[Network Performance]

↳ One important issue in networking is the performance of the network - how good is it?

↳ Network performance is measured in following fundamental ways -
- Bandwidth
- Throughput
- Latency (Delay)

* Bandwidth :-
↳ Informal :- Maximum amount of data that can be transmitted per second.
↳ Formal :- The bandwidth of a network is given by the no. of bits that can be transmitted over the network in a certain period of time.

* Wired Network → Bandwidth in bps.
Bandwidth = Capability
Ex :- Gigabit Ethernet can provide a bandwidth of 1 Gbps.
* Wireless Network → Bandwidth in hertz
A range of frequencies used to transmit signals which is measured in hertz.

[Network Performance]

↳ One important issue in networking is the performance of the network - how good is it?

↳ Network performance is measured in following fundamental ways -
- Bandwidth
- Throughput
- Latency (Delay)

* Bandwidth :-
↳ Informal :- Maximum amount of data that can be transmitted per second.
↳ Formal :- The bandwidth of a network is given by the no. of bits that can be transmitted over the network in a certain period of time.

* Wired Network → Bandwidth in bps.
Bandwidth := Capability
Ex :- Gigabit Ethernet can provide a bandwidth of 1 Gbps.
* Wireless Network → Bandwidth in hertz
A range of frequencies used to transmit signals which is measured in hertz.

* Throughput :-
↳ Informal :- Actual amount of data that passes through the medium.
↳ Formal :- The throughput is a measure of how fast we can actually send data through a network.
↳ Although 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 $T \leq B$, always.

↳ we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link

* Latency (Delay) :-
↳ 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.

• Latency is made of 4 components
1. Transmission Delay
2. Propagation Delay

Latency = Transmission delay + Propogation Delay + Queing Delay + Processing Delay

* Transmission Delay:- Times it takes to place the complete data packet on the transmission medium.

Transmission Time = $\frac{\text{Msg size}}{\text{Bandwith}}$

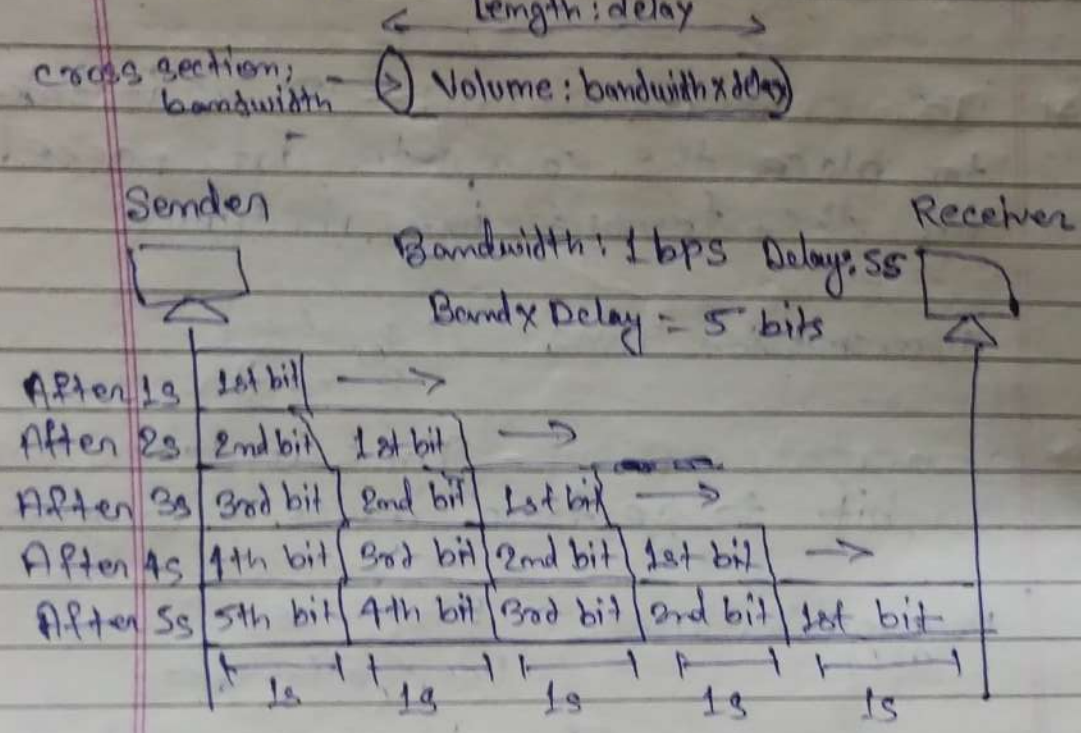
* Propogation Delay:- Time it takes for a bit to go from device A to device B.

Propogation Time = $\frac{\text{Distance}}{\text{Propagation Speed}}$

* Queuing Delay:- The time needed for each intermediate or end device to hold the message before it can be processed.
  - The queuing time is not a fixed factor, it changes with the load imposed on the network.
  - When there is heavy traffic on the network, the queing time increases.

* Processing Delay:- How much time the node takes to process the message.

* Bandwidth Delay Product →
* It defines the no. of bits that can fill the link.



Q. Consider that the link capacity of a channel is 512 kbps and round trip delay time is 1000 ms.

Sol:- The bandwidth delay product = 512 kbps × 1000 ms

$= 512 \text{ kbps} \times 1000 \times 10^{-3} \text{ sec}$

$= 512 \times 1000 \text{ bps}$

$= 512 \times 1000 \times \frac{1000}{10^3}$

$= 512\,000 \text{ bits} / 8$

$= 64,000 \text{ bytes} / 12$

Q what is the propogation time if the distance b/w the two points is 12000 km? Assume the propogation speed to be 2.4×10^8 m/s in cable.

Propogation time = $\frac{\text{Distance}}{\text{Propogation speed}}$

$= \frac{12000 \times 1000 \text{ m}}{2.4 \times 10^8}$

$= \frac{12 \times 10^6}{2.4 \times 10^8}$

$= \frac{12 \times 10}{24 \times 100}$

$= \frac{1}{20}$ ms

$= 0.05$ ms

* Round Trip Time (RTT) —
  - It is the length of time it takes for a signal to sent plus the length of time it takes for an acknowledgement of that signal to be received.
  - This time therefore consists of the propopagation times b/w the two point of signal.
  - If T_p is the Propogation time, then

$$RTT = 2 \times T_p$$

[Flow Control]

↳ Speed matching mechanism.
↳ Flow control coordinates the amount of data that can be sent before receiving an acknowledgement.
↳ Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.
↳ Receiver has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
↳ Receiver must inform the sender before the limits are reached and request that the transmitter to send fewer frames or stop temporarily.

=> Protocols

Noiseless Channels
- Simplest
- Stop-and-wait

Noisy Channels
- Stop-and-wait ARQ
- GO-Back-N-ARQ
- Selective Repeat ARQ

Sliding-Window Protocol

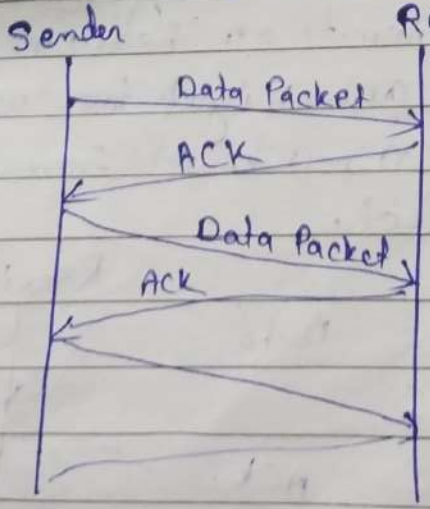
* Stop-and-wait Protocol -

↳ It provides unidirectional data transmission with flow control facilities but without error control facilities.
↳ The idea of stop-and-wait protocol is straightforward.
↳ After transmitting one frame, the sender waits for an acknowledgement before transmitting the next frame.

⇒ Primitives of stop-and-wait Protocol

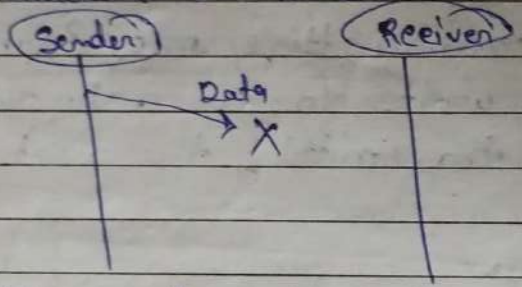
* Sender side -
Rule-1 :- Send one data packet at a time.
Rule-2 :- Send the next packet only after receiving ACK for the previous.

* Receiver Side -
Rule 1 :- Receive and consume data packet.
Rule-2 :- After consuming packet, ACK need to be sent (Flow Control)

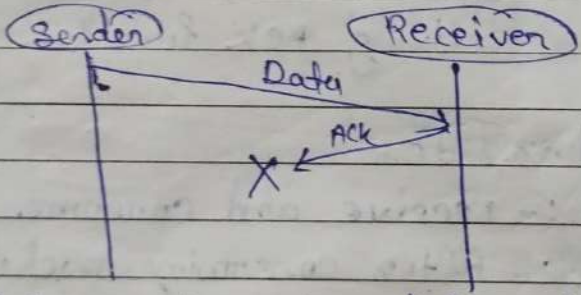


=> Problems of Stop-and-wait Protocol -

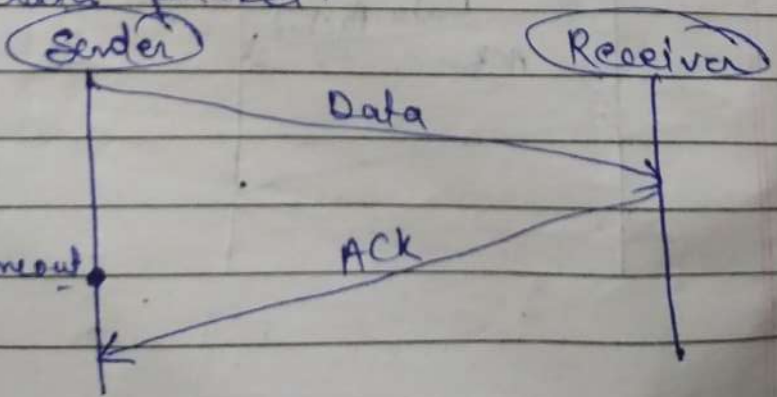
1. Problems due to lost data.
   ↳ Sender waits for ack for an infinite amount of time.
   ↳ Receiver waits for data an infinite amount of time.



2. Problems due to lost ACK.
   ↳ Sender waits for an infinite amount of time for ack.



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.

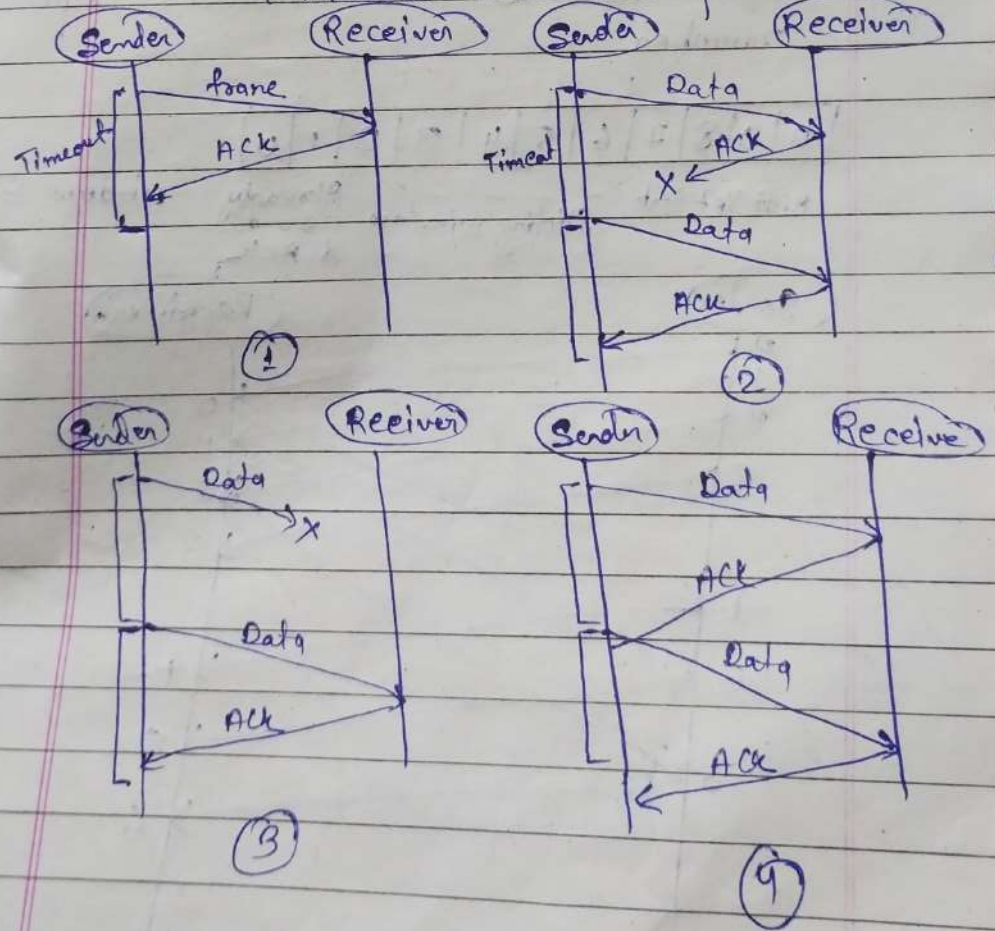


* Stop-and-wait ARQ Protocol —

↳ After transmitting one frame, the sender waits for an ack before transmitting the next frame.

↳ If the ack does not arrive after a certain period of time, the sender times out and retransmits the original frame.

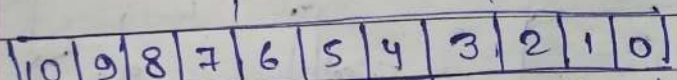
↳ Stop-and-wait ARQ = Stop-and-wait + Timeout Timer + Sequence no.

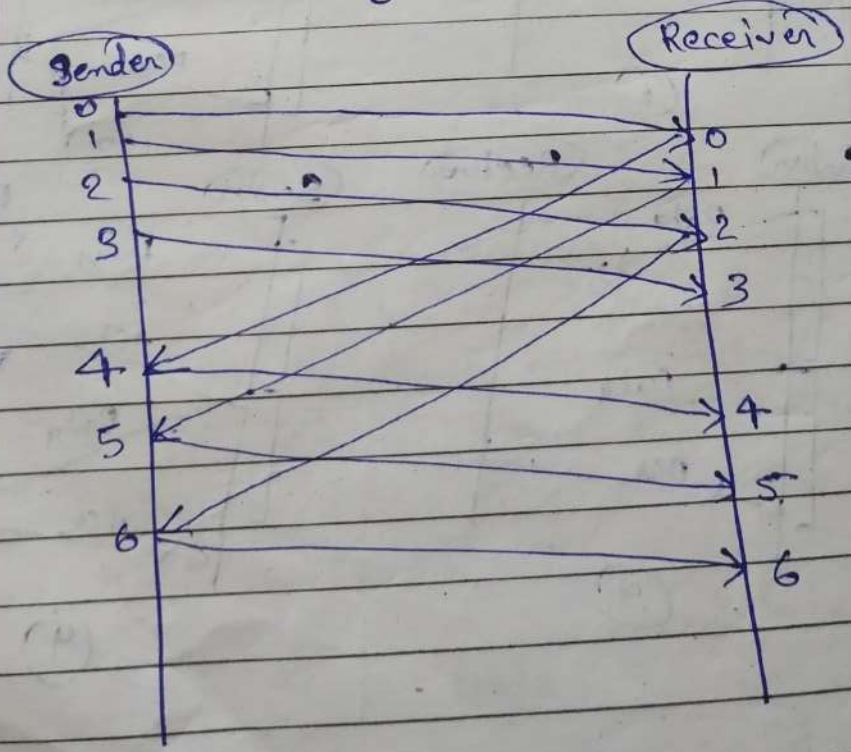


* Sliding Window Protocol -

⇒ Drawbacks of Stop-and-wait ARQ.
- ↳ One frame at a time.
- ↳ Poor utilization of bandwidth
- ↳ Poor Performance

- ↳ Send multiple frames at a time.
- ↳ No. of frames to be sent is based on window size.
- ↳ Each frame is numbered → Sequence number





Sender window size $= 2^m - 1$

Receiver Page No.: 11 = 1

Date: / / 37

* Go-Back-N ARQ

↳ 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 frame.

↳ There are finite no. of frames and the frames are numbered in a sequential manner.

↳ The no. of frames that can be sent depends on the window size of the sender.

↳ If the acknowledgment of a frame is not received within an agreed upon time period, all frames in the current window are transmitted.

↳ The size of the sending window determines the sequence no. of the outbound frames.

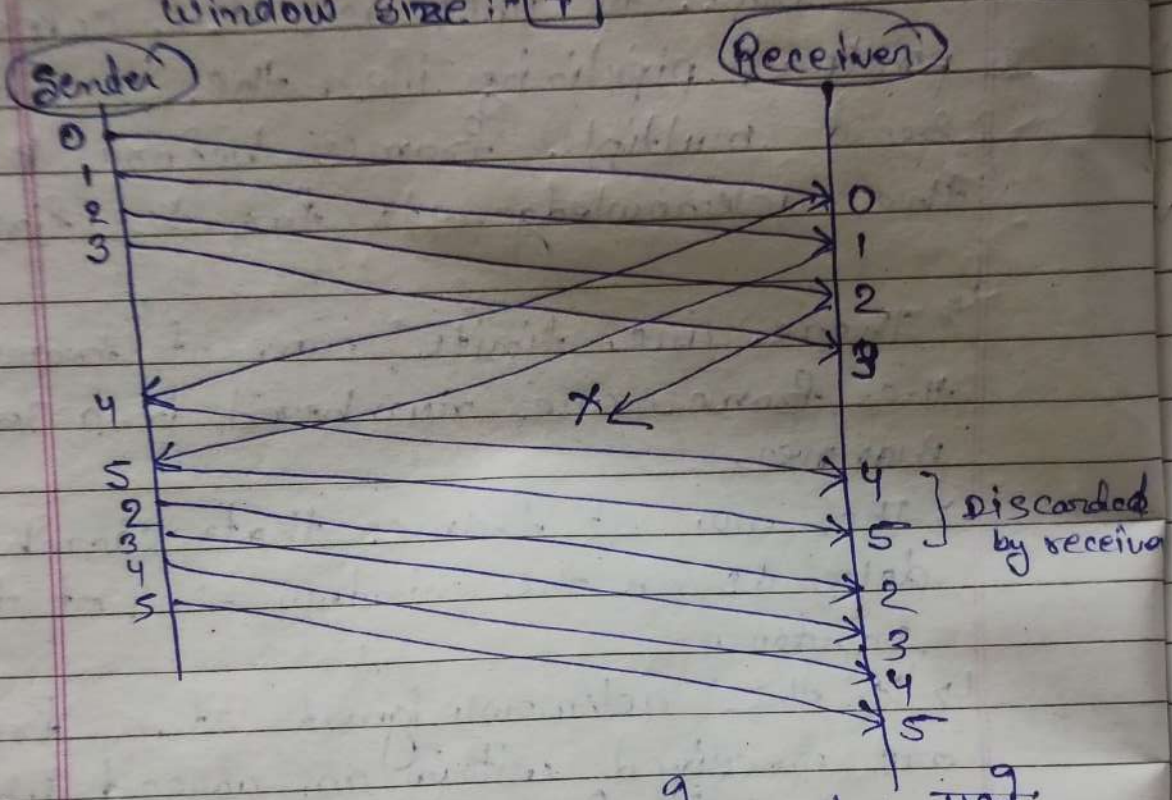
* N - Sender's window size

↳ For example, 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 so on.

↳ The no. of bits in the sequence no. is 2 to generate the binary sequence 00, 01, 10, 11.

10	9	8	7	6	5	4	3	2	1	0

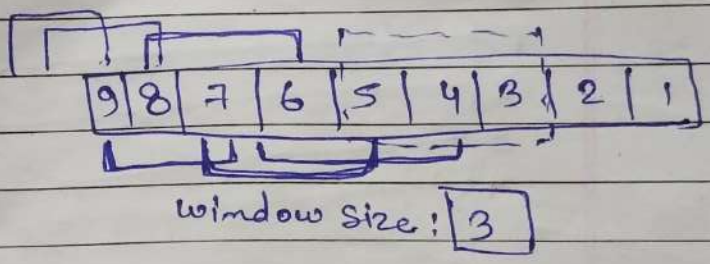
window size :- 4



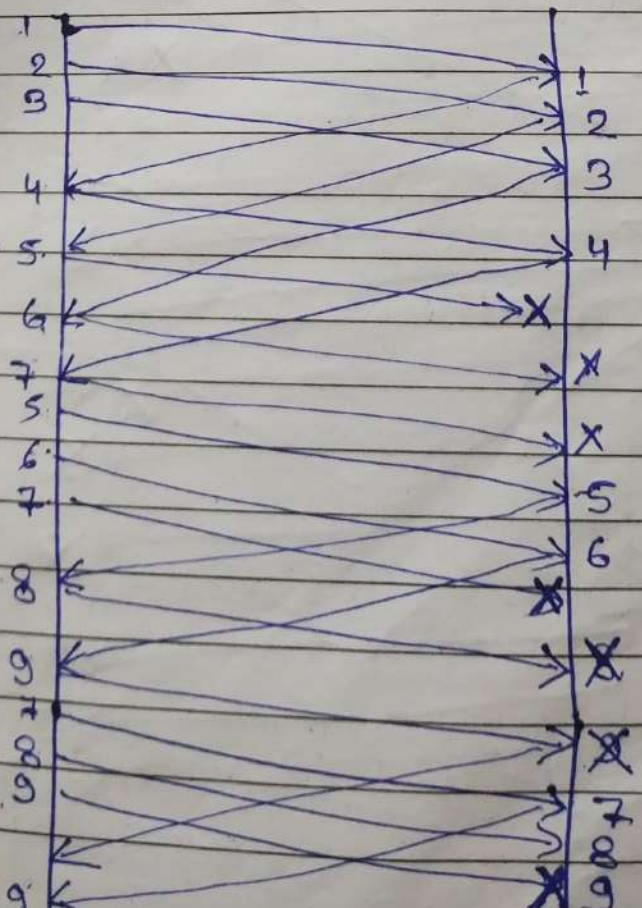
⇒ Go-Back-N technique में sender पहले window size जीतना frame भेज देगा फिर जिसका ACK आएगा तो [window] slide होगा और दूसरा frame send करेगा और ऐसे ही sliding window होता रहेगा लेकिन अगर कोई frame का ack नहीं आया तो फिर sender उस [sliding widow] के पूरे frame को वापस भेजना पड़ेगा ।

Q. 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?

(a) 12
(b) 14
(c) 16
(d) 18

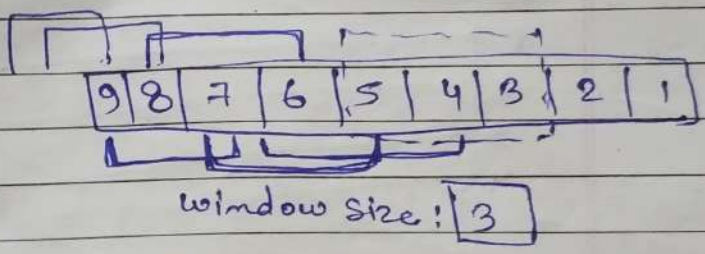


Total no. of packet transmitted = 16

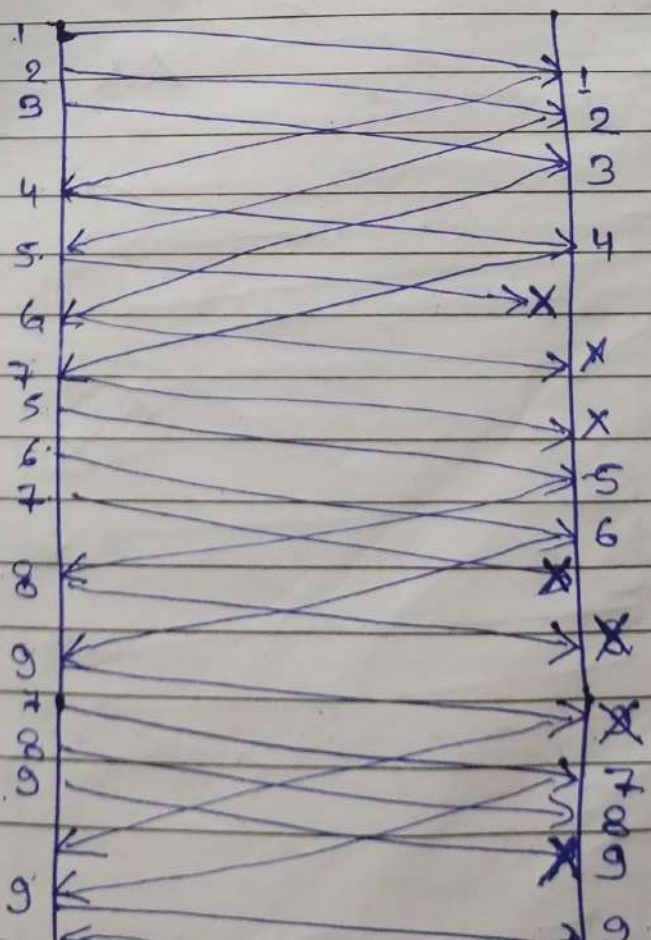


Q. Station A needs to send a message consisting of 9 packets to station B using a sliding window (window size 3) and go-back-n error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that A transmits gets lost (but no ACKs from B ever get lost), then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

(a) 12
(b) 14
(c) 16
(d) 18



Total no. of packet transmitted = 16



Q. 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?

10	9	8	7	6	5	4	3	2	1

every 6th frame corrupted

window size = 4

Ans (Total no. of frame transmitted = 17)

Sender window size = 2^{m-1}

Receiver window size = $2^{m}-1$

Page No.:
Date: / /

* Selective Repeat ARQ —

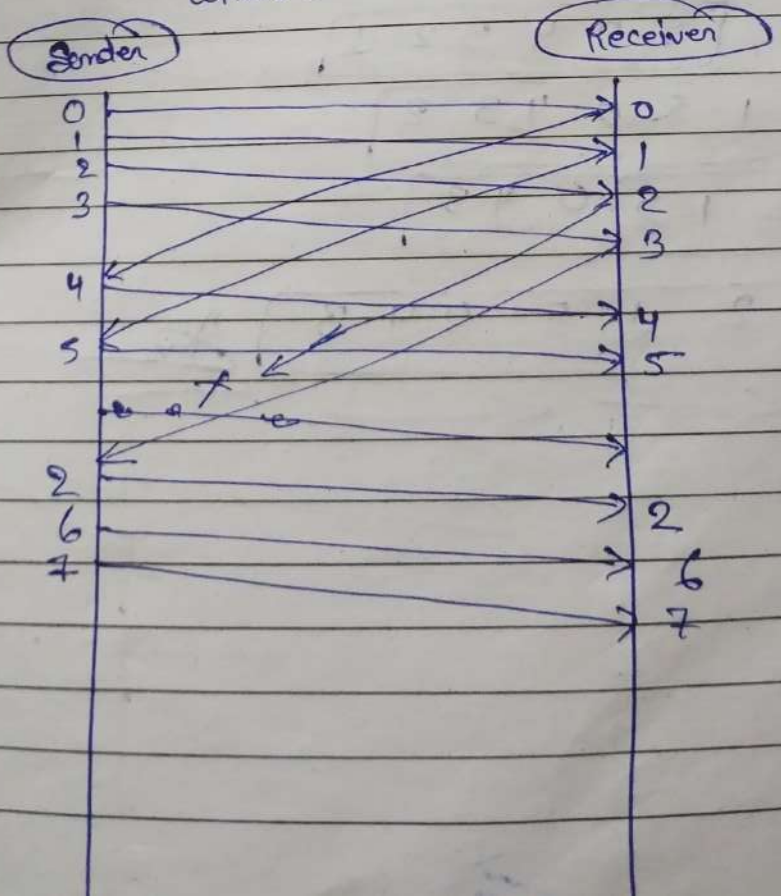
↳ In Selective Repeat ARQ, only the erroneous or lost frames are retransmitted, while correct frames are received and buffered.

↳ The receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

↳ The sender will send/retransmit packet for which NACK is received.

10	9	8	7	6	5	4	3	2	1	0

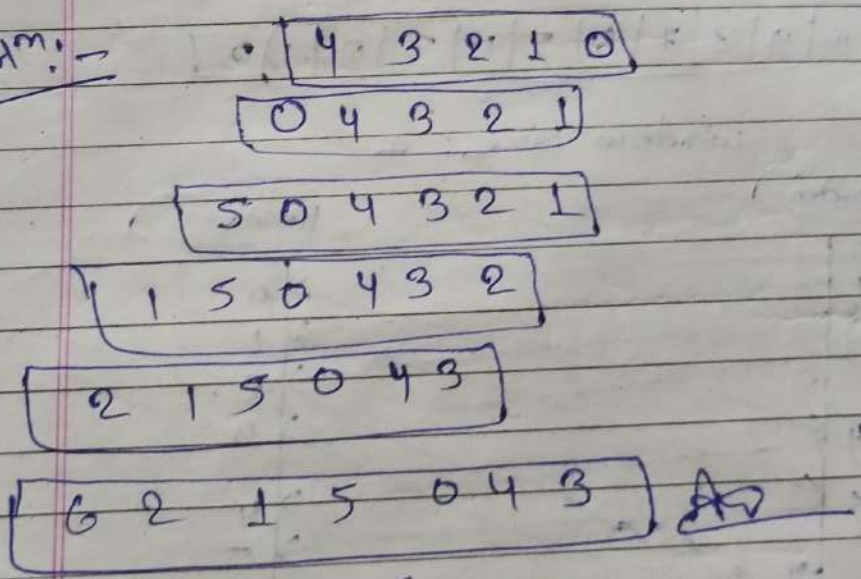
window size: 4



Q In selective Repeat protocol, suppose frames through 0 to 4 have been transmitted. Now, imagine that 0 times out. 5 (a new frame) is transmitted, 1 times out, 2 times out and 6 (another new frame) is transmitted. At this point, what will be the outstanding packets in Sender's window?

a) 341526
b) 3405126
c) 0123456
d) 654321
e) None of the above

Soln:-



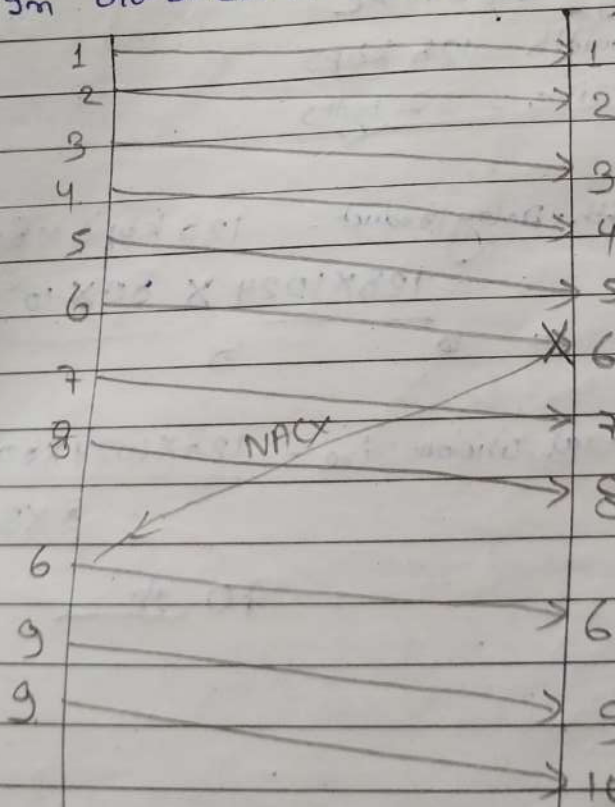
Q. Host A wants to send 10 frames to Host B. The hosts agreed to go with SR ARQ. How many no. of frames are transmitted by host A if every 6th frame that is transmitted by host A is either corrupted or lost? Also compare the no. of transmision of SR ARQ with Go-back-4 ARQ

Every 6th frame corru

10	9	8	7	6	5	4	3	2	1

No of transmission = 11

In Go-back-N No. of transmission = 17



Q The distance b/w two stations M and N is L kilometers. All frames are k bits long. The propogation time per km is t seconds. Let R bits/second be the channel capacity. Assuming the processing delay is negligible, the minimum no. of bits for the sequence no. field in a frame for maximum utilization, when the sliding window protocol is used -

a) $\log_2 \left(\frac{2Lt+R+2k}{k}\right)$

b) $\log_2 \left(\frac{2Lt+R}{k}\right)$

c) $\log_2 \left(\frac{2Lt+R+k}{2}\right)$

d) $\log_2 \left(\frac{2Lt+R+k}{2k}\right)$

Solm:- Let Propagation Delay = Lt sec

Round Trip Time = 2 × Propogation Delay

= 2 × Lt sec

= 2Lt sec

No. of bits transmitted in round trip = 2Lt+R bits

No. of frames = $\left(\frac{2Lt+R}{k}\right)$

Let the bits in the sequence nos. be b.

$2^b = \left(\frac{2Lt+R}{k}\right)$

Take log on both sides, we get

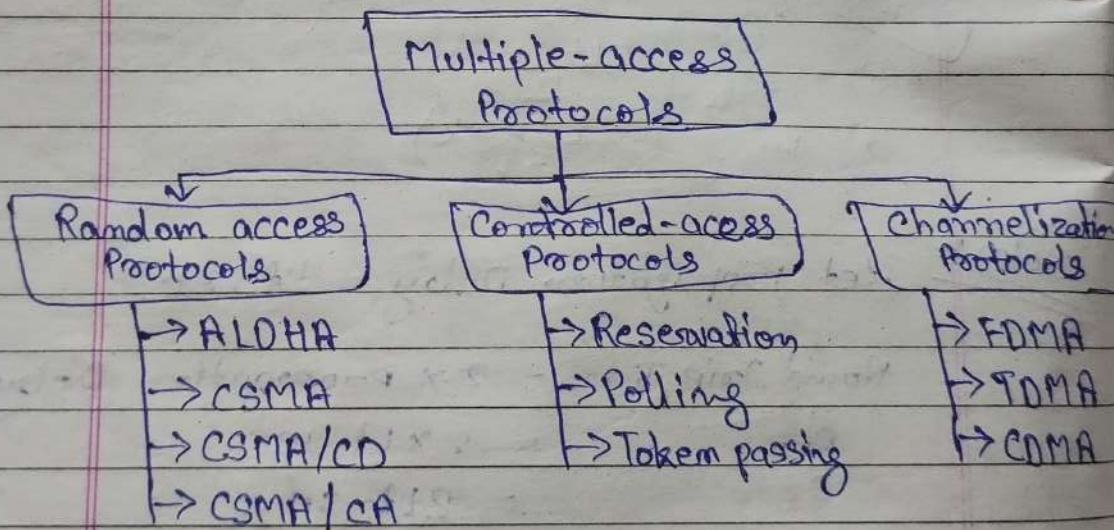
$b = \log_2 \left(\frac{2Lt+R}{k}\right)$ A

[Multiple [Access Control]

Why Multiple Access Protocols ?

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously.

Hence multiple access protocols are required to decrease collision and avoid crosstalk.



* Random Access Protocols –

In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state (idle or busy)

↳ In a Random access method, each station has the right to the medium without being controlled by any other station.

↳ If more than one station tries to send, there is an access conflict (COLLISION) and the frames will be either destroyed or modified.

⇒ To avoid access conflict, each station follows a procedure.

↳ When can the station access the medium?
↳ What can the station do if the medium is busy?
↳ How can the station determine the success or failure of the transmission?
↳ What can the station do if there is an access conflict?

* Controlled-Access Protocols –

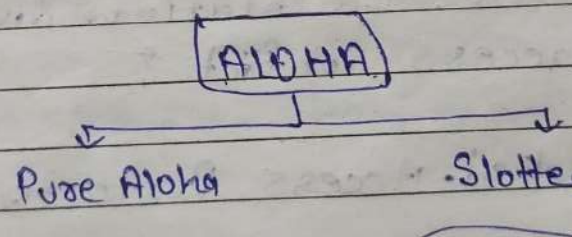
↳ In controlled access, the stations consult one another to find which station has the right to send.
↳ A station cannot send unless it has been authorized by other stations.

* Channelization Protocols -

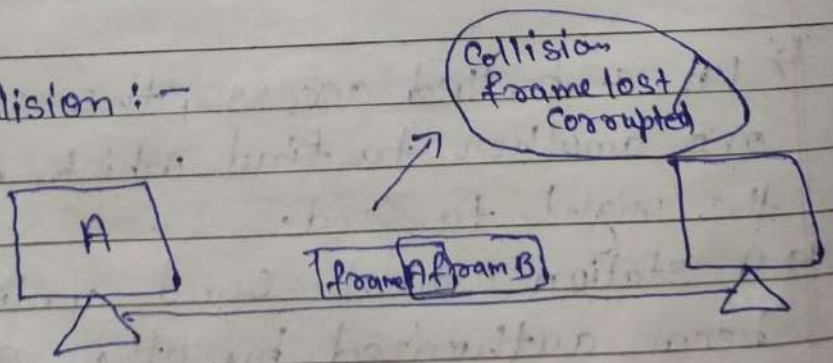
↳ Channelization is a multi-access method in which the available bandwidth of a link is shared in time, frequency or through code, between different stations.

* ~~Pure~~ ALOHA :-

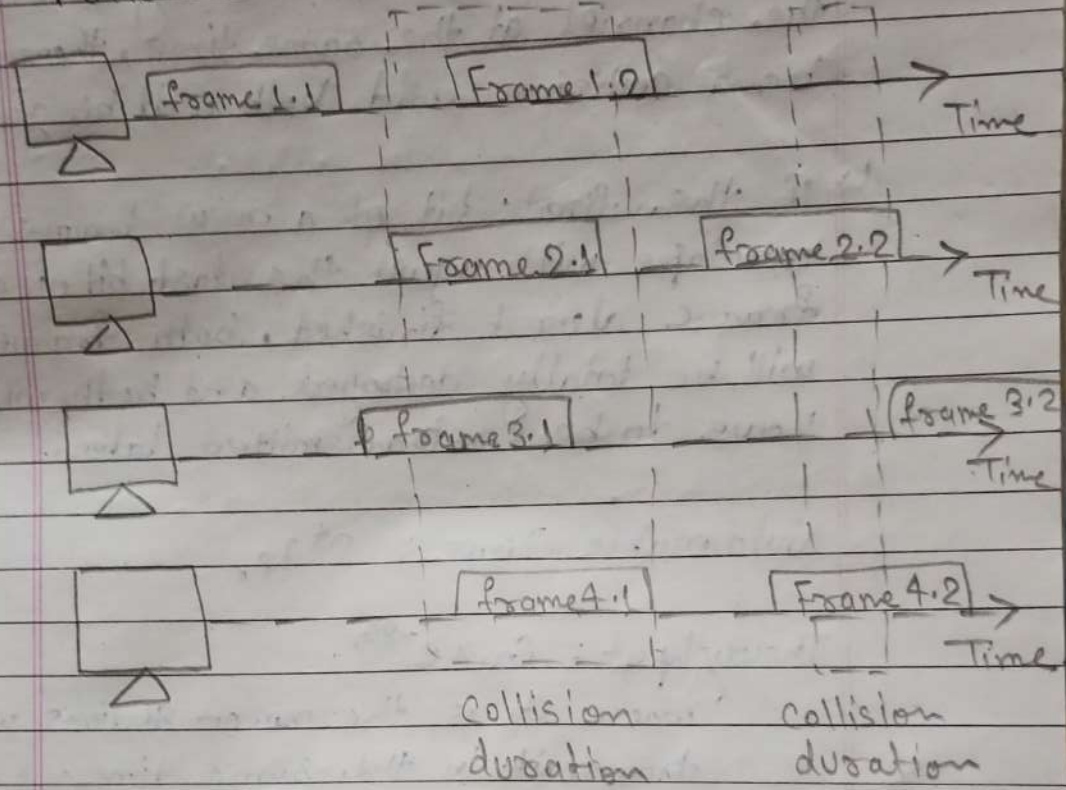
↳ It is a random access protocol
↳ It was actually designed for WLANs but is also appliable for shared medium..
↳ In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.



* Collision :-



⇒ PURE ALOHA



↳ Pure ALOHA allows stations to transmit whenever they have data to be sent.
↳ When a station sends data it waits for an acknowledgement.
↳ If the acknowledgement doesn't come within the allotted time, then the station waits for a random amount of time called back-off time (TB) and re-sends the data.
↳ Since different stations wait for different amount of time, the probability of further collision decreases.
↳ The throughput of pure aloha is maximized when frames are of uniform length.

↳ whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled.

↳ If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

Vulnerable Time = $2^* T_{fr}$

Throughput = $G \times e^{-2G}$;
where G is the no. of stations wish to transmit in the same time.

Maximum throughput = 0.184 for $G = 0.5$ (½)

⇒ Slotted ALOHA -

↳ It was developed just to improve the efficiency of pure aloha as the chances for collision in pure aloha is high.

↳ The time of the shared channel is divided into discrete time intervals called slots.

↳ Sending of data is allowed only at the beginning of these slots.

↳ If a station misses out the allowed time it must wait for the next slot.
This reduces the probability of collision.

↳ Vulnerable Time = Frame Transmission Time

↳ Throughput = $G \times e^{-G}$; where G is the no. of stations wish to transmit in the same time

↳ Maximum Throughput = 0.368 for G = 1

⇒ Pure ALOHA vs Slotted ALOHA

* Pure ALOHA -

↳ Any station can transmit the data at any time

↳ The time is continous and not globally synchronized.

↳ Vulnerable time in which collision may occur = $2 \times T_{fr}$

↳ Probability of successful transmission of data packet = $G \times e^{-2G}$

↳ Maximum Efficiency = 18.4 %. (Occurs at G = 1/2)

↳ Main Advantage : Simplicity in Implementation.

* Slotted ALOHA -

↳ Any station can transmit the data at the beginning of any time slot.
↳ The time is discrete and globally synchronized
↳ Vulnerable time in which collision may occur = T_{fr}
↳ Probability of successful transmission of data packet = $G \times e^{-G}$
↳ Maximum efficiency = 36.8%. (occurs at $G=1$)
↳ Main advantage: It reduces the no. of collisions to half and doubles the efficiency of pure aloha.

* CSMA (Carrier Sense Multiple Access) —
(Carrier: medium/channel)

↳ To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.
↳ Principle of CSMA: "Sense before transmit" or "listen before talk"
↳ Carrier busy = Transmission is taking place.
↳ Carrier idle = No transmission currently taking place.
↳ The possibility of collision still exists because of propagation delay; a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

⇒ Types of CSMA -

i. 1 - Persistent CSMA
ii. P - Persistent CSMA
iii. Non-Persistent CSMA
iv. O - Persistent CSMA

CSMA/CD (CSMA with Collision Detection)
CSMA/CA (CSMA with Collision Avoidance)

* 1 - Persistent CSMA

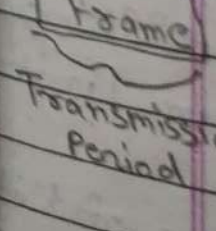
↳ Before sending the data, the station first listens to the channel to see if anyone else is transmitting the data at that moment.
↳ If the channel is idle, the station transmits a frame.
↳ If busy, then it senses the transmission medium continuously until it becomes idle.

↳ Since the station transmits the frame with the probability of 1 when the carrier or channel is idle, this scheme of CSMA is called as 1-Persistent CSMA.
↳ The propagation delay has an important effect on the performance of the protocol.

↳ The longer the propagation delay, the more important this effect becomes, and the worse the performance of the protocol.

* Non-Persistent CSMA -
  - Before sending, a station senses the channel if no one else is sending, the station begins doing so itself.
  - However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
  - Instead, it waits a random period of time and then repeats the algorithm. Consequently this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

* P-persistent CSMA -
  - It applies to slotted channels.
  - When a station becomes ready to send, it senses the channel.
  - If it is idle, it transmits with a probability P.
  - With a probability $Q = 1 - P$, it defers until the next slot.
  - If that slot is also idle, it either transmits or defers again, with probabilities P and Q.
  - This process is repeated until either the frame has been transmitted or another station has begun transmitting.
  - In the later case, the unlucky station acts as if there had been a collission (i.e., it waits a random time and starts again).

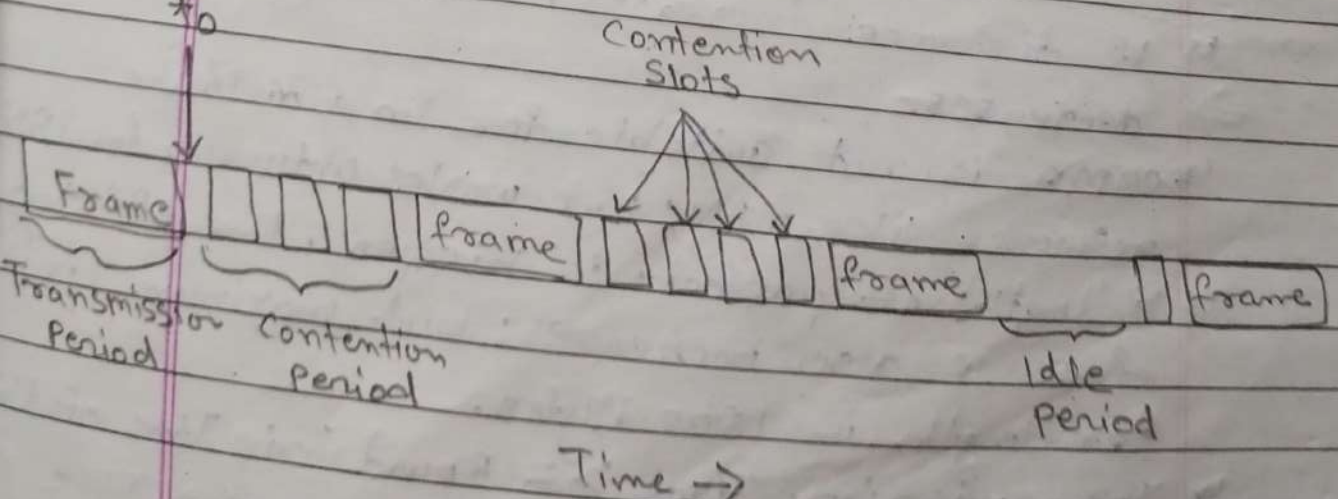


* Non-Persistent CSMA -
  - Before sending, a station senses the channel if no one else is sending, the station begins doing so itself.
  - However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
  - Instead, it waits a random period of time and then repeats the algorithm. Consequently this algorithm leads to better channel utilization but longer delays than 1-persistent CSMA.

* P-persistent CSMA -
  - It applies to slotted channels.
  - When a station becomes ready to send, it senses the channel.
  - If it is idle, it transmits with a probability P.
  - With a probability Q = 1 - P, it defers until the next slot.
  - If that slot is also idle, it either transmits or defers again, with probabilities P and Q.
  - This process is repeated until either the frame has been transmitted or another station has begun transmitting.
  - In the later case, the unlucky station acts as if there had been a collission (i.e., it waits a random time and starts again).
  - If the station initially senses the channel busy it waits until the next slot and applies the above algo

* 0-Persistent CSMA :-
↳ Each node is assigned a transmission order by a supervisory node.

⇒ CSMA/CD - (wired)
↳ If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
↳ Rather than finish transmitting their frames, which are irretrievably garbled anyway, they should abruptly stop transmitting as soon as the collission is detected.
↳ Quickly terminating damaged frames saves time and bandwidth.
↳ This protocol, known as CSMA/CD is widely used on LANs in the MAC sublayer.
↳ Access method used by Ethernet : CSMA/CD.
↳ At the point marked t_0, a station has finished transmitting its frame.



↳ Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision.

↳ Collisions can be detected by looking at the power of pulse width of the received signal and comparing it to the transmitted signal.

↳ After a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.

↳ Therefore, model for CSMA/CD will consist of alternating contention and transmission periods, with idle periods occuring when all stations are quiet.

Formula

↳ Efficiency $= \frac{1}{1+6.44 \times a}$

↳ $a = \frac{T_p}{T_t}$

↳ If distance increases, efficiency of CSMA decreases.

↳ CSMA is not suitable for long distance networks like WAN; but works optimally for LAN

↳ If length of packet is bigger, the efficiency of CSMA also increases; but maximum limit for length is 1500 Bytes.

↳ Transmission Time >= Round Trip Time of

↳ Transmission Time >= 2* propogation Time

1) Interframe space
2) Contention window
3) Acknowledgement

(wireless)

* CSMA/CA (Collision Avoidance)

↳ CSMA/CA is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by beginning transmission only after the channel is sensed to be "idle".

↳ It is particularly important for wireless networks, where the collision detection of the alternative CSMA/CD is not possible due to wireless transmitters desensing their receivers during packet transmission.

↳ CSMA/CA is unreliable due to the hidden node problem and exposed terminal problem.

↳ Solution:- RTS/CTS exchange.

↳ CSMA/CA is a protocol that operates in the Datalink layer.

↳ The access method used by IEEE 802.11 Wi-Fi is CSMA/CA

H.W Find the correct box:—

Multiple Access Method used by Ethernet : CSMA/CA Wi-Fi : CSMA/CD	Multiple Access method used by Ethernet : CSMA/CD Wi-Fi : CSMA/CA

* Controlled Access Protocol -

⇒ Reservation —

↳ A station need to make a reservation before sending data.

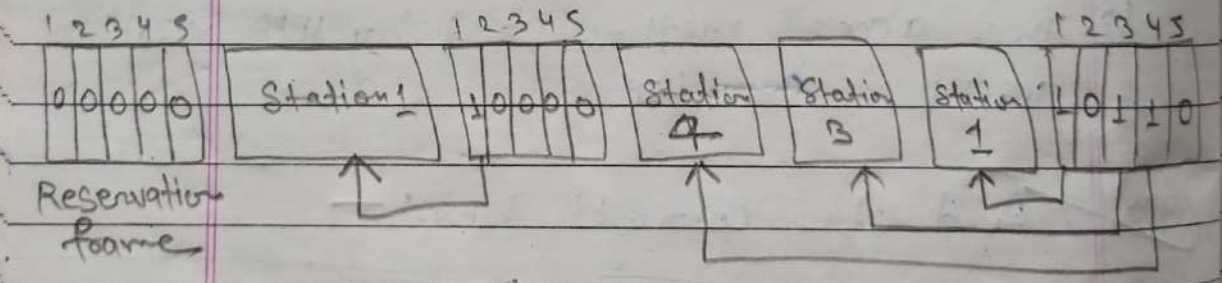
↳ In each interval, a reservation frame precedes the data frames sent in that interval.

↳ If there are N stations in the system, there are exactly N reservation minislots in the reservation frame.

↳ Each minislot belongs to a station.

↳ When a station needs to send a data frame, it makes a reservation in its own minislot.

↳ The stations that have made reservations can send their data frames after the reservation frame.



⇒ Polling -

↳ The polling protocol requires one of the nodes to be designated as a Master node (Primary Station).

↳ The master node polls each of the nodes in a round-robin fashion.

↳ In particular, the master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum no. of frames.

↳ After node 1 transmits some frames, the master node tells node 2 it (node 2) can transmit up to the maximum no. of frames.

↳ The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel.

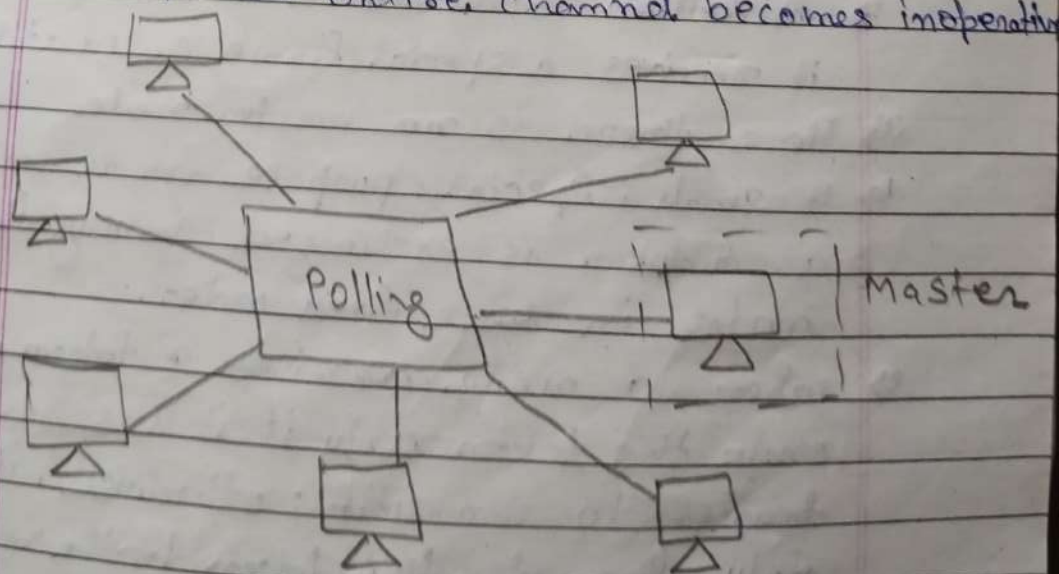
↳ The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.

↳ The polling protocol eliminates the collision.

↳ This allows polling to achieve a much higher efficiency.

↳ The first drawback is that the ~~channel~~ protocol introduces a polling delay - the amount of time required to notify a node that it can transmit.

↳ The second drawback, which is potentially more serious, is that if the master node fails, the entire channel becomes inoperative



⇒ Polling - functions —

* Poll function :- If the primary wants to receive data, it asks the secondaries if they have anything to send.

* Select function :- If the primary wants to send data, it tells the secondary to get ready to receive.

⇒ Efficiency of Polling —

Let T_{poll} be the time for polling and T_t be the time required for transmission of data. Then

$$\text{Efficiency} = \frac{T_t}{T_t + T_{poll}}$$

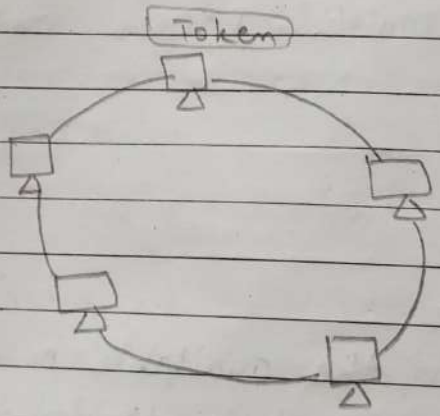
✗ Token Passing —

↳ A station is authorized to send data when it receives a special frame called a token.
↳ Here there is no master node
↳ A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order.
↳ When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node.

↳ If a node does have frames to transmit when it receives the token, it sends up to a maximum no. of frames and then forwards the token to the next node.

↳ Token passing is decentralized and highly efficient. But it has problems as well.

↳ For example, the failure of one node can crash the entire channel. Or if a node accidently neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.



⇒ Performance of Token Passing —

$$S = \frac{1}{1 + a/N} \quad ; \text{ for } a < 1$$

$$S = \frac{1}{a(1 + 1/N)} \quad ; \text{ for } a > 1$$

$$a = \frac{T_p}{T_t}$$

S = Throughput
N = No. of Stations
T_p = Propogation Delay
T_t = Transmission Delay

Transmission Media :-

- Transmission is a multiple access method in which the available bandwidth of a link is shared in time, frequency or through code between different stations.
- Multiplexing - Multiplexing means multiple inputs are combined together and transmitted simultaneously in a shared medium.
- Demultiplexing - Opposite of multiplexing.

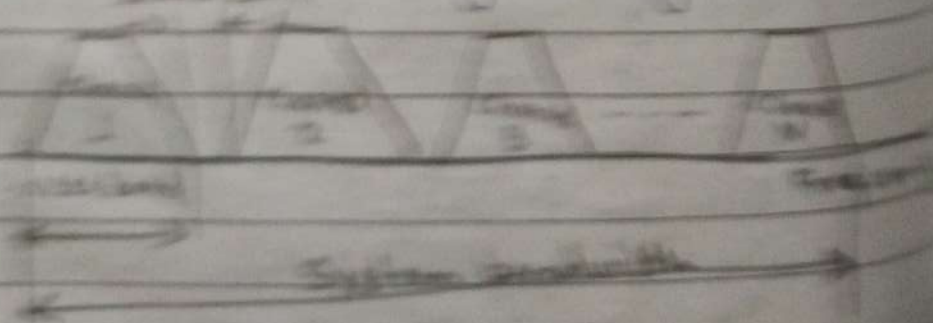
Different Multiplexing Techniques -

1. FDMA
2. TDMA
3. CDMA

- FDMA :-

In FDMA, the available bandwidth of the common channel is divided into bands that are allocated to different users.

- The available bandwidth is shared by all users.
- The FDMA is a physical layer protocol that uses FDM at the physical layer.



⇒ TDMA :-

↳ In TDMA, the bandwidth is just one channel that is time shared b/w different stations.

↳ The entire bandwidth is just one channel

↳ Stations share the capacity of the channel in time.

⇒ CDMA :-

↳ In CDMA, one channel carries all transmissions simultaneously.

↳ CDMA differs from FDMA because only one channel occupies the entire bandwidth of the link.

↳ It differs from TDMA because all stations can send data simultaneously; there is no time sharing

⇒ The assigned codes have two properties :-

1. If we multiply each node by another, we get 0
2. If we multiply each code by itself, we get 4 (the no. of stations).

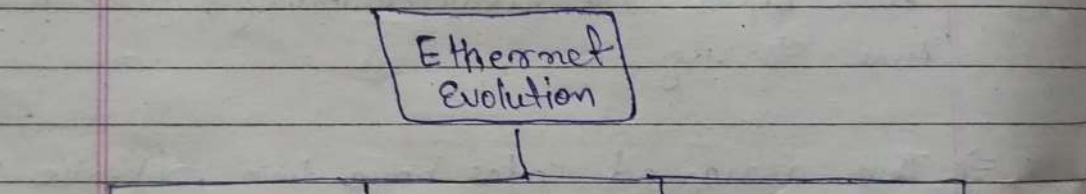
Ex :-

$$\text{Data} = (d_1c_1 + d_2c_2 + d_3c_3 + d_4c_4) \times c_1 = 4 \times d_1$$

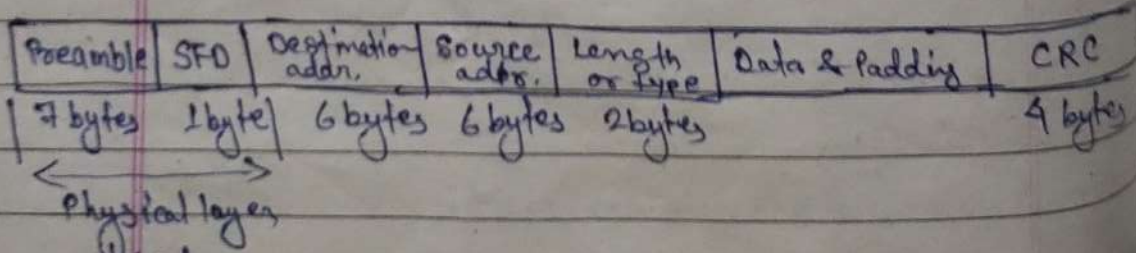
[Ethernet]

↳ One of the most widely used wired LAN technologies.
↳ Operates in the datalink layer and the physical layer.
↳ Family of networking technologies that are defined in the IEEE 802.2 and 802.3 Stands
↳ Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100000 Mbps (100 Gbps)

Ethernet Standards —
↳ Define Layer 2 protocols and layer 1 technologies.
↳ Two Separate Sublayers of the datalink layer to operate :- LLC & MAC



* ~~Preamble~~; Frame Format :-
Synchronization
Preamble :- 56 bits of alternating 1s and 0s.
SFD :- Start frame delimiter, flag (10101011)



* Ethernet frame - MIN and MAX Length

Min payload leng :- 46 bytes
Max payload length :- 1500 bytes

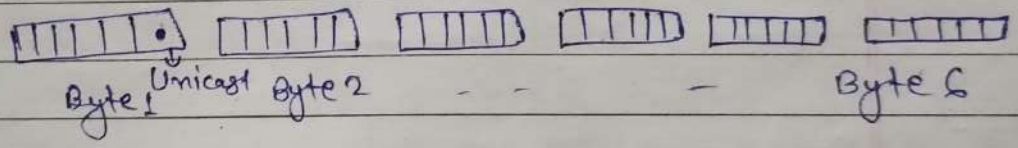
Destination addr	Source addr	Length PDU	Data & Padding	CRC
6 bytes	6 bytes	2 bytes		4 bytes

Minimum frame length :- 512 bits or 64 bytes
Maximum frame length :- 1518 bytes

* Ethernet Address —

↳ Example :- 06:01:02:01:2C:4B

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.
↳ If the bit is 0, the address is unicast; otherwise, it is multicast
↳ If all bits are 1, then it is broadcast addres

[Network Layer]

Addressing - IPv4 Addresses - Classful Addressing Classless Addressing - Subnetting - Network Address Translation (NAT) - IPV6 Addresses - Advantages - Transition from IPV4 to IPV6 - Delivery - Forwarding - Routing - Unicast Routing Protocols - Multicast Routing Protocols

⇒ IPV4 Address -

↳ 32 bits

2^{32} address - (Address Space) 4,294,967,296

Notation

Binary — dotted decimal

* Binary Notation:- 01110101 10010101 00011101 00000010
* Dotted Notation:- 117.149.29.2

(Only 4 octets) - A, B, C, D

$0 \le A, B, C, D \le 255$

0.0.0.0 to 255.255.255.255

* Hexadecimal Notation:-

01110101 10010101 00011101 11101010

75 95 1D EA

0x7595 1DEA

Q. Change the IP from binary to dotted notati.

01110111 :-

$= 1\times2^7 + 1\times2^6 + 1\times2^5 + 0\times2^4 + 1\times2^3 + 1\times2^2 + 1\times2^1 + 1\times2^0$

$= 128 + 64 + 32 + 0 + 8 + 4 + 2 + 1$

$= 239$ A

10000001 00001011 00001011 11101111

= 129.11.11.239 A

128 64 32 16 8 4 2 1

A 10
B 11
C 12
D 13
E 14
F 15

14 / 15

14 / 2 = 7 rem 0
7 / 2 = 3 rem 1
3 / 2 = 1 rem 1
1 / 2 = 0 rem 1

1110

192 | 127
32 | 128
224 | 255
15 | 239

Q.2 111.56.45.78

⇒ 01101111 00111000 00101101 01001110

Q.3 1000 0001 0000 1011 0000 1011 1110 1111

(change it in Hexadecimal notation)

8 1 0 B 0 B E F

⇒ 0X810B0BEF or $810B0BEF_{16}$

Classful Addressing

* Classes of IPV4 address —

⇒ Binary Notation —

i) Class A – 0
ii) Class B – 10
iii) Class C – 110

] Used for General purpose

iv) class D – 1110] → Used for multicast purpose
v) class E – 1111] → Used for Experimental purpose

⇒ ~~Dec~~ Dotted-Decimal Notation —

i) Class A :– 0 – 127
ii) Class B :– 128 – 191
iii) Class C :– 192 – 223
iv) class D :– 224 – 239
v) class E :– 240 – 255

* Subnet Mask -

Class A :- 255.0.0.0 N.H.H.H
Class B :- 255.255.0.0 N.N.H.H
Class C :- 255.255.255.0 N.N.N.H

Class A :- Network - 2^7 128 Net
Host - $(2^{24}-2)$ 16,777,214 hosts

Class B :- Network - 2^{14} Nets (16,384 Nets)
Host - $(2^{14}-2)$ 65,534 hosts

Class C :- Network - 2^{21} (209150 Nets)
Host - 2^8-2 (254 hosts)

Note:- For Host portion
1st bit (0) is reserved for Network
Last bit (255) is reserved for broadcast address

* Subnet mask (Slash notation -

	Decimal Notation	Slash Notation
Class A	255.0.0.0	/8
Class B	255.255.0.0	/16
Class C	255.255.255.0	/24

* To define the n/w and host portions of an address, a devices use a separate 32-bit pattern called a subnet mask.

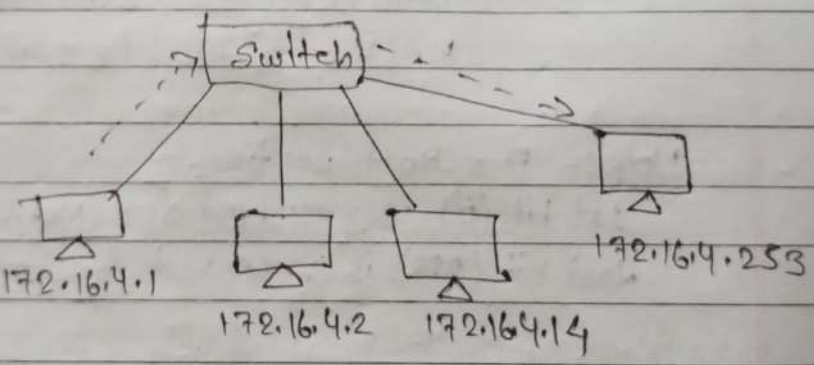
⇒ The subnet mask does not actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address.

⇒ Unicast, Multicast and Broadcast Addre

- Unicast communication is One-to-one.
- Multicast :- one-to-many
- Broadcast :- one-to-all

* Unicast Transmission :- The process of sending a packet from one host to an individual host.

Source : 172.16.4.1
Destination : 172.16.4.253



* Broadcast Transmission :- The process of sending a packet from one host to all hosts in the network.

⇒ Limited Broadcast
Destination :- 255.255.255.255
Routers do not forward a limited broadcast

⇒ Directed Broadcast
Destination :- 172.16.4.255
Hosts within the 172.16.4.0/24 network

* Multicast Transmission :- The process of sending a packet from one host to a selected group of hosts, possibly in different networks.

→ Multicast transmission reduces traffic.
→ The Multicast Address range : 224.0.0.0 to 239.255.255.255
→ Link local - 224.0.0.0 to 224.0.0.255
Example:- routing info. exchanged by routing protocol
→ Globally scoped addresses :- 224.0.1.0 to 238.255.255.255 (
Example: 224.0.1.1 has been reserved for Network Time protocol)

Q:- A host in a class C n/w has been assigned an IP address 192.168.17.9. Find the no. of addresses in the block, the first addresses and the last addresses.

Sol:-
Class C N/w
N.N.N.H

192.168.17.9
This n/w :- 192.168.17.0 — 192.168.17.255
No. of Address = 2^8 = 256
No. of usable address = 256 - 2 = 254
First address :- 192.168.17.0 (N/w address)
Last address :- 192.168.17.255 (Broadcast addr)

Q An address in a block is given as 185.28.17.9. Find the no. of addresses in the block, the 1st address and the last address.

Soln: class B address.
N.N.H.H
~~Total no~~ 185.28.0.0 to 185.28.255.255
(start) (End)

Q An organization follows class A for their internal network. One of the hosts in the network has an IP address 10.200.240.4. Find the no. of addresses, the network address, and the broadcast address of the organization's network.

Sol Class A n/w
N.H.H.H (255.0.0.0 or /8)
10. 200.240.4
N H

This n/w :- 10.0.0.0 ← 10.255.255.255
No. of address :- 2^{24} = 16,777,216
No. of usable adress = 16,777216 - 2 = 16777
First adress = 10.0.0.0.
last adress = 10.255.255.255
(Broadcast)

⇒ Public and Private IP :-

* Early n/w design, when global end-to-end connectivity was envisioned for communication with all internet hosts, intended that IP addresses be globally unique. However, it was found that this was not always necessary as private n/w developed and public address space needed to be conserved.

* Computers not connected to the internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses. Today such private n/w are widely used and typically connect to the internet with NAT, when needed.

⇒ Private IP address —

Class A :- 10.0.0.0 to 10.255.255.255
(10.0.0.0/8)

Class B :- 172.16.0.0 to 172.31.255.255
(172.16.0.0/12)

Class C :- 192.168.0.0 to 192.168.255.255
(192.168.0.0/16)

* The aforementioned are the 3 non-overlapping ranges of IPv4 addresses for private n/w are reserved.

Special use IPv4 addressing –

* Network and broadcast Addresses :- within each network the first and last addresses can't be assigned to hosts.

* Loopback address :- 127.0.0.1 a special address that hosts use to direct traffic to themselves (addresses 127.0.0.0 to 127.255.255.255 are reserved)

* Link-local address :- 169.254.0.0 to 169.254.255.255 (169.254.0.0/16) addresses can be automatically assigned to the localhost.

* Test-NET address :- 192.0.2.0 to 192.0.2.25 (192.0.2.0/24) set aside for teaching and learning purposes, used in documentation and network examples

* Experimental addresses :- 240.0.0.0 to 255.255.255.254 are listed as reserved

Classless Addressing

=> Drawbacks of Classful addressing -

* Lack of Internal Address Flexibility
* Insufficient use of Address Space
* Proliferation of Router Table Entries

Classless Addressing -

- Formal name is Classless Inter-Domain Routing (CIDR)
- Created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B or C address.

- Classless addressing is impossible with the help of subnetting.

	Bit value			Valid Subnet Masks				
Subnet value	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

⇒ Valid Submet masks →

/1 = 128.0.0.0
/2 = 192.0.0.0
/3 = 224.0.0.0
/4 = 240.0.0.0
/5 = 248.0.0.0
/6 = 252.0.0.0
/7 = 254.0.0.0
/8 = 255.0.0.0
/9 = 255.129.0.0
/10 = 255.192.0.0
/11 = 255.224.0.0
/12 = 255.240.0.0
/13 = 255.248.0.0
/14 = 255.252.0.0
/15 = 255.254.0.0
/16 = 255.255.0.0
/17 = 255.255.128.0
/18 = 255.255.192.0
/19 = 255.255.224.0
/20 = 255.255.240.0
/21 = 255.255.248.0
/22 = 255.255.252.0
/23 = 255.255.254.0
/24 = 255.255.255.0
/25 = 255.255.255.128
/26 = 255.255.255.192
/27 = 255.255.255.224
/28 = 255.255.255.240
/29 = 255.255.255.248
/30 = 255.255.255.252
/31 = 255.255.255.254
/32 = 255.255.255.255

256 128 64 32 16 8 4 2 1

Page No.:
Date: / /

77

Subnetting

↳ A subnetwork or subnet is a logical subdivision of an IP network.

↳ The practice of dividing a network into two or more networks is called subnetting.

↳ Computers that belong to a subnet are addressed with an identical most-significant bit-group in their IP addresses.

⇒ Subnetting - 5 Steps

1. Identify the class of the IP address and note the Default Subnet Mask.
2. Convert the Default Subnet Mask into Binary.
3. Note the no. of hosts required per subnet and find the Subnet Generator (SG) and octet position.
4. Generate the new subnet mask.
5. Use the SG and generate the n/w ranges (Subnets) in the appropriate octet position.

Q. Subnet the IP address 216.21.5.0 into 30 hosts in each subnet.

Sol:- Step1:- Class C (Subnet:- 255.255.255.0)
Step2:- 11111111.11111111.11111111.00000000
Step3:- No. of hosts/subnet:- 30 (11110)
SG:- 32
octet position:- 4

128 64 32 16 8 4 2 1

192

11000

78

11 8 4 2 1

11111111.11111111.11111111.111 00000

Step4:- New Subnet Mask:-
255.255.255.224 or /27

Step5:- Network Ranges (Subnets)
216.21.5.0 – 216.21.5.31
216.21.5.32 – 216.21.5.63
216.21.5.64 – 216.21.5.95
216.21.5.96 – 216.21.5.127
216.21.5.128 – 216.21.5.159
and so-on.

Q.2 Subnet the IP address 196.10.20.0 into 52 hosts in each subnet.

Soln:- Step1:- Class C (Subnet:- 255.255.255.0)
Step2:- 11111111.11111111.11111111.00000000
Step3:- No. of hosts/subnet:- 52 (110100)
SG:- 64 ~~6 bits~~
Octet Position:- 4
11111111.11111111.11111111.11000000

Step4:- New subnet mask:-
255.255.255.192 or /26

Step5:- Network Ranges – (Subnets)
196.10.20.0 – 196.10.20.63
196.10.20.64 – 196.10.20.127
196.10.20.128 – 196.10.20.191
and so on
196.10.20.192 – 196.10.20.255

Q3 Subnet the IP address 150.15.0.0 into 500 hosts in each subnet.

Sol:- Step 1:- Class B (255.255.0.0)
Step 2:- 11111111.11111111.00000000.00000000
Step 3:- No. of hosts/Subnets :- 500 (111110100)
SG :- 2
Octet Position :- 3
11111111.11111111.11111110.00000000

Step 4:- New Subnet masks -
255.255.254.0 or /23
Step 5:- Network Ranges -
150.15.0.0 - 150.15.1.255
150.15.2.0 - 150.15.3.255
150.15.4.0 - 150.15.5.255
150.15.6.0 - 150.15.7.255
150.15.8.0 - 150.15.9.255.

$2^9 = 512$ Hosts per N/w (Subnet)
$2^7 = 128$ Subnets (Networks)

Q4 Subnet the IP address 10.0.0.0 into 100 hosts in each subnet.

Sol:- Step 1:- Class A (255.0.0.0)
Step 2:- 11111111.00000000.00000000.00000000
Step 3:- No. of hosts/Subnets :- 100 (1100100)
SG :- 128
Octet Position :- 4
11111111.11111111.11111111.10000000

Step 4 :- New Subnet mask
255.255.255.128 or /25

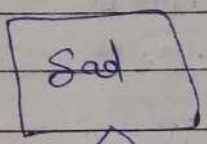
Step 5 :- Network Ranges -
10.0.0.0 — 10.0.0.127
10.0.0.128 — 10.0.0.255
10.0.1.0 — 10.0.1.127
10.0.1.128 — 10.0.1.255
10.0.2.0 — 10.0.2.127

2^7 = 128 Hosts per N/w
2^{17} = 131072 Network

Troubleshoot the connectivity issue in the given subnet.

Troubleshooting 1

Q. Change the mood of the host from sad to happy.



192.168.1.127
255.255.255.224

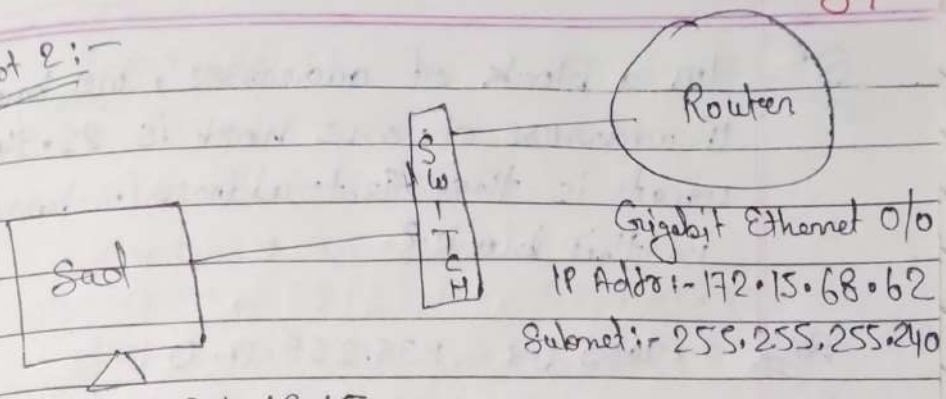
Sol:-

11111111.11111111.11111111.11100000
SG :- 32
Network ranges =
192.168.1.0 - 192.168.1.31
192.168.1.32 - 192.168.1.63
192.168.1.64 - 192.168.1.95
192.168.1.96 - 192.168.1.127
192.168.1.128 - 192.168.1.159

It is assigned to comp but it is not assigned because it is broadcast address

New IP address :- 192.168.1.126 = Computer Happy

Troubleshoot 2:-



IP Address:- 172.15.68.65
Subnet:- 255.255.255.240
Default Gateway:- 172.15.68.62

Soln:- 11111111.11111111.11111111.11110000

SG :- 16

Network Ranges :-

172.15.68.0 — 172.15.68.15
172.15.68.16 — 172.15.68.31
172.15.68.32 — 172.15.68.47
172.15.68.48 — 172.15.68.63 → Router
172.15.68.64 — 172.15.68.79 → Comp. lies
172.15.68.80 — 172.15.68.95 "

⇒ Here computer and Router both are in diff. network so, they can't be able to talk to resolve this we can either change Router address within computer address. 172.15.68.66
or, we can change comp. IP address within Router network range 172.15.68.60

172.15.68.60

Q5 In a block of addresses, we know the IP address of one host is 25.34.12.56/16 what is the first address (network address) in this block?

Sol:- Class B :- 255.255.0.0

11111111.11111111.00000000.00000000

SG :- 1 octet Position = 2

Network Ranges -

- 25.34.0.0 — 25.34.255.255
- 25.35.0.0 — 25.35.255.255
- 25.36.0.0 — 25.36.255.255
- 25.37.0.0 — 25.36.255.255

Ans :- 25.34.0.0

2nd Approach

25.34.12.56

IP → 00011001.00100010.00001100.00111000

Subnet → 11111111.11111111.00000000.00000000

Binary AND → 00011001.00100010.00000000.00000000

25.34.0.0 ✓

Q. In a block of addresses, we know the IP address of one host is 182.44.82.16/26 what is the first address (network add in this block?

Soli:- 1st Approach

11111111.11111111.11111111.11000000

SG = 64 , octet = 4

Network Ranges -

⇒ 182.44.82.0 - 182.44.82.63

182.44.82.64 - 182.44.82.127

182.44.82.128 - 182.44.82.191

182.44.82.192 - 182.44.82.255

256

Ans ⇒ 182.44.82.0

2nd Approach

Subnet → 11111111.11111111.11111111.11000000

IP → 10110110.00101100.01010010.00010000

Binary AND → 10110110.00101100.01010010.00000000

182.44.82.0 ✓

Q6 In a block of addresses, we know the IP address of one host is 25.34.12.56/16 what is the last address (limited broadcast address) in this block?

Soli:- 11111111.11111111.00000000.00000000

SG :- 1 , octet = 2

⇒ 25.34.0.0 - 25.34.255.255

25.35.0.0 - 25.35.255.255

25.36.0.0 - 25.36.255.255

Broadcast Address :- 25.34.255.255

2nd Approach :- On bitwise OR

25 . 34 . 12 . 56

IP → 00011001 . 00100010 . 00001100 . 00111000
Subnet → 11111111 . 11111111 . 00000000 . 00000000
1's Compl of Subnet 00000000 . 00000000 . 11111111 . 11111111

Bitwise OR 00011001 . 00100010 . 11111111 . 11111111

25 . 34 . 255 . 255 ✓

Q. In a block of addresses, we know the IP adress of one host is 182.44.82.16/26 what is the last address in this block?

Sol:- 188 . 44 . 82 . 16

IP → 10111100 . 00101100 . 01010010 . 00010000
Subnet → 11111111 . 11111111 . 11111111 . 11000000
Subnet 1's → 00000000 . 00000000 . 00000000 . 00111111

10111100 . 00101100 . 01010010 . 00111111

188 . 44 . 82 . 31 ✓

Page No.
Date : / / .

Q7 An organization has a class B network and wishes to form subnets for 64 departments. The subnet mask would be.

a) 255.255.0.0
b) 255.255.64.0
c) 255.255.128.0
d) 255.255.252.0

Sol:- 11111111.11111111.00000000.00000000

$2^{\text{No. of 1s}}$:- Total no. of subnets
$2^{\text{No. of 0's}}$:- Total no. of Hosts / Subnets
Total no. of subnets required = 64 (2^6)

Reserve 6 1s in 3rd octet
11111111.11111111.111111 00.00000000
New Subnet Mask : 255.255.252.0

Q8 If a class B network on the Internet has a subnet mask of 255.255.248.0 what is the maximum no. of hosts per subnet?

Sol^n:- Given Subnet:- 255.255.248.0

a) 1022
b) 1023
c) 2046
d) 2047

11111111.11111111.11111000.00000000
2^5 = 32 subnets possible
2^{11} = 2048 - 2 hosts possible/subn
= 2046

Q9 The address of a class B host is to be split into subnets with a 6-bit subnet no. what is the maximum no. of subnets and the maximum no. of hosts in each subnet?

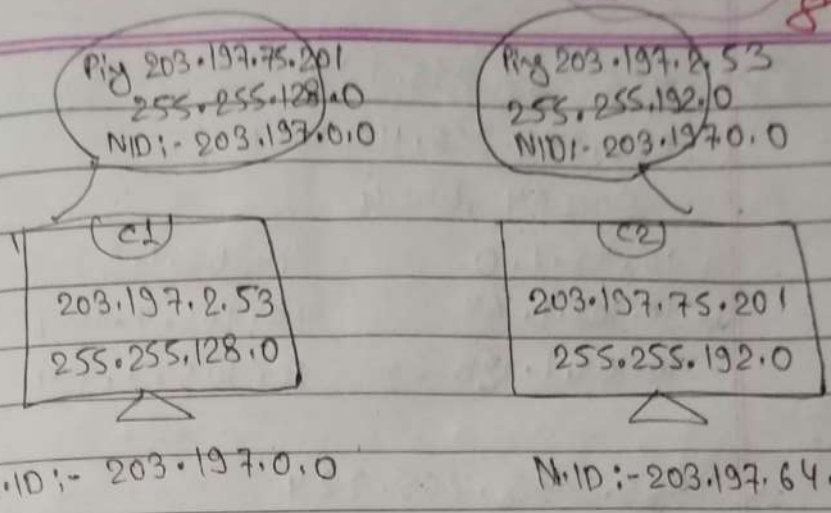
a) 62 subnets and 262142 hosts
b) 64 subnets and 262142 hosts
c) 62 subnets and 1022 hosts
d) 64 subnets and 1024 hosts

Sol:- Class B subnet mask 255.255.0.0
6 bits are used for subnetting
255.255.11111100.00000000
New Subnet:- 255.255.252.0
2^6 = 64 subnets (Maximum 64-2 = 62)
2^{10} = 1024 hosts (Maximum 1024-2 = 1022)

Q10 Two computers C1 and C2 are configured as follows. C1 has IP address 203.197.2.53 and netmask 255.255.128.0. C2 has IP address 203.197.75.201 and netmask 255.255.192.0. which one of the following statement is true?

a) C1 and C2 both assume they are on the same network
b) C2 assumes C1 is on same n/w, but C1 assumes C2 is on a diff. network.
c) C1 assumes C2 is on same n/w, but C2 assumes C1 is on a different n/w
d) C1 and C2 both assume they are on different networks

Sol:-



N.ID:- 203.197.0.0

N.ID:-203.197.64.0

Q11 Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use the same netmask N. which of the values of N given below should not be used if A and B should belong to the same network?

Solⁿ:- a) 255.255.255.0
b) 255.255.255.128
c) 255.255.255.192
d) 255.255.255.224

⇒ 255.255.255.0

255.255.11111111.00000000

SG = 1 , OP = 3 (✓)

10.105.1.0 — 10.105.1.255

10.105.2.0 — 10.105.2.255

⇒ 255.255.255.128

255.255.255.10000000

SG = 128, OP = 4 (✓)

10.105.1.0 — 10.105.1.127

10.105.1.128 — 10.105.1.255

⇒ 255.255.255.192

255.255.255.11000000

SG=64, OP=4

10.105.1.0 — 10.105.1.63

10.105.1.64 — 10.105.1.127 (✓)

10.105.1.128 — 10.105.1.191

⇒ 255.255.255.224

255.255.255.11100000

SG=32, OP=4

10.105.1.0 — 10.105.1.31 (✗)

10.105.1.32 — 10.105.1.63

10.105.1.64 — 10.105.1.95

10.105.1.96 — 10.105.1.127

Q12 In the IPv4 addressing format, the no. of networks allowed under class C address is

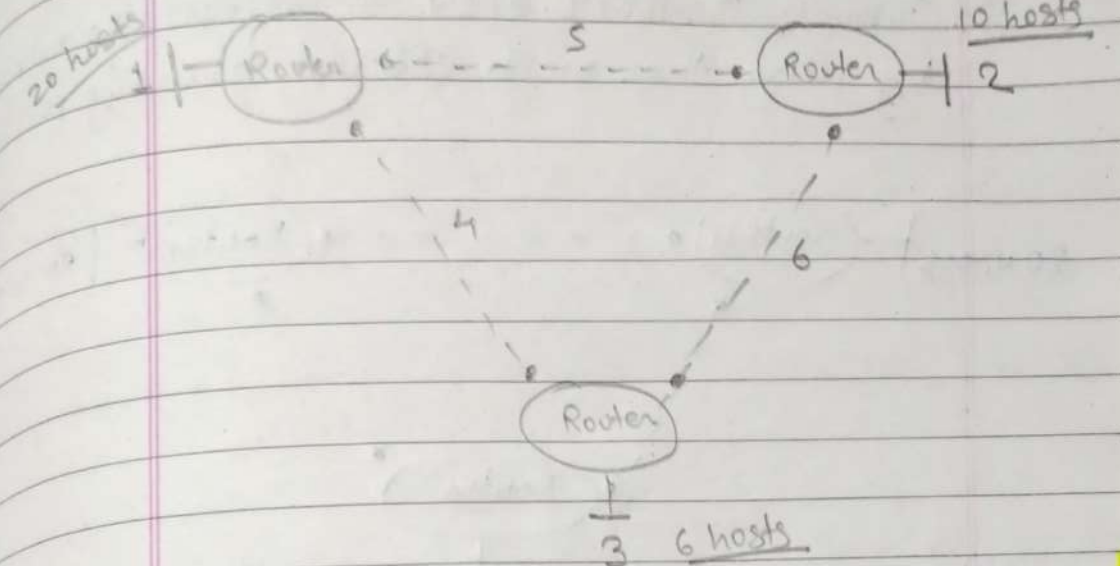
a) 2^{14}

b) 2^{7}

c) 2^{21}

d) 2^{24}

⇒ Fixed Length Subnet Masking (FLSM)



* Classful Addressing -

216.21.5.0 — 216.21.5.255 (1)
216.21.6.0 — 216.21.6.255 (2)
216.21.7.0 — 216.21.7.255 (3)
216.21.8.0 — 216.21.8.255 (4)
216.21.9.0 — 216.21.9.255 (5)
216.21.10.0 — 216.21.10.255 (6)

Subnet Mask :-

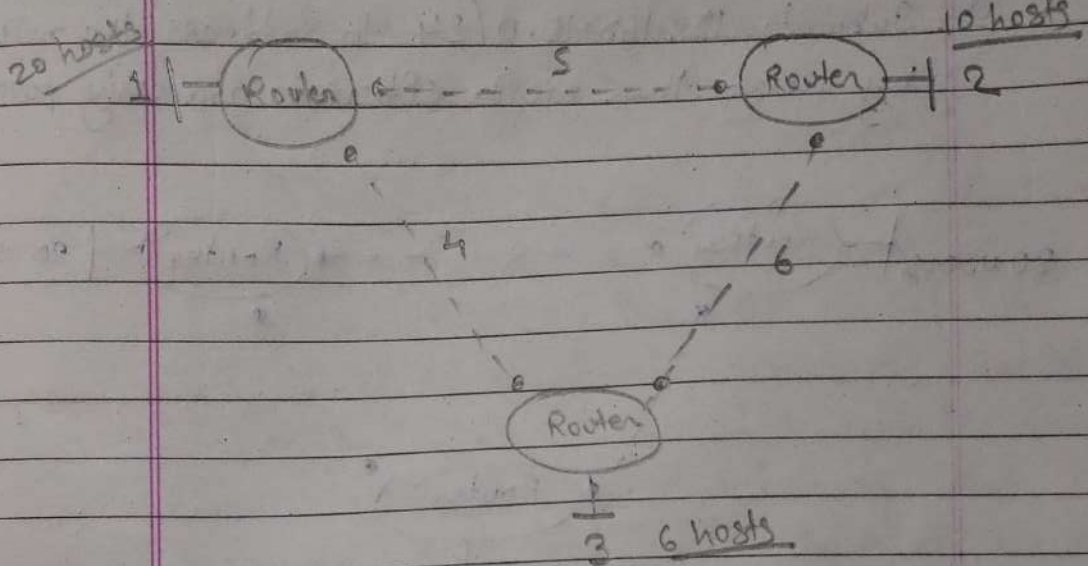
255.255.255.0 or /24

* Classless Addressing -

216.21.5.0 — 216.21.5.31 (1)
216.21.5.32 — 216.21.5.63 (2)
216.21.5.64 — 216.21.5.95 (3)
216.21.5.96 — 216.21.5.127 (4)
216.21.5.128 — 216.21.5.159 (5)
216.21.5.160 — 216.21.5.191 (6)

Subnet Mask :- 255.255.255.224 or /27

⇒ Fixed Length Subnet Masking (FLSM)



* Classful Addressing -

216.21.5.0 — 216.21.5.255 (1)
216.21.6.0 — 216.21.6.255 (2)
216.21.7.0 — 216.21.7.255 (3)
216.21.8.0 — 216.21.8.255 (4)
216.21.9.0 — 216.21.9.255 (5)
216.21.10.0 — 216.21.10.255 (6)

Subnet Mask :-

255.255.255.0 or /24

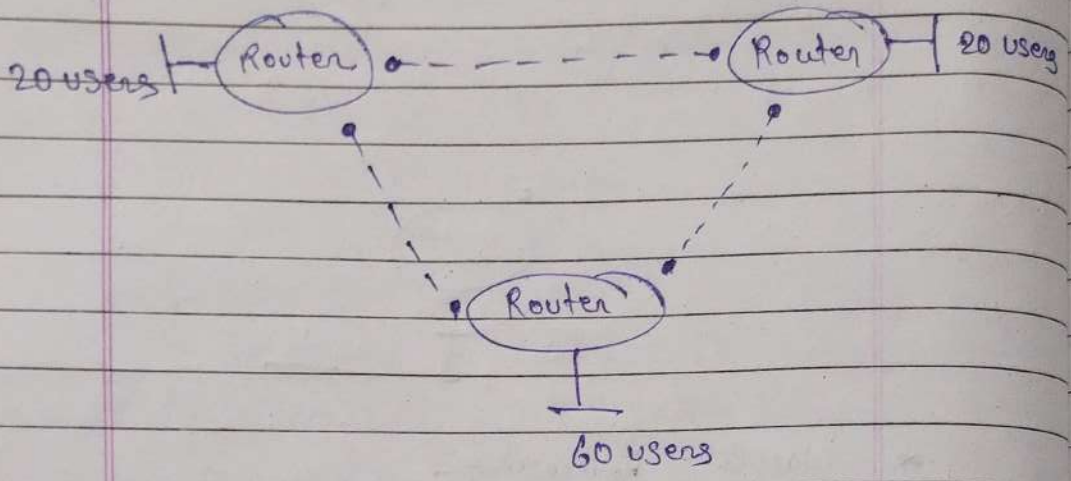
* Classless Addressing -

216.21.5.0 — 216.21.5.31 (1)
216.21.5.32 — 216.21.5.63 (2)
216.21.5.64 — 216.21.5.95 (3)
216.21.5.96 — 216.21.5.127 (4)
216.21.5.128 — 216.21.5.159 (5)
216.21.5.160 — 216.21.5.191 (6)

Subnet Mask :- 255.255.255.224 or /27

⇒ Variable length Subnet Masking

Q Subnet 192.168.10.0/24 to address the network by using the most efficient addressing possible.



Sol^n:- Class C - Default Subnet Mask : 255.255.255.0
11111111.11111111.11111111.00000000
No. of hosts :- 60
SG :- 4
Octet Position :- 4
11111111.11111111.11111111.11111100
New subnet mask :- 255.255.255.252 or /30
Network Ranges -

→ 192.168.10.0 - 192.168.10.63/26
(Handover this to 60 users Network)

→ 192.168.10.64 - 192.168.10.95/27
(Handover this to 20 users Network)

→ 192.168.10.96 - 192.168.10.127/27
(Handover this to another 20 users Network)

→ 192.168.10.128 - 192.168.10.131/30
(Handover this to Crossover Link)

→ 192.168.10.132 – 192.168.10.135/30
(Handover this to crossover Link)

→ 192.168.10.136 – 192.168.10.139/30
(Handover this to crossover Link

Q. An ISP has the following chunk of CIDR-based IP addresses available with it: 245.248.128.0/20. The ISP wants to give half of ~~them~~ this chunk of addresses to organization A, and a quarter to Organization B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B?

a) 245.248.136.0/21 and 245.248.128.0/22
b) 245.248.128.0/21 and 245.248.128.0/22
c) 245.248.132.0/22 and 245.248.132.0/21
d) 245.248.136.0/24 and 245.248.132.0/21

Sol:- 1. Subnet Mask: /20
11111111.11111111.11110000.00000000
2. No. of hosts = $2^{\text{No. of 0's}} = 2^{12}$
3. Handover quarter of the address to organization B = $2^{12}/4 = 2^{12}/2^2 = 2^{10}$
11111111.111111