Homework 1 – Part 2: Internet Architecture & Application Layer

Q1 .

A. Application layer: What are the main network application architectures in the Internet? (mention 3)

Client-server architecture, peer-to-peer architecture, hybrid of client-server and P2P

B. What are the processes are needed to support all the above architectures? Explain which process is used in which architecture and how.

Client and server.

In the client-server architecture, client initiates the communication, server waits to be contacted to begin the session.

In P2P architecture, the same host can be both client and server.

Q2. What are the advantages and disadvantages of:

A. Hierarchical network architectures (mention 3 advantages and 2 disadvantages)

Advantages:

1. Isolates and scopes internal dynamics: dampens oscillations, providing stability to the overall network
2. Supports scalability: aggregation/summary per domain for smaller, more efficient routing tables
3. Allows for flexibility: domains deploy different protocols, policies …

Disadvantages:

1. Overhead of establishing and maintaining the hierarchy (esp. for mobile, dynamic nets)
2. Sub-optimality of routing …

B. Protocol layering (mention at least 2 advantages and 2 disadvantages)

Advantages:

1. Explicit structure allows identification, relationship of complex system's pieces
2. Modularization eases maintenance, updating of system

Disadvantages:

1. One layer may duplicate lower-layer functionality
2. Functionality at one layer may need information that is present only in another layer; this violates the goal of separation of layers.

C. Stateless protocols (mention at least 2 advantages and 2 disadvantages)

Advantages:

1. simplify server design
2. require less resources

Disadvantages:

1. cannot identify users
2. Need to build new TCP connection for every object requested from the same client to the same sever.

Q3. A. How were the original Internet requirements met through its design? (mention 4)

Scalability and economic access; Robustness; reliability; Evolvability

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

Q4. In slide 1-71 of chapter 1 discussed in class, explain the probability of '0.0004' when 35 users are active.
When 35 users are active, the probability that there are 11 or more simultaneously active users is approximately 0.0004, according to the central limit theorem.

Q5. A. What is a DDoS attack?
Distributed denial-of-service attack

B. why is it harder to control than a DoS attack?
The attacker controls multiple sources and has each source blast traffic at the target and leverage botnets with thousands of comprised hosts, which make DDos attacks are much harder to detect and defend against than a DoS attack from a single host.

Q6. What is the first Internet worm, and how did it harm the Internet? [hint: Watch video link posted on canvas]
The Morris worm, created by Robert Tappan Morris.
Functioned as a DoS attack, and the worm made about 6000 limited computers connected to the internet and depleted their computing resources, resulted these computers shut down.

Q7. A. Why is UDP preferred over TCP for IP-telephony/VoIP (like Skype)?
IP-telephony/VoIP are more sensitive to delay, and TCP needs connection which add delays. As a result, UDP provides a better experience for VoIP users as it allows them to enjoy a real-time and uninterrupted call without any delay

B. Why would Skype sometimes use TCP? Give two reasons.
Use congestion control mechanism of TCP; use TCP as a backup if UDP communication fails; Skype use TCP to build connection for a real-audio call.

Q8. Would an application that needs congestion control ever use UDP? Give two examples to support your argument.
Yes.
Like Skype and video streaming they need to transfer information quickly and can tolerate some loss, they will use UDP and need congestion control to make sure the bandwidth.

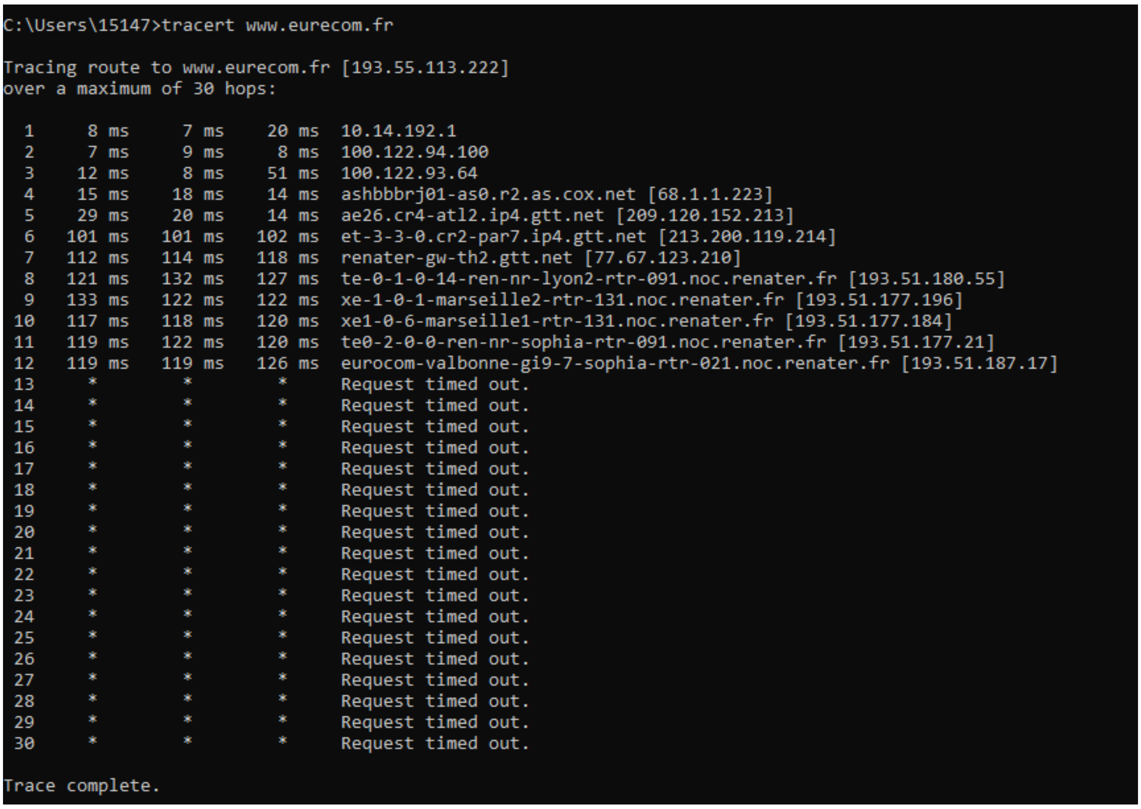
Q9. How do web caches/proxy servers help Internet performance? Explain and list 3 of its benefits from the user and network perspectives. [hint: explain using your understanding of elementary queueing theory and delays, and use graphs as needed]

1. The client doesn't need to request to the server every time, it can get the object if there is one in

the web cache, thus reduce response time

2. Since there is web cache and 0.2-0.7 possibility that the objects requested from client may exist in web cache, then the data rate to browser over the access link can be reduced and the traffic intensity also goes down
3. Users can communicate indirectly through third-party (web caches)

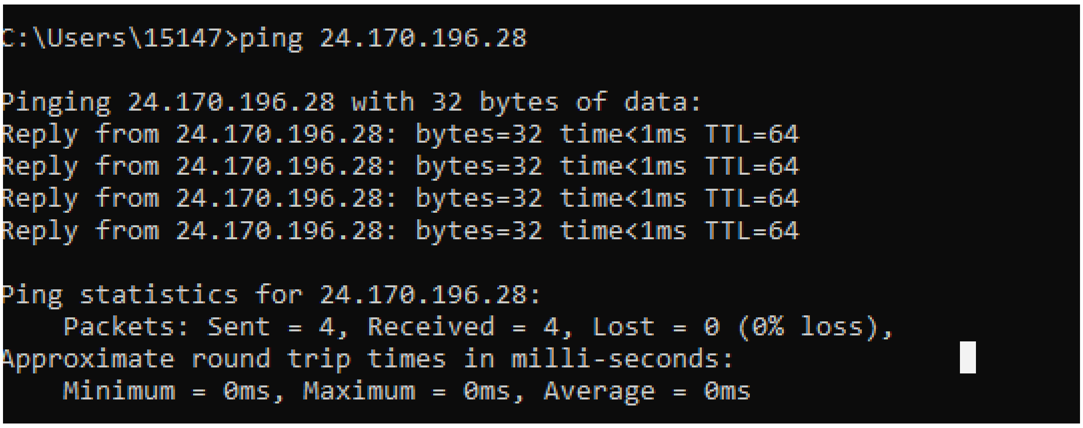
Q10. Use 'traceroute' and 'ping' commands/tools to measure and analyze delays in the Internet:
A. Use traceroute to measure delays between your location and an overseas location (e.g., www.eurecom.fr). Show the trace and annotate it showing the transoceanic link.



```
C:\Users\15147>tracert www.eurecom.fr

Tracing route to www.eurecom.fr [193.55.113.222]
over a maximum of 30 hops:

  1     8 ms     7 ms    20 ms  10.14.192.1
  2     7 ms     9 ms     8 ms  100.122.94.100
  3    12 ms     8 ms    51 ms  100.122.93.64
  4    15 ms    18 ms    14 ms  ashbbbrj01-as0.r2.as.cox.net [68.1.1.223]
  5    29 ms    20 ms    14 ms  ae26.cr4-atl2.ip4.gtt.net [209.120.152.213]
  6   101 ms   101 ms   102 ms  et-3-3-0.cr2-par7.ip4.gtt.net [213.200.119.214]
  7   112 ms   114 ms   118 ms  renater-gw-th2.gtt.net [77.67.123.210]
  8   121 ms   132 ms   127 ms  te-0-1-0-14-ren-nr-lyon2-rtr-091.noc.renater.fr [193.51.180.55]
  9   133 ms   122 ms   122 ms  xe-1-0-1-marseille2-rtr-131.noc.renater.fr [193.51.177.196]
 10   117 ms   118 ms   120 ms  xe1-0-6-marseille1-rtr-131.noc.renater.fr [193.51.177.184]
 11   119 ms   122 ms   120 ms  te0-2-0-0-ren-nr-sophia-rtr-091.noc.renater.fr [193.51.177.21]
 12   119 ms   119 ms   126 ms  eurocom-valbonne-gi9-7-sophia-rtr-021.noc.renater.fr [193.51.187.17]
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

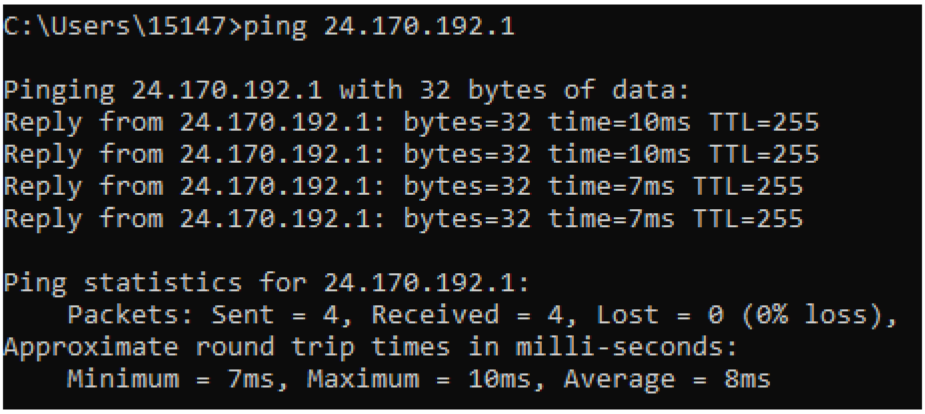
B. Identify machines/routers along the way with: 1. less than1ms delay, 2. 2–10ms delay, 3. 11–100ms delay, more than 100ms delay then ping those machines for 15seconds each and analyze their delays

Less than 1ms delay: (localhost)



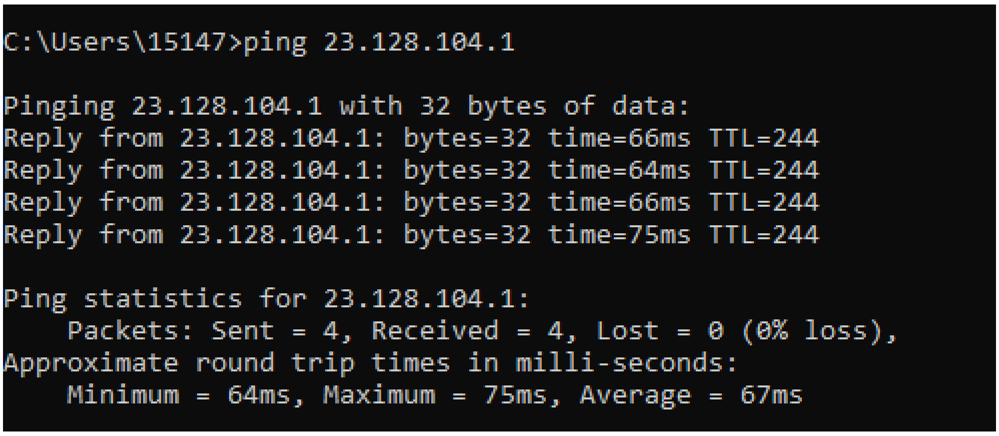
```
C:\Users\15147>ping 24.170.196.28

Pinging 24.170.196.28 with 32 bytes of data:
Reply from 24.170.196.28: bytes=32 time<1ms TTL=64
Reply from 24.170.196.28: bytes=32 time<1ms TTL=64
Reply from 24.170.196.28: bytes=32 time<1ms TTL=64
Reply from 24.170.196.28: bytes=32 time<1ms TTL=64

Ping statistics for 24.170.196.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2-10ms delay: (Gainesville)



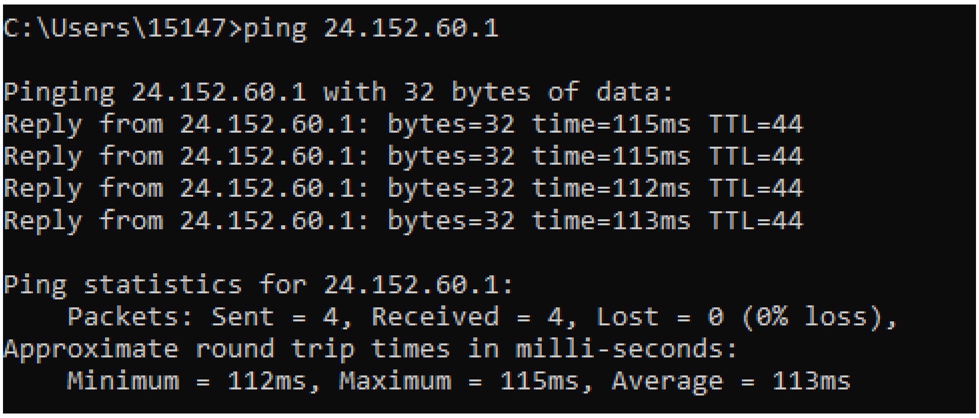
```
C:\Users\15147>ping 24.170.192.1

Pinging 24.170.192.1 with 32 bytes of data:
Reply from 24.170.192.1: bytes=32 time=10ms TTL=255
Reply from 24.170.192.1: bytes=32 time=10ms TTL=255
Reply from 24.170.192.1: bytes=32 time=7ms TTL=255
Reply from 24.170.192.1: bytes=32 time=7ms TTL=255

Ping statistics for 24.170.192.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 10ms, Average = 8ms
```

11-100ms delay: (same country)



```
C:\Users\15147>ping 23.128.104.1

Pinging 23.128.104.1 with 32 bytes of data:
Reply from 23.128.104.1: bytes=32 time=66ms TTL=244
Reply from 23.128.104.1: bytes=32 time=64ms TTL=244
Reply from 23.128.104.1: bytes=32 time=66ms TTL=244
Reply from 23.128.104.1: bytes=32 time=75ms TTL=244

Ping statistics for 23.128.104.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 64ms, Maximum = 75ms, Average = 67ms
```

More than 100ms: (Brazil)



```
C:\Users\15147>ping 24.152.60.1

Pinging 24.152.60.1 with 32 bytes of data:
Reply from 24.152.60.1: bytes=32 time=115ms TTL=44
Reply from 24.152.60.1: bytes=32 time=115ms TTL=44
Reply from 24.152.60.1: bytes=32 time=112ms TTL=44
Reply from 24.152.60.1: bytes=32 time=113ms TTL=44

Ping statistics for 24.152.60.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 112ms, Maximum = 115ms, Average = 113ms
```

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

The location that have the delay of less than 1ms should be in the same apartment or yourself; less than 10ms should be in the same state or city; less than 100ms should be in the same country and more than 100ms should be in the different continent.

[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.]

Q11. 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?

Wireshark is a network packet analyzer which works as a measuring device for examining what's happening inside a network cable

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

Network administrators use it to troubleshoot network problems
Network security engineers use it to examine security problems
Developers use it to debug protocol implementations
People use it to learn network protocol internals

C. What are two unintended purposes?

Wireshark cannot change anything in the network.
Wireshark does not detect violations or interference in the network

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