center of the core and decreases gradually to its lowest at the edge.

(B) single mode

→ This fiber is having much smaller diameter than that of multimode fiber, and with lower density.

→ It uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal.

→ In this case, delays are negligible.

→ optical fibers are defined by the ratio of the diameter of their core to the diameter of their cladding, both expressed in micrometers.

ex. 50/125, 62.5/125, 100/125, 7/125.

→ In typical fiber-optical cable, the outer jacket is made of either PVC or teflon. Inside the jacket are kevlar strands to strengthen the cable. Below the kevlar is another plastic coating to cushion the fiber. The fiber is at the center of the cable, and it consists of cladding and core.

→ There are three connector for fiber-optic cables. The subscriber channel (SC) connector is used for cable TV. The straight-tip (ST) connector is used for connecting cable to networking devices. MT-RJ is a connector that is the same size as RJ-45.

→ Attenuation is ~~such~~ flatter than in the case of twisted-pair cable and coaxial cable. We need fewer repeaters when we use fiber-optic cable.

→ Fiber-optic cable always found in backbone networks.

→ Local-area networks such as 100Base-FX and 1000Base-X uses fiber-optic cable.

Advantages

→ Higher Bandwidth -
→ Less signal attenuation
→ Immunity to electromagnetic interference.
→ Resistance to corrosive materials.
→ Light weight
→ Greater immunity to tapping.

Disadvantages

→ Installation and maintenance
→ Unidirectional light propagation
→ cost.

② Unguided media (Wireless media) (Fig 7.17 page no. 203)

→ Unguided media transport electromagnetic waves without using a physical conductor.
→ Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.
→ Unguided signals can travel from source to destination in several ways. (A) Ground Propagation ⇒ radio waves travel through the lowest portion of the atmosphere.
(B) Sky propagation ⇒ higher frequency radio waves radiate upward where they are reflected back to the earth.
(C) Line of sight propagation ⇒ very high frequency signals are transmitted in straight lines directly from antenna to antenna.
→ We can divide wireless transmission into three broad groups radio waves, micro waves, infrared waves.

Radio Waves

→ electromagnetic waves ranging in frequencies between 3kHz and 1 GHz are called radio waves; and between 1 and 300 GHz are called microwaves.

→ Radio waves, for most part are omnidirectional. when the antenna transmits radio waves, they are propogated in all directions.

→ A sending antenna sends waves that can be received by any receiving antenna.

→ Radio Waves, are particularly those waves that propogate in the sky mode, can travel long distances. ex. AM Radio.

→ Radio Waves, particularly those of low and medium frequencies, can penetrate walls. It is an advantage if the signals are transmitted inside a building and disadvantage if we cannot isolate a communication to just inside or outside a building.

→ This waves are used for multicasting, AM and FM radio, television, maritime radio, cordless phones and paging.

(3) Microwaves

→ electromagnetic waves having frequencies between 1 and 300 GHz.

→ microwaves are unidirectional.

→ The sending and receiving antenna needs to be aligned. A pair of antennas can be aligned without interfering with another pair of aligned antennas.

→ microwave ~~propagation~~ is line of sight.

→ Very high frequency microwaves cannot penetrate walls.

→ The microwave band is relatively wide; almost 299 GHz. Therefore wider subbands can be assigned, and a high data rate is possible.

→ use of certain portion of band requires permission from au
→ microwaves needs unidirectional antennas which is categori as: the parabolic dish and the horn.
→ The parabolic dish antenna is based on the geometry of parabola: Every line parallel to the line of symmetry reflects off the curve at angles such that all the lines intersect in a common point called the focus.
→ The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. outgoing transmissions are broadcast through a horn aimed at the dish.
→ The horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by the curved head. Received transmission are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.
→ microwaves, are useful for unicast communication, they are used in cellular phones, satellite networks and wireless LANs. (fig: 7.21 page. no. 207)

(c) Infrared

→ Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short range communications.
→ Infrared waves, having high frequencies, cannot penetrate walls.
→ This advantageous characteristic prevents interference between one system and another, a short range communication system in one room cannot be affected by another system in the next room.

However, this same characteristic makes infrared signals useless for long range communication.

→ We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

→ The IrDA (Infrared data Association), has established standards for using these signals for communication between devices such as keyboards, mice, PC's, and printers.

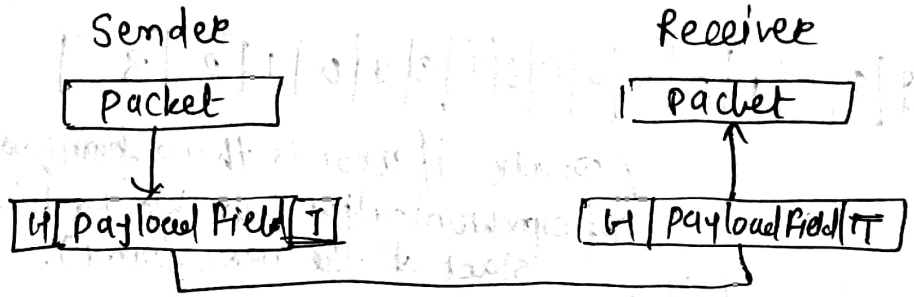
→ This standard originally defined for data rate of 75kbps for a distance upto 8mm. The recent standard defines a data rate of 4mbps.

Data Link Layer (Unit-I)

* Design issues

→ ① services provided to network layer
② framing
③ Error Control
④ flow control

→



} Relation between packets & DLL.

* ① services provided to N/W Layer

(UDP) → unacknowledge connectionless services. — use when error rate is very low

(Data link layer) → acknowledge connectionless service — reliable wireless systems. (wifi). (RUDP).

(TCP) → acknowledge connection oriented service.

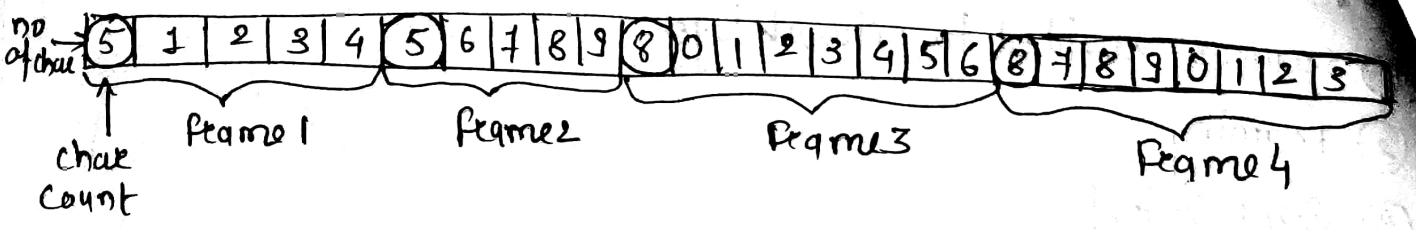
* ② framing

* 4 methods can be used to mark start and end of each frame.
① character count
② flag Bytes with Byte/char stuffing
③ starting & ending flag with bit stuffing
④ physical layer coding violations.

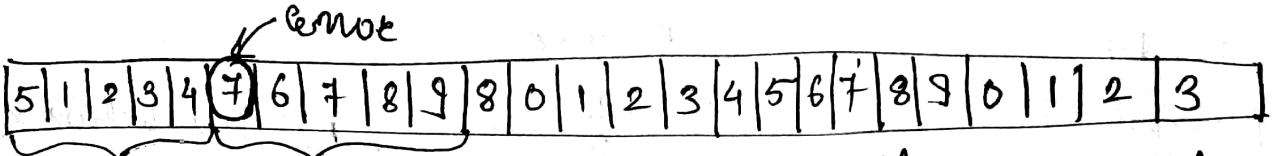
} To make framing secure.

★ ① Character count

(a) Without error (5, 5, 8, 8)



(b) With Errors – one error.



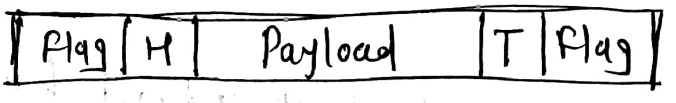
(Disadv - if error is there frame goes out of synchronization & unable to locate the start of the next frame).

★ Flag Bytes with Byte/char stuffing

→ Each frame start an end with special Bytes. – Flag Bytes.

→ If the flag bytes occurs in the frame, stuff an extra escape byte (ESC).

(a) A frame delimited by flag bytes.



Original char				After stuffing				
A	FLAG	B	→	A	ESC	FLAG	B	
A	ESC	B	→	A	ESC	ESC	B	
A	ESC	FLAG	B	→	A	ESC	ESC	ESC	FLAG	B
A	ESC	ESC	B	→	A	ESC	ESC	ESC	ESC	B

(Disadv – Binded to 8-bit character. Not all coding uses 8-bit ex. UNICODE (16-bit))

starting & ending flags with Bit stuffing.

→ each frame begins and ends with a special bit pattern 01111110.

→ when ever the sender sees 5 consecutive 1's, it stuffs 0's.

Eg-(a) The original data.

0110 1111 1111 1111 1111 0010

(b) The data as appear on line.

0110 111110111110111111010010

stuffed bits.

* (4) Physical Layer Coding violations

→ Only applicable to the n/w's in which encoding on the physical medium contains some redundancy.

→ 1011000011 → Before methods.

High low.

→ LAN Coding → one bit - 2 physical Bits.

Eg - manchester encoding → 1 → High-low (10)

0 → Low-High (01)

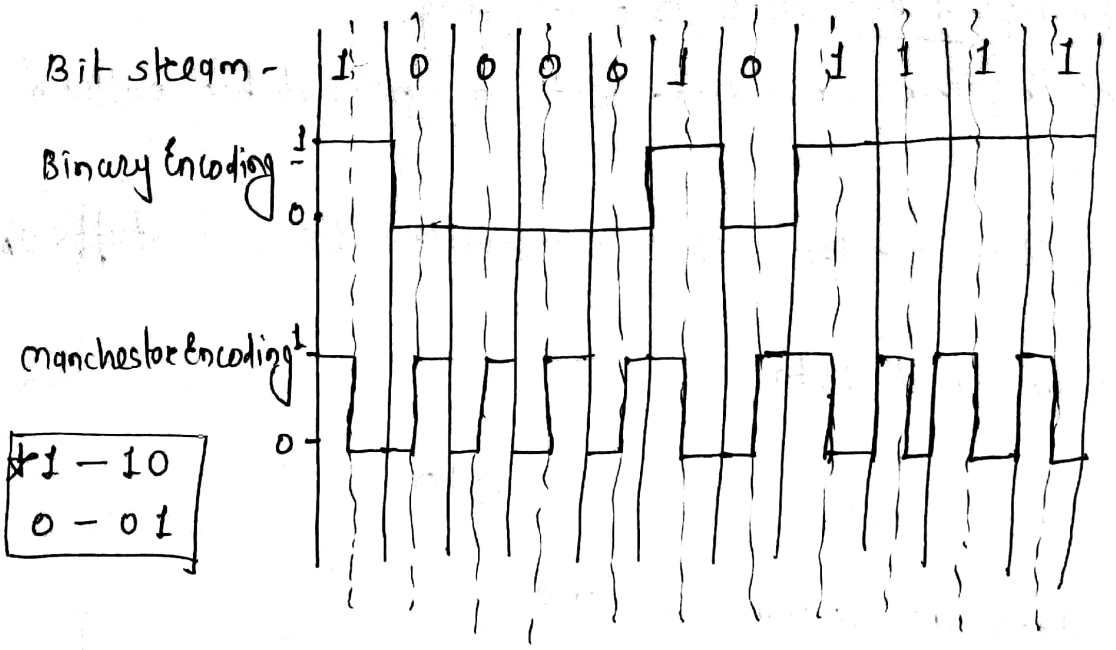
Code Imp Exteq

* manchester encoding

* Bit Period ⟶ Two intervals.

* 1 ⟶ High-low (10)

* 0 ⟶ low-high (01)



1 - 10
0 - 01

③ Error Control

→ After marking the start and end of each frame, we come to the next problem, how to make sure all frames are delivered to the n/w layer at the destination and in the proper order.

→ Suppose sender is just sending the frames without keeping track of it, then it is fine for unacknowledged connectionless service, but not for reliable, connection oriented service.

→ So as a solution we are having acknowledgement mechanism. in which ~~receiver~~ will send positive or negative feedback. If it is positive, sender knows the frame has arrived safely. on the other hand, a negative feedback means something is wrong and frame is transmitted again.

→ An additional complication comes that a frame may lost because of hardware troubles, in this case receiver will not react at all. So we need to introduce timers.

→ The timer is set to expire after an interval long enough for the frame to reach the destination, processed there and to send the ack back to the sender.

→ If timer expires, and ack is not received, frames will be transmitted again.

However, when frames may be transmitted multiple times there is a danger that the receiver will accept same frame multiple times and pass it to the n/w layer more than once.

→ So, the next soln applied is to assign sequence nos. to outgoing frames, so that receiver can distinguish between the retransmitted frames.

* (4) Flow Control

→ After a frame is error free also, sometimes if sender and receiver are not capable of operating at same data rate, then there is a chance of loss of data.

→ Two approaches are commonly used.

① Feedback based Flow Control – the receiver sends feedback giving sender a permission to send more data and telling how receiver is doing.

② Rate-Based Flow Control – the protocol has a built-in mechanism that limits the rate at which senders may transmit data.

* CRC (Cyclic Redundancy Check)

① Bit string → polynomials with coeff. of 0 and 1 only.
② modulo 2 arithmatic → XOR.
③ Generator Polynomial → G(x).
④ sender → bit seq → FCS (frame check sequence) / CRC code.
⑤ FCS → M(x)/G(x). divisor.
(Remainder) (Data)

⑥ Receiver → Data + CRC / G(X)

if there is no remainder.

= 0 - zero

= No error

= Data Accepted.

otherwise = Error = Rejected.

* Eg. Data = 100100

Gen = 1101 = 4

Redundant = 4 - 1 = 3 bits

Quotient → 11101

1101 | 100100000

XOR → 1101

0 1000

1101

Sender ⇒ 0 1010

1101

0 1110

1101

0 0110

if this bit is 0 → 0000

→ key = 0000

0 1100

1101

0 001 ← Remainder.

↓

Original Data + Remainder

= 100100 + 001

⇒ To the receiver key.

Receiver ⇒

XOR	0	1
0	0	1
1	1	0

11101

1101 | 100100001

1101

0 1000

1101

0 1010

1101

0 1110

1101

0 0110

0000

0 1101

1101

0 000

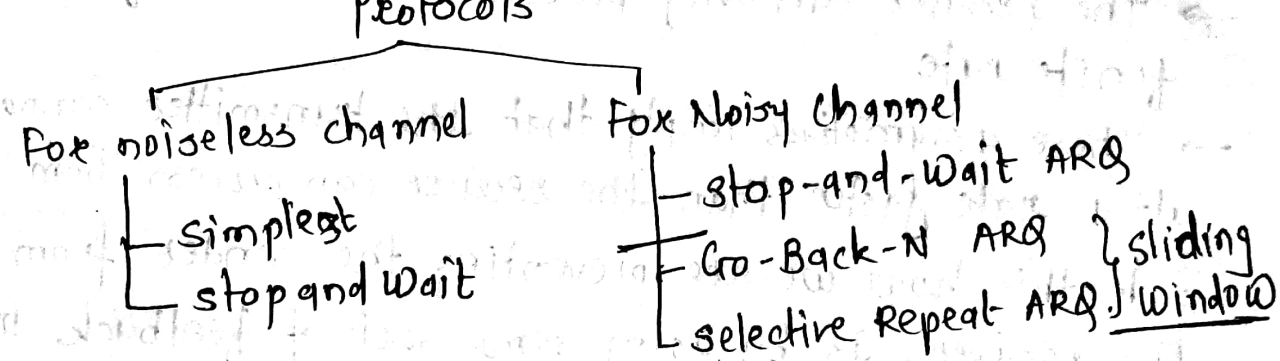
↓↓

No Error

= Accepted.

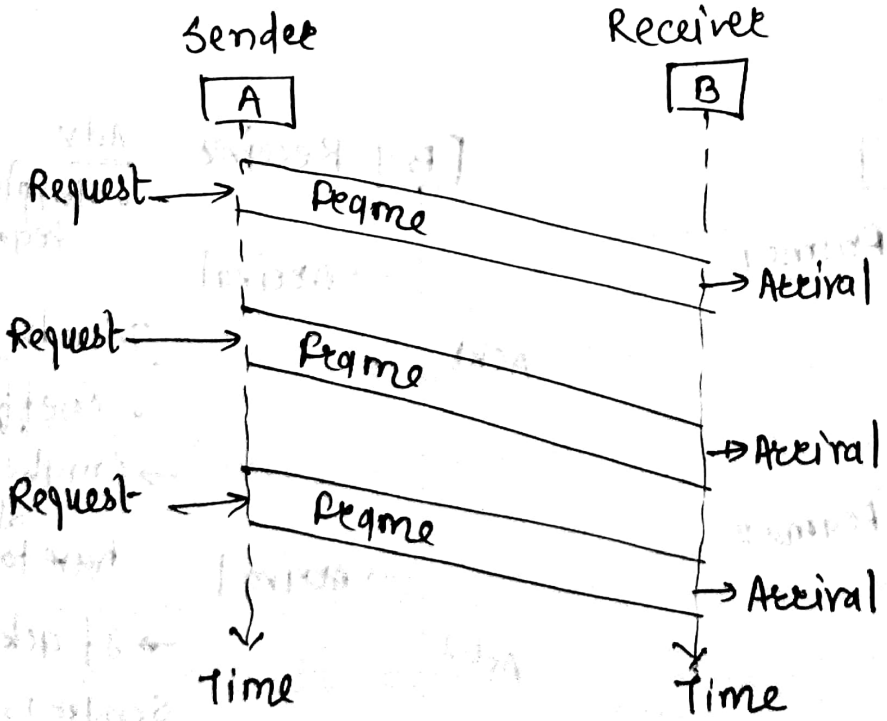
Elementary Data Link Protocols (Unit I)

→ this protocols are normally implemented in s/w by using one of the common programming languages.



① An Unrestricted Simplex Protocol (Fig 11.6 page.no.313)

→ Data are transmitted in one direction only.
→ The transmitting and receiving hosts are always ready.
→ Processing time can be ~~ig~~ ignored.
→ Infinite buffer space is available.
→ No errors occur; i.e; no damaged frames and no lost frames.



⇒ (Disadvantage - Flooding)

(2) A simplex STOP-AND-WAIT Protocol (Fig. 11.8 page no. 316)

→ We assume that Data are transmitted in one direction

→ No errors occur.

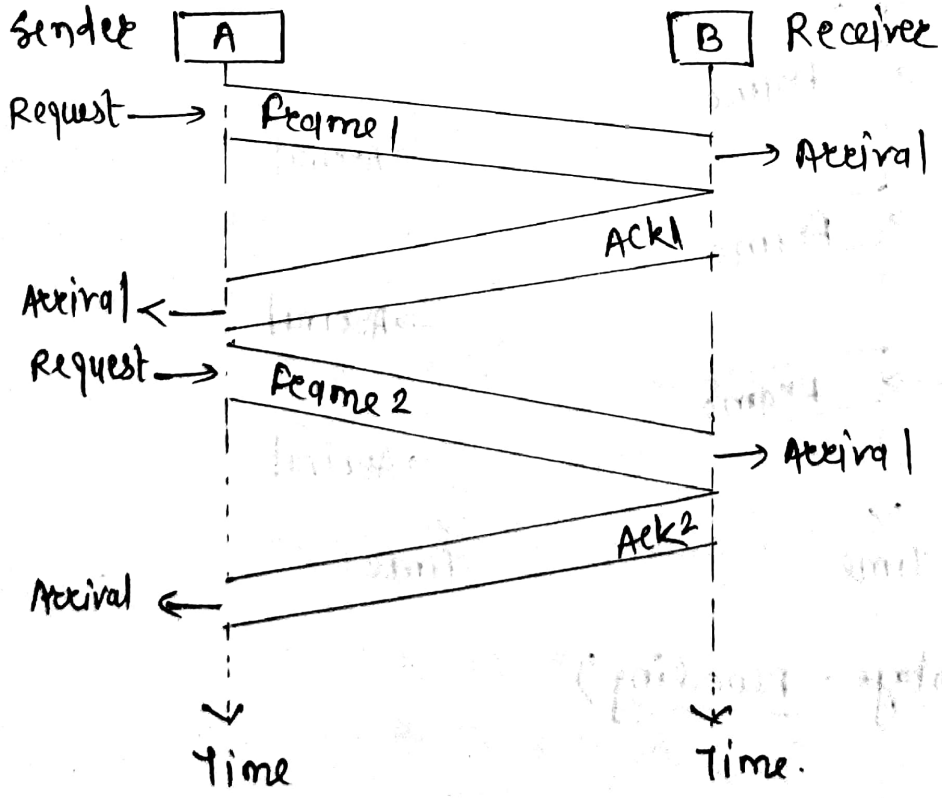
→ The receiver can only process the received information at a finite rate.

→ These assumptions imply that the transmitter cannot send frames at a rate faster than the receiver can process them.

→ In this how we are preventing the sender from flooding the receiver, is by using some sort of feedback to the sender.

→ The receiver send an acknowledge frame back to the sender telling the sender that the last received frame has been processed and passed to the host; permission to send the next frame is granted.

→ The sender, after having sent a frame, must wait for the acknowledge frame from the receiver before sending another frame.



Adv
- simple reliable transmission

Disadv
- inefficient
→ (makes the system slow as we have to wait for Ack)
→ If ack is lost sender is not able to send data anymore

Fig: STOP and WAIT protocol

3) STOP and WAIT protocol for Noisy Channel (ARQ - Automatic Repeat request) (Fig 11.10 page no 359)

→ In this protocol frames may be either damaged or lost completely.

→ The sender would send a frame, the receiver would send an Ack frame only if the frame is received correctly. If the frame is in error the receiver simply ignores it, the transmitter would time out and would retransmit it.

→ One fatal flaw with the above scheme is that if the Ack frame is lost or damaged, duplicate frames are accepted at the receiver without the receiver knowing it.

→

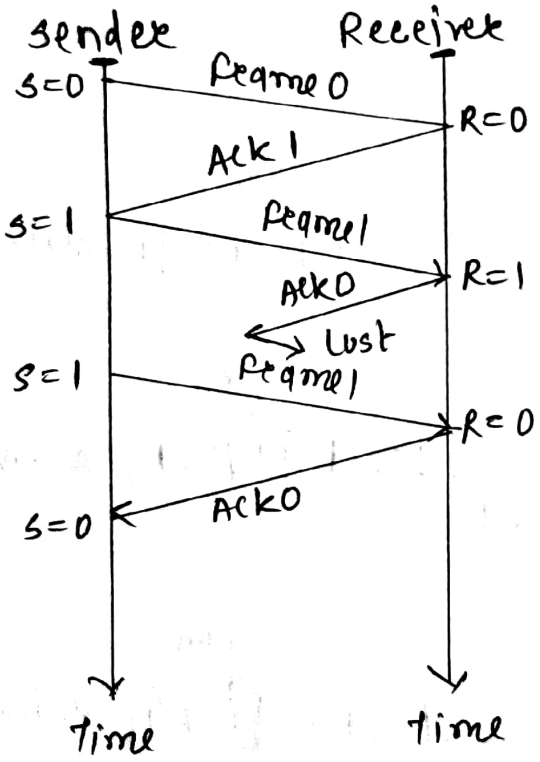


Fig: STOP & WAIT, Lost Ack frame

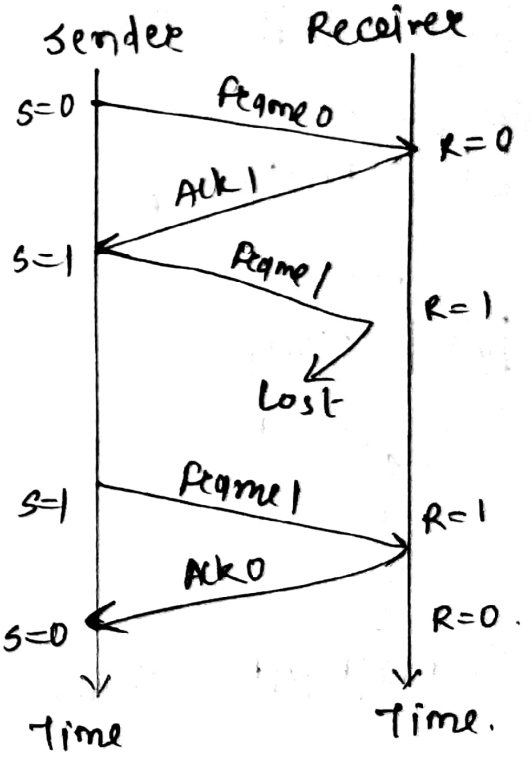


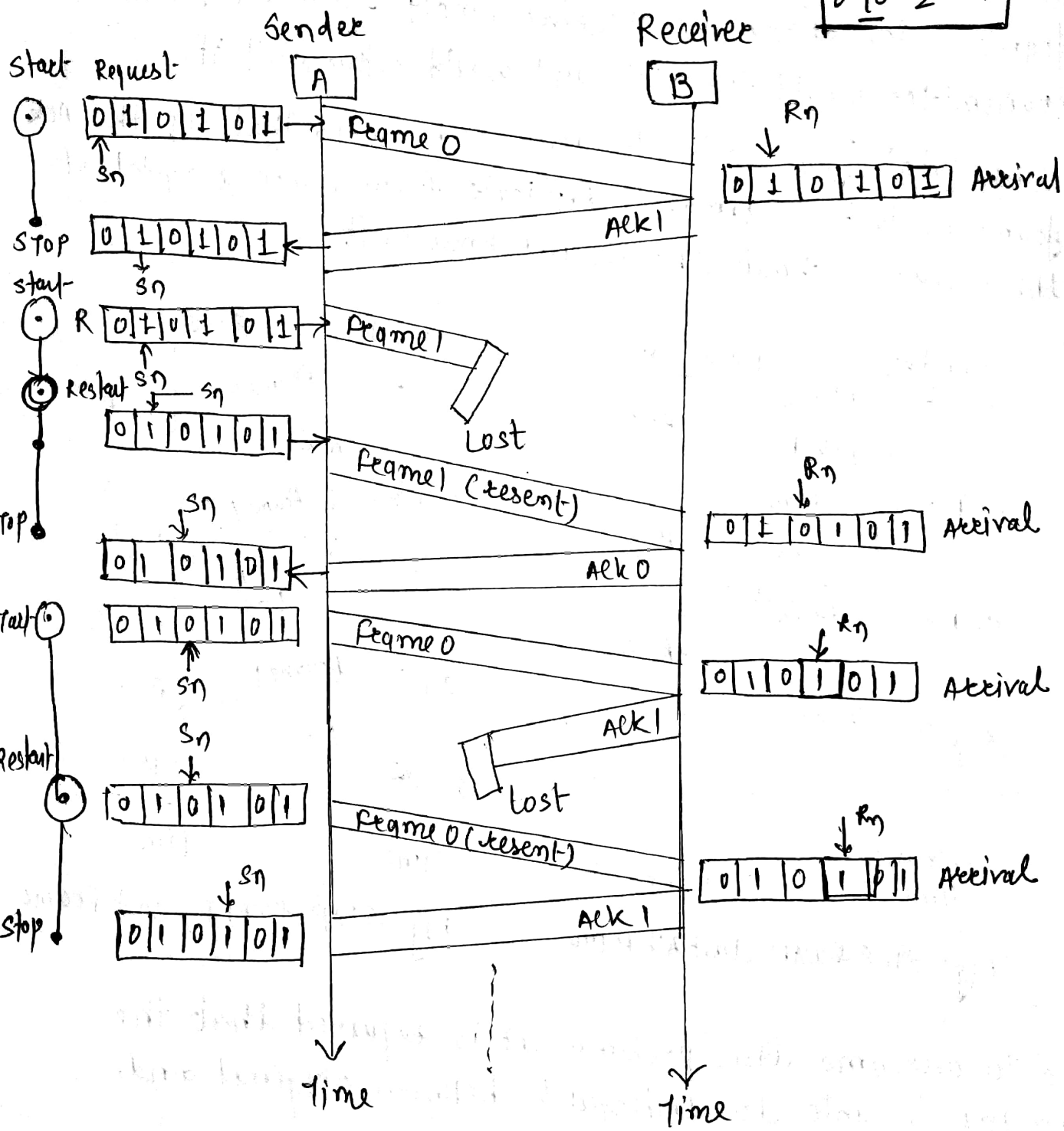
Fig: STOP & WAIT, Lost Frame.

→ To overcome this problem it is required that the receiver be able to distinguish between original and retransmitted frame.

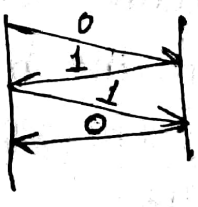
→ One way to achive this is to have the sender put a sequence number in the header of each frame it sends. The receiver the check the sequence number to see if it is new or duplicate frame.

→ the receiver needs to distinguish only 2 possibilities o... Back
or duplicate frame; a 1-bit sequence number is suffic... Slide
→ After receiving the correctly numbered frame, the expect... sequence number is incremented by 1.

* Sequence no. m bit
0 to $2^m - 1$



*(Note - this will achieve both error and flow control).



0 1 1

0	1
1	0

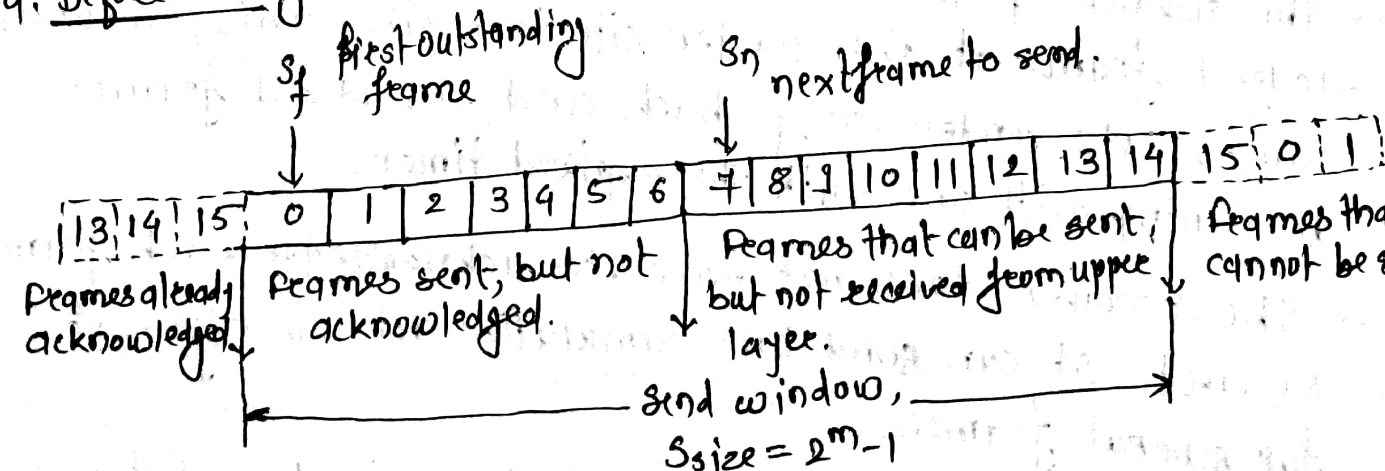
Go Back-N ARQ

* Sliding Window Protocol

* sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames.
* In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver.
* The term sliding window refers to the imaginary boxes to hold frames. That boxes defines the range of sequence numbers.
* the sender's window is an box covering the sequence numbers of the data frames which can be in transit.
* the receivers window is an box covering the sequence numbers of the data frames which are acknowledge correctly.
* If the header of the frame allows m bits for the sequence number, the sequence numbers range from 0 to $2^m - 1$. for eg. if m is 4, the only sequence numbers are 0 through 15. we can repeat the sequence.

* Sliding Window (Go-Back N ARQ) (Diq: 11:14 Design of Go-Back-N ARQ page no. 327).

a. Before sliding



b. after sliding

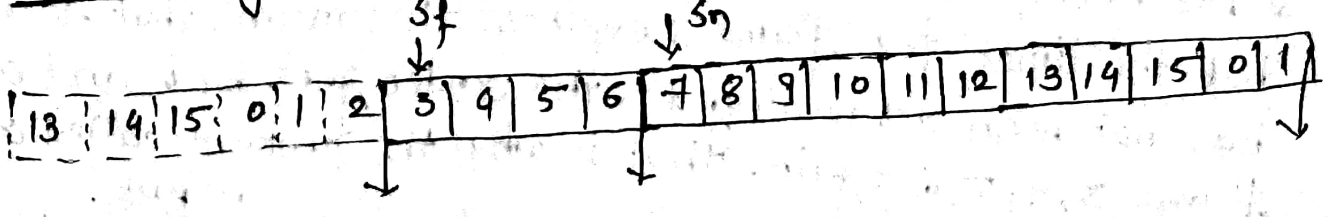
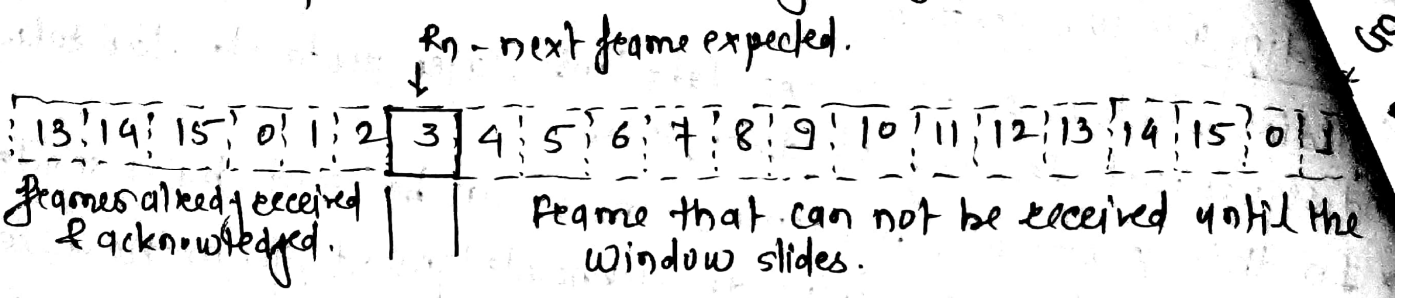
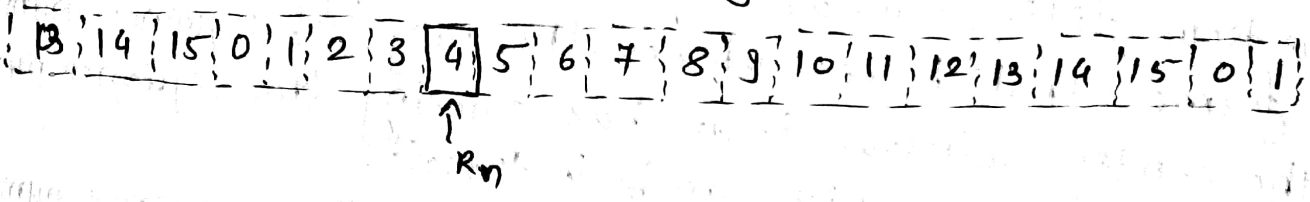


Fig: Send Window

* The acknowledgments in this case are cumulative, meaning more than one frame can be acknowledged by an Ack frame.



a. Before sliding.



b. after sliding.

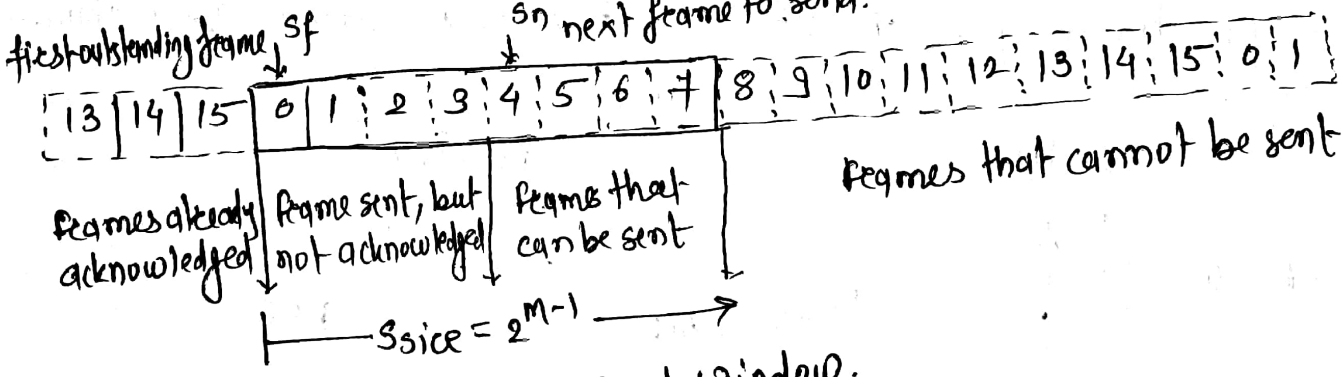
Fig: Receive window.

* The size of the receive window is always 1.
* The receiver sends a positive acknowledgement if a frame has arrived safe and sound and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives one it is expecting.
* The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire. This, in turn, causes the sender to go back and resend all frames, beginning with one with the expired timer.
* The receiver does not have to acknowledge each frame received. It can send one cumulative acknowledgement for several frames.
* For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frame 3, 4, 5, 6 again. That is why the protocol called Go-Back-N ARQ.

(Note: Stop-and-Wait ARQ is a special case of Go-Back-N ARQ in which the size of the window is 1).

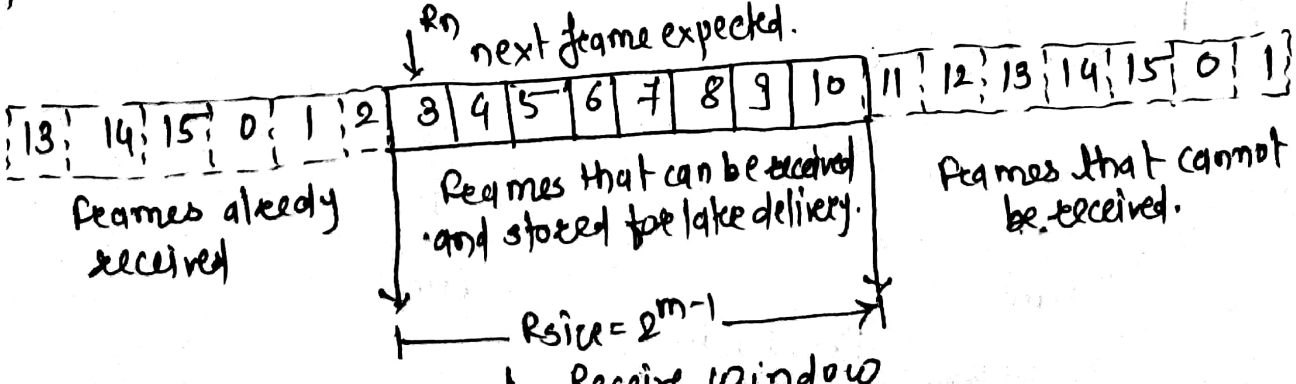
* Selective Repeat Automatic Repeat Request. (Dia. Design of selective Repeat ARQ) 11:20 page no. 334

* Go-Back-N ARQ simplifies the process at the receiver site, still this protocol is very inefficient for a noisy link.
* for noisy links, a frame has a higher probability of damage, which means the resending of multiple frames. this resending uses up the bandwidth and slows down the transmission.
* There is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent. this mechanism is called selective Repeat ARQ.
* this protocol also uses two windows: a send window and a receive window. First the size of the send window is much smaller; it is 2^{m-1}. Second, the receive window is the same size as the send window.
* for example, if m=4, the sequence numbers go from 0 to 15, but the size of the window is just 8.



a. Send window.

* As the sizes of the send window and receive window are the same, all the frames in the send ~~frame~~ window can arrive out of order and be stored until they can be delivered.



b. Receive window

* Piggbacking

→ All three protocols are unidirectional, in real life data frames are normally flowing in both directions.

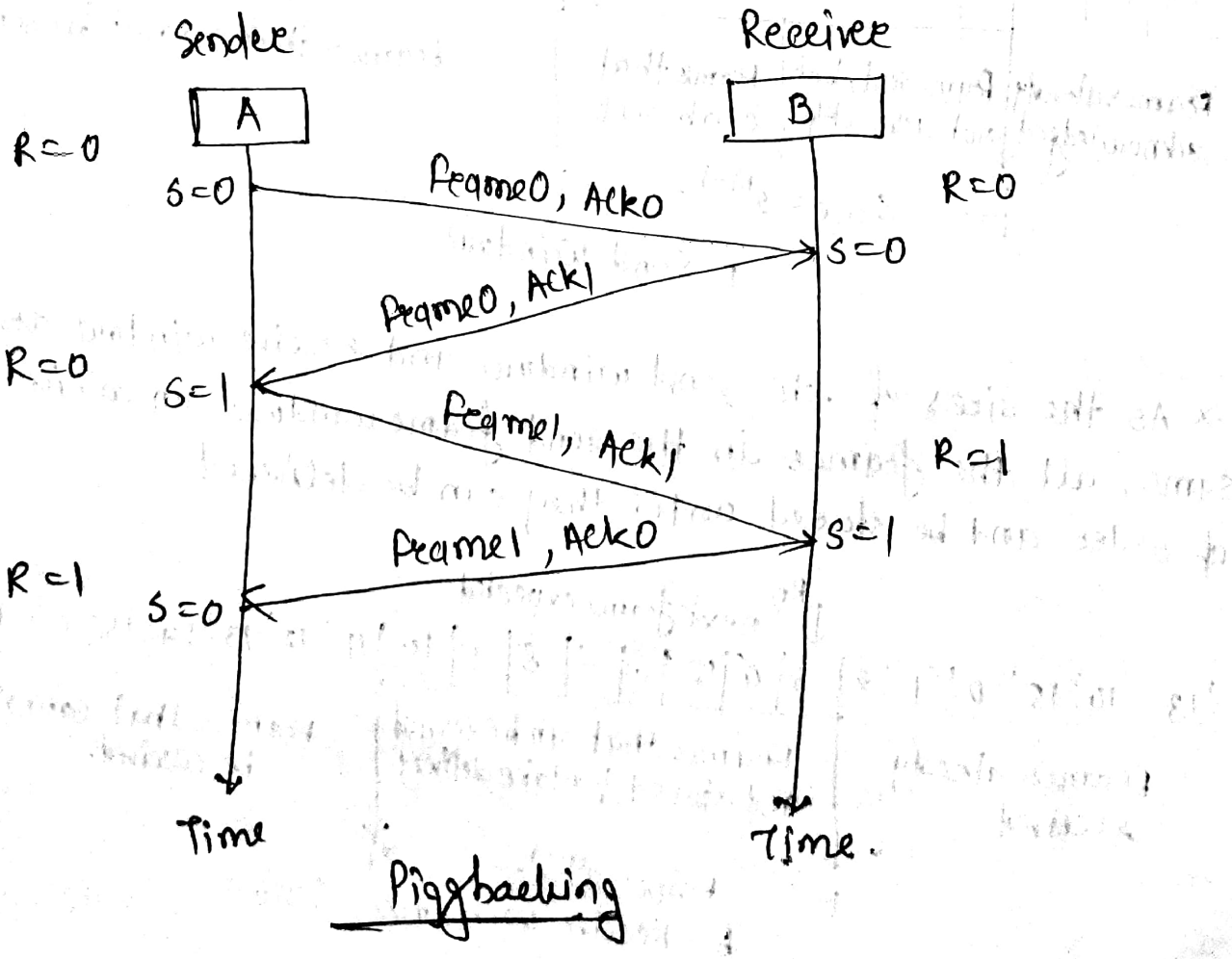
→ This means that control information also needs to flow in both directions.

→ A technique called piggybacking is used to improve the efficiency of the bidirectional protocols.

→ When a frame is carrying data from A to B, it can also carry control information about arrived frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived frames from A.

→ Each node now in this case has two windows: one send window and one receive window. Both also needs to use a timer.

→ In piggbacking both sites must use the same algorithm.



Piggbacking