UNIT- I

INTRODUCTION TO DATA COMMUNICATION

Introduction:-

communication is defined as the exchanging of the information b/w individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term telecommunication, which includes telephony, telegraphy & television.

The word data refers to information presented in whatever form is agreed upon by the parties creating & using the data.

Data communication are the exchange of data between two devices via some form of transmission medium such as wire cable.

The effectiveness of data communication system depends on four fundamental characteristics.

1. Delivery
2. Accuracy
3. Time liness
4. Jitter

1. Delivery:- The system must deliver data to the correct destination. Data must be received by the intended device or user & only by that device or user.

Scanned by TapScanner

2. Accuracy :- The system must deliver the data accurately. Data that have been altered in transmission & left uncorrected are unusable.

3. Timeliness :- The system must deliver data in timely manner. data delivered late are useless.

4. Jitter :- It reffers to the variation in the packet arrival time. it is the uneven delay in the delivery of audio or video packets.

→ Components :-

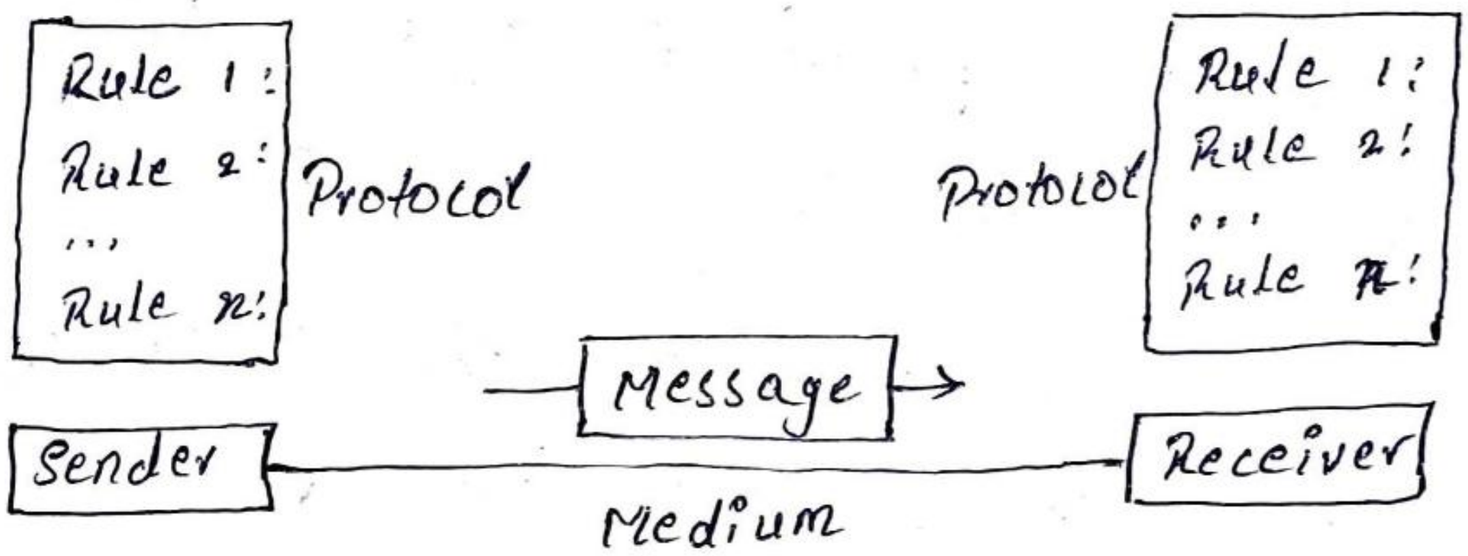


fig :- components of data communication

A data communications system has five components.

1. Message
2. Sender
3. Receiver
4. Transmission medium
5. Protocol

1. Message :- It is the information to be communicated. information can include text, numbers, pictures, audio & video.

Scanned by TapScanner

2. Sender:- Sender is the device that sends the data message. It can be a computer, work station, telephone handset, & so on.

3. Receiver:- The receiver is the device that receives the message.

4. Transmission medium:- It is the physical path by which a message travels from sender to receiver. eg:- coaxial cable, fiber-optic cable, etc.,

5. Protocol:- it is set of rules that govern data communications. It represents an agreement b/w the communicating devices.

→ Data Representation:-

Information today comes in different forms such as text, numbers, images, audio & video.

Text:- In data communications, text is represented as a bit pattern, a sequence of bits (0's or 1's). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, & the processing of representing symbol is called coding. today the prevalent coding system is called unicode, which uses 32 bits to represent a symbol or character used in any language in the world. the American Standard code for information interchange (ASCII), developed some decades ago in

Scanned by TapScanner

the US, now constitutes the first 127 characters in unicode & is also referred to a basic latin.

Numbers:- numbers are also represented by bit patterns. However a code such as Ascii is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations.

Images:- Images are also represented by bit pattern's. in its simplest form, an image is composed of matrix of pixels, where each pixel is a small dot. the size of the pixel depends on the resolution.

for eg. an image can be divided into 1000 pixels or 10,000 pixels, In the second case, there is better representation of the image, but more memory is needed to store the image.

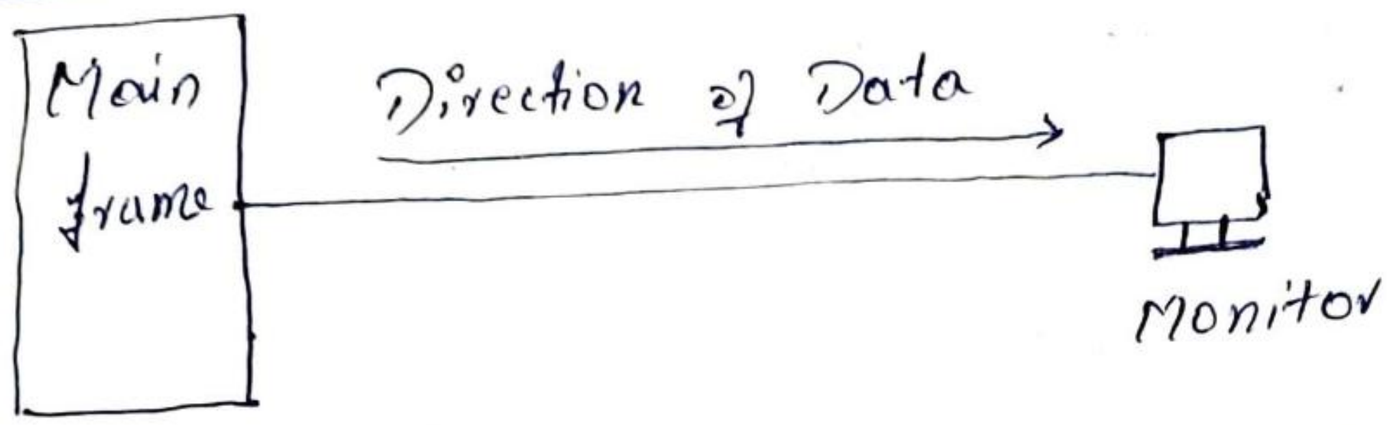
Audio:- It refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continious not discrete. even when we use a uphone to change voice or music to an electric signal we create a continious signal.

Video:- It refers to the recording or broadcasting of a picture or movie.

Scanned by TapScanner

→ Data flow :- communication b/w two devices can be simplex, half-duplex or full-duplex as shown.

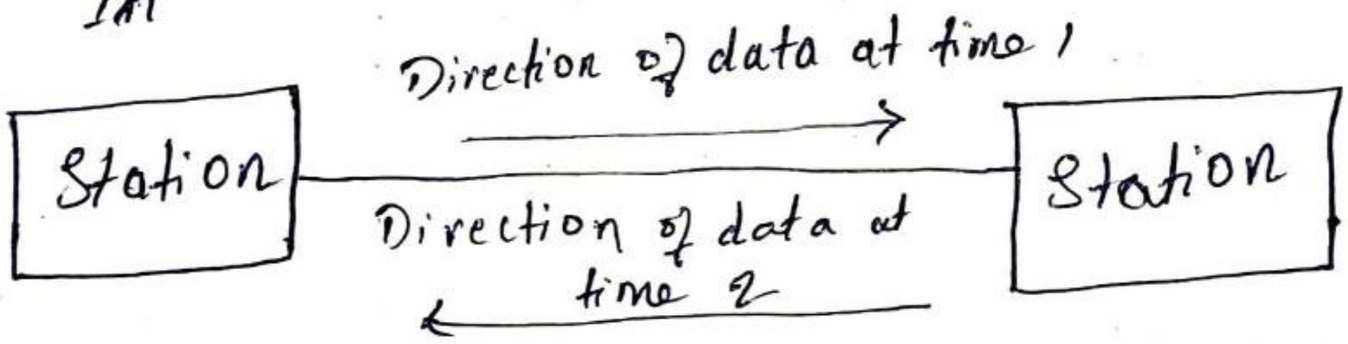
Simplex :-



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

keyboards & traditional monitors are examples of simplex devices.

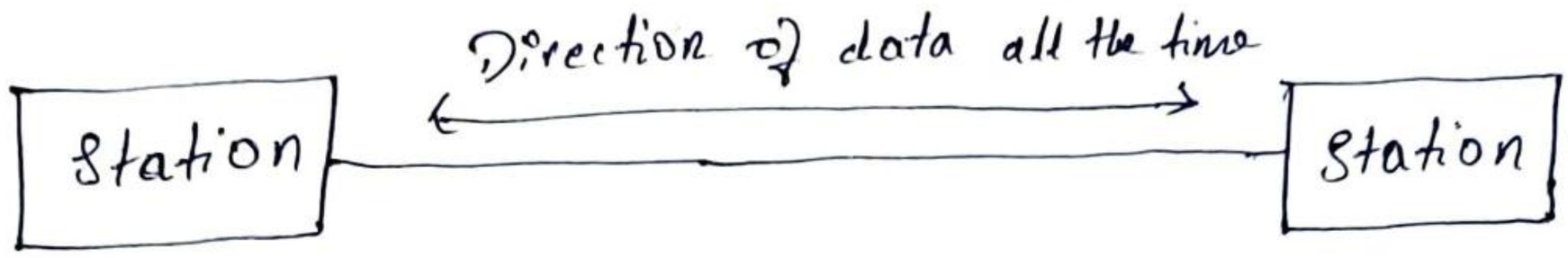
Half duplex :-



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

Scanned by TapScanner

full duplex :-



In full duplex mode both stations can transmit & receive simultaneously.

one common eg. of full-duplex communication is the telephone network. when two people are communicating by a telephone line, both can talk & listen at the same time.

The full-duplex mode is used when communication in both directions is required all the time. the capacity of the channel, however must be divided between the two directions.

→ Networks :-

A network is a set of devices connected by communication links. A node can be a computer, printer or any other device capable of sending and/or receiving data generated by other nodes on the network.

* Distributed Processing :- Most n/w's use distributed processing, in which a task is divided among multiple computers. instead of one single

Scanned by TapScanner

large machine being responsible for all aspects of a process, seperate computers handle a subset.

* Network criteria:-

A network must be able to meet a certain number of criteria. The most important of these are (1) performance
(2) Reliability
(3) security

(1) performance:- It can be measured in many ways, including transit time & response time. transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between and inquiry & response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware & the effeciency of the software.

performance is evaluated by two networking metrics: throughput & delay. we often need more throughput & less delay.

Scanned by TapScanner

② Reliability :- In addition to accuracy of delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure & the n/w's robustness in a catastrophe

③ Security :- It include protecting data from un authorized access, protecting data from damage and development & implementing policies & procedures for recovery from breaches of data losses.

* Physical structures :-

Type of connection: A n/w is two or more devices connected through links. A link is a communication pathway that transfers data from one device to another.

There are two possible types of connections

① point to point

② Multi point

① point to point :- It provides a dedicated link b/w two devices. the entire capacity of the link is reserved for transmission b/w those two devices. Most point-to-point connections use an actual length of wire or cabel to connect the two ends.

Scanned by TapScanner

fig:- point to point

② Multipoint:-

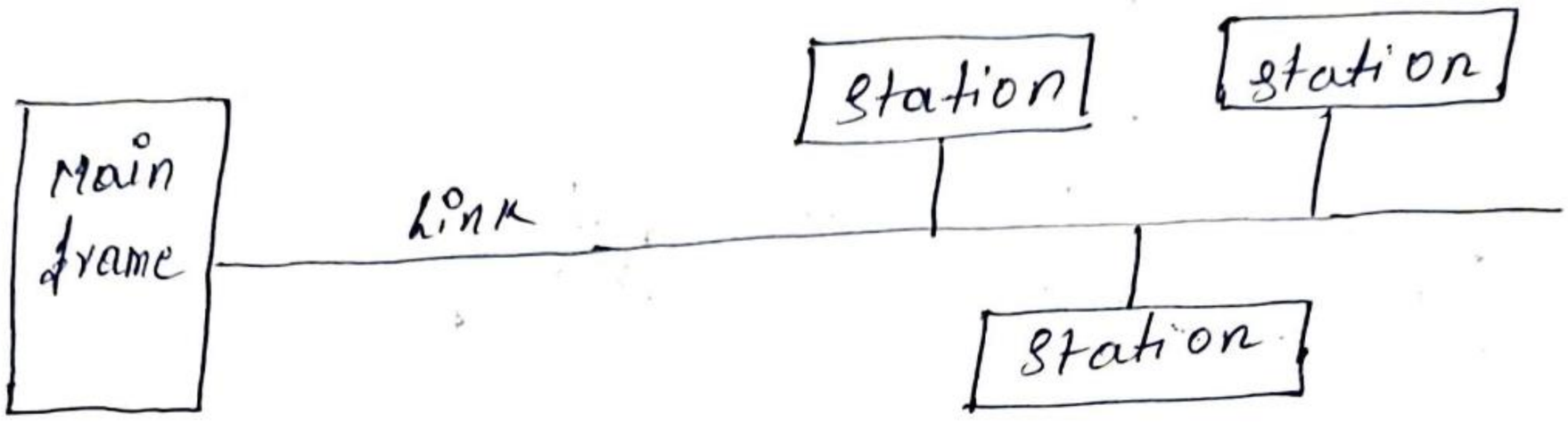


fig:- Multipoint

It is one in which more than two specific devices share a single link

In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. if several devices can use the link simultaneously, it is a spatially shared connection. if user must take turns, it is a time shared connection.

⇒ Physical topology:- It 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 n/w is geometric representation of the relationship of all the links & linking devices to one another. these are four basic topologies

Scanned by TapScanner

① Mesh

② Star

③ Bus

④ Ring

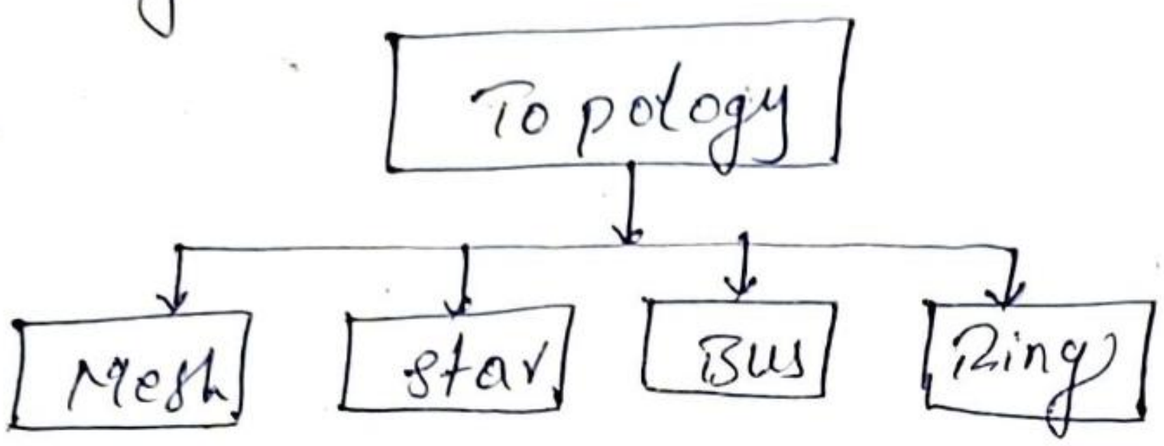


fig:- categories of topology.

① mesh topology

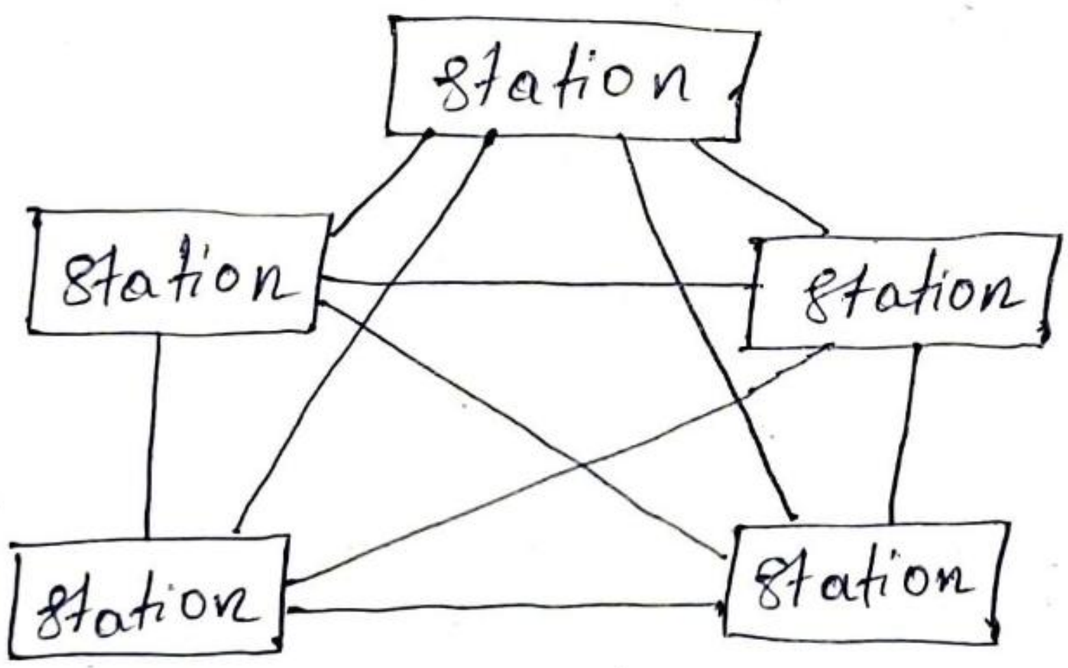


fig:- fully connected mesh topology

In a mesh topology, every device has a dedicated point-to-point link to every other device the term dedicated means that the line carries traffic only b/w the two devices it connects. to find the number of physical links in a fully connected mesh n/w with n nodes, we first consider that each node must be connected to every node.

Scanned by TapScanner

node 1 must be connected to n-1 nodes, & ~~so on~~ same for remaining. we need n(n-1) physical links. However, if each physical link allows communication in both directions. we can say that in a mesh topology, we need

$$\boxed{n(n-1)/2}$$

duplex-mode links.

As shown in the figure to accommodate that many links, every device on the n/w must have n-1 input/output ports to be connected to the other n-1 stations.

A mesh offers several advantages over other n/w topologies. first, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when link must be shared by multiple devices.

second, a mesh topology is robust. if one link becomes unusable, it doesnot incapicate the entire system.

third, there is the advantage of privacy & security.

finally point-to-point link makes fault identification & fault isolation easy..

Scanned by TapScanner

The main disadvantage of a mesh are related to the amount of cabling & the number of I/O ports required.

② Star topology :-

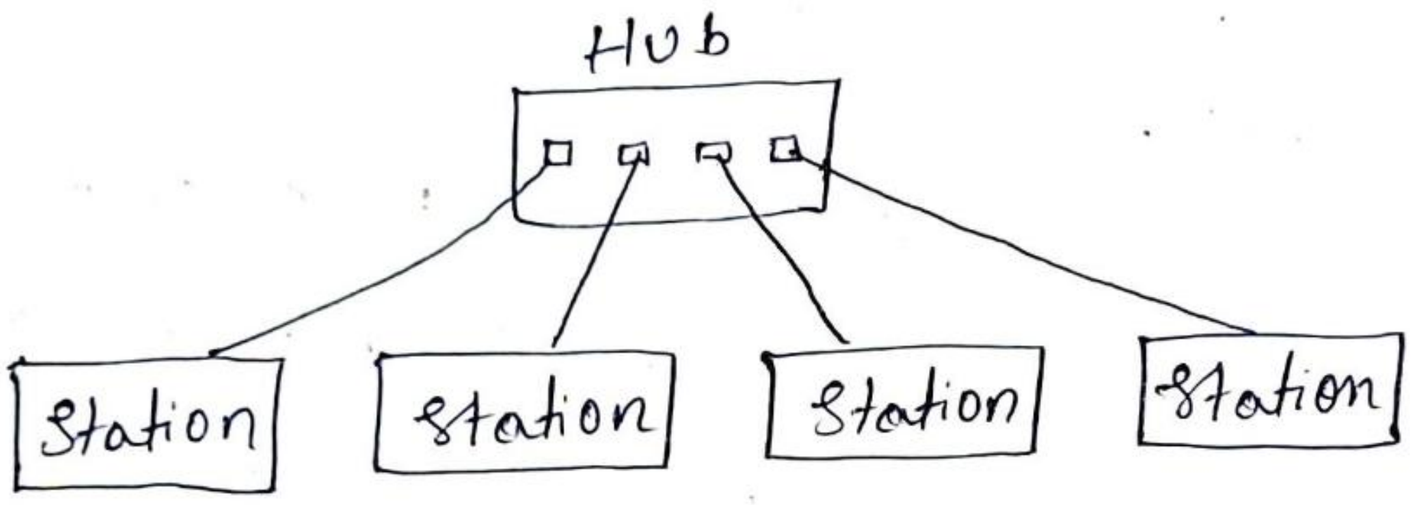


Fig:- Star topology connecting for Stations

In this 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 doesnot allow direct traffic b/w devices. the controller acts as an exchange: if one device want to send data to another, it sends the data to the controller, which then relays the data to the other connected devices.

A star topology is less expensive than a mesh topology.

other advantage is include robustness. If one link fails, only that link is affected.

Scanned by TapScanner

Disadvantage of the star topology is the depedency of the whole topology on one single point, the hub. if hub goes down the whole system is dead.

3 Bus topology :-

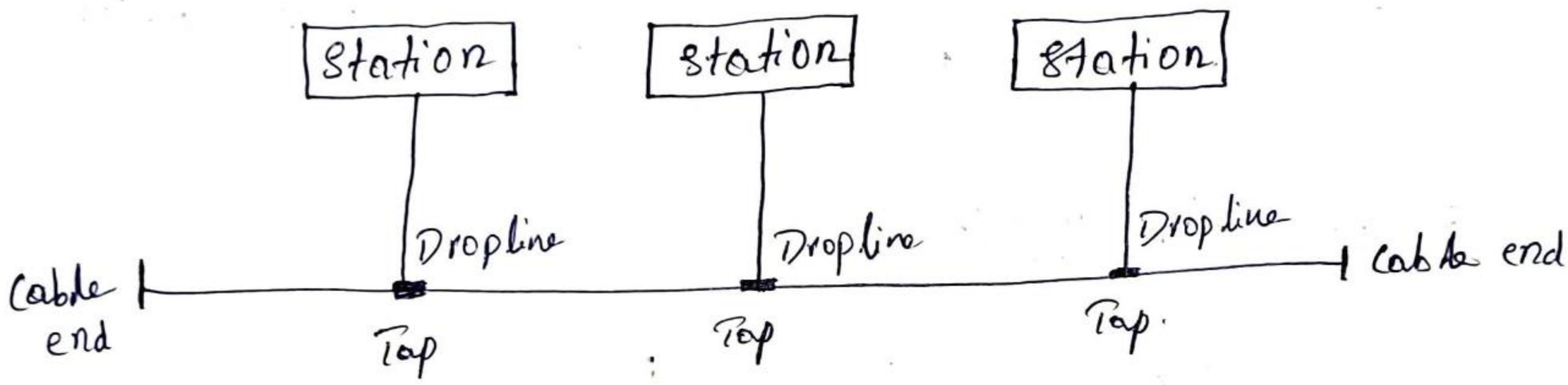


fig:- Bus topology connecting 3 stations.

A bus topology is a multipoint. one long cable acts as backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines & taps. A drop line is a connection running between the device & 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 & weaker as it travels farther & farther.

Scanned by TapScanner

Advantage :-

→ Ease of installation

→ Back bone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.

Disadvantage :-

→ Difficult reconnection of fault isolation

④ Ring topology :-

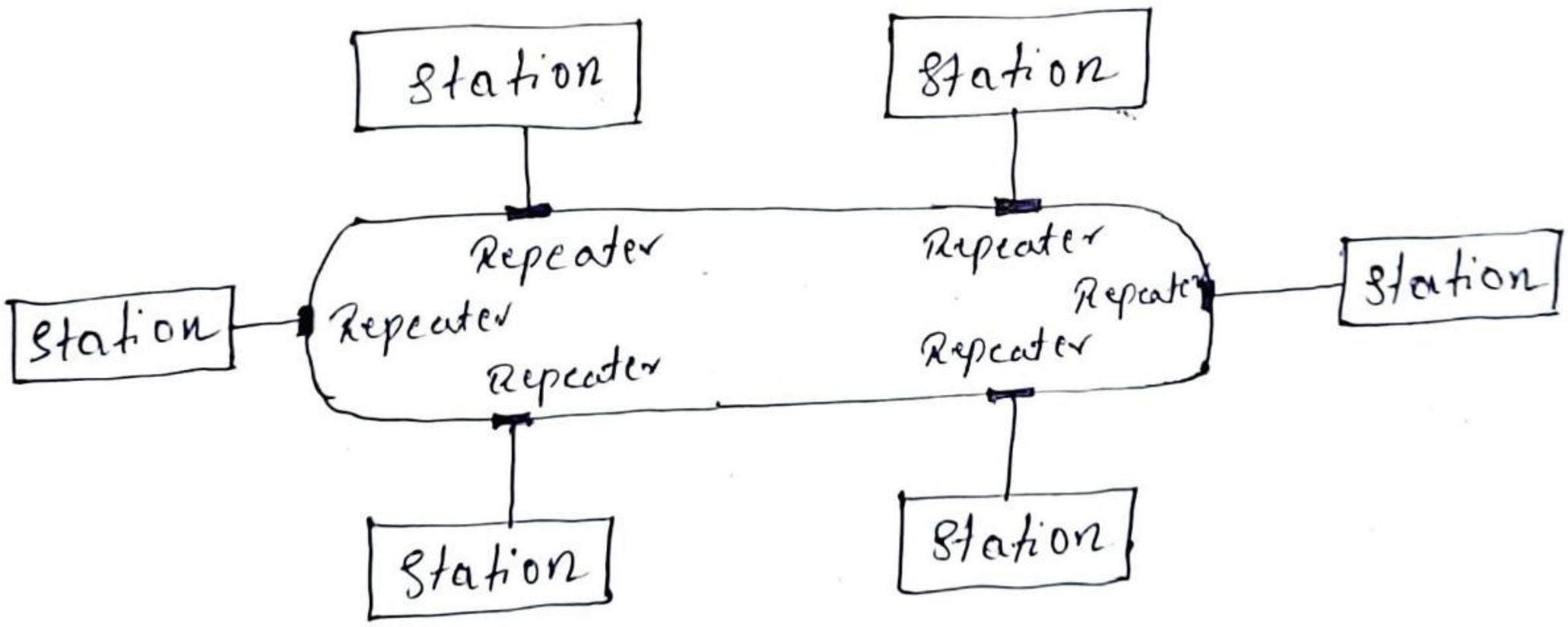


fig:- Ring topology connecting six stations

In 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.

Scanned by TapScanner

when a device receives a signal intended for another device, its repeater regenerates the bits & passes them along.

A ring is relatively easy to install & reconfigure. each device is linked to only its immediate neighbors. To add or delete a device requires changing only two connections.

5 Hybrid Topology :-

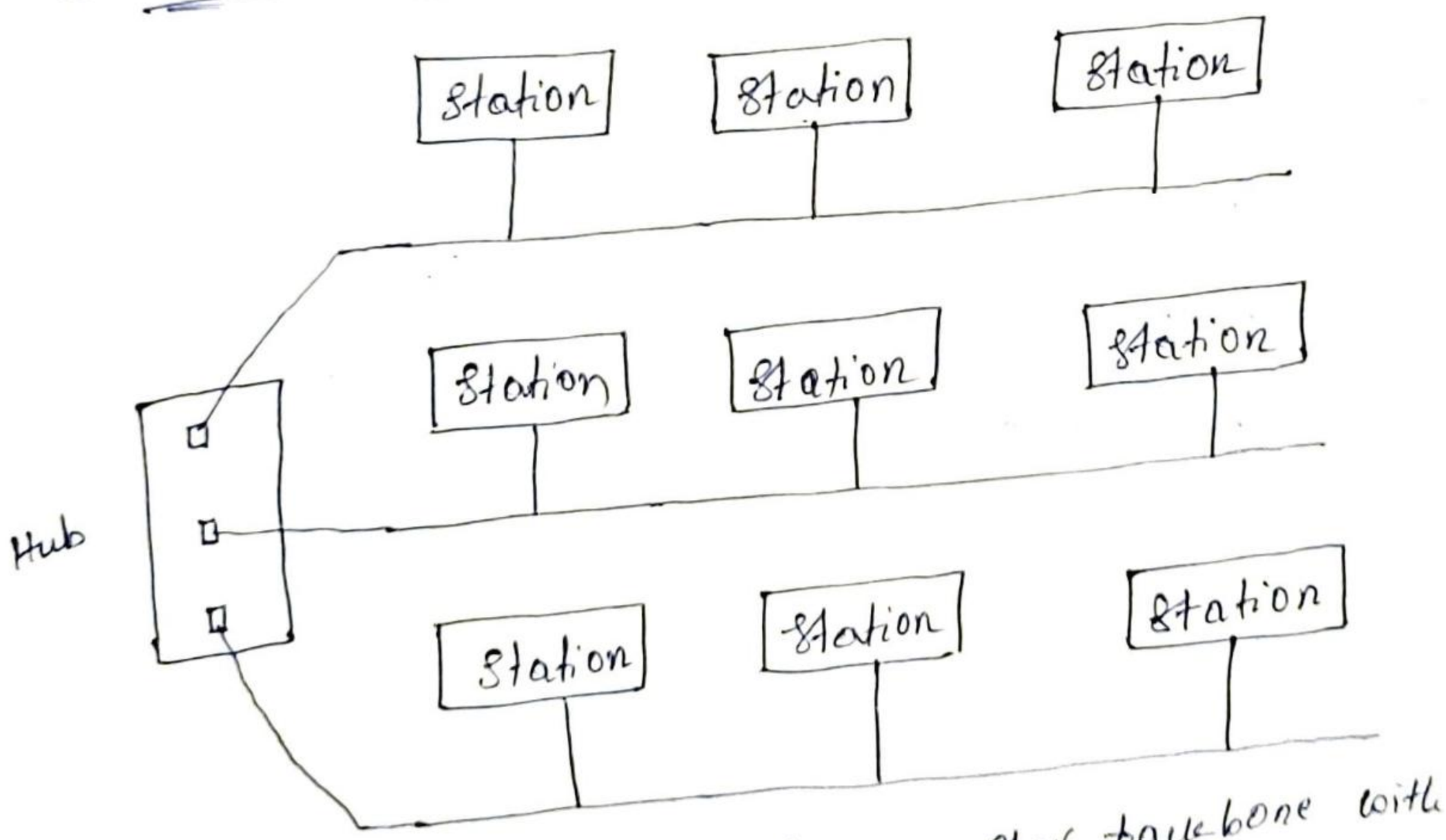


fig :- hybrid topology : a star backbone with three bus networks

Hybrid topology can be formed by connecting two or more topologies together.

Scanned by TapScanner

→ Network models

Computer n/w's are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another. the two best known standard are

① OSI model

② Internet model.

⇒ Categories of Network:-

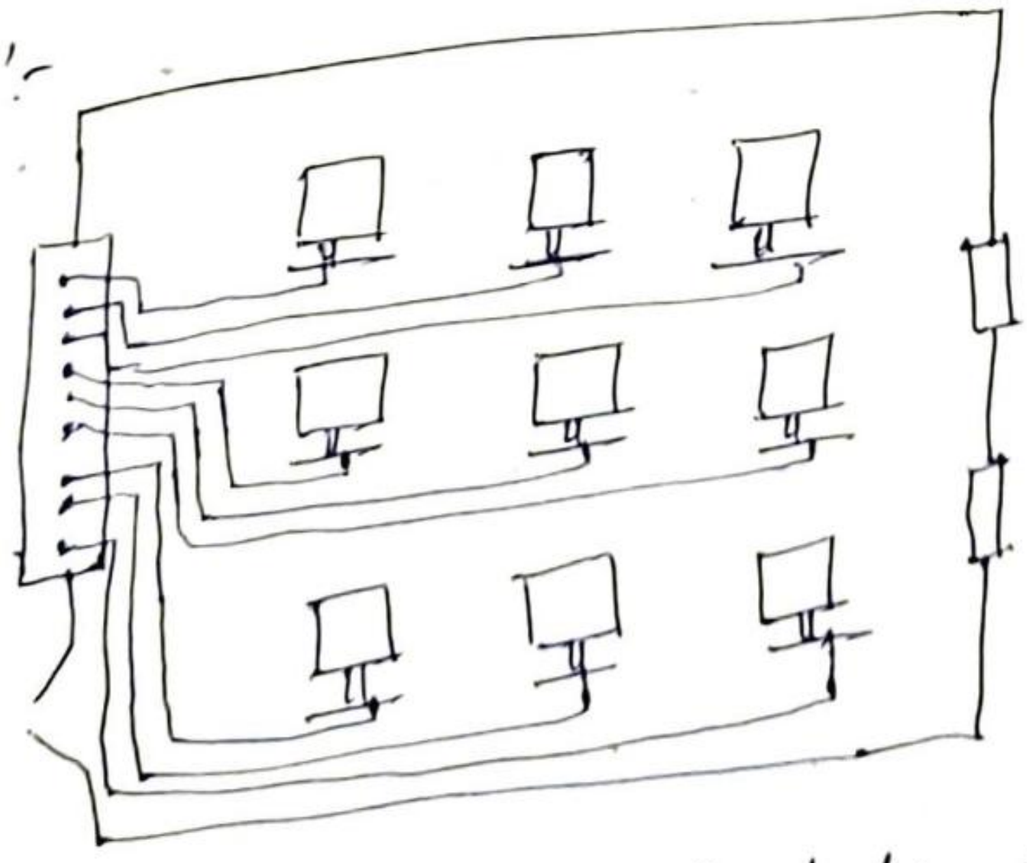
The network based on the size can be categorized into following steps

① Local Area network (LAN)

② Wide Area network (WAN)

③ Metropolitan Area network (MAN).

① LAN:-



It is a privately owned & links the devices in a single office, building or campus. Depending on the need of organisation & type of

Scanned by TapScanner

technology used, a LAN can be as simple as two PC's & a printer in some one's home office. Currently LAN size is limited to a few kilometers.

LAN's are designed to allow resources to be shared b/w personal computers or work stations. the resources to be shared can include hardware, software or data.

(2) WAN :-

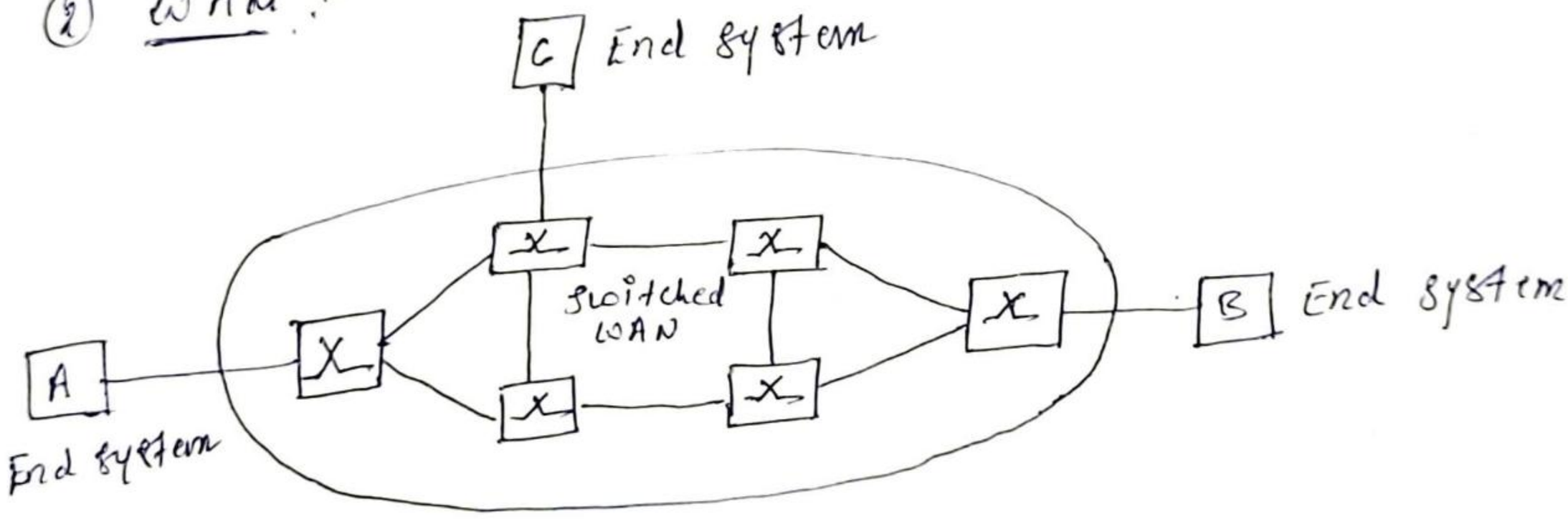


fig (a) Switched WAN

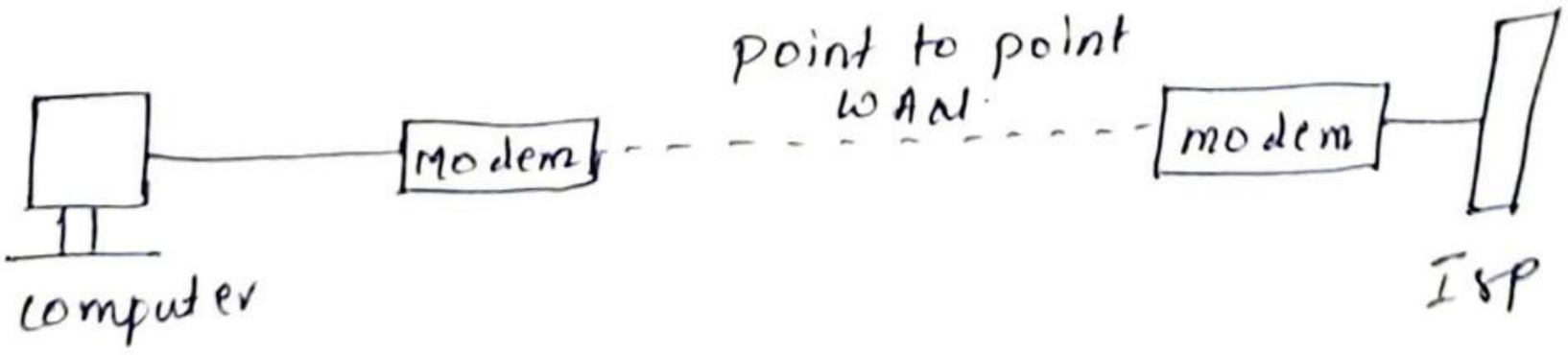


fig (b) point to point WAN.

It provides long-distance transmission of data, image, audio & video information over large geographic areas that may comprise a country, continent or even the whole world.

Scanned by TapScanner

A WAN can be complex as the backbone that connects the internet or as simple as a dial-up line that connects a home computer to the internet. we normally refer to the first as a switched WAN & to the second as point-to-point WAN. the switched WAN connects the end system, which usually comprise a router that connects to another LAN or WAN. The point-to point WAN is normally a line leased from a telephone or a cable TV provider that connects a home computer or small LAN to the internet service provider (ISP). this type of WAN is often used to provide internet access.

③ MAN:- It is a network with a size b/w a LAN & 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. & have endpoint spread over a city or part of city. A good eg. of a MAN is the part of the telephone company n/w that can provide a high-speed DSL line to the customer.

Scanned by TapScanner

→ Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN a MAN or a LAN in isolation: they are connected to one another. When two or more networks are connected, they become an internetwork or internet.

→ The Internet:-

The internet has revolutionized many aspects of our daily life. It has affected the way we do business as well as the way we spend our leisure time. Count the way's you've used the internet recently. perhaps you've sent electronic mail to a business associate, paid a utility bill, read a newspaper from a distant city or looked up a local movie schedule - all by using the internet.

The internet is a structured, organised system. we begin with brief history of the internet.

* Brief history:-

A Network is a group of connected communicating devices such as computers & printers.

Scanned by TapScanner

An internet is two or more networks that can communicate with each other. ~~Two most networks~~

Private individuals as well as various organizations such as government agencies, schools, etc.,

In the mid-1960's, mainframe computer in research organization were standalone devices. computers from different manufacturers were unable to communicate with one another. the advanced Research project agency (ARPA) in the department of Defence was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing cost & elimination duplication of effort.

In 1967 at an association for computing Machinery (ACM) meeting, ARPA presented its idea for ARPANET, a small network of connected computers. the idea was that each host computer would be attached to a specialized computer called an interface message processor (IMP).

Scanned by TapScanner

By 1969 ARPANET was a reality. four nodes, at the university of california (UCLA), Santa Barbra (UCSB), Standard research institute (SRI), & the university of utah, were connected via the IMP's to form a network. Soft ware called the network control protocol (NCP) provided communication b/w the hosts.

In 1972, vint cerf & bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the internetting project.

Shortly thereafter, authorities made a decision to split TCP into two protocols:

* Transmission control protocol (TCP)
* Internetworking protocol (IP).

→ The Internet today :-

It has came a long way since 1960's. today it is not a simple hierarchical structure. It is made up of many wide- & local area networks joined by connecting devices & switching stations. it is difficult to give an accurate

Scanned by TapScanner

representation of the internet bcz it is continually changing - new networks are being added, existing networks are adding addresses, & networks of defunct companies are being removed. today most end users who want internet connection use the service of internet service providers (ISP's).

* International internet service providers

At the top of the hierarchy are the international service providers that connect nations together.

National internet service providers:

The national internet service providers are backbone n/w's created & maintained by specialized companies. there are many national ISPs operating in North America.

Some of the well known are sprint link, PSI Net, UUNet technology, AGIS & internet MCI. To provide connectivity b/w the end users, these backbone n/w's these backbone n/w's are connected by complex switching stations. called network access points.

Scanned by TapScanner

* Regional internet Service providers

Regional internet Service providers or regional isp's are smaller isp's that are connected to the one or more national isp's. they are at the third level of the hierarchy with smaller data rate.

* Local internet Service provider:-

local internet Service provider's provide direct Service to the end users. the local isp's can be connected to the regional isp's or directly to national isp's. Most end users are connected to the local isp's. Note that in the sense, a local isp can be company that just provides internet Services a corporation with a n/w that supplies Services to it own employees, or a non profit organization. such as college or university.

Scanned by TapScanner

→ Protocols & Standards :-

* Protocol :- In computer n/w communication occurs b/w entities in different systems. An entity is anything capable of sending or receiving information. However two entities can not simply send bit streams to each other & expect to be understood. for communication to occur, the entities must agree on a protocol.

A protocol is a set of rules that govern data communications. protocol defines what is communicated, how it is communicated & when it is communicated. the key element of a protocol are syntax, semantics & timing.

* Syntax :- it refers to the structure or format of the data, meaning the order in which they are present.

* Semantics :- It refers to the meaning of each section of bits.

* Timing :- It refers to two characteristics: when data should be sent & how fast they can be sent.

Scanned by TapScanner

Standards :-

Standards are essential in creating & maintaining an open & competitive market for equipment manufacturers & in guaranteeing national & international interoperability of data & telecommunications technology & processes.

Standards provide guidelines to manufacturers, vendors, government agencies & other service providers to ensure the kind of interconnectivity necessary in today's marketplace & in international communication.

* De facto :- Standards that have not been approved by an organized body but have been adopted as standards through widespread use are defacto standards.

+ De jure :- Those standards that have been legislated by an officially recogized body are de jure standards.

→ Standard organizations :-

Standards are developed through the cooperation of standards creation committees, forums, & government regulatory agencies.

Scanned by TapScanner

Standard certain Committees.

1. International organization for Standardization
2. International Telecommunication union.
3. American National Standards Institute.
4. Institute of Electrical & Electronics engineers
5. Electronics Industries Association

forums:- Telecommunication technology developmet is moving faster than the ability of standard committees to ratify standards. the forums work with universities & users to test, evaluate & standardize new technologies.

Regulatory agencies:- All communication technology is subject to regulation by government agencies such as federal communication commission (FCC) in the united states.

→ Internet Standards:- It is a thoroughly tested specification that is useful to and adhered to by those who work with the internet. It is a formalized regulation that must be followed. there is a strict procedure by which a specification attain internet standard status. A specification begins as an internet draft. An internet draft is a working document with no official statement & 6-month lifetime. upon recommendation from the internet authorities, a draft may be published as a Request for comment (RFC). each RFC is edited, assigned a number & made available to all interested parties.

Scanned by TapScanner

⇒ **network models :-**

It is a complicated task, which involves Software, firmware, chip level engineering, hardware & electric pulses.

To ease network engineering the whole network concept is divided into multiple layers.

each layer is involved in some particular task & is independend of all other layers. But as whole, almost all networking tasks depending on all these layers.

layers share data b/w them & they depend on each other only to take i/p & send o/p.

⇒ **Layered tasks :-**

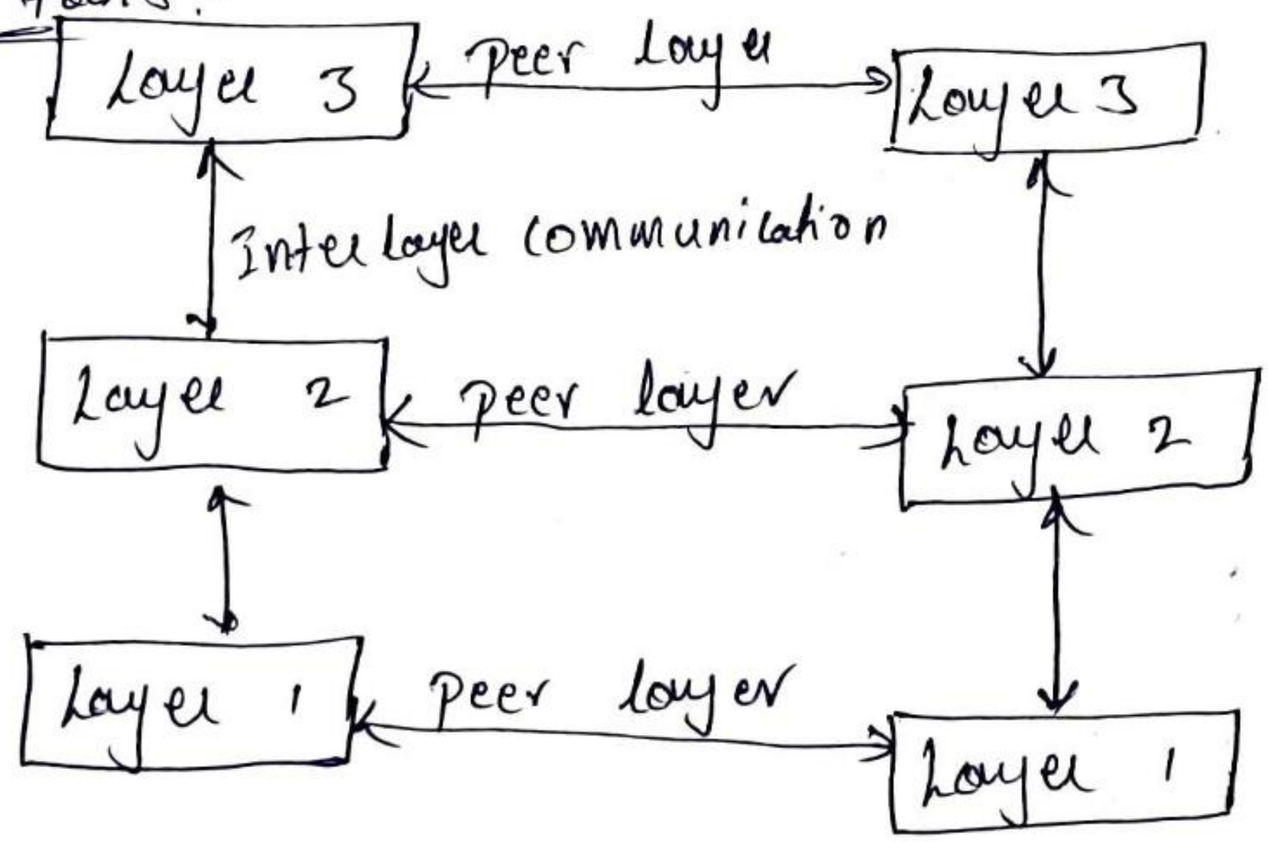


fig :- layered tasks.

In layered architecture of N/w model, one whole N/w process is divided into small tasks. each small task is then assigned to a particular.

Scanned by TapScanner

layer which works dedicatedly to process the task only.

In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. this task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task & passes on to lower layer. if the task is initiated by lower most layer, then the reverse path is taken.

⇒ OSI Model & Layers in OSI Model:-

OSI (open system interconnect) is an open standard for all communication systems. it is established by ISO (international standard organization) & have seven layers. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

Scanned by TapScanner

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

fig:- Seven layers of OSI model

* Application layer:- it is responsible for providing interface to the application user. this layer encompasses protocols which directly interact with the user

* Presentation layer:- It defines how data in the native format of remote host should be presented in the native format of host.

* Session layer:- It maintain sessions b/w remote hosts.

Scanned by TapScanner

* Transport layer:- It is responsible for end-to-end delivery b/w hosts.

* N/w layer:- It is used for address assignment & uniquely addressing hosts in a n/w.

* Data link layer:- It is used for reading & writing the data from & onto the link. link errors are detected at this layers.

* Physical layer:- It defines the h/w, cabling, power o/p, pulse rate, etc.,

⇒ TCP/IP protocol suite:- (internet model)

Application layer
Transport layer
Internet layer
link layer.

It defines internet model which contains 4 layered architecture. OSI model is general communication model but internet model is what the internet uses for

Scanned by TapScanner

all its communications. The internet is independent of its underlying n/w architecture so is its model.

⇒ <u>Addressing</u>:-

if any two devices want to engage in any kind of dialogue, then they should first identify themselves in this complex network transmission arena. so, first they should know each other's respective address (source & destination). In the internet employing TCP/IP protocol, we have four levels of addresses being in use for different layers.

we have four methods for identifying addresses.

* physical address (MAC address)
* logical address (IP address)
* port address
* specific address.

⇒ wireless <u>links</u> & <u>network</u> <u>characteristics</u>:-

these are differences from wired link.

* Decreased Signal Strength: Radio signal attenuates as it propagates through matter (path loss)
* <u>Interface</u> from <u>other</u> sources:- standardized

Scanned by TapScanner

wireless n/w frequencies (eg: 2.4GHz) shared by other devices.

* Multipath propagation:- Radio signals reflects off objects ground, arriving destination at slightly different times.

⇒ WIFI: IEEE 802.11 wireless LAN's :-

It is a set of MAC & physical layer specification for implementing WLAN computer communication in the 900 MHZ & 2.4, 3.6, 5 & 60 GHZ freq. bands.

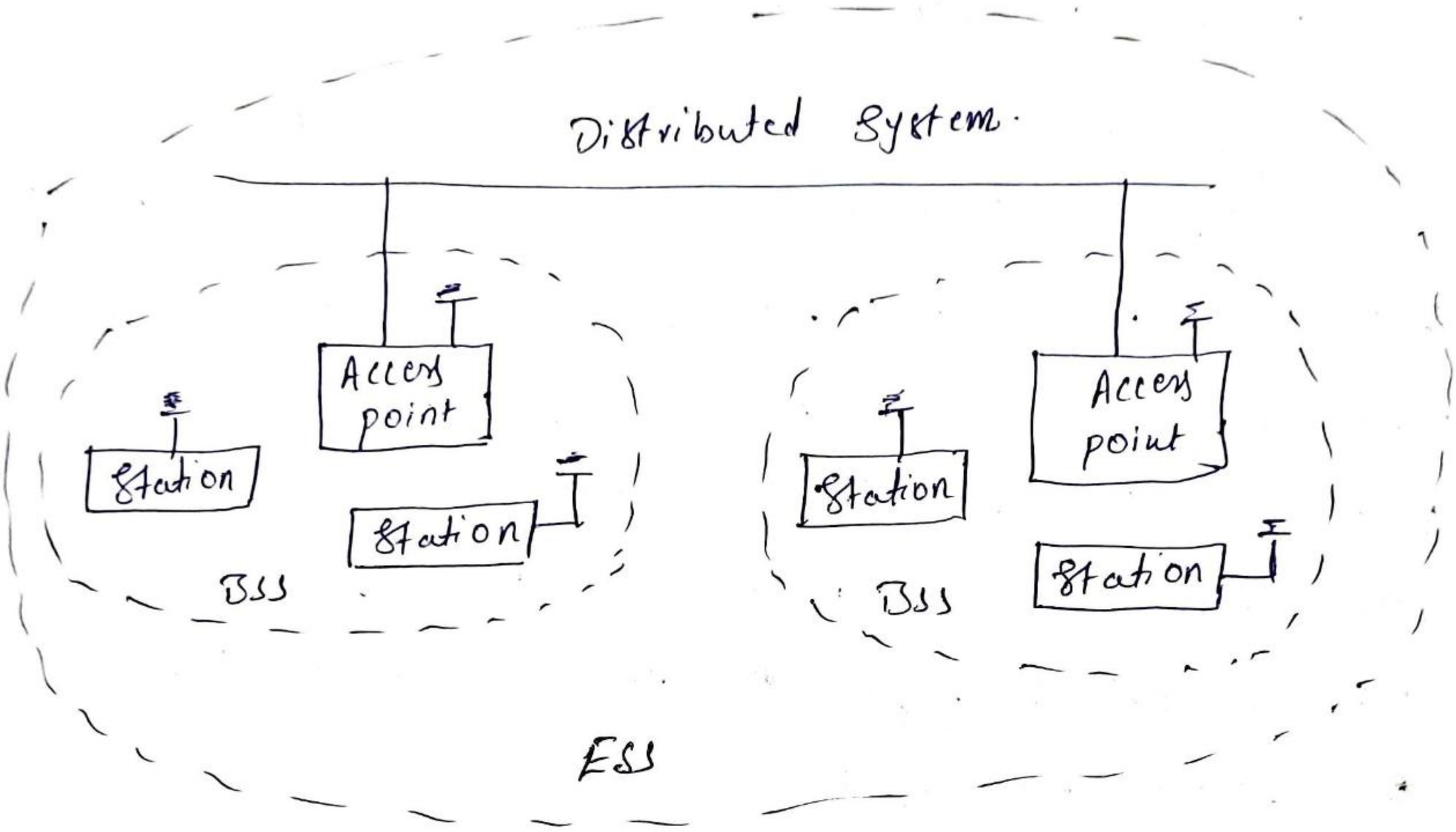
The IEEE developed an international standard for WLAN's. The 802.11 standard focuses on the bottom two layers of the OSI model, the physical layer & data link layer.

It's main objective is to define a MAC sublayer, management protocols & services, & three physical layers for wireless connectivity of fixed, portable & moving devices within local area.

The three physical layers are an IR base band, an FHSS radio in 2.4 GHZ & a DSSS radio in the 2.4 GHZ.

Scanned by TapScanner

⇒ 802.11 Architecture :-



BSS: Basic service set ESS:- Extended service set

fig:- BSS & ESS configuration of 802.11 WLAN

It is designed to support a n/w where most decersion making is distrubuted to mobile stations. this type of architecture has several advantages. It is tolerant of faults in all of the WLAN equipment & eliminates possible bottlenecks a centralized architecture would introduce. the architecture is flexible & can easily support both small, transient n/w's & large, semi permanent & permanent n/w's. In addition the architecture & protocols offer

Scanned by TapScanner

Significant power saving & prolong the battery life of mobile equipment without loosing n/w connectivity.

In IEEE 802.11 standard 2 n/w architectures are defined ① Infrastructure n/w ② point-to-point n/w.

① Infra structure n/w:- It is the architecture for providing communicatin b/w wireless client & wired n/w resources. the transition of data from the wireless to wired medium occurs through AP. an AP (Access point) & its associated wireless client define the coverage area. together all the devices form a basic service set.

② P-to p (Ad-hoc) n/w:- It is used to support mutual communication b/w wireless clients. Typically an ad-hoc n/w is created spontaneously & doesnot support access to wired n/w's. an Ad-hoc n/w doesnot require an Access point.

Scanned by TapScanner

UNIT - II -

Data link layer

→ Introduction:- It concerned with local delivery of frames b/w nodes on the same level of the network.

DLL provides the functional & procedural means to transfer data b/w n/w entities & may also provide the means to detect & possibly correct errors that can occur in the physical layer.

DL frames, as these protocol data units are called do not cross the boundaries of LAN.

Internetwork routing & global addressing are higher layer functions, allowing data link protocols to focus on local delivery, addressing & media arbitration.

eg of DLL:- Ethernet, Point-to-point protocol & HDLC (High level Data link control)

→ Access N/w's:- It is a type of n/w which physically connects an end system to the immediate router on a path from end system to any other distant end system.

eg:- ISP, home n/w's, enterprise N/W, mobile n/w etc.

⇒ Types:- * Ethernet → uses coaxial or twisted cables

* DSL - Digital Subscriber Line

→ It brings connection into home by telephone lines. It can carry both data & voice signals.

* FTTH: fiber to the home

* wireless LAN's:- It links two or more devices using wireless communication within a range.

* 3G & LTE:- long term evaluation.

It uses cellular telephony to send or receive packets

→ Link layer:- It is the lowest layer in the I/P suite. It is the group of methods & communication protocols confined to the link that a host is physically connected to.

It is a physical & logical ~~hardware~~ s/w component used to interconnect host or nodes in N/w & link protocol is a suite of methods & standards that operate b/w adjacent n/w nodes of segment.

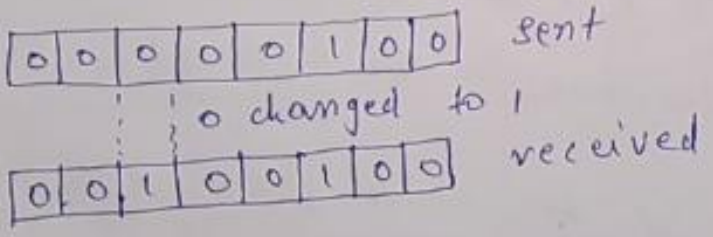
→ Services of Link layer:- It is responsible for

* Multiplexing data streams
* data frame detection
* Medium access
* error control
* It ensures reliable P-to-P & P-to-MP connections in communication n/w.

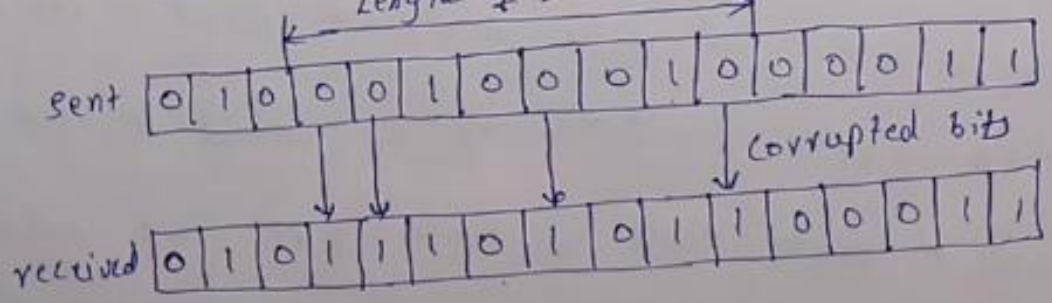
→ Types of errors.

* Single bit error
* Burst error

* Single bit error



* Burst error



→ Redundancy :- The central concept in detecting or correcting errors is redundancy

To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender & removed by the receiver.

→ Detection vs Correction :-

The correction of errors is more difficult than the detection.

In error detection, we are looking only to see if any error has occured.

In error correction, we need to know the exact number of bits that are corrupted & more importantly, their location in the message.

The number of the errors & the size of the msg are important factors. If we need to correct one single error in a 8-bit data unit, we need to consider eight possible error locations. if we need to correct two errors in a data unit of same size, we need to consider 28 possabilities.

⇒ forward error correction Vs Retransmission

forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible if the no. of errors is small.

correction by retransmission is a technique in which the receiver detects the occurance of an error & asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

⇒ Error Detection & correction techniques:-

Error Detection:-

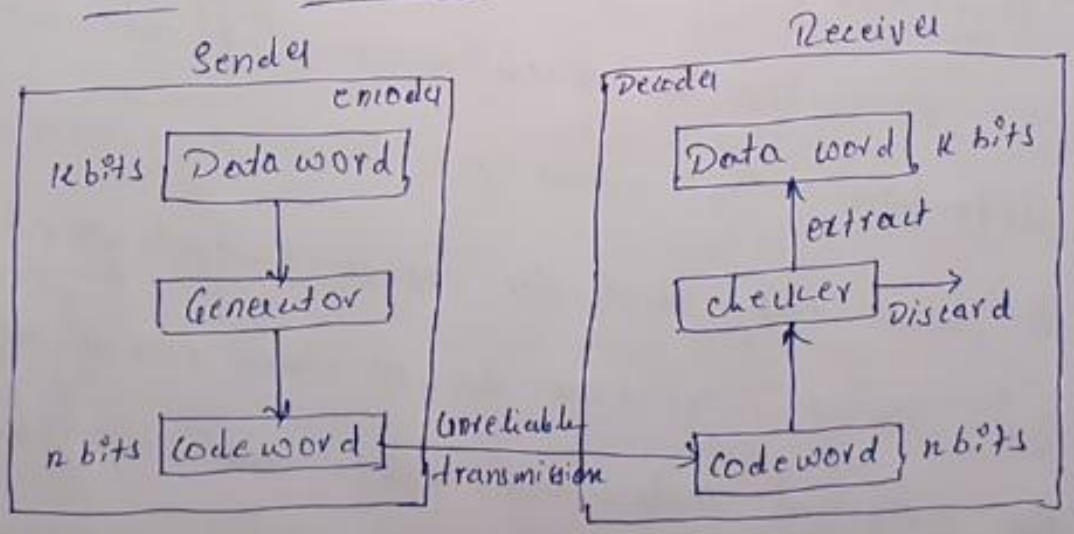


fig:- process of error detection in block coding

The sender creates a codeword out of data words by using a generator that applies the rules & procedures

of encoding. Each code word sent to the receiver may change during transmission. If the received code word is same as one of the valid code words, the word is accepted:

if the received code word is not valid it is discarded. However if the code word is corrupted during transmission but the received word still matches a valid code word, the error remains undetected.

This type of coding can detect only single errors. Two or more errors may remain undetected.

Error correction:-

error correction is much more difficult than error detection. In error detection, the receiver needs to know only that the received code word is invalid. in error correction the receiver needs to find the original code word sent. we can say that we need more redundant bits for error correction than for error detection.

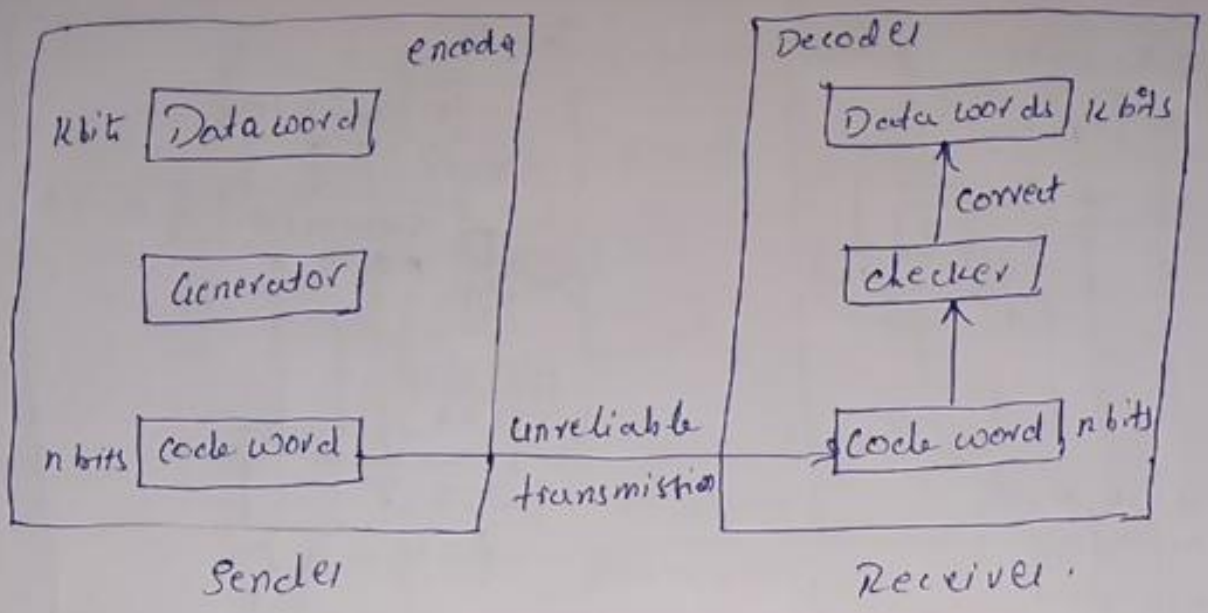


fig:- Structure of encoder & decoder in error correction

fig shows the role of block coding in error correction. we can see that the idea is the same as error detection but the checker functions are much more complex.

⇒ parity check code:-

+ A simple parity check code is a single bit error-detecting code in which $n = k+1$ with $d_{min} = 2$ k = data bits

In the fig. the encoder uses a generator that takes a copy of a 4-bit data word $(a_0, a_1, a_2 \& a_3)$ & generates a parity bit r_0. the data word bits & the parity bit create the 5-bit code word.

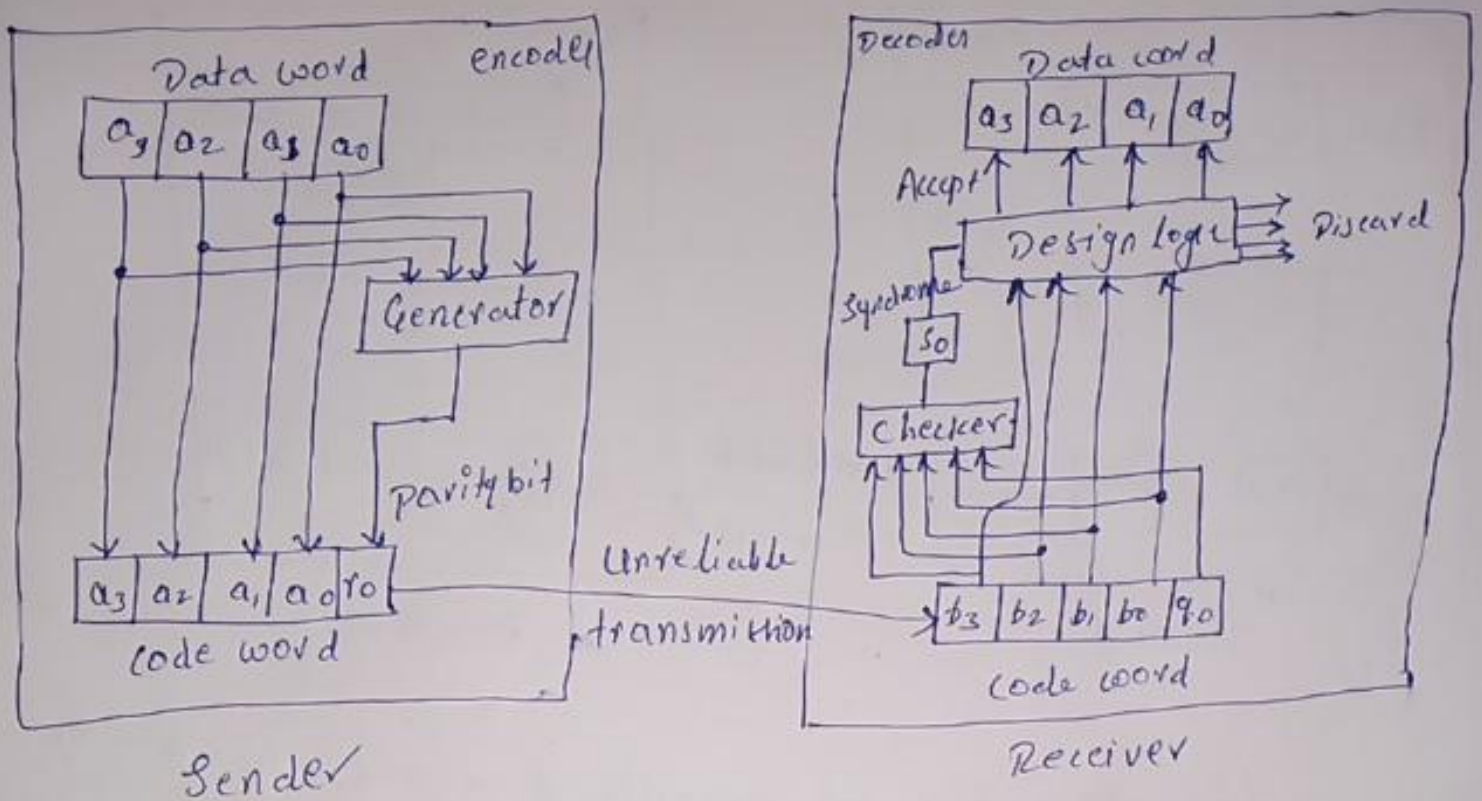


fig: encoder & decoder for simple parity-check code.

Data words	codewords	Data words	codewords
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110

fig: simple parity - check code.

The parity bit that is added makes the no. of 1's in the code word even. this is normally done by adding the 4 bits of the dataword. the result is the parity bit.

where $r_0 = a_3 + a_2 + a_1 + a_0$.

if the no. of 1s is even the result is 0

if the no. of 1's is odd, the result is 1.

In both cases the total no. of 1's in the codeword is even.

the sender sends the codeword which may be corrupted during the transmission. the receiver receives a 5-bit word.

A simple parity-check code can detect an odd no. of errors.

→ Check Summing method :-

Based on the concept of redundancy it is one of the method used for error detection.

In this mechanism, the unit is divided into k sections, each of n bits. All sections are added using 1's complement to get the sum.

This is the complemented & becomes the checksum. there after this check sum is sent with data.

At the receiver side the unit is divided into k sections each of n bits. All sections are added using is complement to get the sum. the sum is complemented. if the result is zero data are accepted other wise rejected.

eg:-

Sender

← 10101001 00111001

the no's are added using is complement arithemetic

```
  10101001
  00111001
  --------
  1 1 1
sum → 10100010
      00011101 (1's complement)
```

the pattern unit is

← 10101001 00111001 00011101
check sum

Receiver.

10101001 00111001 00011101

```
  10101001
  00111001
  00011101
  --------
sum 11111111 →
```

complemet 00000000 means the pattern is OK

→ cyclic codes

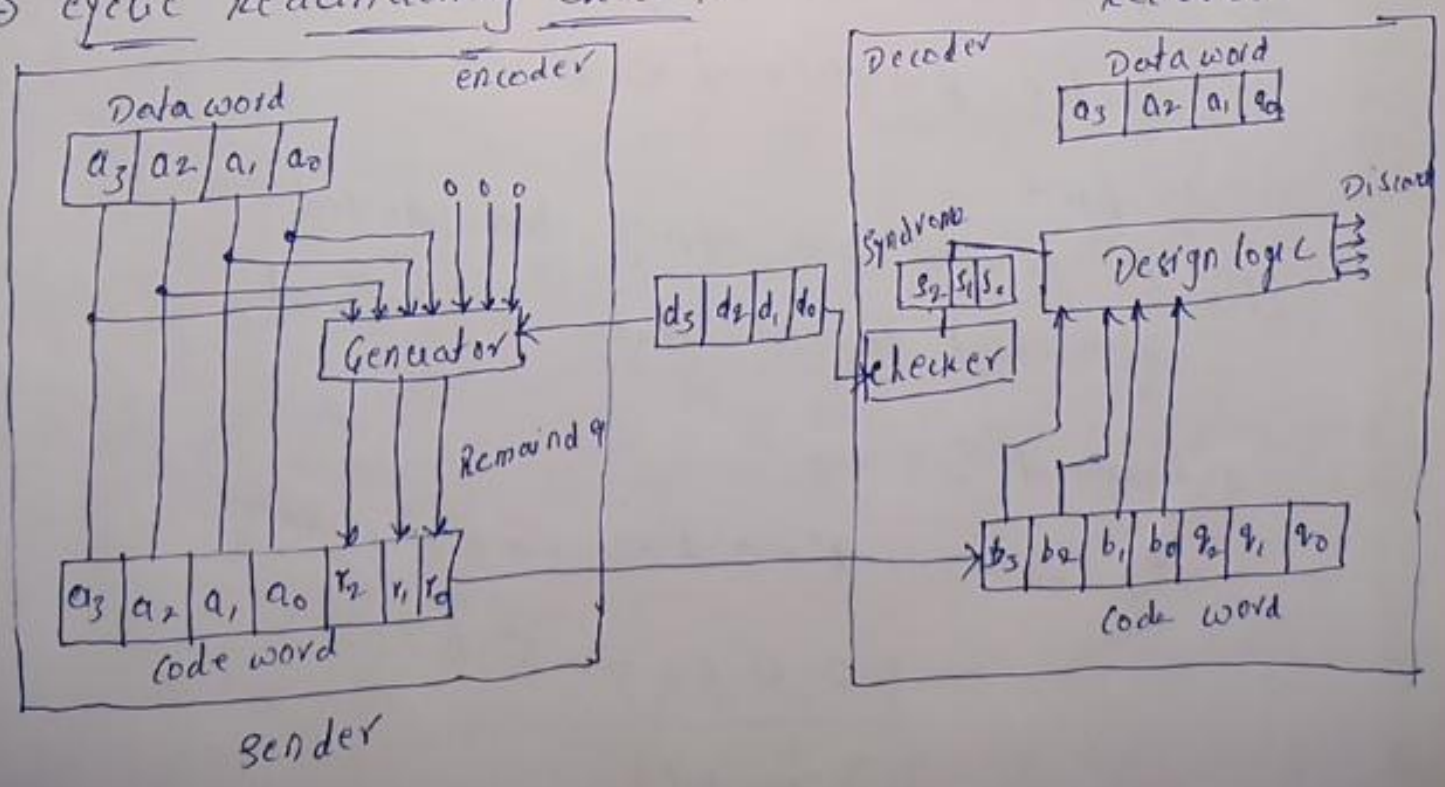
cyclic codes are special linear block codes with one extra property. In a cyclic code, if a code word is cyclically shifted, the result is another code word.

for eg if 1011000 is code word & we cyclically left-shift, then 0110001 is also a code word.

$b_1 = a_0 \quad b_2 = a_1 \quad b_3 = a_2 \quad b_4 = a_3 \quad b_5 = a_4 \quad b_6 = a_5 \quad b_0 = a_6$

In the right most equation the last bit of the first word is wrapped around & becomes the first bit of the second word.

→ cyclic redundancy check:-



* It is error detection method based on binary division.
* In CRC, a set of redundant bits called cyclic redundancy check bits are appended to the end of data.
* So that the resulting data unit becomes exactly divisibly by second, predetermined binary no:
* At the destination, the incoming data is divided by the same no.

→ if the remainder is "0" → data is accepted
otherwise it is rejected.

eg: 1101011011 (original data)
cyclic polynomial → $x^4 + x + 1$

to find
check (a) actual bit string transmitted
(b) check correct data is received.

polynomial is
$x^4 + x + 1 \rightarrow 1 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 x^0$

$\underbrace{10011}_{\text{CRC bits}} \Rightarrow 5$ bits.

⇒ so, a string of 4 '0' is appended to bit stream

⇒ 1101011011 | 0000

appended stream

Tx:

```
          110000101
10011 ) 1101011011 0000
        10011
        -----
        100111
         10011
        -----
         00001
         00000
        -----
          00010
          00000
         -----
           00101
           00000
          -----
            01011
            00000
           -----
             10110
             10011
            -----
              01010
              00000
             -----
               10100
               10011
              -----
                01110
                00000
               -----
                 1110 → Remainder
```

XOR

Rx:

```
          110000101 0
10011 ) 1101011011 1110
        10011
        -----
         10011
         10011
        -----
          00001
          00000
         -----
           00010
           00000
          -----
            00101
            00000
           -----
             01011
             00000
            -----
              10111
              10011
             -----
               01001
               00000
              -----
                10011
                10011
               -----
                00000
                0000
               -----
                  0
```

Replace 4 zero's with CRC

CRC → 1110

original data + CRC

1101011011 1110

↓

transmitted data.

when ever data is '0' data is accepted.

⇒ Framing:-

The data link layer, an needs to pack bits into frames. so that each frame is distinguishable from another.

Framing in the data link layer seperates a message from one source to a destination. by adding a sender & destination addresses.

the destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

* Fixed size framing:-

frames can be fixed or variable size.

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 this we need a way to define the end of the frame & begninning of the next. two approaches were used for this

① character-oriented ② Bit-oriented.

⇒ flow & error control:-

The most important responsibilities of the data link layer are flow control & error control.

flow control:-

It refers to a set of procedures used to restrict the amout of data that the sender can send before waiting for acknowledgement.

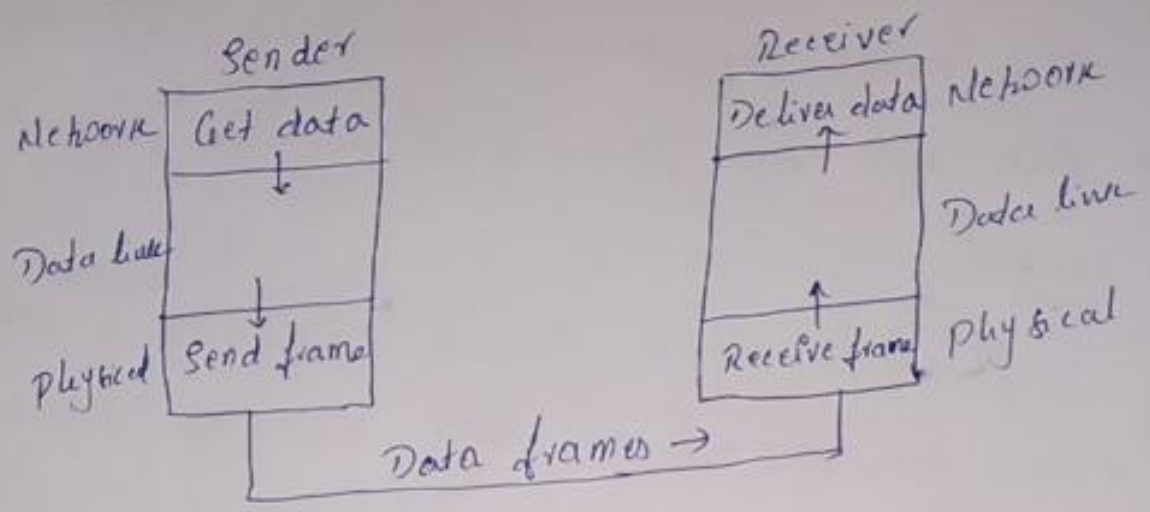
error control:-

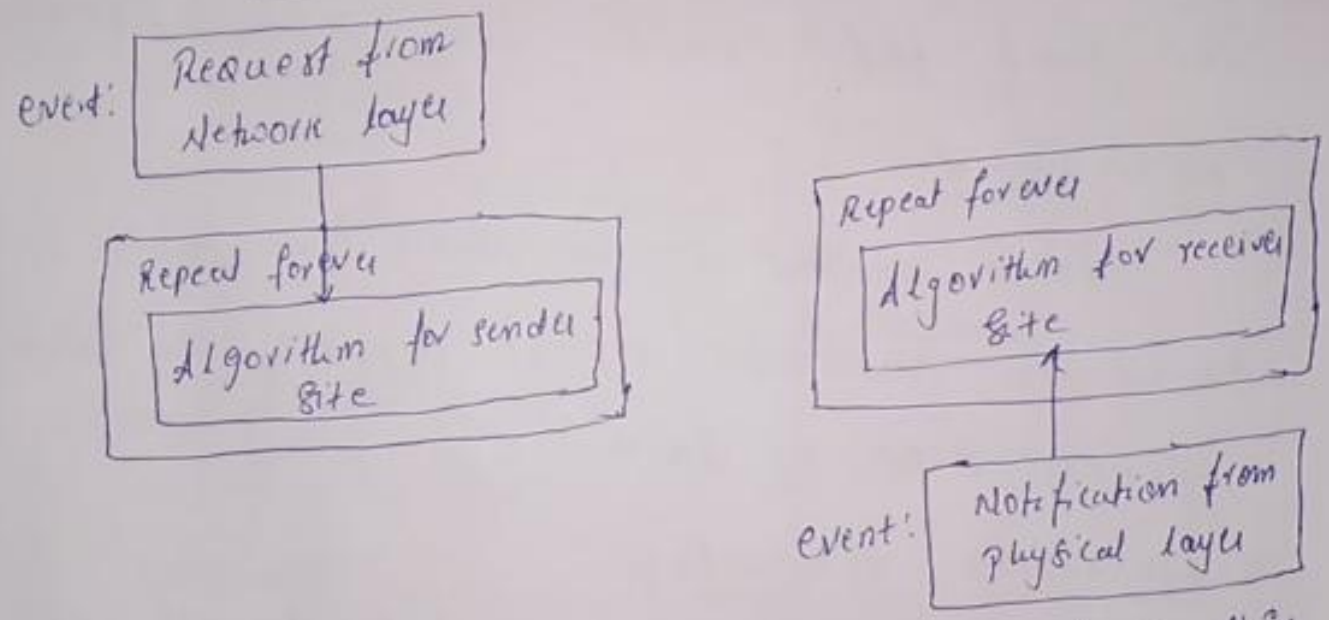
Error control in the data link layer is based on automatic repeat request, which is retransmission of data.

→ Noiseless channels:-

assume we have an ideal channel in which no frames are lost, duplicated or corrupted. we introduce two protocols for this type of channel. the first is a protocol that does not use flow control; the second is the one that does.

① Simplest protocol

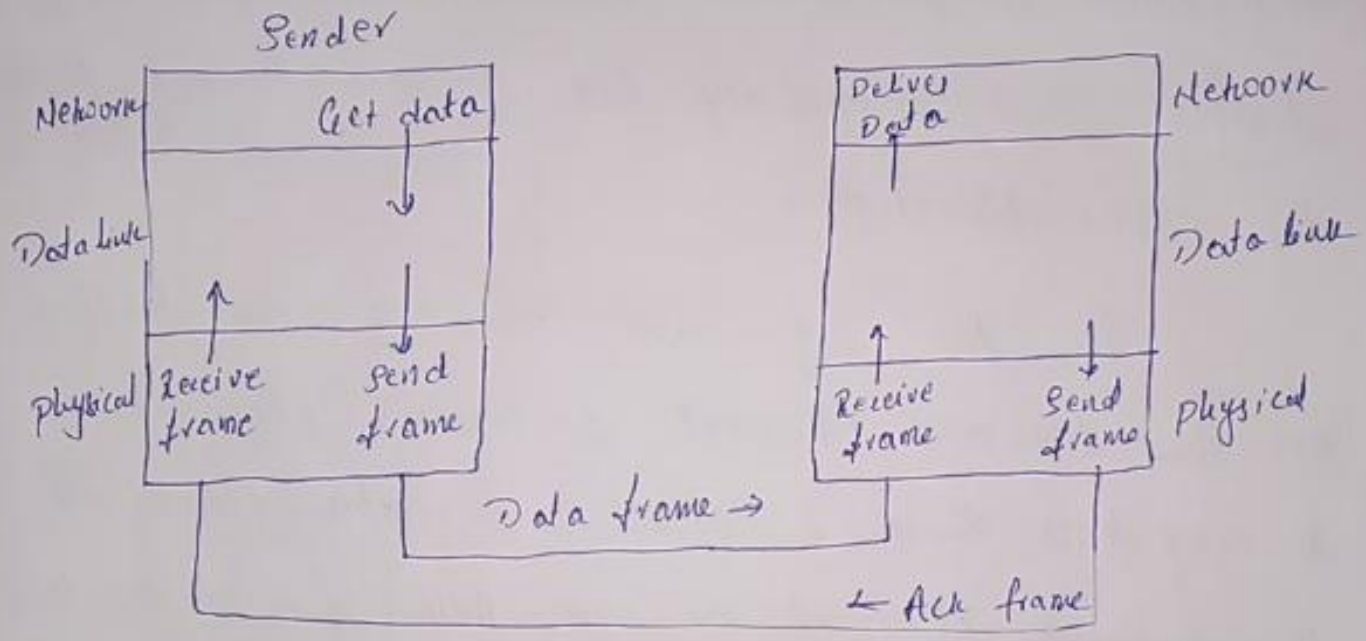




There is no need for flow control in this scheme. the data link layer at the sender site gets data from its network layer, makes a frame out of the data & sends it. the data link layer at the receiver site receives a frame from its physical layer extracts data from the frame & delivers the data to its network layer.

The data layer of the sender & receiver provides transmission services for their network layers.

* Stop & wait protocol :-



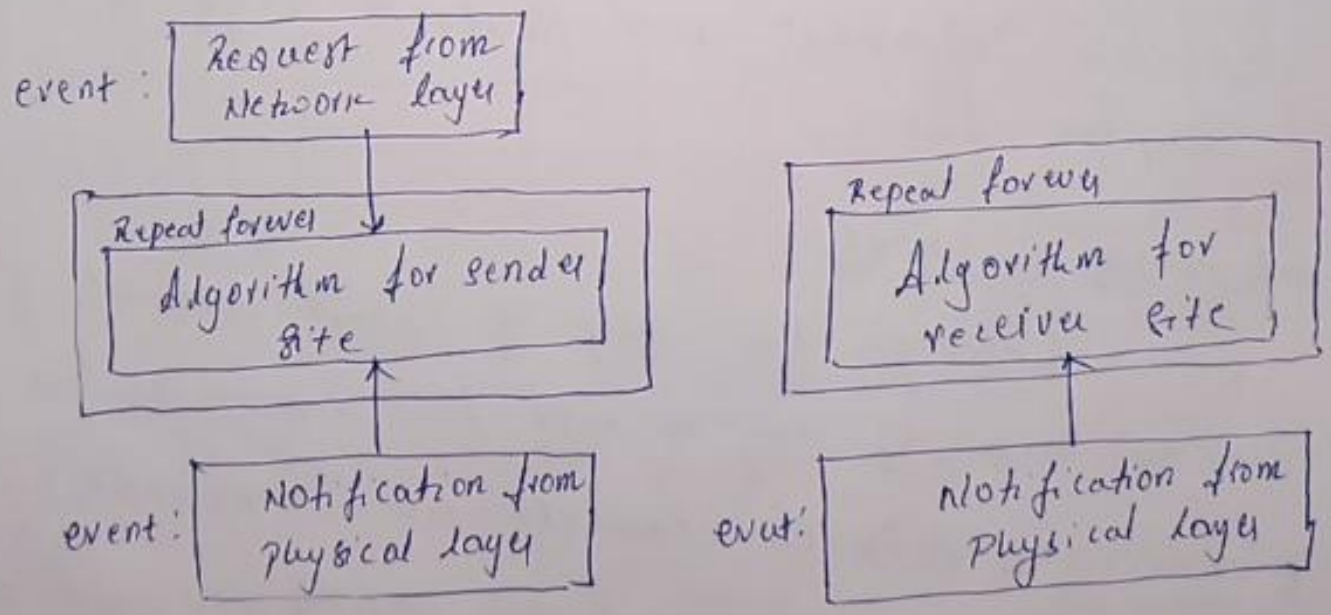


fig:- Design of Stop & wait protocol.

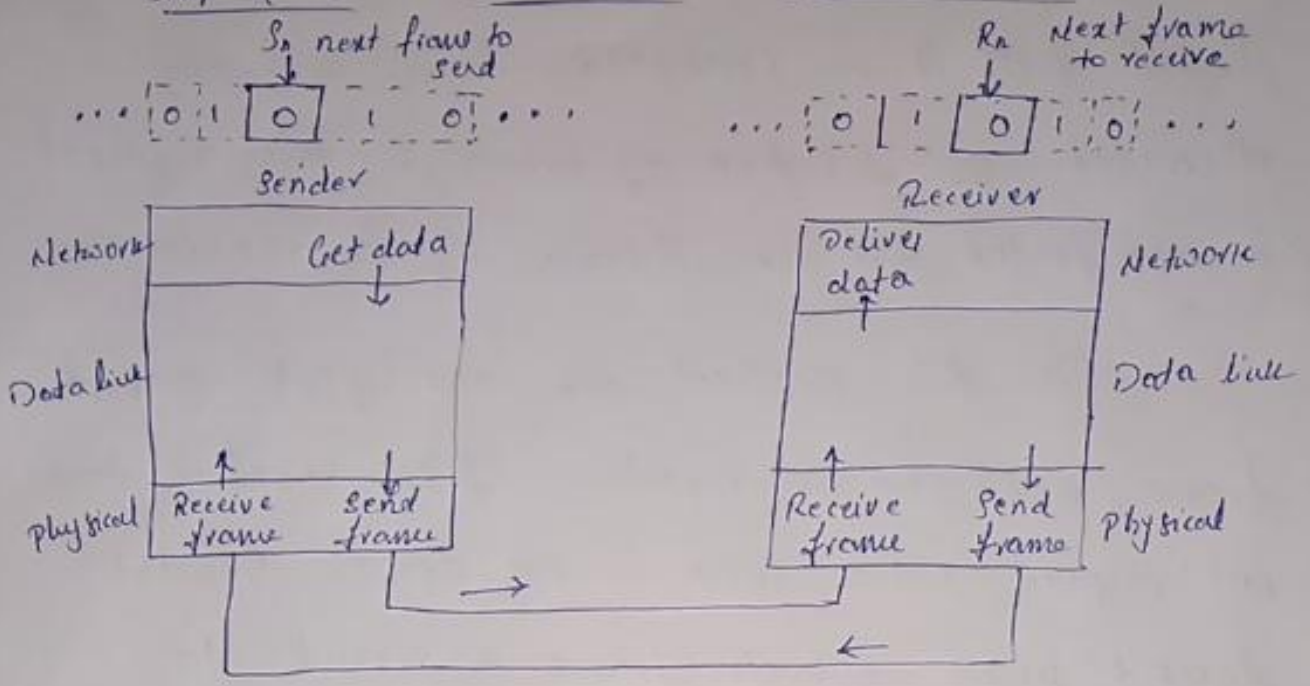
The protocol we discuss is called the stop-&-wait protocol because the sender sends one frame, stops until it receives confirmation from the receiver, & then sends the next frame. we still have unidirectional communication for data frames, but auxiliary Ack frames travel from the other direction.

in the fig. we can see the traffic on the forward channel & reverse channel. At any time, there is either one data frame on the forward channel or one Ack frame on the reverse channel. we therefore need a half-duplex link.

→ Noisy channels:-

Although the stop-&-wait protocol gives us an idea of how to add flow control to its predecessor, noiseless channels are nonexistent. we can ignore the error the error or we need to add error control to our protocols. we discuss three protocols in this section.

* Stop & wait automatic Repeat Request.



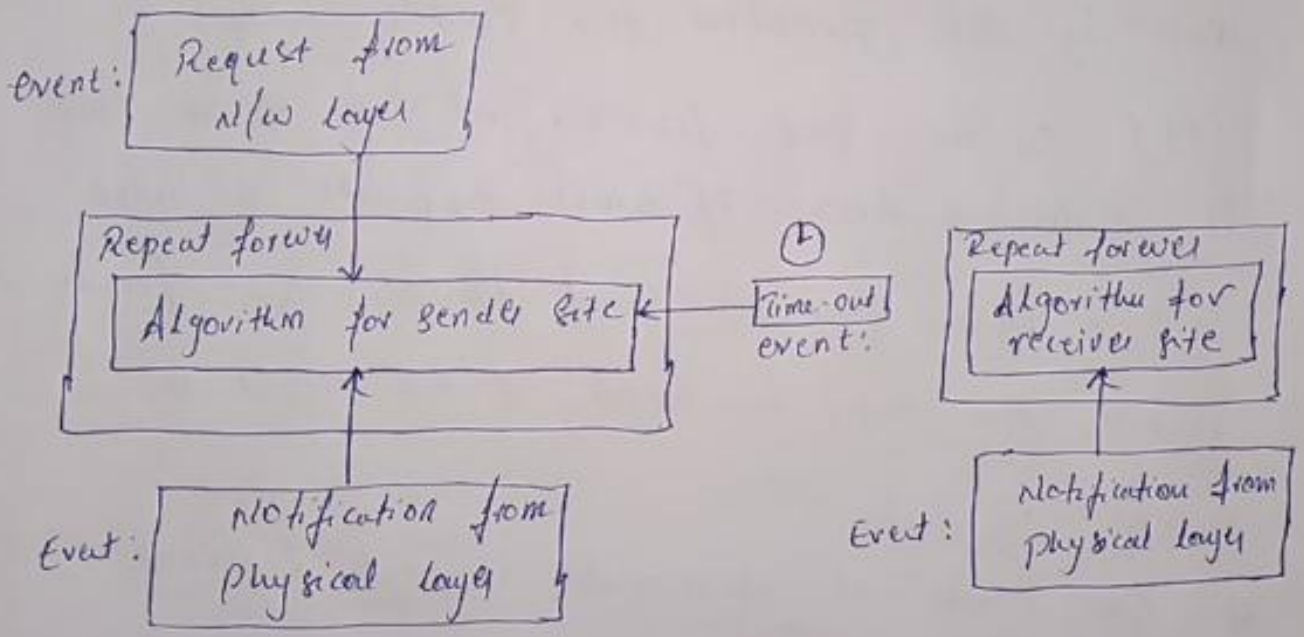


fig: Design of Stop & Wait ARQ protocol.

It adds a simple error control mechanism to Stop & wait protocol.

to detect & correct corrupted frames, we need to add redundancy bits to our data frame.

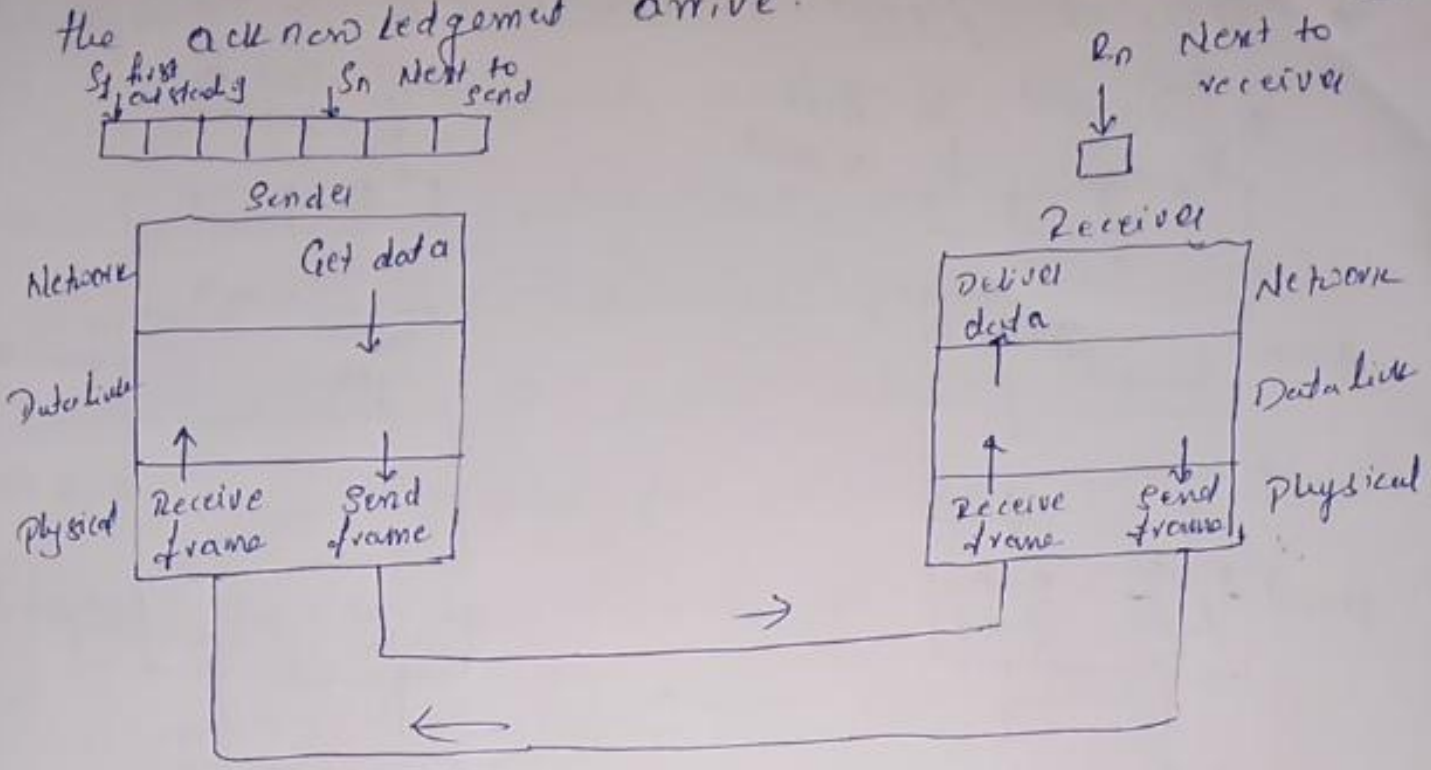
when frame arrives at the receiver site, it is checked & if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver.

In this protocol the corrupted & lost frames need to be resent. if the receiver does not respond when there is an error, sender doesn't know which frame to resend. to remedy this problem the sender keeps a copy of the sent frame. at the same time it starts a timer. if timer expires & there is no Ack for the sent frame the frame is resent, the copy is held, & the timer is restarted.

* Go-Back-N Automatic Repeat Request:-

To improve the efficiency of the transmission multiple frames must be in transition while waiting for Ack. In this protocol we can send several frames before receiving acknowledgement. we keep a copy of these frames until

the acknowledgement arrive.



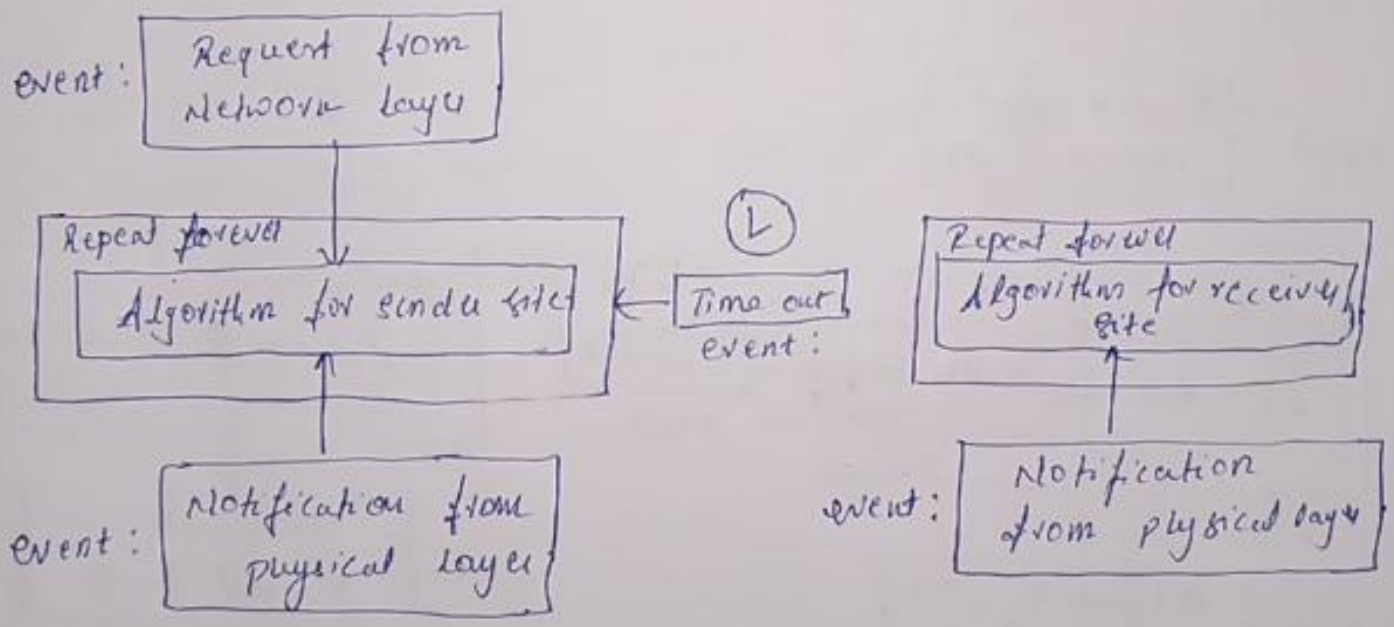


fig:- Design of Go-Back-N ARQ.

In the go back n- protocol the sequence number are modulo 2^m, where m is the size of the sequence number field in bits.

* Selective Repeat Automatic Repeat Request

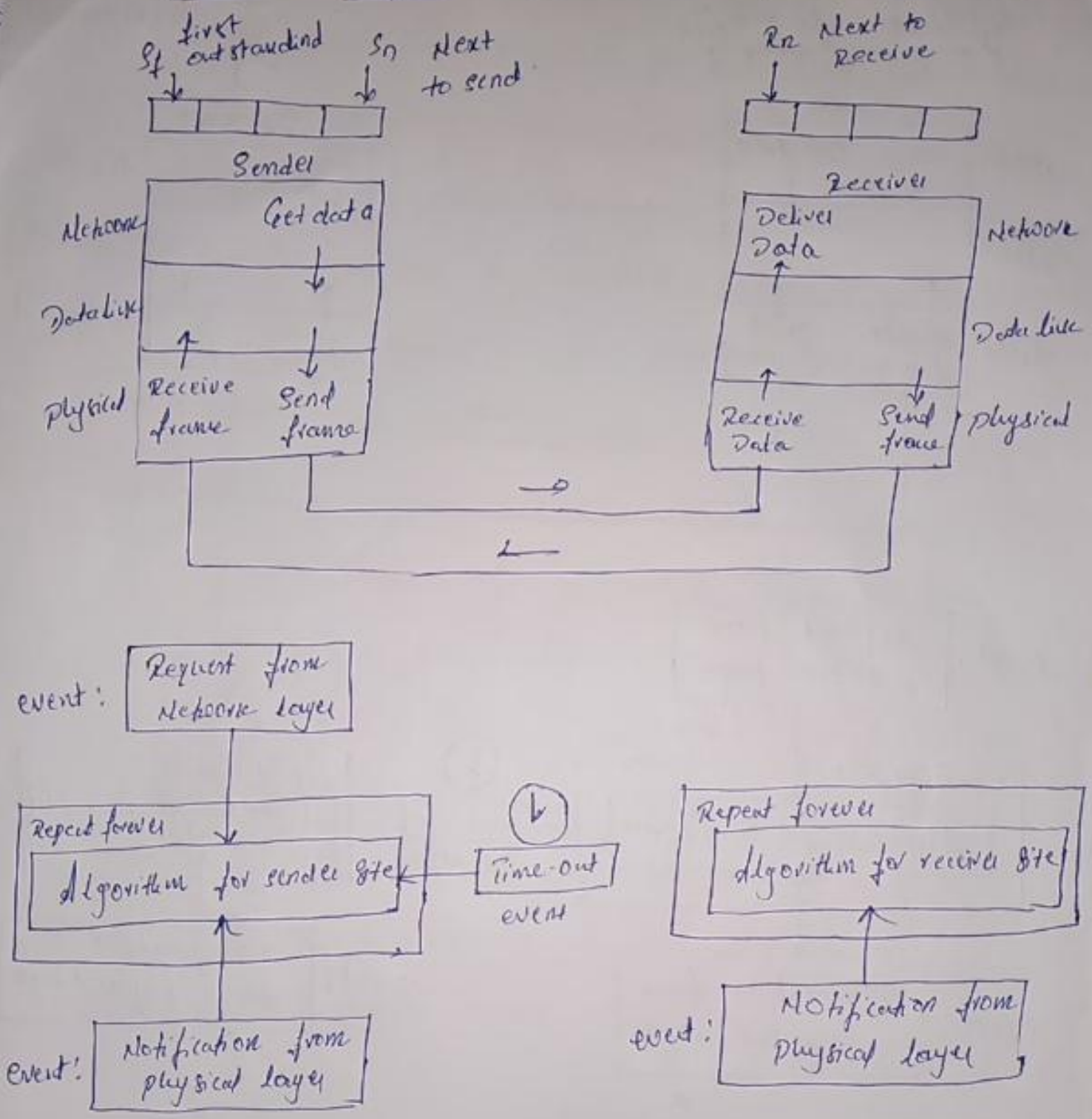


fig: Design of Selective Repeat ARQ

This protocol is very inefficient for noisy link. In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. this resending uses up the bandwidth p

& slows down the transmission. for noisy lines, there is another mechanism that doesnot resend all frames when just one frame is damaged; only the damaged frame is resent. this mechanism is called selective Repeat ARQ. it is more efficient for noisy lines, but the processing at the receiver is more complex.

→ HDLC (High level Data link control):-

It is a bit oriented protocol for communication over point-to-point & multipoint links. It implements the ARQ mechanism.

+ Transfer modes.

① Normal Response mode

② Asynchronous balanced mode.

① Normal Response mode:-

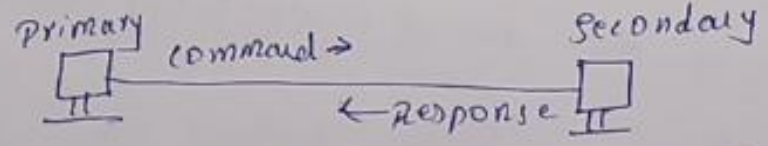


fig ① point to point.

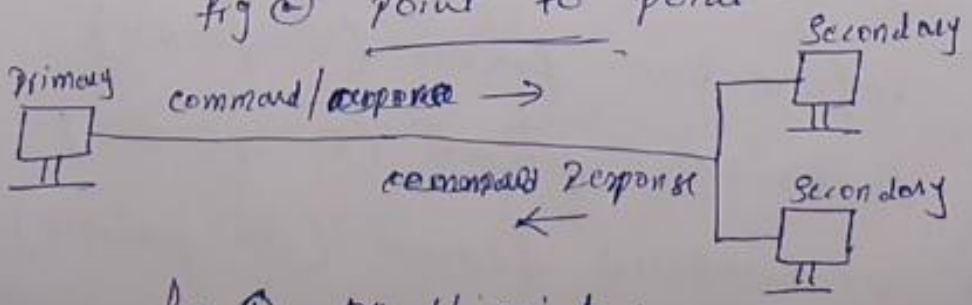


fig ② Multipoint.

In this the station configuration is unbalanced. we have one primary station & multiple secondary stations. A primary station can send commands, a secondary station can only respond. It is used for both point-to-point & multipoint.

② Asynchronous Balanced mode.

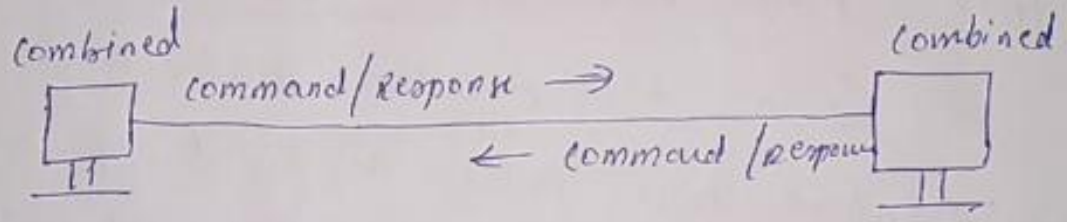


fig:- Asynchronous balanced mode.

In asynchronous balanced mode, the configuration is balanced. the link is point-to point & each station can function as primary & secondary.

This is the most commonly used mode.

frames:-

* information frames (I-frames)
* Supervisory frames (S-frames)
* unnumbered frames (U-frames).

* I frames are used to transport user data & control information relating to user data
* S-frames are used only to transport control information.
* U-frames are reserved for system management.

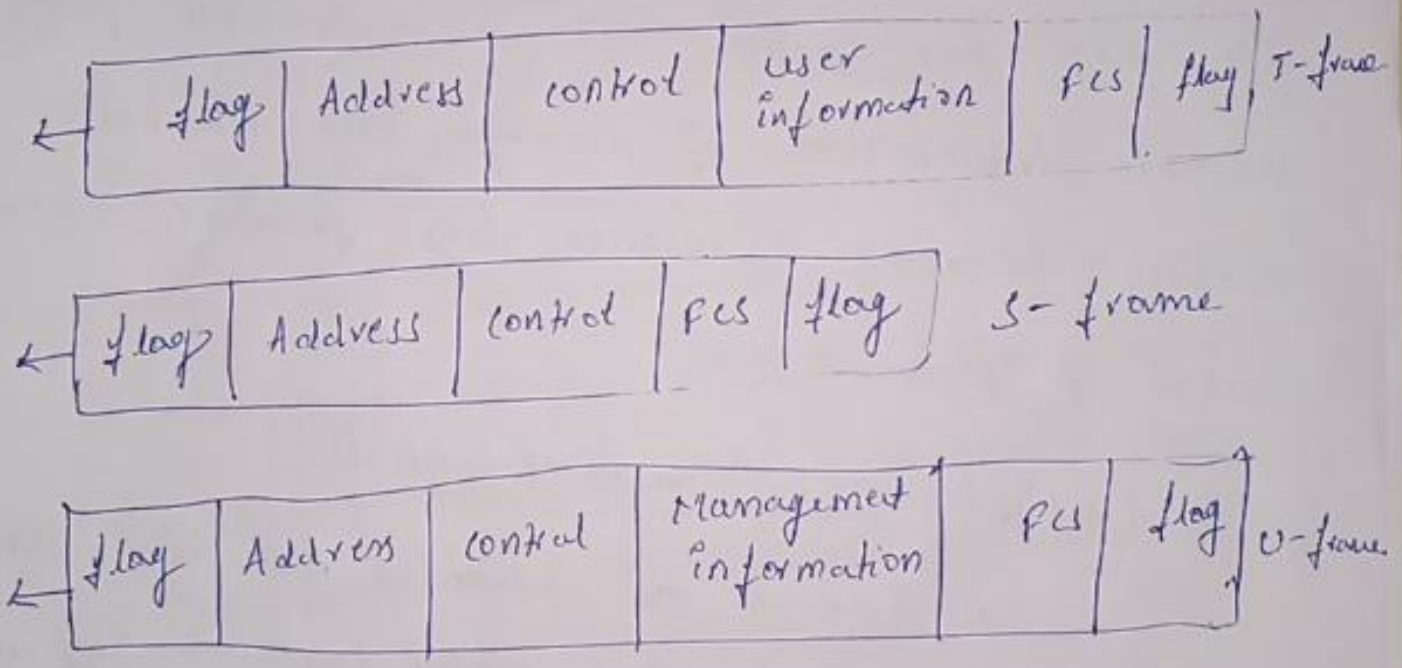


fig:- HDLC frames.

fields.

* flag field
* Address field
* control field
* information field
* FCS field (frame check.

→ Multiple Access protocol

The data link ~~cons~~ layer is responsible for transmission of data b/w two nodes. It's main functions are

* Data link control
* multiple Access control

* Data link control:- It is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control & flow control.

* Multiple access ~~protocol~~ control:-

If there is a dedicated line b/w sender & receiver then data link control layer is sufficient, however if there is no dedicated line present then multiple station can access the channel simultaneously. Hence multiple access protocols are required to decrease collision & avoid cross talk.

Multiple Access protocol

- Random Access protocol
  - Aloha
  - CSMA
  - CSMA/CD
  - CSMA/CA
- controlled Access protocol
  - Reservation
  - polling
  - Token passing
- channelization protocol
  - FDMA
  - TDMA
  - CDMA

⇒ **Random Access:-**

In this all stations have same priority that is no station has more priority than another station. any station can send data depending on medium's state. It has two features.

* there is no fixed time for sending data.
* there is no fixed sequence of stations sending data.

⇒ **Aloha:-** It was designed for wireless LAN, but is also applicable for shared medium. in this, multiple stations can transmit data at the same time & can hence lead to collision & data being garbeld.

* **pure aloha:-**

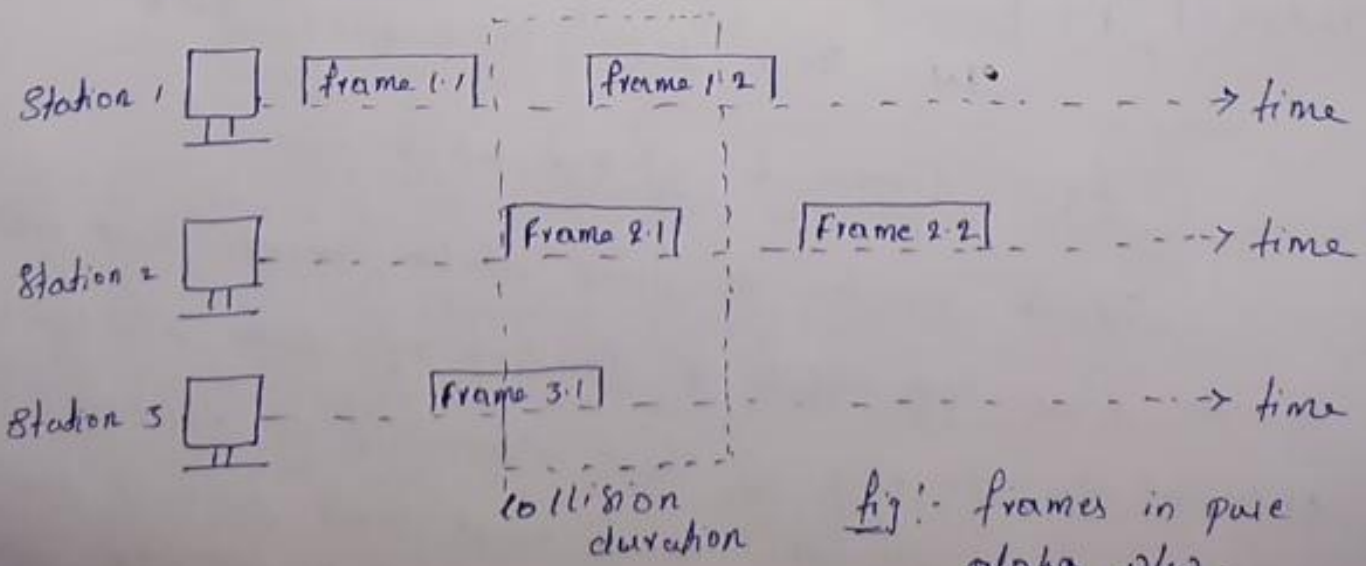


fig:- frames in pure aloha n/w.

when station sends data, it waits for an acknowledgement. if the acknowledgement doesn't come within the alloted time then the station waits for a random amount of time called back-off time (Tb) & re-sends the data. Since different stations wait for different amount of time, the probability of collision decreases.

* Slotted aloha:-

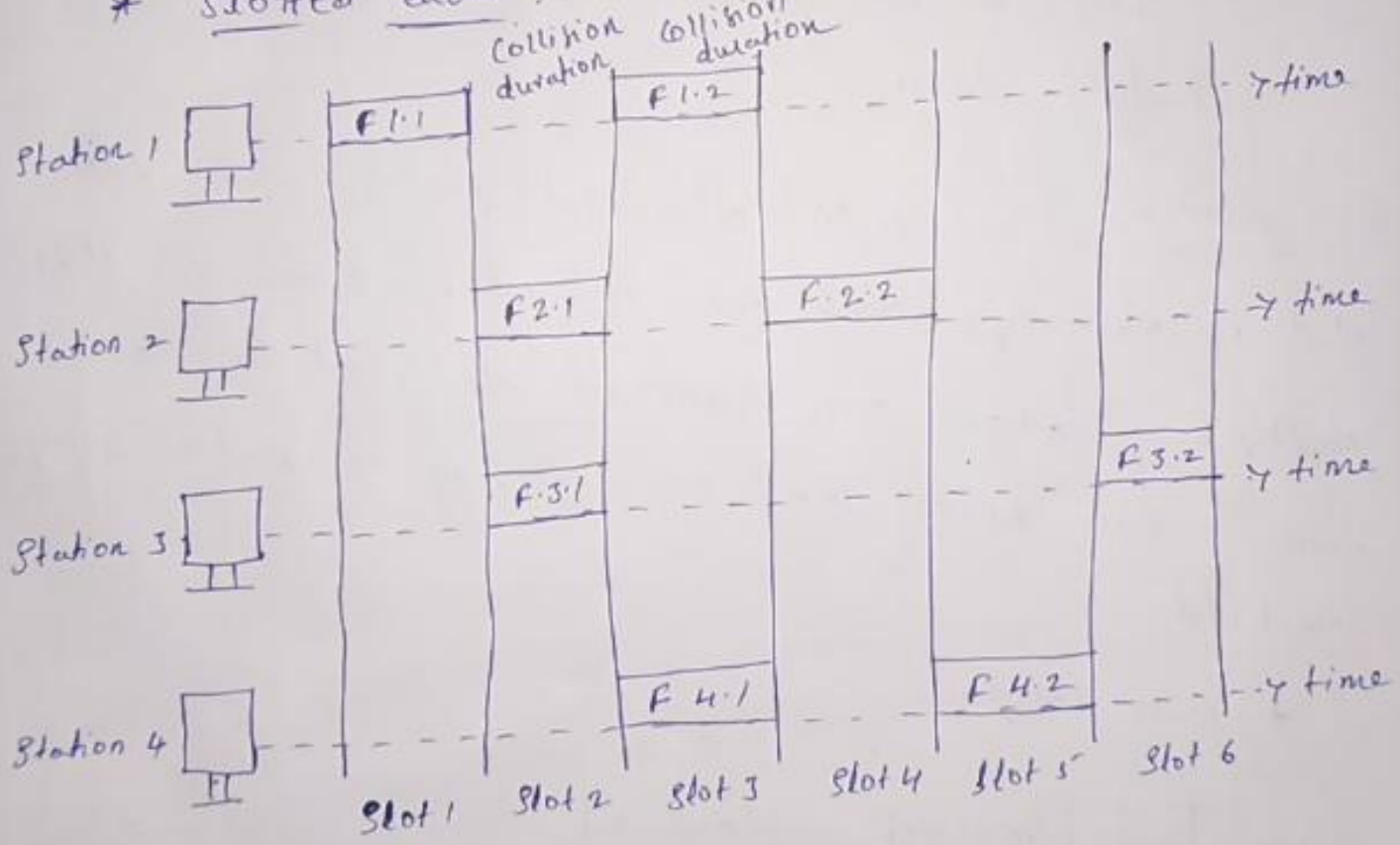


fig:- frames in Slotted aloha o/w

It is similar to pure aloha, except that we devide time into slots & sending of data is allowed only at the begning of these slots. if a station misses out the allowed time, it must wait for next time slot. this reduces the probability of collision.

⇒ <u>Controlled Access</u>:- In this the station seek information from one another to find which station has right to send. It allows only one node to send at a time, to avoid collision of messages on shared medium. three methods are used.

① Reservation

② polling

③ Token passing

① <u>Reservation</u>:-

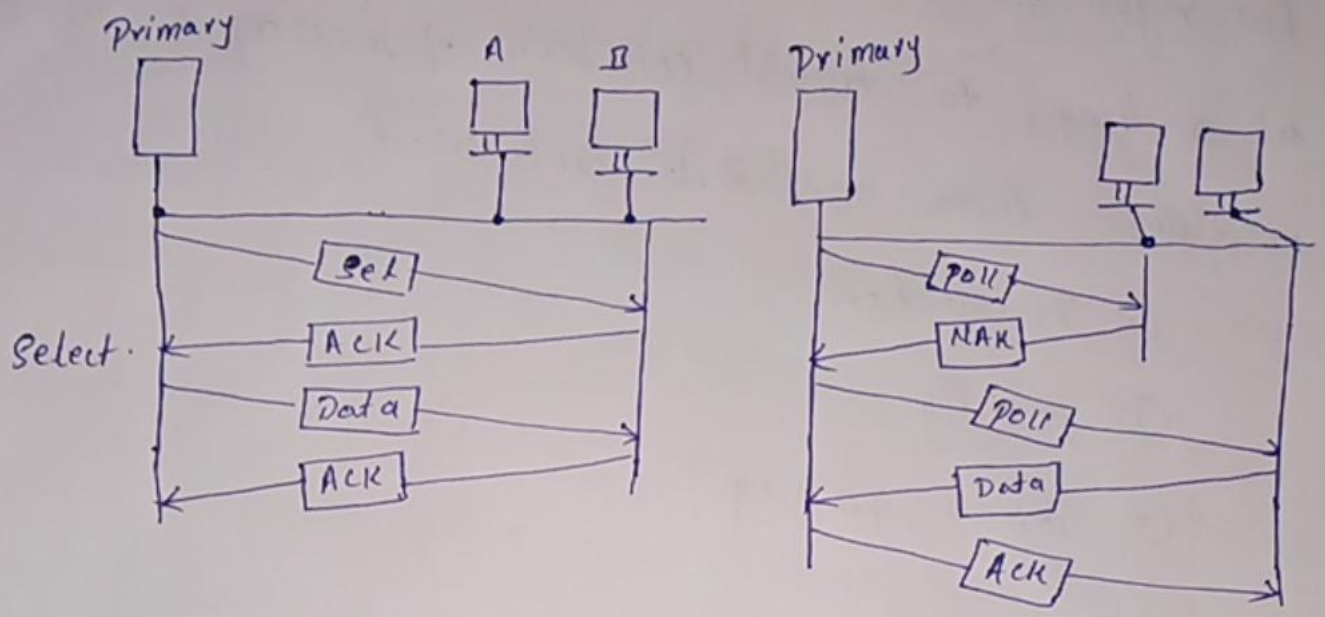
fig:- Reservation access method.

In this method, a station needs to make a reservation before sending data. time is divided into intervals. In each interval, a reservation frame precedes the data frames sent in that interval.

if there are N stations in the system, there are exactly N reservation minislots in the reservation frame. each minislot belongs to a station. when a station needs to send a data frame, it makes a reservation in its own minislot. the stations that medium is occupied (...)

have made reservations can send their data frames after the reservation frame.

② Polling:-



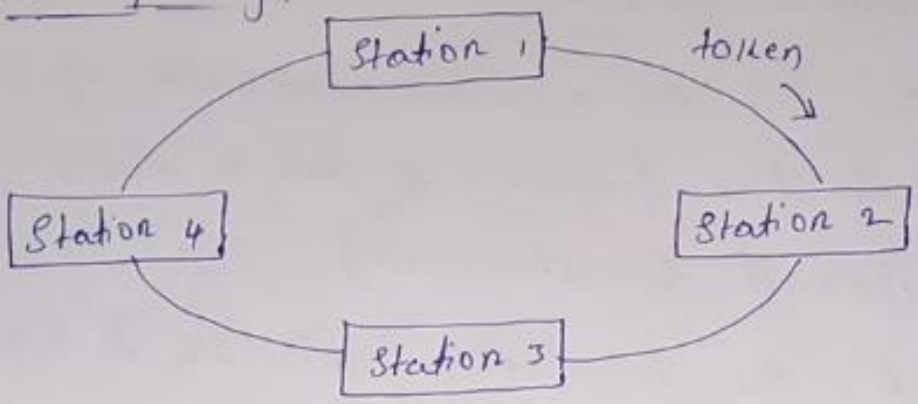
In this one acts as a primary station & the other are secondary stations. all data exchange must be made through the controller.

the msg sent by the controller contains the address of the node being selected for granting access.

Altough all nodes receive the message but the addressed one responds to it & send data, if any. if there is no data a "poll reject" (NAK) message is sent back.

Problems include high overhead of the polling message & high dependence on the reliability of the controller.

(3) Token passing :-



* In token passing scheme, the stations are connected logically to each other in form of ring & access of stations is governed by tokens.
* A token is a special bit pattern or a small msg, which circulate from one station to the next in some predifined order.
* In token ring, token is passed from one station to another adjacent station in the ring, whereas incase of tokken bus, each station uses the bus to send the token to next station in some predefined order.
* In both cases, token represents permission to send if a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. if it has no queued frame, it passes the token simply.
* After sending a frame, each station must wait for all N stations to send the token to their neighbours & the other N-1 stations to send a frame, if they have one.

⇒ channelization protocol:-

In this the available bandwidth of the link is shared in time, frequency & code to multiple stations to access channel simultaneously.

* FDMA:- The available bandwidth is divided into equal bands so that each station can be allocated its own band.

* TDMA:- In this bandwidth is shared b/w multiple stations. to avoid collision time is divided into slots & stations are alloted these slots to transmit data.

* CDMA:- In this method, one channel carries all transmission simultaneously. there is neither division of bandwidth nor division of time.

⇒ 802.11 MAC protocol:- It is popularly known as wifi, lays down the architecture & specifications of wireless LAN's. wifi or WLAN uses high freq. radio waves instead of cables for connecting the devices in LAN.

⇒ MAC frame :-

Frame Control	Duration/ID	Address 1	Address 2	Add 3	Sc	Add 4	Data	CRC
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 - 2312 bytes	4 bytes

Protocol version	Type	Subtype	To DS	From DS	More frag	Retry	Power Mgmt	More data	WEP	order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

* **Frame control (fc) :-** it is 2 bytes long field which defines type of frame & some control information. Various fields present in fc are:

1. version
2. Type
3. Subtype
4. To DS (Distributed system)
5. from DS
6. More frag
7. power management
8. Retry
9. More data
10. WEP
11. order.

* **Duration/ID :-** It is 2 bytes long field which contain the value indicating the period of time in which the medium is occupied (in μs).

* Address 1 to 4:- These are 6 bytes long fields which contains standard IEEE 802 MAC addresses.

* SC (sequence control):- it is 16 bits long field which consists of 2 sub-fields, i.e., sequence number (12 bits) & fragment number (4 bits).

* Data:- it is a variable length field which contain information specific to individual frames which is transferred transparently from sender to the receiver.

* CRC:- It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

UNIT - III

THE NETWORK LAYER

Introduction:- It is the layer 3 of OSI model & the layer that provides data routing paths for network communication, logical connection setup, data forwarding routing & delivery error reporting are the n/w layer primary responsibilities.

⇒ forwarding & routing

In network layer a router is used to forward the packets. each router has a forwarding table. A router forwards a packet by examining a packets header field & then using the header field value to index into the forwarding table.

the value stored in the forwarding table corresponding to the header field value indicates the router's outgoing interface link to which the packet is to be forwarded.

Routing algorithm

↓

forwarding table

Header value	o/p link
0100	3
0101	2
0111	2
1001	1

Scanned with CamScanner

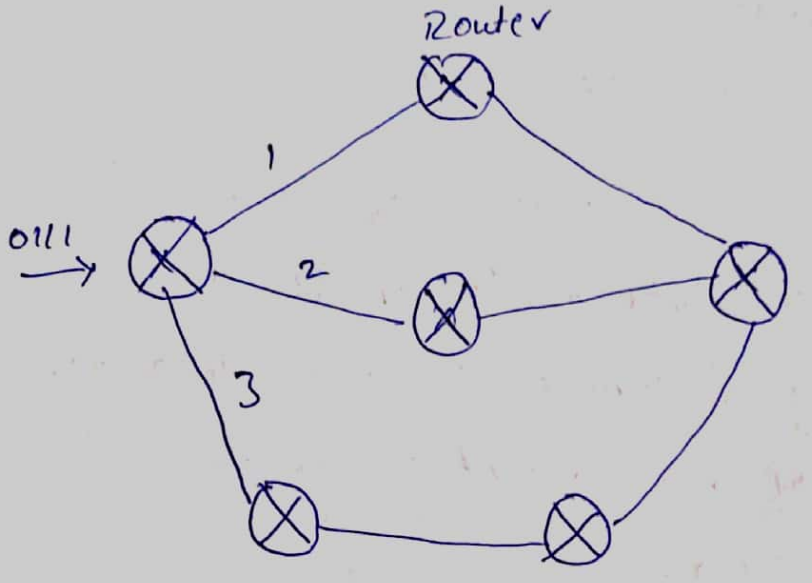


fig:- Routing algorithms determine the values in forwarding table.

→ Services provided by the network layer:-

* Gauranted delivery:- It provides the service which guarantees that the packet will arrive at its destination.

* Gauranted delivery with bounded delay:- It guarantees that the packet will be delivered within a specified host-to-host delay bound.

* In-order packets:- this service ensures that the packet arrives at the

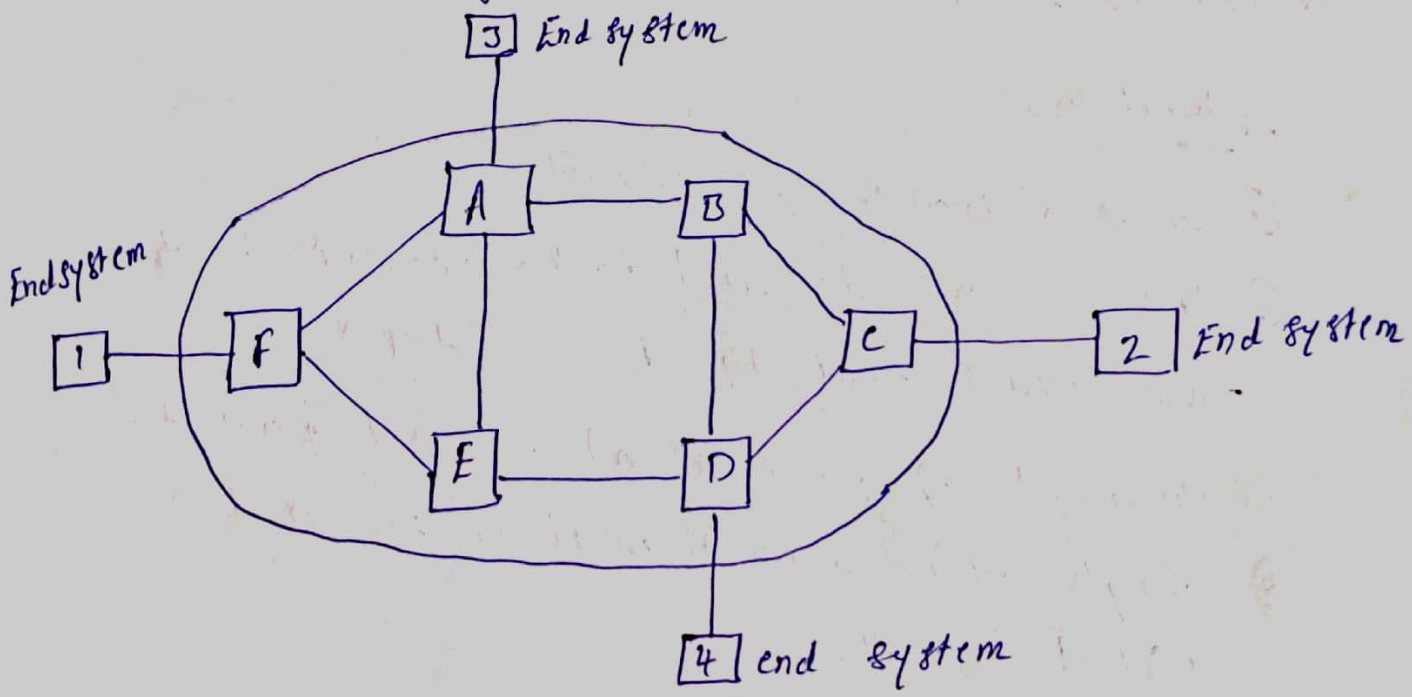
* Gauranted max jitter:- It ensures that the amount of time taken b/w two successive transmissions at the sender is equal to the time b/w their receipt at the destination.

* Security Services:- It is used to provide security by using a session key b/w the source & destination host.

Scanned with CamScanner

⇒ Virtual Circuit & Datagram n/w's :-

Virtual circuit :- It is the computer n/w providing connection-oriented service. It is a connection-oriented network. in virtual circuit resource are reserve for the time interval of data transmission b/w two nodes. this n/w is a highly reliable medium of transfer. virtual circuits are costly to implement.



Congestion control in virtual circuit :- once the congestion is detected in virtual circuit network, closed-loop technique is used. There are different approaches in this technique.

* **No new connection** :- No new connections are established when the congestion is detected. this approach is used in telephone n/w's. where no new calls are established when the exchange is overloaded.

Scanned with CamScanner

* participation of congested routes invalid :-

Another approach to control congestion is allow all new connections but route these new connections in such a way that contested routes is not part of this route.

* Negotiation :- To negotiate different parameters b/w sender & receiver of the n/w, when the connection is established.

Advantages :-

① It is reliable n/w circuit

② packets are delivered to the receiver in the same order sent by the sender.

③ No need for overhead in each packet.

④ Single global packet overhead is used in virtual circuit.

Disadvantages :-

① costly to implement

② provides only-connection-oriented service.

③ Always a new connection setup is required for transmission.

Scanned with CamScanner

⇒ Datagram networks :-

In a datagram n/w, each packet is treated independently of all others. even if a packet is part of a multi packet transmission, the network treats it as though it existed alone. packets in this approach are reffered as data gram. Datagram switching is normally done at network layer.

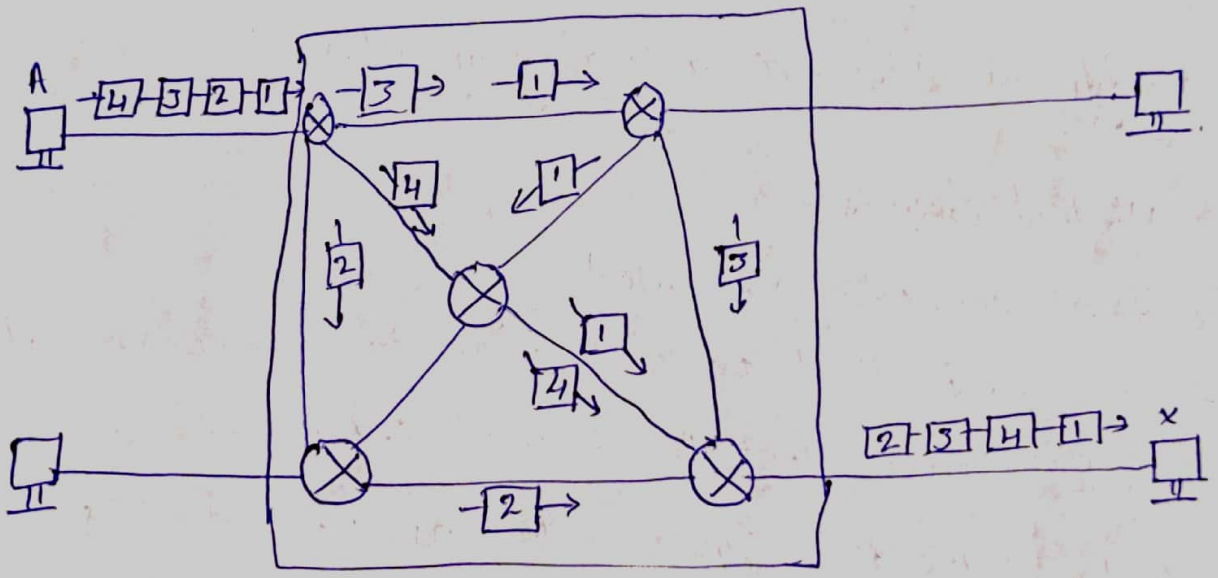


fig:- Datagram n/w deliver data from A to x

In this fig. all four packets belongs to the same message, but may travels to different paths to reach their destination. this is because links may be involved in

Scanned with CamScanner

carrying packets from other sources & do not have the necessary bandwidth available to carry all the packets from A to x.

This approach can cause the datagram of transmission to arrive at their destination out of order with different delays with packets. the datagram n/w's are sometimes reffered to as connectionless networks.

→ Differences b/w VC & Datagram n/w:-

Virtual circuits:-

* it is connection oriented
* The first sent packets reserves resources at each server along the path. Subsequent packets will follow the same path as the first sent packet for the connection time.
* Since all packets are going to follow the same path, a global header is required. only the first packet of the connection requires a global header. the remaining packets generally don't require global headers.
* Since all packets follow a specific path

Scanned with CamScanner

packets are received in order at the destination.

* Virtual circuit switching ensures that all packets successfully reach the destination. No packet will be discarded due to the unavailability of resources.

* Virtual circuits are highly reliable method for data transmission.

* The main issue with VC is that each time a new connection is setup, resources & extra information have to be reserved at every router along the path, which becomes problematic if many clients are trying to reserve a router's resources simultaneously.

Datagram networks:-

* It is a connectionless service. There is no need for reservation of resources as there is no dedicated path for a connection session.

* All packets are free to use any valuable path. As a result intermediate routers calculate routes on the go due to dynamically changing routing tables on routers.

* Since every packet is free to choose any path,

Scanned with CamScanner

all packets must be associated with a header with prior information about the source & upper layer data.

* the connectionless property makes data packets reach the destination in any order, which means that they can potentially be received out of order at the receiver's end.

* Datagram network's are not as reliable as virtual circuits.

* The major drawback of datagram packet switching is that a packet can only be forwarded if resources such as the buffer, CPU, & bandwidth are available, otherwise the packet will be discarded.

* But it is always easy & cost-efficient to implement datagram network as there is no extra ~~bandwidth~~ implementation of reserving resources & making a dedicated path each time an application has to communicate.

* It is generally used by the IP n/w, which is used for data services like the internet.

Scanned with CamScanner

→ Inside a Router - I/P Processing :-

A router is a networking device that forwards data packets b/w computer network.

A router has a number of interfaces by which it can connect to a number of host systems.

functions of a router :-

It performs basically two major functions.

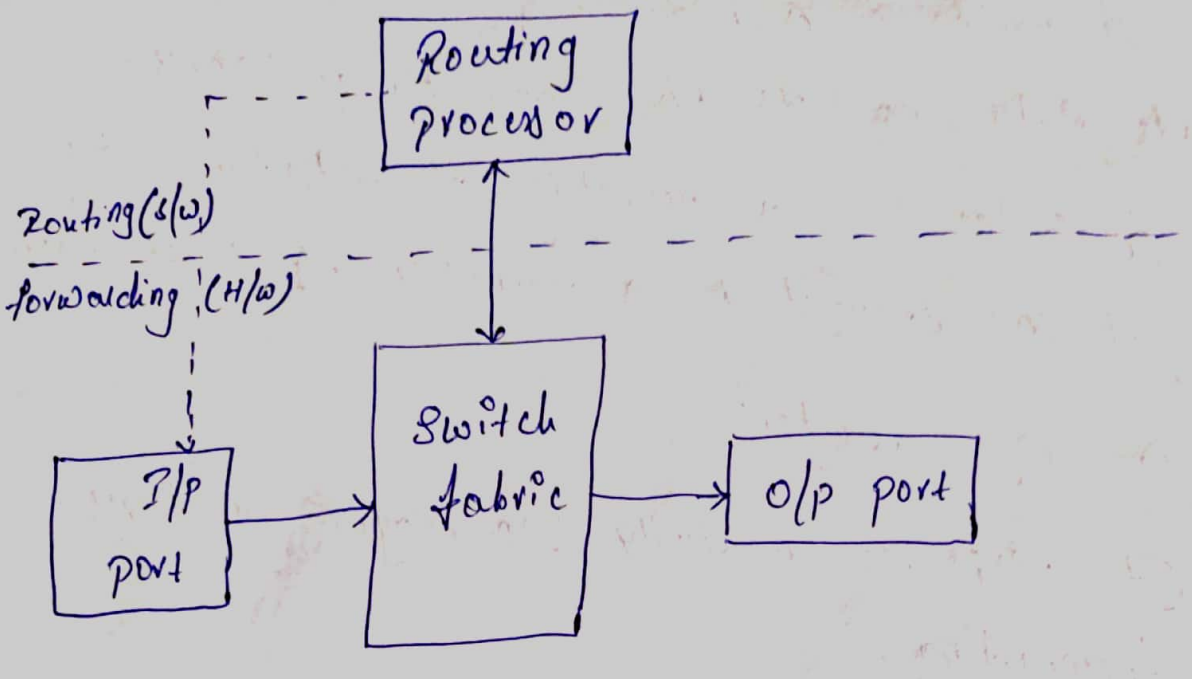
1. forwarding.
2. Routing.

forwarding :- Router receives the packets from its i/p ports, checks it header, performs some basic functions like checking checksum & then looks upto the routing table to find the appropriate output port to dump the packets onto, & forward the packets on to the output port.

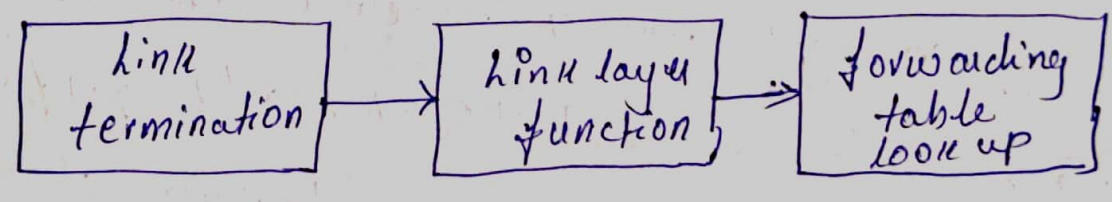
Routing :- It is the process by which the router ascertains what is the best path for the packet to reach the destination, it maintains a routing table which is made using different algorithms by the router only.

Scanned with CamScanner

Architecture of a Router:-



① I/P port:-



It is the interface by which packets are admitted into router, it perform several key functions as terminating the physical link at router, this is done by the leftmost part port in the fig.

Link layer is used for interoperating in link layer like decapsulation.

forwarding table is used to determine the appropriate o/p port based on the destination address.

Scanned with CamScanner

2 Switching fabric :-

It is the heart of router, it connects the I/P ports with the o/p ports. it is the kind of the n/w inside a networking device. the switching fabric can be implemented in no. of ways.

* Switching via memory :- In this we have a processor which copies the packet from I/P ports & sends it to the appropriate o/p. It works as a traditional cpu with i/p & o/p ports acting as i/p & o/p devices.

* Switching via bus :- In this implementation we have a bus which connects all the i/p ports to all the o/p ports. on receiving a packet & determining which o/p port it must be delived to, the i/p port puts a particular token on the packet & transfers it to the bus. All o/p ports are able to see the packets but it will be delivered to the o/p port whose token has been put in, the token is the scrapped off by the o/p port & the packet is forwarded.

Scanned with CamScanner

Switching via interconnection n/w :-

this is more sophisticated n/w, here instead of a single bus we use 2N bus to connect I/P & O/P ports.

③ **O/P port :-** this is the segment from which packets are transmitted out of the router.

O/P port looks at its queuing buffers & takes packets, does link layer functions & finally transmits the packets to outgoing link.

④ **Routing processor :-**

It executes the routing protocols, It employs various routing algorithm like link-state algorithm, distance vector algorithm etc.,

→ **Switching :-** Switching technique will decide the best route for the data transmission from source to destination.

Switching techniques.

- Circuit Switching
  - Space division switches
  - Time division switches
- Message Switching
- Packet Switching
  - Datagram approach
  - Virtual circuit approach

Scanned with CamScanner

→ Circuit Switching

* It establishes a dedicated path b/w sender & Receiver. if once the connection is established the path will remain to exist until the connection is terminated.
* In this technique when user want to send the information a request signal is sent to the receiver then the receiver sends back the ack. to ensure the availability of the path. After receiving the ack, dedicated path transfer the data.
* it is used in public telephone n/w. used for voice transmission
* fixed data can be transferred at a time in circuit switching technology.

Circuit switching can be either of two technologies:

1. Space division switches
2. Multi Stage switches

① Space division switches :- It is a technology single transmission path is accomplished in a switch by using physically separate set of cross points.

It is originally designed for use in analog n/w's but currently using in both analog & digital n/w's.

Scanned with CamScanner

* It has high speed, high capacity & non blocking switches.
* Space division will work under the principal of cross bar switches.

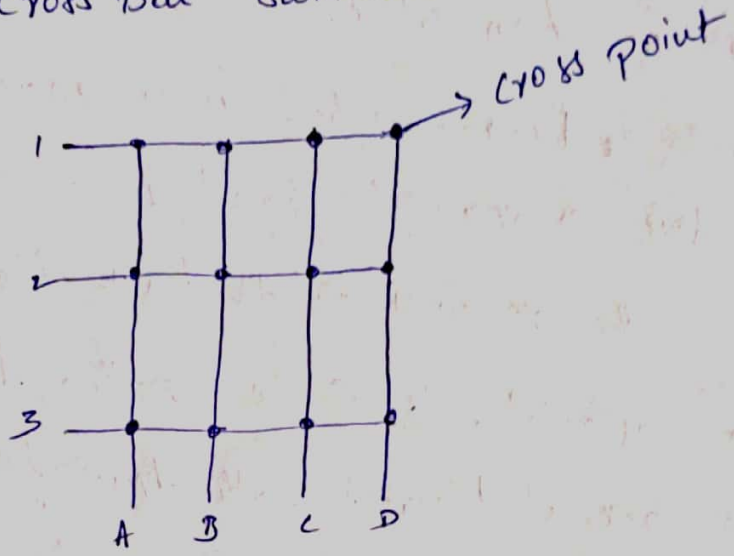


fig:- cross bar switch with 3 I/p's & 4 o/p's.

* crossbar switch have n I/p & o/p lines & have n^2 intersection points known as crosspoints.

Disadvantage:-

* The no of crosspoint increase as the no. of stations increase. therefore it becomes expensive for large switch
* To avoide this will use multi stage switch.

② Multi Stage Switch:-

* It is made by splitting the crossbar switch into the smaller units & then interconnecting them.
* It reduces the no. of cross points
* if one path fails, then there will be availability of another path.

Scanned with CamScanner

Advantages.

* The communication channel is dedicated
* It has fixed band width

Disadvantage:-

* More expensive
* No other data can be transferred in another the channel.

→ Message switching:-

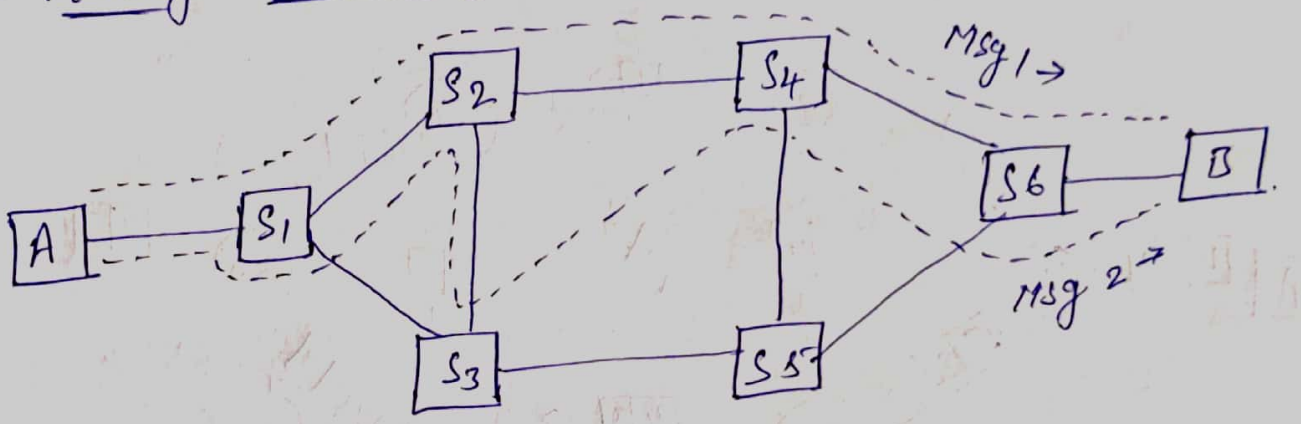


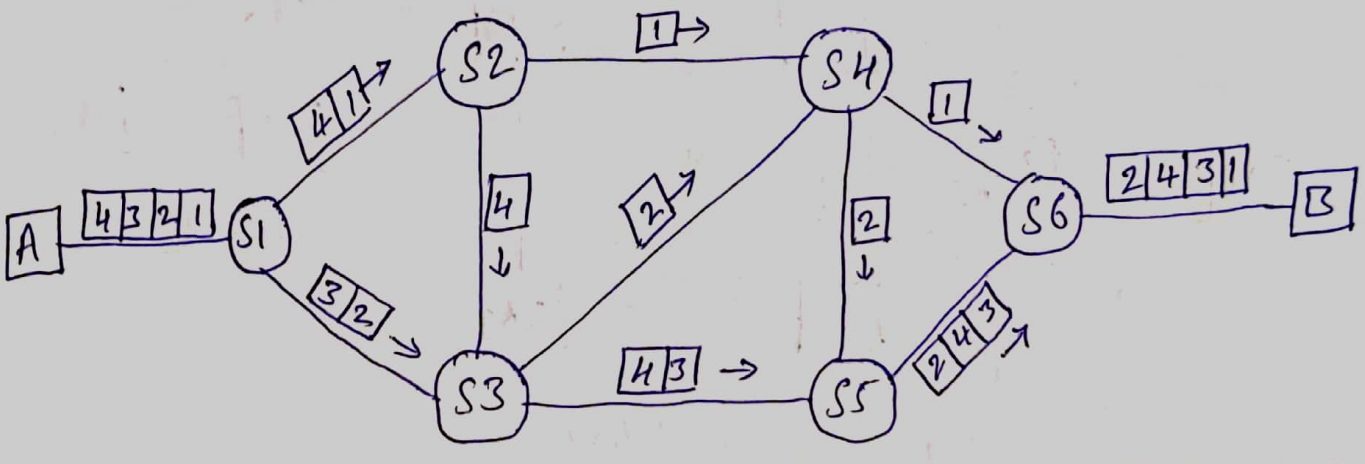
fig:- msg switching.

* A message is transferred as a complete unit & routed through intermediate nodes at which it is stored & forwarded.
* In this no dedicated path is established b/w Sender & Receiver.
* These are programmed in such a way so that they can provide most efficient routes.
* Each & every node stores the entire msg & then forward it to next node.

Scanned with CamScanner

* Data channels are shared among the communication devices that improve the efficiency of using available band width.
* Traffic congestion can be reduced because the message is temporarily stored in the nodes.
* Message priority can be used to manage the N/w.

→ <u>packet</u> <u>Switching</u>:-



* In this messages are divided & sent individually.
* The message splits into smaller pieces known as packets & packets are given a unique no. to identify their order at the receiving end.
* every packet contains some information in its header ~~& packets are~~ & such as source address, destination address & sequence number.
* these will travel accross the n/w by choosing shortest path.

Scanned with CamScanner

* All the packets are reassembled at the receiving end in correct order.
* If any packet is corrupted, then the msg. will be sent to resend the message.
* Ack. will be sent by receiver after the successful receiving of the packet at receiver section.

Approaches of packet switching

1. Datagram packet switching.
2. Virtual circuit switching.

Advantages:-

* cost-effective
* Reliable
* efficient

→ Routing control plane:-

It is the part of a n/w that controls how data packets are forwarded from one place to another. the process of creating a routing table is considered part of control plane. Routers use various protocols to identify n/w paths & they store these paths in routing tables.

Scanned with CamScanner

⟹ Internet protocol :-

The main task of ip is to deliver the packets from source to destination based on the IP address available in the packet header. IP defines the packet structure that hides the data which is to be delivered as well as the addressing method that labels the datagram with a source & destination information.

An IP provides the connectionless service, which is accompanied by two transport protocols, i.e., TCP/IP & UDP/IP, so, IP is also known as TCP/IP or UDP/IP.

IPV4 :- It is the delivery mechanism used by TCP/IP protocols.

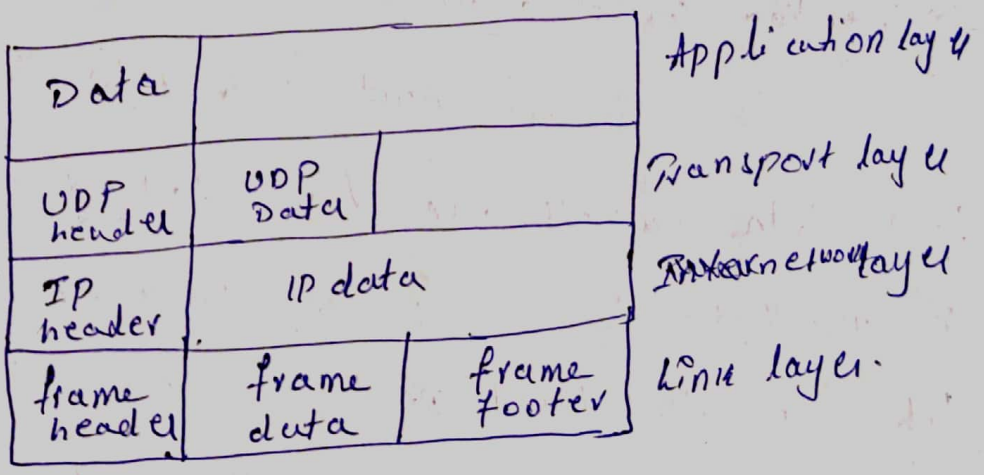


fig :-

It is an unreliable & connectionless datagram protocol. best effort delivery service.

Scanned with CamScanner

The term best-effort means that IPV4 provides no error control or flow control. It assumes the unreliability of the underlying layers & does its best to get a transmission through to its destination, but with no guarantees.

Datagram:- packets in the IPV4 layer are called datagrams. A datagram is a variable-length packet consisting of two parts:

header & data.

the header is 20 to 60 bytes in length & contains information essential to routing & delivery. In TCP/IP it is used to show the header in 4-byte sections.

* Version :- This 4-bit field defines the version of IPV4 protocol. Currently the version is 4. this field tells the IPV4 software running in the processing machine that the datagram has the format of version 4.

* Header length :- this 4-bit field defines the total length of the datagram header in 4-byte words.

Scanned with CamScanner

this field is needed because the length of header is variable.

* Services:- The internet engineering task force (IETF) has changed the interpretation & name of this 8-bit field.

IPV6:- IP V4 has some deficiencies that make it unsuitable for the fast-growing internet.

* Despite all short-term solutions

* Internet must accommodate real-time audio & video transmission. this type of transmission requires minimum delay strategies & reservation of resources not provided in IPV4 design.

* The internet must accommodate encryption & authentication of data for some applications. No encryption or authentication is provided by IPV4.

To overcome these deficiencies, IPV6 was proposed. In IPV6 the IP was extensively modified to accomodate the unforseen growth of the internet. the format & length of the IP address were changed along with the

Scanned with CamScanner

Packet format.

Advantages:-

* Larger address space
* Better header format
* New options
* Allowance for extension
* Support for resource allocation
* Support for more security.

→ ICMP (Internet control msg protocol):-

Since IP does not have an inbuilt mechanism for sending error & control msgs. It depends on ICMP to provide an error control. It is used for reporting errors & management queries. It is a supporting protocol & is used by the n/w devices like routers for sending error messages & operations information.

ICMPv4 packet format:-

Type (8 bit)	code (8 bit)	checksum (16 bit)
Extended Header (32 bit)		
Data / payload (variable length		

Scanned with CamScanner

* Source quench msg:- Decrease the traffic rate for msgs sending to destination
* parameter problem:-
* Time exceeded message:-
* Destination un-reachable:-
* Redirection message

Scanned with CamScanner