Questions 5

Here there are questions about the information you have learned so far. By answering these questions, you can check which topics you understand well and which topics you do not understand well. You may also need to do some research on some questions. But all questions will be related to the information you learned.

Good luck.

1) What happens in the background when you connect to a website? (Let's say you're connected to amazon.com)

2) Why do packets going over the internet follow a different path each time?

3) Let's say you entered amazon.com and after 5 seconds you wanted to refresh the same page for any reason. When you send the request message to the server again, how will the server react to you? (You need to do some research!!!)

4) What type of solutions do giant companies like Google and Amazon have to better serve their customers?

5) What is the 'Internet Backbone'?

6) Why are there so many global ISPs in the world instead of a single Global ISP?

7) What is the 'Internet Exchange Point (IXP)'?

8) Why don't giant companies like to use existing ISP infrastructure? => ISPs vs Giant Companies like Google, Amazon (Do some research)

Questions 5 - Solutions

1)

1) You typed amazon.com in the web browser and clicked enter.

2) Your computer generated a request message and sent this request message to the server of amazon.com that best suits your location.

3) The message went through different POPs and different ISPs and reached one of the Amazon servers.

4) Amazon web server understood that you request the files of the website. For this reason, it created a response message and put all the information about the web page into this response message. (Images, Videos, Links, HTML File and etc.)

5) Web Server sent the response message to you. The response message went through different POPs and different ISPs and reached your computer.

6) Web browser obtained the necessary information from the response message and rendered the page on your screen.

2)

Packets move through a different path each time because routing tables are constantly changing. Many (excessive) events happen every second on the Internet that human perception cannot perceive. For this reason, the processors in the router are constantly making new calculations and changing the routing tables. For this reason, even 2 different packets sent to the same destination consecutively can go on completely different routes.

3)

First of all, you should know the meaning of the refreshing process. If you were on a web page, refreshing the page would bring up the most recent content published on that page. Essentially, you're asking the webpage to send your computer the newest version of the page you're viewing.

Back to my question, if you send a new request message to the server, the server will never question your request and send you the response message you want again. Because the servers do not keep any state information about whether they send you a response message shortly before or not.

The situation that the server stores status information about users complicates the software but we don't like complex solutions in computer science!! We always prefer easy and efficient ways. Hence, instead of more complex software, each time you send a request message to the server, the server will quickly send you a response message.

***If you want more detailed information, I recommend that you should research the concepts of HTTP and Stateless. However, these topics are beyond the scope of this course.

4)

1) Distributed Server Structure: It is a very organized structure spread all over the world.

2) Peering: It is a method that allows 2 networks to connect and exchange traffic directly without having to pay a third party to carry traffic across the Internet. According to statistics, communication with Google Servers is almost 10 times faster by using a peering connection.

5)

We call the universal network of global ISPs as Internet Backbone. I mean all global ISPs come together and form the Internet Backbone. We can think of it as the core of the communication of the whole world.

6)

*There are both technical and economic reasons for this.

1) First of all, we never want a 'Single Point of Failure' to occur and if there was only one global ISP in the world at a single point, we would have to tackle problems with 'Single Point of Failure' and load balancing. I am sure that you can currently analyze this situation very well.

2) Global ISP means communication between countries, and which means a lot of money. Hence, companies that can do business with international competence are very willing to provide global ISP services. By the way, I'm talking about a very serious amount of money so there is serious competition among global ISPs.

.

7)

IXP basically represents the structures that Global ISPs are connected to in order to work synchronously. There is no single IXP. There are several ISPs and the Internet Backbone works efficiently thanks to these IXPs.

8)

In fact, there is a very nice hierarchical and balanced relationship between ISPs. I mean, the hierarchy on the internet was really smooth and efficient. However, giant companies such as Google, Amazon, or Facebook have started to use different structures such as peering instead of using the current infrastructure of the ISPs to reach their customers faster. As a result, the hierarchy of ISPs has started to deteriorate gradually. Because these giant companies started to cover more space than ISPs. They want to access almost everywhere directly. Please do not confuse these giant companies with ISPs. Their aims are different.

Questions 1

Here there are questions about the information you have learned so far. By answering these questions, you can check which topics you understand well and which topics you do not understand well. You may also need to do some research on some questions. But all questions will be related to the information you learned.

Good luck.

1) Let's say you work as a software developer in a small office. Your boss wants the computers in the office to communicate with each other. But he doesn't want them to connect to the internet. What devices can you use in this case?

2) What are the most preferred cable types in a LAN?

3) What is the fastest type of cable for data transmission?

4) Apart from data transmission speed about cables, there is also a concept called 'frequency'. I want you to research the link between frequency and speed.

5) What is the type of network we create by connecting electronic devices in a short distance environment?

6) Suppose your company has many offices in different parts of the world. Employees in these offices sometimes have to send critical files to each other. For this reason, the boss of the company asked you to create a LAN for these offices. Because the boss has the knowledge that LAN is a very secure network. In this case, how would you answer your boss?

7) What devices can we use to create a LAN?

8) Which device do we definitely need to set up a WAN between 2 offices?

9) How do we check whether or not a computer can communicate with another computer?

10) How does a switch work? (Just think of the part we talked about in this course).

11) Why do we call the switch's ports as LAN ports?

12) Can we use the port we want when connecting computers to the switch? Or is there a sequence or rule we should follow?

Questions 1 - Solutions

1)

a) We can connect computers in the same environment using cables and switches.

b) We can connect computers in the same environment using the access point.

c) We can connect devices in the same environment using a home-router. Remember that the home-router has both a switch and access point feature. In other words, we can make this connection with both wireless technology and cable. This is up to us.

2)

There are a number of Ethernet cable categories that can be seen advertised. Cat 5, Cat 6, Cat 7 are all widely available, with Cat 5 being the oldest standard and Cat 7 the newest network cable category and with the highest performance. The different category cables have different levels of performance and as a result, it is important to select a cable that will meet the requirements for the system. The big decision when buying Ethernet cables is making the choice of the best cable. Performance benefit over cost.

For domestic use, Cat5 and Cat 5e cables are currently adequate for most applications. However, technology is constantly improving and these cables are starting to be inadequate.

If you want to be sure of getting the best speeds, then Cat 6 and Cat 6a cables are a good bet. They often don't cost too much more than Cat 5, and for future-proofing then they are a wise option.

3)

Cat 5 (Outdated) -> up to 100 Mbps

Cat 5e -> up to 1.000 Mbit/s

Cat 6 -> up to 1.000 Mbit/s

Cat 6a -> up to 10.000 Mbit/s

Cat 7 -> up to 10.000 Mbit/s

Cat 7a -> up to 10.000 Mbit/s

Fiber Optic -> up to 10.000 Mbit/s

Important => Cat7 cables are susceptible to interference and crosstalk compared to fiber, especially the longer the cable run. That's why POPs of ISPs prefer fiber optic cable when connecting. I mean speed is not the only factor.

4)

Cat 5e -> up to 1.000 Mbit/s, 100MHz

Cat 6 -> up to 1.000 Mbit/s, 250MHz

Cat 6a -> up to 10.000 Mbit/s, 500MHz

Cat 7 -> up to 10.000 Mbit/s, 1000MHz

*The frequency indicates how often the signal can pass through the cable. A Cat7 cable will therefore be able to transfer data faster than a Cat6a cable or A Cat6 cable will be able to transfer data faster than a Cat5e cable.

5)

A local area network (LAN) is a network that interconnects electronic devices within a limited area such as a residence, school, laboratory, university campus, or office building. These electronic devices can be any kind of electronic device you can think of. For example, game consoles, televisions, mobile phones, desktop computers, laptops, air conditioners and etc. Some of these devices are connected to the LAN via wireless technology, while some are connected via cable.

6)

Sometimes a boss may not know what LAN stands for and only know that it is very secure. I mean he just knows the LAN. Doesn't know the Local Area Network. Hence, you must tell your boss the following.

"LAN is very secure, that's true, but to create a LAN, the distance must be limited. If you want offices in different regions of the world to create a company-owned network, we must set up a WAN."

7)

If we want to create a LAN, the device we need to use is the switch. But as you know, home-routers have a switch feature. For this reason, we can create a LAN by using a home-router, too.

On the other hand, as you know, there are access point devices. I want to give extra information here. Assume that there are 5 computers in the office and all of these computers are communicating with wireless technology over the access point. We call such networks Wireless Local Area Network (WLAN) instead of Local Area Network (LAN). Please note that if all devices on the network are connecting via wireless, this is WLAN. On the other hand, if even a single computer in the environment is connected to the network by cable, we call it a LAN.

So let's say we have 5 devices connected to each other via wireless technology in our house. 2 mobile phones, 1 television, and 2 laptops. This connection takes place via home-router. Our home network is now a WLAN. But suppose you connect another computer with a cable to the home router. Our home network has now become a LAN.

8)

As you know, the general purpose of WAN is to connect LANs in different locations and the device that connects different LANs is the router. So if we want to create a WAN, we need to have a router in both offices and we set up the WAN through these routers. These routers can be the routers that we connect to the internet. We do not need different routers to set up a WAN.

9)

If one computer can send a packet to another computer, it means that 2 computers can communicate. Especially system administrators and network experts use this information a lot in troubleshooting processes. Please check the 'ping' command. It is a valid command for both Linux, Windows, and Mac OS.

10)

1) The switch receives a packet from one of its ports and gives this packet to its hardware.

2) The switch looks inside this packet with the help of its hardware and learns the destination address of the packet.

3) The switch forwards the packet to the appropriate port connected to the destination device and sends it to its destination.

**In summary, the switch is a smart device. It receives the packet, checks the packet's destination, and sends the packet to its destination. That's it.

11)

We plug the computers into the ports of the switch and as a result, we create a LAN. For this reason, it is quite logical to call these ports LAN ports.

12)

There is no order or rule to follow. All ports have the same function. However, it is recommended to make the connections to the ports sequentially in order to be neat and not to create cable mess.

Questions 2

Here there are questions about the information you have learned so far. By answering these questions, you can check which topics you understand well and which topics you do not understand well. You may also need to do some research on some questions. But all questions will be related to the information you learned.

Good luck.

1) What device is absolutely necessary for computers in an office to be able to connect to the internet?

2) When we want to connect to the Internet, we connect a cable that comes to our home to the home-router. Who do we purchase this cable from??

3) If a packet is to exit from the network it is in, which device does it have to go to no matter what?

4) There are millions of networks in the world. What is the name of the giant structure that connects all these networks?

5) What is the point of presence (POP)?

6) Why is the distributed POP structure used on the Internet?

7) What is the ARPANET? (You need some reading about it)

8) Why do we want to use a home-router?

9) You know that a very powerful giant router in the middle of the world is a very problematic design for the internet.

   So what if we apply the distributed POP structure to a specific point in the middle of the world? (I mean imagine that the internet is controlled by 300 POPs in the middle of the world.)

10) What are the most important reasons why POPs use fiber optic cables when connecting to each other?

11) What is the Routing Table?

12) What is the Forwarding?

Questions 2 - Solutions

1)

Connecting to the Internet basically represents connecting to a different network or a different computer. We communicate with any device in the world over the Internet. And as you know, if we want to communicate with a different network than the one we are in, we definitely need a router.

***As a result, we definitely need a router if we want to connect to the internet.

2)

ISPs are companies that enable us to connect to the internet. We rent lines from these companies in order to connect to the internet.

3)

A router is like an exit door of a network. If a packet will go out of the network where it is in, it must pass through the router.

4)

The Internet is a vast network that connects computers and electronic devices all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection.

5)

POP is primarily the infrastructure that allows remote users to connect to the Internet. A POP is generally present at an Internet service provider (ISP) or the telecommunication service provider. It can consist of a router, switches, servers, and other data communication devices. An ISP or telecom provider might maintain more than one POP at different locations, with each catering to a distinct user base.

Point of presence (POP) is the point at which two or more different networks or communication devices build a connection with each other. POP mainly refers to a location or facility that connects to and helps other devices establish a connection with the Internet. A POP is not just one single item, system, or device; it's a collection of

telecommunications technologies and equipment that allows users to access the Internet.

6)

a) As you know, load balancing is a very important concept. Suppose there is only one giant router in the middle of the world. Let this router control the internet of the whole world. Imagine billions of packets going to this router at the same time. It's easy to imagine a lot of load on this router. Instead, we distribute all this load by placing POPs in different parts of the world.

b) In addition to the load balancing problem, if the giant router in the middle of the world somehow breaks down, the whole world's Internet will crash down at the same time. If you remember, we called this problem 'Single Point of Failure'. With the distributed POP structure, 'the single point of failure'-related problems is prevented.

c) Thanks to the distributed POP structure, a very serious cable mess is prevented. Imagine all the devices in the world connecting to the same point. What a mess!!!

7)

ARPANET is the ancestor of the Internet infrastructure you learned in this course. This project aimed to keep computers in the USA communicating with each other in the event of a disaster.

Now consider this idea on the internet, the common network of the whole world. Let's say a meteorite hit the earth and a part of the earth got serious damage from this hit. In other words, POPs in a certain area of the world destroyed. But the internet can continue to work and devices in other parts of the world can continue to communicate with each other. This is the power of distributed structure.

8)

Basically, we can configure almost any network by using switches, access points, and routers. However, these individual devices can be more expensive than necessary. For

example, a normal person does not need a 20-port switch. Or a normal person doesn't need a very powerful router that can handle many packets at the same time.

This is where the home-router comes into play. A home-router has both switch, router, and access point features. A home-router is an affordable device and can meet all the needs of a normal person.

9)

So what if we apply the distributed POP structure to a specific point in the middle of the world? (I mean imagine that the internet is controlled by 300 POPs in the middle of the world.)

This is definitely a better solution than the Giant router solution. However, similar problems still persist.

First of all, the giant router design is an already imaginary design. In other words, it is impossible to design a giant, very powerful device to which all electronic devices in the world can be connected. However, an internet structure consisting of many POPs located in a specific part of the world is possible.

If you are aware, the basic logic is to connect the whole world to the internet through a single point and you know what problems this design causes. (Load balancing, single point of failure, cable mess and etc.)

10)

a) Fiber optic is the fastest type of cable.

b) Fiber optic cable is very successful in transmitting data over long distances compared to copper cable. While the probability of data corruption increases as the distance increases in the copper cable, the data is not corrupted in the fiber optic cable even if the distance is too long.

11)

A router looks at the routing table to decide over which path it must send the packet. In short, the routing table is a database storing information related to the best possible routes.

12)

After a router receives a packet, it looks at the routing table and sends it to an appropriate port. This process is called forwarding. The forwarding process is handled entirely within the router. The packet is received on one port and sent to the other port. That's it.

Questions 3

Here there are questions about the information you have learned so far. By answering these questions, you can check which topics you understand well and which topics you do not understand well. You may also need to do some research on some questions. But all questions will be related to the information you learned.

Good luck.

1) Where is a router's routing table created?

2) What is the 'Route Filtering'?

3) What is the 'Congestion Control'?

4) What is the bookish definition of the internet? Does it make sense to you?

5) What's going on in the background when you want to watch a video on Udemy or any website?

6) Why do servers have to be much more powerful than normal computers?

7) 2 offices belonging to the same company located in different regions of the world can easily send files to each other over the internet. Despite this, why would these offices want to set up a WAN?

8) Who is the owner of the Internet? (You should do some reading)

9) Which one is safer? LAN? or Public WAN (WAN with VPN)?

10) Which one is safer? LAN? or Private WAN?

11) What is the 'Tunneling'?

12) What is the 'Site to Site VPN'?

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.

Questions 1

Here there are questions about the information you have learned so far. By answering these questions, you can check which topics you understand well and which topics you do not understand well. You may also need to do some research on some questions. But all questions will be related to the information you learned.

Good luck.

1) What is the 'End to End Encryption?

2) Why is encryption so important?

3) What is the largest WAN in the world?

4) What is the 'Campus Area Network (CAN)'?

5) What is the 'Internet Service Provider (ISP)'?

6) What is the 'Local ISP'?

7) What is the 'Regional ISP'?

8) What is the 'Global ISP'?

9) How does a local ISP directly connect to a global ISP?

Questions 4 - Solutions

1)

'End-to-end encryption' is intended to prevent data from being read or secretly modified, other than by the true sender and recipient(s). The messages are encrypted by the sender but the third party does not have the means to decrypt them. So the third party can only store the data as encrypted. The recipients retrieve the encrypted data and decrypt it themselves.

2)

Encryption is the process through which data is encoded so that it remains hidden from or inaccessible to unauthorized users. It helps protect private information, sensitive data, and can enhance the security of communication between user devices (clients) and servers. In essence, when your data is encrypted, even if an unauthorized person or entity gains access to it, they will not be able to read it.

3)

As you know, different LANs come together to create a WAN. Also, you know that millions of networks come together to create the internet. From here, we can easily understand that the Internet is the world's largest WAN.

4)

Campus Area Network (CAN) is a group of interconnected Local Area Networks (LAN) within a limited geographical area like a school campus, university campus, military bases, or organizational campuses and corporate buildings, etc. A Campus Area Network is larger than a Local Area Network but smaller than Wide Area Network (WAN).

Most CANs are comprised of several LANs connected via switches. The CANs behave just like the LANs. I mean they have similar features. Hence, you can think of a CAN as a special LAN.

5)

Internet service provider (ISP), a company that provides Internet connections and services to individuals and organizations. The ISP gives us a line so that we can connect to the internet for a certain amount of money. So without an ISP, we cannot access the internet.

6)

Local ISP generally represents ISP companies connecting small districts and neighborhoods. It is the most common type of ISP in the world. Normal users usually connect to local ISPs to access the internet. But this is definitely not a must.

7)

Regional ISP usually represents ISP companies connecting cities and provinces belonging to a country. Local ISPs and Regional ISPs combine to form a country's network. If a normal user requests, they can get service from the regional ISP instead of the local ISP.

8)

Global ISPs represent ISPs connecting different countries. They form the basis of international communication.

9)

Here are 2 ways a local ISP can connect directly to the global ISP.

1) Global ISP already has infrastructure at the location of the local ISP. For this reason, if the Local ISP wants to connect to the Global ISP, this connection can be made easily.

2) The local ISP gives enough money to the global ISP. Thus, the global ISP provides the required infrastructure to the local ISP and the connection is established.

**Connecting directly to the Global ISP can increase the speed noticeably.