**Cpre 530 - Assignment 1**

**1. Do homework problems 1 and 11 in Chapter 3 of the book.**

**Find one or two maps of the topology of the internet. Comment on their accuracy.**

* [http://www.pnas.org/content/104/27/11150.full](http://www.pnas.org/content/104/27/11150.full%20)

A model of internet topology using k shell decomposition. Good image at <http://cscis12.dce.harvard.edu/lecture_notes/2009/20090623/images/500px_internet_map_pnas2007.png>

The above topology is the outcome of the research in Boston University. Instead of node degree, “k-shell” decomposition is used to assign a shell index to each node in the Internet. Although node degrees can range from one or two up to several thousands, this procedure splits the network into 40–50 shells only, the precise number depending on the measurement details. This is a limitation. Agent population of the topology comes from over 90 countries. Over all, this is a very general topology but is useful when studying other complex networks.

* <http://www.mundi.net/maps/maps_020/>

The Internet is often likened to an organic entity and this analogy seems particularly appropriate in the light of some striking new visualizations of the complex mesh of Internet pathways. The images are results of a new graph visualization tool, code-named Walrus, being developed by researcher, Young Hyun, at the Cooperative Association for Internet Data Analysis (CAIDA) **[[1]](http://www.mundi.net/maps/maps_020/" \l "ref_1)**. Although Walrus is still in early days of development, I think these preliminary results are some of the most intriguing and evocative images of the Internet's structure that we have seen in last year or two.

<http://www.mundi.net/maps/maps_020/walrus.html>

The image above is a screengrab of a Walrus visualization of a huge graph. The graph data in this particular example depicts Internet topology, as measured by CAIDA's skitter monitor **[[3]](http://www.mundi.net/maps/maps_020/" \l "ref_3)** based in London, showing 535,000-odd Internet nodes and over 600,000 links. The nodes, represented by the yellow dots, are a large sample of computers from across the whole range of Internet addresses.

**Find IP Address of Root DNS Servers.**

|  |  |
| --- | --- |
| **The DNS Root Servers** | **IP Address** |
| A.ROOT-SERVERS.NET. | 198.41.0.4 |
| B.ROOT-SERVERS.NET. | 192.228.79.201 |
| C.ROOT-SERVERS.NET. | 192.33.4.12 |
| D.ROOT-SERVERS.NET. | 128.8.10.90 |
| E.ROOT-SERVERS.NET. | 192.203.230.10 |
| F.ROOT-SERVERS.NET. | 192.5.5.241 |
| G.ROOT-SERVERS.NET. | 192.112.36.4 |
| H.ROOT-SERVERS.NET. | 128.63.2.53 |
| I.ROOT-SERVERS.NET. | 192.36.148.17 |
| J.ROOT-SERVERS.NET. | 192.58.128.30 |
| K.ROOT-SERVERS.NET. | 193.0.14.129 |
| L.ROOT-SERVERS.NET. | 198.32.64.12 |
| M.ROOT-SERVERS.NET. | 202.12.27.33 |

**2. Do lab experiments 1-6 in Chapter 3**

* Develop a list of at least five web sites and five email servers that you think are geographically dispersed across the internet.

**List of websites:**

1. [www.google.com](http://www.google.com)
2. [www.twitter.com](http://www.twitter.com)
3. [www.wikipedia.org](http://www.wikipedia.org)
4. [www.microsoft.com](http://www.microsoft.com)
5. [www.facebook.com](http://www.facebook.com)

**List of Email servers:**

1. [www.gmail.com](http://www.gmail.com)
2. www.atmail.com
3. [www.rediff.com](http://www.rediff.com)
4. [www.Hotmail.com](http://www.Hotmail.com)
5. [www.mail.yahoo.com](http://www.mail.yahoo.com)

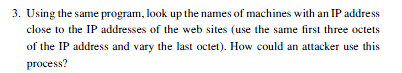
2. Using DNS, look up the IP addresses of each of the sites from experiment 1. For the email servers you will need to set the DNS query type to MX. See the main page for running the program.

IP addresses of websites:

1. 74.125.225.131
2. 199.59.149.230
3. 208.80.152.201
4. 65.55.58.201
5. 69.171.247.21

IP addresses of email servers:

1. 74.
2. 68.180.131.16
3. 213.155.153.132
4. 192.87.106.230
5. 65.54.188.110



a.The nslookup of google is

74.125.225.84 – www.l.google.com. In this case, the neighboring IP’s obtained by changing the last octet are not found.

b. If we change the last octet of an IP address in some case we get a different instance of the same site. For eg: the IP address for facebook.com is mentioned as 63.69.189.16, if we try 63.69.189.14 another instance opens up.

While using nslookup it returned the following:

63.69.189.16 name = www.11-01-ash2-facebook.com.

63.69.189.14 name = www.register-10-01-ash2.facebook.com.

c. Twitter - 199.59.149.198 – www2.twitter.com

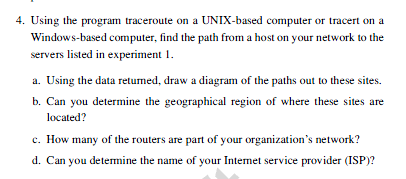
199.59.149.200 - r-199-59-149-200.twttr.com

d. Microsoft - 207.46.232.182 – windowsruby.ae. In this case too, the neighboring IP’s obtained by changing the last octet are not found.

e. Wikipedia - 208.80.152.2 - rr.pmtpa.wikimedia.org

208.80.152.3 - upload.pmtpa.wikimedia.org

Thus in most cases, another server/IP address belonging to that domain is exposed. The attacker can use this process to address spoof a vulnerable user.



My computer

129.186.182.194

129.186.183.254

129.186.254.131

192.245.179.52

164.113.232.225

64.57.21.253

137.164.130.150

72.14.236.178

209.85.250.30

74.125.225.80

129.186.183.254

129.186.254.131

[192.245.179.52]

4.53.34.13

4.69.135.233

12.122.131.165

4.69.135.230

4.69.151.153

4.69.145.140

4.68.62.34

Trace complete

152.63.97.57

Request timeout 19 times

129.186.254.131

192.245.179.52

164.113.232.225

64.57.21.253

137.164.130.174

129.186.254.131

192.245.179.52

64.57.21.253

164.113.232.225

206.223.119.27

64.125.26.253

64.125.26.141

64.125.26.202

64.125.30.178

199.59.149.198

209.66.115.6

199.16.159.51

129.186.183.254

207.46.35.146

Destination unreachable

4.53.34.13

4.69.135.233

4.69.135.230

4.69.151.153

Trace complete

Trace complete

207.46.35.134

207.46.46.11

207.46.47.70

207.46.43.163

207.46.40.94

207.46.40.217

Request timeout 11 times

129.186.183.254

129.186.254.131

192.245.179.52

4.71.0.14

4.69.133.62

4.69.133.41

4.69.137.117

4.69.151.150

208.80.152.222

208.80.152.222

84.40.25.102

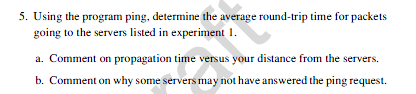
84.40.24.50

Trace complete

B: No geographical region of where these sites are located cannot be determined.

C: Three of them are part of iastate’s network. Their IP addresses are 129.186.183.254, 129.186.254.131 and 192.245.179.52

D: The name of Internet Service Provider cannot be determined.



Average round trip time for:

IP addresses of websites:

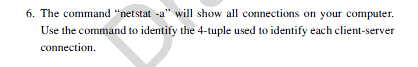
1. [www.google.com](http://www.google.com) – 15ms
2. [www.facebook.com](http://www.facebook.com) – 39ms
3. [www.twitter.com](http://www.twitter.com) – 61ms
4. [www.microsoft.com](http://www.microsoft.com) – 63ms
5. [www.wikipedia.org](http://www.wikipedia.org) – 55ms

IP addresses of email servers:

1. [www.gmail.com](http://www.gmail.com) – 15ms
2. [www.yahoomail.com](http://www.yahoomail.com) – 40ms
3. [www.rediff.com](http://www.rediff.com) – 1ms
4. James.apache.org – 51ms
5. Hotmail.com – 49ms

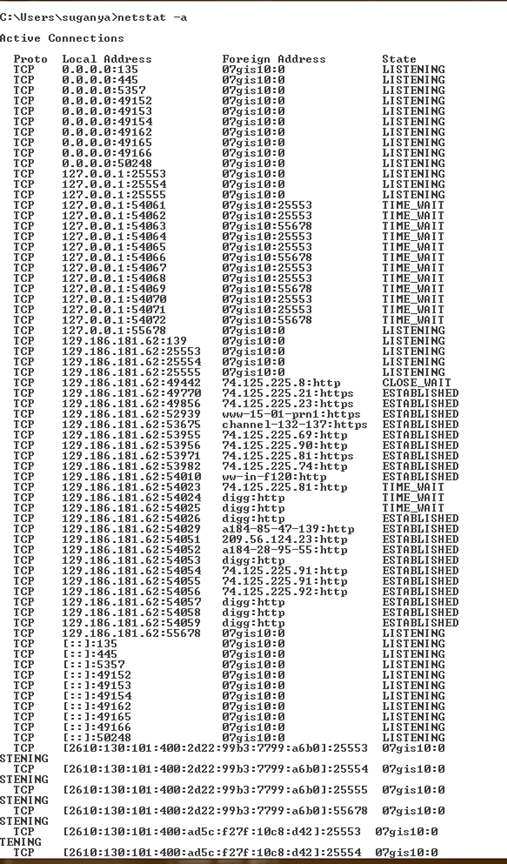
Propagation time: The propagation time is directly proportional to the geographical distance of the server.

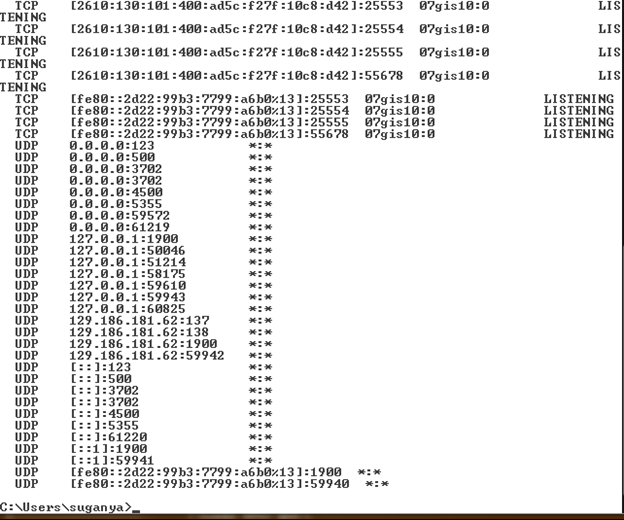
Ping request time out: The reason for the time out could be because there is no reply from the host, or the packet is lost on its way back.



“netstat –a” returns Protocol, Local Address, Foreign Address and State

Below is the list of those connections:





**Reference:**

1. <http://www.tech-faq.com/dns-root-servers.html>
2. <http://www.exclamationsoft.com/exclamationsoft/netmailbot/help/reference/find_mail_server.asp>