**Questions 3 - Solutions**

1)

Routers contain powerful CPUs. These CPUs create routing table entries by using various algorithms related to the routing and best-path and add these entries to the routing table.

2)

Fundamentally, this function defines that a router will never forward a packet back out the same port which received the packet.

3)

A router uses various algorithms to create routing tables. Some algorithms create routing table entries by using the traffic density information of the lines to which a router is connected. And they try to send the packet over the line that has traffic density as little as possible. This situation is called 'Congestion Control'.

4)

Bookish definition of the Internet => "The internet is the network of networks."

For me, it is very logical.  Because the main task of the internet is to connect millions of networks around the world.

5)

a) As soon as you click on the video you want to watch on Udemy.com, your computer generates a request message and sends this message to the server of Udemy.com in the most convenient location for you.

b) Udemy's server looks at the content of the request message and realizes that you want to watch a video. As a result, the server starts sending you the video you want piece by piece. (Streaming)

c) The great thing about 'Streaming' is that you can start to watch the video without having to download the entire video.

6)

A normal computer does not need to communicate with many computers at the same time. Let's say you connected to 10 different websites from your computer at the same time. This means your computer communicates with 10 different computers simultaneously. 10 computers is a very small number.

However, for example, an Udemy server may have to communicate with tens of thousands of user computers at the same time. Therefore, servers need powerful hardware to deal with so many connections.

7)

The internet is a public network. It would be wrong to call the internet absolute insecure. However, when critical operations such as file transferring are to be made, the internet is an environment that should not be trusted. If you send a company-related file directly over the internet, nobody may see or capture this file. But the opposite may also happen. I think it doesn't hurt to be skeptical.

And this is where Wide Area Network comes into play. By using a WAN, you can send your file securely to the destination.

8)

Either nobody owns the Internet, or everybody owns the Internet or something in between. In actual terms, no one owns the Internet, and no single person or organization controls the Internet in its entirety. In theory, the internet is owned by everyone that uses it. Yet, in reality, certain entities exert more influence over the "mechanics" and regulation of the internet than others. There are some organizations that oversee and standardize what happens on the Internet. This control and standardization are required.

9)

Even though the Public WAN is very secure, it still uses the internet infrastructure. For this reason, there is always the possibility of encountering situations that cannot be predicted. But these possibilities are very low.

On the other hand, The LAN network belongs entirely to us. For this reason, it is very secure. Technically, it is very difficult to interfere with a LAN network from the outside. However, if anyone can infect one of our computers in the LAN with a virus, things will change.

10)

As you know, Private WAN represents a private network entirely owned by our company. In other words, instead of using the public infrastructure of the internet, we buy a different line that only belongs to us from the ISP. Therefore, private WAN is definitely more secure than public WAN.

However, a private WAN is still not as secure as a LAN. Because the ISP company from which we purchased the dedicated line can see the files we send. So if you are going to send a file over the private WAN, it makes sense to encrypt this file.

On the other hand, LAN is a network that belongs to us completely. For this reason, no one except us can see what is happening in this network.

11)

Tunneling is a communication method that allows for the movement of the packet from one network to another securely. Tunneling is a special encapsulation method. You can imagine that we are putting a packet into another packet. So, this process lets us send a packet over a public network as if it is going through a private network.

12)

Site-to-site VPNs are frequently used by companies with multiple offices in different geographic locations that need to access and use the corporate network on an ongoing basis. With a site-to-site VPN, a company can securely connect its corporate network with its remote offices to communicate and share resources with them as a single network.