2019 Network and Communication Examination Solution

1. a. i) Ethernet Frame

   ii) Transport Layer Security (TLS) or Secure Sockets Layer (SSL)

   iii) Reliable

   iv) False. Because hash function is one-way and thus cannot be decrypted the other way.

   b. i) Store-and-forward (a.k.a transmission delay) is $\frac{11000}{\frac{800}{8} \cdot 10^6} = 1.1 \times 10^{-4}$ seconds $= 0.11$ ms.

   ii) the total transfer time is thus $9 + 0.11 = 9.11$ miliseconds.

   c. After hitting Enter, the browser will 1️⃣ look up the IP address of the server of `AmazingMovies.org` using DNS, which is either cached or fetched from a DNS server. Next, 2️⃣ a TCP connection will be established betweem my laptop with the address assigned by DHCP server and the remote server of `AmazingMovies.org`. The browser will then 3️⃣ send a `GET` HTTP request to the remote server to fetch the HTML skeleton of webpage of `AmazingMovies.org`. The remote server will 4️⃣ respond with a header indicating that the content is available in a local CDN server. The DNS is used again to look up the IP of the CDN server, and the content will be fetched from the CDN server. Any other resources such as 5️⃣ files or images will then be fetched separately using HTTP `GET` request and their corresponding URL.

   d. The firewall on their machines might be blocking the IP address of the game server or port number. Using a different available port or change the firewall policy to exclude blocking of my game server. We could also fix this using port forwarding.

   e. i) Long password allows more combinations of characters, which takes longer time to crack by brute force.

   ii) Rainbow table might include the common dictionary words (commonly in all-lowercase), which takes less or almost no efforts to decrypt the password.

2. a. i) The attacker can use 1️⃣ bait-and-switch technique to send an email with similar looking to a legitimate email(e.g. promotional sale email or notification from user's workplace) and then insert links to a terrorist propaganda. The attacker can 2️⃣ hack into user's computer using a virus/trojan and forcifully display terrorist propaganda on the screen. The attacker can also 3️⃣ use a fake local DNS server that inserts the wrong IP address for some popular sites so that when user visits the sites they will be direct to the terrorist page.

   ii) They can easily use a proxy server/VPN to disguise themselves from being discovered.

   b. The framentation will result in $\frac{2^{16}-20}{1500-20} = \frac{65535-20}{1500-20} = 44.27 \approx 45$ fragments.

   c. i) For a total number of 2048 hosts, we need a total number of 2050 addresses because we need to include the nerwork address and broadcast address for this interface. It needs $\log 2050 \approx 12$ digits. Hence the subnet mask needs to preserve the first $32 - 12 = 20$ digits and it would be $255.255.240.0$ and $192.168.0.0/20$ in CIDR notation.

ii) There are 2 alternative (or many other) solutions that both achieve £216,000. The first solution is to purchase 33 64-port swithces and only 1 48-port switch so that 48-port switch will be at the center of the star and 64-port switch will be the peripheral ones. This will connect up to $33 * 63 + (48 - 15) = 2094$ hosts and will cost $33 * 6400 + 4800 = 216000$ pounds.

The other way to do this is to buy 45 48-port switches so that there is one 48-port switch at the center of the star and the rest would be the peripheral ones. This will connect up to $44 * 47 + 4 = 2072$ hosts and will cost $45 * 4800 = 216000$ pounds

d. Assume we need to transmit x bits of data.

The utilization of Box1 is then $\#\text{utilization} = \frac{x/(8\times10^9)}{10+x/(8\times10^9)} = \frac{x}{8\times10^{10}+x}$

The utilization of Box2 is then $\#\text{utilization} = \frac{x/(1\times10^9)}{40+x/(1\times10^9)} = \frac{x}{4\times10^{10}+x}$

Apparently, $\#\text{Box1Util} < \#\text{Box2Util}$, hence I will pick Box2

e. i) They are directly involved in the **physical layer**(optical fibre), **data link layer**(Wireless Access Point), and **network layer** (router) of the OSI model in this question statement, but obviously those company also involve in transport layer (QUIC invented by Google) and application layer (their websites and products). But those might not need to appear in the answer prompt.

ii) Monoply over range of things: pricing of internet facilities, other companies have no say in terms of developing new and more efficient protocols, might impede technical advancement. A single company controling every aspect of network can also monitor and manipulate packets and user data. (Dystopia, etc.)