Q1. A. What is a network protocol?

B. Write a simple protocol spec for the following task: consider two people playing a game where one has a secret number in 1 to 10 and the other is attempting to guess it. But the two people can only communicate by each alternatively saying a single number.

Ans:1 =

(A)= Network protocol's are formal standar -ds and policies comprised of rules procedures and formats that define the communication between two or more devices over a network. network protocol governs the end to end processes of timely, secure and managed data or network communication.

(B)= Protocol=

1)= let the person who has the number be A and the one guessing it is B.

2)= A connection request is sent from A to B. and B sends the response after a successful connection.

3)= A sends a signal to start the game (say he sends a number 0 as A and B can only communicate with numbers)

4)= B receives this and sends the guessed number as response.

5)= if A receives the same number as guessed by B, it sends the same number to B and the game can be stopped. A sends the number 0 indicating it was a wrong guess. B receives this and sends the guessed number again and the game continues until correct number is guessed.

Q2. A. What are the basic paradigms (or models) of communication? (mention 3)

B. What are the processes are needed to support all these paradigms?

Ans:2 = Basic Paradigms =

① = Client server model = client and Server are differentiated properly - client send the request and Server sends the respon -se. network management or centralized.

② = Peer to peer model = Client & Server are not differentiated Each entity can behave as client and Server.

③ = Broadcast = Just like peer to peer except a message could be sent by one entity to many entities at the same time.

(B) = To support any communication frame work there should be atleast two parties involved. one that can send the message and other one which can receive the message. if there are no entities to listen or if all the entities are just listening then communication will not happen. so for a succesful communication parties should fall anyof the three categories mentioned above.

Q3. What are the advantages and disadvantages of:

A. Hierarchical network architectures

B. Protocol layering

C. Stateless protocols

Ans-3 =

(A) = Hierarchical network architectures.

Advantages = (1) = Provides stable environment for communication

(2) = Scalable

(3) = routing tables are efficient.

(4) = Network is flexible.

Disadvantages =

(1) = Huge hierarchical architecture requires overhead for establishing and maintaining the architecture.

(B) = Protocol layering =

Advantages =

(1) = Biggest advantage is abstraction

(2) = Protocol layer is extensible.

Disadvantages =

(1) = Having many layers creates the overhead as every layer adds the information and increase communicatio -n overhead.

(2) = Difficult to figure out bad interacti -our among the layers.

(C) = Stateless Protocols =

Advantages =

(1) = Biggest advantage is parties are not required to store anything and manage memory.

(2) = less complex as data is not stored.

(3) = each session is treated as new one.

Disadvantages =

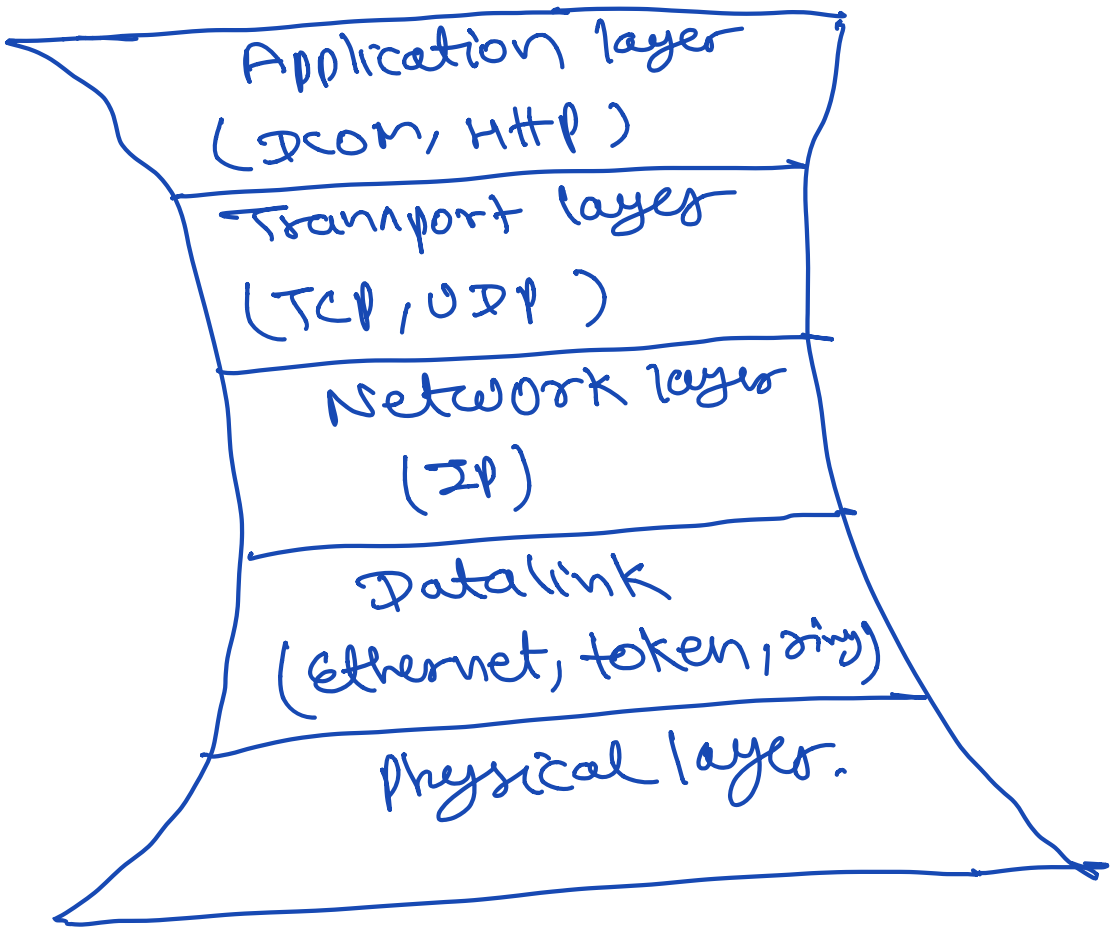
NOT storing data could be disadvantage as well in some cases, customers might want to store data, cookies are used to store information. But that might not serve the purpose always.

Q4. A. What is the *hour-glass* Internet model? (use simple drawing to illustrate)

B. Give two examples of protocols at the *thin waist* of the hourglass? Why are these protocols at the *thin waist*?

Ans.4 =

(A)=



(B)= Network and Transport layers are the two examples of protocols at the thin waist of the hour glass model. The layers at top & botton might contain many protocols But Transport layer has only two protocols (TCP, UDP) and Net

- work layer has only one protocol (IP) which forms the hourglass shape.

Q5. Can the Internet provide guarantees for message delivery and bandwidth? Provide reasons for your answer [hint: you may compare/contrast your answer with the telephone network]

Ans = NO, internet does not provide guarantees for message delivery and bandwidth.

for example in telephone network. we try to establish the connection with the recipient before sending message if the recipient does not pick the call connection is not established, if he picks the call then connection is established and bandwidth is allocated for communication. All the data being exchanged is transmitted to both parties until the connection is disrupted. in case of disruption transmission stops. so after connection bandwidth is guaranteed but messages could get lost due to interruptions.

Q6. A. How were the original Internet requirements met through its design?

B. What are the two main requirements that you see missing from the original design that are much needed today?

Ans-6 =

(A)= while development of internet some goals were underlined -

(1)= Scalability and economic access can be achieved by resource sharing, reducing number of reservations and allowing to utilize it to maximum.

(2)= Robustness = failures could be corrected by rerouting in the same path to ensure proper message delivery By using dynamic routing and establishing stateless connections. robustness could be ensured.

(3)= Reliability = By making an account of acknowledgement, and timely retransmission of distorted packets.

(4) = Evolvability = By reducing the complexity of the network and push

the main functionality at the ends to give space for further growth.

(B) = Security & mobility are the important goals which were missing from the initial design phases. But nowdays they are very important for internet work.

Q7. How does the Internet scale its routing tables?

Ans. 7 = To make overall network simple which in current scenario is huge and complex.

→ The end systems first connect to internet through ISP's (Internet Service Provider)

→ all ISPs are interconnected using IXPs (internet exchange Points) so that any host can send data to each other.

→ The network providers are classified into tier based on their usage.

→ Mostly accessed ones are kept in tier 1 and less frequently visited ones are first connected to regional ISPs which in turn is connected tier 1 ISP.

So based on the type of system joining it is put into an appropriate category and internet scaler accordingly by adding new systems to the network.

Q8. A. What is statistical multiplexing and what is the value it provides over TDM? Give example with numbers to support your argument(s).

B. What is the main disadvantage of statistical multiplexing?

Ans.b = Statistical multiplexing is a kind of communication link. like Dynamic bandwidth allocation. It is also called asynchronous TDM. A communication channel is devided into several digital channels Band on the traffic demand. The link sharing is adapted as necessary. whereas in TDM a fixed sharing of link is created.

Statistical multiplexing ensures that there are no slots that are wasted whereas in TDM slots might get wasted.

(B)= In use cases where dedicated Bandwidth is required statistical multiplexing is not efficient. for example radio and T.V. transmission, data packets are sent continously and hence fixed Bandwidth is required.

Q9. In slide 1-71 of chapter 1 discussed in class, explain the probability of '0.0004' when 35 users are active.

Ans.9 = Packet Switching with 1mbps link.

10% chance = user active.

with 35 users, probability that there will be more than 10 active users at the same time is less than 0.0004. This could be obtained using binomial distribution.

Overall Probability =

$$\sum_{K=11}^{35} {}^{35}C_K (0.1)^K (0.9)^{35-K}$$

Q10. A. What is a DDoS attack? And why is it harder to control than a DoS attack?

Ans-10 = DDOS attack is "Distributed denial of service attack". this type of attack can make any server or network resource unavailable to the users by puting heavy burden on the service by sending very large number of service requests to the server than it can actually handle.

DDOS attack uses more than one computer and Ip address distributed worldwide to put heavy burden and traffic on service. However DOS attack uses only one computer and Ip address. Hence in case of DOS attack when traffic spike is detected, the single computer source can be blocked and the attack could be contained. while in case of DDOS attack since there are multiple attack computer sources & Ip addresses involved It is hard to contain DDOS attack.

Q11. [Extra:] What is the first Internet worm, and how did it harm the Internet? [hint: Watch video link posted on canvas]

Ans.11 = In November, 1988 a malicious program spread over internet affecting more than 10% of all computers connected to internet. It is also called Morris worm because it was written by a cornell univer-sity graduate student named Robert tappan Morris.

This worm affected computers worldwide by overloading them with unknown processes which made computers really slow. It worked by exploiting the vulnerabilities in sendmail, finger and rsh/exec. apparently that worm spread very fast over internet and caused damages estimated to be 100,000$ or more.

This worm exposed internet security risks after one year of invention of internet.

Q12. A. Why is UDP preferred over TCP for IP-telephony/VoIP (like Skype)?

B. Why would Skype sometimes use TCP? Give two reasons.

Ans.12 = Ip-telephony | voip is a form of advanced telephony that allows organizations to use internet for making calls without using landline networks. VOIP uses internet for audio/video transmission.

Since VOIP uses Ip networks for communication Hence TCP | UDP protocols come into picture.

TCP protocol focuses on accurate delivery of all data packets during transmission also this protocol ensures that all packets arrive in order. it ensures no data loss. But it also means that data transmission is delayed.

UDP connections prioritize keeping stream of data going, it has to ensure that the receiving party gets the data packet on time. these characteristics make it ideal for connections that require real time exchange of data.

Therefore UDP is perfect for real time voice calls or VOIP.

(b) = Skype user both types of protocols Tcp and Udp.

Tcp is used for following reasons =

① = Skype for business will use Tcp to transfer the IM, emoji and pictures Since this data packets need high data integrity, if there is any loss then IM, emoji and pictures sent wont be identified. Since data accuracy is important in these cases Tcp protocol is used.

② = Skype sends Audio & video signals using Udp. But it uses Tcp to initiate connections or to Bypass some firewalls that block Udp packets.

Q13. Would an application that needs congestion control ever use UDP? Give two examples to support your argument.

Ans.13 = any application that needs congestion control uses Tcp protocol, Udp is not used because Tcp has a congestion control mechanism on the other hand Udp does not have any congestion control mechanism.

Example.1 = Tcp congestion avoidance algorithm is the primary basis for congestion control in the internet.

Example.2 = Tcp congestion control is also used in data center networks.

Tcp provides several variants of congestion avoidance algorithms to handle different types of congestion problems in different applications. while in Udp there is no support for congestion control.

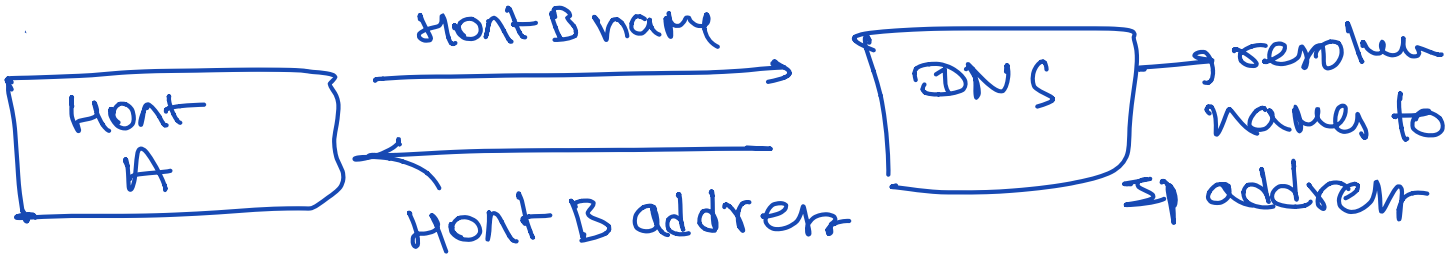
Q14. What are the identifiers needed for process communication across the network? Give example of a connection between two hosts. You can use a simple drawing to aid your answer.

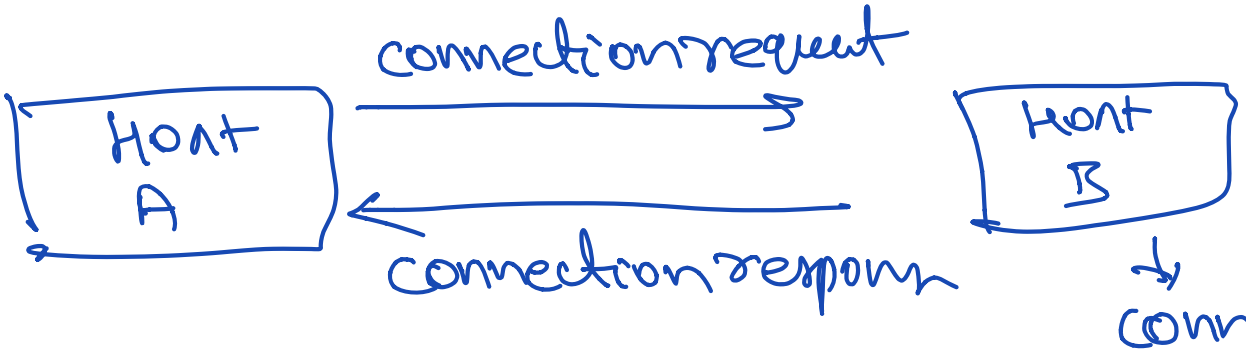
Ans.14 = for a proper communication to happen each process should have a unique identifier.

Identifiers needed =

① = IP address and port number to which connection must be established

② = The networks can also identified by their names using domain name servers (DNS)





→ connected to Host B using IP address.

Q15. Someone suggested that 'HTTP' is a stateful protocol. Argue for or against this statement.

Ans:15 = HTTP is a stateless protocol. It is not a stateful protocol.

All the web applications are also stateless. when a request is sent to the server a connection is established between client and server the server receiver the request, process it and sends the response and then connection is closed.

if any other request is sent then it is treated as a new request and a new connection is established.

Hence Http protocol doesnt preserve state Hence it is stateless.

However Http could be make to look like stateful using session management techniques like cookies, hidden form field, session etc. by using data coming from previous requests it can use same connection for a series of client server interactions.

Q16. How do web caches/proxy servers help Internet performance? Explain its benefits from the user and network perspectives. [hint: explain using your understanding of elementary queueing theory and delays, and use graphs as needed]

Ans-16 = Due to rise in popularity of the web the internet has grown in both voguep size which can result in more network load and unacceptable service response time these are the reasons why web users are suffering from network congestion and server overloading.

web caches / proxy servers can help improve the problems in the infrastructure —

① = Since cache is naturally much nearer to the client than the provider of the content it helps in reducing the latency of the user to obtain web data.

② = Since web data (web pages) are served from cache has to traverse less network compared to when they are served by provider directly, this reduces traffic of network.

③ = cache reduce the number of requests on the content providers.

(4) = caches reduces bandwidth consumption therefore it decreases network traffic and network congestion.

(5) = In case of remote server failure, client can obtain a cached copy at the proxy Hence robustness of web service is enhanced.

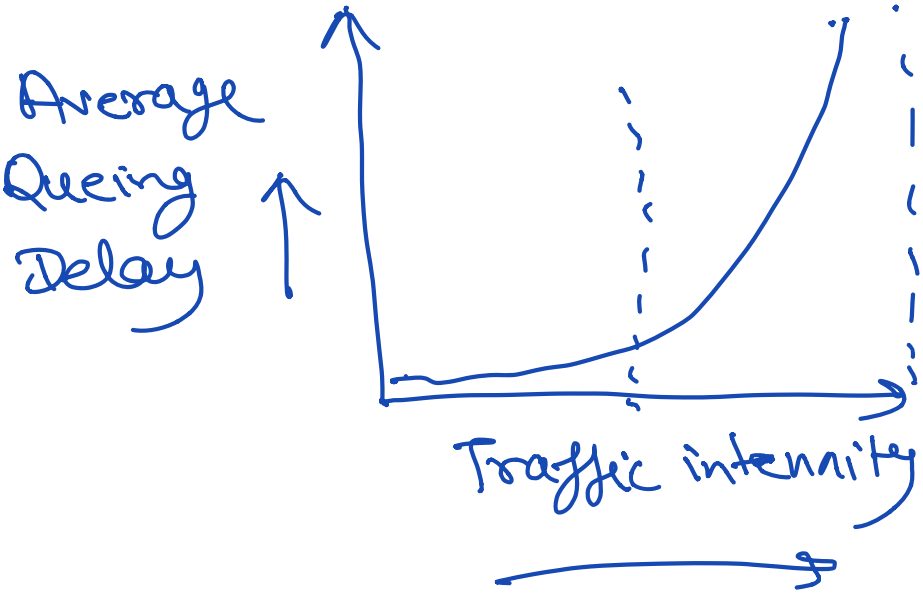
Proxy Servers = A proxy server is an intermediate server between end user and web applications hosted on provider servers. Proxy server acts as firewall & web filter, provide share network connections and cache data to speed up common requests.

(1) = To control and monitor internet usage of employees & children.

(2) = Proxy servers saves bandwidth and improve speeds by caching web data

(3) = proxy servers help improve privacy over internet.

(4) = They increase security.


Average
Queing
Delay
Traffic intensity

Q17. What is the effect of customized content, video streaming and encrypted traffic (e.g., HTTPS) on proxy caching?

Ans.17 =

Q18. A. When is peer-to-peer (p2p) network architecture needed or preferred?

B. What is the main problem in the p2p design?

C. Suggest a solution to the problem in B above.

Ans. 18 =

(A)= The primary goal for peer to peer network is to share resources and help devices work collaboratively. it refers to computer networks using a distributed architecture. It is used to share all kinds of computing resources such as processing power, network bandwidth, disk space etc. P2P networks are preffered for file sharing on the internet, it is ideal for file sharing because it allows the computers connected to receive & send files simultaneously.

(B)= A key problem with P2P networks is security. because of its decentralized nature, there is lack of central administration and control. which is required to combat security attacks. Since P2P systems inherently rely on the dependence of peers with each other

security implications arise from abuse of trust between peers, In a traditional client-server model, internal data need not be exposed to the client but with P2P, internal data might get exposed to fellow peers to distribute the workloa -d hence attackers can utilize this for attacker.

(C) = To address security issues with the P2P networks there are two approaches to secure it =

① = Encrypting P2P traffic = with the encrypted P2P traffic, P2P data stream will be encrypted and wont be easily detectable. which can make P2P traffic secure from attacks and blocks.

② = Anonymous P2P = By anonymizing peers P2P network can Protect identity of nodes and users on the

network, which cant be done by just using encryption.

Q19. Use '*traceroute*' and '*ping*' commands/tools to measure and analyze delays in the Internet:

A. Use *traceroute* to measure delays between your location and an overseas location (e.g., www.eurecom.fr). Show the trace and annotate it showing the transoceanic link.

B. Identify machines/routers along the way with:

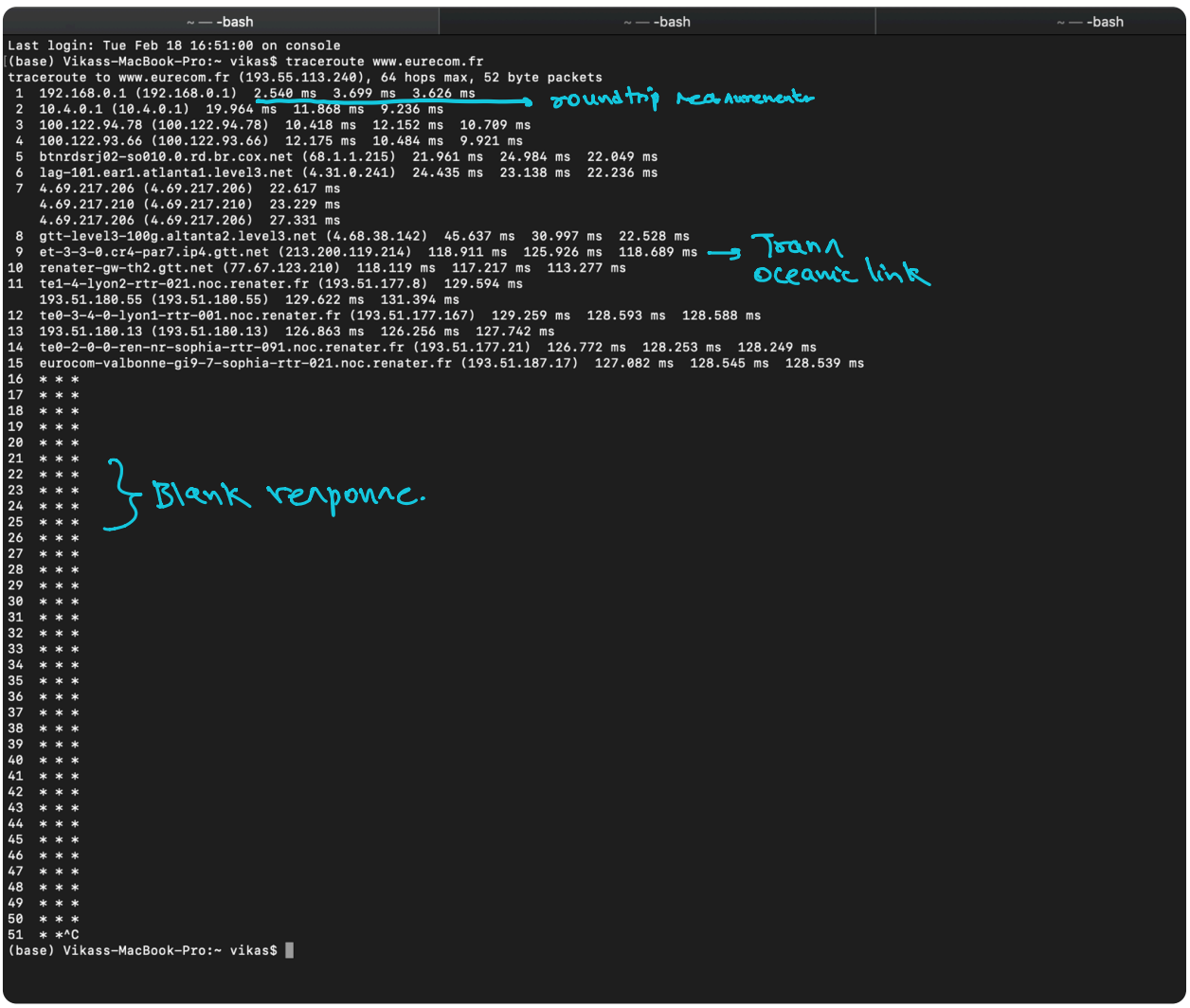
1. less than1ms delay, 2. 2–10ms delay, 3. 11–100ms delay, more than 100ms delay

then *ping* those machines for 15seconds each and analyze their delays

C. Identify the locations of the machines and reason about the differences in delays

[hints: look at the traceroute example in the lecture/book and perform something similar. *traceroute* is called *tracert* on windows. On some machines you need to be super user (sudo) to run traceroute. You may run the commands from your machine or from a UF machine (e.g., storm.cise.ufl.edu), so try and see what works for you.]

Ans-19 =



(B) = 2- 10 ms delay.

```
~ — -bash
[(base) Vikass-MacBook-Pro:~ vikas$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=64 time=3.898 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=9.592 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=10.004 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=3.561 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=9.550 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=3.820 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=3.711 ms
64 bytes from 192.168.0.1: icmp_seq=7 ttl=64 time=9.766 ms
64 bytes from 192.168.0.1: icmp_seq=8 ttl=64 time=11.824 ms
64 bytes from 192.168.0.1: icmp_seq=9 ttl=64 time=10.577 ms
64 bytes from 192.168.0.1: icmp_seq=10 ttl=64 time=4.323 ms
64 bytes from 192.168.0.1: icmp_seq=11 ttl=64 time=3.885 ms
64 bytes from 192.168.0.1: icmp_seq=12 ttl=64 time=9.887 ms
64 bytes from 192.168.0.1: icmp_seq=13 ttl=64 time=8.849 ms
64 bytes from 192.168.0.1: icmp_seq=14 ttl=64 time=10.215 ms
^C
--- 192.168.0.1 ping statistics ---
15 packets transmitted, 15 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 3.561/7.564/11.824/3.082 ms
(base) Vikass-MacBook-Pro:~ vikas$
```

Average round trip = 7.564 ms

11-100 ms delay.

```
~ — -bash
Last login: Tue Feb 18 21:20:37 on ttys001
[(base) Vikass-MacBook-Pro:~ vikas$ ping 10.4.0.1
PING 10.4.0.1 (10.4.0.1): 56 data bytes
64 bytes from 10.4.0.1: icmp_seq=0 ttl=254 time=39.769 ms
64 bytes from 10.4.0.1: icmp_seq=1 ttl=254 time=55.667 ms
64 bytes from 10.4.0.1: icmp_seq=2 ttl=254 time=106.366 ms
64 bytes from 10.4.0.1: icmp_seq=3 ttl=254 time=10.194 ms
64 bytes from 10.4.0.1: icmp_seq=4 ttl=254 time=9.072 ms
64 bytes from 10.4.0.1: icmp_seq=5 ttl=254 time=15.006 ms
64 bytes from 10.4.0.1: icmp_seq=6 ttl=254 time=9.292 ms
64 bytes from 10.4.0.1: icmp_seq=7 ttl=254 time=15.388 ms
64 bytes from 10.4.0.1: icmp_seq=8 ttl=254 time=14.983 ms
64 bytes from 10.4.0.1: icmp_seq=9 ttl=254 time=14.255 ms
64 bytes from 10.4.0.1: icmp_seq=10 ttl=254 time=15.103 ms
64 bytes from 10.4.0.1: icmp_seq=11 ttl=254 time=8.801 ms
64 bytes from 10.4.0.1: icmp_seq=12 ttl=254 time=14.530 ms
64 bytes from 10.4.0.1: icmp_seq=13 ttl=254 time=11.518 ms
64 bytes from 10.4.0.1: icmp_seq=14 ttl=254 time=15.145 ms
^C
--- 10.4.0.1 ping statistics ---
15 packets transmitted, 15 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 8.801/23.673/106.366/25.337 ms
(base) Vikass-MacBook-Pro:~ vikas$
```

avg round trip time = 23.673

11-100 MS delay

```
~ — -bash
[(base) Vikass-MacBook-Pro:~ vikas$ ping 100.122.94.78
PING 100.122.94.78 (100.122.94.78): 56 data bytes
64 bytes from 100.122.94.78: icmp_seq=0 ttl=253 time=15.180 ms
64 bytes from 100.122.94.78: icmp_seq=1 ttl=253 time=16.284 ms
64 bytes from 100.122.94.78: icmp_seq=2 ttl=253 time=10.197 ms
64 bytes from 100.122.94.78: icmp_seq=3 ttl=253 time=9.559 ms
64 bytes from 100.122.94.78: icmp_seq=4 ttl=253 time=13.688 ms
64 bytes from 100.122.94.78: icmp_seq=5 ttl=253 time=17.810 ms
64 bytes from 100.122.94.78: icmp_seq=6 ttl=253 time=15.264 ms
64 bytes from 100.122.94.78: icmp_seq=7 ttl=253 time=15.747 ms
64 bytes from 100.122.94.78: icmp_seq=8 ttl=253 time=14.318 ms
64 bytes from 100.122.94.78: icmp_seq=9 ttl=253 time=9.871 ms
64 bytes from 100.122.94.78: icmp_seq=10 ttl=253 time=15.207 ms
64 bytes from 100.122.94.78: icmp_seq=11 ttl=253 time=15.237 ms
64 bytes from 100.122.94.78: icmp_seq=12 ttl=253 time=16.229 ms
64 bytes from 100.122.94.78: icmp_seq=13 ttl=253 time=10.984 ms
64 bytes from 100.122.94.78: icmp_seq=14 ttl=253 time=16.332 ms
^C
--- 100.122.94.78 ping statistics ---
15 packets transmitted, 15 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 9.559/14.127/17.810/2.575 ms
(base) Vikass-MacBook-Pro:~ vikas$
```

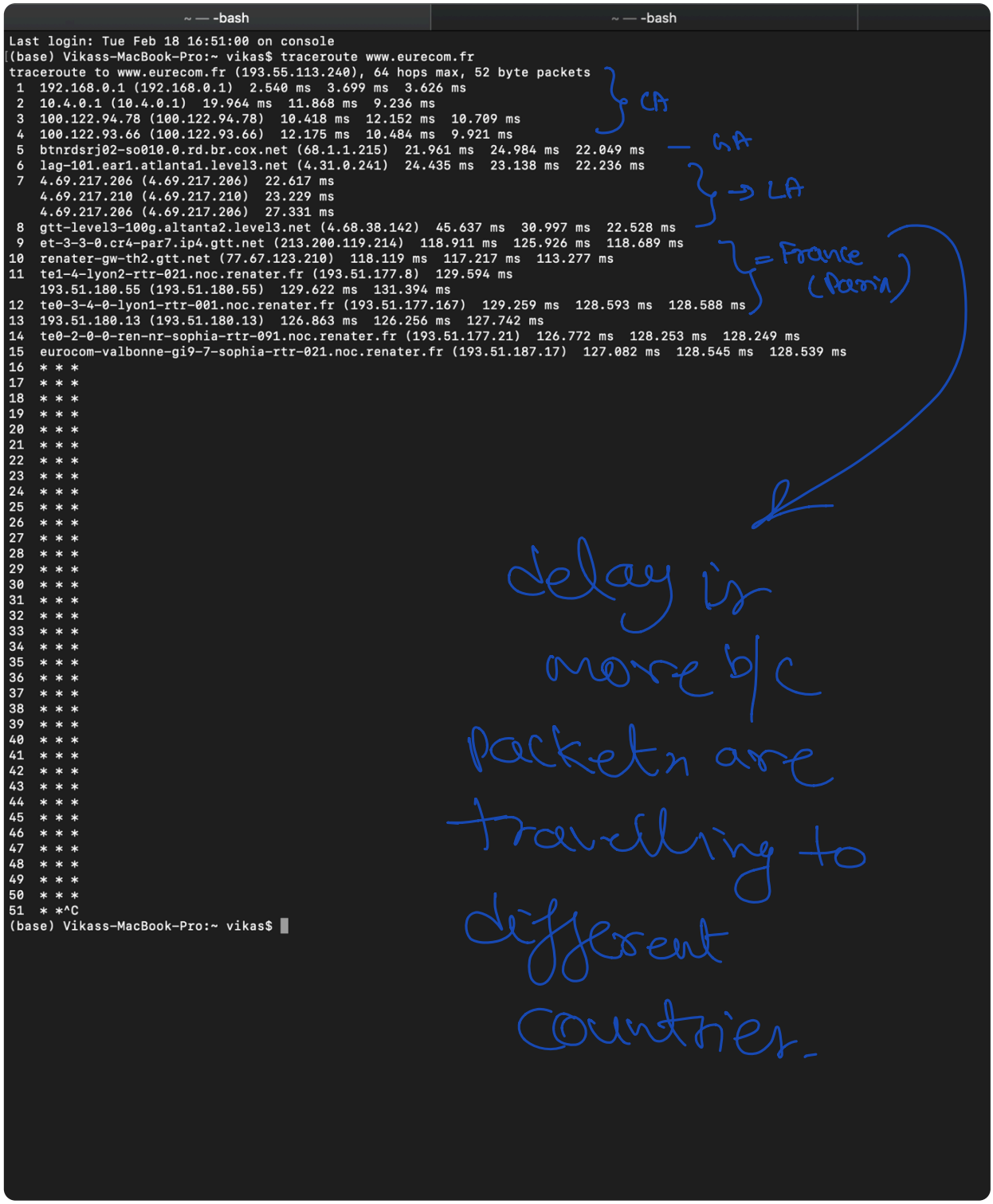
avg roundtrip time = 14.127

>100MS delay

```
~ — -bash
[(base) Vikass-MacBook-Pro:~ vikas$ ping 213.200.119.214
PING 213.200.119.214 (213.200.119.214): 56 data bytes
64 bytes from 213.200.119.214: icmp_seq=0 ttl=50 time=193.632 ms
Request timeout for icmp_seq 1
64 bytes from 213.200.119.214: icmp_seq=2 ttl=50 time=125.221 ms
64 bytes from 213.200.119.214: icmp_seq=3 ttl=50 time=119.582 ms
64 bytes from 213.200.119.214: icmp_seq=4 ttl=50 time=126.878 ms
64 bytes from 213.200.119.214: icmp_seq=5 ttl=50 time=126.583 ms
64 bytes from 213.200.119.214: icmp_seq=6 ttl=50 time=125.132 ms
64 bytes from 213.200.119.214: icmp_seq=7 ttl=50 time=123.491 ms
64 bytes from 213.200.119.214: icmp_seq=8 ttl=50 time=124.181 ms
64 bytes from 213.200.119.214: icmp_seq=9 ttl=50 time=124.669 ms
64 bytes from 213.200.119.214: icmp_seq=10 ttl=50 time=125.250 ms
64 bytes from 213.200.119.214: icmp_seq=11 ttl=50 time=138.724 ms
64 bytes from 213.200.119.214: icmp_seq=12 ttl=50 time=124.200 ms
64 bytes from 213.200.119.214: icmp_seq=13 ttl=50 time=117.879 ms
64 bytes from 213.200.119.214: icmp_seq=14 ttl=50 time=125.167 ms
64 bytes from 213.200.119.214: icmp_seq=15 ttl=50 time=123.990 ms
64 bytes from 213.200.119.214: icmp_seq=16 ttl=50 time=124.427 ms
64 bytes from 213.200.119.214: icmp_seq=17 ttl=50 time=119.576 ms
64 bytes from 213.200.119.214: icmp_seq=18 ttl=50 time=123.698 ms
^C
--- 213.200.119.214 ping statistics ---
19 packets transmitted, 18 packets received, 5.3% packet loss
round-trip min/avg/max/stddev = 117.879/128.460/193.632/16.339 ms
(base) Vikass-MacBook-Pro:~ vikas$
```

avg round trip = 128.460 ms

(Trans Oceanic link)


~ — -bash
~ — -bash
Last login: Tue Feb 18 16:51:00 on console
(base) Vikass-MacBook-Pro:~ vikas$ traceroute www.eurecom.fr
traceroute to www.eurecom.fr (193.55.113.240), 64 hops max, 52 byte packets
1 192.168.0.1 (192.168.0.1) 2.540 ms 3.699 ms 3.626 ms
2 10.4.0.1 (10.4.0.1) 19.964 ms 11.868 ms 9.236 ms
3 100.122.94.78 (100.122.94.78) 10.418 ms 12.152 ms 10.709 ms
4 100.122.93.66 (100.122.93.66) 12.175 ms 10.484 ms 9.921 ms
5 btnrdsrj02-so010.0.rd.br.cox.net (68.1.1.215) 21.961 ms 24.984 ms 22.049 ms
6 lag-101.ear1.atlanta1.level3.net (4.31.0.241) 24.435 ms 23.138 ms 22.236 ms
7 4.69.217.206 (4.69.217.206) 22.617 ms
4.69.217.210 (4.69.217.210) 23.229 ms
4.69.217.206 (4.69.217.206) 27.331 ms
8 gtt-level3-100g.altanta2.level3.net (4.68.38.142) 45.637 ms 30.997 ms 22.528 ms
9 et-3-3-0.cr4-par7.ip4.gtt.net (213.200.119.214) 118.911 ms 125.926 ms 118.689 ms
10 renater-gw-th2.gtt.net (77.67.123.210) 118.119 ms 117.217 ms 113.277 ms
11 te1-4-lyon2-rtr-021.noc.renater.fr (193.51.177.8) 129.594 ms
193.51.180.55 (193.51.180.55) 129.622 ms 131.394 ms
12 te0-3-4-0-lyon1-rtr-001.noc.renater.fr (193.51.177.167) 129.259 ms 128.593 ms 128.588 ms
13 193.51.180.13 (193.51.180.13) 126.863 ms 126.256 ms 127.742 ms
14 te0-2-0-0-ren-nr-sophia-rtr-091.noc.renater.fr (193.51.177.21) 126.772 ms 128.253 ms 128.249 ms
15 eurocom-valbonne-gi9-7-sophia-rtr-021.noc.renater.fr (193.51.187.17) 127.082 ms 128.545 ms 128.539 ms
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
31 * * *
32 * * *
33 * * *
34 * * *
35 * * *
36 * * *
37 * * *
38 * * *
39 * * *
40 * * *
41 * * *
42 * * *
43 * * *
44 * * *
45 * * *
46 * * *
47 * * *
48 * * *
49 * * *
50 * * *
51 * *^C
(base) Vikass-MacBook-Pro:~ vikas$
CA
GA
LA
France
(Paris)
delay is more b/c packets are travelling to different countries.

Q20. Visit the wireshark website at wireshark.org, read the user's manual (
https://www.wireshark.org/docs/wsug_html_chunked/), then answer these questions:

A. What is wireshark?

B. What are some of intended purposes? (mention four)

C. What are two unintended purposes?

[hints: install wireshark and start using it to prepare for future hwks. Read intro posted on canvas.]

Ans.20 =

(A)= wireshark is the network traffic analyzer. it is an essential tool to analyze network traffic in real time and troubleshoot issues on the network. wireshark is free and open source. A network packet analyzer presents captured packet data in as much detail as possible.

(B)= Intended Purposes =

① = Network administrators use it to troubleshoot network problems.

② = Network security engineers use it to examine security problems.

③ = QA engineers use it to verify network applications.

④ = Developers use it to debug protocol implementations.

(c) = unintended Purpose =

(1) = wireshark is not a intrusion detection system. it does not warn unusual activity on the network. rather it could be used to figure out the problem.

(2) = wireshark does not manipulate things on the network. it only measures the activity.