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

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 p nas2007.png

The above topology is the outcome of the research in Boston University. Instead of node degree, õk-shellö 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 40650 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]. 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] 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
- 2. www.twitter.com
- 3. www.wikipedia.org
- 4. www.microsoft.com
- 5. www.facebook.com

List of Email servers:

- 1. www.gmail.com
- 2. www.atmail.com
- 3. www.rediff.com
- 4. www.Hotmail.com
- 5. 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. 74.125.225.128
- 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. 74.125.225.150
- 2. 65.61.115.94
- 3. 204.93.46.65
- 4. 65.55.72.167
- 5. 98.139.237.162
- 3. Using the same program, look up the names of machines with an IP address close to the UP addresses of the web sites. How could an attacker use this process?
 - <u>www.google.com</u>: 74.125.225.128 ord08s09-in-f12.1e100.net 74.125.225.140
 - www.twitter.com: 199.59.149.230

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

• www.wikipedia.com: 208.80.152.201

www.toolserver.com: 208.80.152.230

• <u>www.microsoft.com</u> :65.55.58.201

bizspark.microsoft.com 65.55.58.202

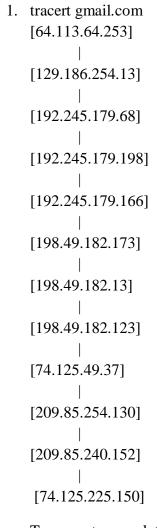
• <u>www.facebook.com</u>:69.171.247.21 orca-api-slb-10-03-frc1.facebook.com 69.171.247.30

Attacker could use this to spoof a user as domain is exposed.

4. Using the program traceroute on a UNIX-based computer or tracert on a windows basec computer, find the path from a host on your network to the servers listed in experiment1.

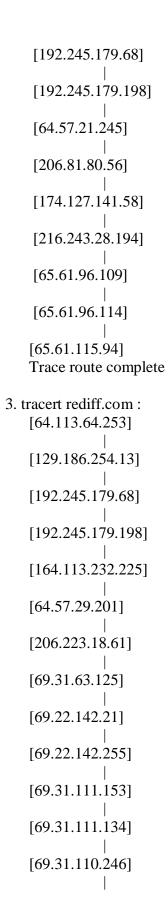
- a. Using the date returned, draw a diagram of the paths out to these sites.
- b. Can you determine the geographical region of where these sites are located?
- c. How many of the routers are part of your organization network?
- d. Can you determine the name of your ISP?

A.



Trace route complete

2. tracert atmail.com
[64.113.64.253]
|
[129.186.254.13



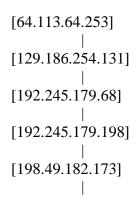
```
[204.93.46.65]
```

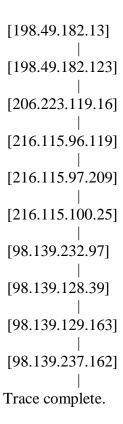
Trace route complete

4. tracert Hotmail.com

Trace complete

5. tracert mail.yahoo.com





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

C: Five of them are part of iastate¢s network. Their IP addresses are

- D: The name of Internet Service Provider cannot be determined.
- 5. Using the program ping, determine the average round trip time for packets going to the servers listed in experiment 1.
 - a. Comment on propagation time versus distance from the servers.
 - b. Comment on why some servers may not have answered the ping request

Average round trip time for:

IP addresses of websites:

- 1. www.google.com-18ms
- 2. www.twitter.com-80ms
- 3. www.wikipedia.org-87ms
- 4. www.microsoft.com-timed out
- 5. www.facebook.com-79ms

IP addresses of email servers:

- 1. www.gmail.com -19ms
- 2. www.atmail.com-timed out
- 3. www.rediff.com-61ms
- 4. www.hotmail.com-71ms
- 5. <u>www.mail.yahoo.com</u>-44ms

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.

6. The command onetstat oao will show all connections on your computer. Use the command to identify the 4-tuple used to identify each client-server connection.

õnetstat óaö returns Protocol, Local Address, Foreign Address and State

Below is the list of those connections:

Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\harish>netstat -a

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	harish-HP:0	LISTENING
TCP	0.0.0.0:445	harish-HP:0	LISTENING
TCP	0.0.0.0:554	harish-HP:0	LISTENING
TCP	0.0.0.0:1025	harish-HP:0	LISTENING
TCP	0.0.0.0:1026	harish-HP:0	LISTENING
TCP	0.0.0.0:1027	harish-HP:0	LISTENING
TCP	0.0.0.0:1028	harish-HP:0	LISTENING
TCP	0.0.0.0:1036	harish-HP:0	LISTENING
TCP	0.0.0.0:2869	harish-HP:0	LISTENING

```
TCP
                       harish-HP:0
       0.0.0.0:3306
                                        LISTENING
                       harish-HP:0
 TCP
       0.0.0.0:5357
                                        LISTENING
 TCP
       0.0.0.0:10243
                        harish-HP:0
                                         LISTENING
 TCP
       10.26.2.162:139
                                          LISTENING
                         harish-HP:0
 TCP
                          209.56.124.25:http
       10.26.2.162:2304
                                             ESTABLISHED
 TCP
                          ord08s09-in-f13:http ESTABLISHED
       10.26.2.162:2793
 TCP
                          ord08s09-in-f25:http ESTABLISHED
       10.26.2.162:2796
 TCP
                          209.56.124.25:http
                                             ESTABLISHED
       10.26.2.162:3159
       10.26.2.162:3499
 TCP
                          ord08s06-in-f28:http ESTABLISHED
 TCP
                          ord08s06-in-f27:http ESTABLISHED
       10.26.2.162:3505
 TCP
            10.26.2.162:3507
                                        server-54-240-170-195:https
ESTABLISHED
 TCP
            10.26.2.162:3508
                                        server-54-240-170-195:https
ESTABLISHED
 TCP
       10.26.2.162:3511
                          50.116.194.21:http
                                             TIME WAIT
 TCP
       10.26.2.162:3513
                          50.116.194.21:http
                                             TIME_WAIT
 TCP
       10.26.2.162:3514
                          209.56.124.24:http
                                             TIME WAIT
 TCP
       10.26.2.162:3515
                          209.56.124.24:http
                                             TIME_WAIT
 TCP
       10.26.2.162:3516
                          209.56.124.24:http
                                             TIME_WAIT
 TCP
       10.26.2.162:3517
                          209.56.124.23:http
                                             TIME_WAIT
 TCP
                          209.56.124.23:http
       10.26.2.162:3518
                                             TIME_WAIT
 TCP
                          ox-173-241-250-12:http TIME_WAIT
       10.26.2.162:3527
 TCP
                          ox-173-241-250-12:http TIME WAIT
       10.26.2.162:3528
 TCP
       10.26.2.162:3529
                          ox-173-241-250-12:http TIME_WAIT
 TCP
       10.26.2.162:3530
                          209.56.124.24:http
                                             TIME WAIT
 TCP
       10.26.2.162:3531
                          209.56.124.24:http
                                             TIME_WAIT
 TCP
       10.26.2.162:3533
                          ord08s06-in-f13:http ESTABLISHED
 TCP
       10.26.2.162:3534
                          ord08s06-in-f13:http ESTABLISHED
 TCP
       10.26.2.162:3535
                          ord08s06-in-f13:http ESTABLISHED
 TCP
                          ord08s06-in-f13:http ESTABLISHED
       10.26.2.162:3536
 TCP
                          ord08s06-in-f13:http ESTABLISHED
       10.26.2.162:3537
 TCP
       10.26.2.162:3538
                          ord08s06-in-f25:http ESTABLISHED
 TCP
       10.26.2.162:3539
                          ord08s06-in-f25:http ESTABLISHED
 TCP
       10.26.2.162:3540
                          ord08s06-in-f25:http ESTABLISHED
 TCP
       10.26.2.162:3541
                          ord08s06-in-f25:http ESTABLISHED
 TCP
       10.26.2.162:3542
                          ord08s06-in-f25:http ESTABLISHED
 TCP
       127.0.0.1:1029
                         harish-HP:27015
                                           ESTABLISHED
 TCP
       127.0.0.1:1030
                         harish-HP:1031
                                           ESTABLISHED
 TCP
       127.0.0.1:1031
                         harish-HP:1030
                                           ESTABLISHED
 TCP
       127.0.0.1:1034
                         harish-HP:0
                                         LISTENING
 TCP
       127.0.0.1:5354
                         harish-HP:0
                                         LISTENING
 TCP
       127.0.0.1:5939
                         harish-HP:0
                                         LISTENING
 TCP
       127.0.0.1:27015
                         harish-HP:0
                                          LISTENING
 TCP
       127.0.0.1:27015
                         harish-HP:1029
                                           ESTABLISHED
 TCP
       [::]:135
                     harish-HP:0
                                      LISTENING
 TCP
       [::]:445
                     harish-HP:0
                                      LISTENING
```

```
TCP
      [::]:554
                     harish-HP:0
                                       LISTENING
TCP
      [::]:1025
                      harish-HP:0
                                        LISTENING
TCP
                                        LISTENING
      [::]:1026
                      harish-HP:0
TCP
      [::]:1027
                      harish-HP:0
                                        LISTENING
TCP
      [::]:1028
                      harish-HP:0
                                        LISTENING
TCP
                      harish-HP:0
                                        LISTENING
      [::]:1036
TCP
                                        LISTENING
      [::]:2869
                      harish-HP:0
TCP
      [::]:3587
                      harish-HP:0
                                        LISTENING
TCP
      [::]:5357
                      harish-HP:0
                                        LISTENING
TCP
                       harish-HP:0
                                         LISTENING
      [::]:10243
TCP
      [::1]:1035
                       harish-HP:0
                                         LISTENING
UDP
                       *:*
      0.0.0.0:86
UDP
                        *:*
      0.0.0.0:500
UDP
                        *:*
      0.0.0.0:3544
                        *.*
UDP
      0.0.0.0:3702
UDP
      0.0.0.0:3702
                        *:*
                        *.*
UDP
      0.0.0.0:3702
                        *:*
UDP
      0.0.0.0:3702
                        *.*
UDP
      0.0.0.0:4500
                        *.*
UDP
      0.0.0.0:5004
                        *.*
UDP
      0.0.0.0:5005
UDP
                        *:*
      0.0.0.0:5093
                        *.*
UDP
      0.0.0.0:5355
                         *.*
UDP
      0.0.0.0:50140
                         *.*
UDP
      0.0.0.0:59824
                         *.*
UDP
      0.0.0.0:59826
                          *:*
UDP
       10.26.2.162:137
                          *:*
UDP
       10.26.2.162:138
UDP
       10.26.2.162:1900
                           *.*
                           *.*
UDP
       10.26.2.162:5353
                           *.*
UDP
       10.26.2.162:58345
                           *:*
UDP
      10.26.2.162:62423
                          *.*
UDP
       127.0.0.1:1900
                          *:*
UDP
      127.0.0.1:56334
UDP
                          *:*
      127.0.0.1:56335
                          *.*
UDP
      127.0.0.1:56336
                          *.*
UDP
      127.0.0.1:59221
                          *.*
UDP
      127.0.0.1:59822
                          *.*
UDP
      127.0.0.1:59823
                          *:*
UDP
      127.0.0.1:59857
                          *.*
UDP
      127.0.0.1:59912
                          *.*
UDP
      127.0.0.1:62424
                      *:*
UDP
      [::]:500
                       *:*
UDP
      [::]:3540
                       *.*
UDP
      [::]:3702
                       *.*
UDP
      [::]:3702
```

```
UDP [::]:3702
                      *:*
                      *:*
UDP
      [::]:3702
                      *:*
UDP
      [::]:4500
                      *:*
UDP
      [::]:5004
      [::]:5005
                      *:*
UDP
UDP
      [::]:5093
                      *:*
                      *.*
UDP
      [::]:5355
                      *:*
UDP
      [::]:50141
UDP
      [::]:59825
                      *:*
UDP
                      *:*
      [::]:59827
                       *:*
UDP
      [::1]:1900
                       *:*
UDP
      [::1]:5353
      [::1]:62422
                       *:*
UDP
UDP [fe80::25da:95e9:3ffd:2f89%12]:1900 *:*
      [fe80::25da:95e9:3ffd:2f89%12]:62421 *:*
UDP
```

 $C:\Users\harish>$