* Basic Terminologies :

- Protocol - set of rules in layer / network
- topologies - Architecture of the network
- MAC Address - physical Address.

* LAYER ARCHITECTURE :

- It simplifies the network design.
- It is easy to debug network applications in layered Architecture.
- Network layers follow a set of rules, called protocol.

* OPEN SYSTEMS INTERCONNECTION (OSI) MODEL :

- The term "open" denotes the ability to connect any two systems which confirm to reference model and associated standards.

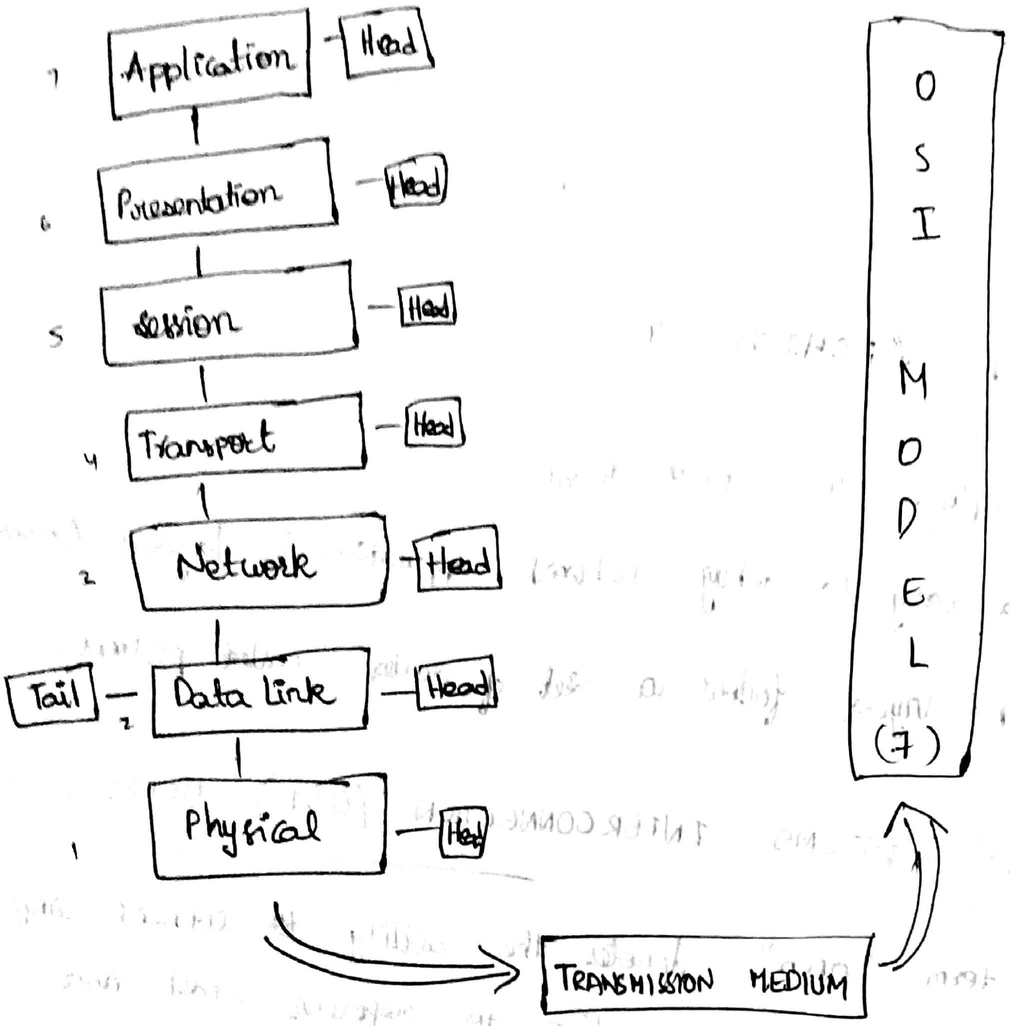
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems.

- This seperation into smaller more manageable functions is known as layering.

Physical - Bits
Datalink - frames
Network - datagram
Transport - Segment
Session - Segment
presentation - message
Application - original Text message

GUDI VARAPRASAD - COMPUTER NETWORKS

*. 7 LAYERS in Reference Model



- Each layer provides a service to the layer above it in the protocol specification.

- The lower 4 layers (Transport, network, data link, physical) are concerned with the flow of data from end to end through networks.

- The upper 3 layers (application, presentation and session) are oriented more towards services to the applications.

GUDI VARAPRASAD - COMPUTER NETWORKS

1. Physical layer - To transmit bits over a medium; to provide mechanical & electrical specifications.

2. Data Link layer - To organize bits into frames; to provide hop-to-hop delivery.

3. Network layer - To move packets from source to destination; to provide internetworking.

4. Transport layer - To provide reliable process-to-process message delivery and error recovery.

5. Session layer - To establish, manage, terminate sessions.

6. Presentation layer - To translate, encrypt & compress data.

7. Application layer - To allow access to network resources.

*. TCP/IP PROTOCOL :

7 layers	5 layers	
Application	Application Layer	Several Application Protocols
Presentation		
Session		
Transport	Transport	Transport protocol
Network	Network	Internet protocol, some helping
Data Link	Data Link layer	Underlying LAN WAN Technology
Physical	Physical layer	
OSI Model	TCP/IP Protocol suite	

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

① **Link layer** :
- Ethernet, PPP, switches (Hardware devices)
- Combination of Physical + Data link layers.
- Includes device driver & network interface card.

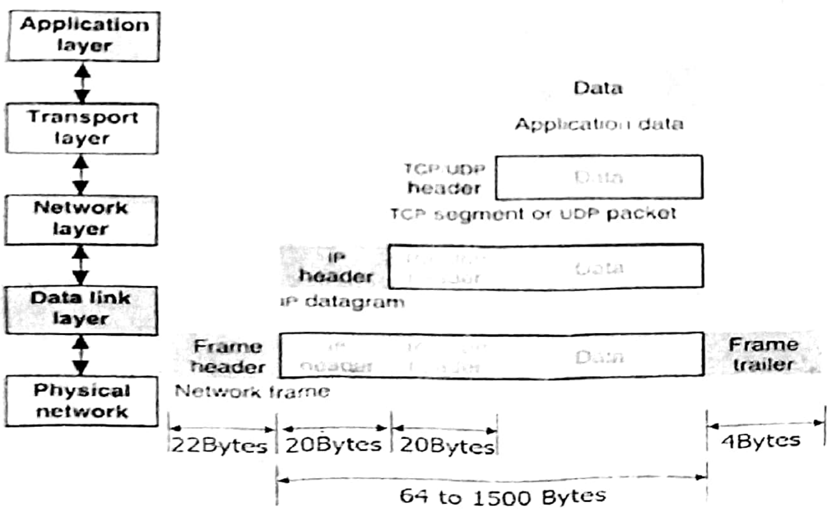
② **Network layer** : handles the movement of packets (Routing)
Internet Protocol (logical address) – Routers are used

③ **Transport layer** : Provides a reliable flow of data between two hosts. (client / server)

→ TCP – Transmission control protocol : Data is transferred in a particular sequence, packets arrive in order at the receiver.

→ UDP – There is no sequence followed in Data Transmission

④ **Application layer** : handles the details of the particular application
Browser is the medium of Transfer (Protocols like HTTP, SMTP, POP3, FTP, ...)



*. ADDRESSING :

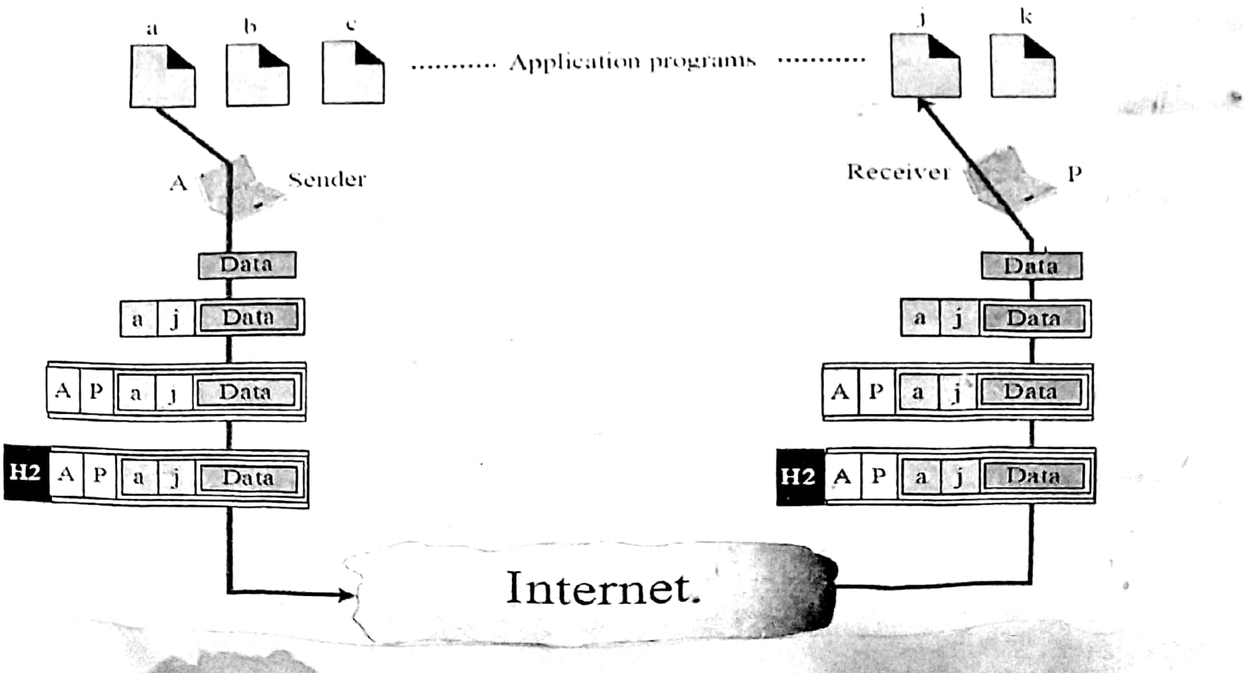
Message	Application layer	— Application specific address
Segment	Transport layer	— Port Address
Datasegment	Network layer	— logical Address (IP)
Frame	Data link layer	— Physical Address (MAC)
Bits	Hardware devices	— phone (device) id

- Most of the local Area networks use a 48-bit (6 byte) physical Address written as 12 hexadecimal bits; every byte (2 hexa) is seperated by colon like :

$$\boxed{07:01:02:01:2C:4B}$$

A 6-byte (12 hexa digits) physical address

- The physical address will change from device to device but the IP address will be same. (logical address) and the port address also remains the same.



GUDI VARAPRASAD - COMPUTER NETWORKS

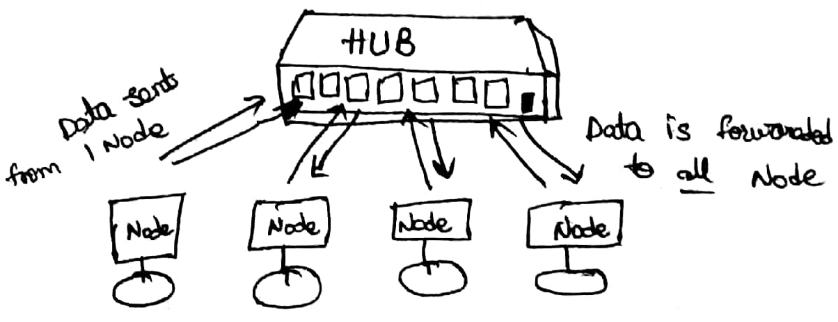
GUDI VARAPRASAD - COMPUTER NETWORKS

*. NETWORKING COMPONENTS & DEVICES :

- Hubs : A device with several ethernet ports.
- Switches : An efficient device designed better than hubs to transfer frames
- Bridges : To avoid network Traffic , connect networks - Bridges.
- Routers : A device to route data around the network.
- Gateways : A device to convert data from one form to other.
- Network interface cards (NICs) :
- ISDN Adapters :
- Wireless Access Points (WAPs) :
- Modems :
- Transceivers (media converters) :
- Firewalls :

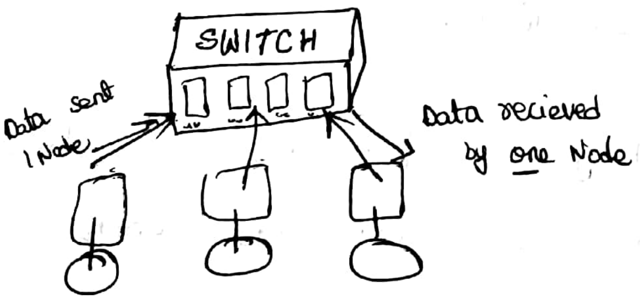
*. Broadcasting :

- The method of sending data to all systems regardless of intended recipient is called Broadcasting.



*. SWITCHES :

- As with hub, computers connect to a switch via a length of twisted pair cable.
- Rather than forwarding data to all the connected ports, a switch forwards data only to the port on which the destination system is connected.
- It looks at the media Access Control (MAC) address of the devices connected to it to determine the correct port.
- A MAC address is unique number that is stamped into every NIC. (Network Interface card).



*. SWITCHING METHODS :

- Cut - through : In a cut - through configuration, the switch begins to forward the packet as soon as it is received.
- Store - Forward : The switch waits to receive the entire packet before begining to forward it. It also performs basic error checking [CRC]
- Fragment - Free : By Reading only the part of packet to identify fragments of transmission.

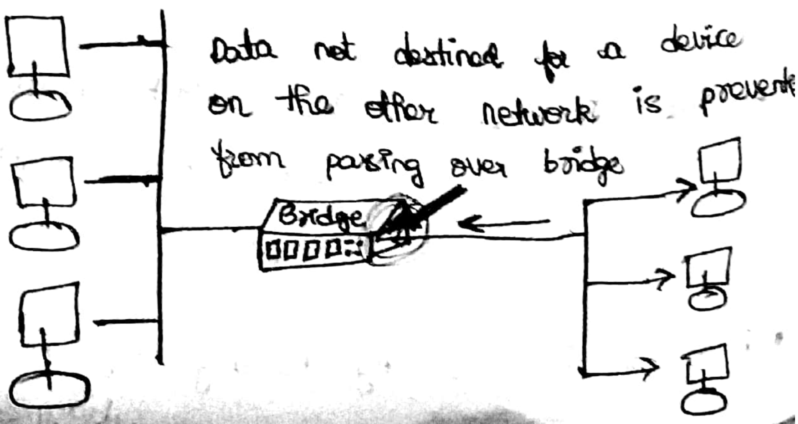
GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- Latency - The time it takes for data to travel between two locations is known as latency. The higher the latency, the bigger the delay in sending the data.

*. BRIDGES :

- Bridges are networking devices that connect networks.
- Sometimes it is necessary to divide networks into subnets to reduce the amount of traffic on each layer subnet or for security reasons.
- Once divided, the bridge connects the two subnets and manages the traffic flow between them.
- A bridge functions by blocking or forwarding data, based on the destination MAC address written into each frame of data.
- If bridge believes the destination address is on network other than that from which the data was received. It can forward data to other networks to which it is connected.



*. ROUTERS :

- Routers are network devices that literally route data around the network.

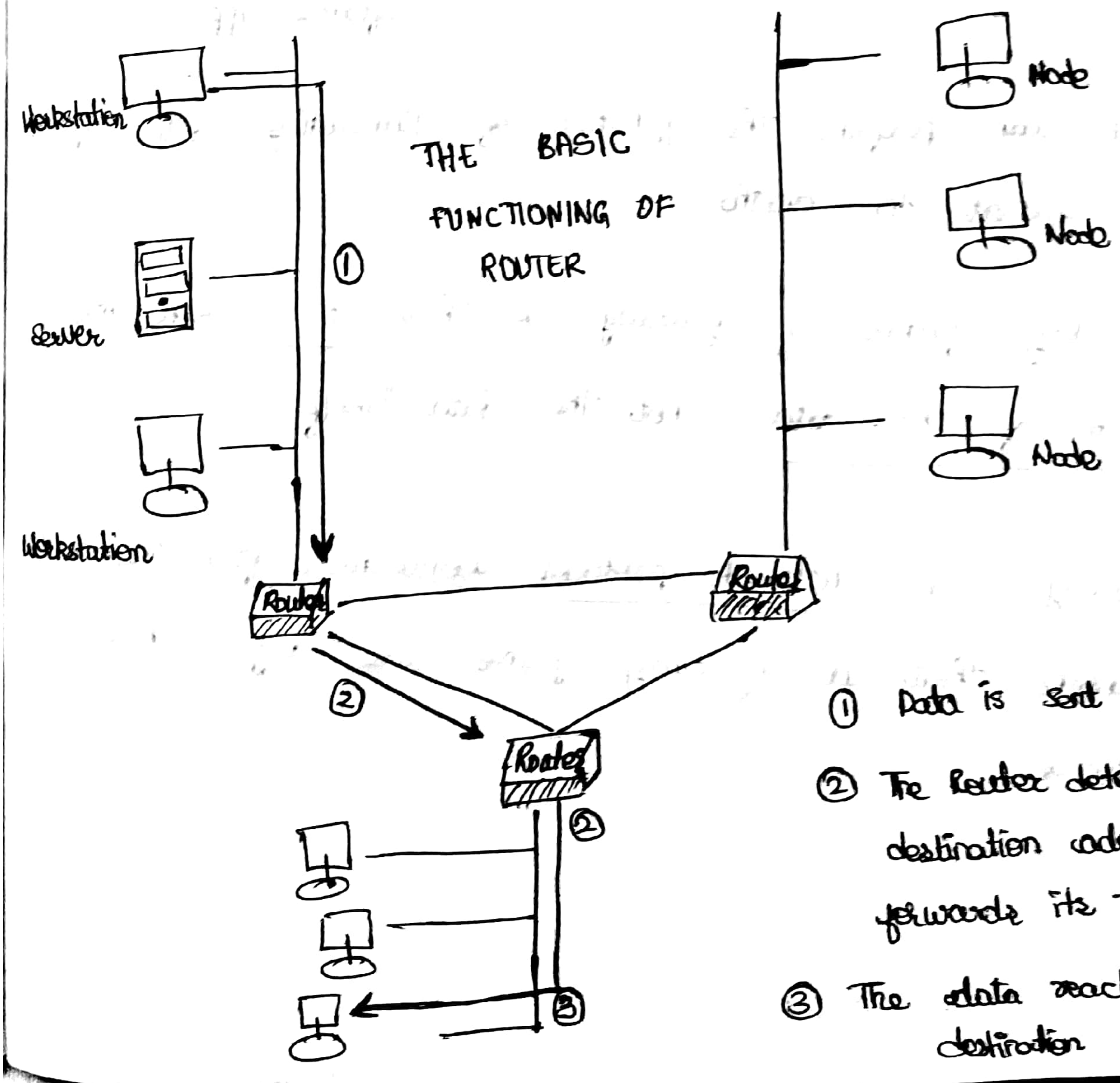
- By examining data as it arrives :

→ The router can determine destination address for the data.

→ Then by using tables of defined ~~users~~ routers, the router determines the best way for data to continue its path.

→ Unlike bridges and switches, which use the hardware configured MAC address.

→ To determine the destination of data, routers use the software configured network address to make decisions.



① Data is sent to Router

② The Router determines the destination address and forwards its to next.

③ The data reaches its destination

GUDI VARAPRASAD - COMPUTER NETWORKS

- When a change does occur on the network, it may take some time for all the routers to learn of the change.

- The process of each router learning the change and updating its routing tables is known as convergence.

- Each time the route is added to table, the node count for the route increases - a problem known as the count to infinity.

*. GATEWAYS :

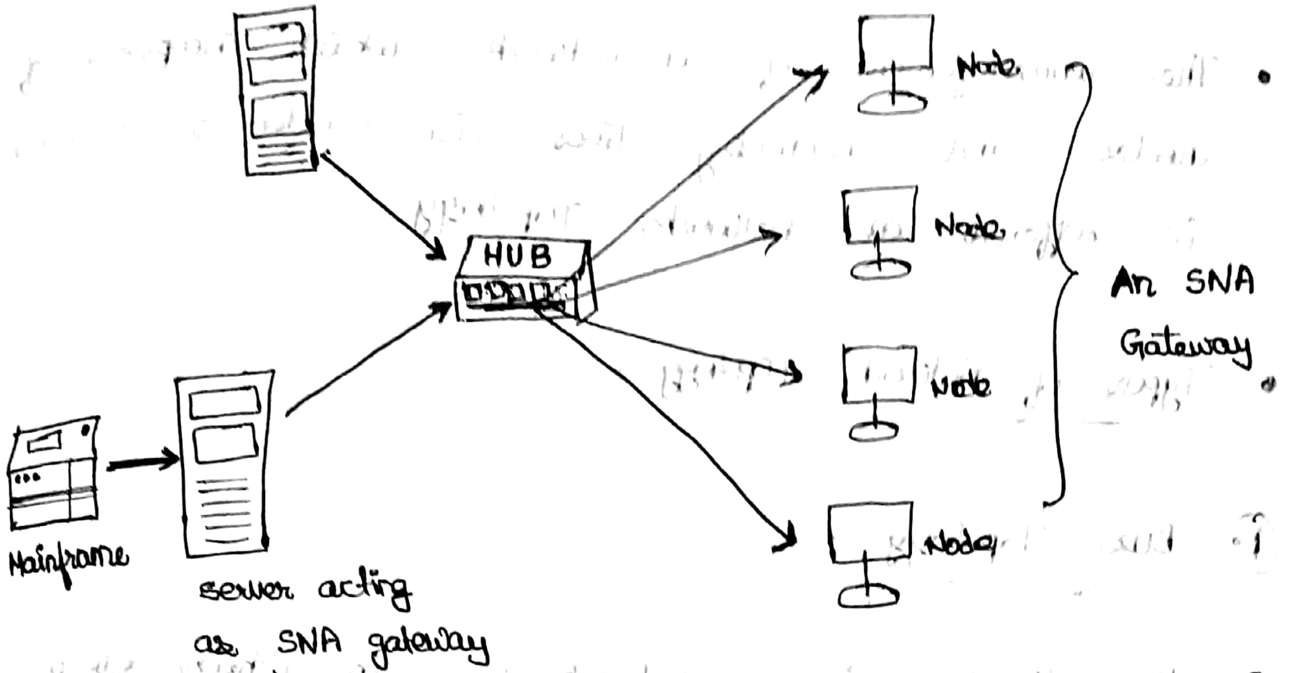
- This term is applicable to → device, system, software app

- That can perform the function of translating data from one format to another.

- The key feature of gateway is that it converts the format of the data, not the data itself.

- Gateways are network protocol converters. Often the two networks that a gateway joins use different base protocols.

GUDI VARAPRASAD - COMPUTER NETWORKS



- These systems transmit mail internally in certain format.
- When email needs to be sent across the Internet to users using a different email system,
- The email must be converted to SMTP (Simple Mail Transfer Protocol)
- This conversion process is performed by software Gateway.
- When computer - server acts as gateway, it also operates as firewall and a proxy server.

Ex

- If you have wireless network at home that gives your entire family access to the Internet, your gateway is the modem. Your ISP provides so you can connect to their network.
- On the other end, the computer that controls all of the data traffic your (Internet Service provider) ISP takes and sends out is itself a node.

GUDI VARAPRASAD - COMPUTER NETWORKS

*. NETWORK TOPOLOGY :

- The arrangement of a network which comprises of nodes and connecting lines via sender & receiver is reffered as network Topology.

- Types of Network Topology :

(1) Bus Topology :

- Bus Topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then its called Linear Bus topology.

- Features of Bus Topology :

→ Transmits data only in one direction.

→ Every device is connected to single cable.

- Advantages of Bus Topology :

→ It is cost effective.

→ Cable required is least compared to other network topology

→ Used in small networks.

→ It is easy to understand.

→ Easy to expand joining two cables together.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

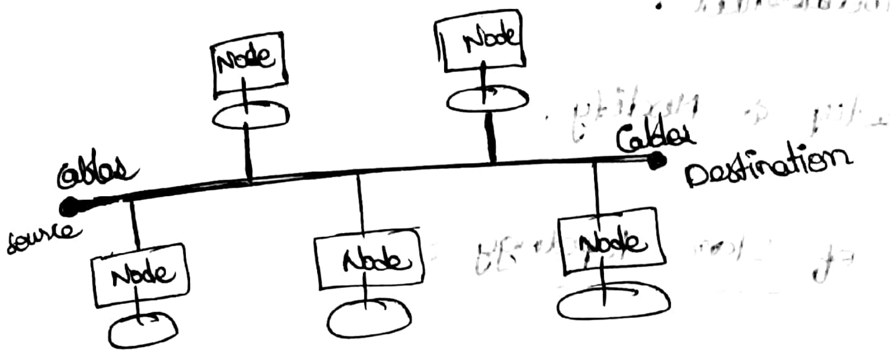
- Disadvantages of Bus Topology :

→ Cables fails then whole network fails.

→ If network traffic is heavy or nodes are more the performance of the network decreases.

→ Cable has a limited length.

→ It is slower than the ring topology.



BUS TOPOLOGY

② STAR TOPOLOGY :

- All the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

- Features of Star Topology :

→ Every node has its own dedicated connection to hub

→ Hub acts as repeater for every data flow.

→ Can be used with twisted pair, optical Fibre.

GUDI VARAPRASAD - COMPUTER NETWORKS

- **Advantages of Star Topology :**

→ Fast performance with few nodes and low network traffic.

→ only that node is affected which has failed, rest of the nodes can work smoothly.

→ Hub can be upgraded easily.

→ Easy to Troubleshoot.

→ Easy to setup & Modify.

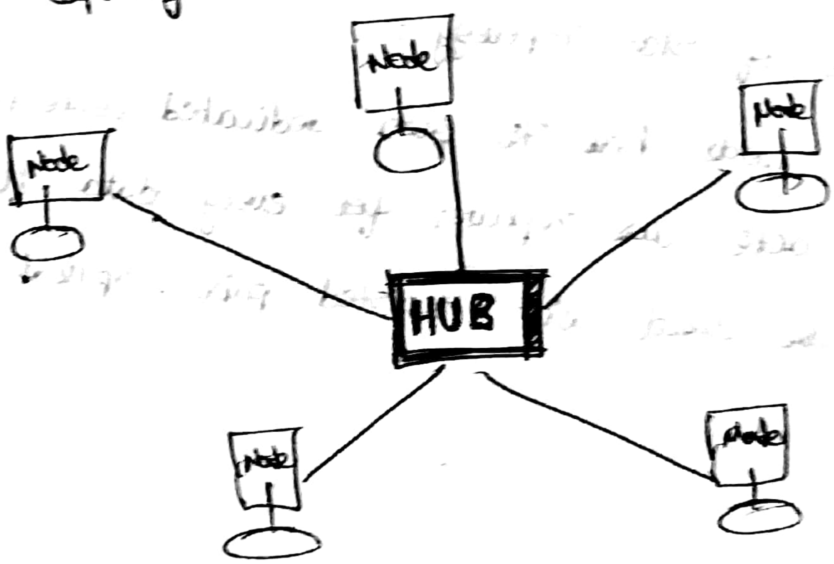
- **Disadvantages of Star Topology :**

→ Cost of Installation is High.

→ Expensive to use.

→ If Hub fails to function, then whole network is stopped because all the nodes depend on the hub.

→ Performance is based on the hub that is depends on its Capacity.



③ RING TOPOLOGY :

- It forms a ring as each computer is connected to another computer, with the last one connected to the first.
- Exactly two neighbours for each device.
- Features of Ring Topology :

→ The no. of repeaters used for Ring Topology with large no. of nodes.

→ The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, (is called Dual Ring Topology.)

→ Data is transferred in sequential manner that is by bit by bit. Data transmitted has to pass through each node of the network, till the destination node.

- Advantages of Ring Topology :

→ Transmitting network is not affected by high traffic. or by adding more nodes, as only the nodes having tokens can transmit data.

→ Cheap to Install & Expand.

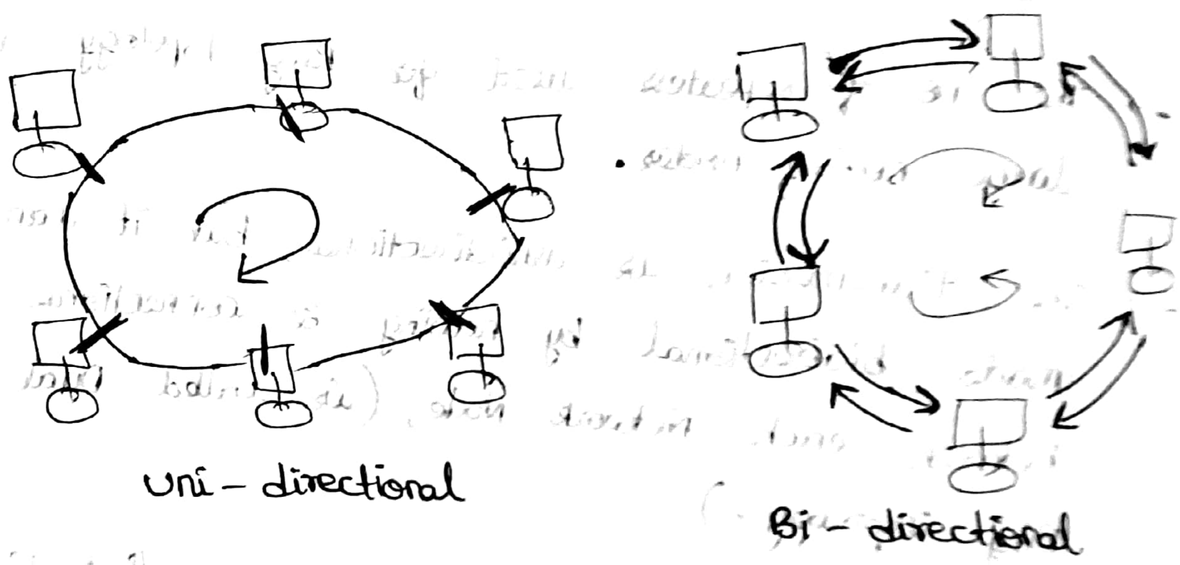
GUDI VARAPRASAD - COMPUTER NETWORKS

- Disadvantages of Ring Topologies :

→ Troubleshooting is difficult in Ring Topology.

→ Adding or deleting nodes (new computers) disturbs the entire network & activity.

→ Failure of 1 computer disturbs the whole network.



④ MESH TOPOLOGY :

- It is point to point connection to other nodes or devices. All the network nodes are connected to each other.

- Mesh has $\frac{n(n-1)}{2}$ physical channels to link n devices.

- There are two techniques to transmit data over Mesh Topology → Routing, → Flooding

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- Types of Mesh Topology :

→ Partial Mesh Topology – Partial connection of devices.

→ Full Mesh Topology → every connection to each & every node.

- Features of Mesh Topology :

→ Fully Connected

→ Robust

→ Not Flexible.

No. of Cables required = $\frac{n \times (n-1)}{2}$

No. of ports required = $(n-1) \times n$

- Advantages of Mesh Topology :

→ Each connection can carry its own data load.

→ It is Robust.

→ Fault is diagnosed easily.

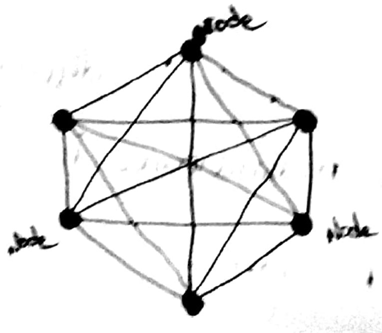
→ Provides security and Privacy.

- Disadvantages of Mesh Topology :

→ Installation and Configuration is difficult.

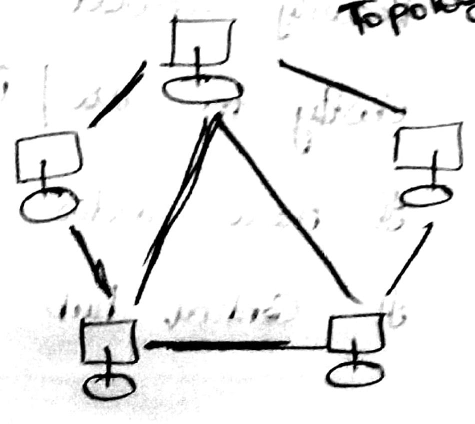
→ Cabling cost is more.

→ Bulk wiring is required.



Full Mesh Topology

Partial Mesh Topology



GUDI VARAPRASAD - COMPUTER NETWORKS

⑤ TREE TOPOLOGY :

- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical Topology. It should at least have three levels of Hierarchy.

- **Features of Tree Topology :**

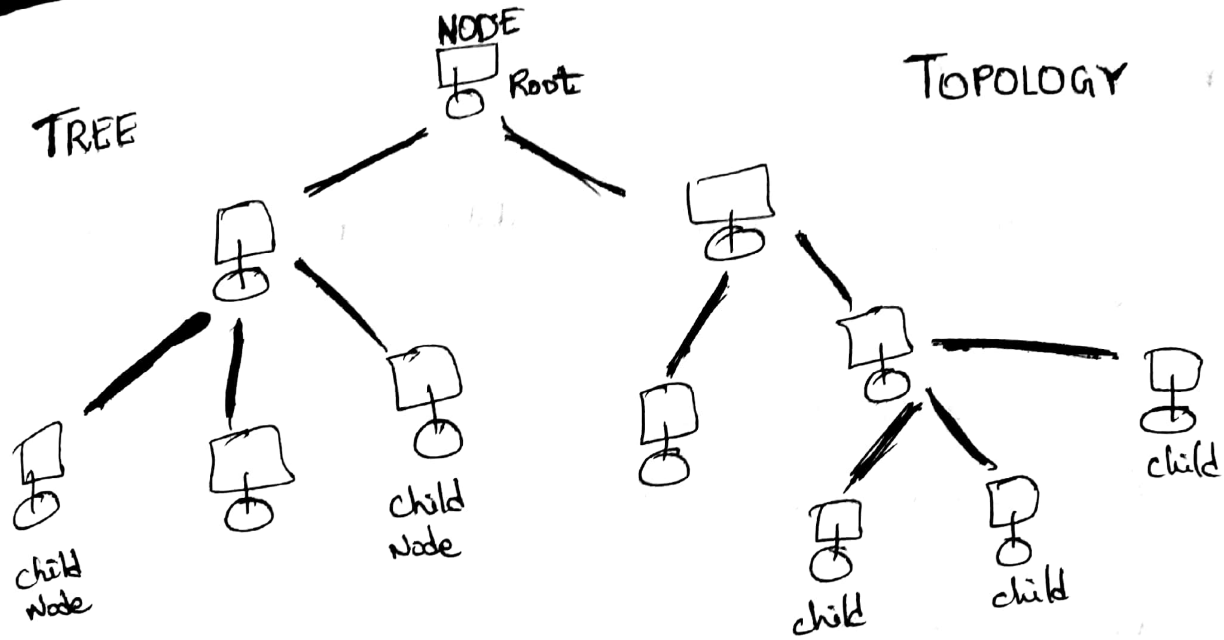
→ Ideal if workstations are located in groups.
→ Used in wide Area Network.

- **Advantages of Tree Topology :**

→ Extension of Bus Topology & star Topology
→ Expansion of Nodes is possible & easy.
→ Easily managed & maintained.
→ Error detection is easily done.

- **Disadvantages of Tree Topology :**

→ Heavily cabled
→ Costly to use / implement
→ If more nodes are added, maintainance is difficult.
→ If Central hub fails, network fails.



⑥ HYBRID TOPOLOGY :

- Hybrid Topology combines two or more Topologies.
- Features of Hybrid Topology :

→ It is a combination of many topologies.

→ Inherits the advantages / disadvantages of the involved topologies.

- Advantages of Hybrid Topology :

→ Reliable as error detecting and trouble shooting is easy.

→ Effective in terms. and Flexible too.

→ Scalable as size can be increased easily.

Parameter	BUS	STAR	RING	MESH
Installation	Easy	Easy	Difficult	Difficult
Cost	inexpensive	expensive	moderate	expensive
Flexible	yes	yes	no	no
Reliability	moderate	high	high	high
Extension	easy	easy	easy	difficult
Robust	no	yes	no	yes

GUDI VARAPRASAD - COMPUTER NETWORKS

*. DATA TRANSMISSION :

- The succesful transmission of data depends on two factors :

1. Quality of the signal being transmitted.
2. Characteristics of the transmission medium.

*. TRANSMISSION TERMINOLOGY :

- Data Transmission occurs between transmitter and receiver over some transmission medium
- Communication is in the form of electromagnetic waves.
- Guided Media - Twisted pair, coaxial cable, optical fiber
- UnGuided Media - (wireless) air, vaccum, seawater.
- Direct Link - No intermediate devices.
- Point to Point - Direct link + only 2 devices share link.
- Multi-point - more than two devices share the link.
- Simplex - signals transmitted in one direction
- Half duplex - both stations transmit but only one at a time
- Full duplex - Simultaneous transmissions.

GUDI VARAPRASAD - COMPUTER NETWORKS

*. FREQUENCY, SPECTRUM & BANDWIDTH :

- Time Domain – Sine wave, square wave, ...
  - → Analog signal – various in a smooth way over time.
  - → Digital signal – Maintains constant level & then changes.
  - → Periodic domain – Pattern over a period of time.
  - → Aperiodic signal – No pattern repeats over a period of time

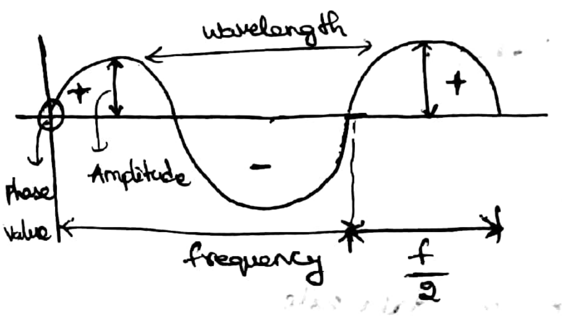
- Wavelength :

→ wavelength is a distance occupied by single cycle.

→ The distance between two points of corresponding phase of two consecutive cycles.

→ wavelength, $\boxed{\lambda = v \cdot T}$ or $\boxed{\lambda = \frac{v}{f}}$.

→ Especially when $v = c$, $c = 3 \times 10^8$ m/s is speed of light in free space.



Sine Wave

wavelength = propogation speed × period

- Period of total signal = Period of fundamental frequency.
- Harmonic frequency = a multiple of fundamental frequency.

GUDI VARAPRASAD - COMPUTER NETWORKS

*. SPECTRUM & BANDWIDTH :

- Spectrum – range of frequencies contained in a signal.
- Absolute bandwidth – width of spectrum.
- Effective bandwidth – narrow band of frequencies containing most of the energy.
- DC Component – Component of zero frequency.
- No DC component ⟹ average amplitude = 0.
- DC Component is undesirable (avg amplitude ≠ 0).
- Bandwidth = frequency of highest – frequency of lowest

*. DATA RATE & BANDWIDTH :

- Data Rate – Rate at which data can be communicated (in bits per second).
- Bandwidth – Constrained by transmitter, medium. (In cycles per second, or Hertz).
- Channel – A communication path.
- IMP Transmission system ∝ Bandwidth ∝ data rate
- Limiting bandwidth creates distortions.
- This is the direct relationship between data rate & bandwidth.
- Data Rate, $\boxed{R = 2f}$, f is fundamental frequency

GUDI VARAPRASAD - COMPUTER NETWORKS

* TRANSMISSION IMPAIRMENT :

- Signals travel through transmission media, which are not perfect.
- Imperfection causes signal impairment.
- Signal at the beginning of medium is not the same as the signal at the end of the medium.
- What is sent is not what is received.
- Three causes of impairment are attenuation, distortion and noise.

- Attenuation : Loss of Energy (insufficient Bandwidth)
- Attenuation works like Doppler Effect.

Example : Suppose a signal travels through a transmission medium and its power is reduced to one half. This means $P2 = 0.5\ P1$. In this case, the attenuation is calculated —

Sol :

$$\boxed{\text{Attenuation} = 10 \log_{10}\left(\frac{P_2}{P_1}\right)}$$

$$= 10 \times \log\left(\frac{0.5P_1}{P_1}\right) = -3 \text{ dB}$$

∴ A loss of 3dB is attenuation in this scenario.

Example : A signal travels through an amplifier and its' power is increased 10 times. This means that $P_2 = 10P_1$.

In this case, the amplification (gain of power) is —

GUDI VARAPRASAD - COMPUTER NETWORKS

$$\boxed{\text{Amplification} = 10 \log_{10}\left(\frac{P_2}{P_1}\right)} \; *$$

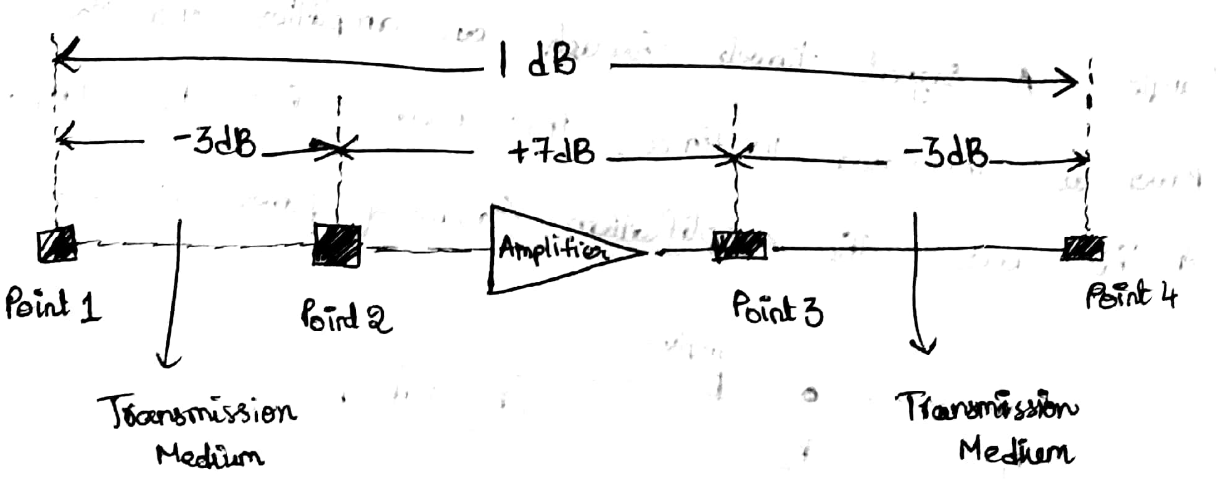
$$= 10 \log_{10}\left(\frac{10 P_1}{P_1}\right) = 10 \text{ dB}.$$

$\therefore$ The gain of power is 10 dB.

Example :

One reason that engineers use the decibel to measure the changes in the strength of a signal is that decibel numbers can be added, subtracted when we are measuring several points instead of just two. In below figure, a signal travels from point 1 to point 4. The signal is attenuated by the time it reaches point 2. Between points 2 & 3, the signal is amplified. Again between 3 & 4, the signal is attenuated. We can find resultant ~~debi~~ decibel value just adding the measurements between each set of points. In this case, the decibel value can be calculated as,

sol : $\text{dB} = -3 + 7 - 3 = 1 \text{ dB}$

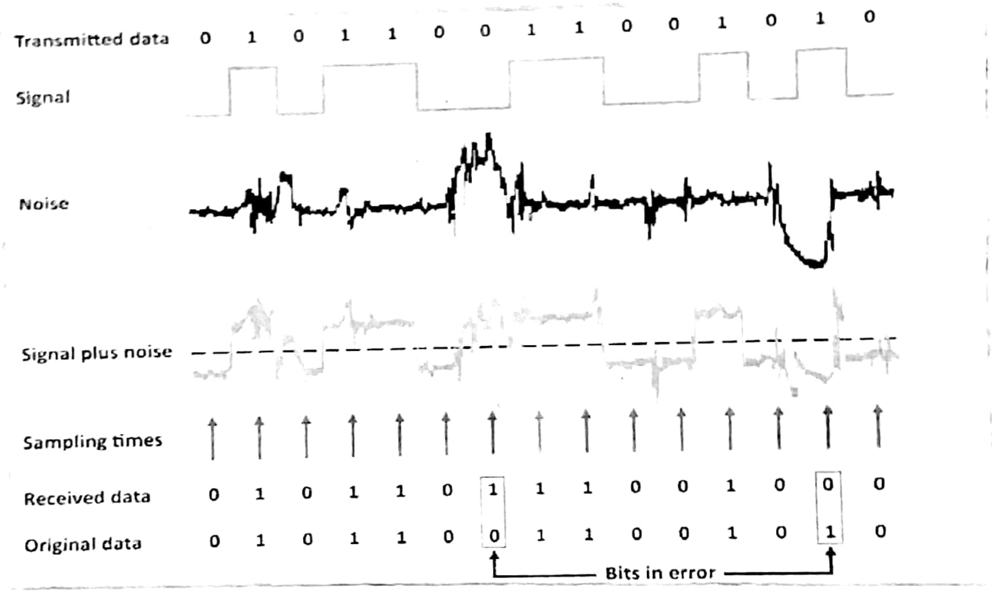


GUDI VARAPRASAD - COMPUTER NETWORKS

*. DISTORTION :

- Signal changes its form or shape
- It occurs in a composite signal made of different frequencies.
- Each signal component has its own propagation speed through a medium and therefore, its own delay in arriving at the final destination.
- Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.

Effect of noise

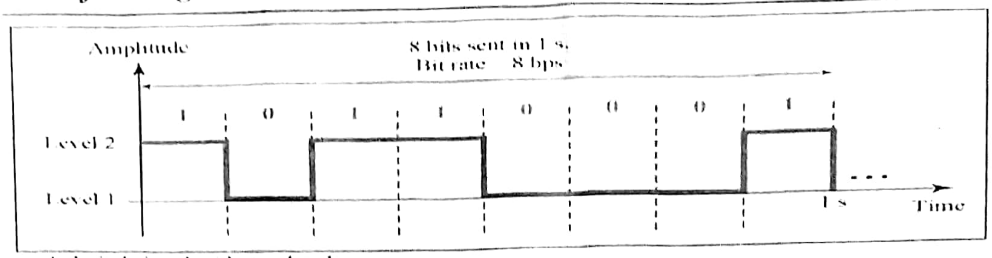


*. NOISE :

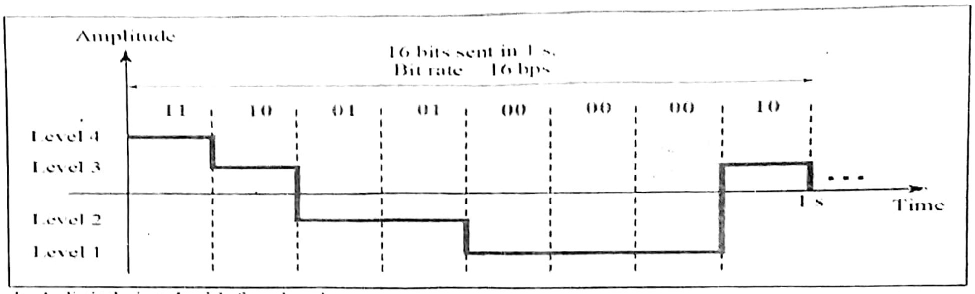
- Noise is another cause of impairment. Several types of noise such as thermal noise, induced noise, cross-talk, and impulse noise, may corrupt the signal.
- Thermal noise is the random motion of electrons in a wire, which creates an extra signal not originally sent by transmitter.
- Induced noise comes from sources such as motors.
- Crosstalk is the effect of one wire on the other.

GUDI VARAPRASAD - COMPUTER NETWORKS

Two digital signals: one with two signal levels and the other with four signal levels

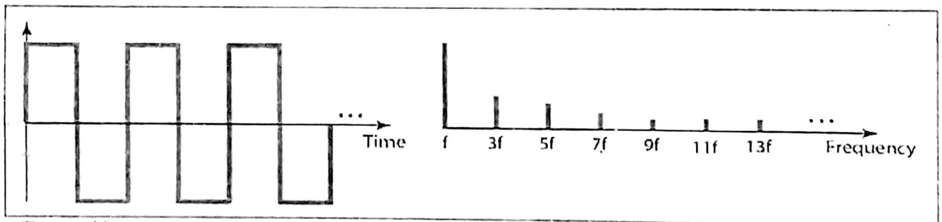


a. A digital signal with two levels

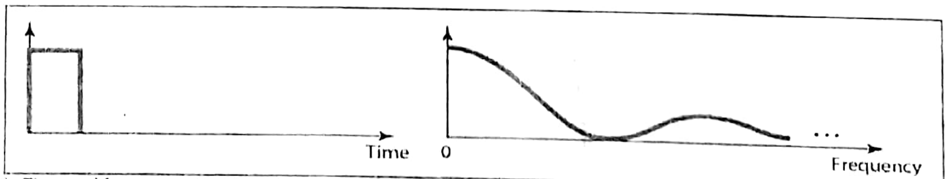


b. A digital signal with four levels

The time and frequency domains of periodic and nonperiodic digital signals



a. Time and frequency domains of periodic digital signal



b. Time and frequency domains of nonperiodic digital signal

GUDI VARAPRASAD - COMPUTER NETWORKS

* CATEGORIES OF NOISE :

1. Thermal Noise :

- Due to thermal Agitation of electrons.
- uniformly distributed across bandwidths.
- Reffered to as white noise.

2. Intermodulation noise :

- Produced by non-linearities in the transmitter, receiver, and/or intervening transmission medium.
- effect is to produce signals at a frequency that is the sum or difference of two original frequencies.

3. Crosstalk :

- A signal from one line is picked by another.
- can occur by electrical coupling between nearby twisted pairs or when microwave antennas pick up unwanted signals.

4. Impulse Noise :

- Caused by external electromagnetic interferences.
- non-continuous, consisting of irregular pulses or spikes.
- short duration and high amplitude.
- Minor annoyance for analog signals but a major source of error in digital data.

GUDI VARAPRASAD - COMPUTER NETWORKS

* **Thermal (White) Noise :**

- Due to thermal agitation of electrons
- Uniformly distributed ,

$$N = KTB \quad \text{(watts)}$$

K - Boltzmann's Constant $= 1.38 \times 10^{-23}$ J/K .

T - Kelvin degrees .

B - Bandwidth in Hz .

* **Signal to Noise Ratio [SNR] :**

- Noise effects ,
  - → distorts a transmitted signal
  - → attenuates a transmitted signal
- Signal to Noise ratio to quantify noise $= S/N$
- usually expressed using decibel (dB .)

$$\boxed{SNR_{dB} = 10 \log_{10}\left(\frac{S}{N}\right)} \ * \qquad \left(SNR = \frac{S}{N}\right)$$

where, S - average signal power

N - Noise power

Example : The power of signal is 10 mW and the power of the noise is 1 µW . What are the values of SNR & SNR_{dB} ?

$$\boxed{SNR = \frac{S}{N}} \qquad \boxed{SNR_{dB} = 10 \log_{10} SNR}$$

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

Here, $S = 10{,}000\ \mu W = 10\ mW$

$N = 1\ \mu W$

$$SNR = \frac{S}{N} = \frac{10{,}000\ \mu W}{1\ \mu W} = 10{,}000$$

$$SNR_{dB} = 10 \log_{10} SNR = 10 \times \log_{10} 10{,}000 = \underline{40}$$

$\therefore$ An SNR greater than 40 dB is considered excellent, whereas a SNR below 15 dB may result in slow, unreliable connection.

__Example__ : The values of SNR and SNR_{dB} for a noiseless channel are :

$$SNR = \frac{\text{signal power}}{0} \cong \infty \qquad \left(\begin{array}{l} \text{Noise} = 0 \\ \text{Noise power} = 0 \end{array} \right)$$

$$SNR_{dB} = 10 \log_{10} \infty \Rightarrow \infty$$

$\therefore$ We can never achieve this ratio in real life, it is an ideal.

---

*. CHANNEL CAPACITY :

- The maximum rate at which data can be transmitted over a given communication path, or channel, under given conditions.
- 4 related factors.
  - → Data rate
  - → Bandwidth
  - → Noise
  - → Error rate

- The main constraint on achieving (to get as high a data rate as possible at a particular limit of error rate for a given bandwidth) this efficiency is noise.

- Data rate :
  - → In bits per second.
  - → Rate at which data can be communicated.

- Bandwidth :
  - → In cycles per second of Hertz.
  - → Constrained by transmitter and medium.

- Noise :
  - → Average level of noise over the communication path.

- Error rate :
  - → Error : 1 becomes 0 ; 0 becomes 1.
  - → At a given noise level, higher data rate ⇒ higher error.

*. DATARATE LIMITS :

A very important consideration in data communication is how fast we can send data, in bits per second, over a channel. Two theoretical formulas were developed to calculate the data rate :

1. Nyquist Equation – ~~Noisy~~ Noiseless channel.
2. Shannon Equation – Noisy channel

GUDI VARAPRASAD - COMPUTER NETWORKS

1. NYQUIST BANDWIDTH :

- Assume noise - free channels.
- Channel bandwidth limits the signal / data rate.
- Given bandwidth B, highest signal rate is 2B : $\boxed{C = 2B}$
- If the rate of signal transmission is 2B then signal with frequencies no greater than B is sufficient to carry signal rate.
- Given binary signal, data rate supported by B Hz is 2B bps. (bits per second)
- Can be increased by using M signal levels :

$$\boxed{C = 2B \log_2 M} \; *$$

C - channel capacity
B - Bandwidth

- However, this increases burden on receiver.
- Noise & other impairments limit the value of M.
- IMP For a noiseless channel, the Nyquist equation bit rate formula defines the theoretical maximum bit rate,

$$\boxed{\text{Bit rate} = 2 \times \text{bandwidth} \times \log_2 L} \; *$$

- There is a limitation due to intersymbol interface, such as is produced by delay distortion. To avoid this, $\boxed{\text{Signal} < B}$.
- Signals with more than two levels can be used i.e. each signal element can represent more than one bit.

e.g., If a signal has 4 different levels, then a signal can be used to represents two bits : 00, 01, 10, 11

GUDI VARAPRASAD - COMPUTER NETWORKS

- With multilevel signalling, the Nyquist formula becomes

* $\boxed{C = 2B \log_2 M}$, M – No. of discrete signal levels
  B – Given bandwidth
  C – Channel capacity (bps).

- Nyquist's formula indicates that, if all other things are equal, doubling the bandwidth doubles the data rate.

Example : Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as,

Sol :
$$\boxed{\text{Bitrate} = 2 \times \text{bandwidth} \times \log_2 L}$$

$$= 2 \times 3000 \times \log_2 2 = 6000 \text{ bps}$$

L – signal level = 2
bandwidth = 3000

Example : Consider the same noiseless channels transmitting a signal with 4 signal levels (for each level, we send 2 bits). The maximum bit rate can be calculated as:

Bandwidth = 3000 Hz
L = 4 (signal level)

$$\text{Bitrate} = 2 \times 3000 \times \log_2 4 = 12000 \text{ bps}.$$
$$= 12 \text{ kbps}$$

GUDI VARAPRASAD - COMPUTER NETWORKS

Example : We need to send 265 kbps over a noiseless channel with a bandwidth of 20 KHz. How many signal levels do we need ?

Bit rate = 265 Kbps = 265000

bandwidth = 20 KHz = 20000

Signal level = L = ?

$$\boxed{\text{Bitrate} = 2 \times \text{bandwidth} \times \log_2 L}$$

$$265000 = 2 \times 20000 \times \log_2 L$$

$$\Rightarrow L = 2^{6.625} = 98.7 \text{ levels}$$

$\therefore$ Levels $\approx$ 99 levels

~~Example~~:

*. 2. SHANNON CAPACITY :

In reality, we cannot have a noiseless channel ; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called Shannon capacity, to determine the theoretical highest data rate for a noisy channel.

$$\boxed{\text{Capacity} = \text{Bandwidth} \times \log_2 (1 + \text{SNR})} \ *$$

$$\text{SNR} = \frac{S}{N} = \frac{\text{Average signal power}}{\text{Noise power}} = \text{Ratio}$$

GUDI VARAPRASAD - COMPUTER NETWORKS

Example : Consider an extremely noisy channel in which the value of the signal to noise ratio is almost zero. In other words, the noise is so strong that the calculated signal is faint. For this type of channel, the capacity C is,

$$\boxed{C = B * \log_2 (1 + SNR)}$$

$$SNR = \frac{S}{N} = \frac{S}{\infty} \simeq 0 \quad \text{(almost zero)}$$

$$C = B * \log_2 (1+0) \Rightarrow \boxed{C = 0}$$

∴ This means that the capacity of this channel is zero regardless of bandwidth. In other words, we cannot receive any data through this channel.

IMP

Example : The signal to noise ratio is often given in decibels. Assume that $SNR_{dB} = 36$ and the channel bandwidth is 2 MHz. The theoretical channel capacity can be calculated as,

$$SNR_{dB} = 10 \log_{10} SNR$$

$$36 = 10 \log_{10} SNR \Rightarrow SNR = 10^{3.6} = 3981$$

$$C = B \log_2 (1 + SNR) = 2 \times 10^6 \times \log_2 (1 + 3981)$$

$$C = 2 \times 10^6 \times 11.96 = 23.92 \times 10^6$$

$$C \approx 24 \text{ Mbps}.$$

GUDI VARAPRASAD - COMPUTER NETWORKS

Special case : If SNR is very high (means noise is almost negligible $\Rightarrow 1+SNR \approx SNR$. In these cases, the theoretical channel capacity is,

$$\boxed{C = B \log_2 SNR} \quad (\text{or}) \quad \boxed{C = \frac{B}{3} \cdot SNR_{dB}}$$

IMP

Example : We have a channel with 1 MHz bandwidth. The SNR for this channel is 63. What are the approximate bit rate & signal level?

$$C = B \log_2 (1+SNR)$$

$$= 10^6 \times \log_2 (1+63) = 6 \times 10^6 \text{ bps} = 6 \text{ Mbps}$$

The shannon formula gives us 6 Mbps, the upper limit. For better performance we choose something lower, 4 Mbps. Then we use the Nyquist formula to find the no. of signal levels.

Bit rate $= 4$ Mbps (assumption based on channel capacity)

Bandwidth $= 10^6$ Hz

$$\boxed{\text{Bit rate} = 2 \times \text{bandwidth} \times \log_2 L}$$

$$4 \times 10^6 = 2 \times 10^6 \times \log_2 L$$

$$\boxed{L = 4}$$

$\therefore$ No. of signal levels ≈ 4

GUDI VARAPRASAD - COMPUTER NETWORKS

*. PERFORMANCE :

- One characteristic that measures network performance is bandwidth.

Example : The bandwidth of a subscriber line is 4 KHz for voice or data. The bandwidth of this line for data transmission can be up to 56,000 bps using a sophisticated modem to change the digital signal to analog.
If the Telephone company improves the quality of the line and increases the bandwidth to 8 KHz, we can send 112,000 bps by using the same technology.

*. THROUGHPUT :

- The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different.
- A link may have a bandwidth of B bps, but we can only send T bps through this link with T always less than B.

*. LATENCY :

- The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

GUDI VARAPRASAD - COMPUTER NETWORKS

Latency = propagation time + transmission time + queuing time + processing delay

IMP *

<u>Example</u> : A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network ?

~~Throughput ≠ Bandwidth~~

Throughput = how fast we can send data

$$= \frac{12,000 \text{ frames}}{60 \text{ seconds}} \times 10,000$$

$$= 2 \times 10^6 \text{ bps} = 2\text{Mbps}$$

$\therefore$ Throughput $= \frac{1}{5} \times$ Bandwidth (in this case)

<u>Example</u> : What are the propagation time and the transmission time for a 2.5 KB message if the bandwidth of the network is 1 Gbps ? Assume that the distance between the sender and receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

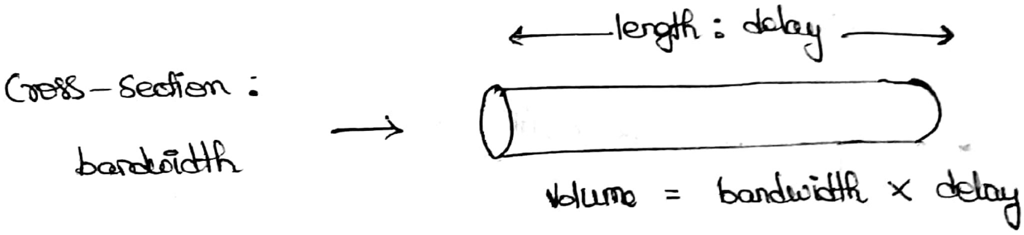
$$\text{Propagation time} = \frac{(12,000 \times 1000)}{2.4 \times 10^8} = 50 \text{ ms}$$

$$\text{Transmission time} = \frac{2500 \times 8}{10^9} = 0.020 \text{ ms}$$

GUDI VARAPRASAD - COMPUTER NETWORKS

Example : We can think about the link between two points as a pipe. The cross section of the pipe represents the bandwidth, and the length of the pipe represents the delay. We can say the volume of pipe defines the bandwidth - delay product, as

Concept of bandwidth - delay product,



Example : A digital signal has 8 levels. How many bits are needed per level? We calculate the number of bits from formula.

levels = L

$$\boxed{\text{No. of bits per level},\ n = \log_2 L} \ *$$

$$\therefore \quad n = \log_2 8 = 3$$

Each signal level is represented by 3 bits.

000   101
001   110
010
011   111
100

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

Example : Assume we need to download text documents at the rate of 100 pages per second. What is the required bit rate of channel ?

Sol : A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits (ascii), the bit rate is,

= 100 pages × 24 lines × 80 char × 8 bits

= 1,636,000 bps = 1.636 Mbps

Example : What is the bit rate for HD TV ?

Answer : HDTV uses digital signals to broadcast high quality video signals. The HDTV screen is normally of ratio 16 : 9. There are 1920 by 1080 pixels per screen. The screen is renewed 30 times per second. 24 bits represent one color pixel.

$$1920 \times 1080 \times 30 \times 24 = 1{,}492{,}992{,}000$$

$$= 1.5 \text{ Gbps}$$

∴ The TV stations reduce this rate to 20 to 40 MBPS through compression.

NOTE : A digital signal is a composite of analog signal with an infinite bandwidth.

NOTE : Baseband transmission of a digital signal that preserves the shape of digital signal is possible only if we have a low-pass channel with infinite / wide bandwidth.

- An example of a dedicated channel where the entire bandwidth of the medium is used as one ~~sig~~ single channel is a LAN.

- Almost every wired LAN today uses a dedicated channel for two stations communicating with each other.

- In a bus topology LAN with multipoint connections, only two stations can communicate with each other at each moment in time (time sharing).

- the other stations need to refrain from sending data.

- In a star topology LAN, the entire channel between each station and the hub is used for communication between these two entities.

NOTE In baseband transmission, the required bandwidth is proportional to the bit rate, if we need to send bits faster, we need more bandwidth.

NOTE If the available channel is a bandpass channel, we cannot send the digital signal directly to the channel; we need to convert the digital signal to an analog signal before transmission.

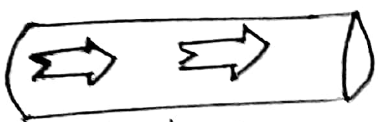
- An example of broadband transmission using modulation is the sending of computer data through a telephone subscriber line, the line connecting a resident to the central telephone office.

GUDI VARAPRASAD - COMPUTER NETWORKS

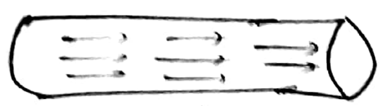
GUDI VARAPRASAD - COMPUTER NETWORKS

- These lines are designed to carry voice with a limited bandwidth.
- This channel is considered a bandpass channel.
- We convert the digital signal from the computer to an analog signal, and send the analog signal.
- We can install two converters to change the digital signal to analog and vice versa at the receiving end. The converted in this case is "MODEM".

- A second example is the digital cellular Telephone.
- For better reception, digital cellular phones convert the analog voice signal to a digital signal.
- Although the bandwidth allocated to a company providing digital cellular phone service is very wide, we still cannot send the digital signal without conversion. The reason is that we only have a bandpass channel available between the persons communicating.
- We need to convert the digitalized voice to a composite analog signal before sending.



Baseband



Broadband

TRANSMISSION MEDIA :

*. Design Factors determining Data Rate & Distance.

1. Bandwidth – Higher bandwidth gives higher data rate
2. Transmission impairments – attenuation, distance limit
3. Interference – overlapping frequency bands
4. No. of receivers – More receivers introduces more atten-uation

*. TWISTED PAIR :

- It is the least expensive and most widely used guided transmission medium.

> Consists of two insulated copper wires arranged in regular spiral pattern.

> A wire pair acts as a single communication link.

> Pairs are bundled into a cable.

> Most commonly used in telephone network for communications within buildings.

→ Unshielded Twisted Pair – Consists of one or more twisted-pair cables, provides no electromagnetic shielding.

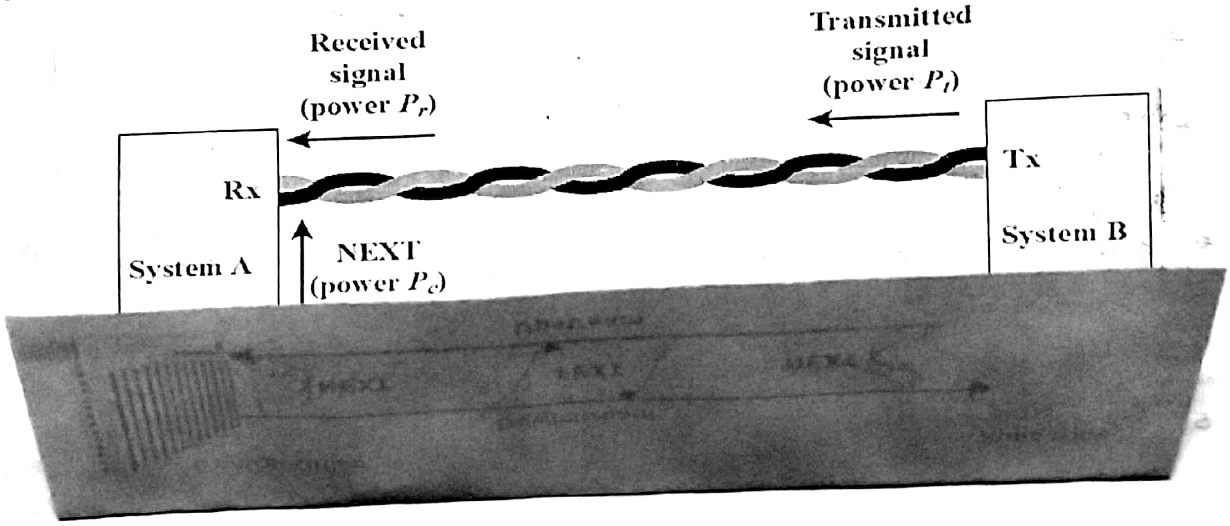
→ Shielded Twisted Pair – Has metal braid or sheathing that reduces interfaces & provides better performance at higher data rates.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*- NEXT – NEAR END CROSS TALK :

- Coupling of signal form one pair of conductors to another.
  - conductors may be the metal pins in a connector or wire pairs in a cable.
- Near end refers to coupling that takes place when the transmit signal entering the link couples back to the receive conductor pair. at the same end of the link.
- Greater NEXT loss magnitudes are associated with less crosstalks noise.

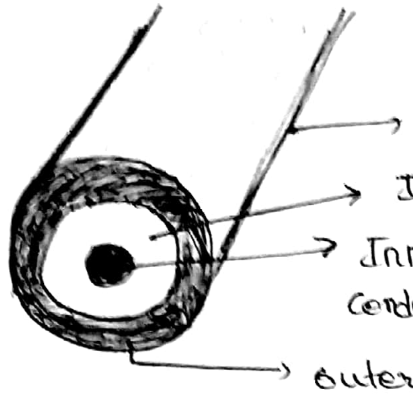


*. COAXIAL CABLE :

- Coaxial cable can be used over longer distances and support more stations on a shared line than twisted pair.
- Consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor.
- Is a versatile transmission medium used in a wide variety of applications.
- Used for TV distribution, long distance telephone transmission and LANs.

GUDI VARAPRASAD - COMPUTER NETWORKS

COAXIAL CABLE

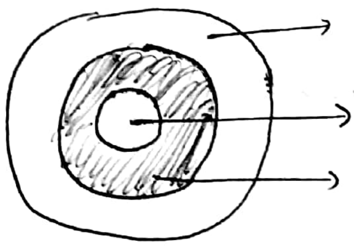


↑ Frequency characteristics superior to twisted pair

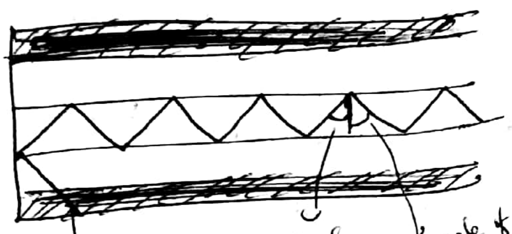
↓ Performance limited by attenuation and noise

*. OPTICAL FIBER :

- optical Fiber is a thin flexible medium capable of guiding an optical ray.
- Various glasses and plastics can be used to make optical fibers.
- Has a cylindrical shape with three sections - core, cladding, jacket.
- Widely used in long distance telecommunications.
- Performance, price and advantages have made it popular to



OPTICAL FIBER



GUDI VARAPRASAD - COMPUTER NETWORKS

*. Uses of Optical Fiber :

- Greater capacity – Data rates of hundreds of Gbps over tens of kilometers have been demonstrated.
- Smaller size lighter weight – Considerably thinner than coaxial, twisted pair. Reduces constructed support requirements.
- Electromagnetic Isolation – Not vulnerable to interference, impulse noise, or crosstalk.
- Greater repeater spacing, Lower attenuation, lower cost.

*. TERRESTRIAL MICROWAVE :

Most common type is the PARABOLIC "DISH"

Typical size is about 3 m in diameter

Antenna is fixed rigidly and focuses a narrow beam to achieve line of sight transmission to the receiving Antenna

usually Located at substantial heights above ground level

A series of microwave relay towers is used to achoive long distance transmission

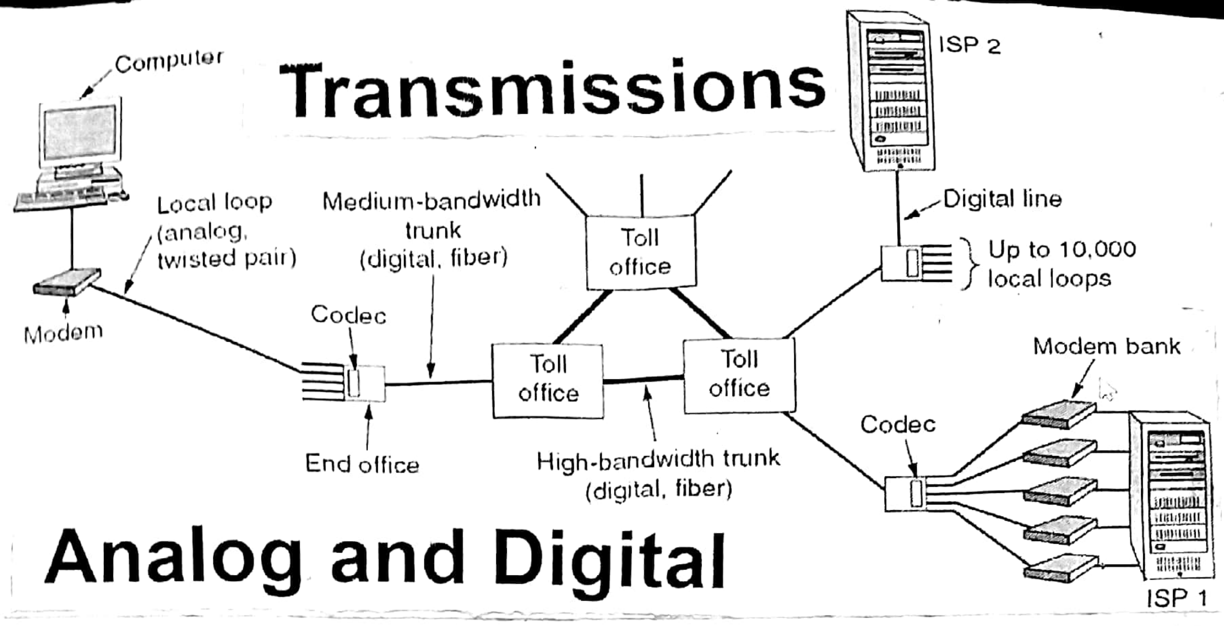
*· TERRESTRIAL MICROWAVE APPLICATION :

- Used for long haul telecommunications service as an alternative to coaxial cable or optical fiber
- Used for both voice and TV transmission.
- Fewer repeaters but requires line of sight transmission.
- 1-40 GHz frequencies, with higher frequencies having higher data rates.
- Main source of loss is attenuation caused mostly by distance, rainfall and interference.

*· SATELLITE MICROWAVE :

- A communication satellite is in effect a microwave relay station.
- Used to link two or more ground stations.
- Receives transmissions on one frequency band, amplifies or repeats the signal, and transmits it on another frequency.
- Frequency bands are called transponder channels.

GUDI VARAPRASAD - COMPUTER NETWORKS



- The use of both analog and digital transmissions for a computer to computer call. Conversion is done by the modems and codecs.

*. DATA ENCODING TECHNIQUES :

- Digital Data, Analog signal [modem].
- Digital data, digital signals [wired LAN] → computer → printer
- Analog data, digital signals [codec] – recording music on CD.
- Pulse Code Modulation (PCM) does the digitization process also called as digital modulation.
- Key factors in PCM are sampling and quantization.
- Analog data, Analog signal (AM, FM, PM).

*. DIGITAL DATA, ANALOG SIGNAL : [MODEM]

- Basis for Analog signaling is a continuous, constant-frequency signal known as the carrier frequency.
- Digital data is encoded by modulating one of the three characteristics of the carrier.

GUDI VARAPRASAD - COMPUTER NETWORKS

- Amplitude, frequency or phase or some combination of these.

MODEMS :

- All advanced modems use a combination of modulation techniques to transmit multiple bits per baud.

- Multiple amplitude and multiple phase shifts are combined to transmit several bits per symbol.

- QPSK (Quadrature Phase Shift Keying) uses multiple phase shifts per symbol.

- Modems actually use QAM (Quadrature Amplitude Modulation.)

- These concepts are explained using constellation points where a point determines a specific amplitude and phase.

*. Digital Data, Digital Signals : [LANs]

- Digital signal - is a sequence of discrete, discontinuous voltage pulses.

- Bit duration : the time it takes for the transmitter to emit the bit.

- Issues :

  - Bit timing.
  - Recovery from signal.
  - Noise immunity.

GUDI VARAPRASAD - COMPUTER NETWORKS

* What factors determine how successful the receiver will be in interpreting the incoming signal?

• SNR • Data Rate • Bandwidth • An increase in data rate (BER ↑)

• An increase in SNR decreases bit error rate ↓.

• An increase in bandwidth allows an increase in data rate ↑.

* Comparision of Encoding Schemes:

• Error detection – can be built in to signal encoding.

• Signal interference & noise immunity.

• Cost and Complexity.

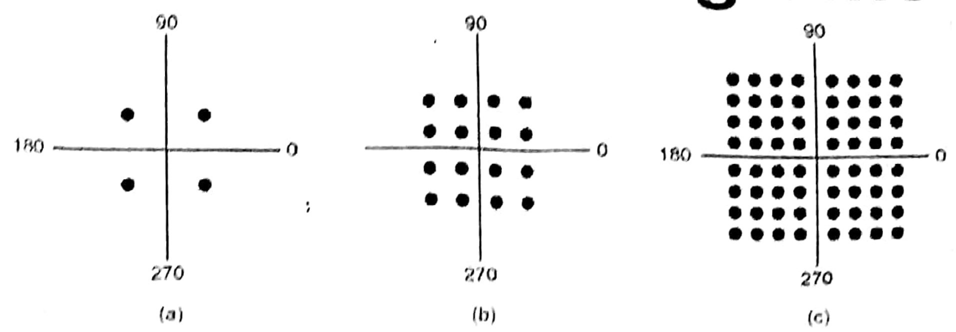
• The encoding scheme is simply the mapping from data bits to signal elements.

• A digital signal is sequence of discrete, discontinuous voltage pulses.

• Each pulse a signal element.

• Encoding scheme is an important factor in how successfully the receiver interprets the incoming signal.

Constellation Diagrams

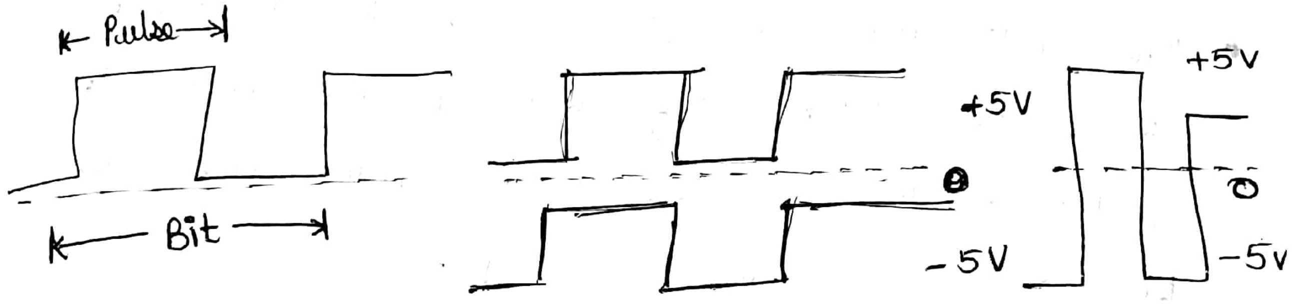


(a) QPSK. (b) QAM-16. (c) QAM-64.

GUDI VARAPRASAD - COMPUTER NETWORKS

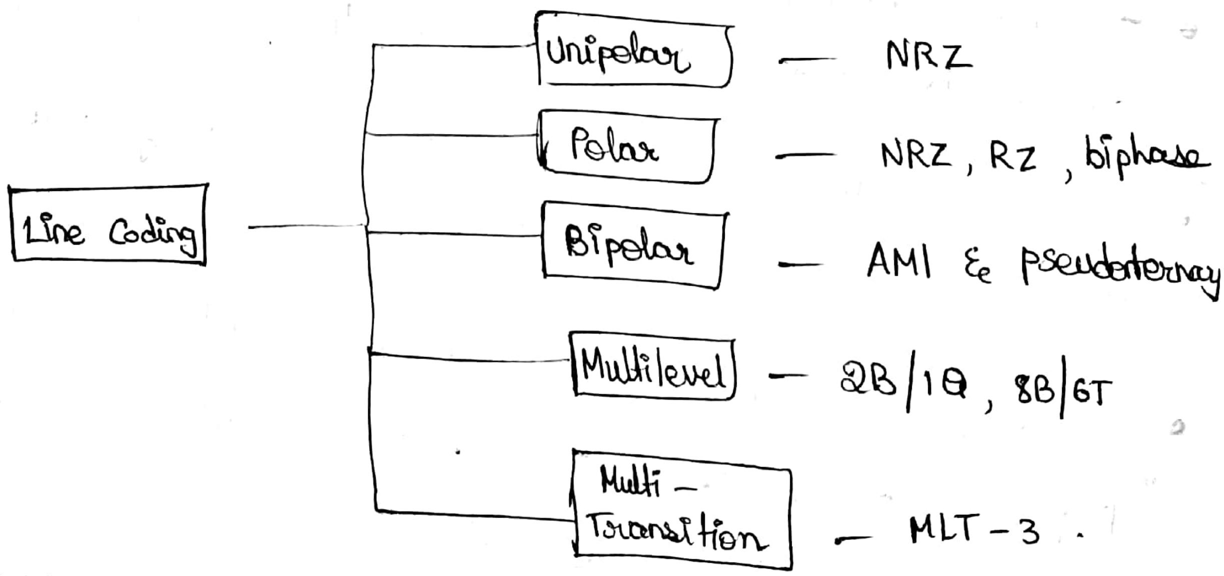
GUDI VARAPRASAD - COMPUTER NETWORKS

*. BASIC TERMS :

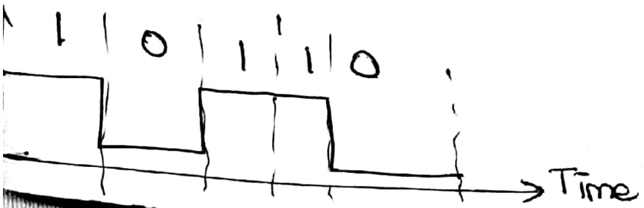


- Signal element : Pulse (of constant amplitude, frequency, phase).
- Unipolar : All positive or All negative voltage.
- Bipolar : Positive or Negative voltage
- Mark/Space : 1 or 0.
- Modulation Rate : 1/Duration of the smallest element = Baud Rate
- Data Rate : bits per second.
- Data Rate = Fn (Bandwidth, Signal/Noise ratio, encoding).

*. LINE ENCODING SCHEMES :



*. UNIPOLAR NRZ value :



Normalized power

$$\frac{1}{2}V^2 + \frac{1}{2}(0)^2 = \frac{1}{2}V^2$$

*. CLOCKING :

- When bits are sent from sender to a receiver across a network they need a mechanism to synchronize their clocks. so they both know when a bit starts and when it stops.

- Clocking information needs to be sent as well as the data so that receiving station can synchronize its own clock with senders' clock.

- Synchronous connections use a seperate clocking line to transmit clocking information.

- Ethernet is asynchronous and it doesnot have a seperate line that could be used to send clocking information.

- Ethernet doesnot have a seperate clocking line that could be used to synchronize the clocks continuously

- Another method is needed for maintaining clock synchronization.

- Encoding method also needs to exhibit other desirable properties, such as maximum signal frequency, data rate, signal-to-noise ratio.

GUDI VARAPRASAD - COMPUTER NETWORKS

*. NRZ (Non-Return to Zero) codes :

- Uses two different voltage levels (one positive and one negative) as the signal elements for the two binary digits.

1. NRZ-L (Non-Return to Zero-level) :

- The voltage is constant during the bit interval.

1 ⟺	negative voltage
0 ⟺	positive voltage

- NRZ-L ~~ris~~ is used for short distances between terminal and modem or terminal and computer.

2. NRZ-I (Non-Return to Zero-Invert on ones) :

- The voltage is constant during the bit interval.

1 ⟺ existence of a signal transition at the begining of the bit time (either a low to high or high to low transition).

0 ⟺ no signal transition at begining of bit time

- NRZ-I is a different encoding scheme (i.e., the signal is decoded by comparing the polarity of adjacent signal elements.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*. Bi-Phase Codes :

- Bi phase codes - require atleast one transition per bit time and may have as many as two transitions.

→ The maximum modulation rate is twice that of NRZ.
→ Greater transmission bandwidth is required.

*. MANCHESTER ENCODING :

- There is always a mid-bit transition {, used as clocking mechanism. }

- The direction of mid bit transition represents the digital data.

= zero 0

= one 1

1	⟺	low to high transition
0	⟺	high to low transition

- Consequently, there may be a second transition at the begining of the bit interval.

*. DIFFERENTIAL MANCHESTER ENCODING :

- mid-bit transition is only for clocking.

1 ⟺ absence of transition at start of bit interval.

0 ⟺ presence of transition at start of bit interval.

- Differential Manchester = Differential + Bi-phase

~~NRZI~~ (opposite)

GUDI VARAPRASAD - COMPUTER NETWORKS

NOTE
- Modulation rate for Manchester and Differential Manchester is twice the data rate → inefficient encoding for long-distance applications.

* . **BIPOLAR Encoding** :

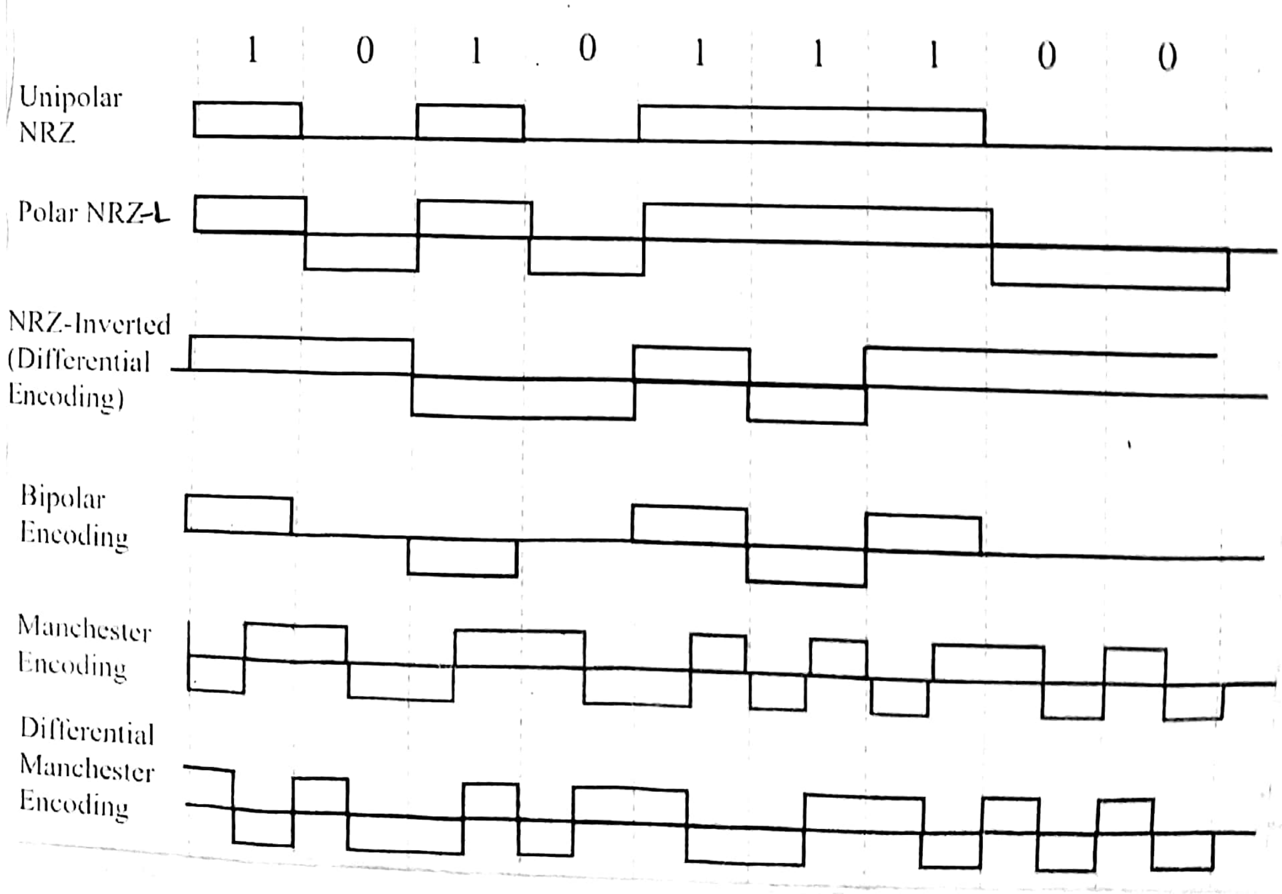
Alternate Mark Inversion

1	⟺	alternating, $+1/2$, $-1/2$ voltage
0	⟺	0 voltage

Pseudoternary

- Has the same issues as NRZI for long string of 0's.
- A systemic problem with polar is the polarity can be backwards.

Encoding schemes



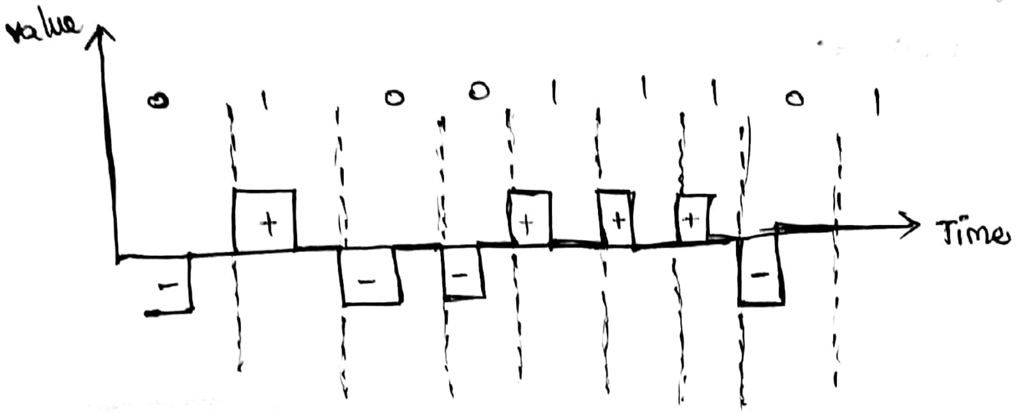
GUDI VARAPRASAD - COMPUTER NETWORKS

*. LINE ENCODING :

Return to zero (RZ) :- e.g. 0 = negative volt
1 = positive volt

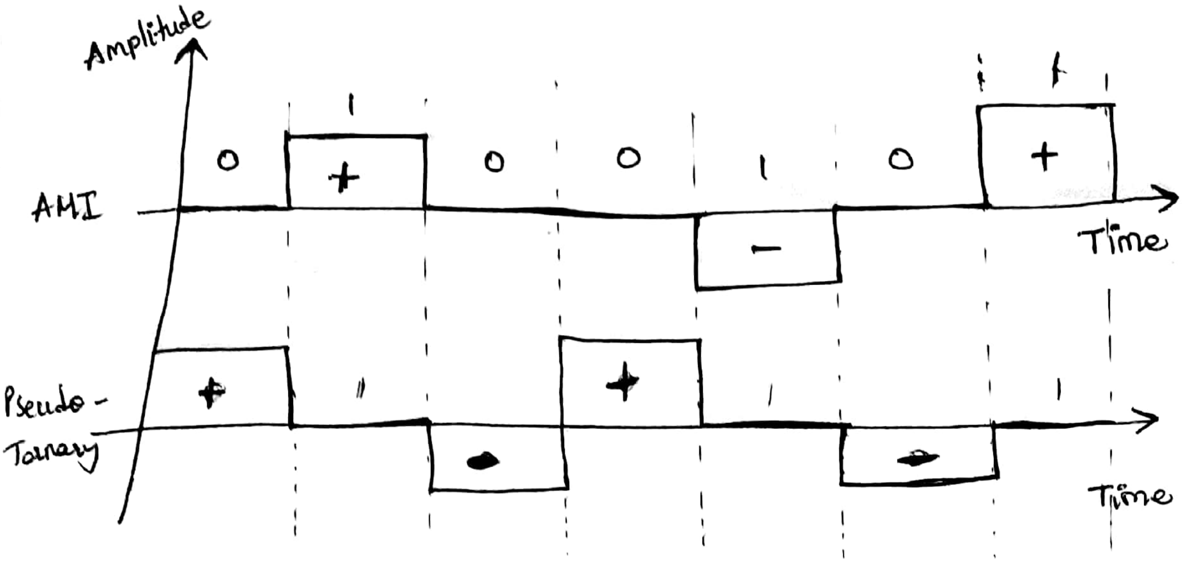
- AND signal must return to zero halfway through each bit interval.
- perfect synchronization.

- Drawback :- 2 signal changes to encode each bit, pulse rate is x2 times of NRZ coding rate. i.e. more bandwidth is required, regardless of bit sequence.



Non-Zero Level ⇒ begining of a new bit

*. AMI (vs) Pseudoternary :



*. SCRAMBLING :

- Doesnot increase the number of bits and does provide synchronization.
- Continuous sequence of zeros create synchronization problems one solution to this this scrambling.
- There are two common scrambling techniques :
  1. B8ZS (Bipolar with 8-Zero substitution).
  2. HDB3 (High density bipolar 3-Zero).
- Scrambling is widely used in satellite, radio relay communications and PSTN modems.

② HDB3 :

- If the no of non-zero pulses after the last substitution is odd, the substitution is pattern will be 000V, which makes the total no. of non-zero pulses even.
- If the no. of non-zero pulses after the last substitution is even, the substitution pattern will be B00V, which makes the total no. of non zero pulses even.

Last Pulse	odd 1's until last subs	even 1's until last subs
−	000−	+00+
+	000+	−00−

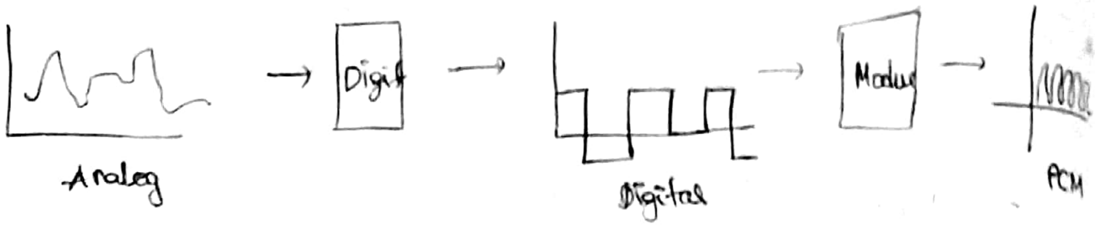
GUDI VARAPRASAD - COMPUTER NETWORKS

* Pulse Code Modulation (PCM):

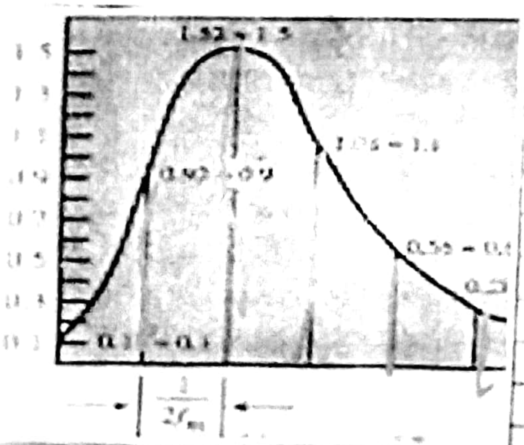
1. Analog signal is sampled. (original in float)
- Analog Data, Digital Signals.

2. The sample signaled is quantisized. (round off value)

3. The Quantisized signal is encoded into bits. (binary value)



- Quantization is the process of asigning a discrete value from a range of possible values to each sample obtained.



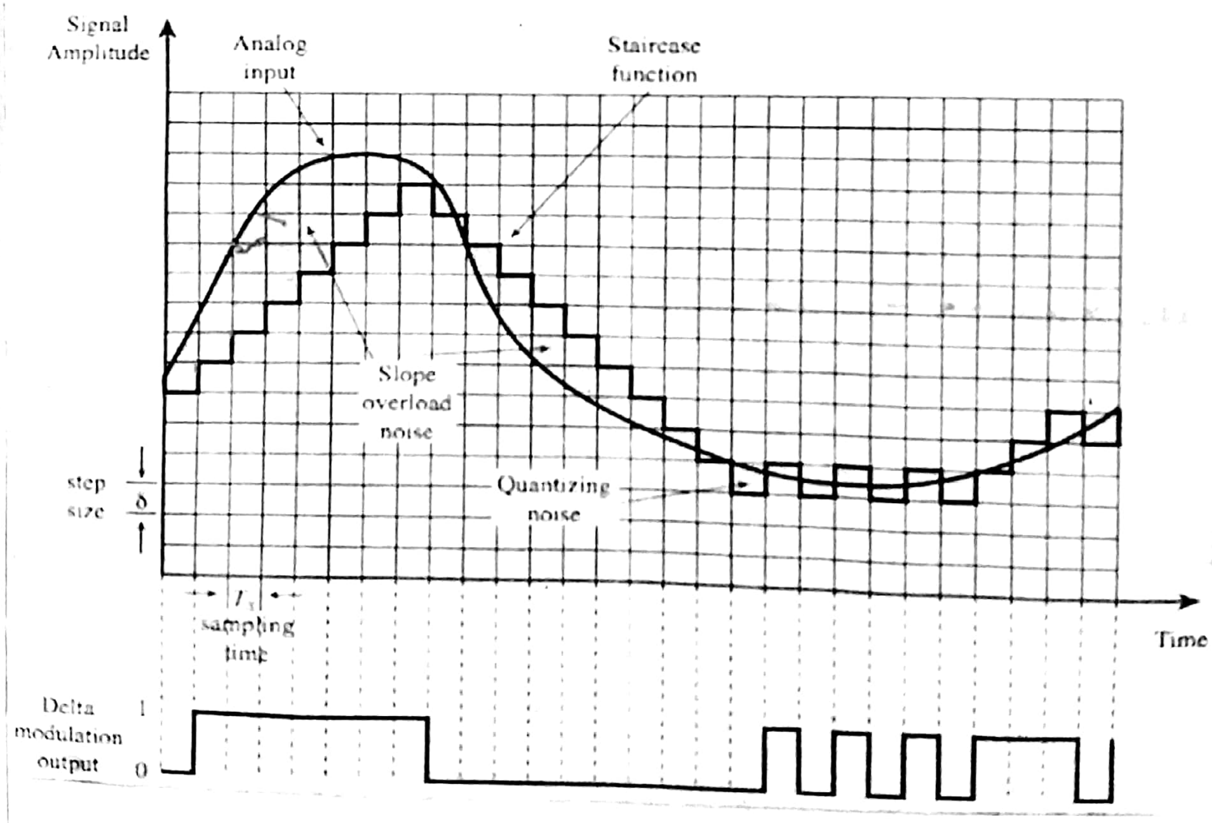
Digit	Binary equivalent	PCM waveform
0	0000	
1	0001	
2	0010	
3	0011	
4	0100	
5	0101	
6	0110	
7	0111	
8	1000	
9	1001	
10	1010	
11	1011	
12	1100	
13	1101	
14	1110	
15	1111	

GUDI VARAPRASAD - COMPUTER NETWORKS

*. DELTA MODULATION :

- Analog input is approximated by a step function.
- Move up or down one level (δ) at each sample interval.
- Binary behaviour :
  - → Function moves up or down at each sample interval.
  - → Moving up : generating 1.
  - → Moving down : generating 0.

- DM versus PCM :
  - → DM simpler implementation.
  - → PCM : better SNR at the same data rate.



GUDI VARAPRASAD - COMPUTER NETWORKS

*. CIRCUIT SWITCHING :

- Circuit switching is used in public telephone networks and is the basis for private networks built on leased lines.

- Circuit switching was developed to handle voice traffic but also digital data.

- With circuit switching a dedicated path is established between two stations for communication.

- Switching and transmission resources within the network are reserved for the exclusive use of the circuit for the duration of the connection.

- The connection is transparent : once it is established, it appears to attached devices as if there were a direct connection.

*. PACKET SWITCHING :

- Packet switching was designed to provide a more efficient facility than circuit switching for bursty data traffic.

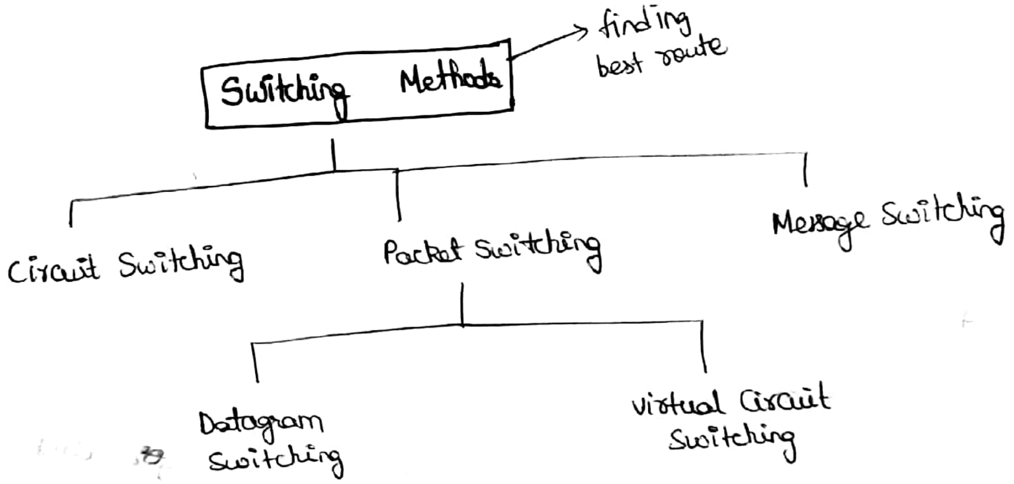
- With packet contains some portion of user data plus control info needed for proper functioning of network.

- With packet switching, a station transmits data in small blocks, called packets.

GUDI VARAPRASAD - COMPUTER NETWORKS

- A key element of packet - switching networks is whether the internal operation is datagram or virtual circuit (VC).
  - With internal VCs, a route is defined between two endpoints and all packets for that VC follow the same route.
  - With internal diagrams, each packet is treated independently, and packets intended for the same destination may follow different routes.

- Examples of packet switching networks are ATM, IP, X-25.



CIRCUIT SWITCHING :

- Circuit Switching is a technique that directly connects the sender and the receiver in an unbroken path.

- Telephone switching equipment,

  Ex : Establishes a path that connects the callers' telephone to the receivers' telephone by making a physical conn.

- With this type of switching technique, once a connection is established, A dedicated path exists between both ends until the connection is terminated.

GUDI VARAPRASAD - COMPUTER NETWORKS

- Routing decisions must be made when the circuit is first established, But there are no decisions made after that time.

- Circuit switching in a network operates almost the same way as the telephone system works.

- A complete initiating the data transfer must ask for a connection to the destination

- Once the connection has been initiated and completed to the destination device.

- The destination device must acknowledge that it is ready and willing to carry on a transfer.

- <u>Circuit switching</u> :

  + There is a dedicated communication path between two stations (end - to - end).

  + The path is a connected sequence for links between nodes

  + on each physical link, a logical channel is dedicated to the connection.

- Communication via circuit switching has three phases :

  + Circuit establishment (link by link).

  + Routing & resource allocation (FDM & TDM).

  + Data Transfer.

  + Circuit disconnect (Deallocate the dedicated resources).

- The switches must know :

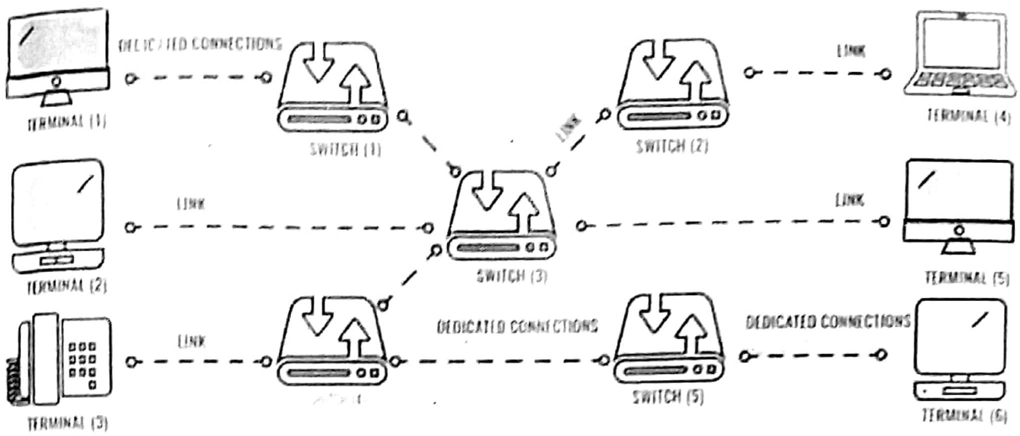
  + How to find the route to the destination and

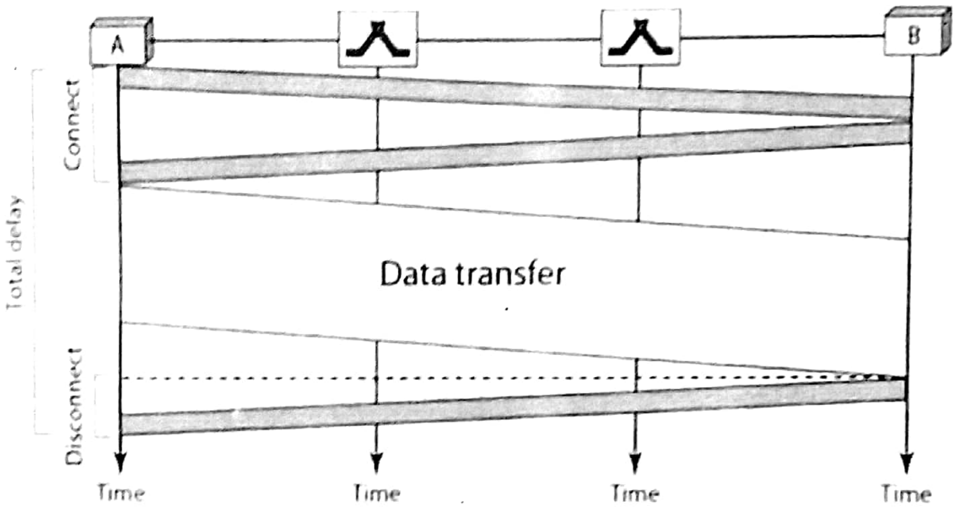
  + How to allocate bandwidth (channel) to establish connection.

GUDI VARAPRASAD - COMPUTER NETWORKS

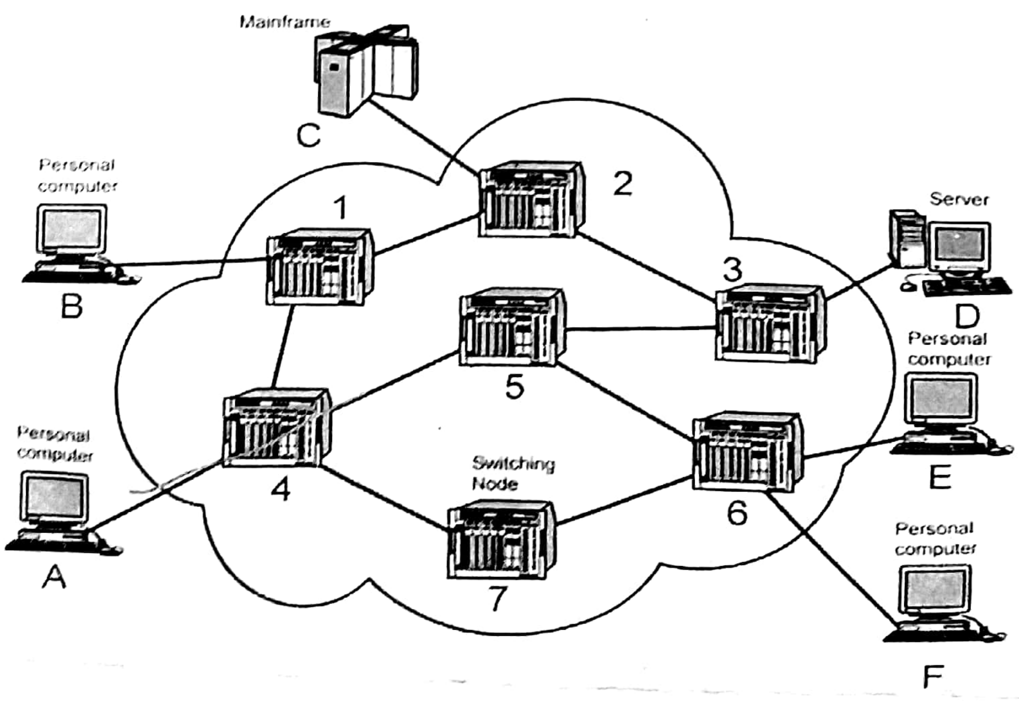
GUDI VARAPRASAD - COMPUTER NETWORKS

CIRCUIT SWITCHING





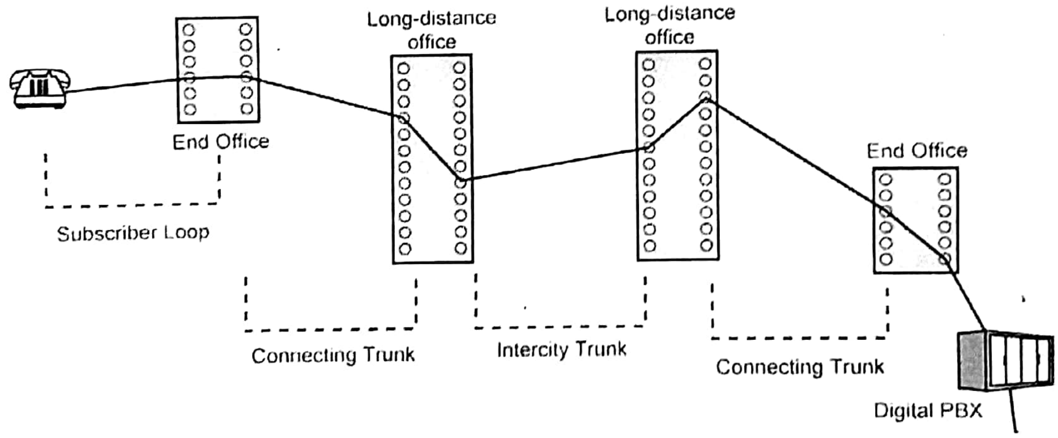
- ***Propagation delay:*** *The time it takes a signal to propagate from one node to the next.This time is generally negligible. The speed of electromagnetic signals through a wire medium, for example, is typically*
- ***Transmission time:*** *The time it takes for a transmitter to send out a block of data. For example, it takes 1 s to transmit a 10,000-bit block of data onto a 10kbps line.*
- ***Node delay:*** *The time it takes for a node to perform the necessary processing as it switches data.*



* CIRCUIT SWITCHING PROPERTIES :

1. Inefficiency
   - channel capacity is dedicated for the whole duration of a connection
   - If no data, capacity is wasted

2. Delay
   - Long initial delay : Circuit establishment takes time
   - Long data delay : after circuit establishment,
   - information is transmitted at a fixed data rate with no delay other than the propagation delay.
   - The delay at each node is negligible.



Subscribers: the devices that attach to the network.

Subscriber loop: the link between the subscriber and the network.

Exchanges: the switching centers in the network.

End office: the switching center that directly supports subscribers.

Trunks: the branches between exchanges. They carry multiple voice-frequency circuits using either FDM or synchronous TDM.

*. CIRCUIT SWITCHING ADVANTAGES & DISADVANTAGES :

- The communication channel (once established) is dedicated.
- Possible long wait to establish a connection during which no data can be transmitted.

GUDI VARAPRASAD - COMPUTER NETWORKS

*. PACKET SWITCHING :

- Packet switching can be seen as solution that tries
  - to combine the advantages of message & circuit switching
  - to minimize the disadvantages of both.

- There are two methods of packet switching : → virtual, → datagram

- In both packet switching methods, a message is broken into small parts, called packets.

- Each packet is tagged with appropriate source & destination addresses.

- Since packets have strictly defined maximum length,
  - they can be stored in main memory instead of disk,
  - therefore access delay and cost are minimized.
  - Also, the transmission speeds, between nodes, are optimized.

- With current technology,
  - packets are generally accepted onto the network on a first-come, first-serve basis.

- If the network becomes overloaded,
  - packets are delayed or discarded ('dropped').

*. PACKET SIZE :

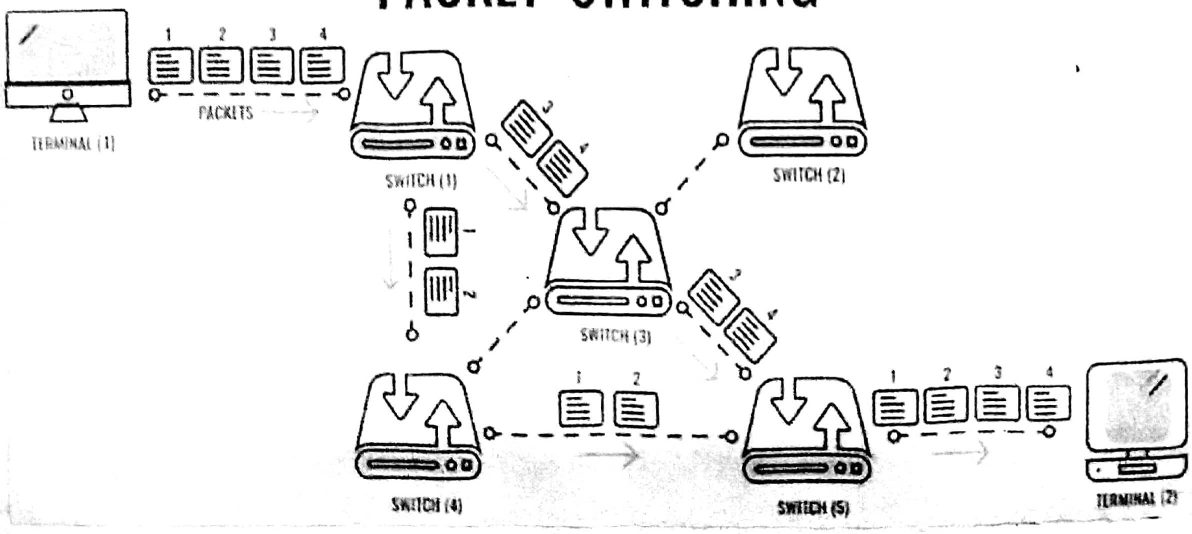
- The size of the packet can vary from 180 bits,
- In other apps, 1024 or 2048 bits for switch
- For ATM switching 53 bytes.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- In Packet switching, the analog signal from your phone is converted into a digital data stream.
- That series of digital bits is then divided into relatively tiny clusters of bits, called packets.
- Each packet has at its begining the digital address
  - A long number -- to which it is being sent.
- The system blasts out all these tiny packets, as fast as it can, and
- They travel across the nation's digital backbone systems to their destination:
- They necessarily don't travel together;
- They don't travel sequentially;
- They don't even all travel via the same route.
- But eventually they arrive at the right point.
  + That digital address added to the front of each string of digital data and at their destination are reassembled into the correct order, then converted to analog form.

PACKET SWITCHING



GUDI VARAPRASAD - COMPUTER NETWORKS

1. DATAGRAM PACKET SWITCHING :

- Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.
- It allows packets to take a variety of possible paths through the network.
- each with the same destination address,
  - don't follow the same route, and
  - they may arrive out of sequence at the exit point node
- Reordering is done at the destination point based on the sequence number of packets.
- It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.

2. VIRTUAL CIRCUIT PACKET SWITCHING :

- In the virtual circuit approach, - a preplanned route is established before any datapackets are sent.
- A logical connection is established when
  - A sender send a "call request packet" to the receiver and
  - the receiver send back an acknowledge packet" call accepted packet to the sender (if the receiver agrees on conversational parameters).
- Virtual circuits imply acknowledgements, flow control, error control. Hence they are reliable.
- That is they have the capability to inform upper-protocol layers if a transmission problem occurs.

GUDI VARAPRASAD - COMPUTER NETWORKS

- In virtual circuit, the route between stations doesn't mean that this is a dedicated path, as in circuit switching.
- A packet is still buffered at each node & queued for output over a line.
- The difference between virtual circuit and datagram approaches:
  - With virtual circuit,
    - the node doesn't need to make a routing decision for each packet.
    - It is made only once for all packets using the virtual circuit.
- It Guarantees that:
  - the packet sent arrive in the order sent
  - with no duplicates or omissions
  - with no errors (high probability) regardless of implementation

Advantages:

- Packet switching is cost effective, because switching devices donot need massive amount of secondary storage.
- Packet switching offers improved delay characteristics, because there are no long messages in the queue (max packet size fixed).
- Packet can be routed (if any busy/disabled links).
- The advantage of packet switching is that many network users can share the same channel at the same time.
- It can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages:

- Protocols are complex
- Cost of implementation
- Packet lost ⟺ sender retransmit data
- Delivery Quality is less.

* **Total time :**

Total time taken transmit a message in circuit switched network

IMP = Connection set up time + Transmission delay + propagation delay + Tear down time.

where,

$$\text{Transmission delay} = \frac{\text{Message size}}{\text{Bandwidth}}$$

$$\text{Propagation delay} = \frac{(\text{No. of hops on way}) \times (\text{dist btwn 2 hops})}{\text{propagation speed}}$$

Ex: Consider all links in the network use TDM with 24 slots and have a data rate of 1.536 Mbps. Assume that host A takes 500 m sec to establish an end to end circuit with host B before begin to transmit the file. If the file is 512 kilobytes, then how much time will it take to send the file from host A to B?

Sol: Given data:

Total Bandwidth = 1.536 Mbps.

Bandwidth is shared among = 24 slots.

Connection setup time = 500 m sec

File size = 512 KB

$$\Rightarrow \text{Bandwidth per user} = \frac{\text{Total Bandwidth}}{\text{No. of users}} = \frac{1.536 \text{ Mbps}}{24}$$

$$= 0.064 \text{ Mbps}$$

GUDI VARAPRASAD - COMPUTER NETWORKS

⇒ Transmission delay $= \dfrac{\text{File size}}{\text{Bandwidth}} = T_t$

$$= \frac{512 \text{ KB}}{64 \text{ Kbps}} = \frac{512 \times 2^{10} \times 8 \text{ bits}}{64 \times 10^3 \text{ bits per sec}}$$

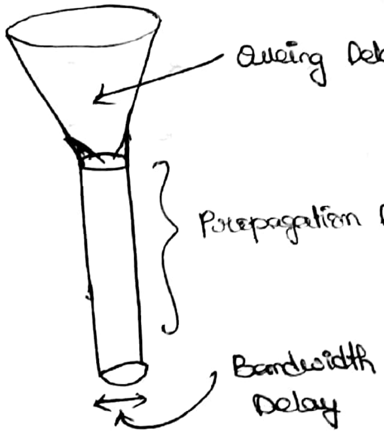
$$= 65.536 \text{ sec} = \underline{\underline{65536 \text{ m sec}}}$$

⇒ Time taken to send a file in circuit switched network

= Connection set up time + Transmission delay

$= 500 \text{ m sec} + 65536 \text{ m sec} = 66036$ ~~sec~~ m sec

$= \underline{\underline{66.036 \text{ sec}}}$



- $\boxed{\text{Propagation Delay} = \dfrac{\text{Distance}}{\text{Propagation speed}}}$

- $\boxed{\text{Transmission Delay} = \dfrac{\text{Message size}}{\text{bandwidth bps}}}$

- $\boxed{\text{Latency} = \text{Propagation delay} + \text{Transmission delay} + \text{Queing time} + \text{Processing Time}}$

Ex: What is the propagation time if the distance between the two points is 12,000 km? Assume the propagation speed to be 2.4×10^8 m/s in Cable.

Sol: We can calculate propagation time as,

$$\text{Propagation time} = \frac{\text{distance}}{\text{Propagation speed}} = \frac{12{,}000 \times 10^3}{2.4 \times 10^8}$$

$$= 50 \text{ ms}$$

GUDI VARAPRASAD - COMPUTER NETWORKS

Ex : What are the propagation time and the transmission time for 2.5 K byte message (an e-mail) if the bandwidth of the network is 1 Gbps ? Assume the distance between the sender and the receiver is 12,000 Km and that light travels at 2.4×10^8 m/s

Sol :

$$\text{propagation time} = \frac{\text{distance}}{\text{propagation Speed}} = 50 \text{ ms}$$

$$\text{Transmission time} = \frac{\text{Message size}}{\text{Bandwidth bps}} = \frac{2500 \times 8}{10^9}$$

$$= 0.020 \text{ ms}$$

Note : In this case, because the message is short & the bandwidth is high, the dominant factor is the propagation time, not the transmission time. The transmission time can be ignored.

CASES :

① Case 1 : A —— B

- Propagation delay is 40 μsec.
- Bandwidth is 1 byte / μsec (1 mB / sec, 8 Mbit / sec).
- Packet size is 200 bytes (200 μsec bandwidth delay).
- The total one-way transmit time is 240 μsec = 200 μsec + 40 μsec

② Case 2 : A ———————— B

Now propagation delay is increased to 4 ms

Total transmit time = 4200 μsec = 200 μsec + 4000 μsec

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

③ Case 3 : A —— R —— B

- We now have two links, each with propagation delay 40 μsec, bandwidth and packet size as in Case 1
- Total transmit time for one 200-byte packet is now 480 μsec = 240 + 240
- There are two propagation delays of 40 μsec each ; A introduces a bandwidth delay of 200 μsec and R introduces a store-and-forward delay (or second bandwidth delay) of 200 μsec.

④ Case 4 : A — R —— B

- Same as Case 3, but with data sent as two 100-byte pack
- Total transmit time = 380 μsec

= 3 × 100 + 2 × 40.

Abbr.	Prefix name	Decimal size	Size in thousands	Binary approximation
K	kilo-	10^3	1,000	$1{,}024 = 2^{10}$
M	mega-	10^6	$1{,}000^2$	$1{,}024^2 = 2^{20}$
G	giga-	10^9	$1{,}000^3$	$1{,}024^3 = 2^{30}$
T	tera-	10^{12}	$1{,}000^4$	$1{,}024^4 = 2^{40}$
P	peta-	10^{15}	$1{,}000^5$	$1{,}024^5 = 2^{50}$
E	exa-	10^{18}	$1{,}000^6$	$1{,}024^6 = 2^{60}$

DATA LINK LAYER — MODULE 3

* • Data Link Layer Design Issues
    - Services provided to the Network Layer
    - Framing
    - Error Control
    - Flow Control

* • Functions of Data Link layer
    - Provide service interface to the network layer
    - Dealing with transmission errors.
    - Regulating data flow (slow receivers not swamped by fast sender)

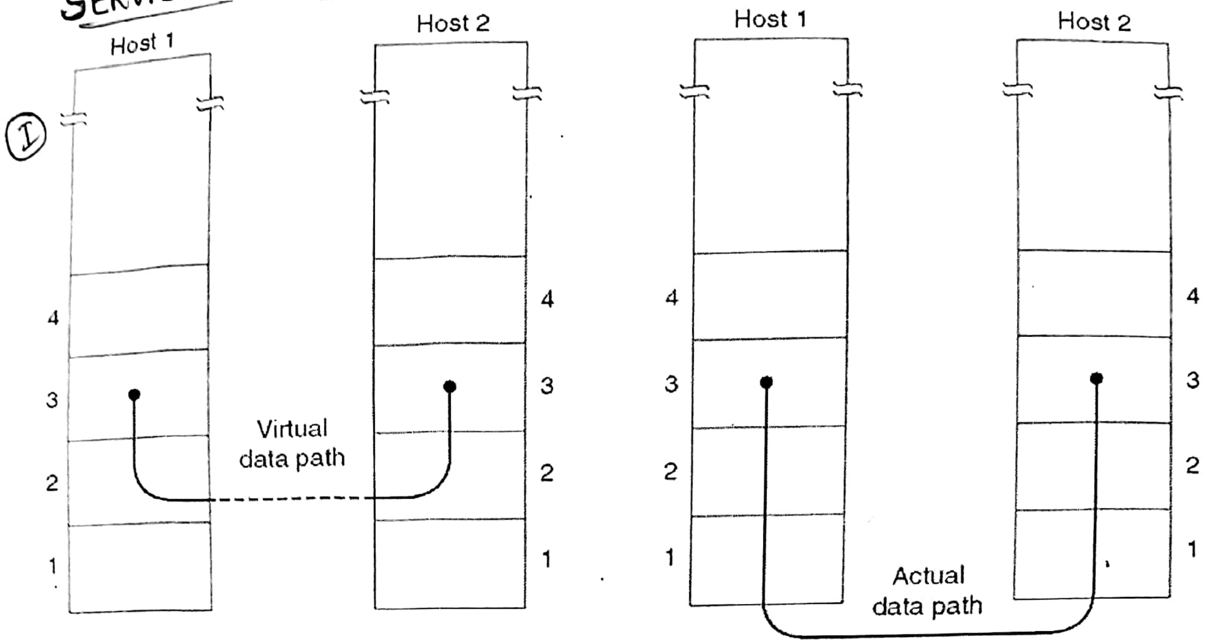
* • Services Provided to Network Layer :

	Service	Example
Connection oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Types of Services – Characteristic, Example

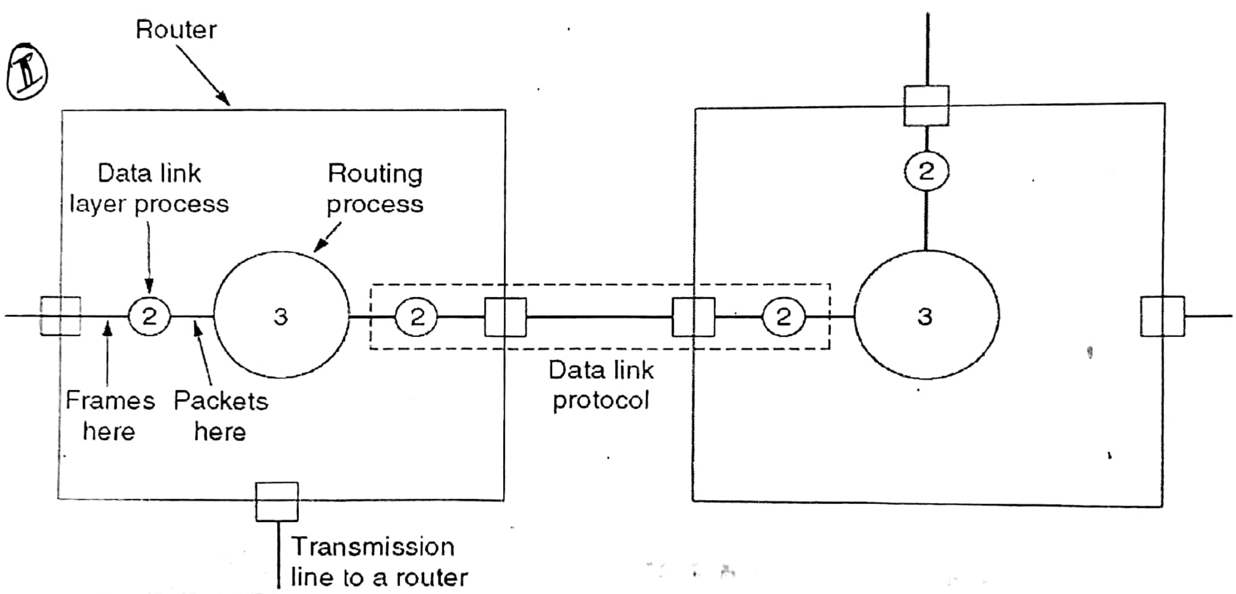
GUDI VARAPRASAD - COMPUTER NETWORKS

SERVICES PROVIDED TO NETWORK LAYER :

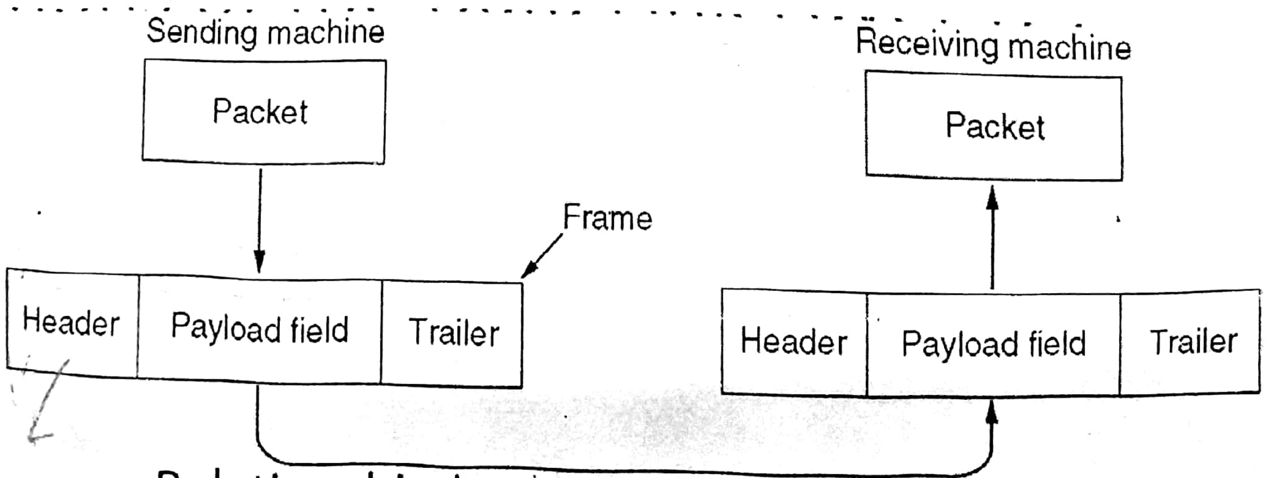


(a) Virtual communication

(b) Actual communication



As a packet travels across the Internet from A to B, it may go along multiple types of links (phone, fiber, wireless), each with different frame sizes and formats. Packet may be encoded in a different way for each link it travels on.



Relationship between packets and frames.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*. TYPES OF SERVICES :

1. Unacknowledged Connectionless Service :

- No independent frames.
- No logical connection is setup between the host machines.
- Error & Data loss is not handled in this service.
- This applicable in Ethernet services and voice communication.

2. Acknowledged Connectionless Service :

- Each frame sent by source machine is acknowledged by the destination machine.
- Resends the frame if Acknowledged is not received.
- Wi-fi (IEEE 802.11) services.

3. Acknowledged Connection oriented Service :

- A logical connection is setup.
- Frames are numbered that keep track of loss of frames and also ensures that frames are received in correct order.
- Setup of connection, sending frames, Release connection.

*. FRAME PARTS :

Flag	Header	Payload Field	Trailer	Flag

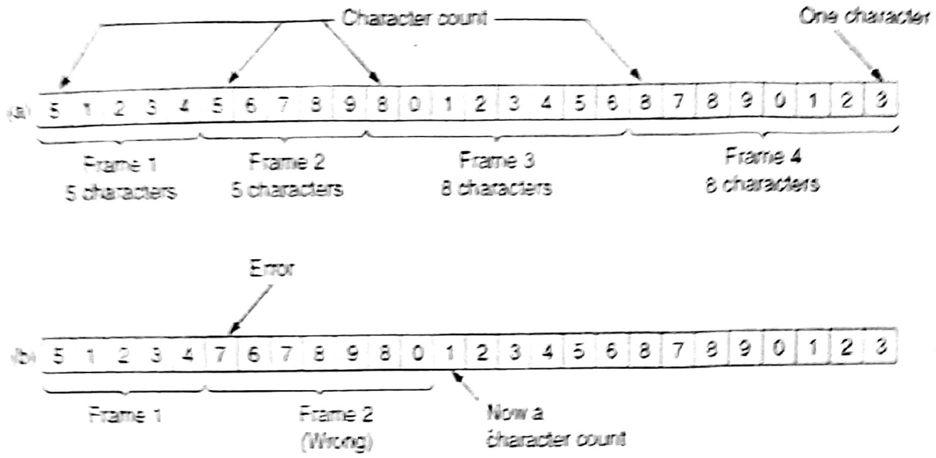
- Framing is of 2 types :

1. Fixed sized framing — ATM Cells
2. Variable sized framing — LAN

FRAMING

A character stream. (a) Without errors. (b) With one error.

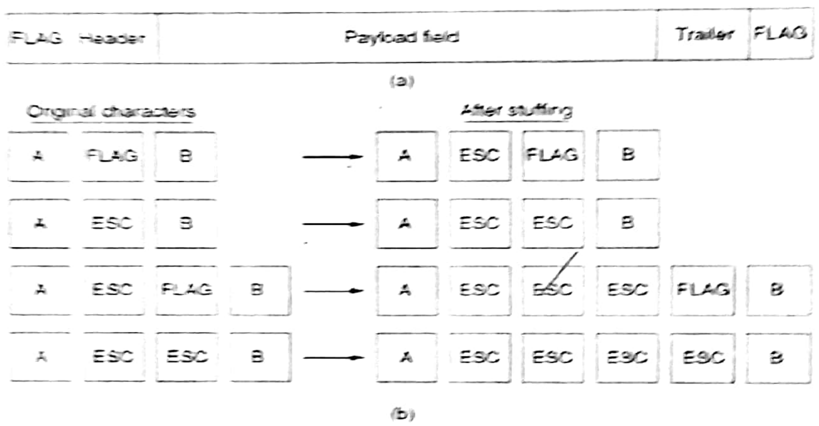
I.



Bit stuffing

IMP

II.

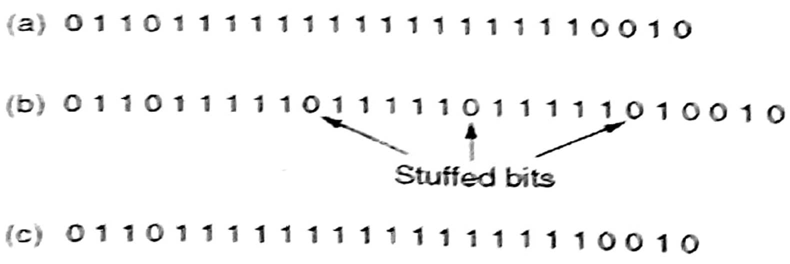


Byte stuffing

A frame delimited by flag bytes.
Four examples of byte sequences before and after stuffing.

IMP

III.



Bit stuffing

Bit stuffing
- The original data.
- The data as they appear on the line.
- The data as they are stored in receiver's memory after destuffing.

GUDI VARAPRASAD - COMPUTER NETWORKS

*. (2) VARIABLE SIZING :

- Length Field - length field determines the size of the frame. It is used in Ethernet (IEEE 802.3)

- End Delimiter - pattern determines the size of frame. It is used in Token rings. If the pattern occurs in the message, then two approaches are used to avoid situation.

(I) Byte Stuffing : A byte is stuffed in message to differentiate from the delimiter. This is also called character-oriented framing.

(II) Bit stuffing : A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit oriented framing.

BIT STUFFING

*INP Whenever 5 Consecutive 1's appear, a 0 will be inserted by the sender, independent of next value (may be it is 0 or 1)

And, whenever receiver encounters 5 Consecutive 1's, it will remove a 0 after it except for begining and ending

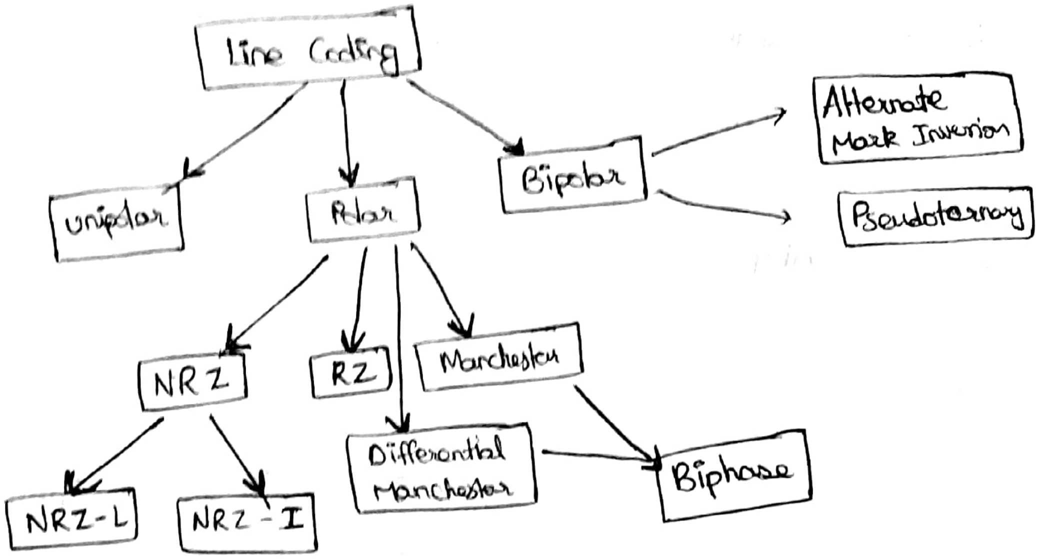
HDLC Protocol : Begining & Ending Sequence → $\underbrace{01111110}_{8 \text{ bits}}$

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

ENCODING SCHEMA :

1. Digital to Digital Encoding



a. Unipolar Encoding :

1 – high voltage 0 – No voltage

b. Non Return to Zero level :

0 – high level

1 – low level

c. Non Return to Zero Inverted :

0 – no transition at begining of interval

1 – transition at beginning of interval

d. Manchester :

= Zero 0 0 – high to low transition

= One 1 1 – low to high transition

GUDI VARAPRASAD - COMPUTER NETWORKS

e. Differential Manchester :

Always a transition in middle of interval

0 - transition at begining of interval

1 - no transition at begining of interval

f. Bipolar - AMI :

0 - no line signal

1 - { positive (if before 1 was negative)
 negative (if before 1 was positive)

Alternating "1"

g. Bipolar - Pseudoternary :

0 - { Positive (if before 0 was negative)
 negative (if before 0 was positive)

Alternating "0"

1 - no line signal

h. Return to Zero RZ :

0 - negative voltage 1 - positive voltage

i. B8ZS :

Same as Bipolar AMI, except that any string of eight zeros is replaced by string with two code violation

j. HDB3 :

Same as bipolar AMI, except that any string of four zeros is replaced by a string with one code violatio

GUDI VARAPRASAD - COMPUTER NETWORKS

(optional)
*. FUNCTIONS OF TRANSPORT LAYER IN OSI MODEL :

- The transport layer in the open system Interconnection (OSI) model is responsible for end to end delivery over a network.
- whereas the network layer is concerned with end-to-end delivery of individual packets and it does not recognize any relationship between these packets.
- Specific functions of Transport Layer as follows :

① Service point addressing :

- Computers often run many programs at same time. Due to this, source to destination delivery means delivery from specific job (currently running program) on one computer to specific job (currently running program) on other computer not only one computer to the next.
- For this reason, the transport layer added a specific type of address to its header, it is referred to as a service point address / port address.
- By this address each packet reaches the correct computer and also the transport layer gets the complete message to the correct process on that computer.

② Flow control :

- The transport layer also responsible for the flow control mechanism between the adj layers of TCP/IP model

Ex :

Files = 500 Bytes

(ABC) —— bandwidth = 4 Mbps, dist = 3000 km —— (BCD) —— bandwidth = 10 Mbps, dist = 900 km —— (CDE)

Data travel with speed of light, $C = 3 \times 10^8$ m/s

Calculate transmission delay

✓ Transmission delay = $\frac{\text{File Size}}{\text{Bandwidth}}$

Btwn ABC — BCD = $\frac{500 \times 8}{4 \times 10^6} \approx 10^{-3}$ = 1 m sec

Btwn BCD — CDE = (Find)

✓ Propagation delay = $\frac{\text{distance of link}}{\text{Speed propagation}}$ =

Btwn ABC — BCD = $\frac{3000 \times 10^3}{3 \times 10^8} = 10^{-2} \approx$ 10 m sec

Btwn BCD – CDE = (Find)

end to end delay = (ABC – BCD) + (BCD – CDE) . . . Add all

Units :

Byte = 8 bits

Mbps = 10^6 bits per second

ms = 1×10^{-3} seconds

Speed of light (c) = 3×10^8 m/s

= 3×10^5 km/s

< 2 km — Twisted Pair

< 10 km — Co Axial Cable

> 10 km, < 40 km — optical Fibre

Twisted Pair for longer distance,

→ Amplifier

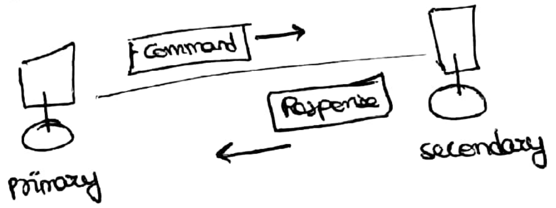
→ Repeater

GUDI VARAPRASAD - COMPUTER NETWORKS

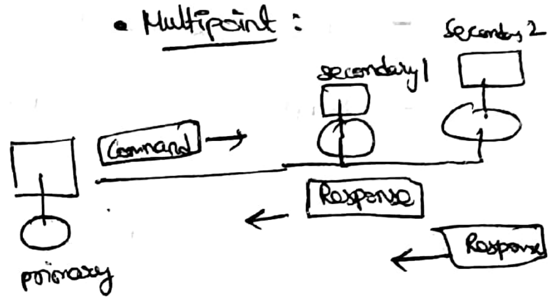
GUDI VARAPRASAD - COMPUTER NETWORKS

- HDLC : High level Datalink Control Protocol

- Point to Point :



- Multipoint :



- ISO 33009 , ISO 4335
- Most widely used DLC protocol
- A Bit oriented protocol
- supports both half-duplex and full-duplex communication over point to point & multipoint link.

- Primary station :
  - Controls operation of link
  - Issues commands (frames)
  - Maintains separate logical link to each secondary station

- Secondary station :
  - Under control of primary station
  - Issues responses (frames)

- Combined station : (~~Normal~~ Asynchronous Response Mode)
  - May issue commands and responses.
  - Combines the features of primary & secondary stations.

- Link Configuration – Unbalanced : (Normal Response Mode)
  - one primary and one or more secondary stations
  - supports full duplex and half duplex.

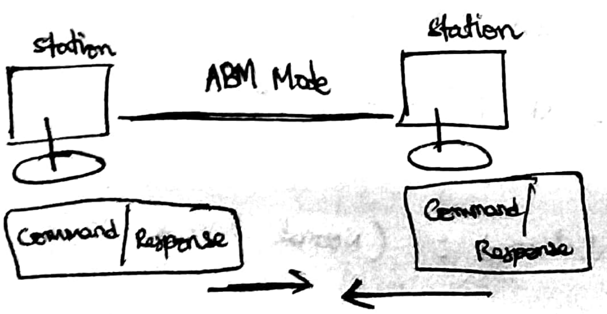
GUDI VARAPRASAD - COMPUTER NETWORKS

- **Balanced link Configuration :** (Asychronous Balance Mode)
  - Two combined stations
  - Supports Full duplex & Half duplex

- **Normal Response Mode :** (NRM)
  - Unbalanced configuration.
  - Primary can only initiate transmission.
  - Secondary may only transmit data in response to command (poll) from primary.
  - Used on multi-drop lines.
  - Host computer as primary
  - Terminals as secondary

Ex : Point to Point | Multipoint

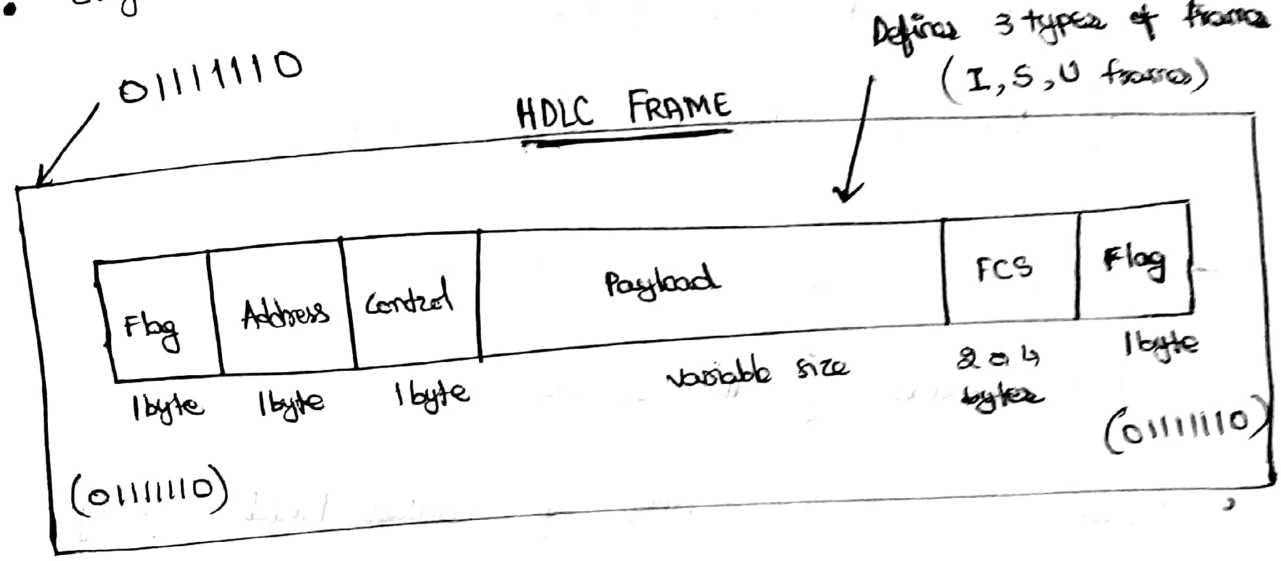
- **Asynchronous Balanced Mode :** (ABM)
  - Balanced configuration
  - Either station may initiate transmission without receiving permission
  - Most widely used
  - No polling overhead
  - Combined station is scenario



*. FRAME STRUCTURE IN HDLC Protocol :

- Synchronous transmission
- All transmissions in frames
- Single frame format for all data and control exchanges.

(works same like Bit Stuffing)



Flag Fields :

- Delimit frame at both ends
- 01111110
- Receiver hunts for flag sequence to synchronize containing
  01111110
  - The transmitter inserts 0 bit after every sequence of five 1s with the exception of flag fields.
  - If receiver detects five 1s it checks next bit,
    - → 0 , it is deleted
    - → 10 → accept as flag
    - → 11 → abort the connection

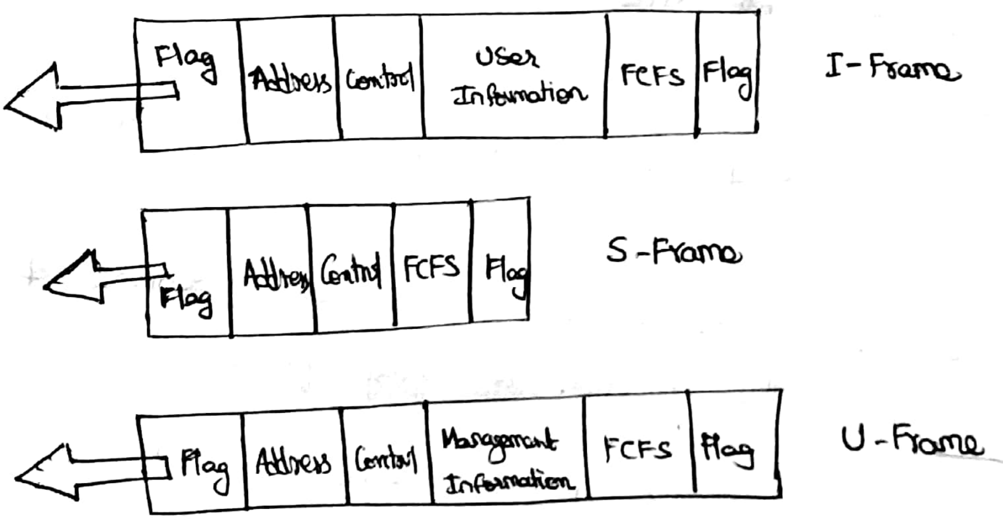
Control Fields :

- Different for different frame type

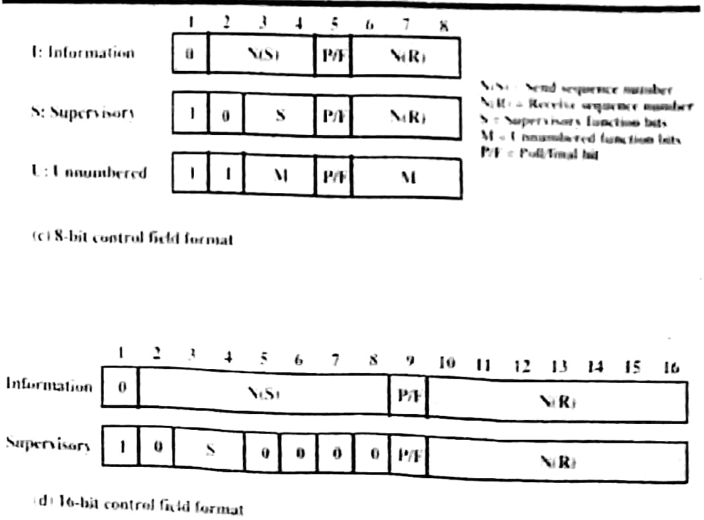
GUDI VARAPRASAD - COMPUTER NETWORKS

- I Frame (information frame)
  - → Data to be transmitted to user (next layer up)
  - → Flow & error control piggybacked on information frame
- S Frame (Supervisory frame)
  - → Used for Flow & Error Control
- U Frame (Unnumbered Frame)
  - → Supplementary link Controls

• First one or two bits of control Field identify frame type.



Control Field Diagram



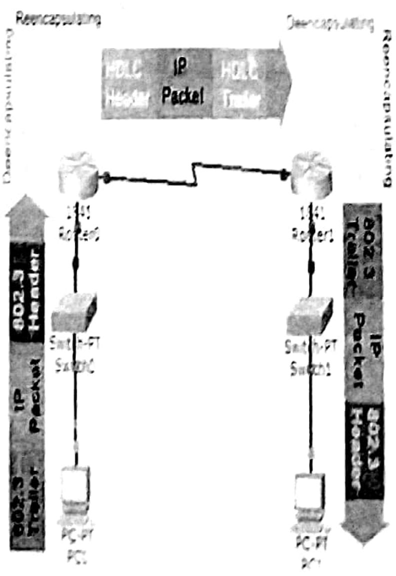
(c) 8-bit control field format

(d) 16-bit control field format

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- layer 3 destination address.
- Since destination address is connected with serial link router will forward this frame in serial interface.
- Serial interface will re-encapsulate the frame with serial encapsulation protocol. In our example it is HDLC.
- After re encapsulation this frame will be forwarded from serial interface.
- This frame will be received in serial interface of Router R1
- R1 will de-encapsulate the frame in packet to find the layer 3 destination address.
- Since destination address is connected via FastEthernet, it will forward this packet in FastEthernet interface.
- Fast Ethernet will re-encapsulate the packet in Ethernet Frame
- After re-encapsulation of this Frame, it will be forwarded from FastEthernet interface
- Through switch, this frame will be received at PC1.
- PC1 will receive this frame in exactly same format as it was packet by PC0 without knowing how it makes it way to him.



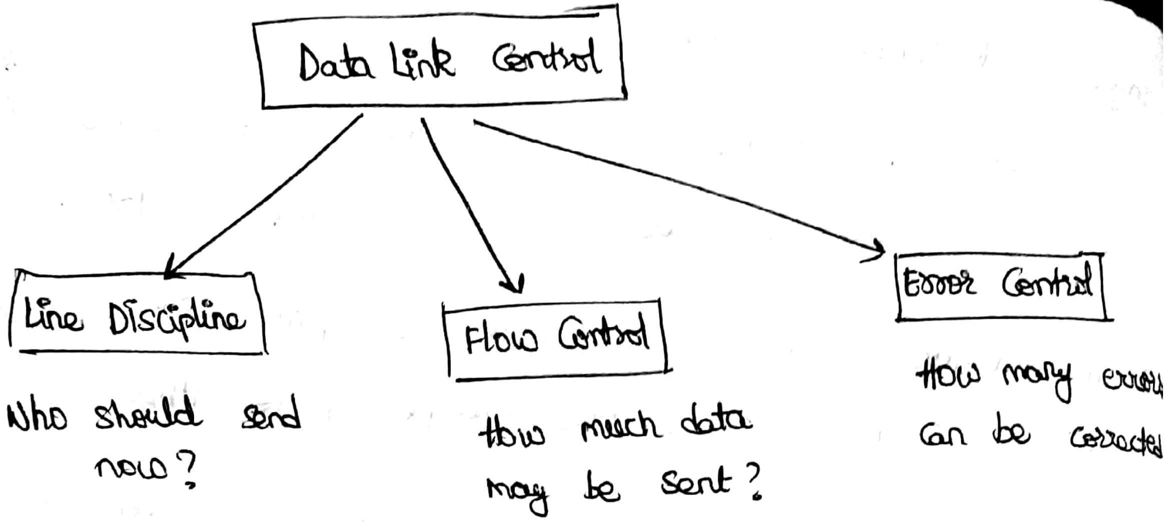
Data link layer of PC0 will warp this IP packet in 802.3 header and trailer. Once wrapped, it becomes frame.

Physical layer of PC0 will put this frame in wire.

Through switch this frame will be received in Router R0.

Router will de-encapsulate the frame in packet to find out the

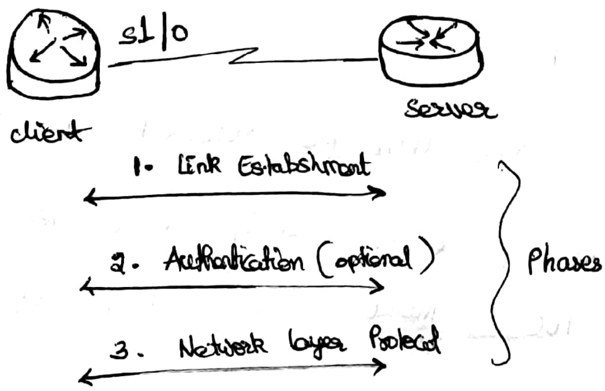
GUDI VARAPRASAD - COMPUTER NETWORKS



- <u>Flow Control</u> - refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

- <u>Error Control</u> - in data link layer is based on automatic repeat request, which is the retransmission of data.

*. <u>PPP - Point to Point</u> Protocol :



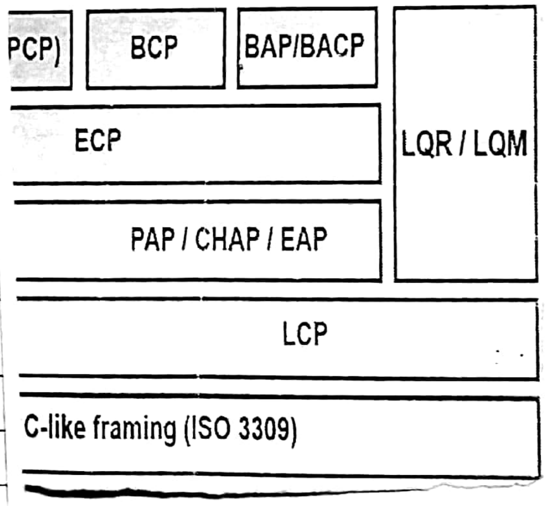
- Although HDLC is a general protocol that can be used for both point-to-point and multipoint config, one of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP).

- PPP is byte oriented protocol.

- PPP is byte-oriented protocol using byte stuffing with the escape byte 01111110.

- <u>PPP services</u>:
  - It defines the format of the frame to be exchanged between devices.
  - It defines how two devices can negotiate the establishment of the link and the exchanged of data.
  - It defines how network layer data are encapsulated in the data link frame.
  - It defines how two devices can authenticate each other.

L2 Function	Description	Provided by PPP Protocol
Framing	Serial lines provide bit transport, thus a means for finding the start of packets is required	HDLC (not part of PPP protocol suite but provided by ISO 3309 HDLC). PPP defines HDLC as default framing protocol.
Link setup, control	Link characteristics like maximum frame size need to be negotiated between both ends	LCP
Authentication	Client (and optional server) authentication make sure the right communication partners talk to each other	PAP / CHAP / EAP
Encryption	Communication may need confidentiality.	ECP along with encryption algorithms like 3DES or AES
Bandwidth allocation for multi-links	To fulfill increased bandwidth demands, bonding of multiple channels may be required (Multilink PPP-MLPPP)	BAP / BACP
Bridging / routing mode on both ends	The link ends may be operated in bridged or routed mode. Bridging requires a control protocol.	BCP
Setup of network functions	Each network protocol (IP, IPX) requires its own control protocol for functions like IP address assignment.	NCP (IPCP)
Data compression on link	Serial links are typically slow (modem lines etc.), so compression increases available bandwidth	CCP
Monitoring the link	The link quality may need to be monitored	LQR / LQM



- PPP is not a single protocol but a protocol suite containing protocols that address various aspects of point to point layer 2 communication.

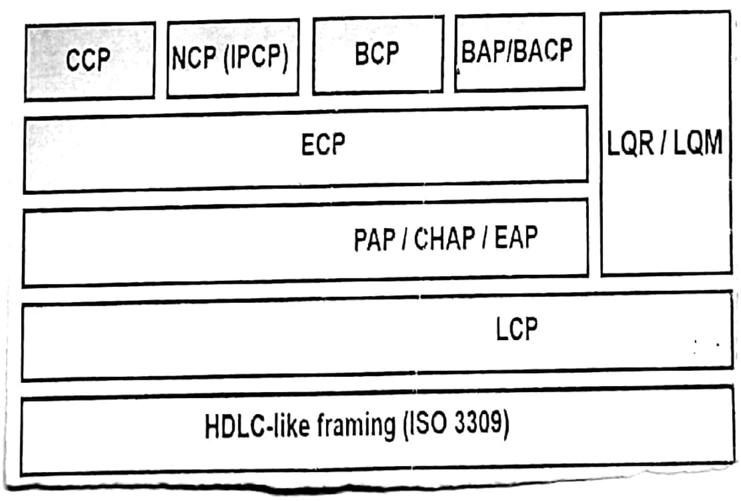
- PPP is an asymmetric protocol suite. The 2 parties in PPP session are the initiator (I, usually client) and responder (R, usually server).

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- PPP is byte-oriented protocol using byte stuffing with the escape byte 01111110.

- PPP services :
  - It defines the format of the frame to be exchanged between devices.
  - It defines how two devices can negotiate the establishment of the link and the exchanged of data.
  - It defines how network layer data are encapsulated in the data link frame.
  - defines how two devices can authenticate each other.

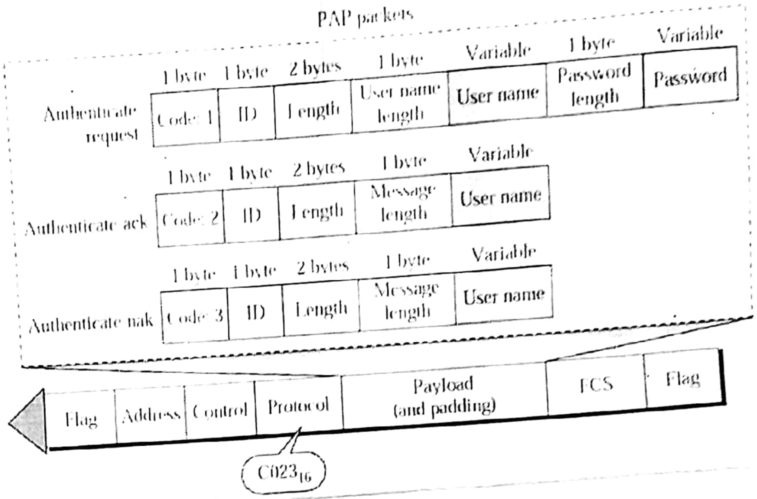


ol Stack : AKA (RFC 1661)

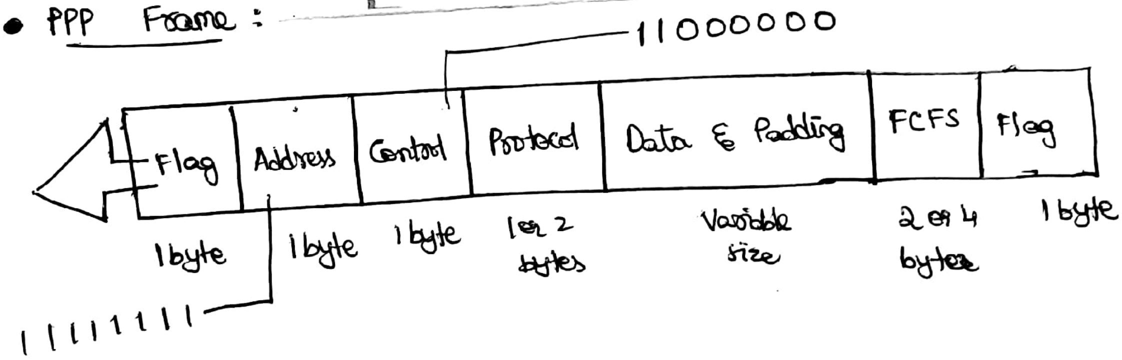
- PPP is not a single protocol but a protocol suite containing protocols that address various aspects of point to point layer 2 communication.

- PPP is an asymmetric protocol suite. The 2 parties in PPP session are the initiator (I, usually client) and responder (R, usually server).

- PPP's main functions are :
  - + Packet encapsulation and framing on point to point link
  - + Link setup (LCP sub - protocol)
  - + Authentication
  - + Network control, basically assigning an IP address and DNS server address to clients.



- PPP Frame :



* . TRANSITION STATE :

- Idle state : The idle state means that the link is not being used. There is no active carrier, and the line is quiet.

- Establishing Link : When one of the end point starts the communication, the connection goes into the establishing state. In this state, options are negotiated between the two parties.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

If the negotiation is successful, the system goes to the authenticating state (if authentication is required) or directly to the networking state.

- Authenticating state : The authenticating state is optional. If the result is successful, the connection goes to the networking state; otherwise, it goes to the terminating state.

*. LCP & NCP :

A. LCP (Link Control Protocol) :

- LCP is used for establishing the link options like :
  a. Authentication protocol to be used.
  b. Header compression / address Field compression.
  c. Maximum Receive Unit (MRU)

- LCP periodically tests the link with symmetric LCP - Echo requests / replies. LCP brings down the link gracefully when it is no longer in use.

B. NCP (Network Control Protocol) :

- NCP is used for the dynamic assignment of an IP address to the client for the assignment of a primary and secondary DNS Server.

- The host must set a default gateway IP address. (the link is PPP, thus typically the link is unnumbered i.e. without an IP address on the server side).

*. Authentication Protocols :

- Authentication plays a very important role in PPP becau where PPP is designed for use over dial-up links where verification of user identity is necessary.

- Authentication means validating the identity of a user who needs to access a set of resources.

IMP
- PPP uses two protocols for authentication : Password Authentication protocol (PAP) and challenge Handshak Authentication Protocol (CHAP).

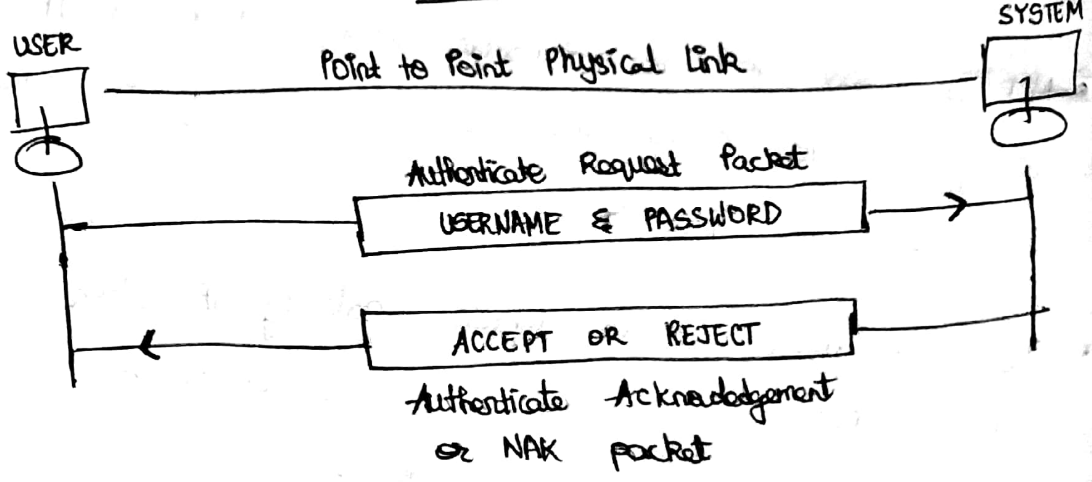
PAP :

- The PAP is a simple authentication procedure with two steps :

1. The user who wants to access a system sends an ID (identification) and a password.

2. The system checks the validity of the identification and password and either accepts or denies a connection.

PAP

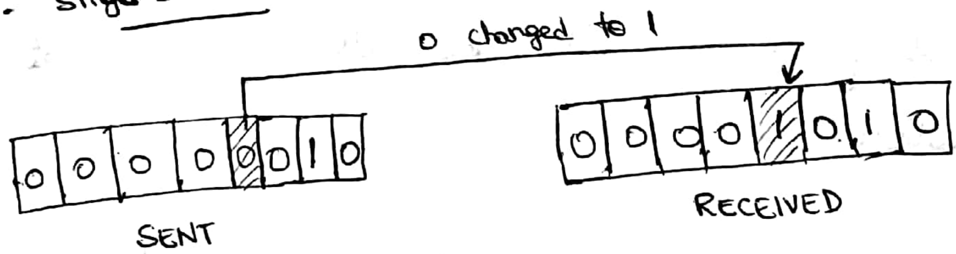


GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*. TYPES OF ERRORS :

1. Single Bit error :

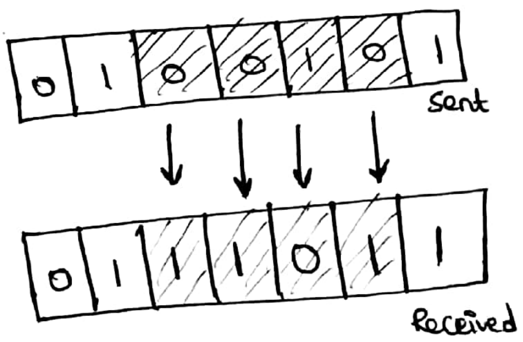


- Single bit errors are the least likely type of errors in serial data transmission because the noise must have a very short duration which is very rare. However this kind of errors can happen in parallel transmission.

Ex :

- If data is sent at 1 Mbps then each bit lasts only $1/1000\,000$ sec or $1\,\mu s$.
- For a single bit error to occur, the noise must have a duration of only $1\,\mu s$, which is very rare.

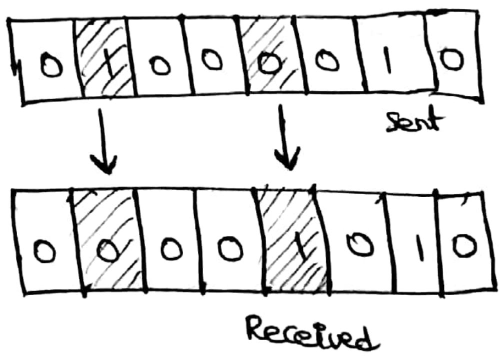
2. Burst error :



$1 \rightarrow 0$
$0 \rightarrow 1$ } need not be consecutive

- burst is measured from 1st corrupted bit to last corrupted bit. { SERIAL TRANSMISSION }

3. Multiple Bit error :

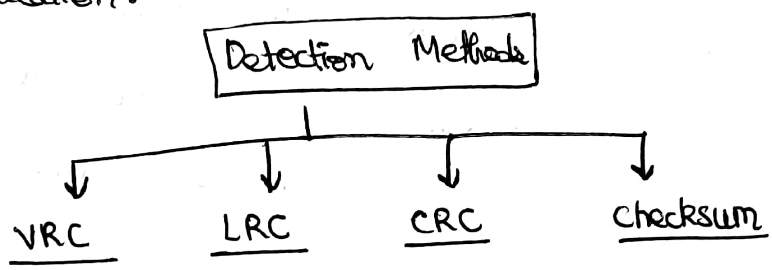


TWO ERRORS

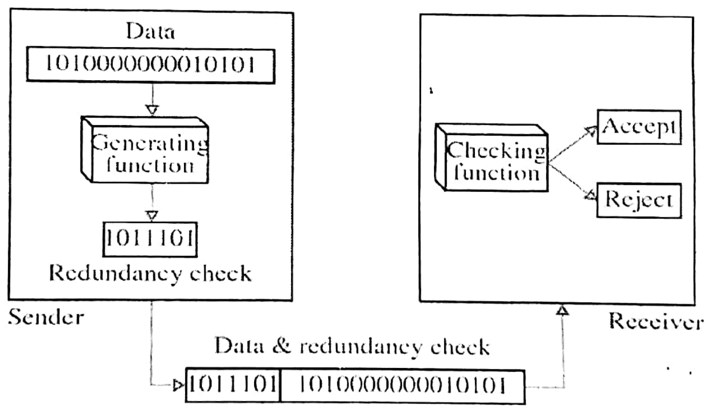
*. ERROR DETECTION :

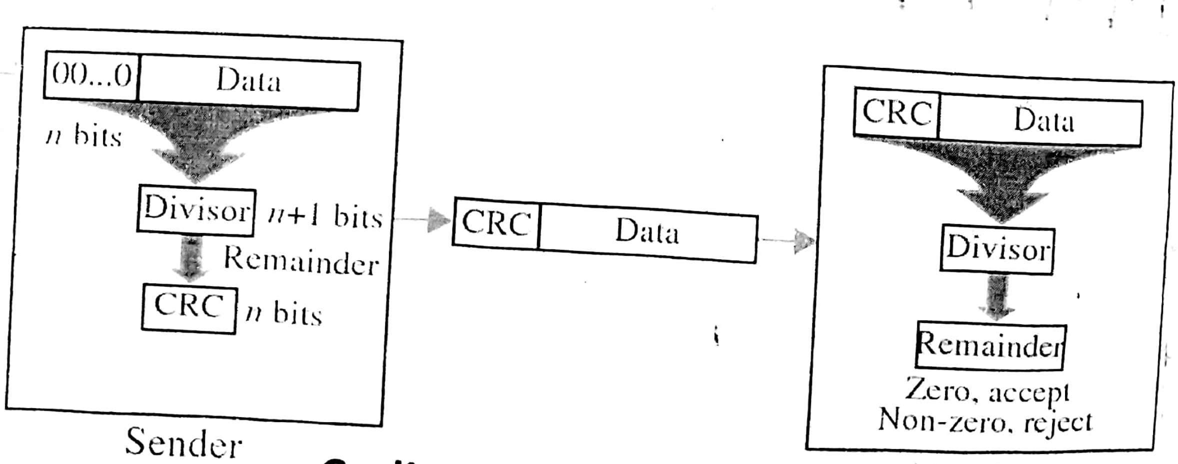
- Error detection uses the concept of redundancy, which means adding extra bits for detecting error at the destination.

- Four types of Redundancy checks are used in data communication.



Redundancy





Cyclic Redundancy Check

GUDI VARAPRASAD - COMPUTER NETWORKS

* Cyclic Redundancy Check (CRC):

- Given a K bit frame or message, the transmitter generates an n-bit sequence, known as frame check sequence (FCS), so that an resulting frame, consisting of (K+n) bits, is exactly divisible by some predetermined number.

- The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.

Ex: Binary division

```
            111101
1101 ) 100100000        (111101  => Quotient
 ⇓  (-) 1101                     → Divident
Divisor  1000
     (-) 1101
          1010
     (-)  1101
          01110
     (-)   1101
           0110
     (-)   0000
            1100
     (-)    1101
             001    => Remainder
```

- Any ~~redun~~ error detection technique, we are going to append the redundant bits with the message because this redundant bit will only enable the receiver to detect whether there is an error or not.

GUDI VARAPRASAD - COMPUTER NETWORKS

Ex :

Find the CRC for the data blocks 100100 with the divisor 1101

Algorithm : CRC Generation at Sender side :

1. Find the length of the divisor 'L'. (0's to be)
2. Append 'L-1' bits to the original message.
3. Perform binary division operation.
4. Remainder obtained for division = CRC.

Note : The CRC must be of L-1 bits.

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

In the Question,

Length of Divisor, L = 4

Append, L-1 = 4-1 = 3 bits (0's are to be appended)

Now, original message = 100100

After appending to original message = 100100**000**

After performing division (binary), — check back

Quotient = 111101 Remainder = 001 (3 bits)

CRC : 001 (Remainder)

Data Transmitted : 100100**001** (append CRC to original message)

100100 → original message

001 → CRC

GUDI VARAPRASAD - COMPUTER NETWORKS

Ex :

Find the CRC for 1110010101 with the divisor $x^3 + x^2 + 1$?

divisor = $x^3 + x^2 + 1$ → polynomial take Quotients = 1 1 0 1.

x^3	x^2	x^1	x^0
1	1	0	1

L = 4 , L−1 = 4−1 = 3 (append 3 bits)

1110010101000 → appended original message

divisor = 1101

After Binary division,

Quotient = 0100011010 0 Remainder = 100

CRC = ~~100~~ 100

1110010101100

Data Transmitted : 1110010101 | 100 ✓

original message | CRC

CRC analyzation at Receiver side :

1. Receiver gets the Data Transmitted from sender side
2. The divisor is common for both sender & Receiver. The protocol decides the divisor (polynomial)
3. Perform Binary divison with same divisor & dividend as the Data transmitted.
4. If Remainder = 0 → Receiver accepts the data & there are no errors during transmission.

Else Remainder ≠ 0 → Receiver rejects the data concluding there are transmission errors.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*- SINGLE BIT ERROR CORRECTION :

- Also called Hamming Code Error Correction
- Given by R.W. Hamming
- Easy to implement
- 7 bit hamming code is used commonly.

1. Data Bit – Data to be transmitted ~ 4
2. Parity Bit – Additional bits to detect error in transmission ~ 3

} In 7 bit Hamming Code

D7	D6	D5	P4	D3	P2	P1

→ 7 bit Hamming Code

P_1 → depends on $D_3\ D_5\ D_7$

P_2 → depends on $D_3\ D_6\ D_7$

P_4 → depends on $D_5\ D_6\ D_7$

Parity Bits ~ 2^n $\forall\ n = 0, 1, 3, \dots$

$(P_1, P_2 \dots P_{2^n})$

- Working for even parity (combination of P, D values) should have even 1's

Ex :

Transmit 4 bit data 1011. Identify Noise.

1	0	1	1
D_7	D_6	D_5	D_3

D_7	D_6	D_5	P_4	D_3	P_2	P_1
1	0	1		1		

At Sender side channel,

1	1	1	1

$P_1 \rightarrow P_3 \; D_5 \; D_7 \Rightarrow P_1 = 1$ So, even parity

$P_2 \rightarrow D_3 \; D_6 \; D_7 \Rightarrow P_2 = 0$ So, even parity

0 1 0 1

$P_4 \rightarrow D_5 \; D_6 \; D_7 \Rightarrow P_4 = 0$ So, even parity

0 1 0 1

1	0	1	0	1	0	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

Bits Sent Message :

1010101

Any change $\Downarrow$ NOISE

1010101 $\longrightarrow$ Sender sent Message

Assume Receiver received bit stream as 1110101

The receiver will analyse Parity bits $P_1 \; P_2 \; P_4$ & decide if there is any noise in chanel & error in transmitted bit stream.

Received Message bit stream $\Rightarrow$

1	1	1	0	1	0	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

According to this, Analyzing parity bits will be

$P_1 \rightarrow D_3 \; D_5 \; D_7 \sim 1 \; 1 \; 1 \; 1$ ✓ even parity ✓

$P_2 \rightarrow D_3 \; D_6 \; D_7 \sim 0 \; 1 \; 1 \; 1$ ✗ even parity ✗

$P_4 \rightarrow D_5 \; D_6 \; D_7 \sim 0 \; 1 \; 1 \; 1$ ✗ even parity ✗

D_3, D_5, D_7 values are correct. left over corrupted is D_6 $\Rightarrow$ D_6 must be corrupted because of noise

GUDI VARAPRASAD - COMPUTER NETWORKS

So, Receiver corrects the bit stream as

1	0	1	0	1	0	1

✓ Correct.

<u>Ex</u>: If the 7 bit hamming code word received by a receiver is 1011011. Assuming the even parity state whether the received code word is correct or wrong. If wrong located the bit having error.

<u>Sol</u>: Receiver received ⇒

1	0	1	1	0	1	1
D_7	D_6	D_5	P_4	D_3	P_2	P_1

Receiver checks for Parity bits are even parity or not P_1 P_2 P_4 combinations

$P_1 \rightarrow D_3\ D_5\ D_7 \sim 1\ 0\ 1\ 1$ ✗ even parity ✗

$P_2 \rightarrow D_3\ D_6\ D_7 \sim 1\ 0\ 0\ 1$ ✓ even parity ✓

$P_4 \rightarrow D_5\ D_6\ D_7 \sim 1\ 1\ 0\ 1$ ✗ even parity ✗

other way to correct error is,

P_4 D_5 D_6 D_7

1 1 0 1 → even parity failed ✗

⇒ Make $\boxed{\text{Parity bit} = 1}$ ⇒ $P_4 = 1$

P_2 D_3 D_6 D_7

⇒ 1 0 0 1 → even parity correct ✓

⇒ Make $\boxed{\text{Parity Bit} = 0}$ ⇒ $P_2 = 0$

GUDI VARAPRASAD - COMPUTER NETWORKS

P_1	D_3	D_5	D_7
1	0	1	1

$\rightarrow$ even parity failed ✗

$\Rightarrow$ Make $\boxed{\text{Parity bit} = 1}$ $\Rightarrow$ $P_1 = 1$

Now Parity bits are $(P_4\ P_2\ P_1)$

$\sim (P_4\ P_2\ P_1) \equiv (1\ 0\ 1)_2 = (5)_{10}$ Binary into decimal Conversion

Value is 5 $\Rightarrow$ D_5 is corrupted

Received $D_5 = 1$ $\Rightarrow$ Correction to $\boxed{D_5 = 0}$ ✓

$\therefore$

P_7	D_6	D_5	P_4	D_3	P_2	P_1	
1	0	1	1	0	1	1	$\rightarrow$ Received
1	0	0	1	0	1	1	$\Rightarrow$ After Correction

$\therefore$ Sender sent message was $= 1001011$

If parity bits are $P_1\ P_2\ P_4\ P_8$ $\Rightarrow$

$P_1 \rightarrow D_3\ D_5\ D_7\ D_9\ D_{11}$

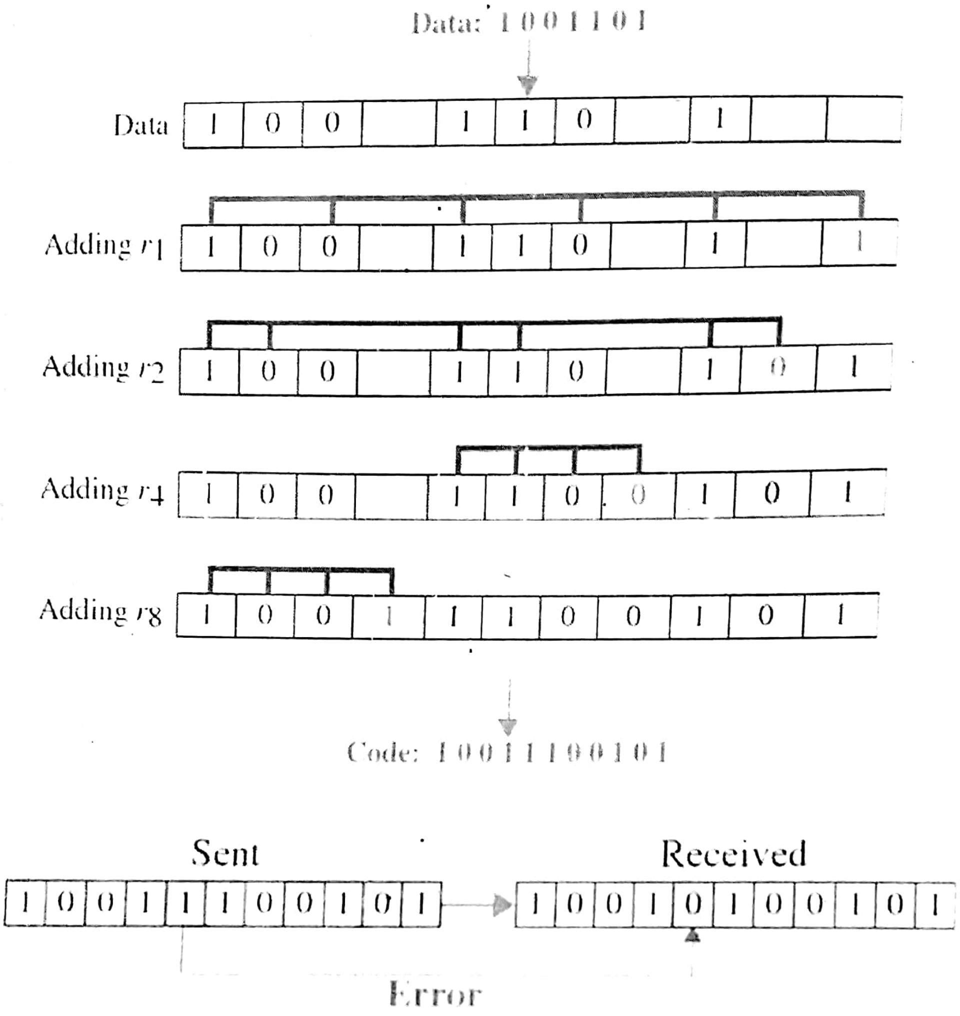
$P_2 \rightarrow D_3\ D_6\ D_7\ D_{10}\ D_{11}$

$P_4 \rightarrow D_5\ D_6\ D_7$

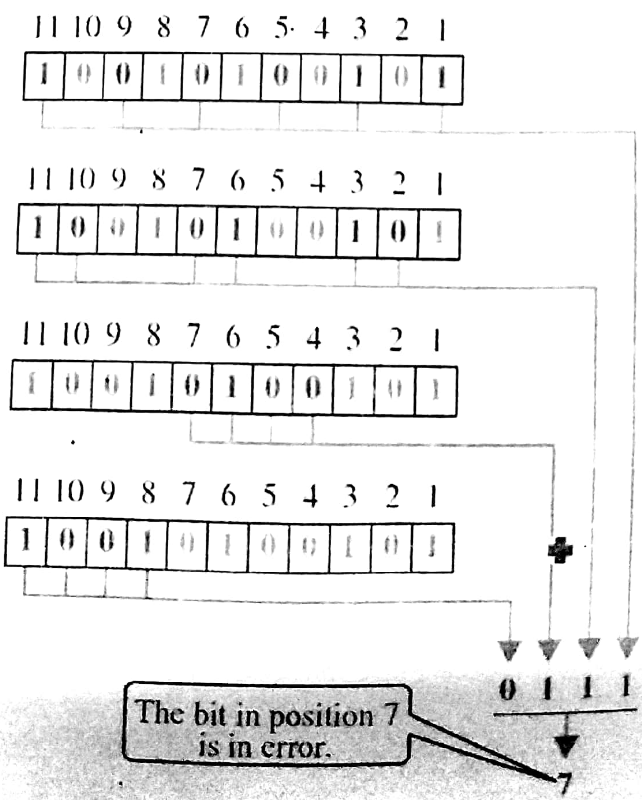
$P_8 \rightarrow D_9\ D_{10}\ D_{11}$

GUDI VARAPRASAD - COMPUTER NETWORKS

Example of Hamming Code



Error Detection



GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

Ex : Hamming Code for message $(1000)_2$

Given $m = 1000$ (4 bits)

$r = ?$

Formula, $\boxed{2^r \geq m+r+1}$ take least possible value for r given m

Initially put $r = 1 \rightarrow 2^1 \geq 4+1+1$ × false

Next put $r = 2 \rightarrow 2^2 \geq 4+2+1$ × false

Next put $r = 3 \rightarrow 2^3 \geq 4+3+1$ ✓ True

$\therefore \boxed{r = 3}$ P_1 P_2 P_4 Satisfying $2^r \geq m+r+1$ for $m = 4$

$\therefore$ $\boxed{\text{Transmitted message bit stream} = m+r}$

$T = m+r = 4+3 = 7$

1	0	0		0		
D_7	D_6	D_5	P_4	D_3	P_2	P_1

Given 1 0 0 0
D_7 D_6 D_5 D_3 $\Rightarrow$ Find P_1 P_2 P_4

Condition / Combination must satisfy even parity.

$P_1 \rightarrow D_3\, D_5\, D_7$
$\Downarrow$
1 0 0 1
$P_1 = 1$

$P_2 \rightarrow D_3\, D_6\, D_7$
$\Downarrow$
1 0 0 1
$P_2 = 1$

$P_4 \rightarrow D_5\, D_6\, D_7$
$\Downarrow$
1 0 0 1
$P_4 = 1$

$\therefore$ Hamming code to be tramitted to receiver side $=$ 1 0 0 1 0 1 1

GUDI VARAPRASAD - COMPUTER NETWORKS

Data link layer :

- It is responsible for moving data (frames) from one node to another node.

SERVICES PROVIDED BY DATA LINK LAYER :

- Framing
- Error Control
- Flow Control → speed matching mechanism
  → How much data ?
- Physical Addressing
- Access Control

slow Sender → Fast Receiver. (✓)

Fast Sender → slow Receiver (X) data Loss

Protocols (Flow Control)

- Noiseless Channels
  - Simplest
  - Stop & Wait
- Noisy channel
  - Stop & Wait ARQ
  - Go Back N ARQ
  - Selective Repeat ARQ

* Stop & Wait Protocol :

- Stop & wait protocol is data link layer protocol for transmission of frames over noiseless channels.
- It provides unidirected data transmission with flow control facilities but without error control facilities.
- The idea of stop & Wait protocol is straight Forward.
- After transmitting one frame, the sender waits for an

acknowledgement before transmitting the next Frame.

- Primitives of Stop & Wait protocols include :

SENDER SIDE :

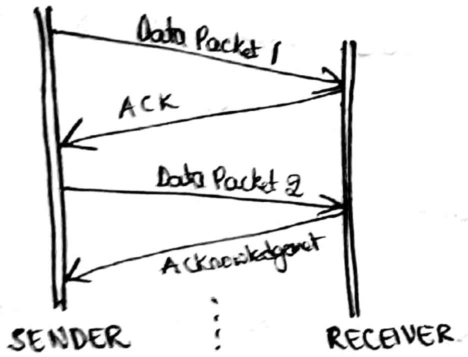
Rule 1 : Send one data packet at a time.

Rule 2 : Dont send next packet untill acknowledgement is received

RECEIVER SIDE :

Rule 1 : Receive & consume data packet

Rule 2 : Then Acknowledgement needs to be sent (Flow control).



Problems :

① Problems due to lost data:

- Sender waits for ack for an infinite amount of time.
- Receiver waits for data for an infinite time.

② Problems due to Lost ACK :

- Sender waits for ACK for infinite time.

③ Problems due to delayed ACK/data :

- After timeout on sender side, a delayed ACK might be wrongly considered as ACK of some other data packet.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- Sender waits for ACK for an infinite time ?

→ Introduce "time out" on sender side.

- Ack not received in given "time out" period ?

→ Give senders' packet a sequence #SN,
If receiver sends back Request number == #SN, as ACK
Then send next packet with sequence #SN + 1.
otherwise, Resend the packet having #SN to receiver.

For problem, & solution is :

- Sender doesnot wait for infinite amount of time. There is a timer set at the sender where when a frame is sent, if it doesnot receive ACK in given amount of time, it would send the same frame again.

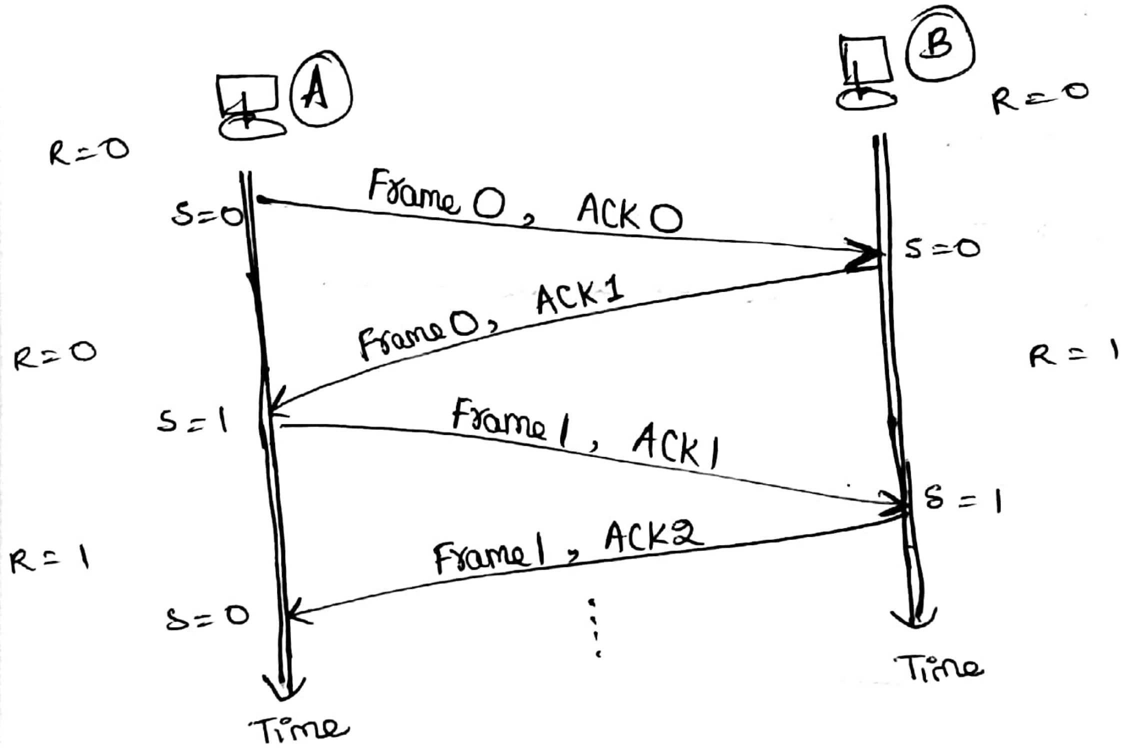
- Sometimes, Stop& Wait protocol doesnot have any problems as it is a noiseless channel protocol where no frames gets lost.

* <u>SIMPLEST PROTOCOL</u> :

- It has no flow or error control
- Data Frames are travelling in unidirection from sender to receiver.
- The data link layer of receiver immediately removes header from the frame & hands the data packet to its network layer.

*. PIGGY BACKING :

- A method to combine a dataframe with ACK.
- Here, station A & B both have data to send.
- Instead of sending seperately, station A sends a data frame that includes an ACK
- Station B also does the same thing.



~~• Error correction in Stop & Wait P~~

*. STOP & WAIT ARQ :

- If the acknowledgement doesnot arrive after a certain period of time, the sender times out and retransmit the original frame.

ARQ – Automatic Repeated reQuest protocol.

- $\boxed{\text{Stop \& Wait ARQ protocol} = \text{Stop \& Wait} + \text{Time out Timer} + \text{Sequence Number}}$ *IMP

GUDI VARAPRASAD - COMPUTER NETWORKS

*. SLIDING WINDOW PROTOCOL :

- Drawbacks of Stop & Wait ARQ Drawbacks Protocol :

→ one frame at a time

→ Poor utilization of bandwidth

→ Poor Performance.

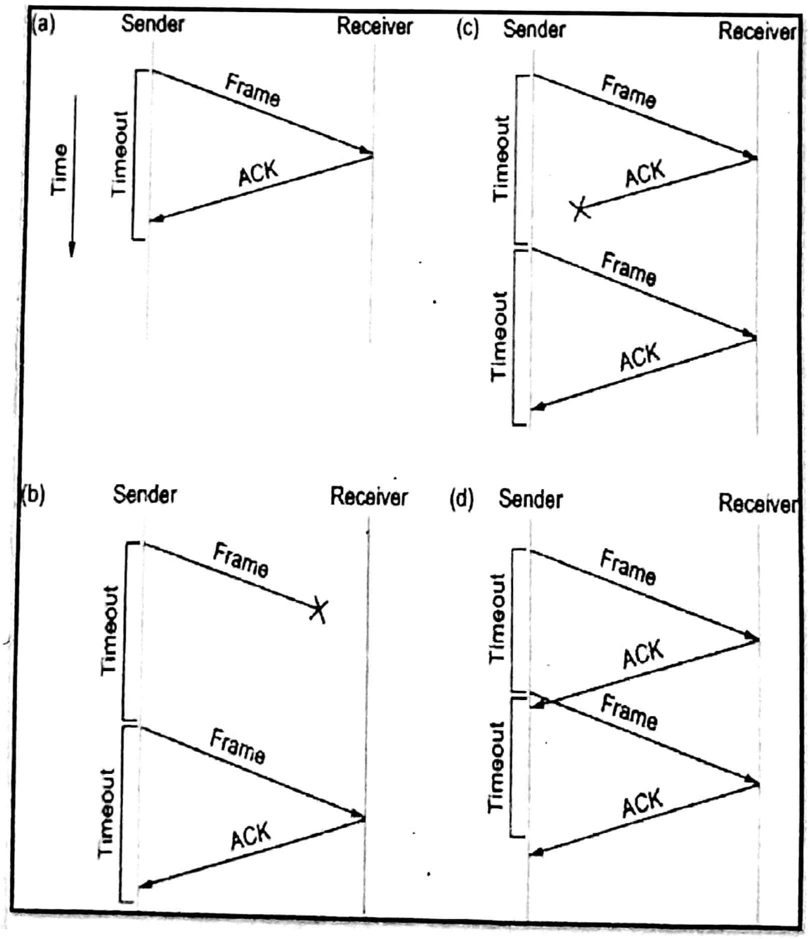
- Advantages of Sliding Window protocol :

→ Send multiple frames at a time.

→ No. of frames to be sent is based on Window size

→ Each frame is numbered → Sequence Number.

STOP & WAIT NRQ PROTOCOL



(a) The ACK is received before the timer expires

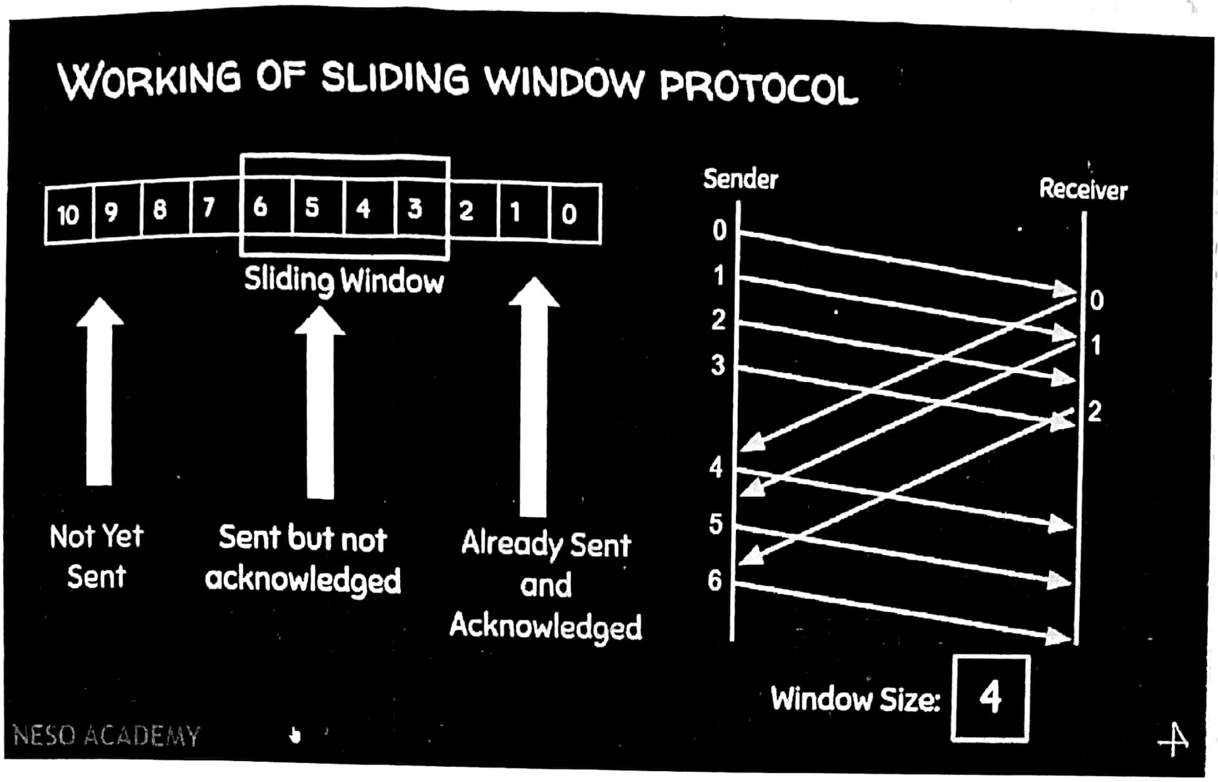
(b) The original frame is lost

(c) The ACK is lost

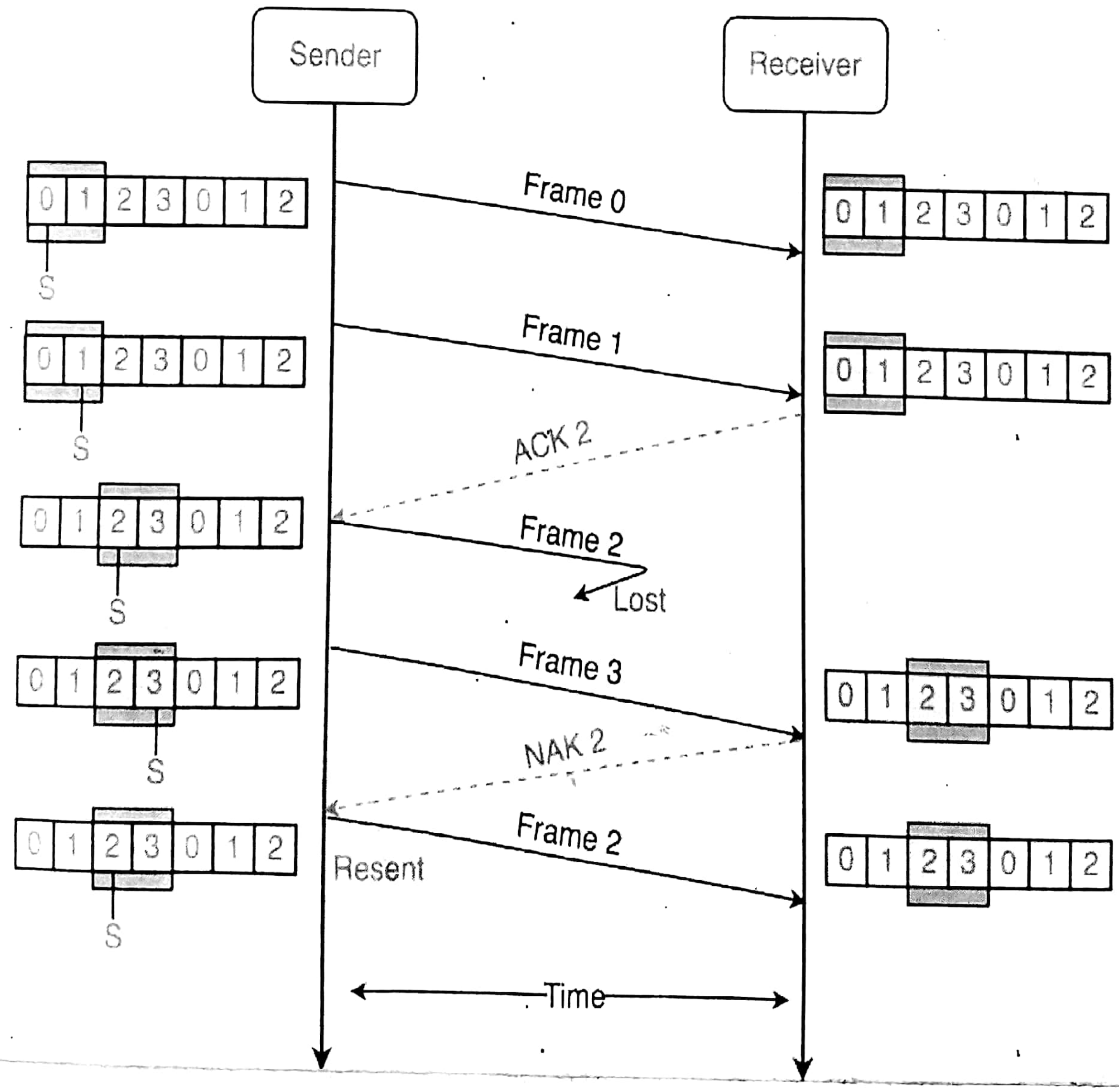
(d) The timeout fires too soon

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS



Sliding Window Protocol



GUDI VARAPRASAD - COMPUTER NETWORKS

*. GO BACK-N ARQ :

- A type of sliding Window protocol.
- N - is the sender window size, i.e. 'N' frames can be sent by sender to receiver before expecting an ACK
- Go-Back-N ARQ uses the concept of protocol pipelining i.e. the sender can send multiple frames before receiving the acknowledgement for the first time.
- There are Finite no. of frames & frames are numbered in sequential manner.
- The no. of frames that can be sent depends on the window size of the sender.

IMP
- If the acknowledgement of the frame is not received, within an agreed upon time period, all frames in current window are transmitted.
IMP

- THE size of sending window of determines the sequence no. of the outbound frames.
- Ex : N - Sender's Window size

If the sending window size is 4 (2^2), then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, ... and.

$2^{2} = 4$ → 00 = 0, 10 = 2, 01 = 1, 11 = 3

$2^{3} = 8$ → 000, 001, 010, 011, 100, 101, 110, 111 — 0 1, 3 4, 6 7

- The number of bits in sequence number is 2 to generate the binary sequence 00, 01, 10, 11

GUDI VARAPRASAD - COMPUTER NETWORKS

Problems on Go-Back-N ARQ Protocol :

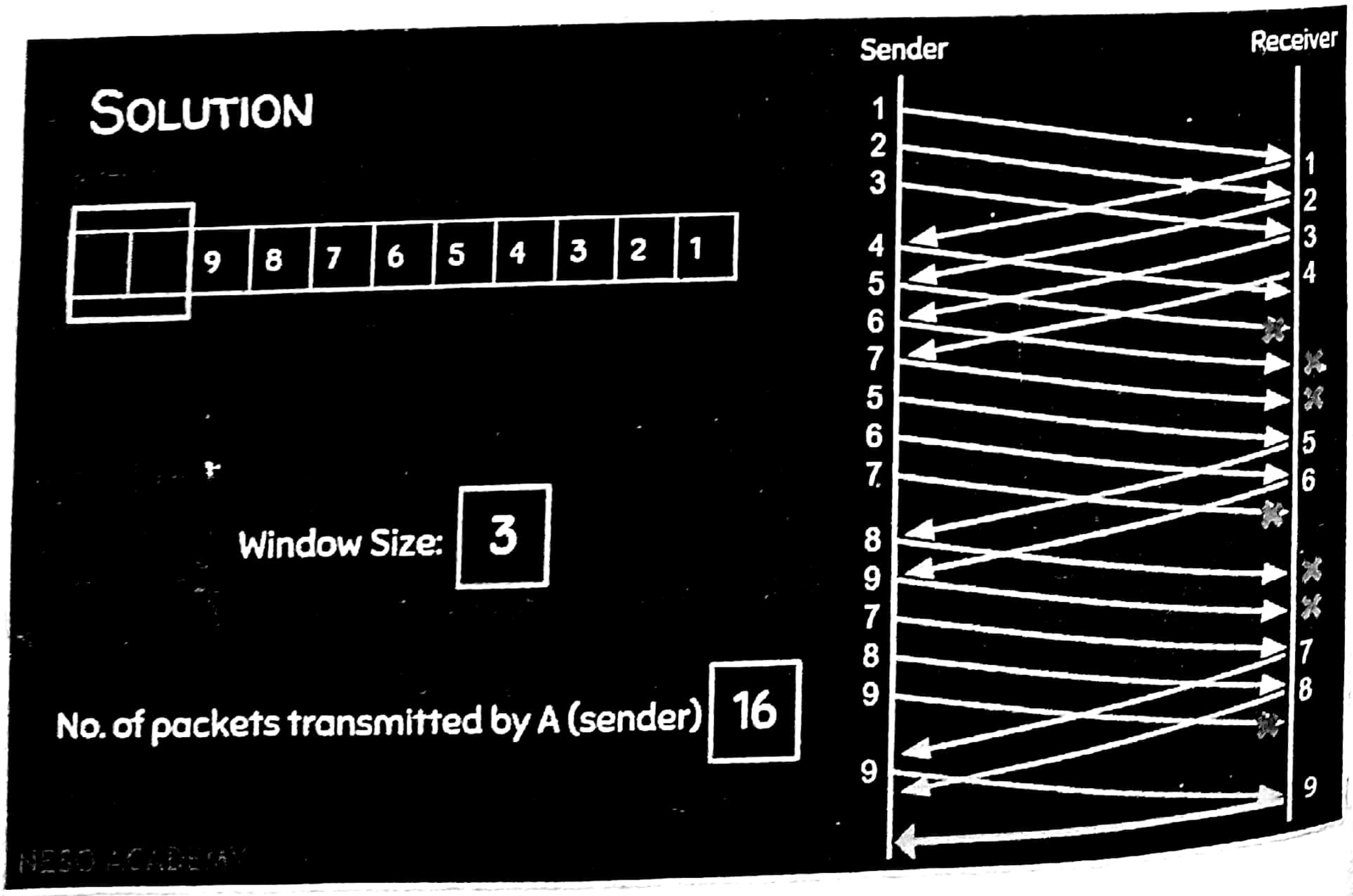
Question :

Station A needs to send a message consisting of 9 packets to station B using a sliding window (window size 3) and go back-N error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that A transmits gets lost (but no ACKs from B ever get lost), then what is the no. of packets that A will transmit for sending the message to B ? [GATE 2006]

Sol : $N = 3$

Frame size = 9 (9 packets)

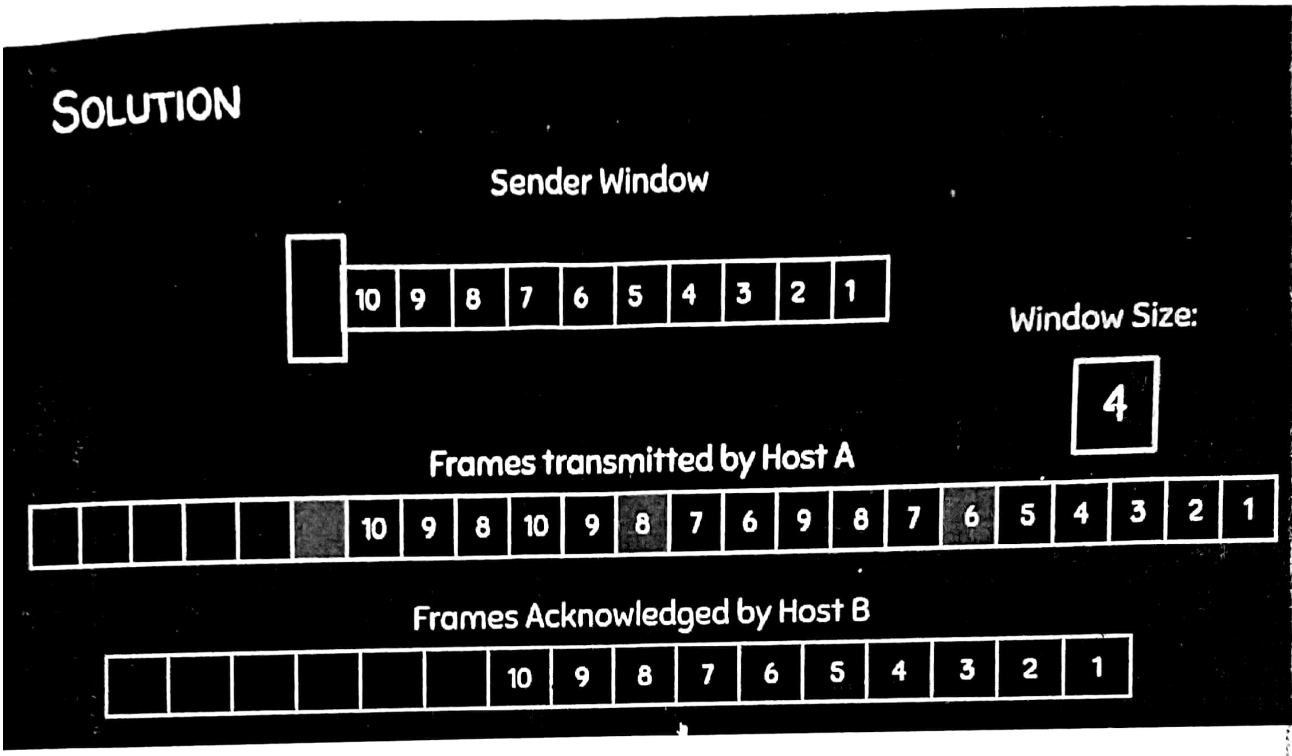
every 5th packet



GUDI VARAPRASAD - COMPUTER NETWORKS

Question :

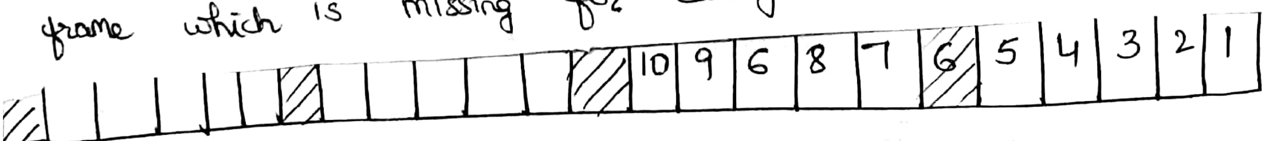
Host A wants to send 10 frames to Host B. The hosts agreed to go with Go-Back 4. How many no. of frames are transmitted by Host A if every 6th frame that is transmitted by host A is either corrupted or lost ?



Total Frames transmitted by A (sender) = 17

*. SELECT REPEAT ARQ :

- In selective Repeat ARQ, only the erroneous or lost frames are transmitted, while correct frames are received and buffered.
- The receiver will keep track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing for damaged.



No. of frames transmitted by Host A in SR ARQ = 11

GUDI VARAPRASAD - COMPUTER NETWORKS

*. Station A uses 32 byte packets to transmit message to station B using a sliding window protocol. The round trip delay between A and B is 80 ms. & the bottleneck bandwidth on the path between A and B is 128 kbps. What is the optimal window size that A should use ?

Sol :

Delay = 80 ms

Bandwidth = 128 Kbps

Packet size = 32 bytes

$$\boxed{\text{Bandwidth - Delay product} = \text{Bandwidth} \times \text{Delay}}$$ *

$= 128 \text{ Kbps} \times 80 \text{ ms} = 128 \times 1024 \times 80 \text{ ms}$

$= 128 \times 1024 \times 80 \times 10^{-3}$ bits

$= \dfrac{128 \times 1024 \times 80 \times 10^{-3}}{8}$ bytes

$$\boxed{\text{optimal Window Size} = \frac{\text{Bandwidth - Delay product}}{\text{Packet Size}}}$$ *

$= \dfrac{128 \times 1024 \times 80 \times 10^{-3}}{8 \times 32} = 40$

---

*. The distance between two stations M and N is L kilometers. All frames are K bits long. The propagation time per kilometer is t seconds. Let R bits/second be the channel capacity. Assuming the processing delay is negligible, the minimum no. of bits for the seq. no. field in a frame for maximum utilization, when

the sliding window protocol is used, is :

sol : Given,

distance = L km

frame size = k bits

propagation time = t sec

channel capacity = R bps

Min. no. of bits for seq. no. field = ?

$\boxed{\text{Propagation Delay} = \text{total distance} \times \text{propagation time}}$ *

$= L \cdot t$ sec

$\boxed{\text{Round Trip Time} = 2 \times \text{propagation Delay}}$ *

$= 2 \times Lt = 2Lt$ sec

No. of bits transmitted $= 2LtR$ bits

No. of frames $= \dfrac{2LtR}{K}$

In sliding window protocol, bits sequence no. = b

& No. of frames $= 2^b$

$\Rightarrow \quad 2^b = \dfrac{2LtR}{K} \quad \Rightarrow \quad \boxed{b = \log_2\left(\dfrac{2LtR}{K}\right)}$

GUDI VARAPRASAD - COMPUTER NETWORKS

CRUX :

- In the Go Back N protocol, the size of the sender window must be less than 2^m.
- The size of receiver window is always 1.

Ex : If $m = 2$, $\boxed{\text{window size} = 2^m - 1} = 3$

- Go Back N ARQ is inefficient, Many frames must be retransmitted in noisy link. It slow downs transmission & Consumes more Bandwidth.

Ex : IMP

Using 5-bit sequence numbers, what is the maximum size of send and receive windows for each of the following protocols ?

a. Stop & Wait ARQ
b. Go back N ARQ
c. Selective Repeat ARQ.

Sol :
m = seq num = 5

a. Stop & wait ARQ → Sender Window = 1 (1)
→ Receiver Window = 1 (1)

b. Go back N ARQ → Sender window = 31 $(2^m - 1)$
→ Receiver window = 1 (1)

c. Selective Repeat ARQ → Sender window = 16 $\left(\frac{2^m}{2}\right)$
→ Receiver window = 16 $\left(\frac{2^m}{2}\right)$

$2^m - 1$ → Sender window in Go back N ARQ

$\frac{2^m}{2}$ → Sender & Receiver window in SR ARQ

Remaining all cases 1 -

GUDI VARAPRASAD - COMPUTER NETWORKS

Useful Terms :

- Propagation Delay = (Distance between Routers) / (Velocity of propagation)

- Round Trip Time = 2 × propagation Delay

- Time out = 2 × Round Trip Time

- Time to Live = 2 × Time out (Max TTL = 180 sec)

- Total time = (Transmission delay for Data Packet) + 2 × (Propagation delay for data or ACK)

- Efficiency (η) = $\dfrac{\text{Useful Time}}{\text{Total time cycle}} = \dfrac{1}{1 + 2 \times \left(\dfrac{\text{propagation delay}}{\text{Transmission delay}}\right)}$

- Throughput = Efficiency (η) × Bandwidth

- Also, Efficiency (Factors affecting) $\eta = \dfrac{1}{1 + 2 \times \left(\dfrac{\text{distance between}}{\text{velocity}}\right)} \times \dfrac{\text{Bandwidth}}{\text{size of Data Pack}}$

Ex :
If the bandwidth of line is 1.5 Mbps, RTT is 45 m sec and packet size is 1 KB, then find the efficiency in stop & wait.

Sol :

Given :

Bandwidth = 1.5 Mbps

RTT = 45 m sec

packet size = 1 KB

GUDI VARAPRASAD - COMPUTER NETWORKS

For Transmission Delay,

$$\text{Transmission Delay} = \frac{\text{Packet size}}{\text{Bandwidth}}$$

$$= \frac{1\ KB}{1.5\ Mbps} = \frac{2^{10} \times 8 \text{ bits}}{1.5 \times 10^{6} \text{ bits ps}} = 5.461 \text{ m sec}$$

Calculating Propagation Delay,

$$\text{Propagation Delay} = \frac{\text{Round Trip Time}}{2}$$

$$= \frac{45 \text{ m sec}}{2} = 22.5 \text{ m sec}$$

For ratio, a

$$\boxed{a = \frac{T_p}{T_t}} = \frac{\text{Propagation delay}}{\text{Transmission delay}} = \frac{22.5 \text{ m sec}}{5.461 \text{ m sec}} = 4.12$$

Link utilization or Efficiency, (η)

$$\boxed{\eta = \frac{1}{1+2a}} = \frac{1}{1+(2 \times 4.12)} = 0.108 = 10.8\ \%$$

Ex :

A channel has a bit rate of 4 Kbps and one way propagation delay of 20 m sec. The channel uses stop & wait protocol. The transmission time of acknowledgement frame is negligible, To get channel efficiency of atleast 50 %, what is minimum frame size ?

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

Sol : Given,

Bandwidth = 4 Kbps

Propagation delay (T_p) = 20 m sec

Efficiency $(\eta) >= 50\%$

Let the required frame size = L bits

For Transmission Delay,

Transmission delay $(T_t) = \dfrac{\text{Packet size}}{\text{Bandwidth}}$

$$= \frac{L \text{ bits}}{4 \text{ Kbps}} = \frac{L}{4} \times 10^{-3} \text{ sec}$$

Condition for efficiency to be atleast 50%

HINT

★ For efficiency to be atleast 50%,

$$\boxed{\frac{1}{1+2a} >= \frac{1}{2}}$$

also, $\boxed{a <= \frac{1}{2}}$ ★

$$a = \frac{\text{Propagation delay}}{\text{Transmission delay}}$$

$$a = \frac{20 \text{ msec}}{\left(\frac{L}{4} \times 10^{-3}\right) \text{sec}} = \frac{20 \times 10^{-3} \text{ sec}}{\left(\frac{L}{4}\right) \times 10^{-3} \text{ sec}} = \frac{80}{L}$$

$$\frac{80}{L} <= \frac{1}{2} \quad \text{(condition)}$$

$$\Rightarrow \quad L >= 160$$

∴ Frame size must be atleast 160 bits

GUDI VARAPRASAD - COMPUTER NETWORKS

Note : Assume

$T_t = 1\ ms$, $T_p = 2\ ms$, Bandwidth = 6 Mbps

Efficiency , $\eta = \dfrac{1}{1+2a}$, $a = \dfrac{T_p}{T_t}$

$a = \dfrac{2}{1} = 2\ ms$

$\eta = \dfrac{1}{1+2a} = \dfrac{1}{1+2(2)} = 1/5 = 20\%$ efficiency

Throughput $= \eta \times$ Bandwidth

$= 1/5 \times 6 = \underline{1.2\ Mbps}$

---

*. ETHERNET BASICS :

- Topologies – Linear bus , Star bus
- Signaling – Mainly baseband (digital)
- Access methods – CSMA/CD
- Specifications – IEEE 802.3
- Transfer speed – 10 Mbps, 100 Mbps , or above
- Cable types – Coaxial Cables , UTP .
- It is one of the most widely used Wired LAN Technologies.
- operates in Data Link layer and the physical Layer.
- Ethernet Evolution →
  - Standard Ethernet ~ 10 Mbps
  - Fast Ethernet ~ 100 Mbps
  - Gigabit Ethernet ~ 1 Gbps
  - 10 Gigabit Ethernet ~ 10 Gbps

*. Ethernet Frame :

Minimum payload length = 46 bytes.

Maximum payload length = 1500 bytes.

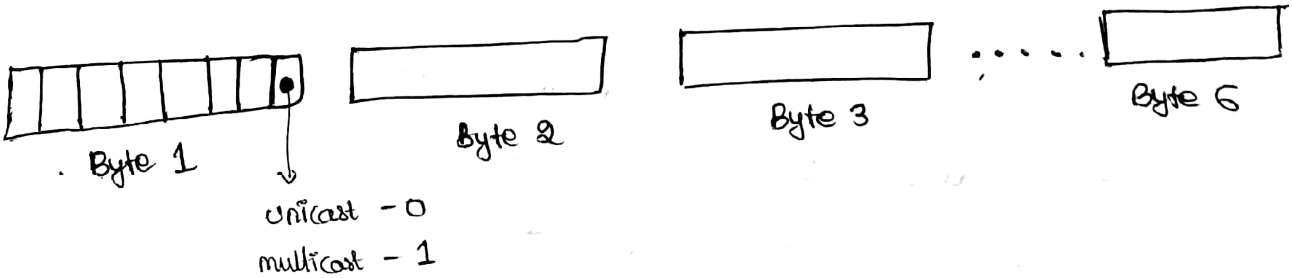
Maximum frame length = 12,144 bits or 1518 bytes.

Minimum ~~paylon~~ frame length = 512 bits or 64 bytes.

*. Ethernet Address – MAC Address

Ex : 06 : 01 : 02 : 01 : 2C : 4B

~ 6 bytes ⟺ 12 hex digits ⟺ 48 bits



- The least significant bit of the first byte defines the type of address. → source address
- If the bit is 0, the address is unicast, otherwise, it is multicast. → destination address
- If all bits are 1 ⇒ then it is broadcast address.

Ex :

What is the hexadecimal equivalent of the following Ethernet address ?

0101 1010	0001 0001	0101 0101	0001 1000	1010 1010	0000 1111
5 A	1 1	5 5	1 8	A A	0 F

5A : 11 : 55 : 18 : AA : 0F → Answer

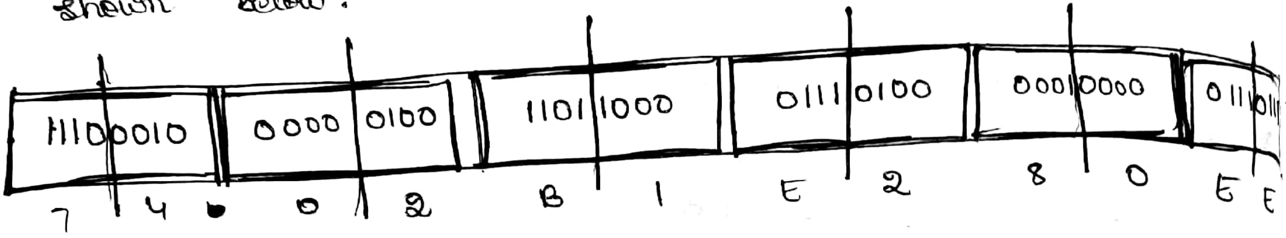
GUDI VARAPRASAD - COMPUTER NETWORKS

Ex :

Show how the address 47 : 20 : 1B : 2E : 08 : EE is sent out on line.

Sol :

The address is sent left to right, byte by byte; for each byte, it is sent right to left, bit by bit, as shown below.



Ex :

Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10,000 bits. Assume the signal speed in the cable to be 2,00,000 km/s.

Sol :

Bandwidth = 500 Mbps

Rate Size = 10^4 bits

Signal speed = 2×10^5 km/sec

Transmission time $\geq$ 2 × propagation time

$$\frac{\text{Message size}}{\text{Bandwidth}} \geq 2 \times \frac{\text{Length}}{\text{Propagation speed}}$$

$$\frac{10^4 \text{ bits}}{500 \text{ Mbps}} \geq \frac{2 \times \text{length}}{2 \times 10^5 \text{ km/sec}}$$

Length $\leq$ 2 Km $\Longrightarrow$ Max. length = 2 Km

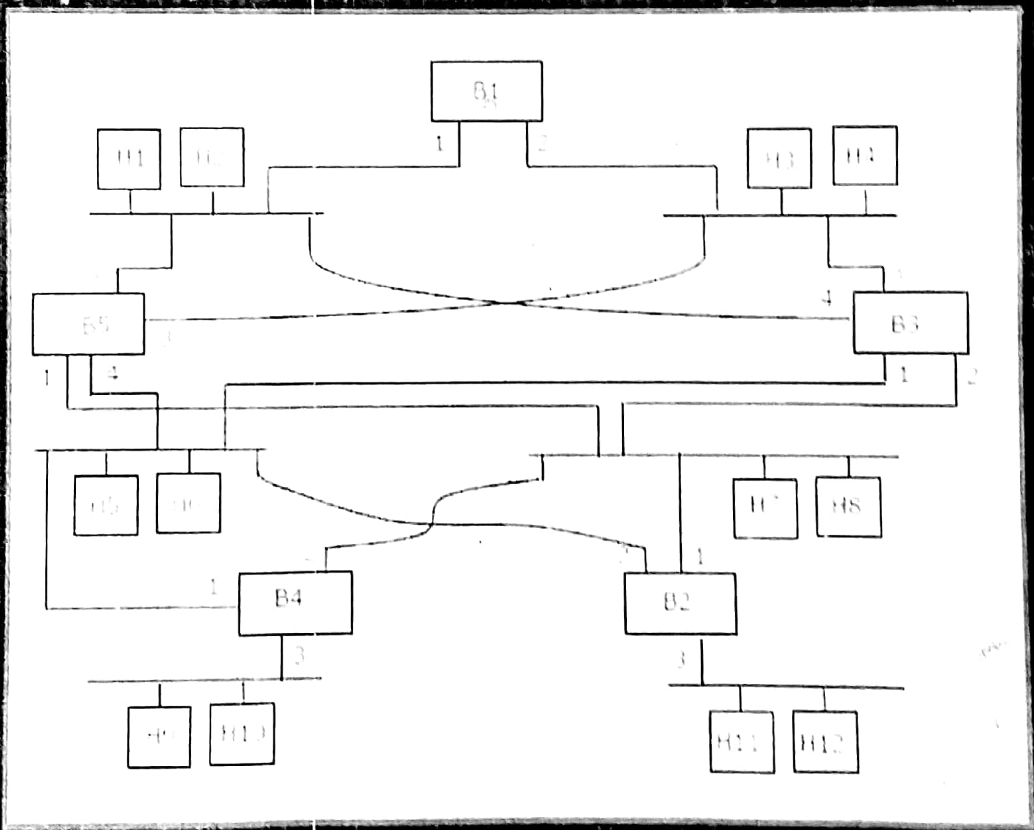
GUDI VARAPRASAD - COMPUTER NETWORKS

* SPANNING TREE PROTOCOL :

QUESTION

Consider the diagram shown below where a number of LANs are connected by (transparent) bridges. In order to avoid packets looping through circuits in the graph, the bridges organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root sends out (one or more) data units to enable the setting up of the spanning tree of shortest paths from the root bridge to each bridge.

Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflicts are always resolved in favour of the port with the lower index value. When there is a possibility of multiple bridges forwarding to the same LAN (but not through the root port), ties are broken as follows: bridges closest to the root get preference and between such bridges, the one with the lowest serial number is preferred.



For the given connection of LANs by bridges, which one of the following choices represents the depth first traversal of the spanning tree of bridges?

[GATE CS 2006]

(A) B1, B5, B3, B4, B2

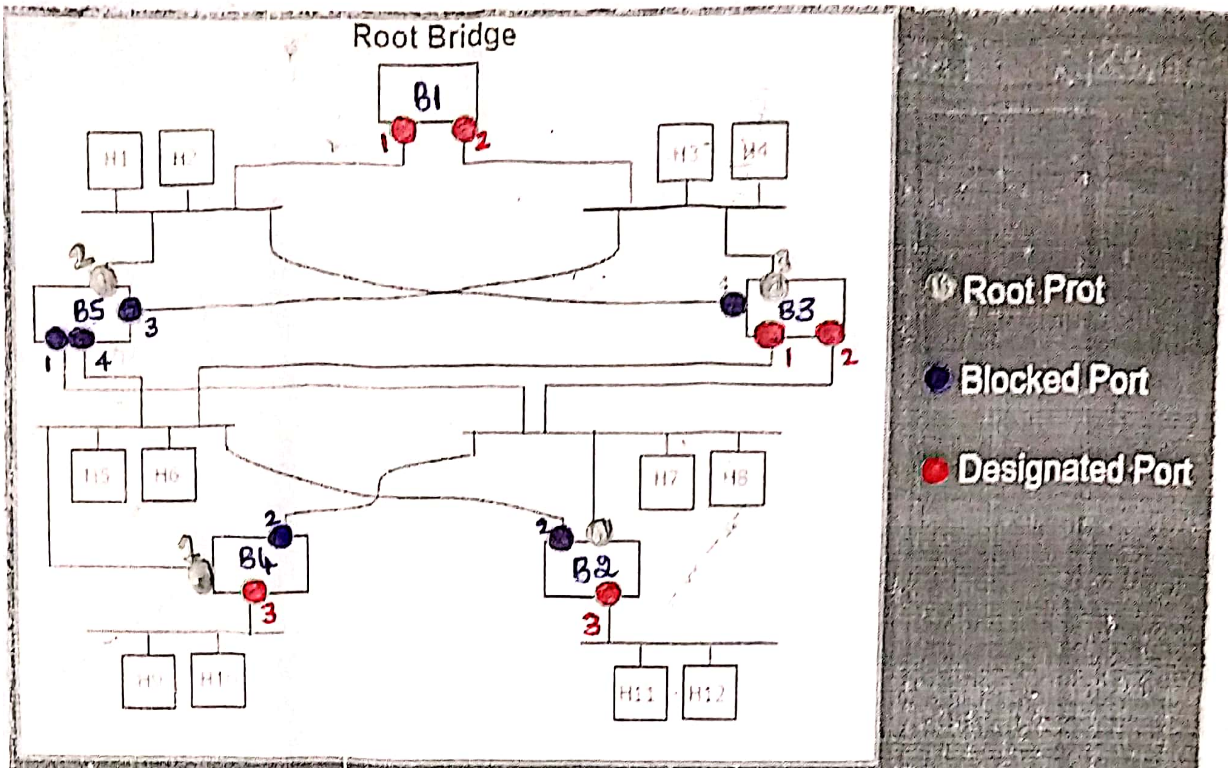
(B) B1, B3, B5, B2, B4

(C) B1, B5, B2, B3, B4

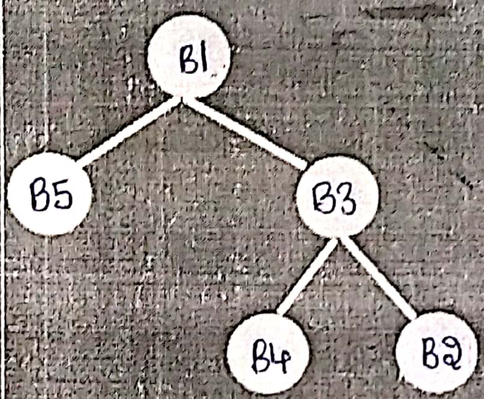
(D) B1, B3, B4, B5, B2

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS



SOLUTION



B4 and B2 are connected through B3 (Not B5) because B3 has lower serial number than B5.

One DFS traversal of tree is: B1 – B5 – B3 – B4 – B2

Missed concepts :

- 802.3 – Media Access Control
- 802.5 – Token Ring Standard.
- 802.11 – Wireless Fidelity , IEEE Distributed System .
- Reliable Transmission .
- ATM .
- Multiple Access Protocols .
- Controlled Access Protocols .

GUDI VARAPRASAD - COMPUTER NETWORKS

MODULE - 4 : NETWORK LAYER

Network layer role :

- Source to Destination delivery. (different networks)
- Performed by using logical address (IP address)
- IP address = Network ID + Host address
- Routing (RIP, OSP protocols).
- Routers are used deliver / communicate.
- Fragmentation - divide the packets inorder to avoid congesion.

*. Class A in IP addressing :

- Dotted Decimal representation - IP address
- No. of IP address = 2^{31} (total 32 bits)
- By default MSB is 0. → represents Network ID (First 8 bits)
- Remaining 24 bits → No. of users inside this network
- No. of Networks in class A = $2^7 = 128$
  - → null address 0.0.0.0
  - → loop back 127.0.0.0
- Used IP address = $128 - 2 = 126$
- No. of Hosts Possible in every network = $2^{24} - 2$
- Class A → $x.0.0.0$ ~ network address
  - ⋮ → hosts
  - → $x.255.255.255$ ~ broadcast (directed) address

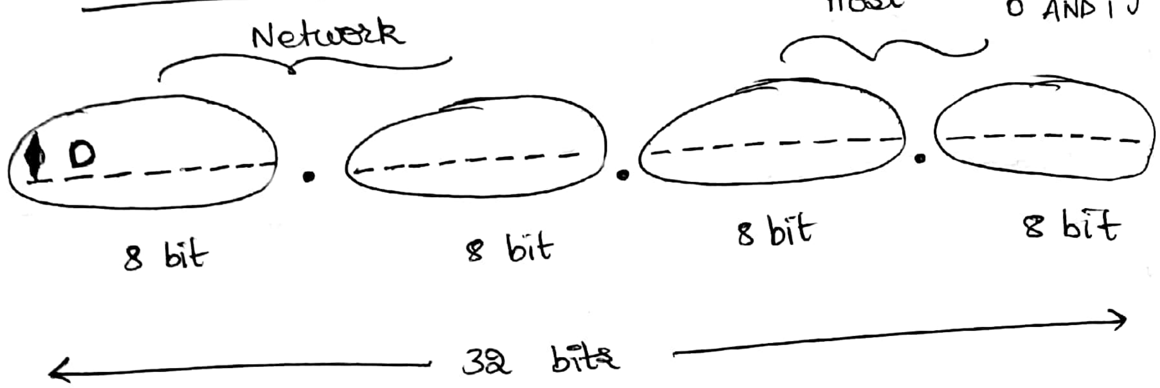
$x \in [0, 127]$

GUDI VARAPRASAD - COMPUTER NETWORKS

- Default Mask helps to extract network ID.
- Default Mask of class A = 255.0.0.0
- Network ID = $\underbrace{\underset{\text{binary}}{(\text{Given IP})}\ \text{AND}\ \underset{\text{binary}}{(\text{Default Mask})}}_{\text{each bit}}$

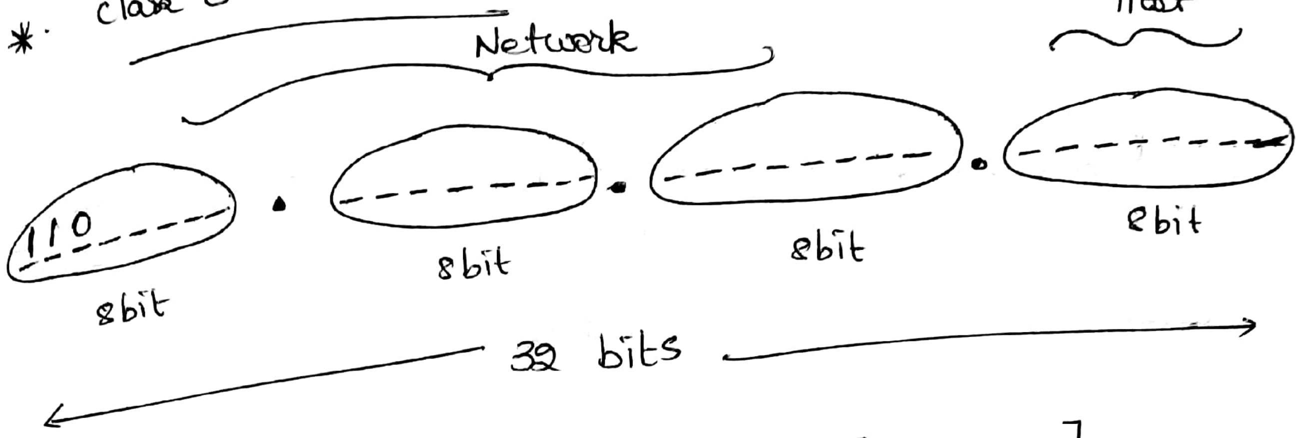
1 AND 1 = 1
1 AND 0
0 AND 0
0 AND 1 } = 0

✱ CLASS B IP Addressing :

- 

- Range = 128 to 191 , $x \in [128, 191]$
- No. of IP Addresses = 2^{30} ($\approx$ 25% of total)
- No. of Networks = $2^{14} \sim 16384$ $\left\{ \begin{array}{l} 64 \times 256 \\ 2^6 \times 2^8 \end{array} = 2^{14} \right\}$
- No. of Hosts in each Network = $2^{16} \sim 65536$
- No. of used Hosts = $2^{16} - 2$ = 65534
- 128.0.0.0 → Network
  ⋮ → Host
  128.0.255.255 → Broadcasting
  Class B, $x \in [128, 191]$
- Default Mask of class B = 255.255.0.0
- Network ID = $\underset{\text{binary}}{(\text{Given IP})}$ AND $\underset{\text{binary}}{(\text{default Mask})}$

* Class C IP Addressing :



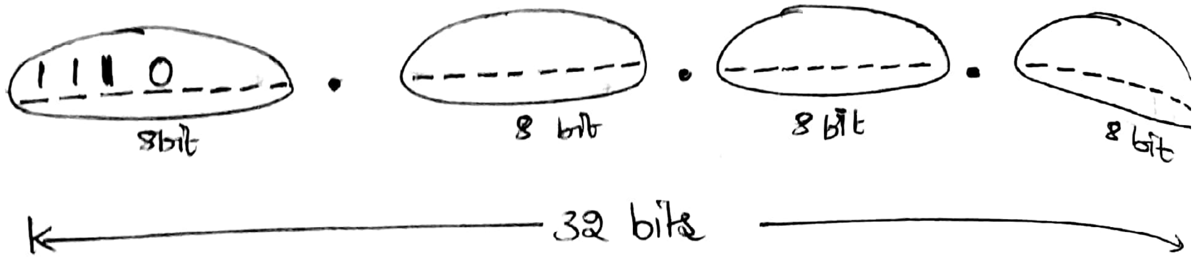
- Range = 192 to 223 , $x \in [192, 223]$
- No. of IP address = 2^{29} ($\approx$ 12.5% of total)
- No. of Networks = 2^{21} $\left\{ \begin{matrix} 32 \times 256 \times 256 \\ 2^5 \times 2^8 \times 2^8 \end{matrix} = 2^{21} \right\}$
- No. of Hosts in each Network = $2^8 = 256$
- No. of used hosts = $2^8 - 2 = 254$
- class C → x.0.0.0 → Network
  ⋮ → Host
  → x.0.0.255 → Broadcasting

  $x \in [192, 223]$
- Default Mask of class C = 255.255.255.0

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

* Class D IP Addressing :



- Range = 224 to 239.
- No. of IP Address = 2^{28}.
- Reserved for Multicasting, Group Email/ Broadcast.

No Networks
No hosts
Not used

* Class E IP Addressing :

- Reserved for ~~Multi~~ Military Purpose / Sensitive Groups.

- Range = 240 to 255
- No. of IP Address = 2^{28}
- No Hosts, Not used, No Networks.

GUDI VARAPRASAD - COMPUTER NETWORKS

<u>question</u> : Given IP Address = 201.20.30.40

Find Network ID, 4th Host ID, Last Host ID, Broadcast Address.

<u>sol</u>: IP Address = 201.20.30.40

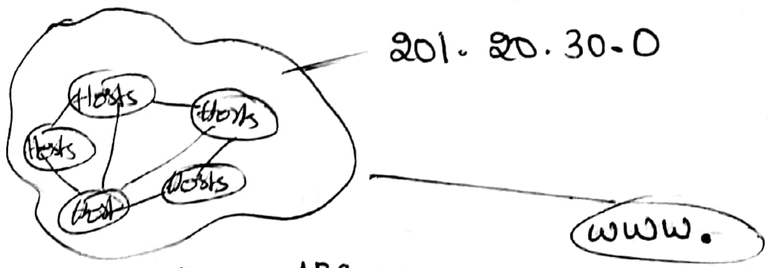
Class C Range = 192 to 223

1st octect (8 bits) = 201 ✓ $\boxed{\text{Class C}}$

Default Mask of class C = 255.255.255.0

$$
\begin{array}{r}
201.20.30.40 \\
255.255.255.0 \\
\hline
201.20.30.0
\end{array}
\quad (AND)
$$

- 201.20.30.0 ⟶ Network ID



organization ABC.com

1st Host ID = 201.20.30.1

- 4th Host ID = 201.20.30.4
- last Host ID = 201.20.30.254
- Broadcast Address = 201.20.30.255

Limited (within same) – 255.255.255.255.

direct (another outside network) – 201.20.30.255

* Problems with classful Addressing :

- Wastage of IP Addresses.
- Maintenance is time consuming.
- More prones to errors.
- Flexibility of IP. ⟶ solved by (classless)
- Not secured (security Problems)

---

*. CLASSLESS ADDRESSING : (CIDR)

- No concept of class / only Blocks
- Fullfill of user demand without extra, waste.
- ⟵ 32 bit ⟶

Block ID	Host ID

- Notation : x.y.z.w/n where { n - no. of bits represent block/network; n - mask (1111's) }

e.g., 200.10.20.40/28

28 → mask (28 1's - Block ID)

28	4
Block bits	Host bits

- No. of Hosts = $2^4 = 16$
- ~~Network ID~~ Mask of Network = 255.255.255.240

mask = 28

11111111.11111111.11111111.11110000

255   255   255   240

GUDI VARAPRASAD - COMPUTER NETWORKS

200 . 10 . 20 . 40 / 28 → Given

↓

200 . 10 . 20 . 00101000

8bit 8bit 8bit 4bit

28 bit → block ID (no change) (same)

⇓

200 . 10 . 20 . 00100000

$\boxed{200 . 10 . 20 . 32/28}$ → Network IP address
Block ID or Network ID

[OR]

255 . 255 . 255 . 240	=	Mask (AND)
200 . 10 . 20 . 40	=	Given IP
200 . 10 . 20 . 32/28	=	after AND operation

- **Rules** :

1. Address should be contiguous
2. No of Address in block must be in power of 2.
3. First address of every block must be evenly divisible by (with) size of block.

200 . 10 . 20 . 32 /28 → Network ID

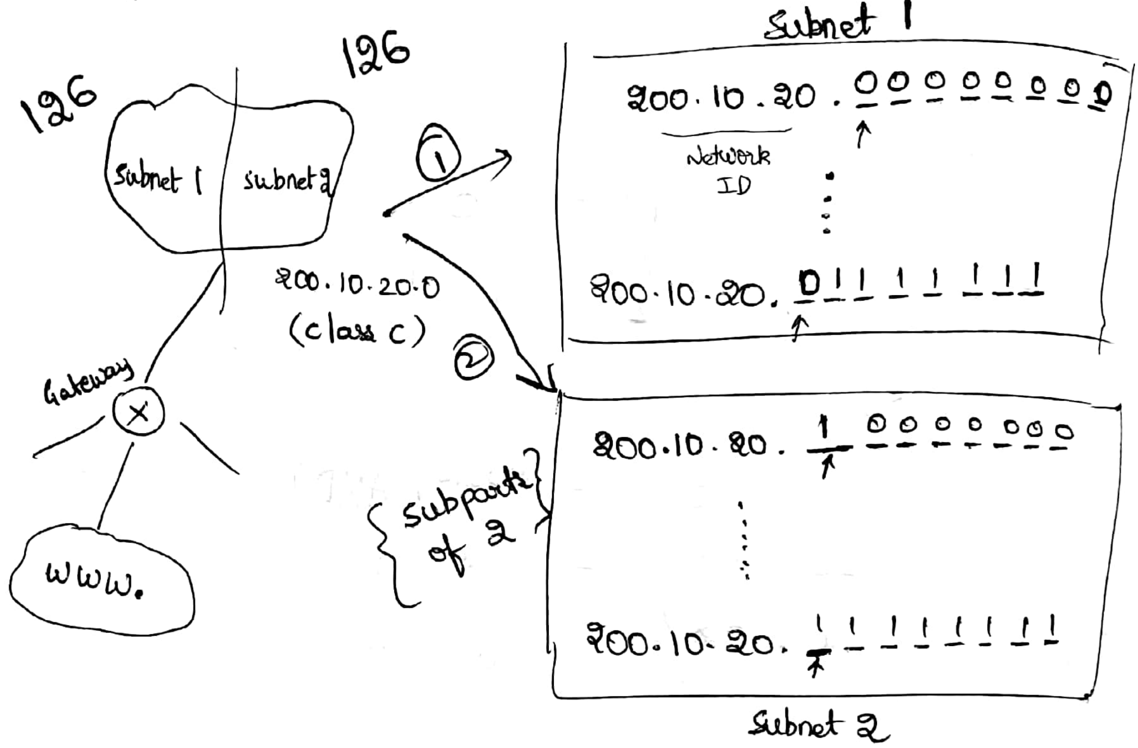
⋮ → Hosts

200 . 10 . 20 . 47 / 28 → Broadcasting Address

GUDI VARAPRASAD - COMPUTER NETWORKS

*. SUBNETTING in Classful Addressing :

- Dividing the big network into small networks.



Subnet 1 :

IP : 200.10.20.0 to 200.10.20.127

Broadcast : 200.10.20.127

Network : 200.10.20.0

Hosts total = 128 (but usable Hosts = 128 - 2 = 126)

Subnet 2 :

IP : 200.10.20.128 to 200.10.20.255

Broadcast : 200.10.20.255

Network : 200.10.20.128

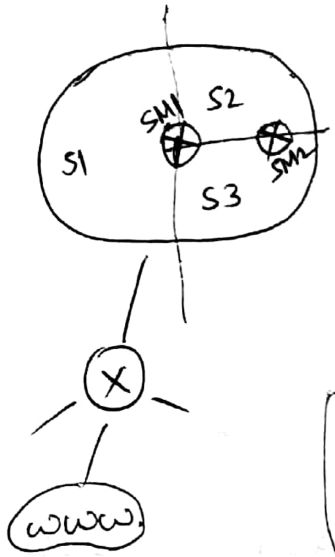
Hosts total = 128 (but usable Hosts = 128 - 2 = 126)

$\boxed{\text{SUBNET MASK : 255.255.255.128}}$

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*. VARIABLE LENGTH SUBNET MASKING : (VLSM)



S1: 200.10.20.0 0 0 0 0 0 0 0
⋮
200.10.20.0 1 1 1 1 1 1 1

Subnet 1

Subnet 2

S2: 200.10.20.1 0 0 0 0 0 0 0
⋮
200.10.20.1 0 1 1 1 1 1 1

S3: 200.10.20.1 1 0 0 0 0 0 0
⋮
200.10.20.1 1 1 1 1 1 1 1

Subnet 3

Subnet 1 (S1)	Subnet 2 (S2)	Subnet 3 (S3)
200.10.20.0 to 200.10.20.127 } IP	200.10.20.128 to 200.10.20.191 } IP	200.10.20.192 to 200.10.20.255 } IP
Hosts Usable = 126	Hosts Usable = 62	Hosts usable = 62
Usable IP total = 250	Subnet Mask = 255.255.255.128	SM2
SM1	Subnet Mask = 255.255.255.192	

*. SUBNETTING IN CLASSLESS INTERDOMAIN ROUTING :

- Denoted using | (slash) in IP addresses.

e.g.,   195.10.20.128/26

Network ID bits = 26 bits

Host ID bits = 32 − 26 = 6 bits

$195.10.20.128/26 \Rightarrow \underbrace{195.10.20.10}_{\substack{26\text{ bits}\\ \text{NID}}}\underbrace{000000}_{\text{Host}}$

Total hosts = $2^6 = 64$

Used hosts = 64 − 2 = 62

Now subnetting,

Subnet 1 (32)

195.10.20.10 0 0 0 0 0 0 ~ 195.10.20.128/27

⋮

195.10.20.10 0 1 1 1 1 1 ~ 195.10.20.159/27

Subnet 2 (32)

195.10.20.10 1 0 0 0 0 0 ~ 195.10.20.160/27

⋮

195.10.20.10 1 1 1 1 1 1 ~ 195.10.20.191/27

Fixed bits = $\underset{\text{NID}}{26} + \underset{\text{Subnet bit}}{1} = 27$

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

GATE

* Classless interdomain routing (CIDR) receive a packet with address 131.23.151.76. The Router's routing table has following entities:

Prefix	output Interface
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

Packet will be forwarded to which interface?

~~3~~ 1

Sol:

Given 131.23.151.76 = destination IP

1st

131.23.151.76 → 131 . 00010111 . 151 . 76
131.16.0.0/12 → 131 . 11110000 . 0 . 0 (AND)

131.16.0.0 ⇐ 131. 00010000 . 0 . 0

↓

Matched with given prefix ✓ (this is the interface with 3)

2nd

131.23.151.76 → 131. 00010111 . 151 . 76
131.28.0.0 → 131. 11111100 . 0 . 0 (AND)

131. 00010100 . 0 . 0

≠ 131. 20.0.0 ⇐

⇓

Not matched with prefix 131.28.0.0 ✗

4th

131.23.151.76 → 131. 00010111 . 151 . 76
131.22.0.0 → 131. 11111110 . 0 . 0 (AND)

131. 00010110. 0 . 0

= 131.22.0.0 ⇐

⇓

Matched with prefix

Matched with prefix → 131.16.0.0/12 ~ 3

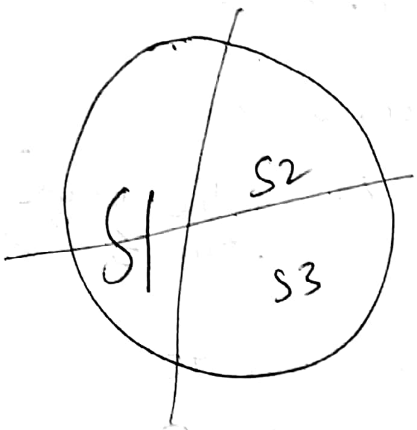
→ 131.22.0.0/15 ~ 1

IMP ★ IMP Where the /? in prefix is bigger, the routing table of router selects that.

$/15 > /12 \Rightarrow$ Interface 1 is selected

∴ Packet is delivered to interface 1

✱. Variable Length Subnet Masking in CIDR :



245.248.128.0/20

NID = 20

HID = 32 − 20 = 12

Hosts total = 2^{12}

Used Hosts = $2^{12} - 2$

$\underbrace{245.248.1000}_{\substack{\text{Network} \\ \text{NID bits} \\ 20}}|\underbrace{0000.00000000}_{\substack{\text{Host HID bits} \\ 12}}$

245.248.1000 0 | 0 0 0 . 0 0 0 0 0 0 0 0

245.248.1000 0 | 1 1 1 . 1 1 1 1 1 1 1 1

} S1

i.e. 245.248.128.0/21 to 245.248.135.255/21

GUDI VARAPRASAD - COMPUTER NETWORKS

Subnet 2 (S2) :

245.248. 1000 1 0 | 0 0 . 0 0 0 0 0 0 0 0

⋮

245.248. 1000 1 0 | 1 1 . 1 1 1 1 1 1 1 1

i.e. S2 $\boxed{245.248.136.0/22 \text{ to } 245.248.139.255/22}$

Subnet 3 (S3) :

245.248. 1000 1 1 | 0 0 . 0 0 0 0 0 0 0 0

⋮

245.248. 1000 1 1 | 1 1 . 1 1 1 1 1 1 1 1

i.e. S3 $\boxed{245.248.140.0/22 \text{ to } 245.248.143.255/22}$

---

* IPV4 HEADER :

- Connectionless less – Datagram Service
- Datagram ← Header size = 20 – 60 Bytes

  Datagram ← Payload (our Msg) = 0 – 65515 Bytes

  2^{16}

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

IPV4 → 0100

multiply by 4

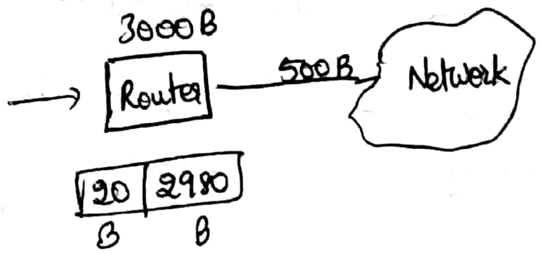
VER $\boxed{4 \text{ bits}}$	HLEN $\boxed{4 \text{ bits}}$	Type of Service (DSCP) $\boxed{8 \text{ bits}}$	Total Length $\boxed{16 \text{ bits}}$	
Identification bits $\boxed{16 \text{ bits}}$			Flag $\boxed{3 \text{ bits}}$	Fragment offset $\boxed{13 \text{ bits}}$
Time to LIVE TTL $\boxed{8 \text{ bits}}$	Protocol $\boxed{8 \text{ bits}}$		Header checksum $\boxed{8 \text{ bits}}$	
Source IP Address $\boxed{32 \text{ bits}}$				
Destination IP Address $\boxed{32 \text{ bits}}$				
options & Padding				

Total Size = 160 bits = 20 Bytes

*. Fragmentation in IPV4 :

Ex : A datagram of 3000 B (20B of IP Header + 2980 B of IP Payload) reached at Router and must be forward to link with MTU of 500 B. How many fragments will be generated and also write MF, offset, Total length value of all.

Sol :



Header Payload

500 ⟶ 20 + 480

$$\left\lceil \frac{2980}{480} \right\rceil \overset{\text{ceiling value}}{=} 7$$

P7	P6	P5	P4	P3	P2	P1
100 +20	480 + 20	480 + 20	480 + 20	480 + 20	480 + 20	480 + 20

Total length of P1 to P6 = 500B each

Total Length of P7 = 120 B

MF →	0	1	1	1	1	1	1
	P7	P6	P5	P4	P3	P2	P1
	P7	P6	P5	P4	P3	P2	P1
offset →	360	300	240	180	120	60	0

+ + + + + adds 60 to previous

$\frac{480}{8} = 60$ fixed division.

*. IPV6 Header :

0110

Version (4)	Priority (8)	Flow Level (20)
Payload length (16)	Next Header (8)	HOP Limit (8)
Source Address (128)		
Destination Address (128)		

Base Header = 40 Bytes (320 bits) = Fixed

Extension Headers :

1. Routing Header (43)
2. Hop by Hop option (0)
3. Fragment Header (44)
4. Authentication Header (51)
5. Destination options (60)
6. Encapsulating security Payload (50)

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

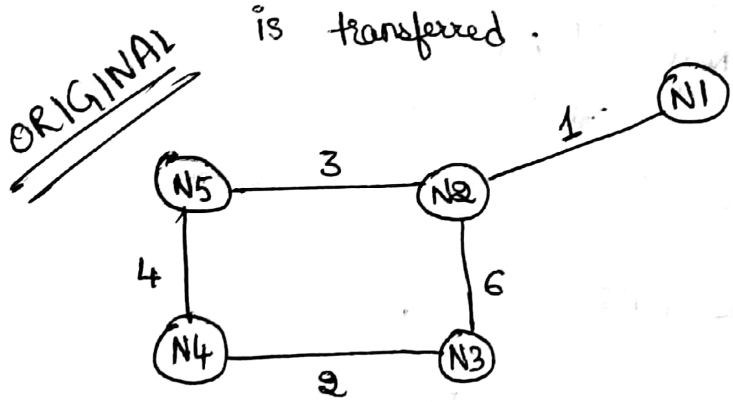
*. ROUTING PROTOCOLS :

- Routing Protocols
  - Intra Domain
    - Distance Vector (RIP) — IMP ***
    - Link state (OSPF)
  - Interdomain
    - Path Vector (BGP)

Dynamic updating of Routing table & optimal sharing of data.

*. DISTANCE VECTOR ROUTING :

Ex : Consider A Network & following routers N1, N2, N3, N4, N5 & respective distances. A packet is transferred.



N1 Local Routing Table

Destination	Distance	Next
N1	0	N1
N2	1	N2
N3	∞	–
N4	∞	–
N5	∞	–

N2 Local Routing Table

Destination	Distance	Next
N1	1	N1
N2	0	N2
N3	6	N3
N4	∞	—
N5	3	N5

GUDI VARAPRASAD - COMPUTER NETWORKS

N3 Routing Table

Dest.	Dist.	Next
N1	∞	–
N2	6	N2
N3	0	N3
N4	2	N4
N5	∞	–

N4 Routing Table

Dest	Dist	Next
N1	∞	–
N2	∞	–
N3	2	N3
N4	0	N4
N5	4	N5

N5 R. Table

Dest	Dist	Next
N1	∞	–
N2	3	N2
N3	∞	–
N4	4	N4
N5	0	N5

- only Neighbour - sharing to
- only Distance vector - shares only

At N1 : N2

At N2 : N1, N3, N5

At N3 : N4, N2

At N4 : N3, N5

At N5 : N2, N4

After (1) instance

At N1 : N2 $\boxed{1 \quad 0 \quad 6 \quad \infty \quad 3}$

similarly N2, N3, N4

N1 RT

Dest	Dist	Next
N1	0	N1
N2	1	N2
N3	7	N2,N3
N4	∞	–
N5	4	N5

At N5 : N2 $\boxed{1 \quad 0 \quad 6 \quad \infty \quad 3}$

N4 $\boxed{\infty \quad \infty \quad 2 \quad 0 \quad 4}$

N5 RT

Dest	Dist	Next
N1	4	N2
N2	3	N2
N3	6	N4
N4	4	N4
N5	0	N5

ROUTING ORIGINAL ALGORITHM

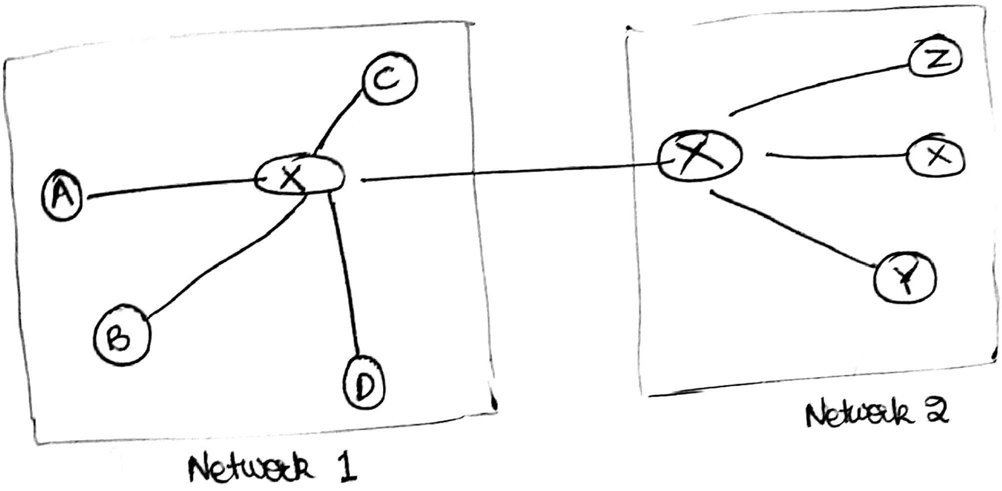
shortcut

Dijakshtra's Algo

GUDI VARAPRASAD - COMPUTER NETWORKS

*. ARP (Address Resolution Protocol) :

- layer 3 protocol (Network layer).
- Converts IP address to MAC Address.



- A to C

IP_A	MAC_A	IP_C	FF--F

→ communicate with all → Broadcast Message

C to A (Reply)

IP_C	MAC_C	IP_A	MAC_A

→ Unicast Message

- A to Z ⇒ A to Router (Network 1) + Router to Z (Network 2)

The same procedure broadcast then Unicast.

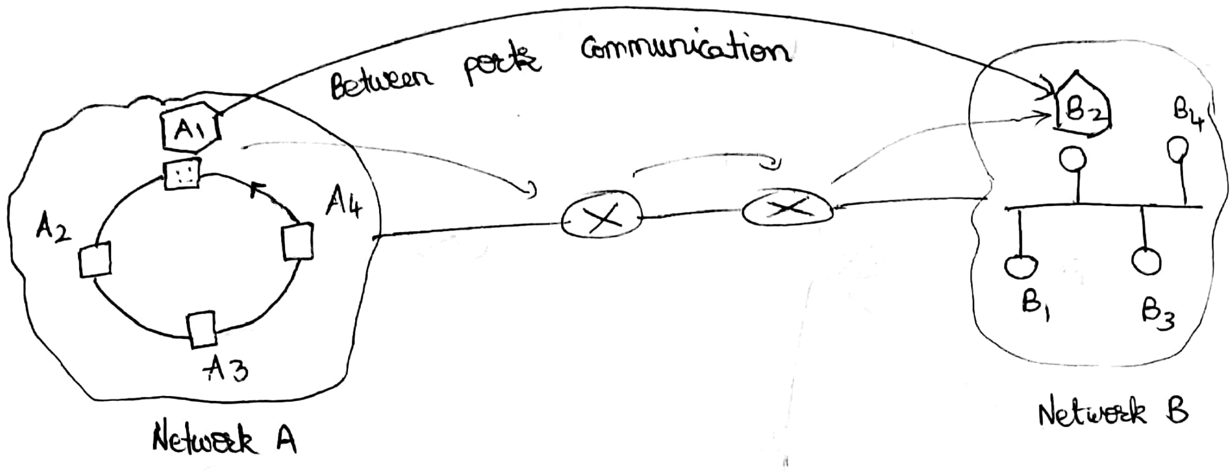
- 1st MAC Address is founded & then IP Address.

← 8 bits + 8 bits → ← 16 bits →

Hardware Type	Protocol Type
Hardware Length / Protocol Length	Operations (1, 2)
Sender Hardware Address (6B for Ethernet)	
Sender Protocol Address (4B for IP)	
Target Hardware Address	
Target Protocol Address	

MODULE - 5 : TRANSPORT LAYER

- End to End delivery (Port to Port)



- Uses two most important protocols → TCP, → UDP
- Error Control → TCP's checksum (error detection).
- Congestion Control & Flow Control.
- Segmentation of data from Application data
- Multiplexing / Demultiplexing.

* TCP (Transmission Control Protocol) :

- **Byte Streaming :**

→ The total data coming from different applications in an application layer is segmented as segments (Collection of bytes).

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- Connection Oriented :

→ TCP is mainly for reliability.
→ It uses 3-way Handshaking protocol.

- Full Duplex :

→ Two applications can communicate at same without data loss.

→
- Piggy Backing :

→ Go back - N, Selective Repeat protocol to send data & Acknowledgement.

- Error Control :

→ TCP supports error control & receiver can detect the error easily.

- Flow Control :

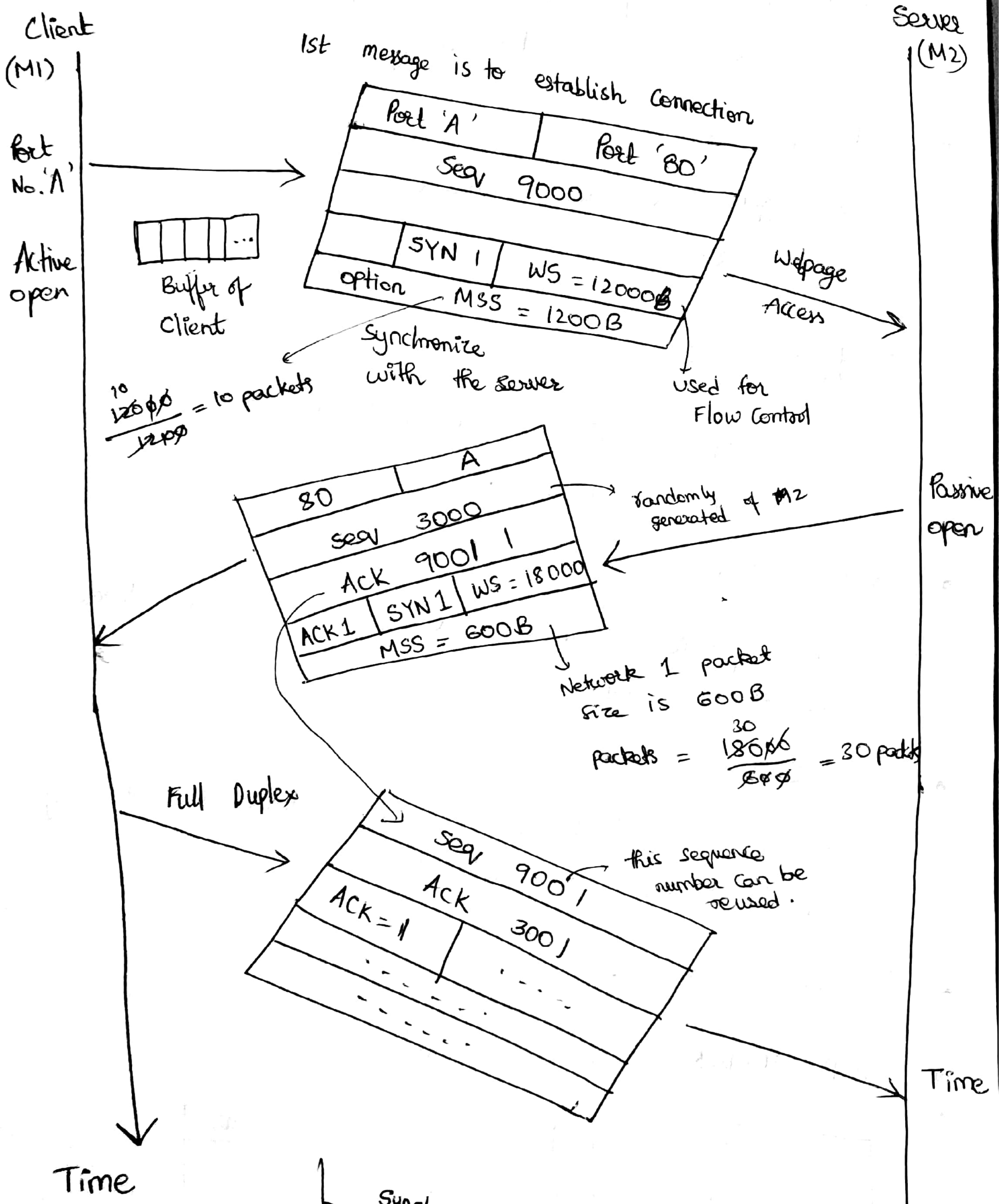
→ Flow in data packets following restrictions in receiving size. to ensure no data loss.

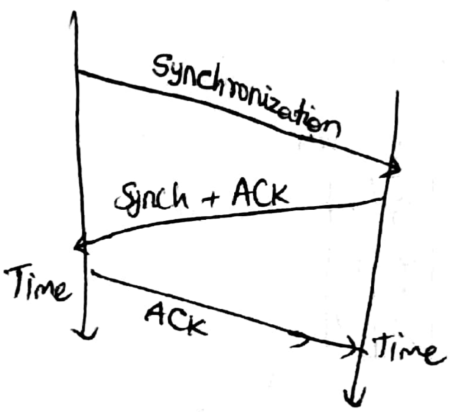
- Congestion Control :

* TCP HEADER : (20 to 60 Byte)

Source Port (16 Bit)					Destination Port (16 bit)			
Sequence Number (32 bit)								
Acknowledge Number (32 bit)								
HLEN (4 bit)	6	URG	ACK	PSH	RST	SYN	FIN	Window size (16 bit)
Checksum (16 bit)					(16 bit) URGENT Pointer			
options & Padding (40 Bytes)								

* TCP Connection Establishment :





3 way Hand shaking
⇓
for Connection establishment

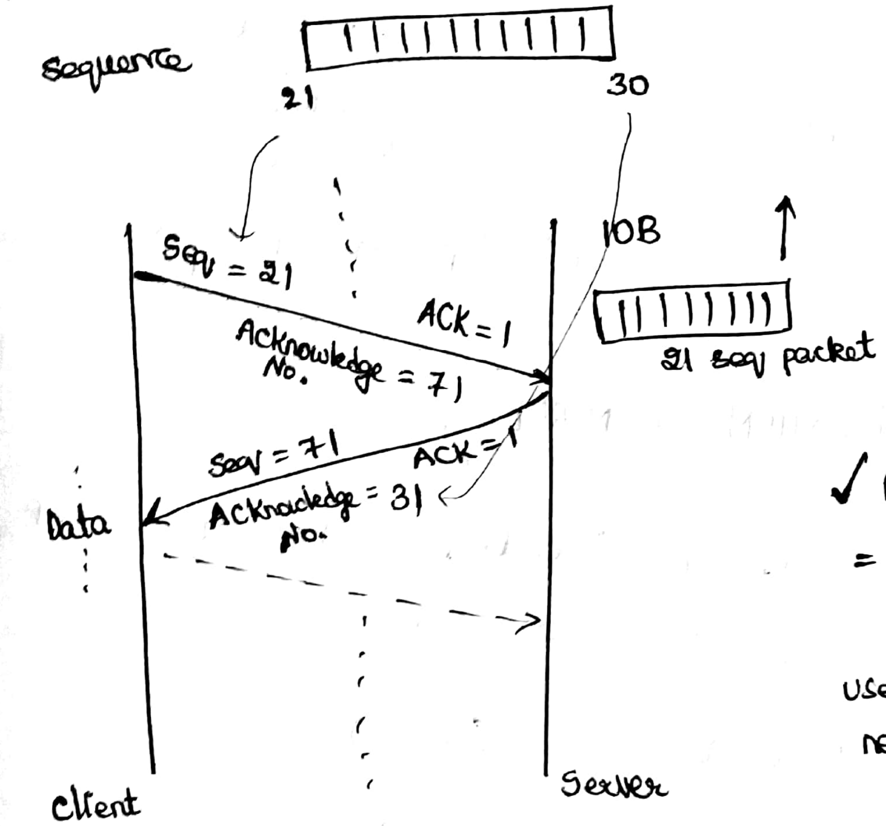
GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*. TCP Data Transfer :

- Full Duplex mode ⇒ client $\underset{both}{\overset{both}{\rightleftarrows}}$ server.
- They negotiate window size and then communicate.

Assume window size = 10B



✓ Piggybacking :

= Data + Acknowledge

⇓

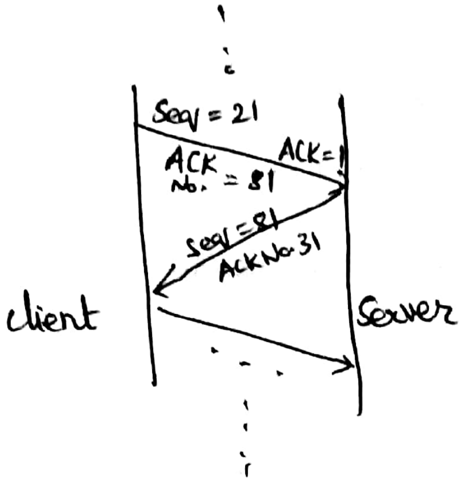
used to reduce network trafficing

✓ Pure ACK : If there is no data to be sent, then only ACK is sent but will never wait for data since it may lead to timeout & retransmit of data.

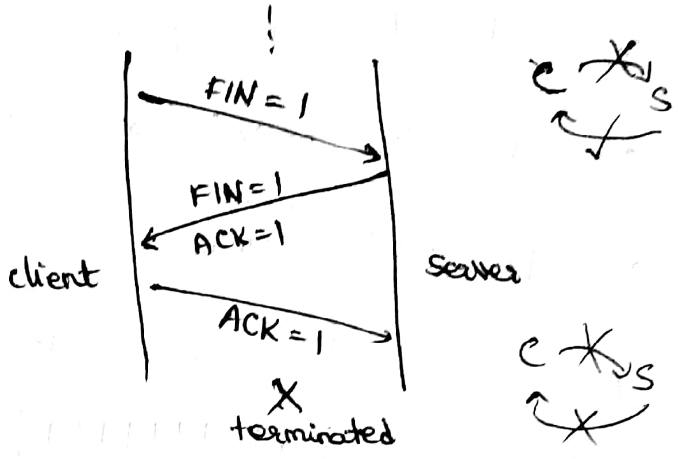
*. TCP Connection Termination :

- A client sends FIN = 1 (set). When client wants to terminate.
- Serve receives that & releases all the resources called "HALF DUPLEX" → C $\rightleftarrows$ S

GUDI VARAPRASAD - COMPUTER NETWORKS



Connection
Data Transfer



Connection
termination

(3 step or 4 step)

*. TCP CONGESTION CONTROL :

Ex : Let the size of Congestion window of a TCP Connection in two cases when

Case I : Timeout occur (Severe)

Case II : 3 ACK Received (Low)

~~Case III~~ :

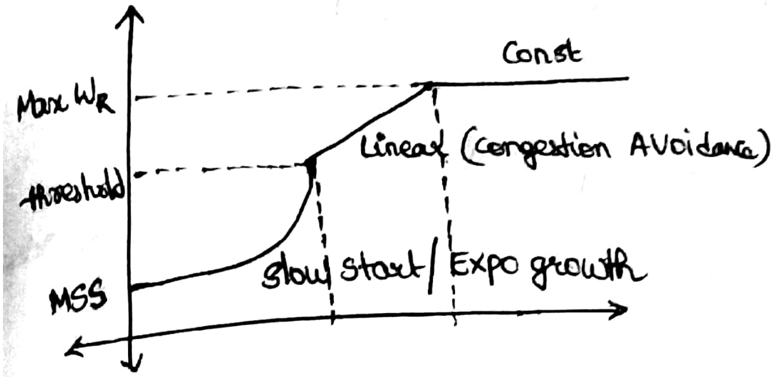
is 32 KB. The RTT of a connection is 100 m sec and MSS = 2 KB. The time taken (m sec) by TCP Connection to get back to 32 KB Congestion window is ______ and ______ respectively.

Sol :

MSS = 2 KB

Cong. window size = 32 KB

~~Router~~ Round trip time = 100 m sec



★ IMP diagram

window size = $\frac{\text{threshold}}{w/s}$ = $\frac{32}{MSS}$ = $\frac{32}{2}$ = 16

timeout

↑ 2 → 4 → 8 → 16 → 18 → 20 → 22 → 24 → 26 → 28 → 30 → 32

2 → 4 → 8: exponential (slow start)

16: stop since reached threshold

total segments = 12

Round triptime for ack = 100 msec

propagation = 12 × 100 = 1200 msec ✓

Trips = 12 − 1 = 11

Case II : threshold value = $\frac{\text{Cong. window size}}{MSS}$ = 16

directly starts from Congestion Avoidance

16 18 20 22 24 26 28 30 32

total segments = 9

propagation delay + acknowledge time = 100 = RTT

= 900 msec ✓

Trips = segments − 1 = 9 − 1 = 8

GUDI VARAPRASAD - COMPUTER NETWORKS

*. USER DATAGRAM PROTOCOL : (UDP)

- It is a connectionless protocol.
- Unlike TCP, UDP is unreliable & there is no order

Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)

Actual size $= 2^{16}$

Header	Payload

8 bit

$\Rightarrow = 65527$ max size

Checksum (16) bits = UDP Header + UDP Data + Pseudo header of IP

↓

Used for error control (hash value of data to check at receiver side)

*. Advantages of UDP : (Applications)

- Query Response Protocol (one request one reply) = DNS DHCP
- IMP Speed (online games, Voice over IP) → because of less overhead → AIMD is used
- Broadcasting / Multicasting [RIP].
- Continuous streaming [Skype, Youtube].
- stateless protocol — not needed to store the connection information / values.
  ((UDP) HTTP / HTTPS

★ Amazon / Flipkart ⇒ uses stateful

GUDI VARAPRASAD - COMPUTER NETWORKS

*. TCP (vs) UDP :

TCP	UDP
• Connection oriented	• Connection less
• Reliability	• Less Reliable
• Error control is mandatory	• Error control is optional
• Slow transmission	• Fast transmission (speed ↑)
• More overhead	• Less overhead
• Flow control, Congestion control } Used	• No Flow control, Congestion control.

*. REMOTE PROCEDURE CALLS :

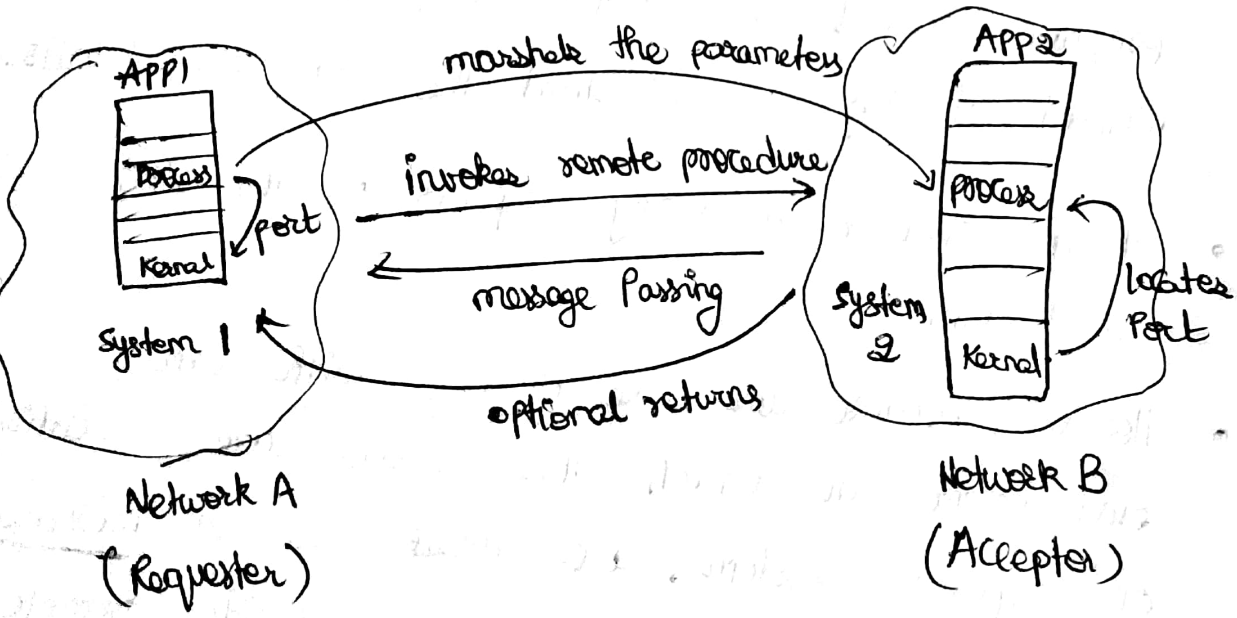
- Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details.
- It is similar in many respects to the IPC mechanism.
- However, because we are dealing with an environment in which the processes are executing on seperate system, we must use a message based communication scheme to provide remote service.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

- In contrast to the IPC facility, the messages exchanged in RPC communications are well structured and are thus no longer just packets of data.
- Each message is addressed to an RPC daemon listening to a port on the remote system, and each contains an identifier of the function to execute and the parameters to pass to that function.
- The function is then executed as requested, and any output is sent back to the requester in seperate message.

Procedure :



GUDI VARAPRASAD - COMPUTER NETWORKS

*. Flow Control (vs) Congestion Control :

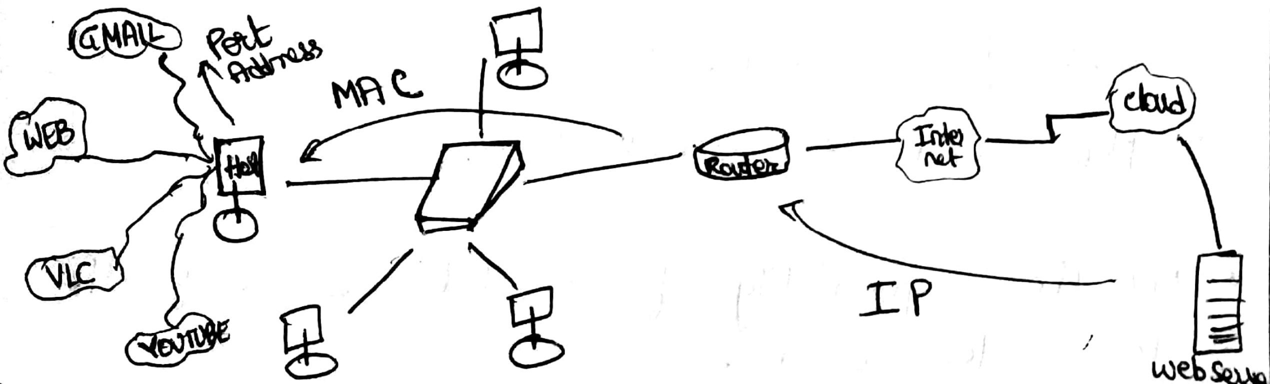
Congestion Control	Flow Control
• Congestion Control is needed when buffers in packet switches overflow or cause congestion.	• Flow control is needed when the buffers at the receiver are not ~~deplete~~ depleted as fast as the data arrives.
• Congestion is end to end, it includes all hosts, links and routers	• Flow is between one data ~~sender~~ sender & one receiver. It can be done on link-to-link or end to end basis.

*. PORT ADDRESSING :

Analogy :

- Reaching our city = Reaching our network (IP Add)
- Reaching our Appartment = Reaching host (MAC Address)
- IMP Reaching the right host = Reaching right process of APP (Port Address)

- Port = Communication endpoint
- Fixed port numbers (0 - 1023)
- Dynamic port numbers (1024 - 65535) → assigned by OS



* Addressing :

(Refer Module 1) → Addressing / Data traversals

---

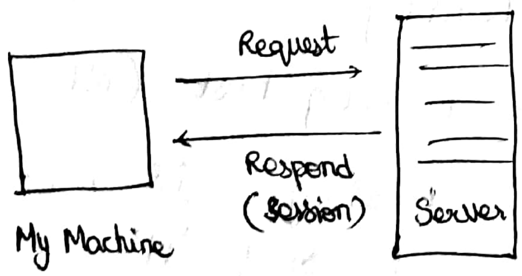
* QUALITY OF SERVICE : (QOS)

- QOS is an overall performance measure of computer network.
- Flow characteristics of QOS are :

1. Reliability
2. Delay
3. Jitter
4. Bandwidth

---

* SESSION LAYER :



- Responsibilities :

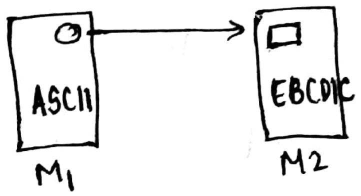
→ Authentication, Authorization.
→ Session Restoration, checkpoint. (Session Beans)
→ Webinar / Web conference.
→ Flow Control & synchronization.

- Not the responsibility of OS but the role of APP to create sessions.

GUDI VARAPRASAD - COMPUTER NETWORKS

GUDI VARAPRASAD - COMPUTER NETWORKS

*. PRESENTATION LAYER :



- Code Conversion (Formatting).
- Encryption / Decryption.
- Compression. (Data)

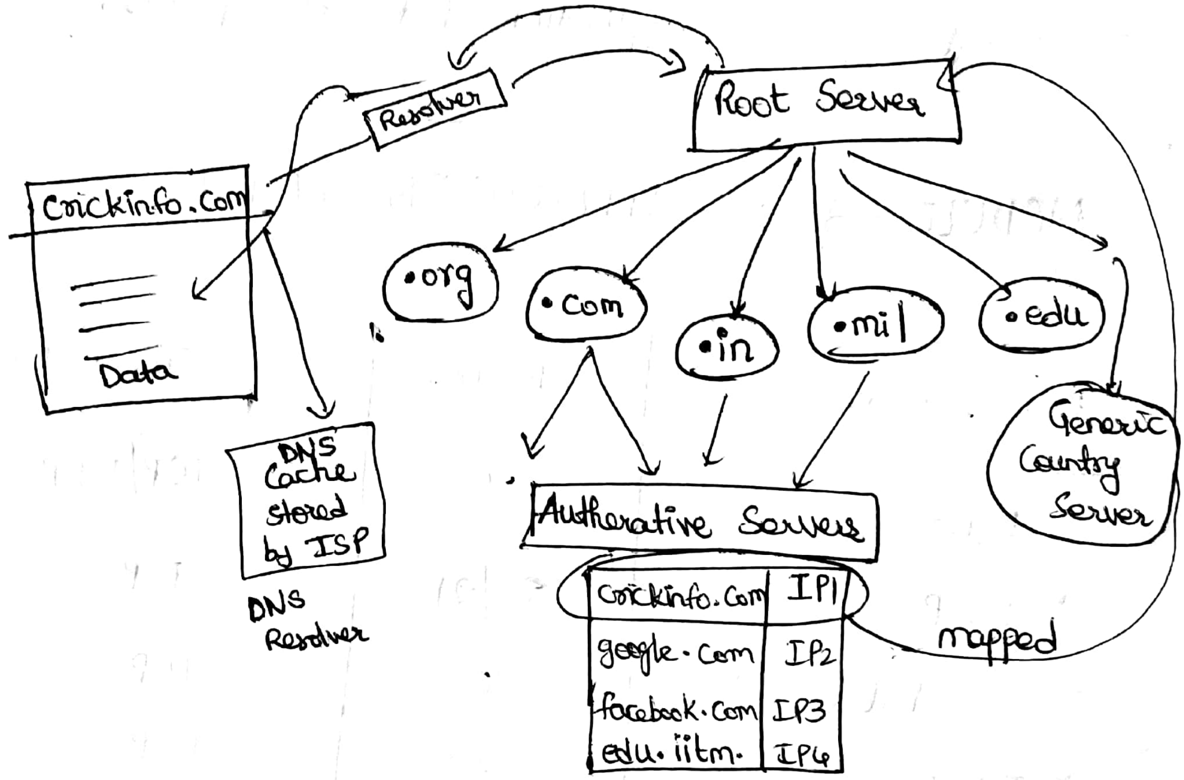
- Helps application to view.
- Handled by the application but not by OS.

MODULE - 6 : APPLICATION LAYER

Protocol Name	Port No.	Transport Protocol
Echo	7	TCP/UDP
* FTP	20/21	TCP
Secure Shell (SSH)	22	TCP
* Telnet	23	TCP
* SMTP	25	TCP
* DNS	53	UDP
✓ DHCP	67/68	UDP
TFTP	69	UDP
* HTTP	80	~~UDP~~ TCP
POP	110	~~TCP~~ TCP
NTP	123	UDP
* HTTPS	443	TCP
✓ RIP	520	UDP

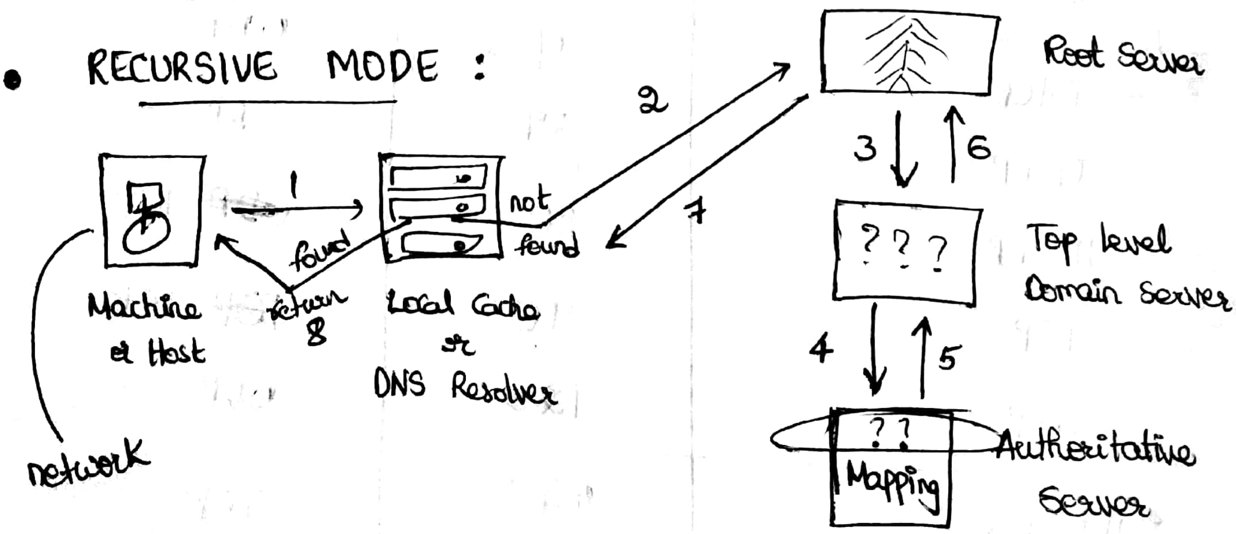
GUDI VARAPRASAD - COMPUTER NETWORKS

* DOMAIN NAME SYSTEM (DNS) :

- We use to map domain names with IP address.
- IP addresses are dynamic but domain name shouldn't be changed (static).
- 

* DNS Types & services :

- RECURSIVE MODE :



- Uses UDP protocol (speed ↑)

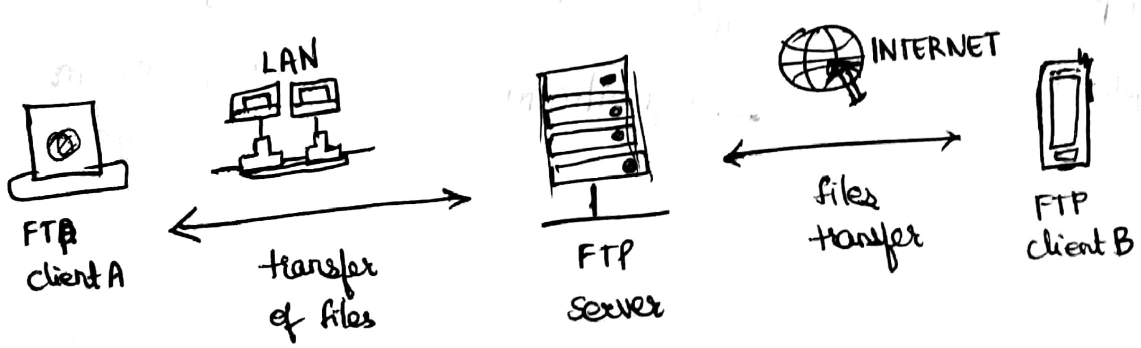
GUDI VARAPRASAD - COMPUTER NETWORKS

*- HTTP (Hyper Text Transfer Protocol) :

- Port Number = 80.
- Widely used to fetch webpages of www.
- Itself not reliable but use TCP to achieve.
- Inband Protocol - 1st DNS request + data from same port.
- Stateless Protocol - Not stores info about connection.
- HTTP 1.0 : Non-Persistent.
- HTTP 1.1 : Persistent.
- Commands (Head, GET, POST, PUT, DELETE, CONNECT).

*- FTP (File Transfer Protocol) :

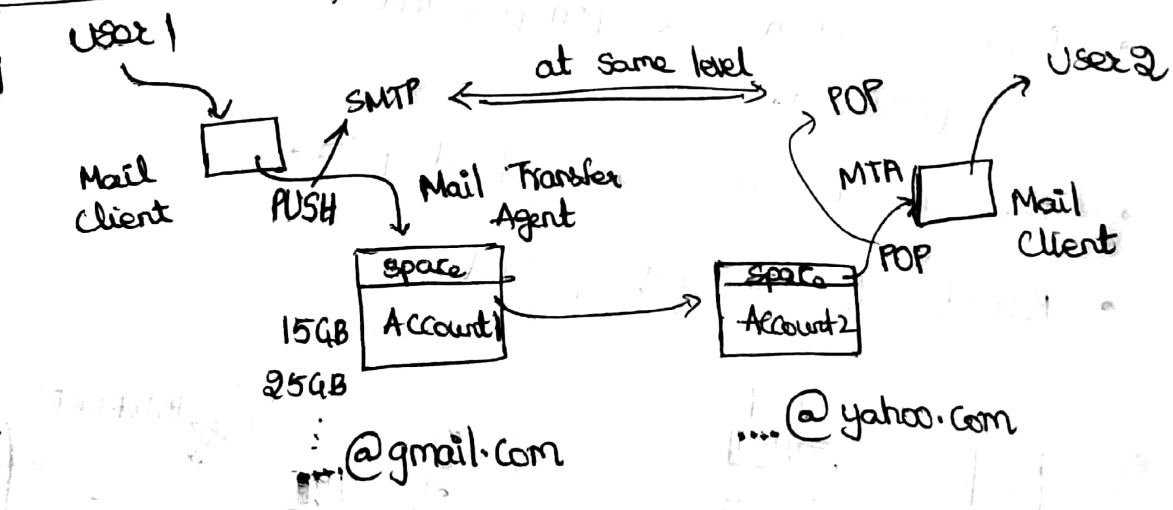
- Port Number = 20 (Data) or 21 (Control)
- Data connection is non-persistent. Control connection is persistent.
- Not Inband since uses different ports.
- Reliable & stateful protocol.



* SMTP (Simple Mail Transfer Protocol) & POP (Post office Protocol):

- FTP is synchronous but SMTP & POP is both synchronous & asynchronous.
- SMTP uses Port No. = 25 for pushing the mail.
- By default POP3 protocol works on two ports:
  Port - 110: this is the default POP3 non-encrypted port.
- Port 995 - this is the port you need to use if you want to connect using POP3 securely.
- MIME (Multipurpose Internet Mail Extensions).

Working of SMTP And POP Protocols



GUDI VARAPRASAD - COMPUTER NETWORKS

*. ALL NETWORKING Protocols & DEVICES :

⑦ Application Layer	Data/Message	Firewalls, Gateways, PC, Phones	DNS, HTTP, HTTPS, FTP, DHCP, SMTP, POP, Telnet
⑥ Presentation Layer	Data/Message	Firewall	MIME, SSL
⑤ Session Layer	Data/Message	Firewall	PAP, RPC
④ Transport layer	Segment	Gateways, Firewalls	TCP, UDP, SCTP
③ Network layer	Packet Datagram	Router, BRouter, 3-layer Switch	IPV4, IPV6, ICMP, IGMP ARP, RARP
② Data link layer	Frames	Bridge, NIC, 2-layer switch	IEEE 802.3, CSMA, HDLC, IEEE 802.5
① Physical layer	Bits	cables, Hub, Repeater, Fiber	IEE 802.11

*. TORRENT : A distributed system that shares a file through a peer to peer (P&P) network.

*. VPN : (Virtual Private Network) It is an extended private network across public network and enables users to send/receive data across share public network.

GUDI VARAPRASAD - COMPUTER NETWORKS