# 2016 Answers

**1) a) i)** Flow control refers to the control of the amount of data that a sender can transmit without overflowing the receiver.

There are three main mechanisms for flow control:

**Stop & Wait**

- Most simple to implement.
- Least efficient as an ACK has to be received for every single packet before the next packet can be sent.

**Go-Back-N**

- More complex to implement.
- Much more efficient at handling errors, as only the window has to be resent.

**Selective Repeat**

- Most complex to implement, as a sliding window has to be set up on both the sender and receiver sides.
- Most efficient at handling errors as it can isolate the individual frames that are causing the errors and have them resent.

**ii)** *diagram*

**iii)** Selective Repeat vs Go-Back-N.

Advantages of **Selective Repeat**:

- Better at handling transmission errors as it can isolate individual bits through the sliding window on the receiver end.a
- More efficient as by handling errors faster it can process more data in a certain time frame.

Disadvantages:

- More complex to set up, owing to the fact that it has two sliding windows:
    - One for the sender
    - One for the receiver

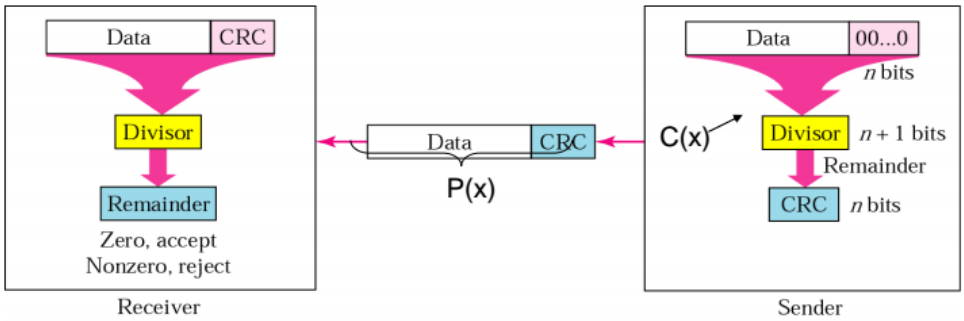
Advantages of **Go-Back-N**:

- Simpler to set up.
- With a low error-rate transmission, is just as fast as selective repeat.

Disadvantages:

- Less efficient at handling errors as it has to return the entire window to the sender for resending.

**b) i)**




CRC is calculated on the sender's end by adding a number of zeros to the message equal to the highest power of the polynomial dividing it. In this case, $x^8$ is the highest term, so we add 8 zeros to the end of 1011001001001011.

CRC division should use XOR, not binary division.

Divisor: $x^8+x^2+x+1$ = 100000111
Dividend: 1011001001001011 + 00000000 = 1011001001001011000000000

```
                ____________________________
100000111|1011001001001011000000000
         |100000111|||
         | 011000111||
         | 000000000||
         |  110001110|
         |  100000111|
         |   100010010
         |   100000111
         |    000101011
         |    ........
                      xyz   <= remainder of division (checksum)
```

**ii)** The CRC checksum is sent to the receiver in the CRC portion of the frame containing the data. The checksum is the remainder of the division. If the remainder was 001, 001 would be added to the data.

```
          Data                  CRC Checksum
|1011001001001011000000000|    xyz    |
```

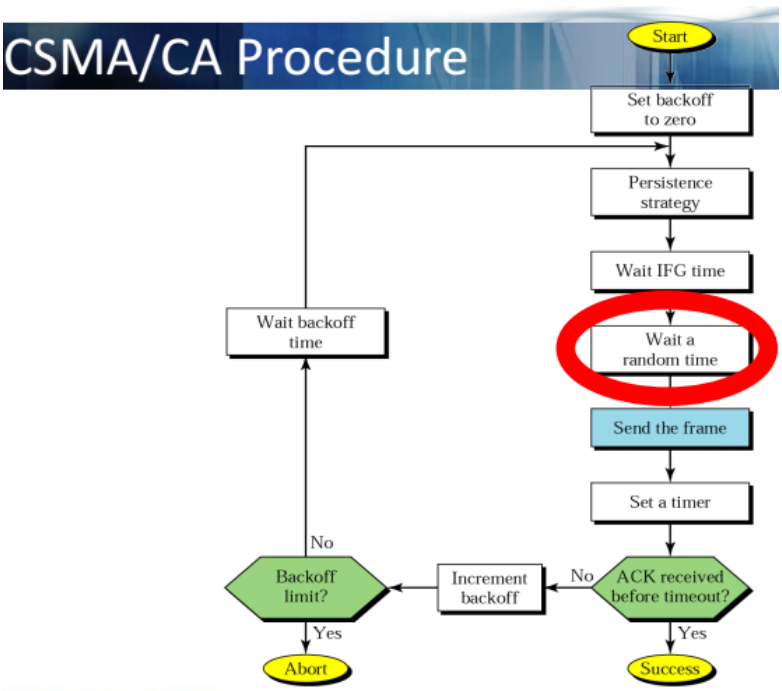
The checksum is added to the end of the message. This divided by the polynomial should give a remainder of zero if the message has been successfully transmitted. If not, the message has been corrupted.

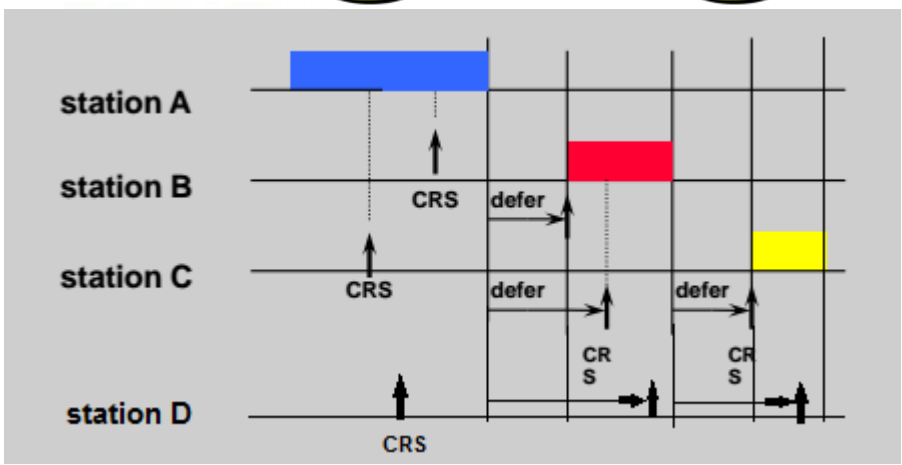
```
                ____________
                ............
                           0
```

**2) a) i)**

**Carrier Sense Multiple Access** with **collision avoidance** operates as follows for this scenario:

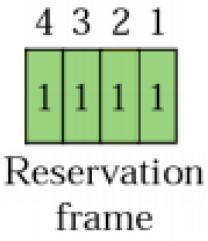
- Each station checks to see if the transmission medium is currently not being used.
- If it is the case that the medium is free, each station chooses a random time using binary exponential backoff and waits until that time has expired.
- Once that chosen time has passed, the station attempts to send the data.
    - Should the medium be in use, the station will wait for medium to become free once more before choosing a new backoff.
- Should a collision occur with two stations, *-+both will stop transmission, all will choose a new backoff as the medium is now free once more, and the process repeats.
- Should an ack from the receiver not arrive before the timeout occurs at a station, the backoff is incremented and the station attempts a retransmission.



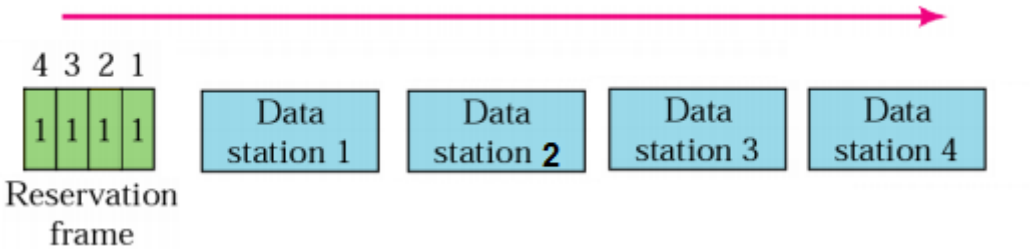
Time Division Multiple Access with a reservation protocol works as follows for this scenario:

- Stations who wish to transmit data register themselves as a 1 on the registration frame before the allocated transmission time begins.




In this scenario, frame will look like above

- This informs all the other stations about all planned communication.
- Each station registered to send then gets access to the full bandwidth for 1/ (number of users registered to transmit) of the time.
- This cycle will repeat until the stations are finished transmitting and no longer register in the reservation frame to transmit.

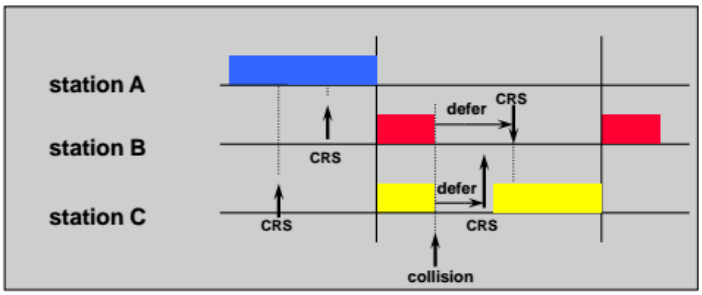



A sample time cycle of the TDMA with reservation

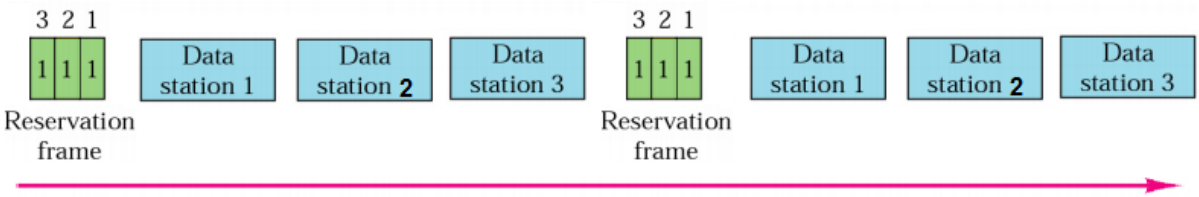
**ii)**

Contrast CSMA/CD against an 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 the frames.

- CSMA/CD




- **TDMA (wired)**




Data transmission for CSMA/CD only stops when a collision occurs and in the short time after while stations are doing their randomized binary exponential backoff, which grow for the

stations if more collisions occur. TDMA on the other hand, only stops sending data when the reservation frame is being filled out.

CSMA/CD also sends the entire data payload in one go, i.e. every packet sent until medium is free will contain only data from a single station. In comparison, TDMA will allow the sending packets, where every sequential sent packet is from a different source.

**2) b) i)**

Distributed Coordination Function (DCF)

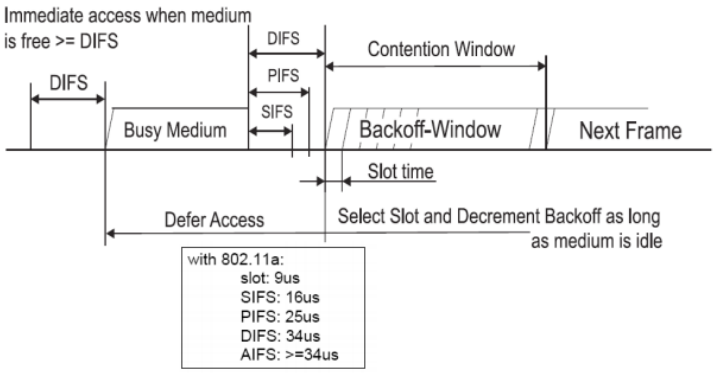
- Stations compete for access to the medium
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- No collision detection
    - Not practical on wireless network
    - Transmitting station cannot distinguish incoming weak signals from noise and effects of own transmission.

DCF is the basis of the standard CSMA/CA access mechanism. Like Ethernet, it first checks to see that the radio link is clear before transmitting. To avoid collisions, stations use a random backoff after each frame, with the first transmitter seizing the channel. In some circumstances, the DCF may use the CTS/RTS clearing technique to further reduce the possibility of collisions.

Point Coordination Function (PCF)

- Used by access points
- Point coordinator polls stations.
- Polling by centralized polling master – or point coordinator
- Uses PIFS
    - PIFS smaller than DIFS
    - Gives coordinator priority over individual stations
- Point coordinator polls in round-robin to stations configured for polling
    - When poll issued, polled station may respond within SIFS
    - If point coordinator receives response, it issues another poll

Coordinators are used to ensure that the medium is provided without contention. Point coordinators reside in access points, so the PCF is restricted to infrastructure networks. To gain priority over standard contention based services, the PCF allows stations to transmit frames after a shorter interval.



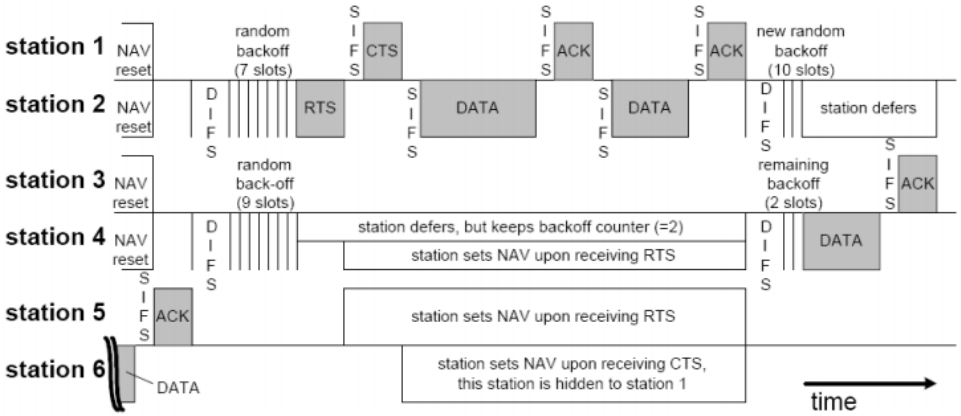

- Short IFS (SIFS) defines the minimum time between frames
- DCF IFS (DIFS) defines the time between the end of one transmission and the beginning of a subsequent transmission

Importance of interframe spaces: A station must sense the status of the wireless medium before transmitting. If it finds that the medium is continuously idle for **DCF Interframe Space** (DIFS) duration, it is then permitted to transmit a frame. If the channel is found busy during the DIFS interval, the station should defer its transmission. (Allows transmission of data without handshake if medium idle for allotted time)

**2) b) ii)**

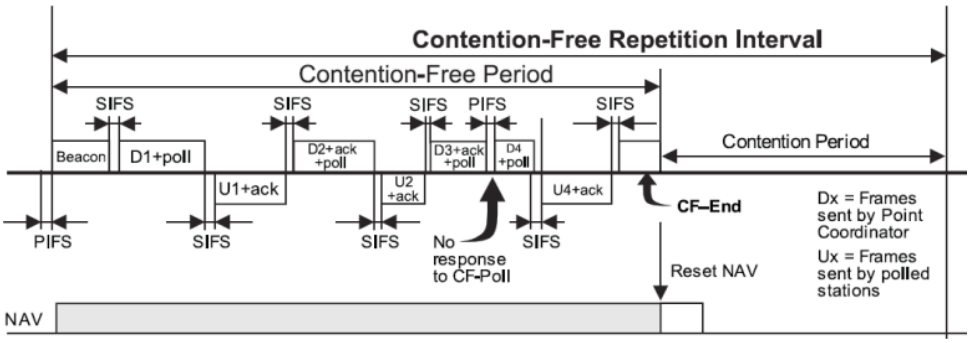
Explain the coordination of communication between an access point and 5 laptops when using DCF and when using PCF.

**DCF**




Like these but with 5 stations

**PCF**

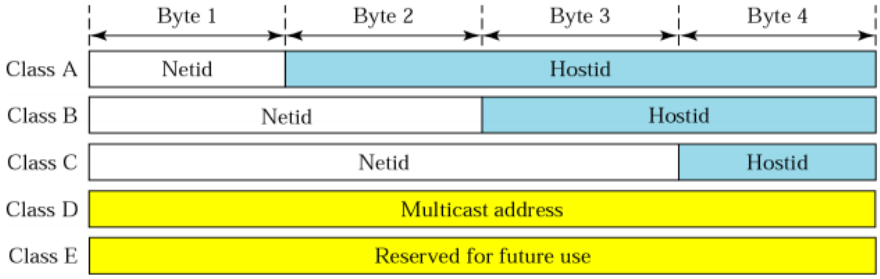


Question 3)

a) 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.

**3) a) i)** Classful addressing divides an IP address into 4 possible classes, based on the number of devices required by the Network.




In a **Class A** network, the first byte of the IP address is used to specify the Network address, and the following 3 bytes are used as Host addresses. As a result, this allows for $2^7$-2 (126) Network addresses (127 is reserved for loopback) and $2^{24}$-2 Host addresses (A Host address with all zeroes is the network number, and a host address consisting of all 1s is the broadcasting IP). Directed at international organisations.

Similarly, in a **Class B** address, the first two bytes of the IP address represent the network ID, and the following 2 bytes represent the Host Address, giving $2^{14}$ Network addresses and $2^{16}$ Host addresses. Directed at large companies.

Class C uses the first three bytes to represent the network ID, and the final byte to represent the host address.

Etc.

It's seems that Classes A, B and C are in actual use. Then D is reserved for multi-casting groups where packets are sent from one sender to many receivers and the E has been reserved for future use and Research & Development. I think this diagram is pretty misleading as A, B, C don't actually use up all the space the diagram says they do.

I found this https://www.computerhope.com/jargon/i/ip.htm article the most useful
I hope that clears something up but I'm not 100% sure myself =)

Another source had this to say:
https://superuser.com/questions/394407/how-does-cidr-slow-the-exhaustion-of-ipv4
"under the classful scheme, ½ of the entire IPv4 address space was reserved as 128 class A networs, ¼ was reserved for class B networks, ⅛ was reserved for class C networks, $^1/_{16}$ was reserved for class D (multicast), and the last $^1/_{16}$ was reserved for class E (undefined future use)."

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

**ii)** NAT is a method of mapping one IP address space to another by modifying packets as they cross a Routing Device. It is mostly used to hide an entire IP address space behind a single private IP address. The hidden address is changed into a single public IP address as the new source of an outgoing packet, which then appears to have originated at the Routing Device rather than the hidden host. This is used to reduce the effects of IPv4 exhaustion, as the hidden IP address space can be reused across Networks, and a single IP address can be mapped to an entire Network via the Routing Device.

CIDR is a means of breaking up classes of IPv4 address into more manageable and distributable chunks. Before CIDR a company (eg Ford Motors) would be allocated an entire Class A Network, So Ford has 16,777,216 addresses allocated to it, even though it only has 160,000 employees worldwide. Does Ford really need over 100 publicly-routable addresses per employee? Probably not, so CIDR is able to break that network down and distribute it based on demand and necessity.

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

IPv6 is a big IP address written in hexadecimal and separated by semicolons. (128 bits). More addresses moar internets devices. Less need for NAT as each device can have a unique IP.