Tt Question 1:

a)

i) Ethernet frame

ii) TLS

iii) Reliable

iv) False. Since encryption implies a corresponding decryption method, which should not exist for a proper hash function

b)

i)

11000 \* 8 / (800 \* 10^6) = 0.11 ms

ii)

1.1 \* 10 ^ -4 + 9 \* 10 ^ -3 = 9.11 ms

c)

ip is assigned when the host first join the network

get the ip address from DNS server using UDP

set up TCP connection to the CDN

send HTTP GET request to CDN

CDN checks cache, forwards request to backend if its a cache miss

CDN sends HTTP requests

d

Firewall blocks the ip address or port number

Use the command iptables to modify the ACL list

(could also be NAT, fix with port forwarding)

e)

i)

The longer the password the less likely it is to unhashed using brute force. And it is also computationally more expensive to crack.

ii)

Rainbow table very often contains the common words and phrases.

Question 2

i)

spam email

Man in the middle attack – DNS poisoning

Hijack social media accounts

click baits

Obfuscated links (i.e. goo.gl)

ii)

Tor, Proxy, VPN, Tails OS, IP spoofing?

b)

2 ^ 16 B

2 ^ 16 / (1500 - 8) = 44

Alternative solution:

Max UDP datagram size: 65535 B

Excluding 20B IP header: 65515 B

Available space for data in the IPv4 packet: 1500 - 20 = 1480 B (multiple of 8 B)

Number of fragments: 65515 B / 1480 B = 44.3 → 45 packets (?)

\*exclude the 8 B UDP header as well? I got 44.502 ~= 45 fragments as well

Alternative explained:

Max UDP packet size is 65535B, data inside the packet is 65535 - 20 = 65515B.

Each IP fragment has header 20B. Fragment data aligned at multiple of 8 bytes.

8k + 20 <= 1500 (MTU)

k <= 185, so max integer k is 185

So max data per fragmented frame is 8k = 1480B.

65515 / 1480 = 44.27, so it is fragmented into 45 frames.

c)

i)

/20 or 255.255.240.0 (need to reserve one address as a network address and one as a broadcast address, so /21 cannot be used)

(pls explain why not /21 for 2048 users ? expansion ? - because 2048 hosts means that YOU NEED +1 for broadcast address and +1 for network address so 2050 addresses required in total,

**the max # of hosts = 2 ^ (32 - # of bits used for subnetting) - 2** (one for network one for broadcast address) )

ii)

As the switches are connected acyclically, we can view the structure as a tree. Each *p*-port switch adds *p* ports to the network and uses up 2 port (1 on itself and 1 on the parent).

Apart from the "root" switch which is not connected to a parent, therefore does not use the 2 ports.

(48-2)*x* + (64-2)*y* + 2 >= 2048

46*x* + 62*y* >= 2046

From the above inequality, we can see that the cost per port of a 48 port switch is

4800/46 = 104.347826087

And the cost per port of a 64 port switch is

6400/62 = 103.225806452

Meaning that 64 port switches are more cost effective, therefore we should use as much of it as possible. We could maximise yand minimise xby setting xto 0:

0 + 62y >= 2046n

y >= 33n

This proves that the most cost effective way is to buy 33 64-port routers and no 48-port routers.

d)

Assume L bits of data is to be transfer. After using the standard formula we know that box 2 is better.

Let L = 1,000

Box 1 -

Transmission Time = Packet Size / Transmission Speed = 1,000/8\*10^9

Line Utilisation = Transmission Time / (10 + Transmission Time ) = 1.24 \* 10^-8 %

Box 2 -

Transmission Time = Packet Size / Transmission Speed = 1,000/10^9

Line Utilisation = Transmission Time / (40 + Transmission Time ) = 2.49 \* 10^-8 %

e)

i)

Application layer: Google.com and Amazon.com

Transport Layer: QUIC

Network Layer: router mentioned in question

Data Link: wireless AC

Physical: Optic Fiber

ii) A danger with a company owning all layers of the OSI model is they might reach monopoly, which gives them unethical abilities: can trace any usage, directly impact prices, accessible websites…

Violate net neutrality