Telecommunications Exam Solutions

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

2017 Exam:

Q1 (a) – Flow Control

The High-Level Data Link Control (HDCL) describes a number of frames shown below.

- *Node A Address = 1000 1111*
- *Node B Address = 1111 0000*
- *S-Frame ACK = 00*
- *S-Frame NAK = 11*
- *Flag Byte = 0111 1110*

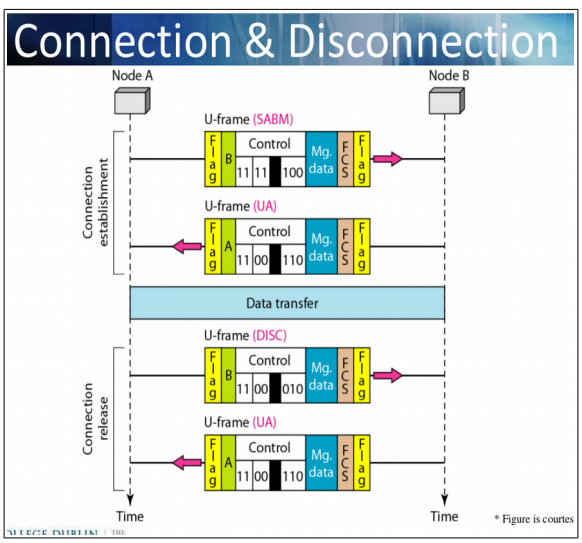
I) Draw the frames of the transmission for Stop-and-Wait

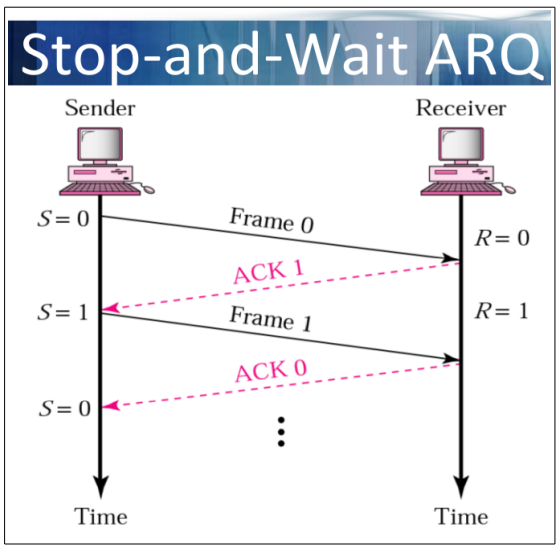
**** U-Frame – Setup****
**** I-Frame – Information Transfer****
**** S-Frame – ACK / NAK****

- First send **U-Frame** between nodes to setup the connection
-Wait for **U-Frame** response (ACK)

- Use **I-Frame** to send information between nodes
- Wait for **S-Frame** to return ACK / NAK
- If NAK re-send **I-Frame**
- If ACK send next **I-Frame**

- After 5 transactions send **U-Frame** to disconnect





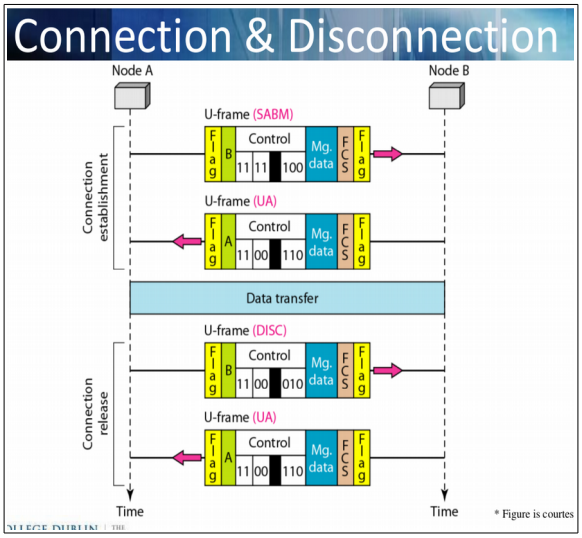
I) Draw the frames of the transmission for Selective Repeat

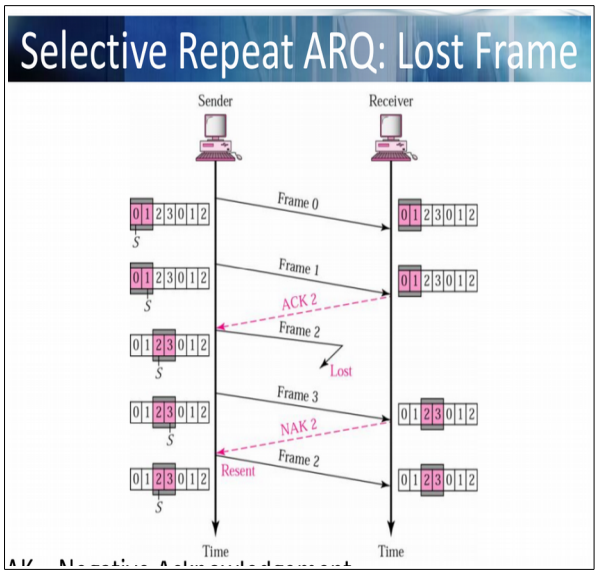
**** U-Frame – Setup****
**** I-Frame – Information Transfer****
**** S-Frame – ACK / NAK****

- First send **U-Frame** between nodes to setup the connection
-Wait for **U-Frame** response (ACK)

- Use **I-Frame** to send information between nodes
- Continuously send **I-Frames** to node B
- Wait for **S-Frame** to return ACK / NAK

- If NAK re-send **I-Frame** based on what NAK it is I.e NAK3
- If ACK continue sending next **I-Frame**





ii) Explain the process that takes place when the information being transferred includes the same bit-sequence as the flag byte.

When the information being transferred contains the same bit-sequence as the flag byte this is resolved using the process called **bit stuffing**.

This is when for example the flag is 01111110. (6 ones in a row).

If the information contains this same bit sequence, after every 5 ones, a 0 is inputted after it as a guard, this is then removed when extracting the information.

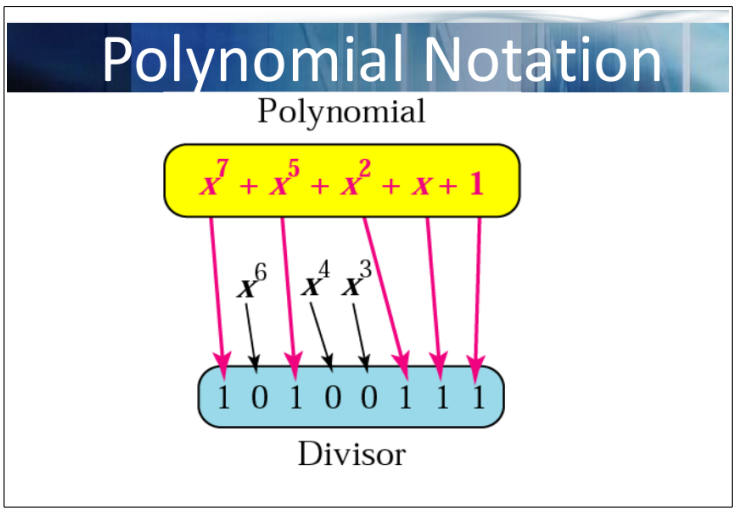
FLAG
Old Info : [01111110]110010
New Info : 01111101011001 0

Q1 (b) – Flow Control

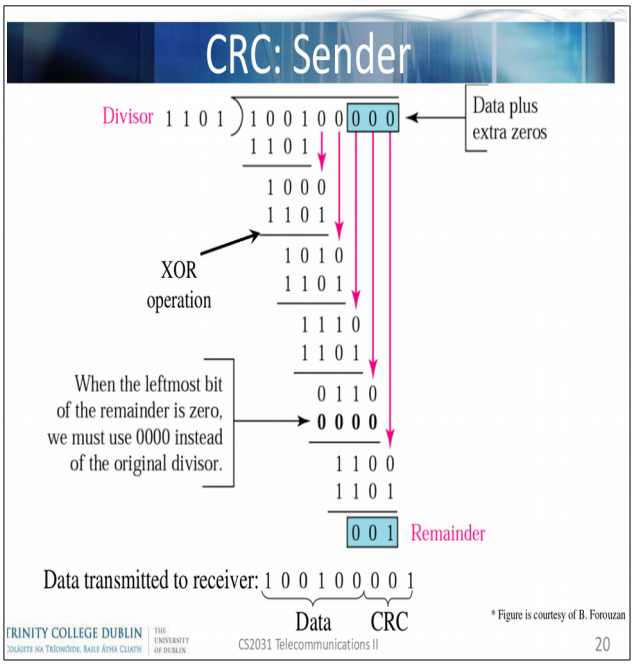
*I) Assume you have a connection that exhibits **sporadic burst errors**. Transmissions across the connection are **not costly** and the **transmission delay** is **short.** Propose an error detection approach and contrast it against alternatives.*

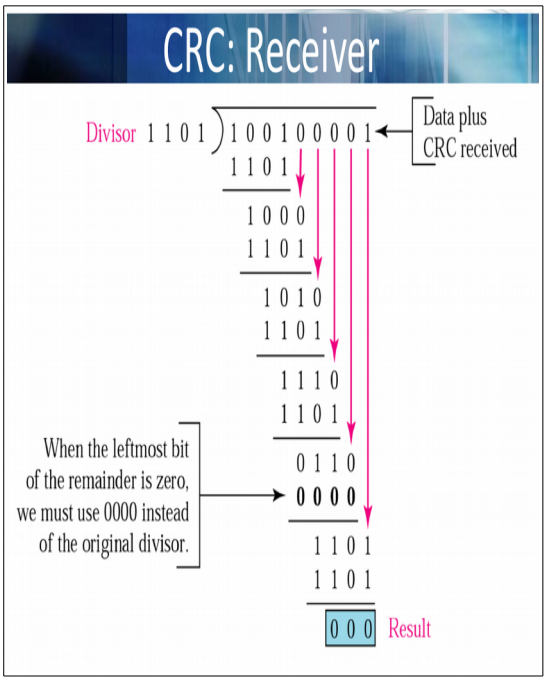
Burst Errors are when errors are found to be **spread across a wide range of bits** and not just focused single bit errors.

As a result the entire information must be checked to ensure validity. To achieve this the desired error checking method would be **Cyclic-Redundancy Check (CRC)**. This is achieved using what is called a **Checksum** value. The Checksum value is generated as a result of a defined **polynomial** which can be generated as follows.



The **Cyclic-Redundancy Check (CRC)** is done as follows.





CRC is the preferred method for **sporadic burst errors** as it ensure the validity of the entire data, whereas **Checksum** or **Even Parity** check only account for single bit errors.

*ii) Assume you have a connection that exhibits **few errors** that are generally limited to **single bits**. Transmissions across the connection are **costly** and the **transmission delay** is **long.** Propose an error detection approach and contrast it against alternatives.*

When checking for single bit errors you have two options:

- **Even Parity Check**
- **Checksum**

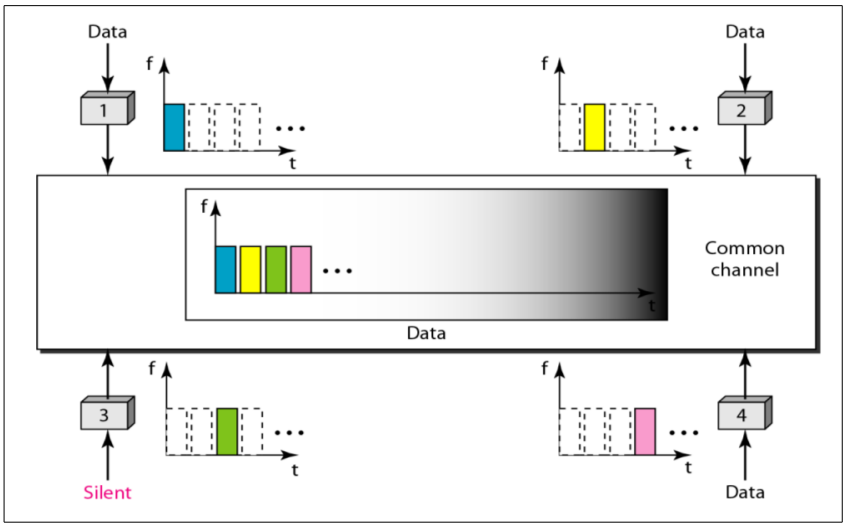
Since transmissions over the network are costly you would want to transmit as **little information as possible**. The more ideal method for this would be to use **Even Parity Bit** as it means only one extra bit of data is needed to be transferred per section (the parity bit). This results in a total data transfer of $(k + 1) * b$ (k being sections, n being number of sections, b being bits per section).

Whereas for **Checksum** each section is added and then complemented and the resulting checksum is transferred. This results in a total data transfer of $(k + k/n) * b$ (k being sections, n being number of sections, b being bits per section).

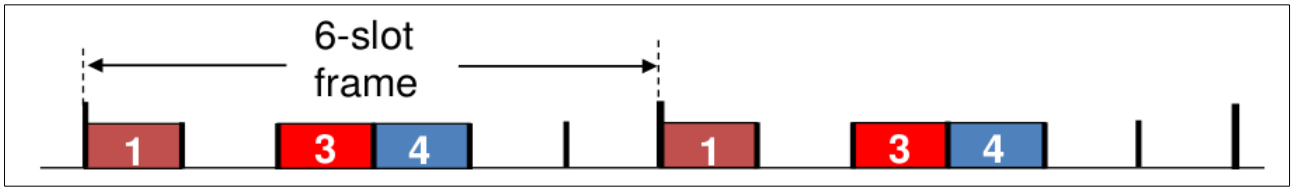
Q2 (a) – Medium Access Control

*I) Assume that your wired network currently uses **Time-Division Multiple Access (TDMA)** to accommodate 6 stations. Explain how stations gain access to this medium and the advantages and disadvantages of this approach.*

In Time-Division Multiple Access (TDMA) users are granted access to the full bandwidth of the network for 1/N of the time.



Access to the channel is in *rounds*. Each station gets a fixed length slot in each round. Unused slots go idle.



TMDA Advantages:

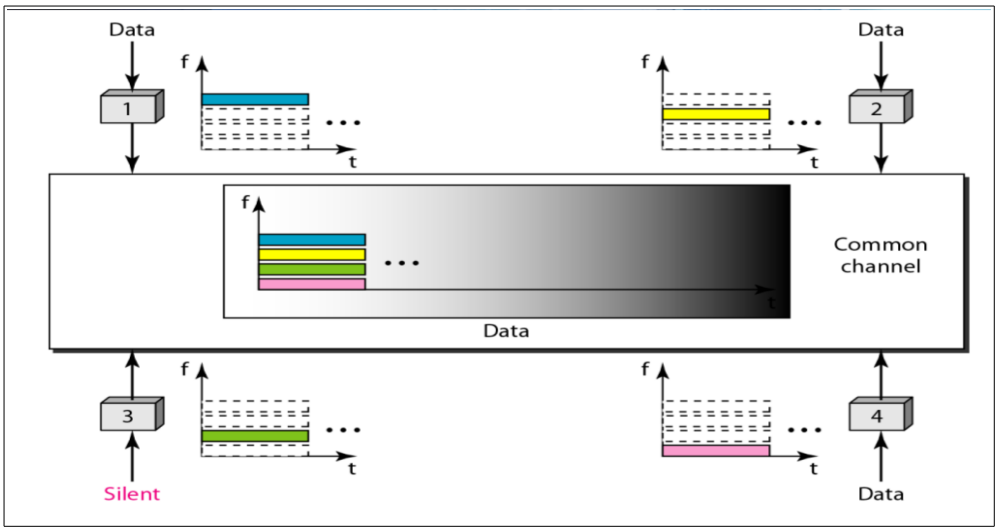
- Efficient use of frequency spectrum.
- Operational costs lower than FDMA.
- Suitable for various types of traffic (e.g voice, data, video)
- Resources used effectively, preserves battery life

TMDA Disadvantages:

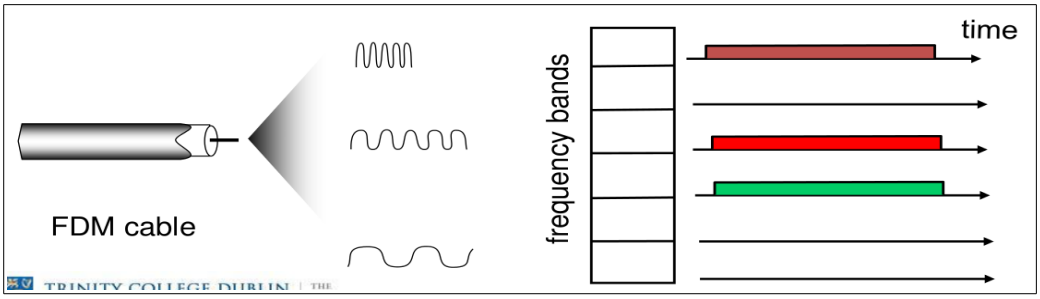
- Network and spectrum planning require more efforts.
- Multi path interference affects call quality.
- Switching between base station cells results in dropped calls.

II) Propose an alternative protocol to TDMA that would be suitable for a varying number of stations . Explain how stations would gain access to this protocol and discuss the advantages and disadvantages.

In Frequency-Division Multiple Access (FDMA) users are granted 1/N of the total bandwidth for an unlimited amount of time.



Channel spectrum is divided into various frequency bands depending on the number of users. Each station is assigned a fixed frequency band. Unused transmission time in frequency bands go idle.



FDMA Advantages:

- Separate bands for uplink and downlink.
- Stations can transmit and receive simultaneously.
- Very simple to implement with respect to hardware.
- Efficient when managing constant traffic.

FDMA Disadvantages:

- Frequencies allocated permanently, waste of spectrum when idle.
- Network and spectrum planning is difficult.
- Guard bands to prevent interference, waste of resources.
- Requires RF filters, increasing costs.
- Maximum bit rate is constant, doesn't suit varying data rates.

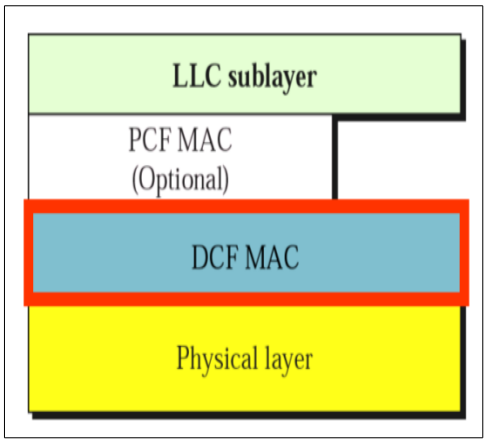
Q2 (b) – Medium Access Control

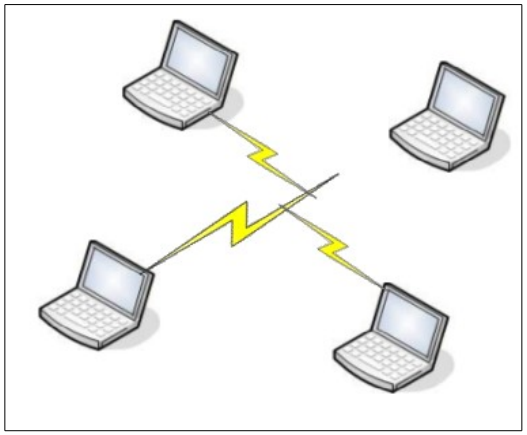
IEEE 802.11 defines two methods of medium access control, the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF).

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

Distributed Coordination Function (DCF):

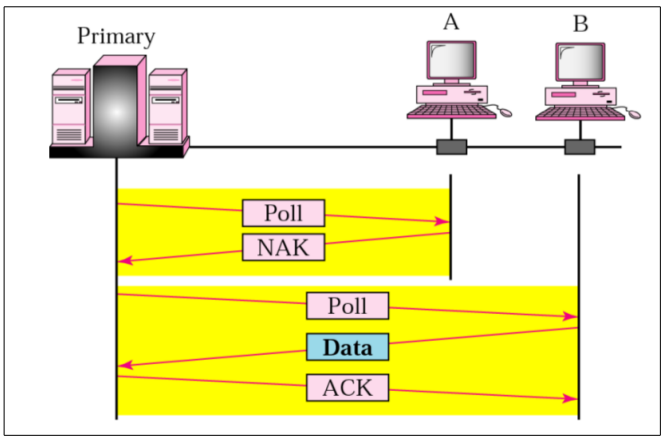
- This is when stations compete for access to the medium.
- First checks to ensure radio link is clear before transmission.
- If not idle, wait using exponential backoff
- Hidden station / Expose station problem.
- Used CSMA/CA (no collision avoidance).
- Uses DIFS (Distributed Interframe Spaces)

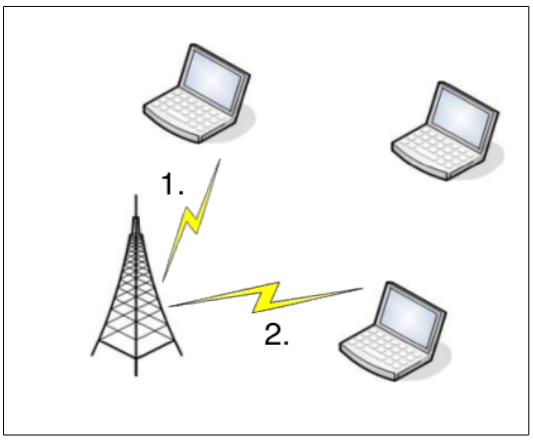




Point Coordination Function (DCF):

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



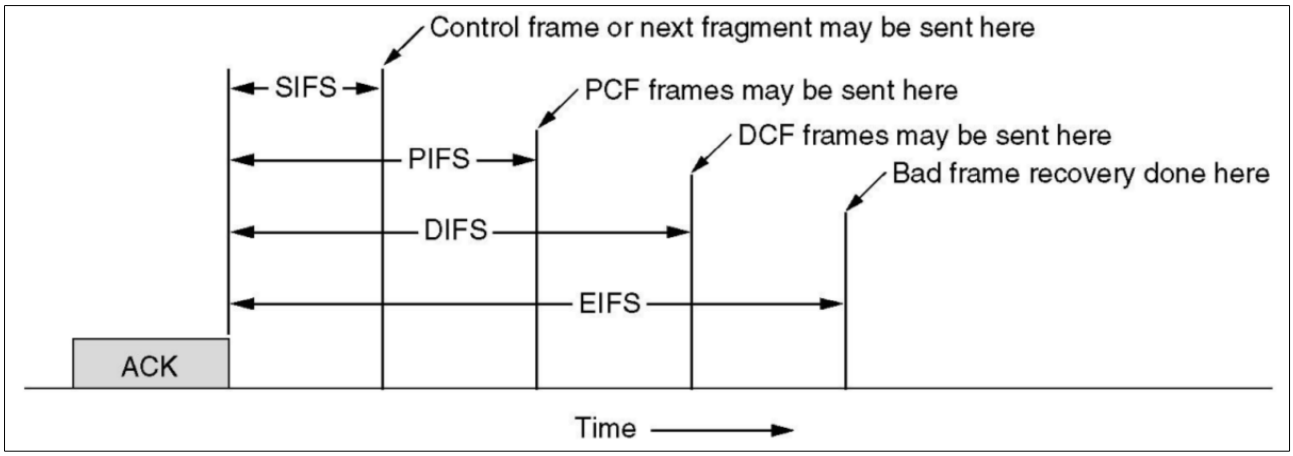


Interframe Spaces

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.

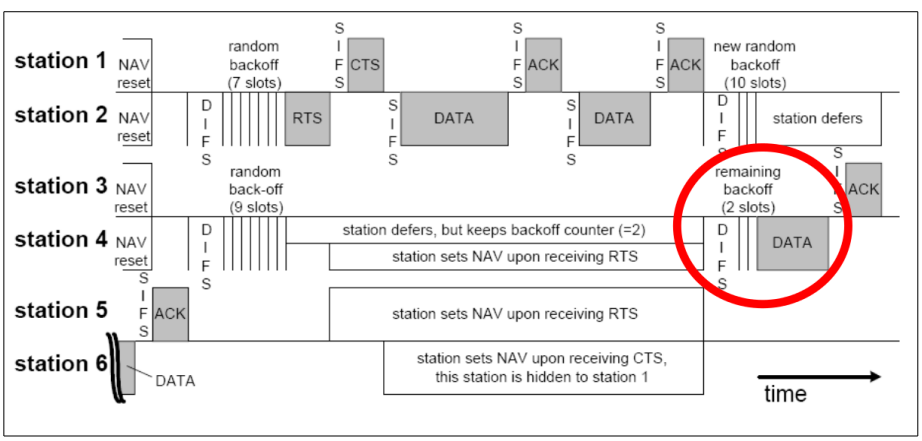
SIFS < PIFS < DIFS



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

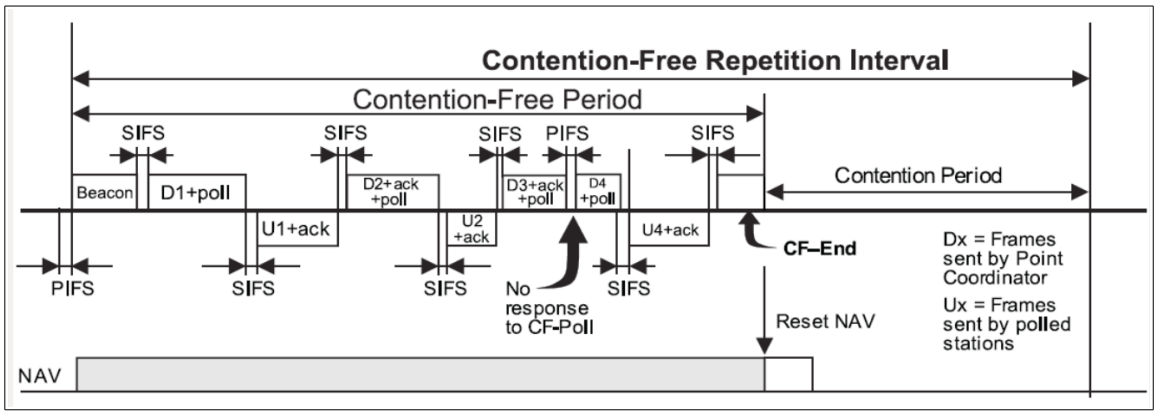
A) Distributed Coordination Function (DCF)

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)*

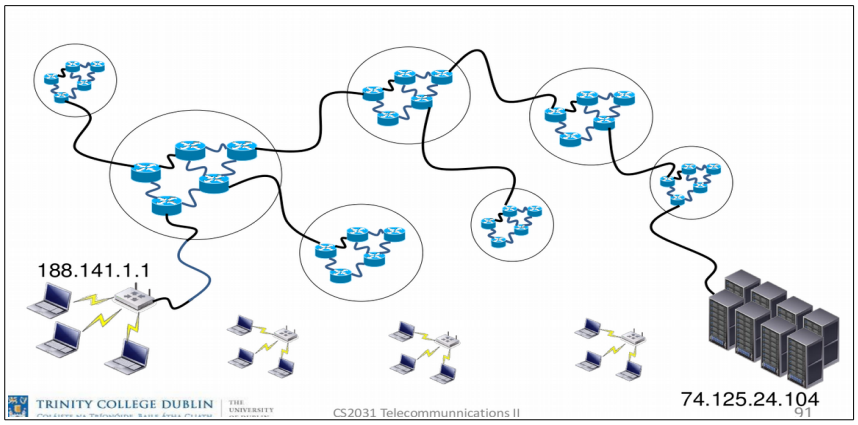
1. Wait SIFS, poll next station.
2. If ACK, allow to transmit, when finished wait PIFS.
3. Else poll next station.



Q2 (a) – Routing

Trinity College currently uses Class B network addresses within the range 134.226.0.0 to 134.226.255.255 for a number of its network node. The network has around 20,000 nodes. The traffic of 200 of these nodes is allowed to pass to the internet without being blocked by routers. The traffic of the remaining nodes is never directly routed into the internet.

I) Describe the routing of an IP packet from a node inside the network to a server outside the network, blocked & unblocked by routers.



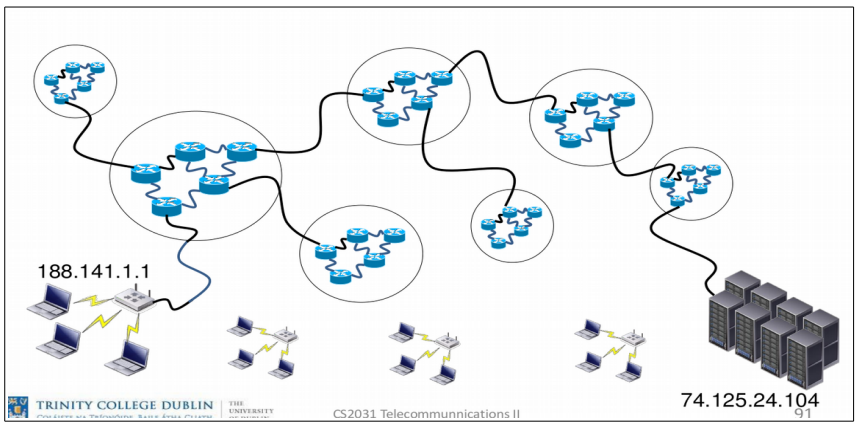
Router Connection:

1. Laptop A sends IP packet to its connected router.
2. Connected router knows how to get to destination.
3. Router forwards packet to connected gateway/router.
4. Packet arrives at outer-network (74.125.0.0)
5. Packet is then routed throughout subnet-work until it arrives at destination.
6. Packet decoded at destination (Google – 74.125.24.104).

Non-Router Connection:

1. Laptop (node) is connected directly to the internet.
2. Laptop sends IP packet directly to ISP with a defined destination.
3. Packet does not need to go through a router as it is connected directly to the internet.
4. Packet traverses the internet.
5. Packet arrives at outer-network (74.125.0.0).
6. Packet is then routed throughout subnet-work until it arrives at destination.
7. Packet reaches destination node (Google – 74.125.24.104).
8. Packet decoded at destination.

I) Describe the routing of an IP packet from a node outside the network to a node inside the network, blocked & unblocked by routers.

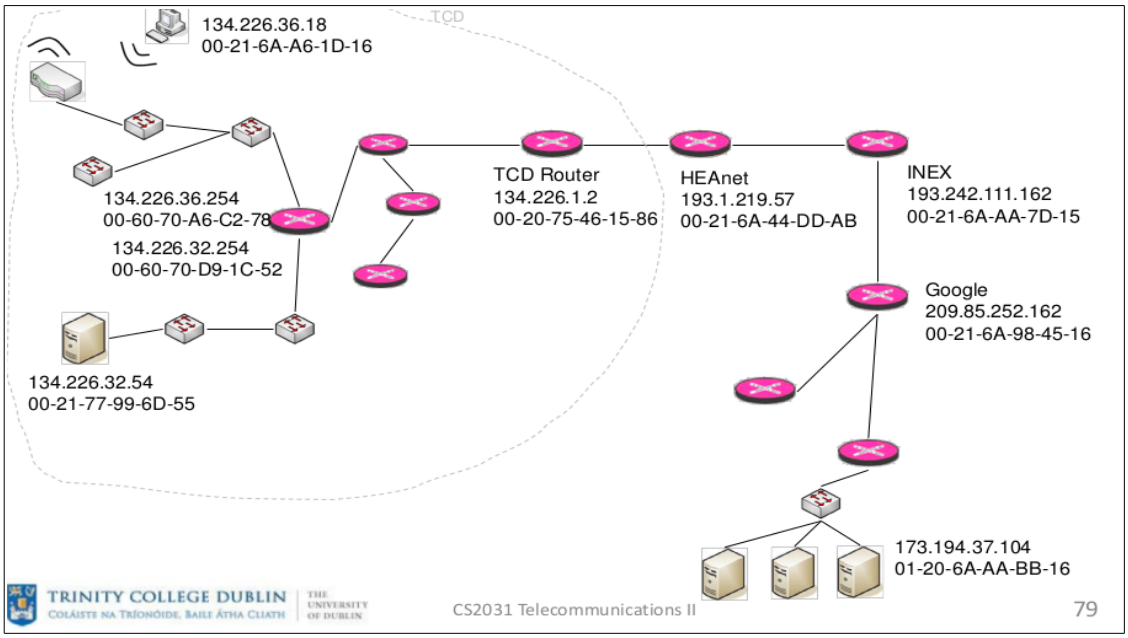


Router Connection:

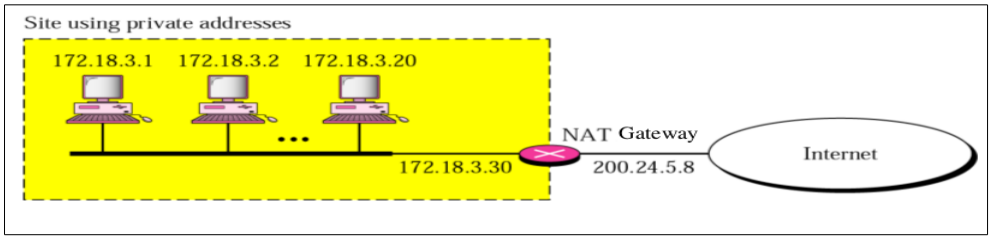
1. Google server at 74.125.24.105 would like to send packet to Trinity node (188.141.1.1)
2. Server sends IP packet to its connected router.
3. Router sends packet to the outer-network router (74.125.0.0).
4. Router then forwards packet to the respective gateway/router (next hop).
5. This is repeated until packet arrives at Trinity address (188.141.0.0).
6. Packet is then routed through sub-network until it arrives at 188.141.1.1.
7. Packet is decoded at node.

Non-Router Connection:

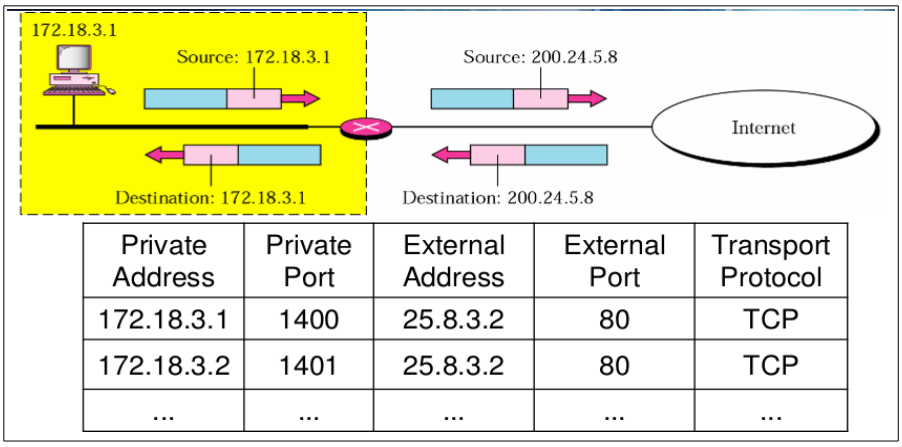
1. Google server is directly connected to the internet.
2. Packet does not need to be sent to outer-network, sent directly to next gateway.
3. Packet is routed throughout the internet.
4. Packet is then routed through sub-network until it arrives at 188.141.1.1.
5. Packet is decoded at node.



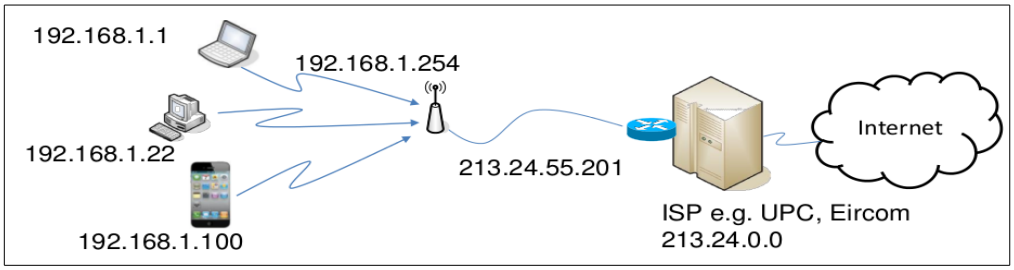
II) Describe the application of Network Address Translation (NAT) to the network of Trinity College , the possible allocation of addresses and the effect that this may have on the consumption of publicly routed IP addresses.



NAT Gateway translates traffic from the local network to the IP address of the gateway. This involves processing outgoing & incoming packets (translating addresses, re-calculating checksums etc). The Gateway maintains a table to match incoming and outgoing packets including ID's for applications.



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
...	...	...	...	...



Within the Trinity college network Network Address Translation (NAT) may be used to direct traffic between the subnetworks within the college e.g SCSS and the other schools. Network Address Translation (NAT) may be used multiple times say in the following order:

<u>Packet for SCSS Node (134.226.60.215)</u>

1. Arrives out outer network NAT Gateway (134.226.0.0)
2. Routed to sub-network SCSS NAT Gateway (134.226.60.0)
3. SCSS NAT Gateway forwards packet directly to SCSS Node (134.226.60.215)

Q3 (b) – Routing

Link State Routing (LSR) represents one of the major routing concepts.

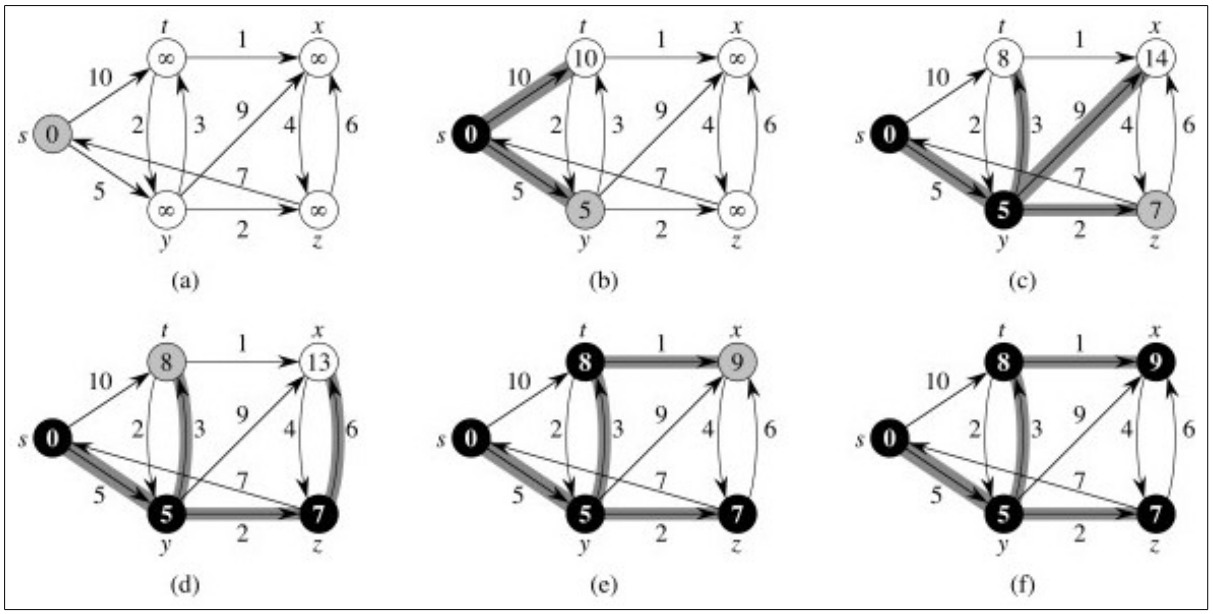
I) Describe the two components of LSR ie the establishing of a view of the topology and the execution of Dijkstra's Shortest Path algorithm.

The first component of Link State Routing (LSR) is the establishment of a view of the topology. All nodes and routers within the network must share their information either to each other or to an external controller. The information they must share in order to allow for Dijkstra's shortest path algorithm to be executed is:

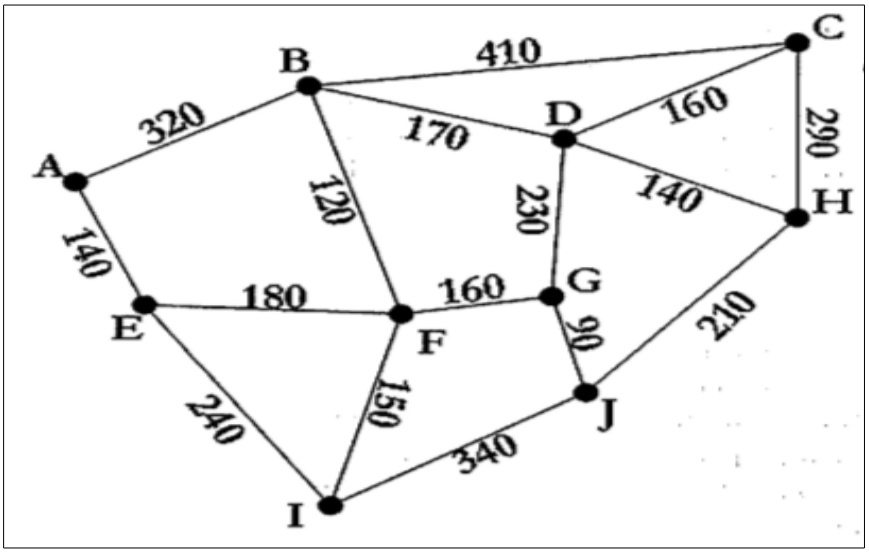
- List of all connected nodes/routers
- Distance to all connected nodes/routers

Once this information has been shared it is then possible for Dijksta's shortest path algorithm to be run. In short hand Dijkstra's algorithm is executed as follows:

1. Choose a source node
2. Assign a cost of 0 to this node and make it the first permanent node
3. Examine each neighbor node of the last permanent node
4. Assign a cumulative cost to each node and make it tentative
5. Among the list of tentative nodes
   a) Find the node with the smallest cumulative cost and make it permanent
   b) If node can be reached from more than one direction choose the one with shortest cumulative cost
6. Repeat steps 3 to 5 until every node becomes permanent.



I) Explain the process of establishing a routing table for node I using the two components with the help of the following diagram.



First of all, either an external controller or each node within the graph is informed of the connections to each other node and their respective distances.

1. Node I is selected as root node
2. Add Node I to Settled Nodes
3. Examine all nodes adjacent to Node I:
    - Node E – 240
    - Node F – 150
    - Node J – 340
4. Add each of the nodes to Tentative Nodes
5. Select Node F and add to Settled Nodes
6. Examine all nodes adjacent to Node F:
    - Node G – 160
    - Node E – 180
    - Node B – 120
7. Repeat steps until all nodes are settled.

Routing Table

Tentative Nodes

I	0	-

Routing Table

I	0	-

Tentative Nodes

E	240	I
F	150	I
J	340	I

Routing Table

I	0	-
F	150	I

Tentative Nodes

E	240	I
~~F~~	~~150~~	~~I~~
J	340	I

Routing Table

I	0	-
F	150	I
E	240	I

Tentative Nodes

~~E~~	~~240~~	~~I~~
J	340	I
G	150+160	F
B	150+120	F
E	150+180	F

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E

Tentative Nodes

J	340	I
G	150+160	F
~~B~~	~~150+120~~	~~F~~
A	150+180 +140	E

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E
G	310	F

Tentative Nodes

J	340	I
~~G~~	~~150+160~~	~~F~~
A	240+140	E
C	270+410	B
D	270+170	B

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E
G	310	F
J	340	I

Tentative Nodes

~~J~~	~~340~~	~~I~~
A	240+140	E
C	270+410	B
D	270+170	B
J	310+90	G
~~D~~	~~310+230~~	~~G~~

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E
G	310	F
J	340	I
A	380	E

Tentative Nodes

~~A~~	~~240+140~~	~~E~~
C	270+410	B
D	270+170	B
H	340+210	J

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E
G	310	F
J	340	I
A	380	E
D	440	B

Tentative Nodes

C	270+410	B
~~D~~	~~270+170~~	~~B~~
H	340+210	J

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E
G	310	F
J	340	I
A	380	E
D	440	B
H	550	J

Tentative Nodes

C	270+410	B
~~H~~	~~340+210~~	~~J~~
C	440+160	D
~~H~~	~~440+140~~	~~D~~

Routing Table

I	0	-
F	150	I
E	240	I
B	270	E
G	310	F
J	340	I
A	380	E
D	440	B
H	550	J
C	600	D

Tentative Nodes

C	270+410	B
~~C~~	~~440+160~~	~~D~~
C	550+290	H

****ALL NODES HAVE NOW BEEN SETTLED****