

Networks and Internet Applications

Continuous Assessment Test - CA1

Nicolas D'Alessandro Calderon

Answers

1. Find some graphic material (video, infographic, etc.) that briefly explains the history of the Internet. View it and share it through the classroom forum, briefly explaining why you chose it.

Video shared in the forum: <https://www.youtube.com/watch?v=U5zHadHP7nM>

2. Answer the following questions about IP addressing:

- a. For the address: **148.83.98.65/22** calculate the network, the broadcast address and the range of hosts.

- The subnet mask /22 means that the first 22 bits are fixed, corresponding to 255.255.252.0
- The remaining 10 bits are for the hosts $2^{10} = 1024$ addresses in total.
- From this, one is for the Network Address, one for the Broadcast Address and the remaining 1022 addresses for the hosts.
- With this subnet mask /22 or 255.255.252.0 we have that the addresses change in 4 by 4 in the third octet since $256 - 252 = 4$.
- This means that we are in the block starting at 96 and ending in 99 since $98 / 4 = 24$ with modulus 2. So, if we multiply $24 * 4 = 96$. So, Network = 148.83.96.0, first usable host = 148.83.96.1, last usable host = 148.83.99.254 and broadcast address 148.83.99.255.

Element	Function	Value
Network Address	Beginning of the group	148.83.96.0
Host Range	Range of addresses available to use	148.83.96.1 - 148.83.99.254
Broadcast Address	For sending messages to everyone	148.83.99.255

b. In a network with 1000 hosts, what is the minimum netmask that would support that number of hosts?

- To find the /n in a network of 1000 hosts we will use the formula $\text{Hosts} = 2^{(32 - n)} - 2$ where n is the number of bits used for this network, $2^{(32 - n)}$ are the number of possible addresses minus 1 for the network and 1 for the broadcast.
- We search for the minimum value that gives at least 1000 hosts which is /22 since $2^{(32 - 23)} - 2 = 510$ Not enough, $2^{(32 - 22)} - 2 = 1022$ OK
- So, the minimum netmask that would support 1000 hosts is /22 or 255.255.252.0.

Netmask /n	Decimal Format	Hosts Available
/22	255.255.252.0	1022

c. The network to which the address **148.83.98.65/22** belongs needs to be segmented into at least 42 subnets. Calculate the required subnet mask, and the first five resulting subnets.

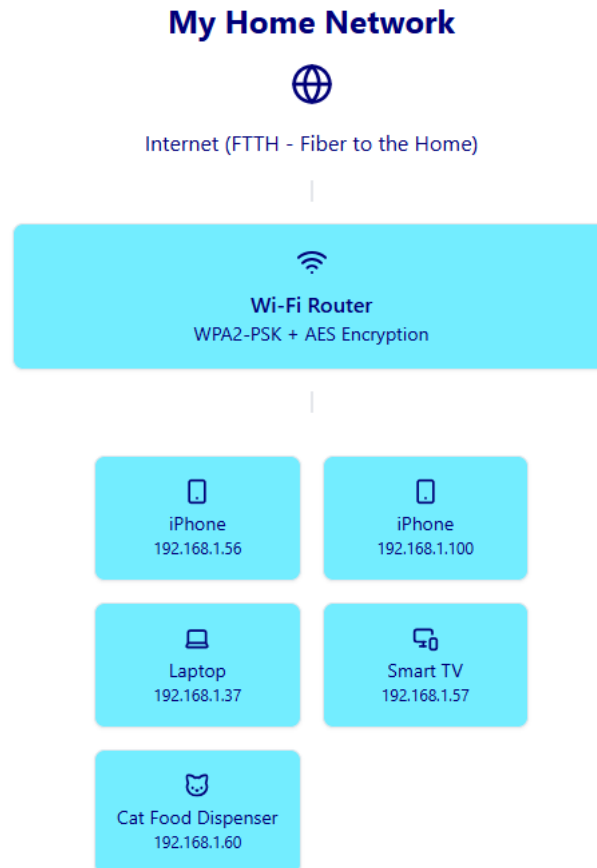
- From the previous exercises we know that for this system starting at 148.83.96.0/22 we have 1024 IP addresses in total.
- So, if we want to divide into at least 42 subnets, we need to find how many bits are required.
- We will apply the formula $2^n \geq \text{subnets needed}$.
- In this case the minimum n will be $2^5 = 32$ (not enough), $2^6 = 64$ OK. So, 6 bits more are required to divide.
- /22 + 6 bits = /28, meaning that the new subnet is /28 or 255.255.255.240 in decimal, where each subnet has 16 addresses in the fourth octet: $2^{(32 - \text{mask} / n)} = 2^{(32 - 28)} = 16$.

Required subnet Mask /n	Decimal Format
/28	255.255.255.240

- Since the base subnet was 148.83.96.0, and the step is 16, the first 5 resulting subnets for our new subnet mask /28 or 255.255.255.240 are:

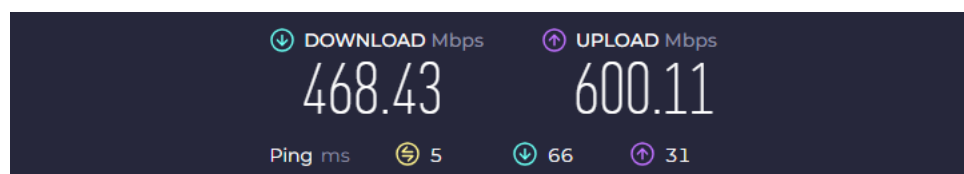
148.83.96.0/28
148.83.96.16/28
148.83.96.32/28
148.83.96.48/28
148.83.96.64/28

3. Make a diagram of your home Internet connection, including all the main elements, such as hosts, routers, switches, access points, and IoT devices. Answer the following questions:



- a. What type of Internet access do you have (fiber optics, ADSL, etc.)? Explain its main characteristics (bandwidth, latency, etc.) and include a technical comparison between your type of access and another, such as 5G connections.

My internet connection is **FTTH (Fiber To The Home)** provided by Movistar.



Based on this recent speed test, my bandwidth is approx. **468 Mbps for Download and 600 for Upload with a very low latency of 5 ms**. Since I work from home in an online games development company, this kind of connection is ideal for streaming, videoconferencing, online gaming or downloading large files. Compared to other types of access such as ADSL or 5G, this fiber offers more stability and speed.

- b. Identify any security device or mechanism on your network (such as a firewall, VPN, etc.) and explain how it protects your network (packet filtering rules, user authentication, etc.)



Nombre Wifi: MOVISTAR_10AA

Ocultar nombre Wifi: ☐ Sí ☒ No

Clave Wifi: (Introduce letras, números y caracteres especiales (@,&!,+, etc) para que tu clave wifi tenga seguridad alta)

Nivel de seguridad de la contraseña: Media

Estado Red Inalámbrica: ☒ Activado ☐ Desactivado

 Aviso: Los métodos de cifrado WPA o WEP no son compatibles con WPS (2.0). Si seleccionas alguno de ellos la funcionalidad WPS quedará desactivada en tu router.

Tipo de cifrado: WPA2-PSK

Encriptación: AES

Número canal WiFi: Auto

Canal actual: 6

- My wireless network uses WPA2-PSK with AES encryption.
- I use a custom password and not the default by fabric.
- The router allows me to hide the SSID MOVISTAR_10AA, but since it is not a strong protection because it can be detected with basic tools, it is set to visible.
- The router has a Firewall included for filtering connections and the WPA2 encryption ensures that only users with the password can connect.

- c. What is the model of your router, and what is its default password? Explain the security implications of keeping the default password.

The model of my router is MitraStar GPT-2541GNAC provided by Movistar, the default is MOVISTAR_10AA and the default password is in the sticker under the router.

I have changed to a custom password, but many people don't change it. The security implications for not changing can be that anyone that enters my home and has physical access to the router can see the password and connect. Also, some default passwords are repetitive and predictable so attackers can connect to the Wi-Fi and access private data or change the router configuration.

4. In the following link you can see the transoceanic cables that support Internet communications: <https://www.submarinecablemap.com/>. Choose one and find out its technical specifications (bandwidth, physical medium, etc.)



Selected cable: **MAREA**

This cable has been working since May 2018 and is recognized as one of the fastest in the world. It was designed to transmit high speed data between North America and Europe. Its route avoids seismic zones to improve stability.

Technical Specifications:

Cable Length

6605 Km

Landing Points

Virginia Beach, EEUU

Bilbao, Spain

Capacity

200TBps

Owners

Meta, Microsoft, Telxius

Suppliers

SubCom

5. The Internet is a network of networks structured in layers (*tiers*) where several ISPs (Internet Service Providers) are interconnected with each other.



- a. Comment on the different types of ISPs that can be found and what role they play.

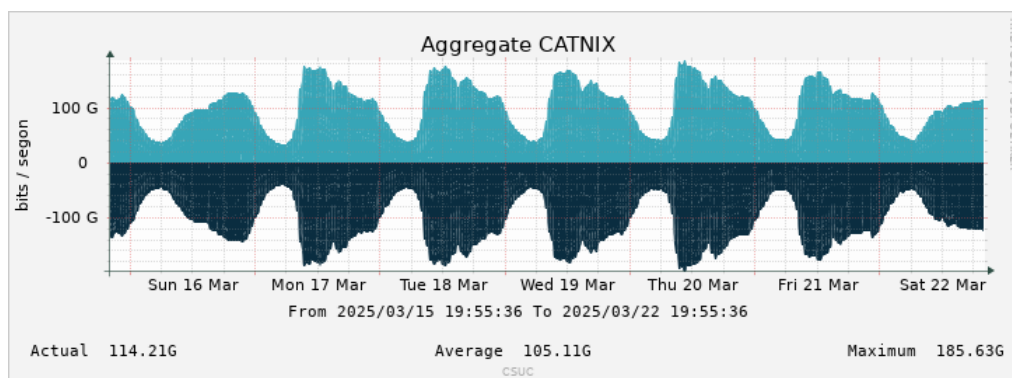
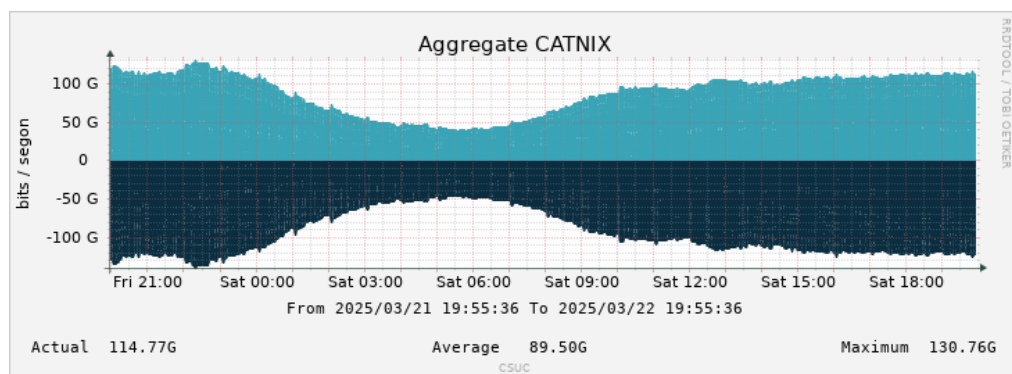
- **ISP Tier 1:** Global operators that owns the infrastructure. They are the biggest in the world, with their global infrastructure that includes elements such as submarine cables, datacenters, etc. They have peering agreements that include free traffic exchange among each other. Example: AT&T, NTT or Deutsche Telekom
- **ISP Tier 2:** These are the regional or national operators. They are smaller than the previous ones, but very important. They also maintain some peering agreements, but they buy ISP Tier 1 connection. Examples in Spain: Telefonica (Movistar), Orange, etc.
- **ISP Tier 3:** These are local operators that buy traffic to Tier 2 or 3 ISPs. Examples in Spain: Netllar (Catalunya), Euskaltel (Basque Country), etc.

b. What types of technologies and techniques do Tier 1 ISPs use to interconnect with each other?

- High-capacity fiber optics such as **Dense wavelength division multiplexing (DWDM)** which is a fiber-optic transmission technique that involves the process of multiplexing many different wavelength signals onto a single fiber.
- Submarine cable systems such as the MAREA cable connecting 6600 km from Virginia Beach to Sopot in Poland described in exercise 4.
- High-capacity routers called backbone routers.
- Datacenters and redundant systems in case of failure.
- The already mentioned Peering agreements to share traffic with no cost.
- Border Gateway Protocol BGP to exchange routes.

c. Consult the following web address and locate an IXP in Spain: <https://www.internetexchangemap.com/>. Connect to their website and indicate what peak traffic can be reached in a day.

- One of the IXP in Spain is CATNIX located in Sant Adrià de Besòs, Barcelona. Based on their website, we find a graph from March 22, 2025, where it shows that **the peak traffic in one day reached 130.76 Gbps.** and in the weekly graph we found that the **maximum peak traffic reached 185.63 Gbps.**



6. The Internet is based on a protocol stack, so that each layer is seen as a service that is offered to the higher level, and takes advantage of the services of the lower level (vertical communication). At the same time, each layer communicates following a protocol with its counterpart on another machine (horizontal communication).

In the late 1970s, the ISO (International Organization for Standardization) proposed the OSI stack as a model to follow when designing communications networks.

- a. Find information about the OSI model and make a diagram of the two (Internet and OSI) where the similarities and differences are seen.

OSI Model vs Internet Protocol Stack



- b. Briefly explain them.

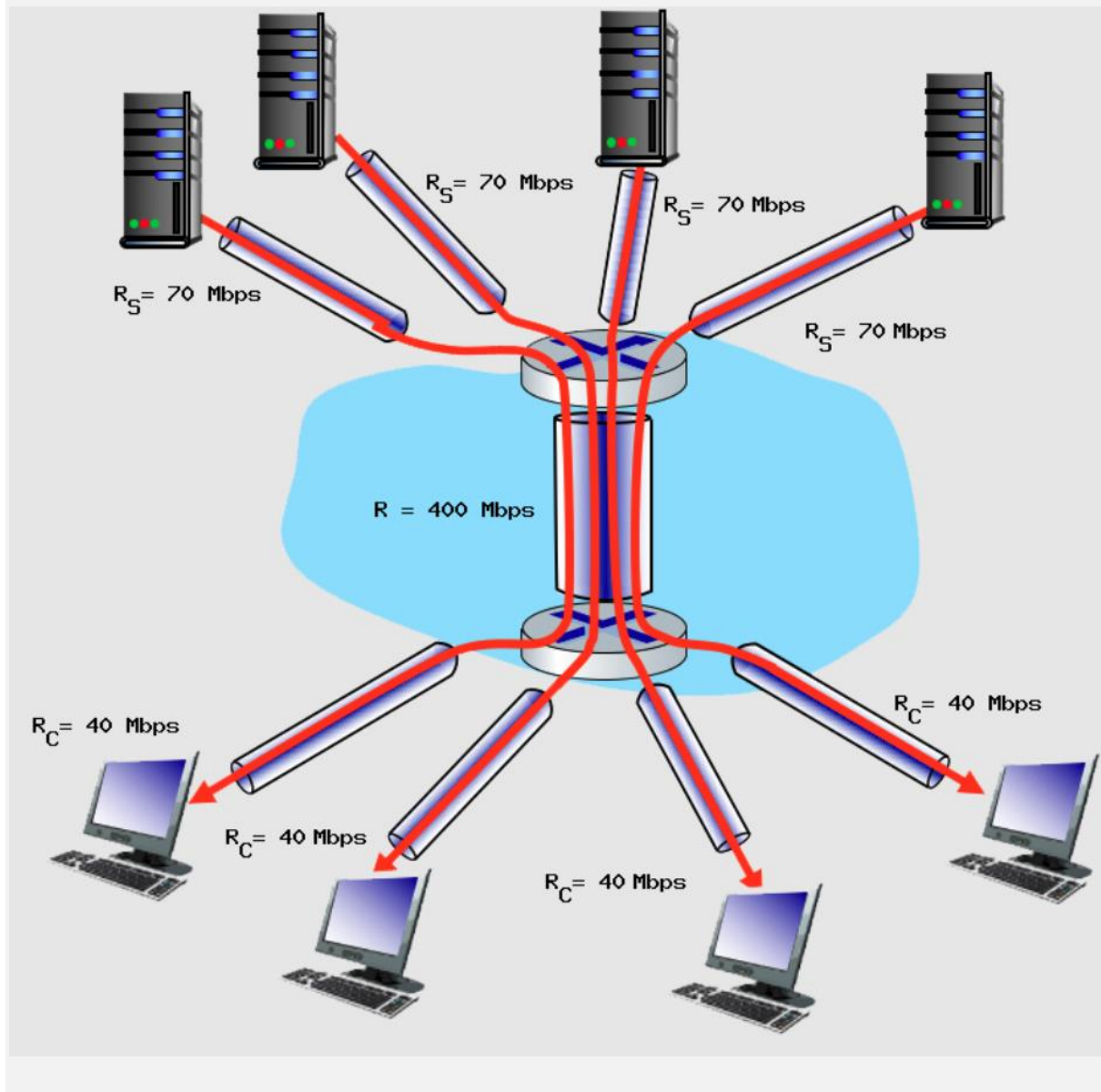
Similarities: As we can see, both models have a layered architecture of communication to separate concerns. Both follow the principle of encapsulation where each layer adds its own header to the data.

Differences: OSI has 7 layers since the application functionality is divided into three distinct layers. Internet protocol stack model has 4 broader layers which is more practical and that's why it is currently the most used in real-world systems.

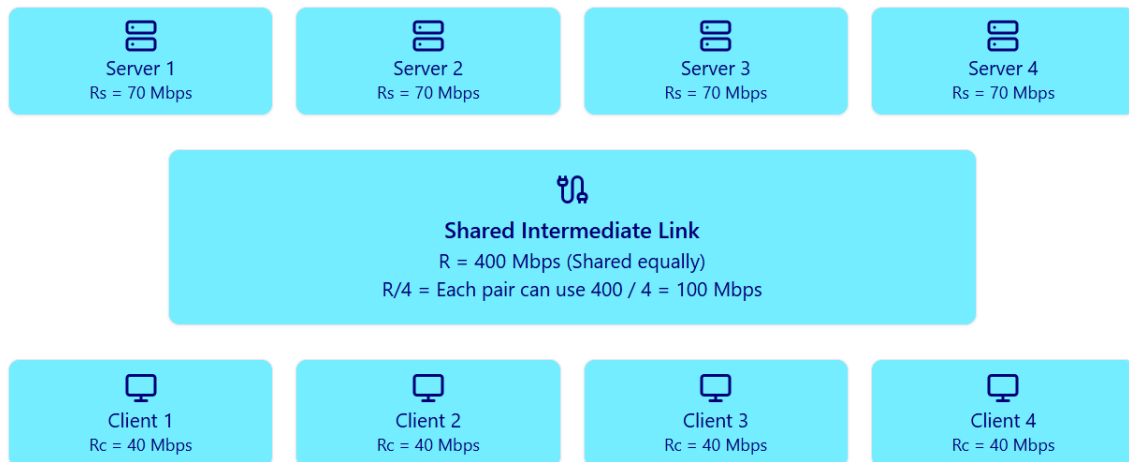
- c. Find out if there are currently any products or systems that follow the OSI model.

While the OSI model is not directly implemented in modern products it has a great influence on the design of currently used devices and protocols. For example, Cisco use the OSI model as an education reference for its technical documentation (<https://learningnetwork.cisco.com/s/article/osi-model-reference-chart>). Also, Wireshark, the tool used in the PR1, organize layers in a very similar way that the OSI model <https://medium.com/the-cabin-coder/viewing-osi-layers-on-wireshark-a51b77cfbd72>.

7. In the following figure, four servers are connected to four clients by four three-hop paths. They all share a common link with a transmission capacity of $R = 400$ Mbps. The four links from the servers to the shared link have a transmission capacity of $R_S = 70$ Mbps. Each of the four links from the intermediate shared link to a client has a transmission capacity of $R_C = 40$ Mbps.



Client-Server Throughput Sharing



- a. What is the maximum end-to-end throughput, in Mbps, for each of the four client-to-server pairs, assuming the intermediate link is equally shared (divides its transmission rate equally)?

The maximum end-to-end throughput is 40 Mbps, corresponding to the lower link, meaning that **each client-server has a maximum throughput of 40 Mbps.**

- b. Which link of all, Rc, Rs, or R is the bottleneck?

Rs = 70 Mbps, R = 100 Mbps, Rc = 40 Mbps,
The bottleneck is the minimum of these three, so **the bottleneck link is Rc = 40 Mbps.**

- c. Assuming the servers are transmitting at their maximum possible speed, what is the percentage utilization of the Rs links?

If the servers transmit at their maximum possible speed 70 Mbps, they will be anyway limited by Rc which is 40 Mbps, **so the percentage utilization of the Rs links will be current traffic / total capacity = 40/70 = 57.14%**

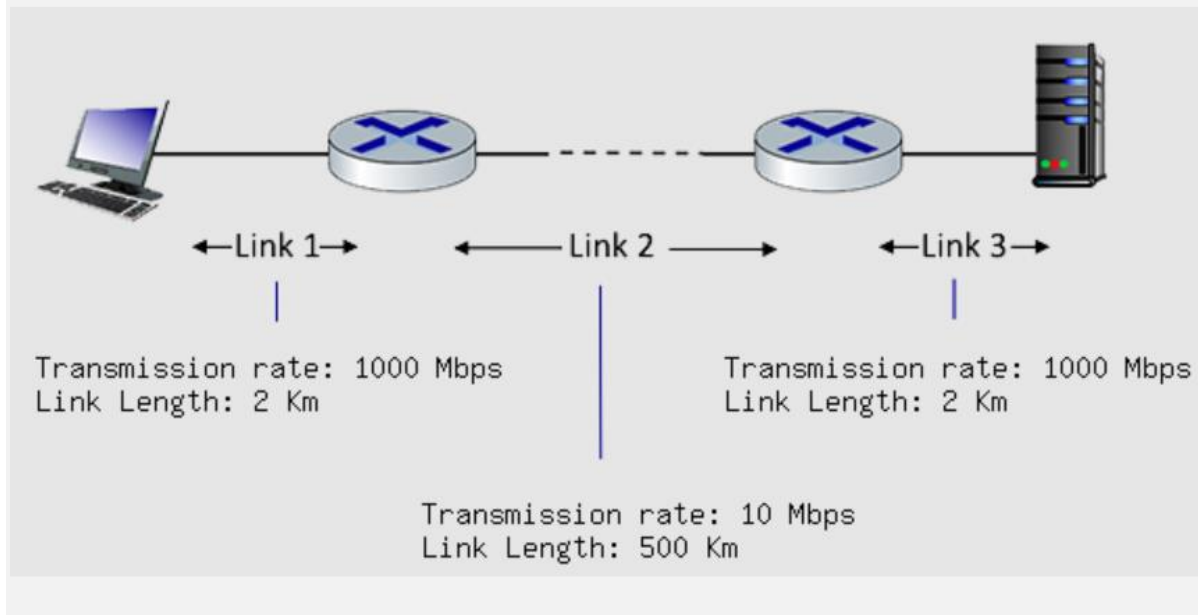
- d. Assuming the servers are transmitting at their maximum possible speed, what is the percentage utilization of the Rc links?

Since the clients receive 40 Mbps which is their full capacity, **the percentage of utilization of the Rc links will be current traffic / total capacity = 40/40 = 100%**

- e. Assuming the servers are transmitting at their maximum possible speed, what is the percentage utilization of link R?

Since each client-server connection is receiving 40 Mps the total traffic will be $4 \times 40 = 160$ Mbps, **so the percentage of utilization of R link will be current traffic / total capacity = 160/400 = 40%**

8. In the following figure we see three links, each with the specified transmission rate and length. Assuming that the length of a packet is 4000 bits and that the speed of light propagation delay on each link is 3×10^8 m/s, answer the following questions:



- a. What is the transmission delay and propagation delay for each link?

$$\text{Transmission delay} = \text{Packet Size } L / \text{Transmission Rate } R = L/R$$

- Link 1:** $4000 \text{ bits} / 1000 \text{ Mb/s} = 4000 \text{ bits} / 10^9 \text{ bits/s} = 4 \times 10^{-6} \text{ s} = \mathbf{4 \text{ microseconds}}$
Link 2: $4000 \text{ bits} / 10 \text{ Mbps} = 4000 \text{ bits} / 10^7 \text{ bits/s} = 4 \times 10^{-4} \text{ s} = \mathbf{400 \text{ microseconds}}$
Link 3: $4000 \text{ bits} / 1000 \text{ Mbps} = 4000 \text{ bits} / 10^9 \text{ bits/s} = 4 \times 10^{-6} \text{ s} = \mathbf{4 \text{ microseconds}}$

$$\text{Propagation delay} = \text{Distance } d / \text{Speed of light Propagation } s = d/s$$

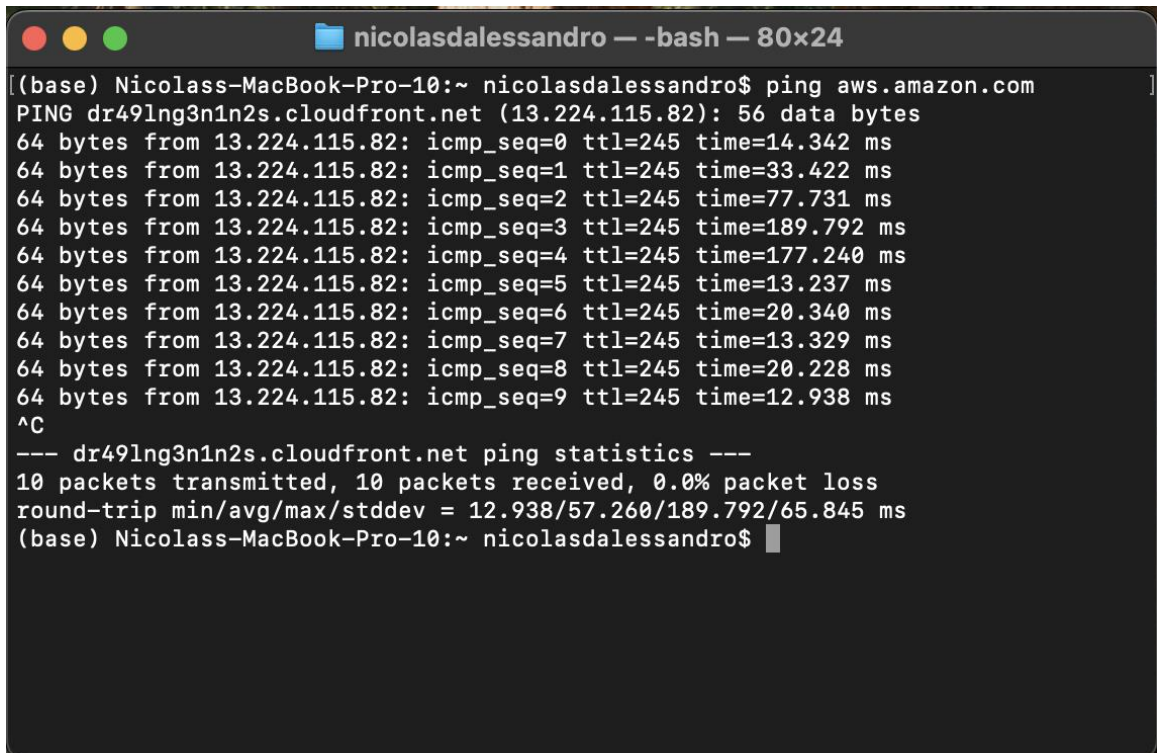
- Link 1:** $2000 \text{ m} / 3 \times 10^8 \text{ m/s} = 6.67 \times 10^{-6} \text{ s} = \mathbf{6.67 \text{ microseconds}}$
Link 2: $500000 \text{ m} / 3 \times 10^8 \text{ m/s} = 1.67 \times 10^{-3} \text{ s} = \mathbf{1670 \text{ microseconds}}$
Link 3: $2000 \text{ m} / 3 \times 10^8 \text{ m/s} = 6.67 \times 10^{-6} \text{ s} = \mathbf{6.67 \text{ microseconds}}$

- b. What is the total delay?

$$\text{Total Delay} = (\text{Link 1 transmission} + \text{Link 1 propagation}) + (\text{Link 2 transmission} + \text{Link 2 propagation}) + (\text{Link 3 transmission} + \text{Link 3 propagation})$$

$$\text{Total Delay} = 4 + 6.67 + 400 + 1670 + 4 + 6.67 = \mathbf{2091.34 \text{ microseconds} \approx 2.09 \text{ milliseconds}}$$

9. The ping command is a network diagnostic tool used to verify connectivity between two hosts. Run a ping against any machine on the Internet and answers the following questions (attach a screenshot of the command output):



```

nicolasdalessandro — -bash — 80x24
((base) Nicolass-MacBook-Pro-10:~ nicolasdalessandro$ ping aws.amazon.com
PING dr49lng3n1n2s.cloudfront.net (13.224.115.82): 56 data bytes
64 bytes from 13.224.115.82: icmp_seq=0 ttl=245 time=14.342 ms
64 bytes from 13.224.115.82: icmp_seq=1 ttl=245 time=33.422 ms
64 bytes from 13.224.115.82: icmp_seq=2 ttl=245 time=77.731 ms
64 bytes from 13.224.115.82: icmp_seq=3 ttl=245 time=189.792 ms
64 bytes from 13.224.115.82: icmp_seq=4 ttl=245 time=177.240 ms
64 bytes from 13.224.115.82: icmp_seq=5 ttl=245 time=13.237 ms
64 bytes from 13.224.115.82: icmp_seq=6 ttl=245 time=20.340 ms
64 bytes from 13.224.115.82: icmp_seq=7 ttl=245 time=13.329 ms
64 bytes from 13.224.115.82: icmp_seq=8 ttl=245 time=20.228 ms
64 bytes from 13.224.115.82: icmp_seq=9 ttl=245 time=12.938 ms
^C
--- dr49lng3n1n2s.cloudfront.net ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 12.938/57.260/189.792/65.845 ms
(base) Nicolass-MacBook-Pro-10:~ nicolasdalessandro$

```

- a. What is the destination IP address?

The **destination IP address is 13.224.115.82**. In this case when we initiated the ping, the request was resolved to a CloudFront hostname dr49lng3n1n2s.cloudfront.net and the IP.

- b. What is icmp_seq ?

The **icmp_seq is a sequence number starting from 0 where each new packet increments the value in 1**.

It helps to track which packets are returned and if any are missing.

- c. What is TTL and what does it mean?

The Time To Live TTL is a value in the IP header that limits the “hops” (amount of time or quantity of devices like routers) that the packet can go through before being discarded.

Certain operating systems use different initial values, but from this initial number, each router that the package crosses will decrease the TTL by 1, so when it reaches 0 the packets are discarded. This helps to prevent the packet will circulate in infinite routing loops.

d. What does the time field indicate ?

The time field indicates what is called RTP or Round-Trip Time which represents the total time in milliseconds that each ping packet travels to its destination and returns to our device. We can say that it represents a direct measure of the network latency.

e. Has there been any packet loss?

No, in this example we can see that 10 packages were sent, 10 received so 0.0% loss.

f. What percentage of packet loss can be considered acceptable in a network?

The acceptable packet loss may depend on the application, but as a rule a good network should have a 0% packet loss.

Up to 1% can be ok in some cases but 2% or more can make our connection slow or unstable.

g. What was the average propagation delay and in what unit of time is it measured?
Depending on what factors can it vary?

The average delay in our example was 57.260 milliseconds. This delay can change depending on factors such as the distance to the server, the internet traffic, the device or router and the type of connection (cable, Wi-Fi, Fiber, etc.)

10. Find a news story about cybersecurity. Choose one published in the last month (include the date) and detail which concepts from the "*Networks under attack*" section of Kuroses's book are covered in it.

This news talks about the raise in cyberattacks to Spanish companies in the last years, attack vectors and recommended protective measures:

<https://cadenaser.com/cmadrid/2025/03/18/se-incrementan-los-ciberataques-a-empresas-principales-vectores-de-ataque-y-como-protegerse-ser-madrid-sur/>

Analysis of concepts from Kurose's chapter "Networks Under Attack" covered in this article:

Confidentiality

Attackers gain access to sensitive company data, violating data confidentiality.

Integrity

Some attacks modify or corrupt data, affecting its accuracy and credibility.

Availability

Ransomware and other attacks disrupt access to systems, making services unavailable for a short or long time.

Social Engineering

Use of phishing emails and fraud to trick employees into opening malicious content or providing credentials.

Access Control

The article indicates weaknesses in third-party provider systems, suggesting access control and perimeter defense errors.

References

Kurose, James F. **Computer Networking: A Top-Down Approach**. Eighth edition. Boston [etc.] : Addison-Wesley, cop. 2021. ISBN 9781292405513

In addition to the learning material given for this unit, I have consulted the following materials in the internet:

"What is an IP Address? // You at Subnetting // EP 1."

<https://www.youtube.com/watch?v=5WfiTHiU4x8>

"Centro de Datos y Puntos Neutros de Internet."

Ministerio de Economía, Gobierno de España.

<https://conectemos.mineco.gob.es/es/punto-contacto-unico/centro-de-datos-puntos-neutros-internet>

"Dense Wavelength Division Multiplexing."

ScienceDirect, Elsevier.

<https://www.sciencedirect.com/topics/computer-science/dense-wavelength-division-multiplexing>

"MAREA Submarine Cable."

Telxius Telecom.

<https://telxius.com/nuestra-red/marea/>

"Modelo OSI y Wireshark – Prezi Presentation."

Prezi.

<https://prezi.com/p/mhipq2ooh-l2/modelo-osi-wireshark/>

"El Comando Ping – Preguntas Frecuentes."

AlexHost.

<https://alexhost.com/es/faq/el-comando-ping>

"Time to Live (TTL) – What Is TTL?"

Cloudflare Learning Center.

<https://www.cloudflare.com/es-es/learning/cdn/glossary/time-to-live-ttl/>