Telecommunications Exam Solutions

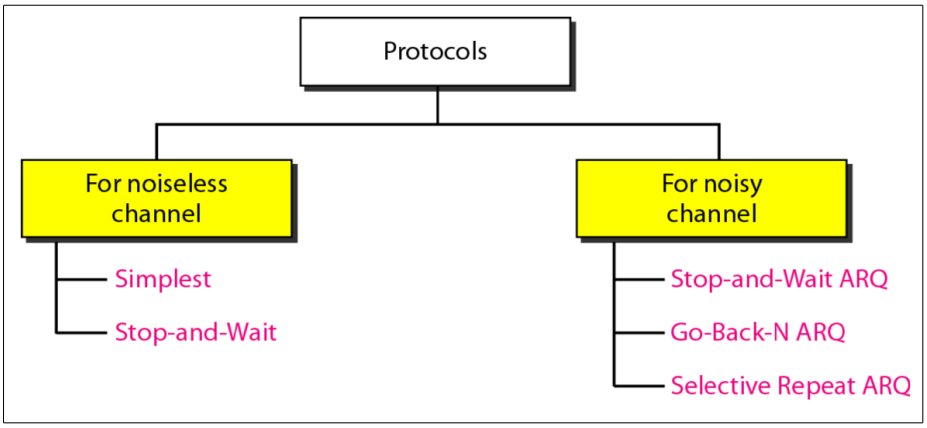
- Two hour Exam
- Answer 2 of 3 Questions
- 1 hour per question

2016 Exam:

Q1 (a) – Flow Control

I) Define the term 'flow control' and explain the trade-off in the design of flow control mechanisms by discussing a number of flow control mechanisms.

Flow Control is the method by which the amount of data transmitted to a receiver is controlled. It determines how packets are sent between two nodes within a telecommunication network and defies how errors should be handled.



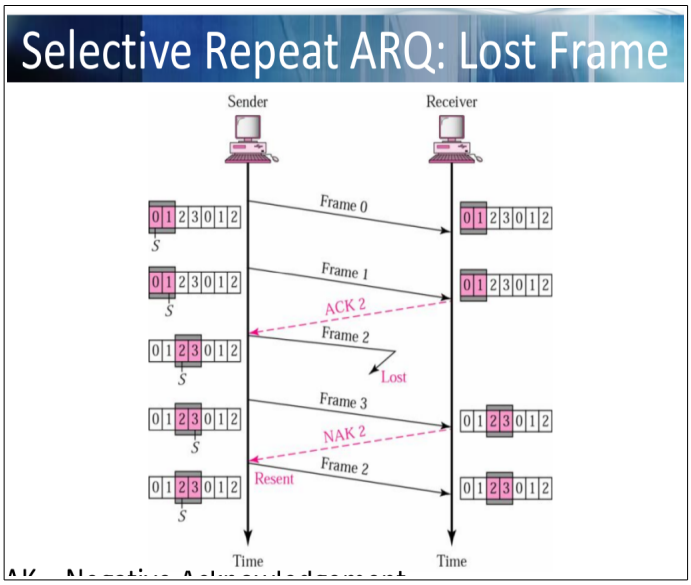
A) Stop-And-Wait ARQ: This is when a sender waits to receive an ACK from the receiver before sending the next packet. Good because it ensures no packets are lost, however it is time consuming and isn't very efficient.

B) Go-Back-N ARQ: This is when if an ACK for a specific frame has not been received within a given time frame the system re-sends all subsequent frames from the last ACK onwards. This is good because it allows transmission to continue, however all subsequent frames must be resent which is very ineffecient.

C) Selective Repeat ARQ: This is when a receiver keeps track of the frame it expects next, informing the sender also which frame it expects. If a receiver receives a packet that does not match the packet number it expected it returns an NAK informing the sender of which packet it is missing. This is good because it allows continuous transmission and it also enables individual packets to be resent rather than the entire transmission.

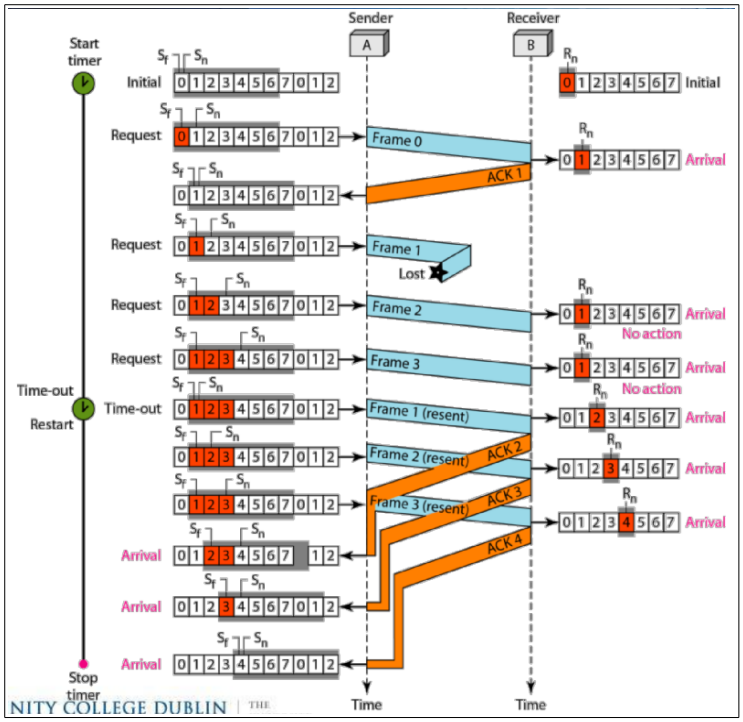
II) Assume that you are asked to provide a Selective Repeat mechanism and a Go-Back-N mechanism for communication between two stations A and B. Describe with the help of diagrams the exchange of 10 frames between A and B for both mechanisms.

1. Selective Repeat ARQ



- Frame 0 is the first packet sent between A and B.
- Frame 1 is then sent, receiver expected this frame, returns ACK2 (expects Frame 2 next)
- Frame 2 is lost, next frame received is Frame 3.
- This is the wrong frame so receiver returns NAK2 informing that it expected Frame 2.
- Frame 2 is resent.

2. Go-Back-N ARQ



- Frame 0 is sent, senders receives an ACK informing it that Frame 1 is expected next.
- Frame 1 is sent, but is lost. Transmission continues and no ACK is received within time period.
- Transmission is timed out. System goes back to last ACK and re-sends Frame 1.
- Transmission continues from here onwards and all subsequent are re-transmitted to receiver.

III) Discuss the advantages and disadvantages of a Selective Repeat Mechanism in comparison to a Stop-and-Wait mechanism.

By using a Selective Repeat Mechanism it enables you to fluidly transmit between a sender and a receiver whilst also handling any lost packets quite efficiently as only individual lost packets need to be resent.

In comparison, a Stop-and-Wait mechanism doesn't allow for fluid transmission as the sender must halt transmission and wait to receive an ACK from the receiver before transmitting the next frame. This is not ideal in a real-life situation where transmission times may be long and transmissions may expensive.

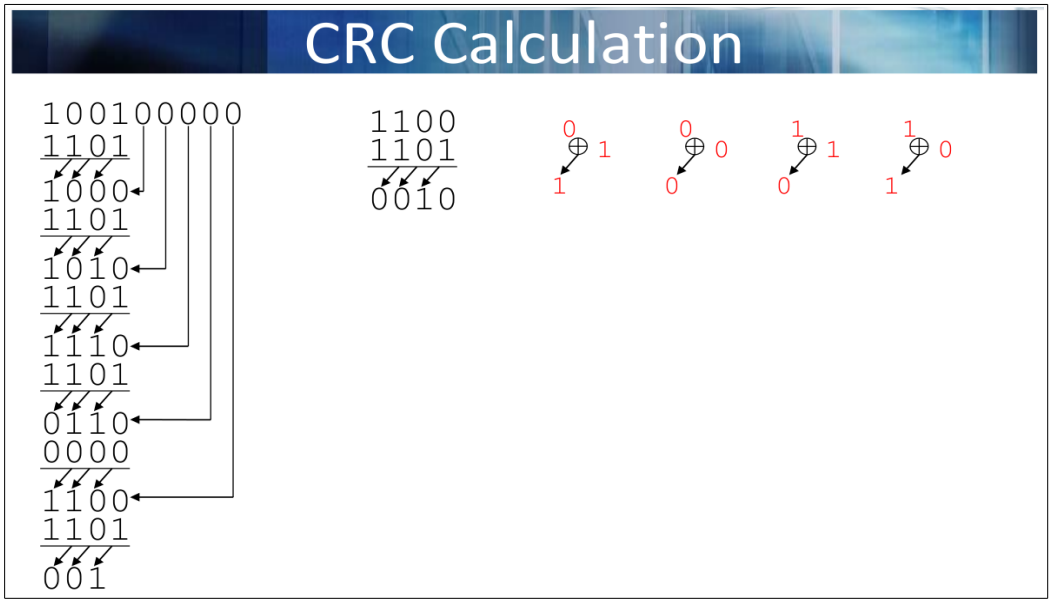
Q1 (b) – Cyclic Redundancy Checks

Cyclic-Redundancy Checksums (CRCs) may be used as error control mechanisms in the Link layer. Suppose we want to transmit the message 1011001001001011 and protect it from errors using the CRC-8 polynomial x^8+x^2+x+1.

I) Describe the calculation of a CRC and demonstrate the first four steps of the calculation.

When selecting the CRC devisor it should :

- Not be divisible by x
- Be divisibly by x+1



1. Divide Payload (+ MSB e.g x^3 * 0's for remainder) by selected CRC polynomial e.g 1101
2. Perform **XOR** between the bits, shifting left each bit
3. Carry down the next bit, perform the XOR operation again
4. Repeat until no more bits to carry down
5. Remainder is then your CRC value to be transmitted

1. *Polynomial x^8+x^2+x+1 to bit value:*

   $x^8+x^2+x+1 \rightarrow 100000111$ = CRC Divisor
   since x^8 ***ADD ON 8 0's***

2. *Divide first n message bits by CRC divisor*

```
1011001001001011[00000000]
100000111
-------------
011000111
```

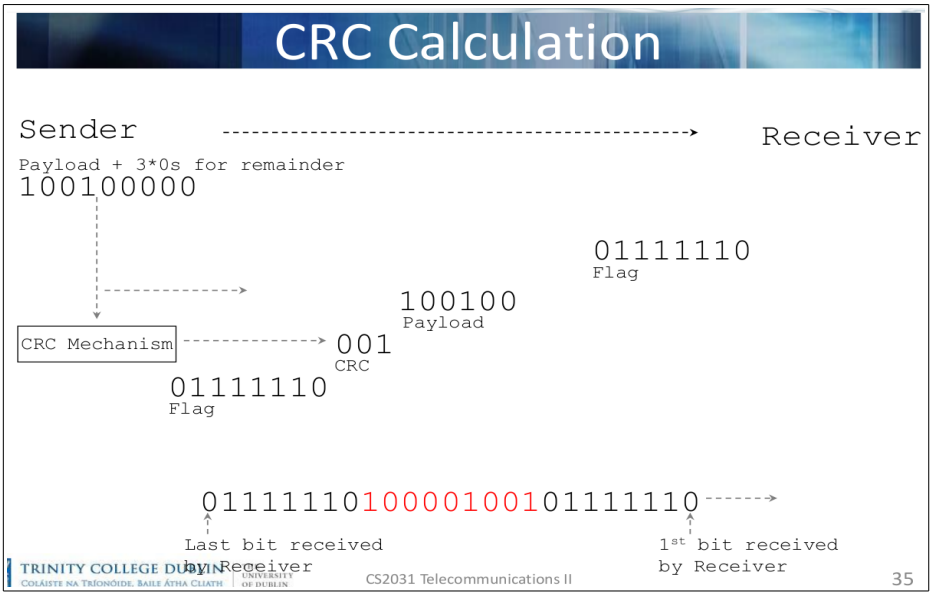
3. *Divide new remainder n message bits by CRC divisor*

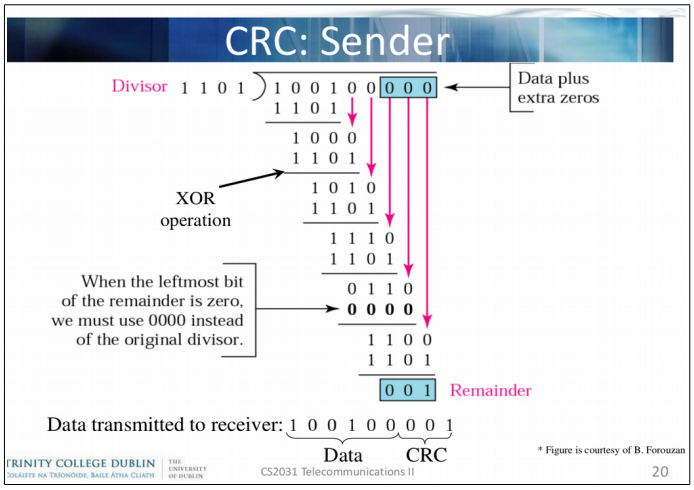
```
~~10110010010~~01011[00000000]
100000111
-------------
011000111
100000111
-------------
110000000
```

4. *Divide new remainder n message bits by CRC divisor*

```
~~101100100100~~1011[00000000]
100000111
-------------
011000111
100000111
-------------
110000000
100000111
-------------
100001110
```

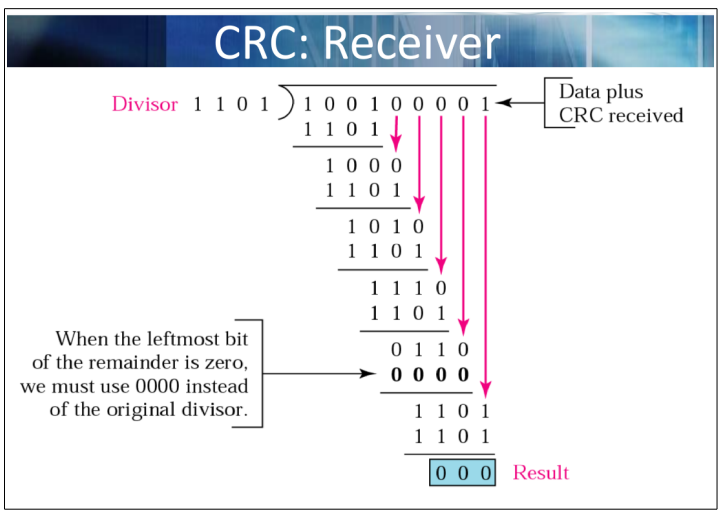
II) Show the data bits and CRC bits of the bit sequence that would be transmitted and discuss the interpretation of the possible outcomes of the calculation at the receiver





Sender Process:

1. The payload + 3*0s are sent to the CRC mechanism.
2. The CRC mechanism uses the CRC polynomial to calculate the CRC for the payload.
3. The packet is then formed in the form [FLAG] [CRC] [PAYLOAD] [FLAG].
4. Packet is sent to receiver.



Receiver Process:

1. The receiver receives a packet, extracts the payload + CRC.
2. The CRC mechanism divides the Payload+CRC by the polynomial.
3. If remainder is 0, correct bits, otherwise incorrect bits.

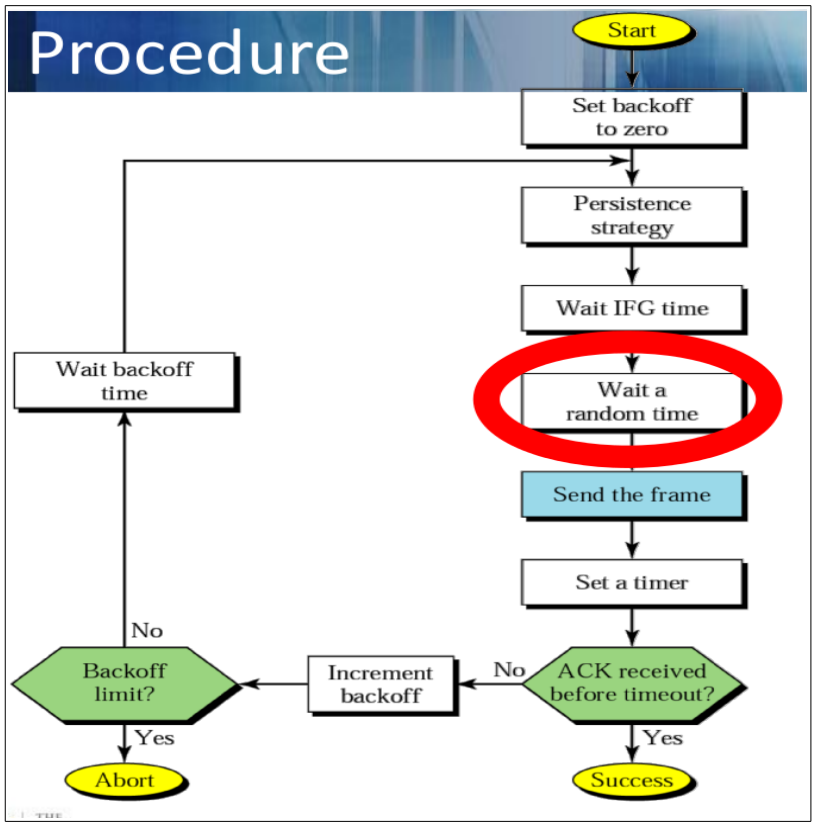
Q2 (a) – Multiple Access Control

Carrier Sense Multiple Access (CSMA) with Collision Detection (CA) and Time Division Multiple Access (TDMA) are used as a mechanism for medium access control in wireless networks.

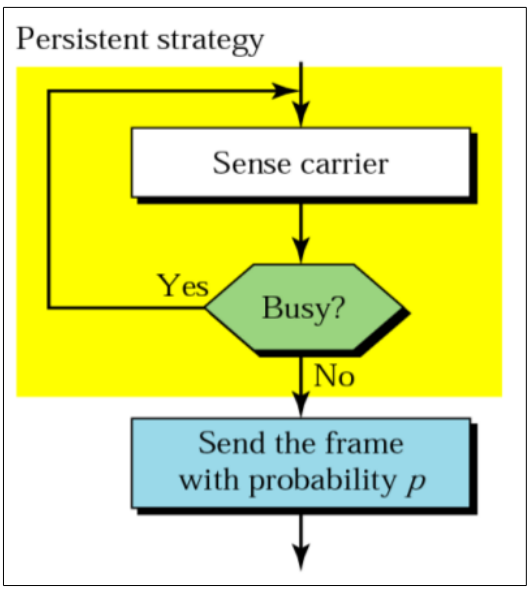
I) Assume that four stations use a wireless medium to commnicate. All stations intend to transmit data at the same time as other stations. The access to the medium is controlled by a CSMA/CA scheme or a TDMA scheme with a reservation protocol. Discuss both access control schemes for the above scenario.

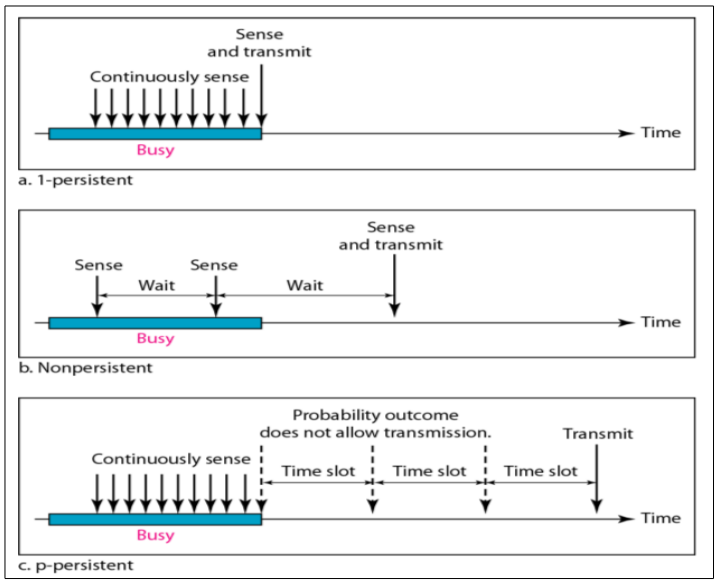
1. Carrier Sense Multiple Access – Collision Avoidance (CSMA/CA)

CSMA/CA follows the following protocol:



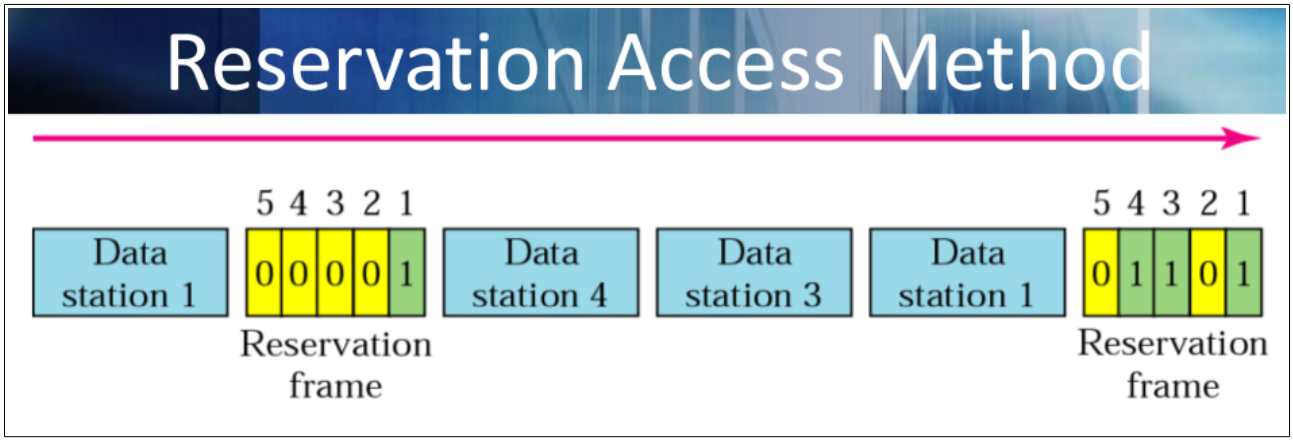
1. Start
2. Set backoff to 0
3. Persistence Strategy
4. Wait IFG+Random Time
5. Send the frame
6. Set a timer
7. Wait for ACK
8. If no ACK, increment backoff and wait
9. Repeat from step 3





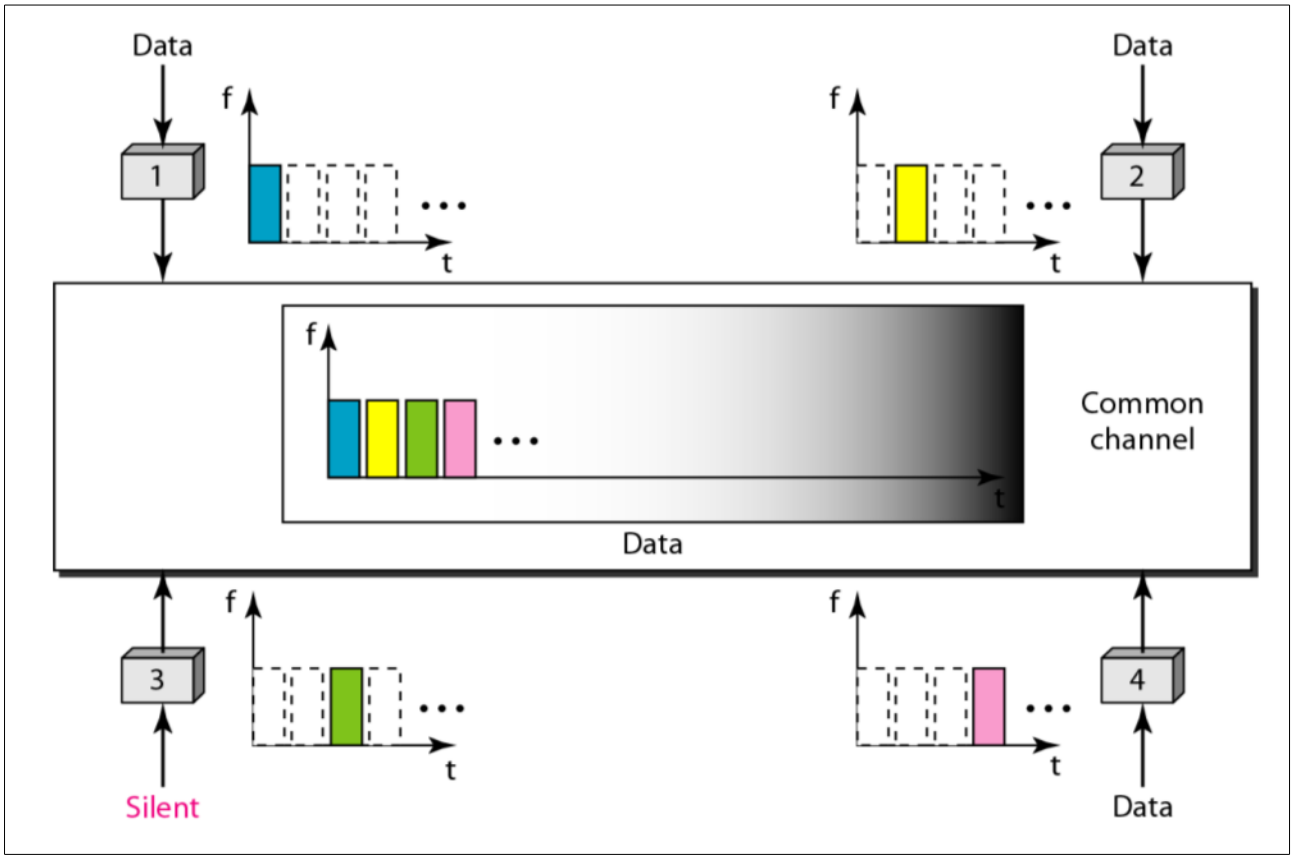
2. Time Division Multiple Access (TDMA) – With Reservaton Frames

In TDMA with Reservation Frames, when a station wants to transmit data it must transmit a 1 during its slot in the reservation frame.



All stations are informed about all planned communication. However, there are limited number of pre-allocated slots/stations.

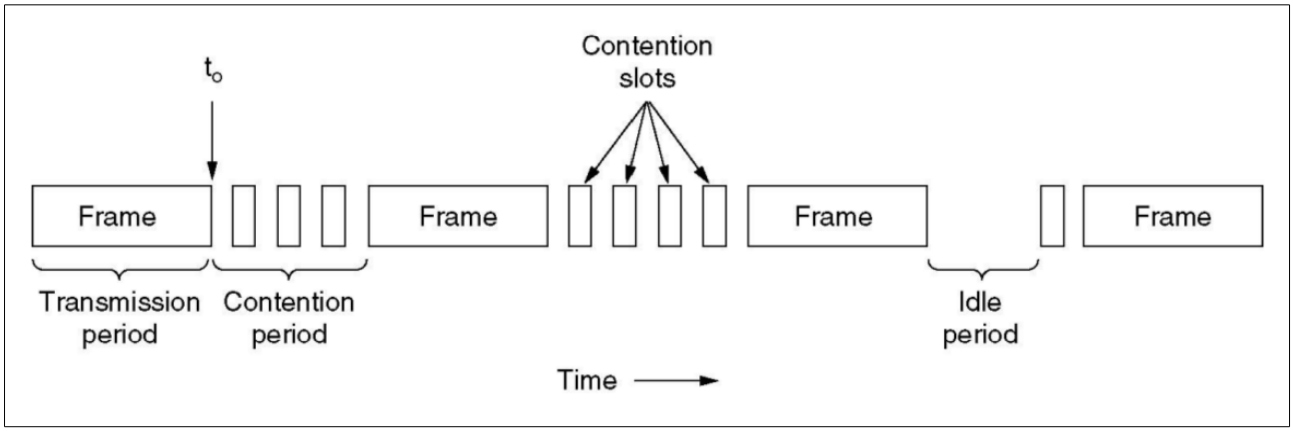
TDMA Flow Diagram:



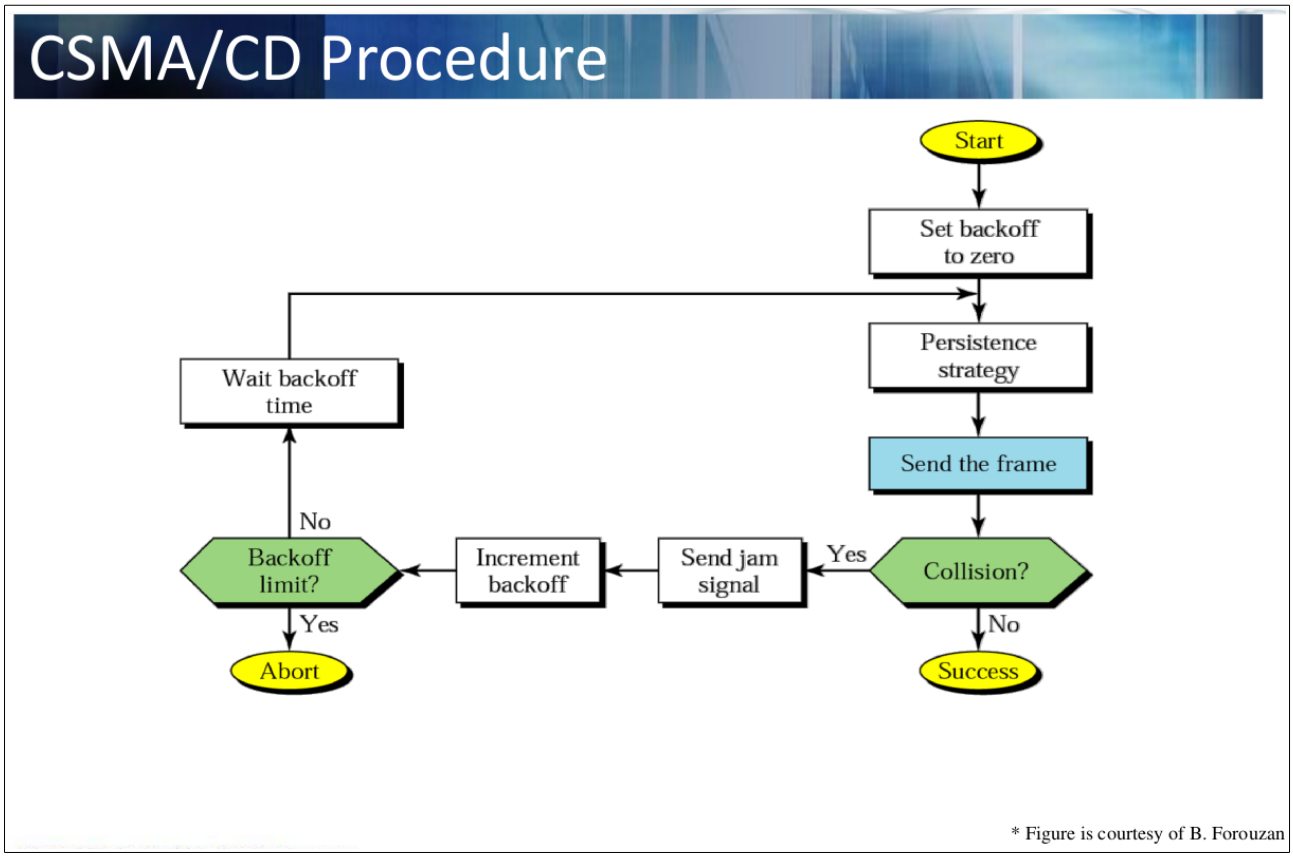
II) Contrast CSMA/CD with any access method of your choice on an example of 3 nodes wanting to transmit over a wired network. Use diagrams to visualize the chronological exchange of frames.

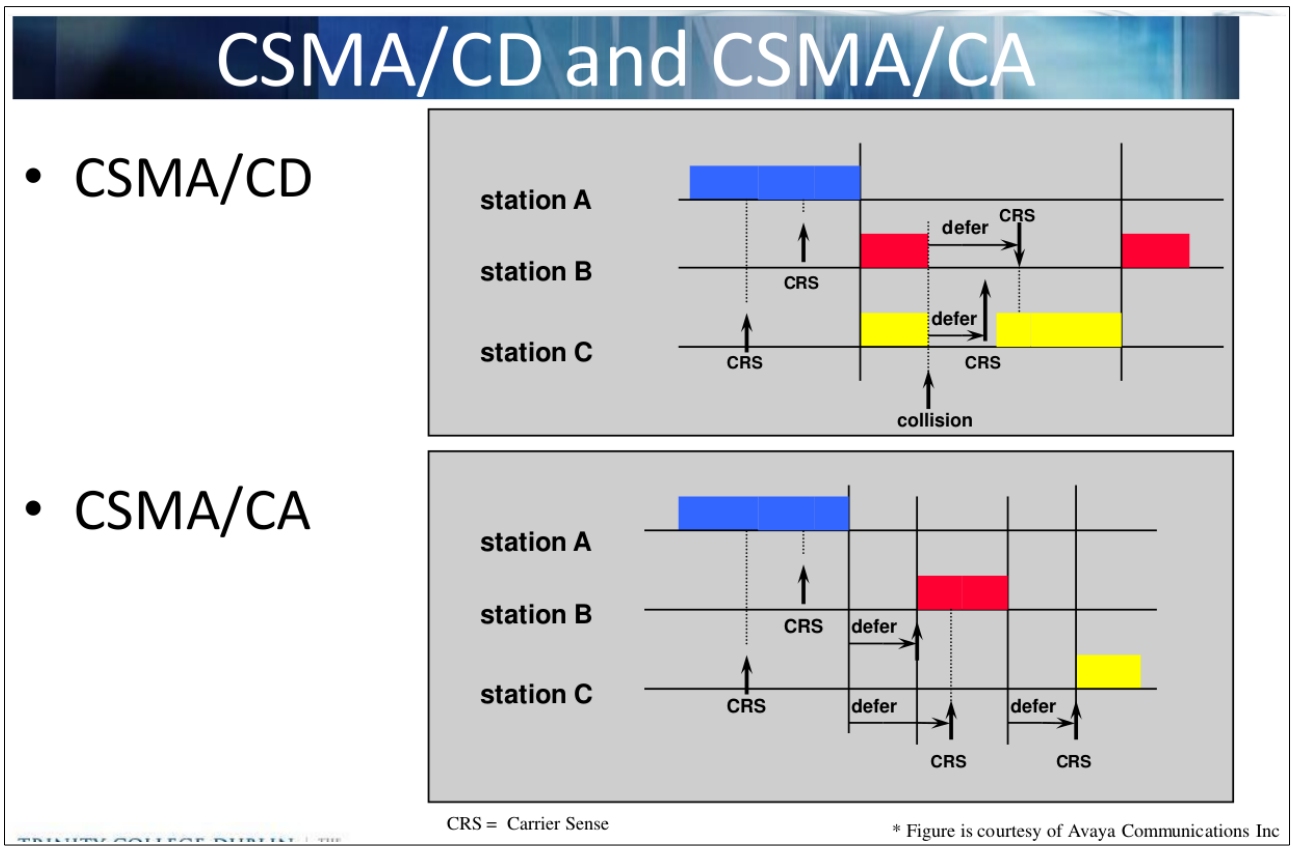
In CSMA/CD stations can be in one of three states:

1. Contention: Waiting to transmit a frame
2. Transmission: Transmitting a frame
3. Idle: Nothing to send



-When a collision occurs, all stations involved jam transmissions
-They then increment backoffs respectively
-They then re-transmit, and check for collision again





CSMA/CD:

1. Station A Transmits a Frame (BLUE)
2. Station B&C send Carrier Sense to see if Medium is being used
3. Both Station B (RED) & Station C (YELLOW) begin transmission at the same time
4. Collision Occurs
5. Both stations jam signals and defer transmission
6. Station C (YELLOW)'s defer is smaller, allowing it to transmit first
7. Station B (RED) polls the medium again
8. Station B (RED) eventually transmits

CSMA/CA:

1. Station A Transmits a Frame (BLUE)
2. Station B&C send Carrier Sense to see if Medium is being used
3. Both Station B (RED) & Station C (YELLOW) defer transmission backoffTime
4. Station B (RED) has the smaller defer and begins transmission
5. Station C (YELLOW) polls the medium again using CRS
6. When medium becomes free Station C (YELLOW) defers once more
7. Station C (YELLOW) eventually transmits its packet

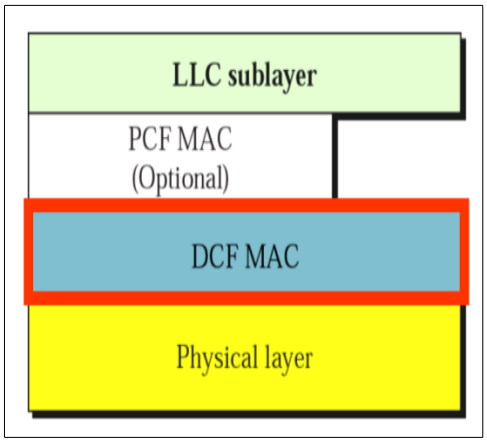
Q2 (b) – Medium Access Control

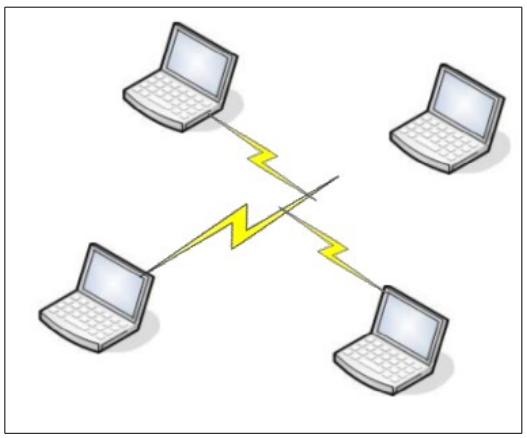
IEEE 802.11 defines two methods of medium access control, the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF).

I) Describe the two methods DCF and PCF and discuss the importance of interframe spaces.

Distributed Coordination Function (DCF):

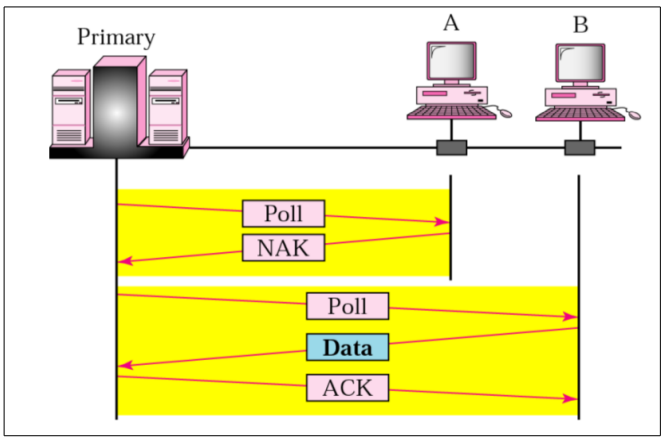
- This is when stations compete for access to the medium.
- First checks to ensure radio link is clear before transmission.
- If not idle, wait using exponential backoff
- Hidden station / Expose station problem.
- Used CSMA/CA (no collision avoidance).
- Uses DIFS (Distributed Interframe Spaces)

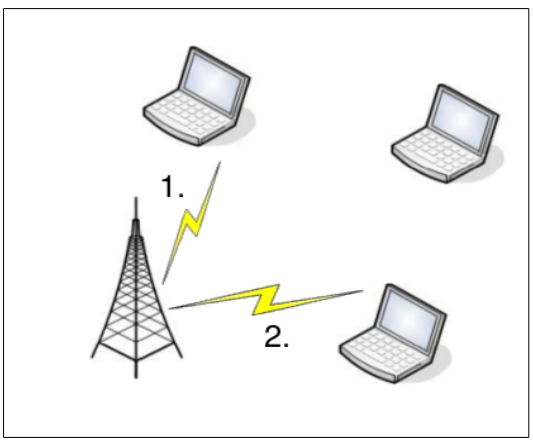




Point Coordination Function (DCF):

- This is when a point coordinator polls stations.
- Polls stations to see if they desire access to medium.
- Uses round-robin technique when polling.
- Stations must respond within SIFS.
- Uses PIFS (Point Interframe Spaces).



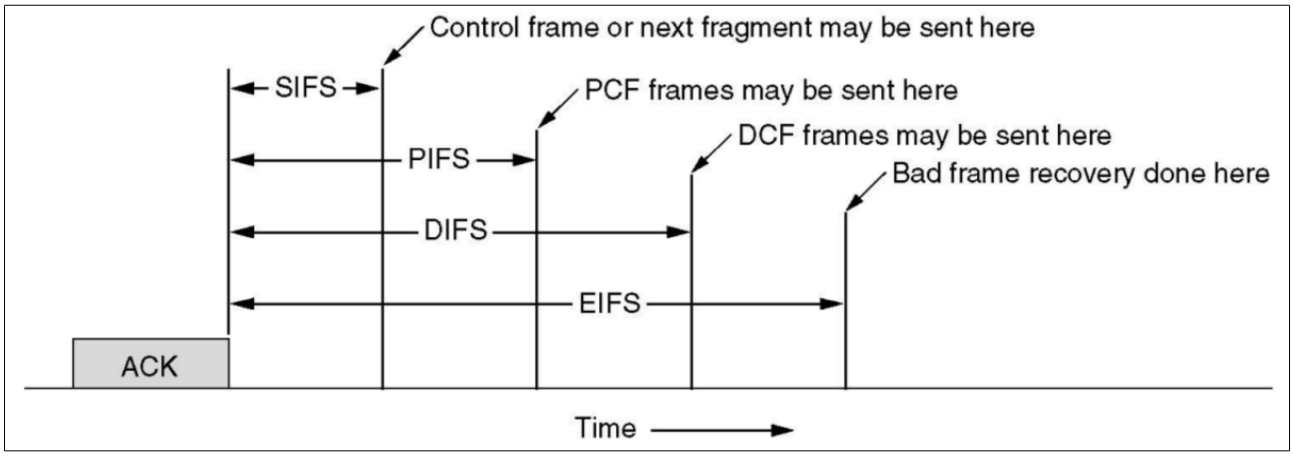


Interframe Spaces

Interframe spaces define the minimum time between frames. They are important as they directly influence how long stations must wait before gaining access to a medium.

- Short IFS (SIFS): The minimum time between frames.
- Distributed IFS (DIFS): The minimum time between the end of a transmission and the start of the next transmission.
- Point IFS (PIFS): The minimum time before polling station will allow transmission of the next transmission.

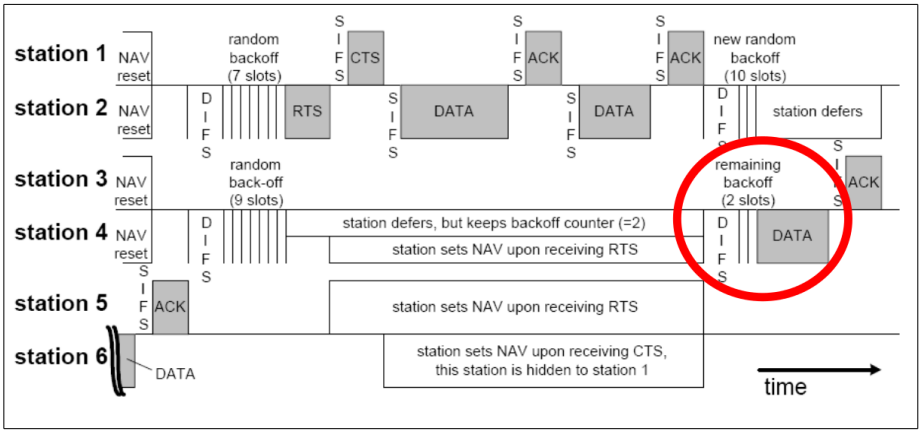
SIFS < PIFS < DIFS



II) Explain the coordination of communication between an access point and 5 laptops when using DCF and PCF.

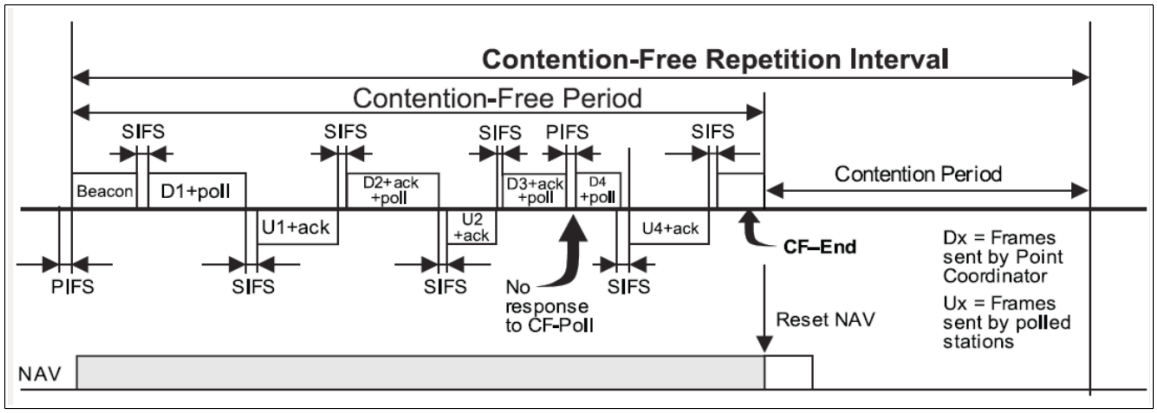
A) Distributed Coordination Function (DCF)

1. All stations wait DIFS + random backoff.
2. Station with least backoff attempts to gain access.
3. Someone succeeds and begins transmission (RTS – Right to Send).
4. Other nodes backoff exponentially.
5. Transmission finishes and medium is free for next transmission.



B) *Point Coordination Function (PCF)*

1. Wait SIFS, poll next station.
2. If ACK, keep track and remember station would like to transmit
3. Poll next station
4. When all stations are polled, allow transmission in round-robin fashion.



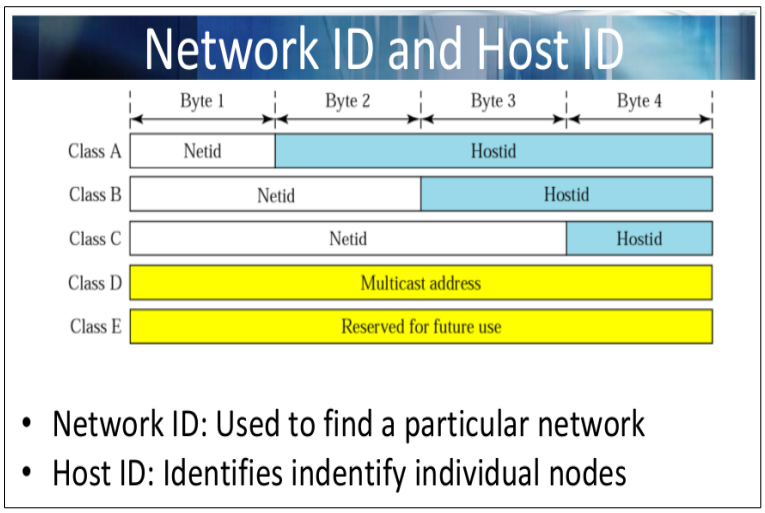
Q3 (a) – IPv4 vs IPv6

Internet Protocol version 4 (IPv4) and version 6 (IPv6) addresses represent two of the main forms of addressing in the Network Layer.

I) Explain the concept of classful addressing, the motivation for the introduction of this concept and the 5 classes that were suggested for the use with IPv4 addresses.

IP Addresses under IPv4 are represented as a 32-bit number, which allows for 4,294,967,296 possible combinations of addresses.

Classful addressing is the concept of dividing this 32-bit number into four different types of classes as described in the diagram below:

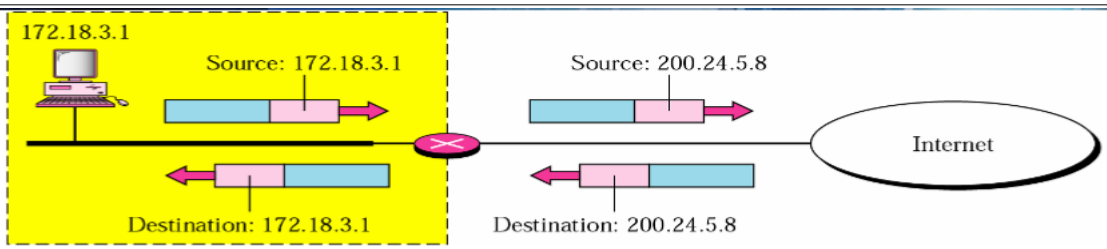


- **Class A** – International Organisations
- **Class B** – Large Companies
- **Class C** – Smaller Companies

II) Describe the concept of Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR) and their effect on the consumption of IPv4 addresses.

1. Network Address Translation (NAT)

In Network Address Translation (NAT) the NAT Gateway translates traffic from the local network to the IP address of the gateway. This involves processing of outgoing & incoming traffic, translation between addresses, recalculation of checksums etc.



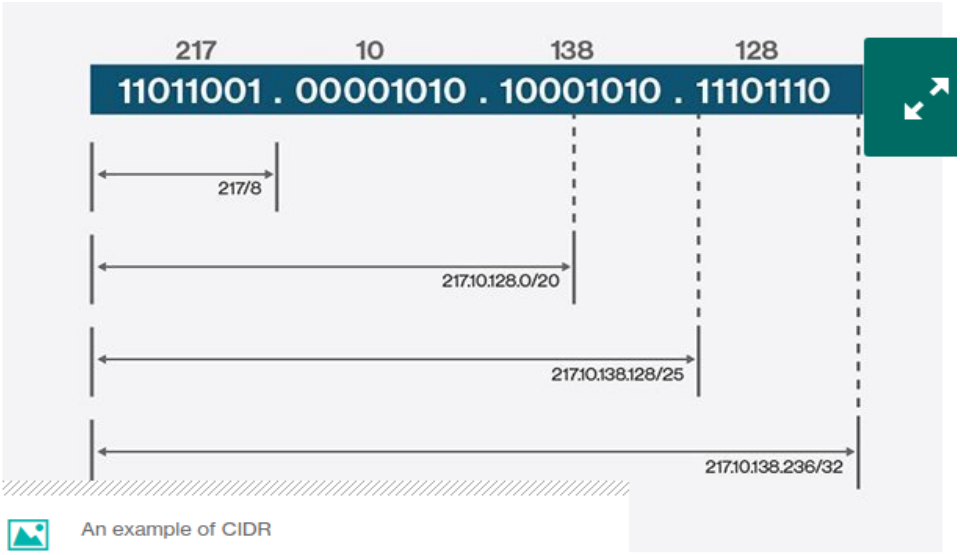
Private Address	Private Port	External Address	External Port	Transport Protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

The gateway maintains a table to match incomig & outgoing packets including IDs for applications. This is useful as it permits internet service providers and enterprises to masquerade private network address space with only one publicly routable IPv4 address on the internet interface of a router rather than allocating a public address to each network device.

2. Classless Inter-Domain Routing (CIDR)

A CIDR network address looks like this under IPv4:

```
192.30.250.00/18
```



An example of CIDR

The “192.30.250.0.” is the network address itself and the “18” says that the first 18 bits are the **NETWORK PART** of the address, leaving the last 14 bits for the **HOST ADDRESS**.

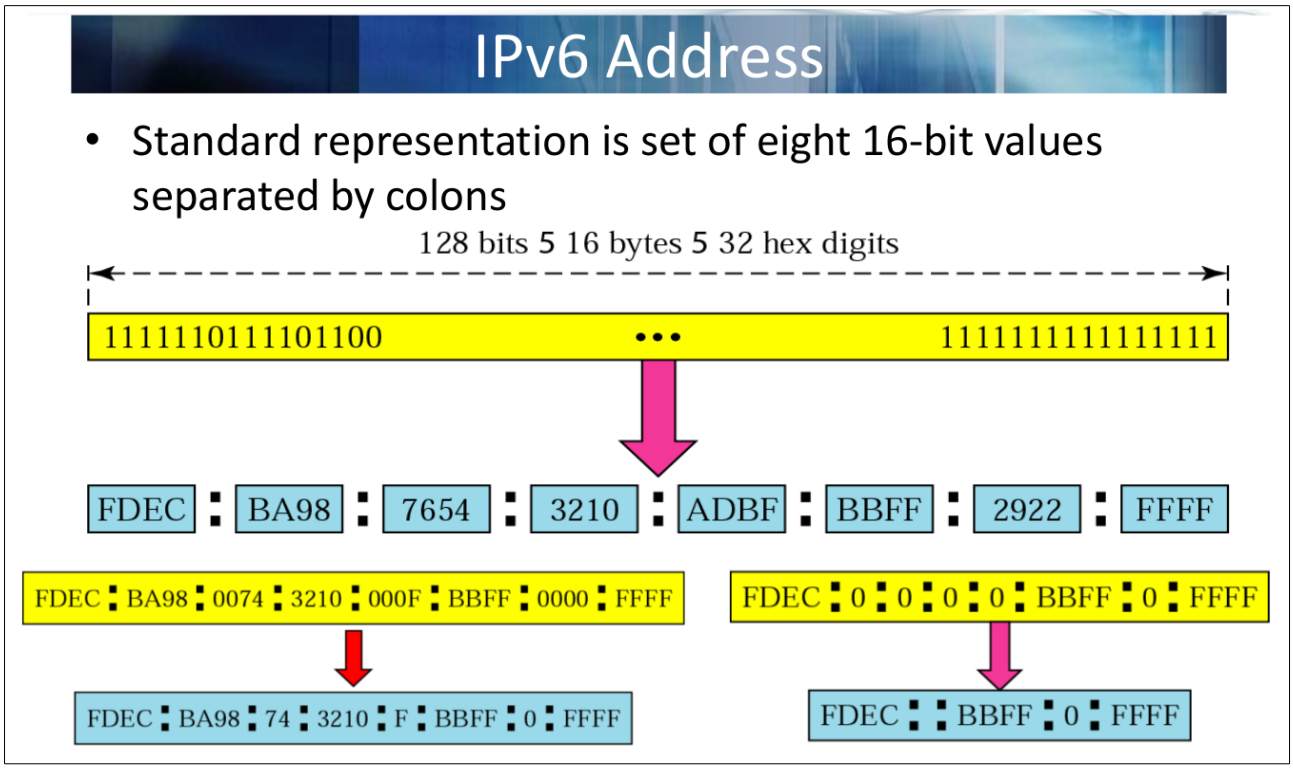
This allowed for a large majority of unused IP addresses under the IPv4 Protocol to be freed up significantly increasing the useful life of IP addresses.

III) Discuss the format of IPv6 addresses and the changes that the introduction of IPv6 addresses represents in contrast to IPv4 addresses

The change from IPv4 addresses to IPv6 addresses is mainly to create/free up more address spaces to be used on the internet.

We saw previously that IPv4 addresses were a 32-bit number limiting it to 4,294,967,296 possible combinations of addresses. Whereas in IPv6, addresses are represented as a fixed-length 128-bit address which gives way to a total of 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses.

IPv6 addresses are represented as 8 x 16-bit values (HEX). Values that contain all 0s can be abbreviated within colons. IPv6 addresses take the following format:



Q3 (b) – Distance Vector Routing

I) Explain the exchange of routing information in a Distance Vector routing approach on the same topology shown in figure 1 and contrast it with the establishment of Routing Tables in Link State routing approaches. Your description should be accompanied by diagrams that visualise the concepts.

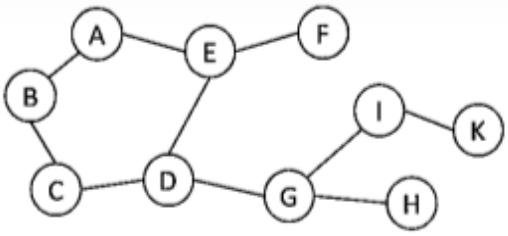


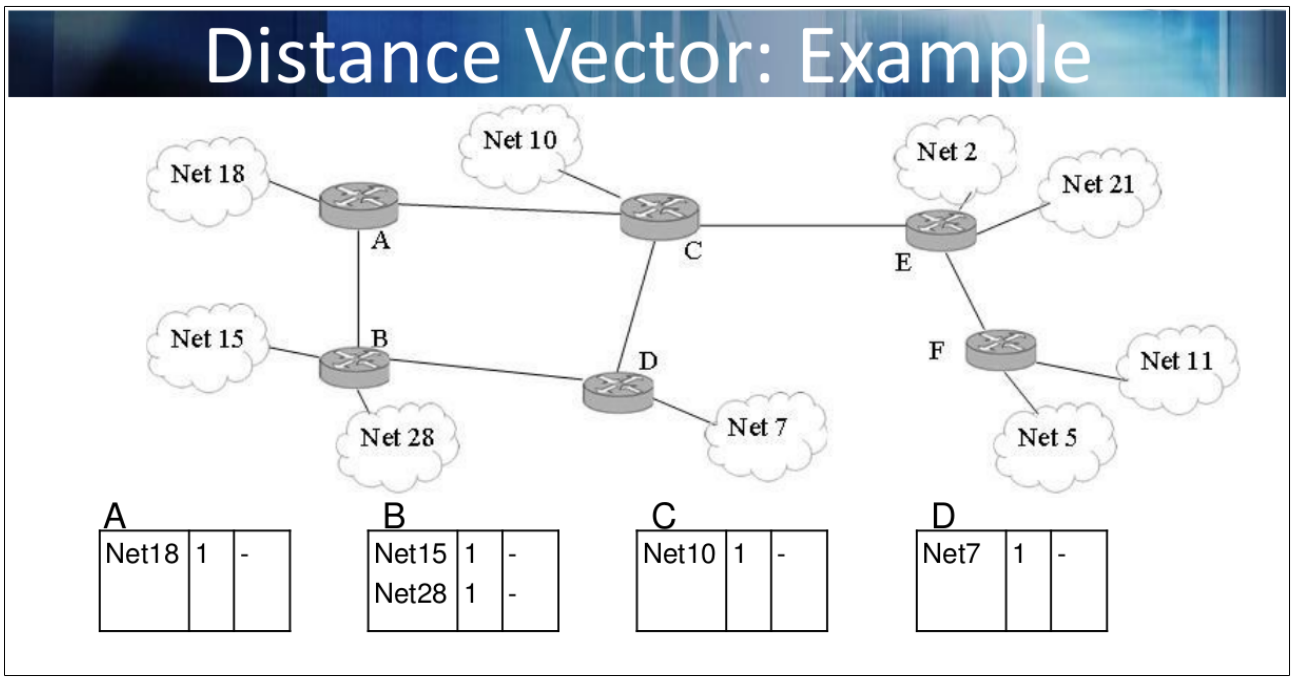
Figure 1: Sample Topology showing routers A to K and their interconnection

1. Distance Vector Routing

In Distance Vector Routing routes propagate through the exchange of routing tables. It is entirely based on communication with neighbors. Each node within the network maintains a set of triples e.g in the form of a HashMap in the following order:

{Destination, Cost, NextHop}

When a new route or a shorter route is found, updates are shared with directly connected neighbours. This can be done either periodically or whenever a single change occurs. Each router knows the networks that are immediately connected to it.



The algorithm for handling updates is as follows:

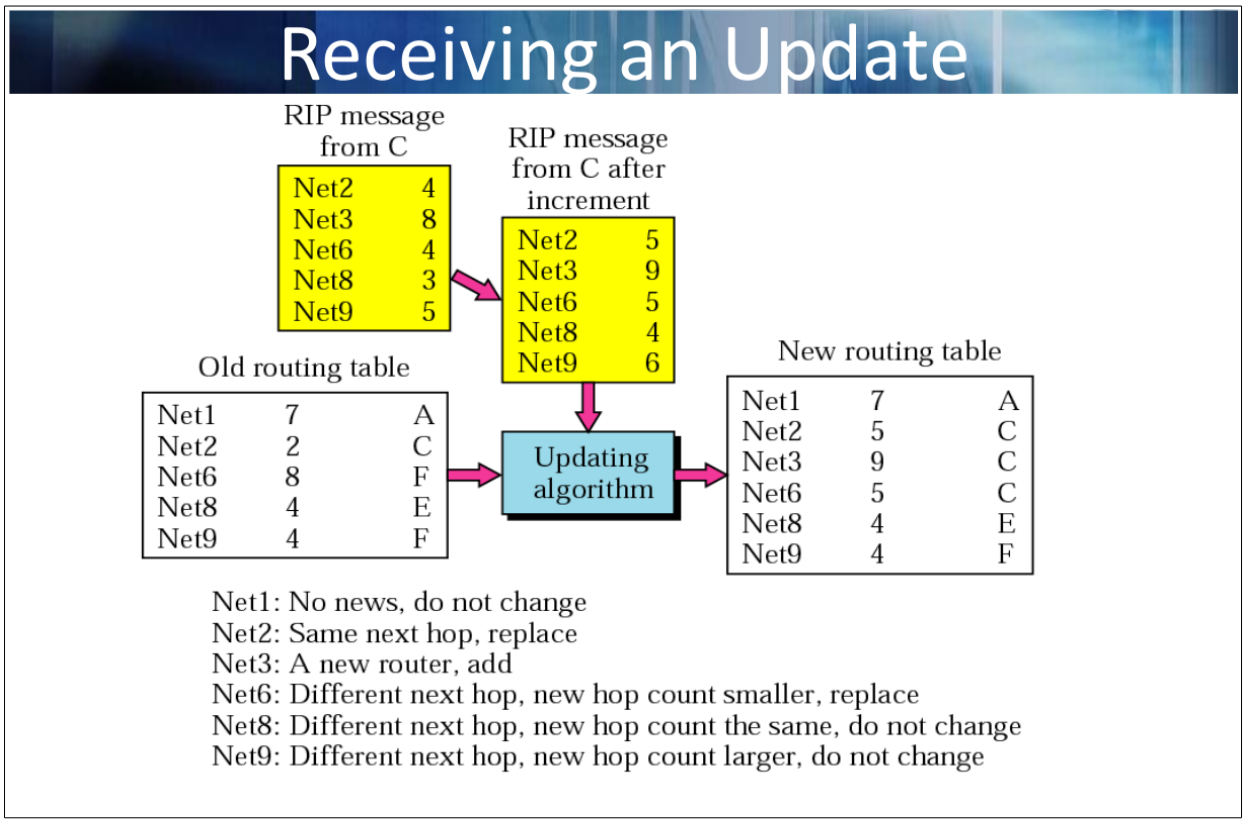
1. Add one hop to the hop counts (since node receiving update from n will be node n+1)

2. Repeat the following steps for each location in the update:

   a) If (destination not in routing table)
   -Add the advertised information to the table

   b) Else if (nextHop is the same)
   -Replace entry in table with new entry

   c) Else if (newHopCount < currentHopCount)
   -Replace entry in table with new entry



2. Link State Routing

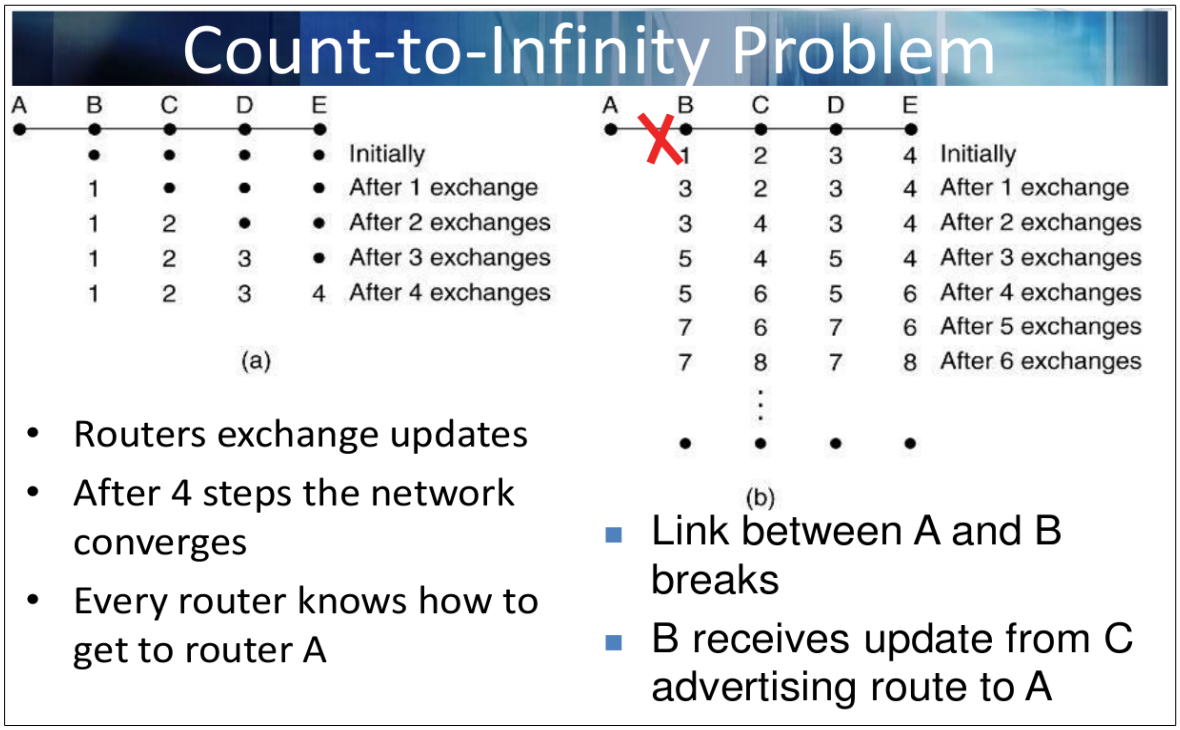
In Link State Routing the network establishes a view of the complete topology initially. It then uses Dijkstra's Shortest Path algorithm to establish the shortest path throughout the network.

Knowledge is shared about the neighborhood and this knowledge is shared to every router in the network.

Once an entire topology has been established, the network runs Dijkstra's shortest path algorithm for every single node within the network and establishes a Shortest Path table respectively for each node defining the optimal route throughout the network.

II) Discuss the effects of router failures in a Distance Vector routing approach and the mecanisms that have been proposed to address these effects.

One issue with Distance Vector Routing is the Count to Inifinity Problem. This is when a link breaks between two nodes. Take for example the link between A and B breaks. B receives an update from C advertising route to A.



Solutions to Count to Infinity:

1. Impose upper bound on maximum distance.
2. Split horizon : Don't inform node B the new distance to A if node B is the nodes the next hop towards A.
3. Split horizon with poisoned reverse : C should tell node B that its distance to node A is ∞ when node B is C's next-hop towards A.