

**Assignment Cover Sheet**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Student name:** | **Sarah Narayamy Tavares Silva** | | | | | |
| **Student number:** | **2960992** | | |  | | |
| **Faculty:** | **Computing** | | |  | | |
| **Course:** | **Computing Science** | | | **Stage/year:** | **3** | |
| **Subject:** | **Networks and Data Communications** | | | | | |
| **Study Mode:** | Full time | **X** |  | Part-time |  |  |
| **Lecturer Name:** | **Brendan Fogarty** | | | | | |
| **Assignment Title:** | **Tutorial Sheet 2** | | | | | |
| **No. of pages:** |  | | |  | | |
| **Disk included?** | Yes |  |  | No | **X** |  |
| **Additional Information:** | (ie. number of pieces submitted, size of assignment, A2, A3 etc) | | | | | |
|  | | | | | |
|  | | | | | |
| **Date due:** | **08/10/2019** | | |  | | |
| **Date submitted:** |  | | |  | | |
|  | | | | | | |
| **Plagiarism disclaimer:**  *I understand that plagiarism is a serious offence and have read and understood the college policy on plagiarism. I also understand that I may receive a mark of zero if I have not identified and properly attributed sources which have been used, referred to, or have in any way influenced the preparation of this assignment, or if I have knowingly allowed others to plagiarise my work in this way.*  *I hereby certify that this assignment is my own work, based on my personal study and/or research, and that I have acknowledged all material and sources used in its preparation. I also certify that the assignment has not previously been submitted for assessment and that I have not copied in part or whole or otherwise plagiarised the work of anyone else, including other students.*  **Signed: Sarah Narayamy Tavares Silva Date:** | | | | | | |

## **Please note:** Students **MUST** retain a hard / soft copy of **ALL** assignments as well as a receipt issued and signed by a member of Faculty as proof of submission.

**Question 01: Error Control**

1. **Compare the Single Bit Parity and CRC error checking mechanisms under three appropriate headings.**

Please Note: *One of the headings must be the error detection capability.*

CRC error checking mechanism can detect burst errors while Single bit parity mechanism as the name says can only detect a single error.

Parity check is done by adding an extra bit to make a number either even or odd depending on which one you are using. The CRC involves binary division of the data by a divisor generated by using polynomials.

Parity check is a very simple mechanism while CRC is quite complex to apply because involves the divisor, polynomials and a long division.

**Question 2: Single Bit Parity**

1. **The following bit patterns are being prepared for transmission, state the bit pattern transmitted in each scenario**.

Please Note: You must clearly show all workings and state any assumptions in your solution.

Assuming a single bit parity is ODD

1. 01111000

* Count the numbers of 1’s = 4
* Since the count is an even number, we must append a 1 at the end to be the parity bit in order to get a correct ODD number.
* The message sent altogether is = 011110001

1. 00110101

* Count the numbers of 1’s = 4
* Since the count is an even number, we must append a 1 at the end to be the parity bit in order to get a correct ODD number.
* The message sent altogether is = 001101011

1. 1011000

* Count the numbers of 1’s = 3
* Since the count is an ODD number, we must append a 0 at the end to be the parity bit so the number of 1’s stays an ODD number.
* The message sent altogether is = 10110000

1. **Show with the aid of an example how a receiver can detect an error in a received bitstream if single bit parity is the error checking mechanism.**

The receiver must ensure that the total number of 1’s of the data plus the parity bit is ODD or EVEN, depending on which error checking mechanism is being used.

Assuming we are using the EVEN error checking mechanism, the receiver receives the following message:

110011001

In which the last 1 is the parity bit.

If we count the number of 1’s before the parity bit, we find 4. Thus when we sum the number of 1’s and the parity bit we end up with 5 which is an ODD number. Since we are using the EVEN error checking mechanism, the fact that this sum is an ODD number indicates that there is an error in the message.

**Question 3: CRC**

1. **A communications system is using CRC as the error checking mechanism, if the data to be transmitted is 0101111000 and the generator polynomial is** **X3 + X + 1, determine the bit pattern that will be transmitted.**

Please Note: You must clearly show all workings and state any assumptions in your solution.

1. Use the polynomial to generate the binary divisor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Polynomial** | **X3** | **X2** | **X1** | **+1** |
| **Divisor** | 1 | 0 | 1 | 1 |

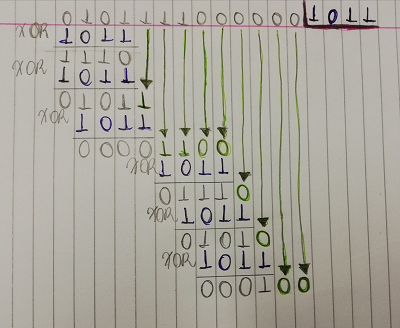
1. The number of dummy bits to append to the data is equal to the width of the divisor minus 1.

Dummy bits = 4 - 1 = 3

1. The dummy bits are appended to the data:

0101111000000

1. Do the long division using the XOR subtraction.



The last 3 digits of the remainder is used to append CRC to the data to be transmitted, which will be:

0101111000100

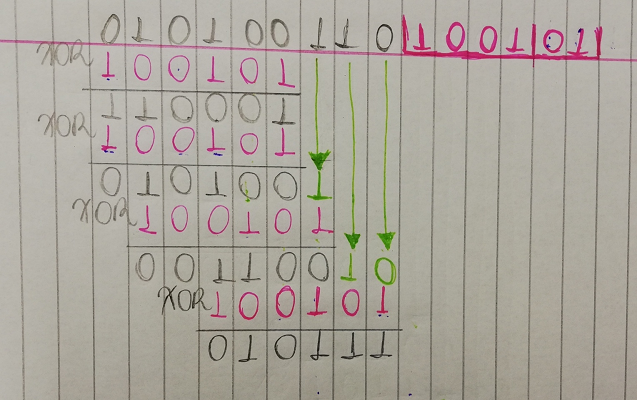
1. **A communications system is using CRC as the error checking mechanism, if the receiver receives the following bit pattern 010100110, determine if the received bit pattern has errors if the generator polynomial used to generate the CRC was X5 + X2 + 1**

Please Note: You must clearly show all workings and state any assumptions in your solution.

1. Use the polynomial to generate the binary divisor

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Polynomial** | **X5** | **X4** | **X3** | **X2** | **X1** | **+1** |
| **Divisor** | 1 | 0 | 0 | 1 | 0 | 1 |

1. Do the long division using the XOR subtraction.



Compare the last 3 digits of the remainder of the division with the last 3 digits of the received pattern:

Remainder = 111

Received = 110

When there is no match in this comparison, it means that there is an error in the bit pattern

**Question 4: Block Parity**

**A communications system is using Block Parity as the error control mechanim. A TX is preparing the following bit pattern for transmission 0101111010100011110000011000 Determine the bit pattern to be transmitted stating any assumptions in your solution**.

Assuming the block parity is even

1. Build the table with parity column and parity row following the bit pattern transmission and adding the parity bit at the end of each column and each row according to the block parity chosen (in this case even).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **0** | **1** | **0** | **1** | **1** | **1** | **1** | **1** |
| **0** | **1** | **0** | **1** | **0** | **0** | **0** | **0** |
| **1** | **1** | **1** | **1** | **0** | **0** | **0** | **0** |
| **0** | **0** | **1** | **1** | **0** | **0** | **0** | **0** |
| **1** | **1** | **0** | **0** | **1** | **1** | **1** | **1** |

1. The bit pattern to be transmitted is the whole sequence that was created in the table, row by row:

01011111 01010000 11110000 00110000 11001111

**Question 5: Framing 01**

1. **In the context of data communications, define what a frame is.**

A frame is a data transmission unit used at the layer 2 (data link layer) of the OSI model, after the packets were encapsulated from the Network Layer; they have a header which indicates the beginning and end of a block of data. If a frame becomes too large, the packet would be divided into smaller frames, making the flow control and error control more efficient. It contains four parts: Frame header which contains the source and the destination addresses of the information; Payload field which contains the message to be delivered; Trailer which contains the error detection and error correction bits and a Flag which marks the beginning and end of the frame.

1. **With the aid of diagrams, explain any two approaches to framing.**

* **Character based framing**: this approach is suitable for transmission of texts as the flag is chosen as a character that is not used for text encoding. The biggest problem of this protocol is whether the pattern of the flag byte is present in the message byte sequence. In order to not misinterpret this flag byte during the message as the flag that determines the end of the frame, byte stuffing mechanism is used by adding a special byte such as End Delimiter (ED) before every byte in the message with the same pattern as the flag byte. The disadvantage of this approach is that by adding too much bytes on the message, it increases the size of the frame.
* **Bit oriented framing:** this approach is suitable for transmitting any sequence of bits as the data is transmitted as a sequence of bits that can be interpreted either as text of multimedia data. In this protocol the flags are a bit pattern of generally 8-bits and comprises of six or more consecutive 1s (usually 01111110 is used). In order to not misinterpret this flag bit pattern during the message as the flag that determines the end of the frame, a bit- stuffing mechanism is used by adding an extra 0 bit whenever a 0 bit is followed by five consecutive 1 bits in the message. The same extra bit is removed by the receiver when it gets the message and sends the un-stuffed message to the upper layers.

**Question 6: Framing 02**

1. **HDLC is a protocol used at the data link layer of the OSI model. A TX is preparing the following bit pattern for transmission: 01110100100000101000000. Show the bit pattern after the TX bit stuffs it.**

HDLC protocol determines that after every five consecutive 1’s a 0 will be stuffed in order to differentiate from the flag which contains 6 consecutive 1’s. In this case, reading from right to left, we can see that there is no sequence of five 1’s, which means that the bit pattern for transmission will not be changed by Tx, thus the message to be sent will be as follow:

**01110100100000101000000**

1. **HDLC is a protocol used at the data link layer of the OSI model. A RX receives the following bit pattern: 1000010001010000001000 Show the bit pattern after the TX bit strips it.**

As mentioned in section a of this exercise, an additional 0 will be stuffed after five consecutive 1’s in the bit pattern. When the receiver (Rx) receives the message it does the opposite by stripping the same 0 that was previously added by Tx. Thus, Rx will be searching for a sequence of five 1’s and remove the following 0. In this case, reading from right to left, we can also see that there is no five consecutive 1’s in the bit pattern so the message to be read will be as follow:

**1000010001010000001000**

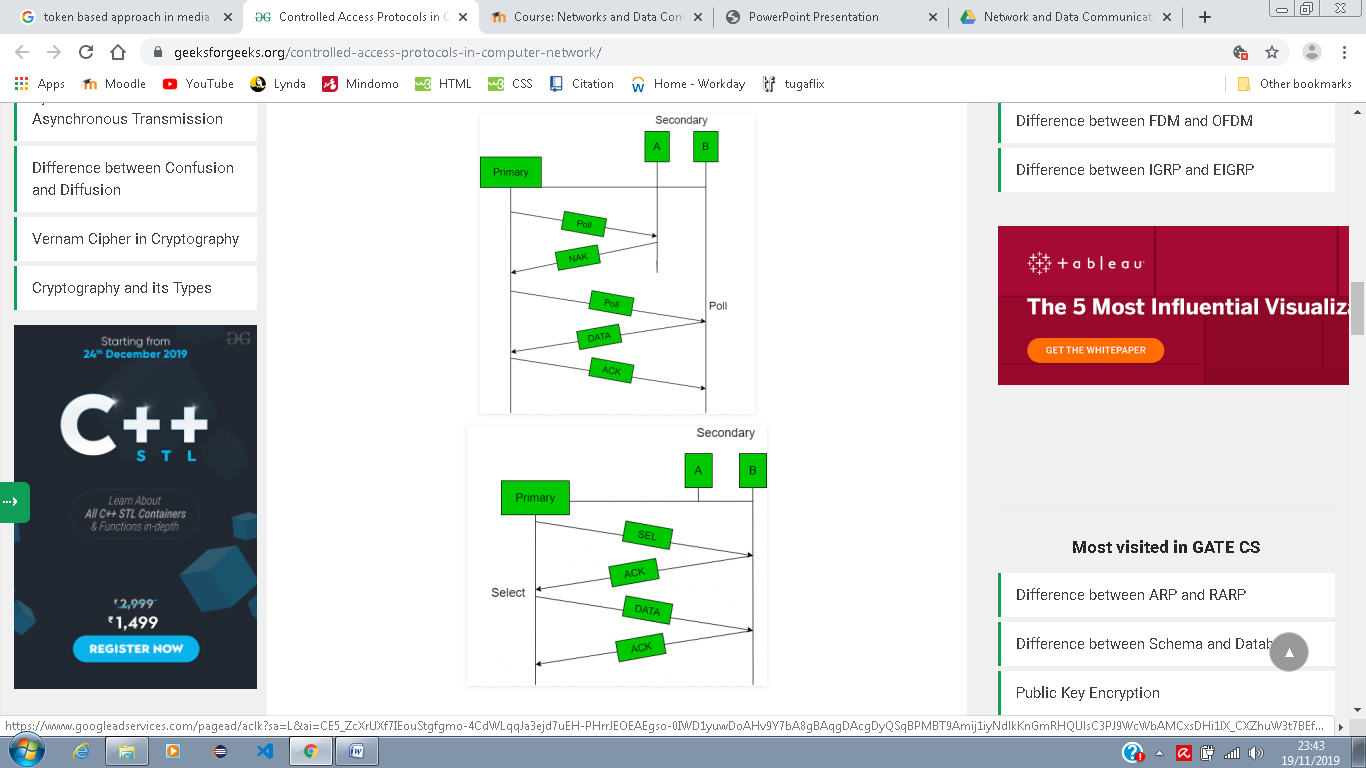
**Question 7: Media Access Control**

1. **Explain what Media Access Control is and why it is necessary.**

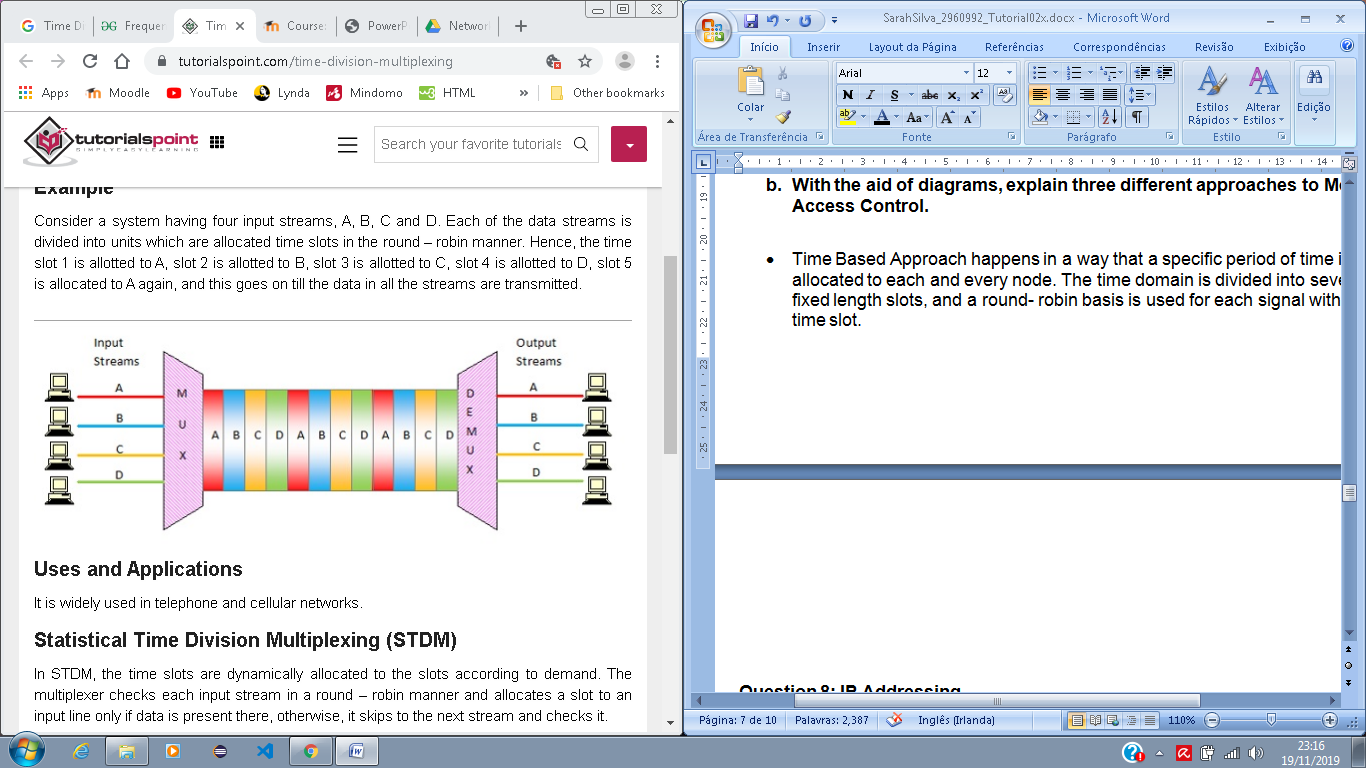
Media Access Control or MAC is a sub layer of the layer 2 (Data Link Layer) in the OSI model. MAC is used to provide an addressing mechanism and allow each node available on a network to communicate with other nodes either on the same or a different network.

1. **With the aid of diagrams, explain three different approaches to Media Access Control.**

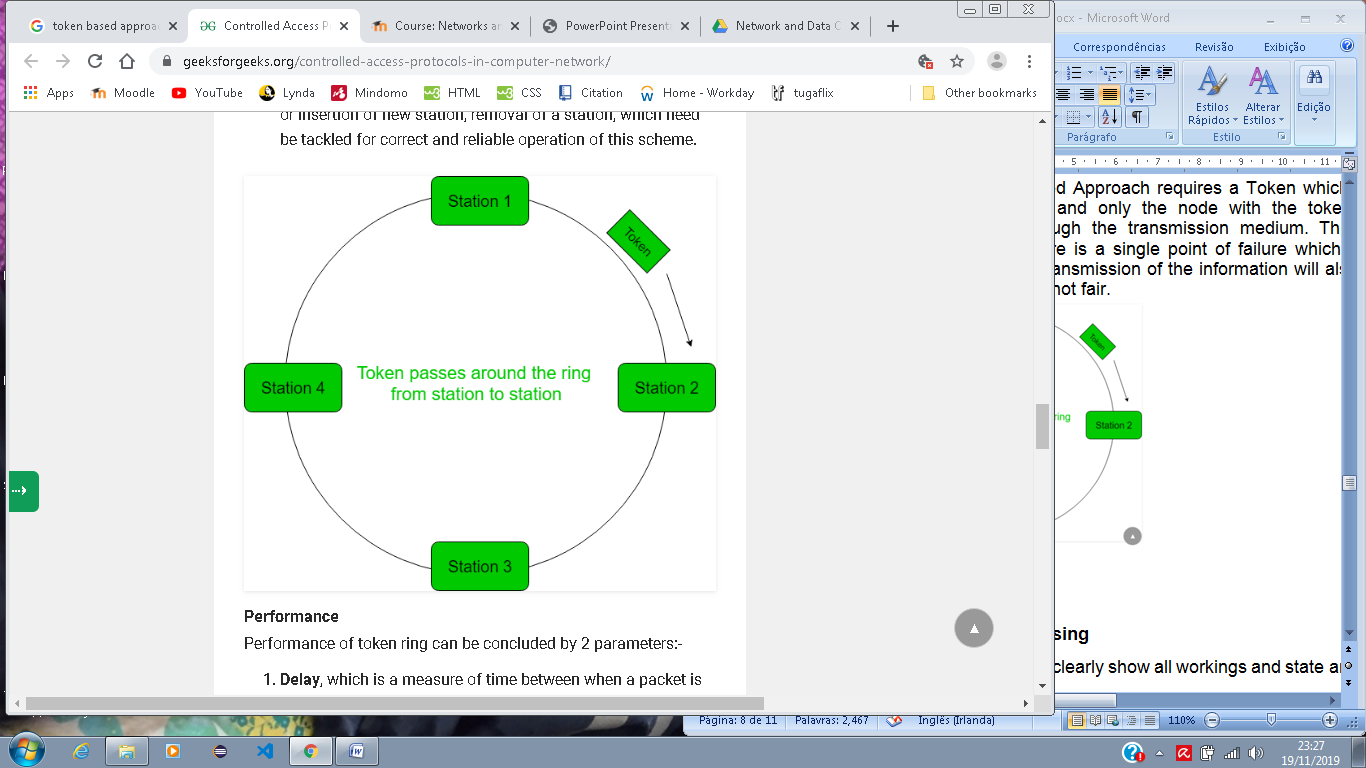
* In the Polling approach, a Controller (primary station), controls access to the transmission medium. The secondary stations ask the controller for access to the transmission medium. Thus, if the transmission medium is busy, the access is denied but if the transmission medium is free, the access is granted. This approach avoids collision but the controller can be a point of failure in case it is corrupted.



* Time Based Approach happens in a way that a specific period of time is allocated to each and every node. This approach is meant to be fair as all nodes has its time, but on the other hand, the data transfer rate is slow and the transmission medium is idle if a node has no data to transmit.



* The Token Based Approach requires a Token which is passed on from Node to Node and only the node with the token can transmit the information through the transmission medium. This technique avoids collision but there is a single point of failure which is the token, if it is corrupted, the transmission of the information will also be affected, also, this approach is not fair.

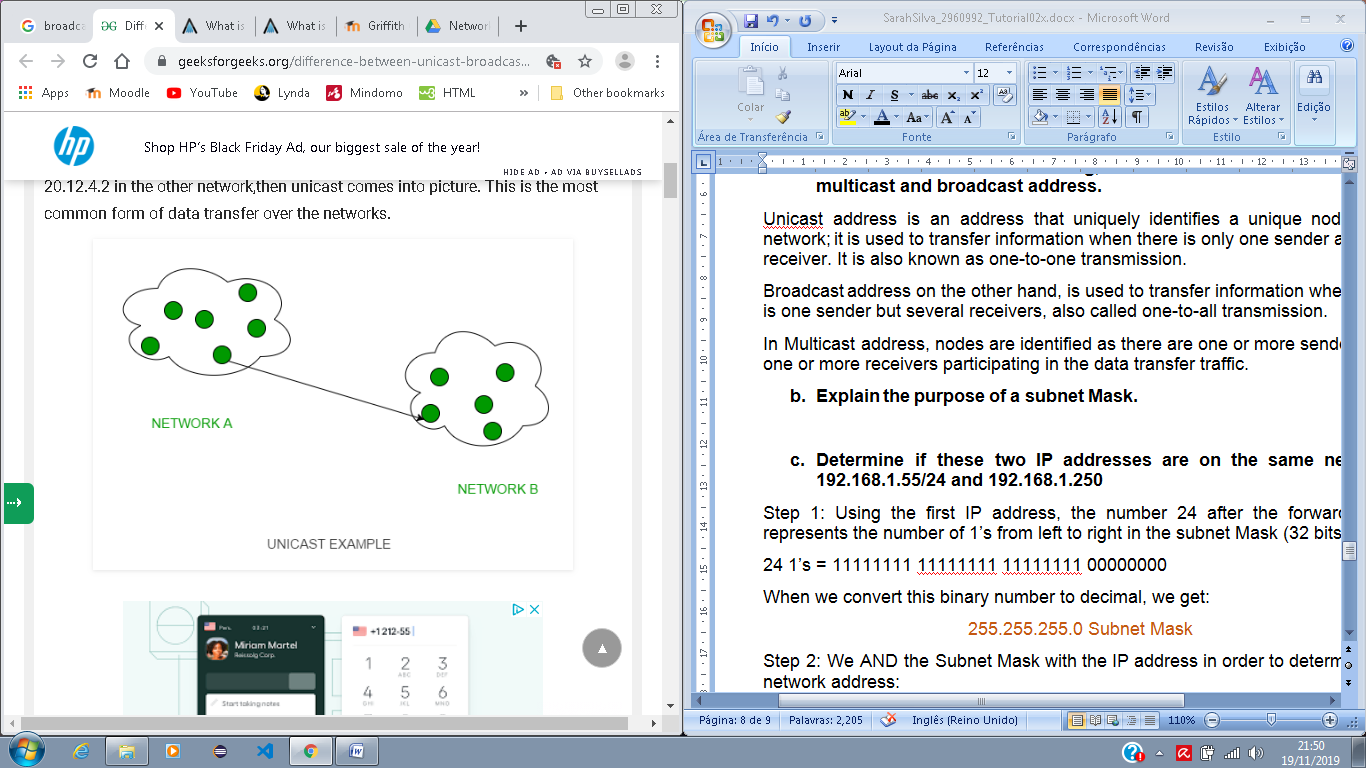


**Question 8: IP Addressing**

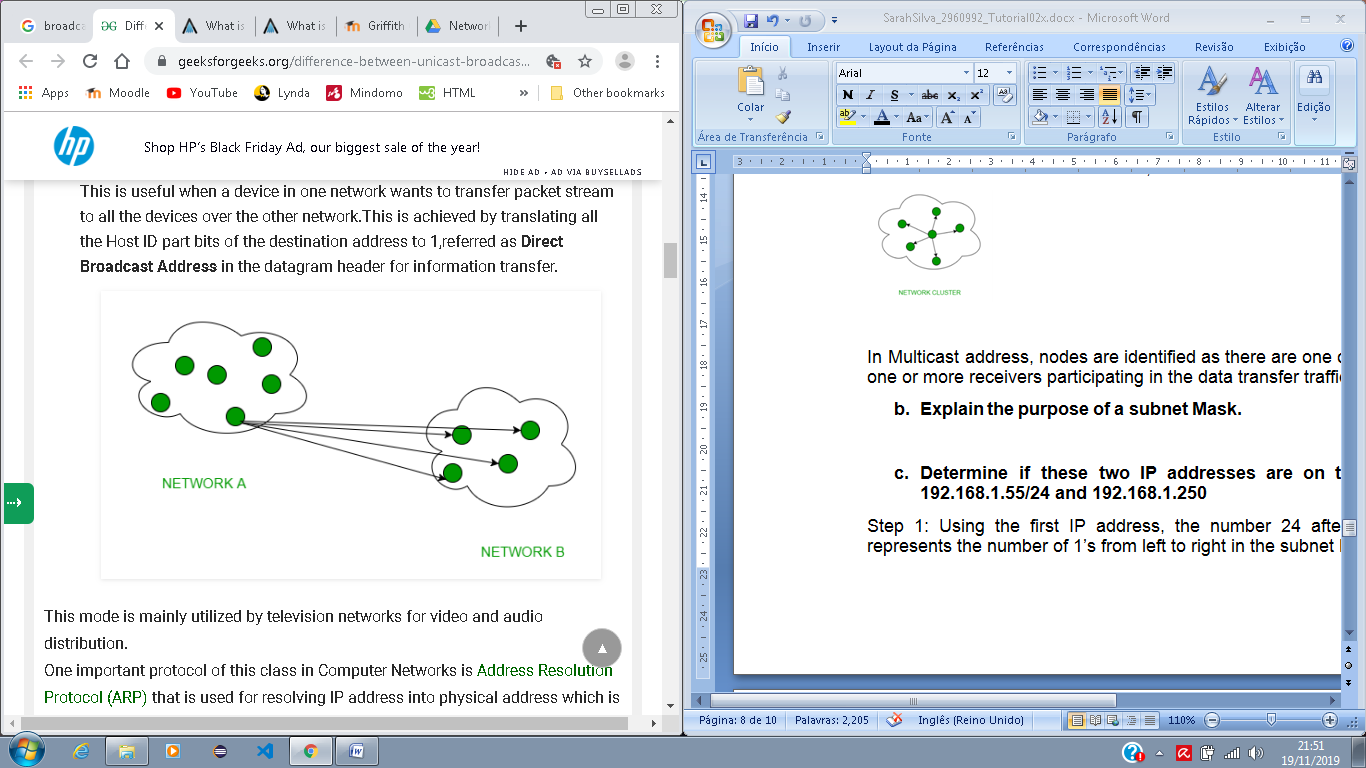
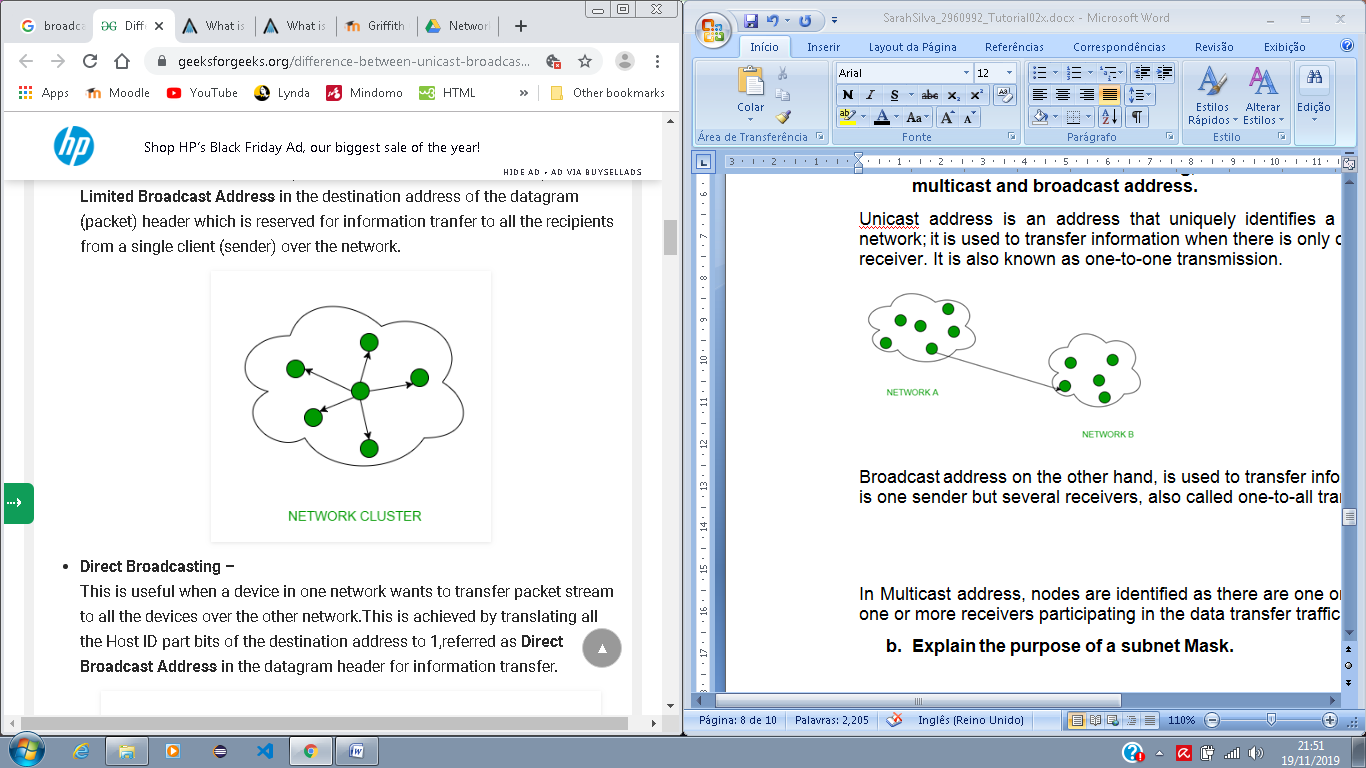
Please Note: You must clearly show all workings and state any assumptions in your solution.

1. **In relation to IPv4 addressing, differentiate between a unicast, multicast and broadcast address.**

Unicast address is an address that uniquely identifies a unique node on a network; it is used to transfer information when there is only one sender and one receiver. It is also known as one-to-one transmission.



Broadcast address on the other hand, is used to transfer information when there is one sender but several receivers, also called one-to-all transmission.



In Multicast address, nodes are identified as there are one or more senders and one or more receivers participating in the data transfer traffic.

1. **Explain the purpose of a subnet Mask.**

The purpose of a Subnet Mask is to define a range of IP addresses to be used within a network. It uses the format as an IPv4 address with four sections of 8 bits numbers separated by dots. Each of these sections can vary from 0 to 255. The IP addresses of each device within a network will depend on how the Subnet Mask is presented. For example, if the Subnet Mask is a typical class C IP address such as 255.255.255.0; because the three first sections of the Subnet Mask are full (255 out of 255), the first three sections of the devices must be also identical; and the last section of the devices can be anything from 0 to 255. Thus any device could have an IP address such as 100.20.1.99 and 100.20.1.240 but not 100.10.1.99.

1. **Determine if these two IP addresses are on the same network: 192.168.1.55/24 and 192.168.1.250**

Step 1: Using the first IP address, the number 24 after the forward slash represents the number of 1’s from left to right in the subnet Mask (32 bits).

24 1’s = 11111111 11111111 11111111 00000000

When we convert this binary number to decimal, we get:

255.255.255.0 Subnet Mask

Step 2: We AND the Subnet Mask with the IP address in order to determine the network address:

192.168.1.55

AND

255.255.255.0

192.168.1.0 Network Address

Step 3: We OR the Network Address with the inverted Subnet Mask in order to determine the Broadcast Address:

192.168.1.0 Network Address

OR

0.0.0.255 Inverted Subnet Mask

192.168.1.255 Broadcast Address

Step 4: Comparing the two IP address from the question, they are both in the same network because they both have the first three sections identical and the last section vary from 1 to 254.

**Question 9 and 10: Network Simulation**

**Use PacketTracer to simulate two networks which are separated by a router. Network 1 will contain 4 PCs and a printer. Network 2 will contain a server with Web, DHCP and DNS enabled. These services will be available to the devices on Network 1. The DNS Server table should contain a single entry YourNameYourStudentNumber.com (e.g. BrendanFogarty0123456789.com). The DHCP server should serve out IP addressing info to the PCs on Network1. The number of addresses served out should be equivalent to the last two digits of your student number + 5. (For example, if the last two digits of your student number are 37, your DHCP server should have a total of 42 addresses in its Pool).**

