Tutorial 1: Introduction to Networking

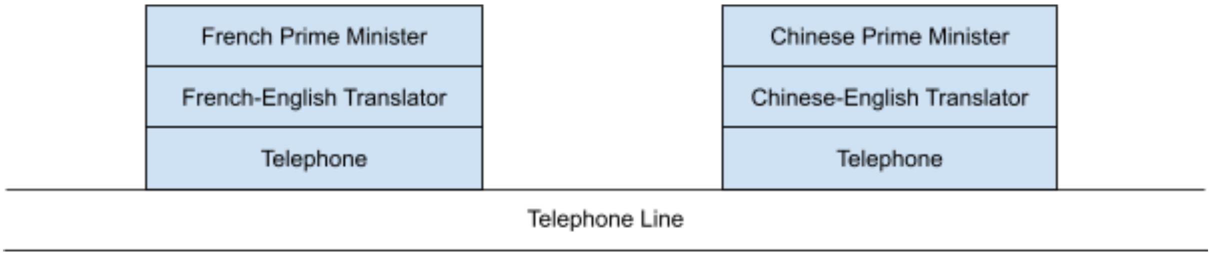
Question 1

Part A

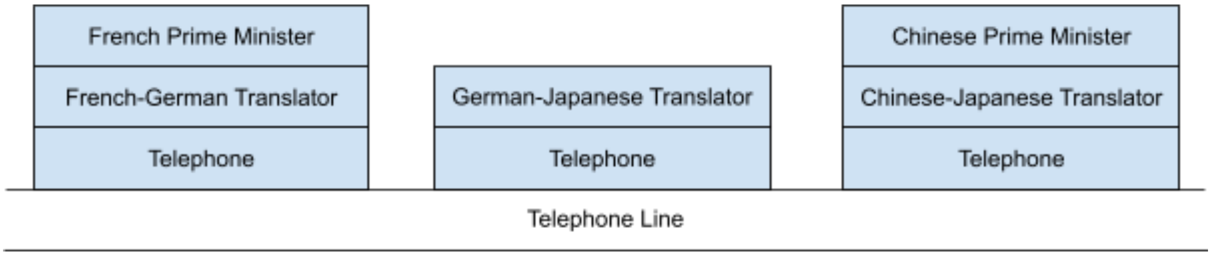
Function	Layer of the OSI Model	Model of the TCP/IP Model
Dividing the transmitted bit stream into frames	Data Link	Network Access
Determining which route to use through the subnet (LAN)	Network: LAN	Network Access
Determining which route to use through the internet	Network: Internet	Internet
Determining which application to communicate with in a remote host	Transport	Transport

Question 2

Part A



Part B



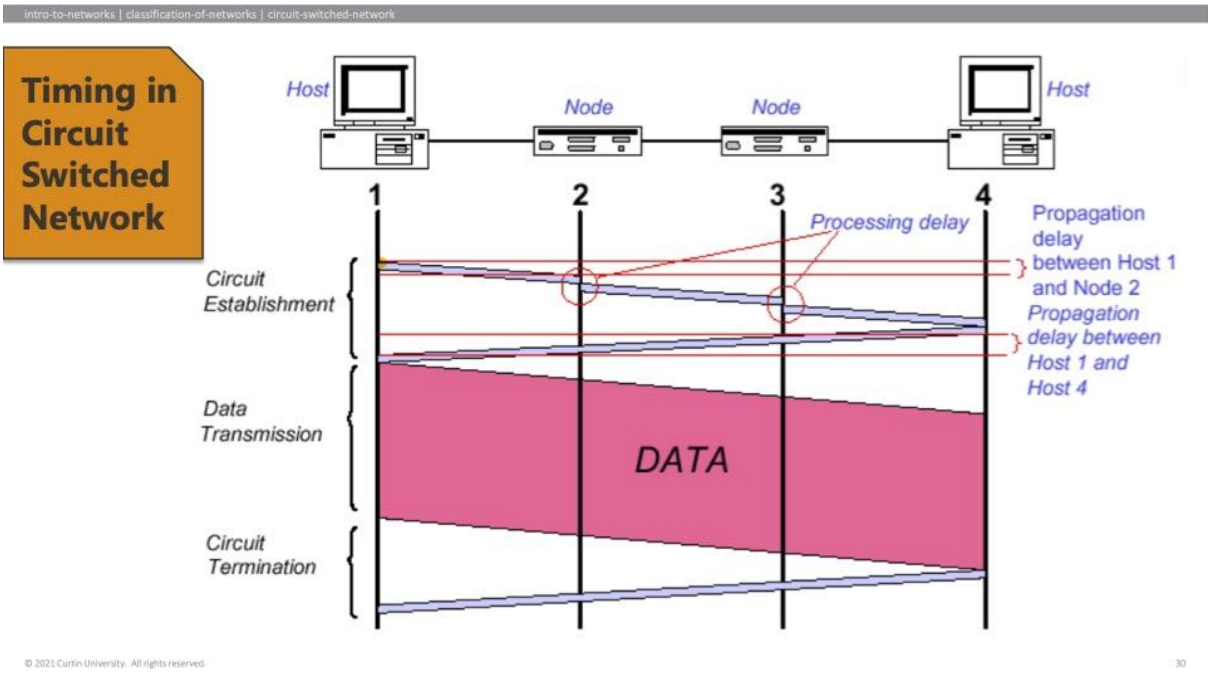
Question 3

- $size = (650 \times 100)\ MB$
  $size = (650 \times 100 \times 1000)\ KB$
  $size = (650 \times 100 \times 1000 \times 1000)\ B$
  $size = (650 \times 100 \times 1000 \times 1000 \times 8)\ b$
- $time = 4.5\ hr$
  $time = (4.5 \times 60)\ min$
  $time = (4.5 \times 60 \times 60)\ s$

- $bandwidth = size \, / \, time$
  $bandwidth = (650 \times 100 \times 1000 \times 1000 \times 8) \, / \, (4.5 \times 60 \times 60) \; bps$
  $bandwidth \approx 32 \; bps$

Question 4

Part I



intro-to-networks | classification-of-networks | circuit-switched-network

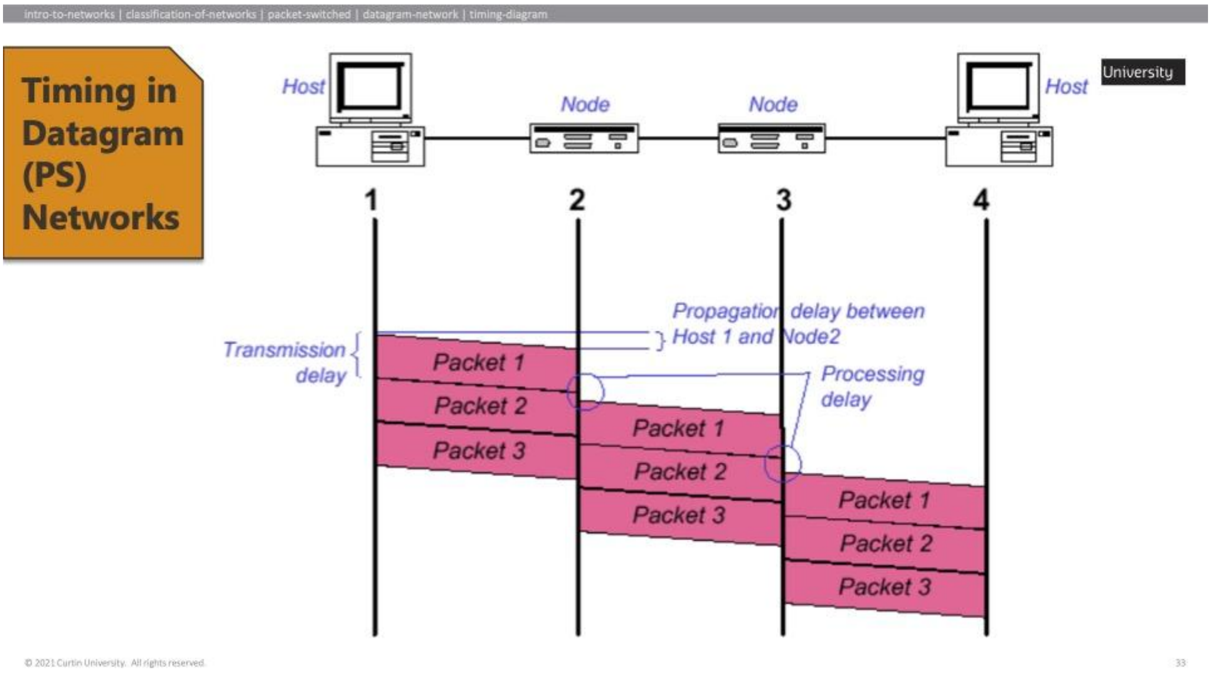
Timing in Circuit Switched Network

© 2021 Curtin University. All rights reserved.

30

$$delay = N \times D + L \div B$$

Part II



intro-to-networks | classification-of-networks | packet-switched | datagram-network | timing-diagram

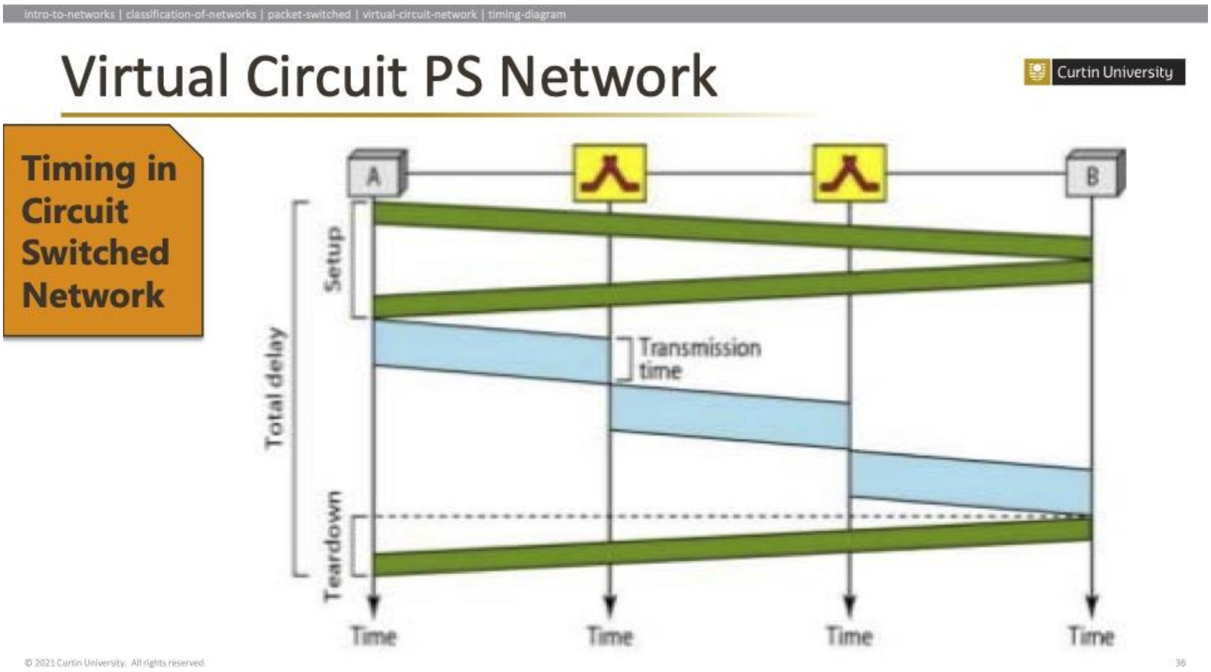
Timing in Datagram (PS) Networks

© 2021 Curtin University. All rights reserved.

33

$$delay = N \times D + N \times (P \div B)$$

Part III



intro-to-networks | classification-of-networks | packet-switched | virtual-circuit-network | timing-diagram

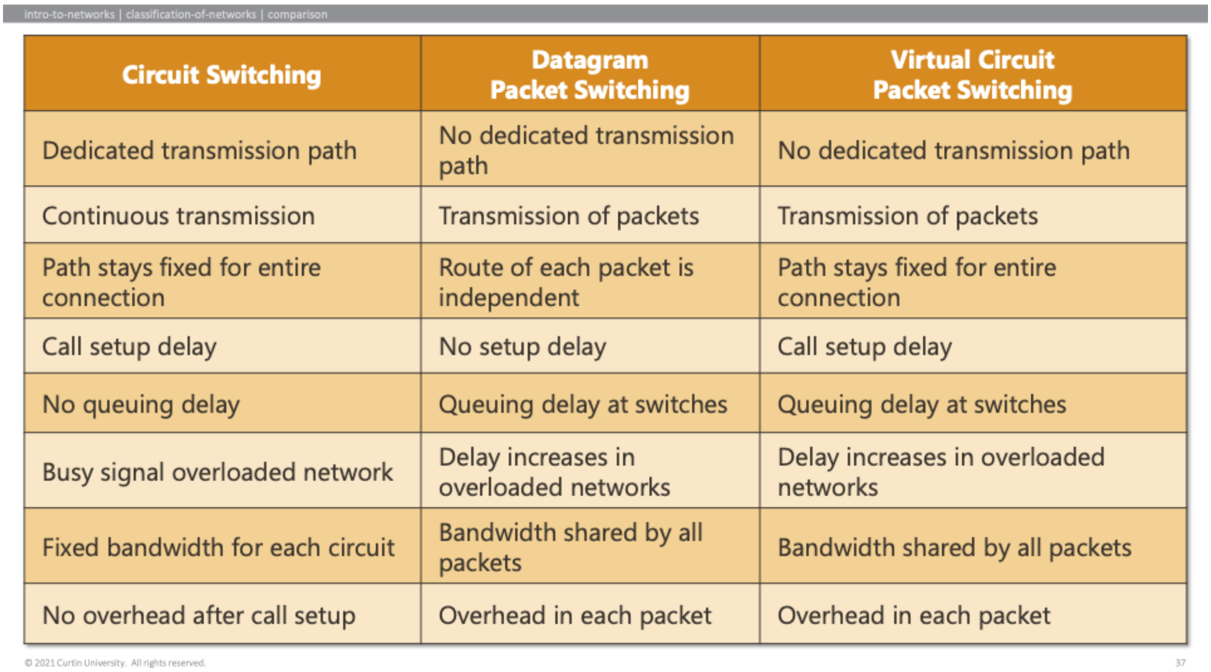
Virtual Circuit PS Network

Curtin University

Timing in Circuit Switched Network

$$delay = (NP + N - 1) \times (P \div B) + N \times D,\ where\ NP = [L \div (P - H)]$$

Question 5



intro-to-networks | classification-of-networks | comparison

Circuit Switching	Datagram Packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated transmission path	No dedicated transmission path
Continuous transmission	Transmission of packets	Transmission of packets
Path stays fixed for entire connection	Route of each packet is independent	Path stays fixed for entire connection
Call setup delay	No setup delay	Call setup delay
No queuing delay	Queuing delay at switches	Queuing delay at switches
Busy signal overloaded network	Delay increases in overloaded networks	Delay increases in overloaded networks
Fixed bandwidth for each circuit	Bandwidth shared by all packets	Bandwidth shared by all packets
No overhead after call setup	Overhead in each packet	Overhead in each packet

- An example of a Circuit Switching network is a Public Switched Telephone Network (PTSN)
- An example of a Datagram Packet Switching network is the internet
- An example of a Virtual Circuit Packet switching network is Async Transfer Mode (ATM)
    - However, ATM networks have become obsolete since modern-day PS networks are more reliable

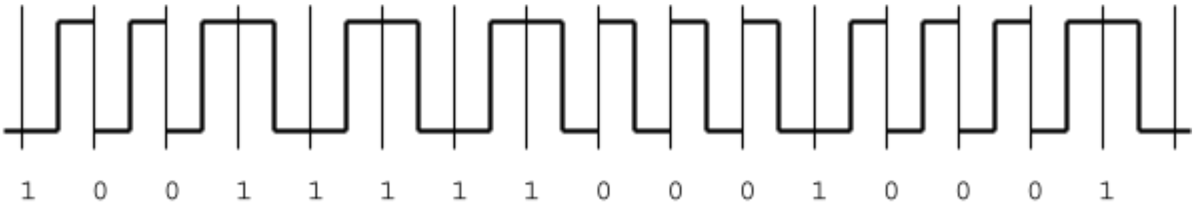
Tutorial 2: Physical Layer

Question 1

- $sum =- 5 - 3 - 3 - 8 + 10 + 6 + 12$
  $sum = 9\ Db$
- $9 = 10log(p_2 \div p_1),\ where\ p1 = 1\ W$
  $9 = 10log(p_2)$
  $p_1 = 10^{(9 \div 10)}\ W$

Question 2

Differential Manchester Encoding



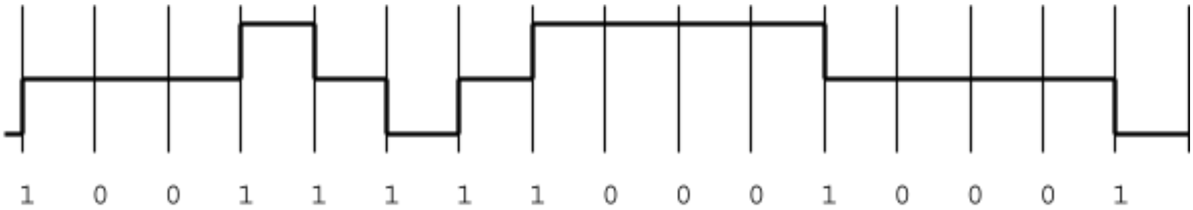
Definitions

- 1: *no transition*
- 0: *transition*

Notes

- The initial power level is 1

MLT-3 Encoding



Definitions

- 1: *transition*
- 0: *no transition*

Question 3

Bandwidth is the maximum amount of data transfer per second. *Speed* is the end-to-end data transfer per second. *Latency* (a.k.a delay or lag) is the amount of time it takes for data to travel from its source to its destination. *Throughput* is the actual amount of data transfer per second (after taking into account latency, network speed, packet loss etc).

Question 4

Some last mile technologies include: Dialup, ISDN, NBN and Cellular (5G). The key significance of NBN is that it is the national network of communication infrastructure currently being built on behalf of the federal government. It is mainly used for internet and phone [Voice over Internet Protocol (VoIP)] and aims to deliver network speeds of 50Mbps to 1Gbps. NBN also makes use of fiber optic cable.

Question 5

Millimeter waves are higher frequency radio waves that can carry more data and they are from a lesser used band of the frequency spectrum (i.e. it is less congested). These waves support having a massive Multiple-input and Multiple-output (MIMO) antenna since the relationship between the wave frequency and antenna size is inversely proportional. This disadvantage of millimeter waves (or more generally, high frequency waves) is that they have more collisions with obstacles in the air and/or on the ground, and therefore, service shorter distances than 4G.

Tutorial 3: Data Link Layer I

Curtin University

Data Link Layer I

Prof. Ling Li | Dr. Nadith Pathirage | Tutorial 03

Semester 1, 2021

Q1

Consider the case of transmitting 1250 Bytes frame over on a link with a delay of 200ms (millisecond) when the length of the link is 200km. Assume that acknowledgment packets are of negligible size, processing time at a node is negligible, and the link is error-free.

Calculate the transmission efficiency of the following ARQ methods if the transmission rates are 1Kbps, 1Mbps, 1Gbps and the lengths of the same link are 20Km, 200Km, 2000Km, 20000Km respectively.

a. Stop-and-wait ARQ?

b. Go-Back-N ARQ where W is large enough to keep the channel fully busy?

c. Selective-Repeat ARQ where W is 7?

Q1

Frame Size = L = 1250 * 8 bits = 10000 bits

Prop rate = 200km/(200*10^{-3}s) =1000 km/s

T_{frame} = L / (Transmission rate) (in seconds)

T_{prop} = Distance / (Prop rate)   (in seconds)

Stop-and-wait ARQ

$$S = \frac{1}{1+2a}$$

i) T_{frame} = L / (Transmission rate) = 10000 / 1000 = 10s

T_{prop} = Distance / (Prop rate) = 20 /1000 = 0.02s

$a = T_{prop} / T_{frame} = 0.02/10 = 0.002$ $s = 1/ (1+2a) = 1/1.002 = 0.996\ (99.6\%)$

ii) T_{frame} = L / (Transmission rate) = 10000 / 1000000 = 0.01s

T_{prop} = Distance / (Prop rate) = 2000 /1000 = 2s

$a = T_{prop} / T_{frame} = 2/0.01 = 200$ $s = 1/ (1+2a) = 1/401 = 0.0025\ (0.25\%)$

Distance Transmission rate	20Km	200Km	2000Km	20000Km
1Kbps	99.8%			
1Mbps			0.25%	
1Gpbs				

Go-Back-N ARQ with a large W

…… (W >= 2a + 1) to keep the channel fully busy?

$$S = \begin{cases} 1, & \boldsymbol{W \geq 2a + 1} \\ \dfrac{W}{(2a+1)}, & \boldsymbol{W < 2a + 1} \end{cases}$$

s = 1

Selective-Repeat ARQ where W = 7

Curtin University

$$S = \begin{cases} 1, & \boldsymbol{W \geq 2a+1} \\ \dfrac{W}{(2a+1)}, & \boldsymbol{W < 2a+1} \end{cases}$$

i) T_{frame} = L / (Transmission rate) = 10000 / 1000 = 10s

T_{prop} = Distance / (Prop rate) = 20 /1000 = 0.02s

a = T_{prop} / T_{frame} = 0.02/10 = 0.002 $W \geq 2a+1$ s = 1

ii) T_{frame} = L / (Transmission rate) = 10000 / 1000000 = 0.01s

T_{prop} = Distance / (Prop rate) = 2000 /1000 = 2s

a = T_{prop} / T_{frame} = 2/0.01 = 200 $W < 2a+1$ s = w/ (1+2a) = 7/401 = 0.0175 (1.75%)

Distance Transmission rate	20Km	200Km	2000Km	20000Km
1Kbps	100%			
1Mbps			1.75%	
1Gpbs				

Q2

Curtin University

Consider a sliding window protocol (Go-Back-N ARQ) used for flow control on a given data link where the data rate is 8,000 bits/second, the propagation delay is 0.25 second, and the frame size is 1600 bits. Assume that acknowledgment packets are of negligible size, processing time at a node is negligible, and the link is error-free. What is the minimum window size which will allow full utilization (efficiency) of the link?

Frame Size = L = 1600 bits

$T_{prop} = 0.25s$

$T_{frame} = 1600 / 8000 = 0.2$ s

$a = 0.25s / T_{frame} = 1.25$

In order to have a full link utilization: $W \geq 2a + 1$

W_{min} = round_up(2 *1.25 + 1) = 4

Q3

Curtin University

Assume data in 8-bit words as shown below:

10011001 11100010 00100100 10000100

a. Calculate the checksum at the sender's end and the receiver's end

Refer to lecture notes for binary calculation

Sender's End	**Receiver's End**
b1 = 10011001 = 153	b1 = 10011001 = 153
b2 = 11100010 = 226	b2 = 11100010 = 226
b3 = 00100100 = 36	b3 = 00100100 = 36
b4 = 10000100 = 132	b4 = 10000100 = 132
x = (b1 + b2 + b3 + b4) mod 2^8-1	b5 = 11011010 = 218 *(checksum block)*
37 = 547 mod 255	
	x = (b1 + b2 + b3 + b4 + b5) mod 2^8-1
checksum c = -x mod 255	0 = 765 mod 255
c = -37 mod 255	
c = 218	checksum c = -0 mod 255
c = 11011010	c = -0 mod 255
	c = 0
	c = 0

Codeword = 10011001 11100010 00100100 10000100 11011010

Q3

Assume data in 8-bit words as shown below:

10011001 11100010 00100100 10000100

b. State an example of an error that checksum fails to detect?

Sender sent	10011001 11100010 00100100 10000100 11011010
Receiver received	11100010 10011001 00100100 10000100 11011010

Can’t be detected by checksum

Q4

Given the data word (1011011), or data polynomial D(x) = $x^6 + x^4 + x^3 + x^1 + 1$ and given the generator polynomial G (x) = $x + 1$

a. Find the codeword C(x)

b. Assume the received message H (x) is **H(x) = C(x) + E(x)**, where E(x) is the error polynomial

   i. When H(x) contains no errors show that H(x) is divisible by G(x)

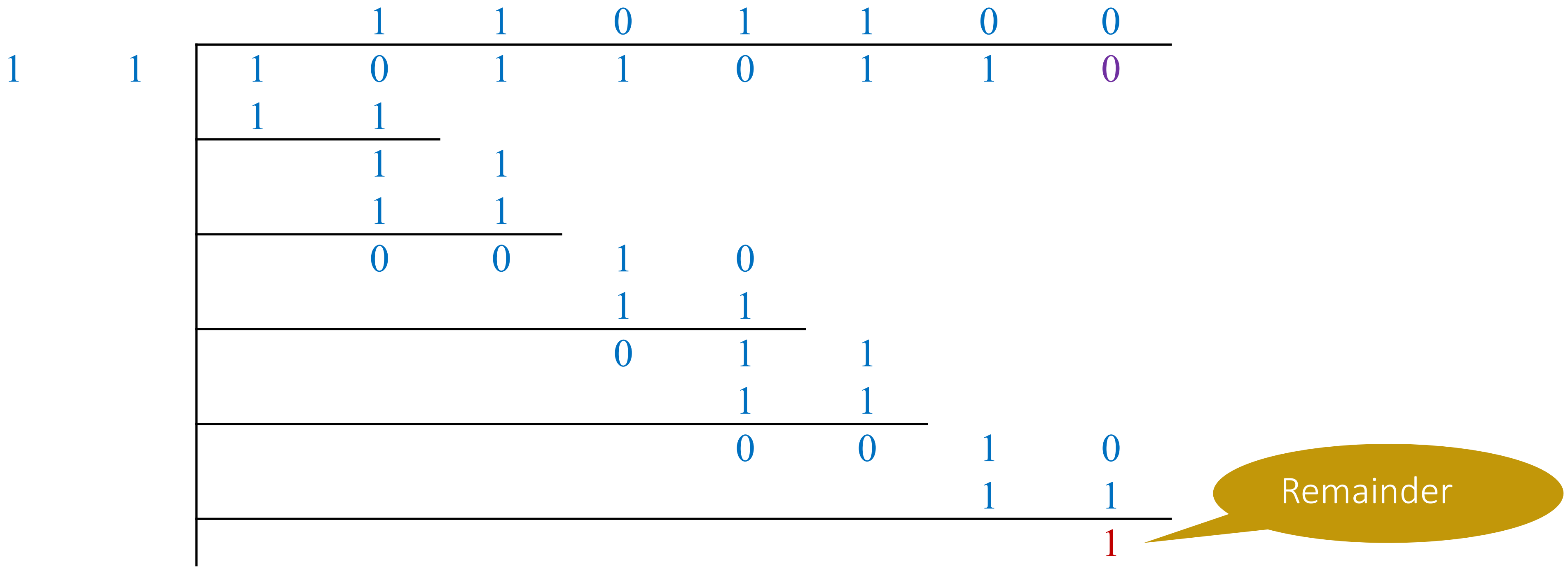
   ii. Determine whether the error is detectable when:

      - E(x) = 1
      - E(x) = $x + 1$
      - E(x) = $x^3 + x$

Q4

Given the data word (1011011), or data polynomial $D(x) = x^6 + x^4 + x^3 + x^1 + 1$ and given the generator polynomial $G(x) = x + 1$ (11)

a. Find the codeword C(x) (For detailed explanation please see lecture notes)



```
             1  1  0  1  1  0  0
         ------------------------
 1  1   | 1  0  1  1  0  1  1  0
          1  1
         ------
             1  1
             1  1
         ---------
             0  0  1  0
                   1  1
         ---------------
                   0  1  1
                      1  1
         ------------------
                      0  0  1  0
                            1  1
         ------------------------
                               1
```

Codeword = 10110111

Q4

Given the data word (1011011), or data polynomial $D(x) = x^6 + x^4 + x^3 + x^1 + 1$ and given the generator polynomial $G(x) = x + 1$

b. Assume the received message H (x) is **H(x) = C(x) + E(x)**, where E(x) is the error polynomial

   i. When H(x) contains no errors show that H(x) is divisible by G(x)

XOR (since E(x) here just indicates which bits are in error during transmission)

Divide H(x) by G(x) and show that the remainder = 0

Q4

Determine whether the error is detectable when:

- E(x) = 1

Received: 10110111 + 00000001 = 10110110

```
                 1  1  0  1  1  0  1
            ------------------------
1  1     |  1  0  1  1  0  1  1  0
            1  1
            -----
               1  1
               1  1
            --------
               0  0  1  0
                     1  1
            --------------
                     0  1  1
                        1  1
            -----------------
                        0  0  1  0
                              1  1
            ------------------------
                                 1
```

Error detected

Q4

Determine whether the error is detectable when:

- $E(x) = x^3 + x$

Received: 10110111 +
00001010

= 10111101

```
                1   1   0   1   0   1   0
            -----------------------------
1   1   |   1   0   1   1   1   1   0   1
            1   1
            -----
                1   1
                1   1
                -----
                0   0   1   1
                        1   1
                        -----
                        0   0   1   0
                                1   1
                                -----
                                0   1   1
                                    1   1
                                    -----
                                        0
```

Error undetected

Q5

Show byte-stuffing & destuffing steps for the following data bits if PPP frame is used?

01000001 01111101 01000010 01111110 01010000 01110000 01000110

Convert to Hex: 41 7D 42 7E 50 70 46
Look for the Flag (7E) and Control Escape (7D): 41 7D 42 7E 50 70 46

Stuffing

7D will be replaced by the byte 7D and (7D XOR 20) = 5D
7E will be replaced by the byte 7D and (7E XOR 20) = 5E

Hence the complete byte string to be sent: 7E 41 7D 5D 42 7D 5E 50 70 46 7E

Destuffing

Received bits after Hex Conversion: 7E 41 7D 5D 42 7D 5E 50 70 46 7E

Look for the bytes 7E and 7D: 7E is the flag; If 7D is encountered, look into the next byte
7E 41 7D 5D 42 7D 5E 50 70 46 7E

Replace (7D <next byte>) with (<next byte> XOR 20)
7E 41 7D 42 7E 50 70 46 7E

Q6 (Optional. For information only)

In some networks the data link layer requests all damaged frames to be retransmitted. Assume that the acknowledgement frame is never lost. If the probability of a frame being damaged on a particular link is *p*, what is the normalized throughput of the link if stop-and-wait ARG is used?

Hint:

$$\sum_{i=1}^{\infty}(i \times x^{i-1}) = \frac{1}{(1-x)^2} \qquad for(-1 < x < 1)$$

Q6 (Optional)

The time to transmit a frame successfully is

$$T = T_{frame} + 2\ T_{prop}$$

Suppose the frame or ACK *is lost*, two transmission attempts are required, therefore,

$$T = T_{frame} + \textbf{timeout} + T_{frame} + 2\ T_{prop}$$

Assume timeout = $2\ T_{prop}$

Therefore

$T = 2\ (T_{frame} + 2\ T_{prop})$ for two transmissions

Q6 (Optional)

Suppose for successful transmission each frame has to be transmitted *k* times on average, then

$$\boldsymbol{T = N_x (T_{frame} + 2\, T_{prop})}$$

The probability of a frame requires exactly *k* transmissions , *P(k)*, equals the probability of the first *k-1* attempts failing, (p^{k-1}), multiplies the probability of the *k*-th transmission succeeding, (*1-p*).

Therefore the mean number of transmission is

$$N_x = \sum_{k=1}^{\infty}(k \times T(k)) = \sum_{k=1}^{\infty}(k \times (1-p) \times p^{k-1}) = \frac{1}{(1-p)^2}(1-p) \;\; = \frac{1}{(1-p)}$$

Q6 (Optional)

Normalized throughput

$$S = \frac{T_{frame}}{N_x(T_{frame} + 2T_{prop})} = \frac{1}{N_x(1+2a)}$$

$$\boldsymbol{S} = \frac{1 - \boldsymbol{P}}{1 + 2\boldsymbol{a}}$$

Tutorial 4: Data Link Layer II

Question 1

Byte Stuffing

1. **Convert to hexadecimal**
   41 7D 42 7E 50 70 46
2. **Locate flag (7E) and escape (7D) bytes**
   41 7D 42 7E 50 70 46
3. **Replace 7D with the byte 7D and (7D XOR 20)**
   7D XOR 20 = 5D
4. **Replace 7E with the byte 7D and (7E XOR 20)**
   7E XOR 20 = 5E

Therefore, the complete string will be 7E 41 7D 5D 42 7D 5E 50 70 46 7E

Byte Destuffing

1. **Convert to hexadecimal**
   7E 41 7D 5D 42 7D 5E 50 70 46 7E
2. **Remove flag (7E) bytes**
   41 7D 5D 42 7D 5E 50 70 46
3. **Locate 7E and escape (7D) bytes; if 7D is found, look into the next byte**
   41 7D 5D 42 7D 5E 50 70 46
4. **Replace 7D <next byte> with <next byte> XOR 20**
   5D XOR 20 = 7D and 5E XOR 20 = 7E

Therefore, the complete string will be 41 7D 42 7E 50 70 46

Question 2

CSMA/CD with binary exponential backoff. In this protocol:

- Each station listens before transmitting
- If more than one device accesses the medium, there is a collision
- Both devices detect the collision, stop transmitting, try again after a random amount of time
- If successive transmission attempts fail, the backoff time is progressively increased. If the number of attempts exceeds the attempt limit, an error is reported

After a collision has occurred, each node waits either 0 or 1 time slots before retransmitting. If a further collision occurs, each node waits 0, 1, 2 or 3 time slots. In general, after n collisions, a random number between 0 and $2n$ - 1 time slots is chosen, and the node waits that number of time slots before attempting to retransmit, for $n \le 10$. This is called binary exponential back-off.

Binary exponential back-off delay is used to keep the probability of nodes continuing to collide low.

Question 3

- Broadcast domains = 7
- Collision domains = 14

Question 4
In wireless communication, a signal can be interrupted by a variety of factors, thus the detection of such occurrences is effectively impossible. Therefore, collision avoidance is the most preferred protocol in wireless communication. CSMA/MA is one such protocol used for sharing data in a wireless medium.

Question 5
It is not safe due to the Evil Twin threat. An evil twin is a fraudulent Wi-Fi access point that appears to be legitimate but is set up to eavesdrop on wireless communications. This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves setting up a fraudulent website to which they are then lured.

Tutorial 5: Network Layer I

Question 1

Address / Mask	**Mask (Binary)**	**Next hop**
129.47.104.0/21	**01101**000	Interface 0
129.47.112.0/21	**01110**000	Interface 1
190.34.116.0/22	**011101**00	Interface 2
129.47.192.0/19	**110**00000	Router 1
Default Router	N/A	Router 2

Part A

The subnet 01010101 does not belong to any of the listed networks Therefore, the packet is forwarded to Router 2.

Part B

The subnet **01101**110 belongs to the network with the ID 129.47.104.0/21. Therefore, the packet is forwarded to Interface 0.

Part C

The subnet **110**11101 belongs to the network with the ID 129.47.192.0/19. Therefore, the packet is forwarded to Router 1.

Part D

The subnet **011101**11 belongs to the network with the ID 190.34.116.0/22. Therefore, the packet is forwarded to Interface 2.

Part E

The subnet 01101010 does not belong to any of the listed networks. Therefore, the packet is forwarded to Router 2.

Question 2

	Source MAC Address	Destination MAC Address	Source IP Address	Destination IP Address
Link 1	AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC	10.1.1.1	10.1.3.3
Link 2	AA:AA:AA:AA:AA:AA	CC:CC:CC:CC:CC:CC	10.1.1.1	10.1.3.3
Link 3	DD:DD:DD:DD:DD:DD	EE:EE:EE:EE:EE:EE	10.1.1.1	10.1.3.3
Link 4	11:11:11:11:11:11	33:33:33:33:33:33	10.1.1.1	10.1.3.3
Link 5	11:11:11:11:11:11	33:33:33:33:33:33	10.1.1.1	10.1.3.3

Question 3

Part A
0.0.0.0 is the address of “this host”. In other words, the primary IP address of the machine executing the instruction. In DHCP, when a unique address has not yet been determined, 0.0.0.0 is used as the Source IP (i.e. the DHCP Discover Packet). In the context of a Router, 0.0.0.0 represents the Default route. Moreover, 0.0.0.0 cannot be assigned to an interface or used as a destination address.

Part B
0.0.0.18 is the address of the host with the host address 18 on “this local network”.

Part C
255.255.255.255 is the broadcast address of “this local network”.

Part D
161.115.255.255 is the broadcast address of the network 161.115.0.0/16

Question 4
In address 123.132.23.0/24, 8 bits are allocated for the host address. Subnetting to create 16 subnets will require $\log_2 16 = 4$ bits. The remaining bits will provide $2^4 = 16$ host addresses. Recall that the addresses 0000 and 1111 are reserved to specify “this host” and for broadcasting, respectively. Therefore, there are 14 addresses available for hosts.

Question 5
Part A
::192:168:0:1 is valid. It is the short form of 0.0.0.0.192.168.0.1.

Part B
2002:c0a8:101:42 is valid. It is the short form of 2002:c0a8:0101:0:0:0:0042.

Part C
2003:dead:beef:4dad:23:46:bb:101 is valid.

Part D
:: is valid. It is “Unspecified”.

Part E
2002 is invalid. There are two “colon pairs”.

Tutorial 6: Network Layer II

Question 1

Processed	L(1)	P(1)	L(3)	P(3)	L(4)	P(4)	L(5)	P(5)	L(6)	P(6)
{2}	3	2-1	3	2-3	2	2-4	inf	–	inf	–
{2, 4}	3	2-1	3	2-3	2	2-4	3	2-4-5	inf	–
{2, 4, 1}	3	2-1	3	2-3	2	2-4	3	2-4-5	inf	–
{2, 4, 1, 3}	3	2-1	3	2-3	2	2-4	3	2-4-5	8	2-3-6
{2, 4, 1, 3, 5}	3	2-1	3	2-3	2	2-4	3	2-4-5	5	2-4-5-6
{2, 4, 1, 3, 5, 6}	3	2-1	3	2-3	2	2-4	3	2-4-5	5	2-4-5-6

Question 2

Hops	L(1)	P(1)	L(3)	P(3)	L(4)	P(4)	L(5)	P(5)	L(6)	P(6)
0	inf	–	inf	–	inf	–	inf	–	inf	–
1	3	2-1	3	2-3	2	2-4	inf	–	inf	–
2	3	2-1	3	2-3	2	2-4	3	2-4-5	8	2-3-6
3	3	2-1	3	2-3	2	2-4	3	2-4-5	5	2-4-5-6
4	3	2-1	3	2-3	2	2-4	3	2-4-5	5	2-4-5-6

Question 3

This may cause the “Count to Infinity” problem in a distance vector routing protocol as B will think that C can contact A, add 1 its advertised route and send an update. C will think that it can get to A via B, update its routing table using information received from B and send an update etc. until distance = 16.

Question 4

The purpose of a Hold-down timer in RIP is to suppress any routing updates for a specified period of time after a poison route is received to allow the offline router some time to converge.

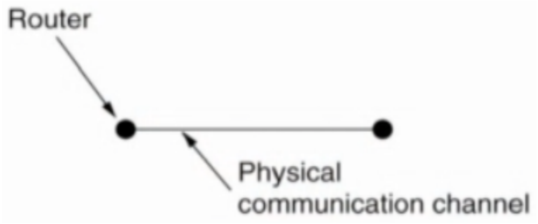
Question 5

In RIP, network size is limited by the max hop count. Exceeding the count will be considered as costing infinity and will be unreachable. In contrast, OSPF follows a modular approach to split the network into areas where a group of routers in an area will have the same LSDB. The backbone area (which is a special type of area) will connect all other areas to perform routing between areas. This is also known as hierarchical design of OSPF. Therefore, OSPF is more suitable for a large network.

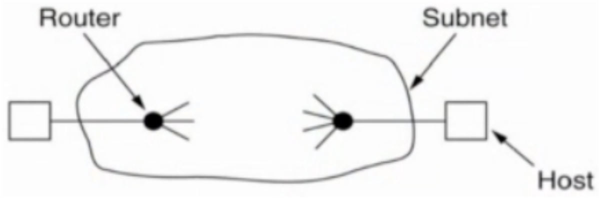
Tutorial 7: Transport Layer I

Question 1

Node-to-node Communication



End-to-end Communication



The Transport layer facilitates end-to-end communication for individual applications by providing communication services for a process in a host to a process in another host.

Question 2

Basis	**Data Link Layer**	**Transport Layer**
Addressing	MAC	Port number
Connection-establishment	No	Yes, using a 3-way handshake
Connection-release	No	Yes, using a 3- or 4-way handshake
Flow control and buffering; error-control; and sequencing	Yes, using Stop-and-Wait etc.	Yes, using Sliding Window etc.
Multiplexing	No	Yes, both upward and downward
Crash recovery	No	Yes

Question 3

Some reasons why are:

1. Process IDs are OS-specific and using process IDs would have made these protocols OS-dependent
2. A single process may establish multiple channels of communication. A single process ID (per process) as the destination identifier cannot be used to distinguish between these channels

3. Having processes listen-in on well-known ports is relatively straight-forward, but listening-in on well-known process IDs is impossible.

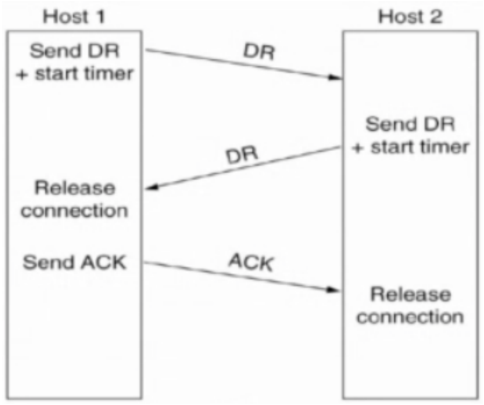
Question 4

It has to be large enough to prevent a situation wherein a packet is received by the destination but its ACK is not received by the source. If this occurs, the sender may introduce duplicate packets into the network.

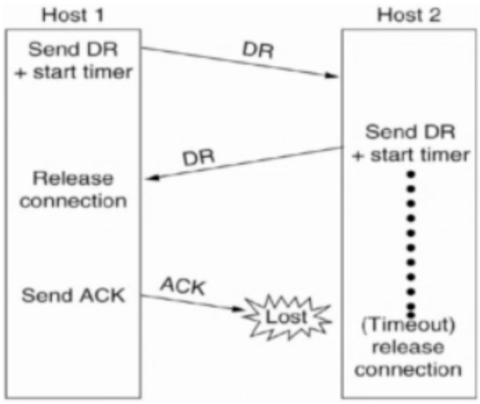
Question 5

Three-way Handshake

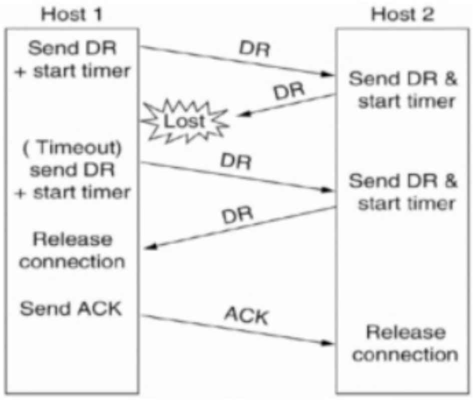
Normal Three-way Handshake



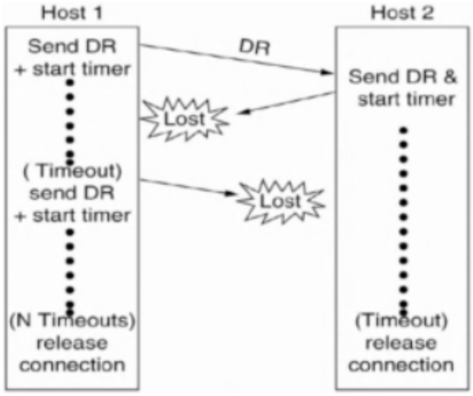
Final ACK is Lost



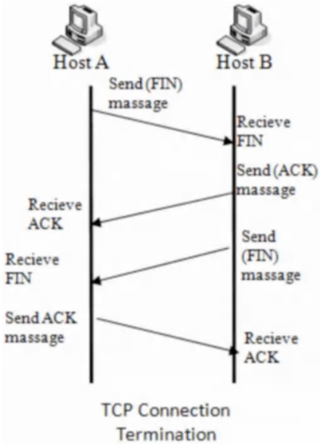
Response is Lost



Response is Lost and Subsequent DRs are Lost


Host 1
Host 2
Send DR + start timer
DR
Send DR & start timer
Lost
(Timeout) send DR + start timer
Lost
(N Timeouts) release connection
(Timeout) release connection

<u>Four-way Handshake</u>



Question 6

In regards to a datagram service (packet switching) network, transport entities expect TPDUs to be lost regularly, and thus, are well-prepared to cope should any TPDUs be lost. In regards to a connection-oriented (virtual-circuit packet switching) network, the loss of the virtual circuit is handled by establishing a new one and probing the remote transport entity for any and all received and lost TPDUs.

Question 7

Strategy used by Client/Sender	**Strategy used by Server/Receiver**					
	First ACK, then Write			**First write, then ACK**		
	AC(W)	**AWC**	**C(AW)**	**C(WA)**	**WAC**	**WC(A)**
Always retransmit the last TPDU	OK	DUP	OK	OK	DUP	DUP
Never transmit the last TPDU	Loss	OK	Loss	Loss	OK	OK
Retransmit only in state S0 (No TPDU outstanding)	OK	DUP	Loss	Loss	DUP	OK
Retransmit only in state S1 (TPDU outstanding)	Loss	OK	OK	OK	OK	DUP

Tutorial 8: Transport Layer II

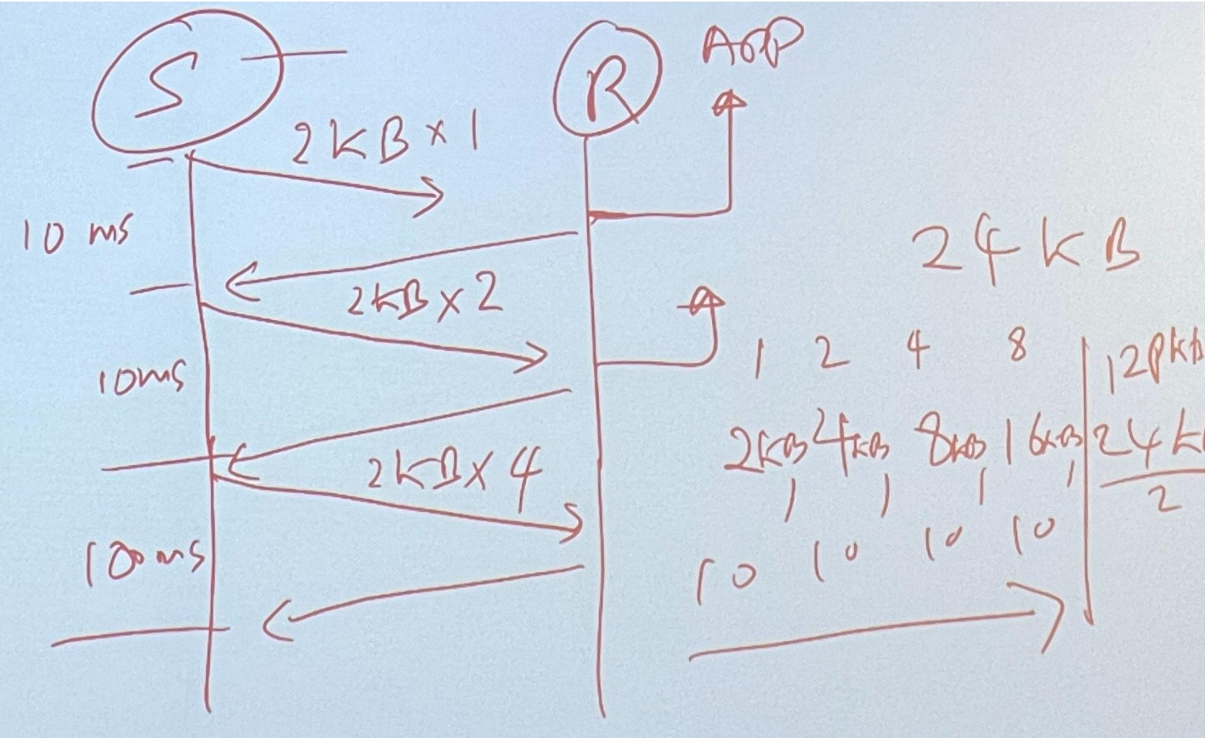
Question 1
No, despite the fact that in both cases, the sender is slowed down, their objectives are not the same. The objective of flow control is to prevent overflow of the receiver's buffer. This is done by slowing down the sender. On the other hand, the objective of congestion control is to protect the network from being overloaded. This is also done by slowing down the sender whenever a datagram is lost or delayed excessively in the network.

Question 2
The advantage is that the typical choke packet method will affect the sender, whereas the hop-by-hop choke packet method will affect each hop it passes through. The hop-by-hop choke packet method requires each hop to reduce its transmission even before the choke packet arrives at the sender. Therefore, it is quicker in handling congestion.

Question 3
Firstly, the warning bit method explicitly sends a congestion notification to the sender by setting a specific bit, whereas the RED method implicitly notifies the sender by simply dropping one of its packets. Secondly, the warning bit method drops a packet only when there is no buffer space left, whereas the RED method drops packets before the entire buffer is exhausted.

Question 4
It was difficult to detect congestion back then because networks were not as reliable as they are today. Back then, packet loss could occur due to a transmission error or packet discard due to congestion. Therefore, it was significantly more difficult to isolate the root cause.

Question 5



Question 6
TCP is called a byte-stream protocol because it sends data as a stream of bytes, as opposed to messages in UDP. UDP differs from TCP in this regard as TCP does not preserve message boundaries like UDP. If UDP is used in the Transport layer, the Application layer is responsible for segmenting data into messages. The preferred protocol for multicasting or broadcasting a message is UDP as TCP does not support either multicast or broadcast.

Question 7
The main difference between UDP and TCP is that UDP is connectionless while TCP is connection-oriented. Furthermore, UDP offers an unreliable delivery of packets whereas TCP offers an ordered delivery of packets. If a DNS packet is lost, there will be no automatic recovery. This will not cause a problem as DNS is idempotent, meaning operations can be repeated without harm. When a process makes a DNS request, it starts a timer and if the timer expires, the process simply makes the request again.

Tutorial 9: Application Layer I

Question 1
They are Client-Server and Peer-to-Peer.

Question 2
They are:

- Data Integrity
  - Some apps (e.g. those involving file transfer and/or web transaction) require reliable data transfer
  - Whereas, other apps (e.g. those involving audio input/output) can tolerate some loss
- Timing
  - Some apps (e.g. those involving internet telephony or interactive games) require low delay to be "effective"
- Throughput
  - Some apps (e.g. multimedia apps) require a minimum amount of throughput to be "effective"
  - Whereas, other apps (e.g. "elastic apps") make use of whatever throughput they can get
- Security
  - Encryption, data integrity etc.

Question 3
Its purpose is to provide encryption for unencrypted TCP traffic, data integrity and end-point authentication.

Question 4
Since HTTP is "stateless" (i.e. the server retains no information about past client requests), it does so by using cookies.

Question 5
Unlike the traditional GET method, the Conditional GET method will not send the requested object if the version stored in the client's cache is up-to-date. Moreover, Conditional GET also has:

- No object transmission delay
- Lower link-utilisation
- The header line `if-modified-since:<date>`

Question 6
One such solution is by using web caches implemented using a proxy server. Under this scheme, the browser (client) sends a HTTP request for a particular object to the proxy server (server). Upon receiving the request, the proxy server then checks if the requested object is in the cache. If so, the proxy server sends, to the browser, a HTTP response with the cached object. Otherwise, the server sends a HTTP request for the object to the origin server (server). Upon receiving the request, the origin server obtains the object and then sends, to

the proxy server, a HTTP response with the object. Thereafter, the proxy server forwards the object to the browser.

Question 7
Web sockets:

- Bi-directional (unlike HTTP uni-directional request-response)
- Persistently connected
- A message-oriented protocol
- For real-time apps
- Non-reliant on UI/browser refreshes
- Run on HTTP and carry different types of messages (application layer)

Web sockets are different in the sense that TCP sockets are connections in the Transport Layer, where a socket is indicated by an IP address and a port. With TCP sockets, byte streams (note that message boundaries are not preserved) as opposed to HTTP messages–which are used in HTTP and WebSocket–are used to read and send data. TCP primitives such as `bind()`, `listen()`, `connect()`, `send()`, `receive()` and `close()` are the library procedures of the TCP entity, helping a TCP socket to function properly.

Question 8
The internet is a network of networks, whereas WWW is a distributed system that runs on top of the internet; it is not a network.

Question 9
POP3 is a stateless protocol. With POP3, if one were to view their emails from the server on one device, those same emails will appear unread if they were viewed on a different device. On the other hand, IMAP is a stateful protocol. With IMAP, if one were to view their emails from the server on one device, those same emails will appear in the same state (i.e. read/unread) if they were viewed on a different device.

Tutorial 10: Application Layer II

Question 1
A DHCP server allocates an IP address to a device for a certain time period (denoted by the Lease Length field in a DHCPOffer message). Therefore, it is required to renew the lease once it has expired to obtain a new IP address or preserve the same address.

Question 2
Yes, recall that an IP address consists of a network number and a host number. If a machine has two Ethernet cards, it can be on two separate networks, and if so, it needs two IP addresses.

Question 3
Its purpose is to maintain the mapping between hostnames and IP addresses. Since DNS servers are arranged hierarchically to support the entire DNS namespace, one advantage of a DNS server over a host file is that it is much faster in DNS name resolutions than a host file which contains millions of records. Furthermore, DNS servers provide fault tolerance in case of a failure (e.g. having primary and secondary DNS servers).

Question 4

1. DNS name resolutions for Alice's mail server, a Mail Transfer Agent (MTA), which is responsible for resolving the outgoing mail server (mail.cs.curtin.edu.au) is configured on their computer.
2. The email is sent/pushed to the email queue of Alice's mail server via SMTP
3. Alice's mail server performs the DNS name resolutions for Bob's mail server (cs.ai.yale.edu)
4. The email is sent/pushed to the mailbox of Bob's mail server via SMTP
5. Bob's PC resolves the incoming mail server (mail.cs.curtin.edu.au) when they check for their email via POP3/IMAP
6. Bob can then download or access the emails in the mailbox of their mail server.

3. DNS name resolutions for cs.ai.yale.edu
    a. A request is sent to the Curtin DNS server
        i. If the domain name being queried is managed by the server, the matched RR (authoritative record) is returned
        ii. If a matched RR exists on the cache, the cached RR (non-authoritative record) is returned
        iii. Else, the recursive query method is used to send a query to the DNS server for the top-level domain, edu
    b. The .edu name server (NS) receives the query and follows steps i, ii, and iii
    c. The .yale NS receives the query and follows steps i, ii, and iii
    d. The .cs NS receives the query and follows steps i, ii and iii
        - It is responsible for holding the RR record
        - Once the record is located on the DNS database at this NS, it will be returned
    e. The returned RR will be forwarded to the .yale NS, the .edu NS, and lastly, the .curtin NS.
        - These servers may choose to cache it for future use

1. DNS name resolutions for cs.curtin.edu.au
    a. A request is sent to the Curtin DNS server
        i. If the domain name being queried is managed by the server, the matched RR (authoritative record) is returned
        ii. If a matched RR exists on the cache, the cached RR (non-authoritative record) is returned
        iii. Else, the recursive query method is used to send a query to the DNS server for the top-level domain, au
    b. The .au NS receives the query and follows steps i, ii, and iii
    c. The .edu NS receives the query and follows steps i, ii, and iii
    d. The .cs NS receives the query and follows steps i, ii, and iii
        - It is responsible for holding the RR record
        - Once the record is located on the DNS database at this NS, it will be returned
    e. The returned RR will be forwarded to the .curtin NS, the .edu NS, the .au NS, and lastly, the .curtin NS.
        - These servers may choose to cache it for future use

Question 5

Napster depends on a centralised server which holds information about the clients and the data parts which they hold, while Gnutella does not rely on a centralised server at all. Gnutella discovers the peers dynamically by means of the ping-pong method.

Question 6

1. A user registers with the tracker to get the list of peers, becoming a peer themselves
2. Assuming the newly joined peer has no data to be shared, they wait until they are randomly selected by other peers for receiving data (optimistic unchoking).
3. Eventually, the newly joined peer becomes one of the other peers' (e.g. Peer B) top four providers
4. Peer B becomes one of the newly joined peer's top four providers in return, mutually benefiting, tit-for-tat.

Question 7

When a node downloads a page of a website, it acts as a web server (i.e. it hosts the page) to the connecting nodes.

Tutorial 11: Emerging Networking Technologies

Question 1
They are physical objects that are embedded with sensors, software and other technologies with the purpose of exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to highly complex industrial systems. Examples of IoT “things” include household appliances, wearable monitoring equipment and smart manufacturing devices.

Question 2
It is an approach to network management that enables dynamic programmatically efficient network configuration. SDN attempts to centralise network intelligence in one network component by disassociating the forwarding process of network packets (which is done by the data plane) from the routing process (which is done by the control plane). The control plane consists of one or more controllers, which are considered the brain of the SDN network where the whole intelligence is incorporated.

	SDN	**Traditional Networks**
Control	Centralised	Distributed
Coupling	Data plane and control plane are decoupled by software	Data plane and control plane are mounted on the same plane
Configuration	Automatic; less time-consuming	Manual; more time-consuming
Structural Complexity	Low	High
Troubleshooting Difficulty	Low; recall, control is centralised	High; recall, control is distributed
Maintenance Cost	Low	High

Question 3
The creation of blocks is not an easy process and cannot be done instantly. Blockchain follows a mechanism to slow down the creation of new blocks; it is called Proof of Work (PoW). Tampering with a block requires recalculating the hash values of all the blocks ahead of the tampered block which requires a considerable amount of time. Furthermore, the distributed nature of blockchain allows any entity (referred to as a node) to keep a copy of the ledger (the blockchain) and renders it impossible for one to alter the content of a block (due to Distributed Consensus).

Question 4
It is important to have a digital signature as it helps verify the transaction by the money sender. Furthermore, it is important to have a unique ID as it prevents the duplication of the ledger entries (in addition to the digital signatures).

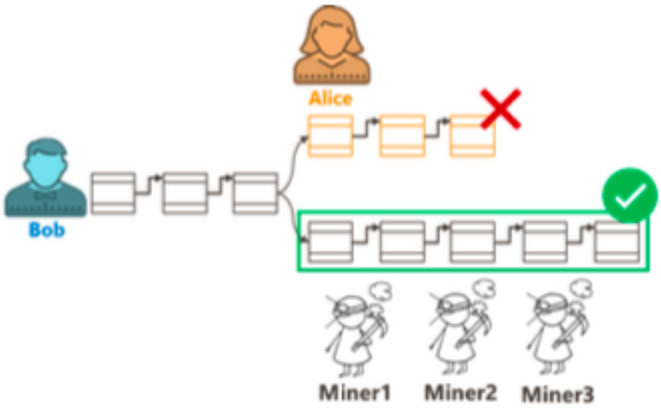
Question 5

They are:

- Broadcasting of transactions
- Acceptance of only signed transactions
- Elimination of overspending
- Distributed consensuses
- The usage of mechanisms to prove work (namely, PoW and PoS)

Question 6

Let's say an intruder, named Alice, managed to win the lottery in PoW a few times against other miners and then sent a fraud block to another node, Bob. However, to be the longest chain (i.e. chain of blocks that took the most effort to build), Alice needs to have more than 50% of the computing resources shared amongst all miners (which is impossible) so that she can always win the lottery in PoW with high probability. Note that Bob will eventually reject Alice's chain in favour of the longer chain if the intruder fails to be the longest chain.



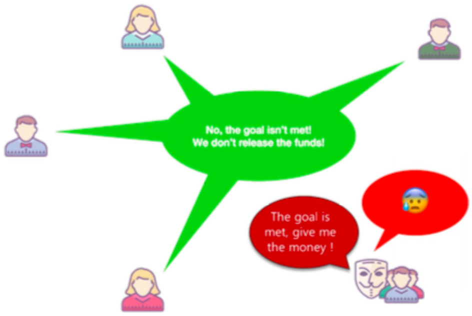
Question 7

PoS holds a stake (a security deposit) from a validator to ensure the integrity of the minting/forging (much like mining in PoW). This can help mitigate the biggest problem associated with PoW, the high energy usage in mining.

Question 8

They are computer programs stored on the blockchain. Key features are:

- Immutability – once a smart contract is created, it cannot be modified
- Output validation – the output of the contract is validated by everyone in the network
- Safe release – a single person cannot force the contract to release the funds


No, the goal isn't met!
We don't release the funds!
The goal is met, give me the money !
😰