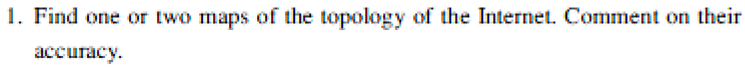
Cpre 530 - Assignment 1

Fall 2011

Suganya Baskaran

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



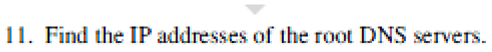
1. Find one or two maps of the topology of the Internet. Comment on their accuracy.

1. 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_pnas2007.png

The above topology is the outcome of the research in Boston University. Instead of node degree, we will use the “k-shell” decomposition to assign a shell index to each node in the Internet. Although node degrees can range from one or two up to several thousands, we find that 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.

2. http://cheleby.cse.unr.edu/ This is Cheleby: An Internet Topology Mapping System, Internet Telescope will collect topology information from the Internet using PlanetLab. Goal is Subnet-level Internet Mapping. Good picture at
http://cheleby.cse.unr.edu/images/Internet.jpg

Build an efficient system that produces a map of the Internet such that
–Alias IP addresses that belong to the same router,
–Star (*) occurrences that stand for the same router,
–IPs that belong to the same subnet are identified.

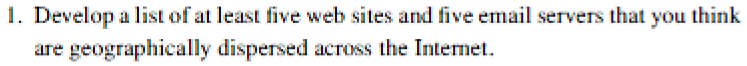


11. Find the IP addresses of the root DNS servers.

The DNS root servers are thirteen DNSserver clusters which are responsible for delegating DNS requests to the top level domain (TLD) nameservers.
The DNS Root Servers
A.ROOT-SERVERS.NET.
Operator: Verisign Naming and Directory Services
IP Address: 198.41.0.4
B.ROOT-SERVERS.NET.
Operator: Information Sciences Institute
IP address: 192.228.79.201
C.ROOT-SERVERS.NET.
Operator: Cogent Communications
IP Address: 192.33.4.12
D.ROOT-SERVERS.NET.
Operator: University of Maryland
IP Address: 128.8.10.90
E.ROOT-SERVERS.NET.
Operator: NASA Ames Research Center
IP Address: 192.203.230.10
F.ROOT-SERVERS.NET.
Operator: Internet Systems Consortium, Inc.

IP Address: 192.5.5.241
G.ROOT-SERVERS.NET.
Operator: U.S. DOD Network Information Center
IP Address: 192.112.36.4
H.ROOT-SERVERS.NET.
Operator: Autonomica/NORDUnet
IP Address: 128.63.2.53
I.ROOT-SERVERS.NET.
Operator: Autonomica/NORDUnet
IP Address: 192.36.148.17
J.ROOT-SERVERS.NET.
Operator: VeriSign Naming and Directory Services
IP Address: 192.58.128.30
K.ROOT-SERVERS.NET.
Operator: Reseaux IP Europeens – Network Coordination Centre
IP Address: 193.0.14.129
L.ROOT-SERVERS.NET.
Operator: Internet Corporation for Assigned Names and Numbers
IP Address: 198.32.64.12
M.ROOT-SERVERS.NET.
Operator: WIDE Project
IP Address: 202.12.27.33
The DNS root servers have not been changed between 29 January, 2004 and today — 22 November, 2006

Question 2 Do lab experiments 1-6 in Chapter 3



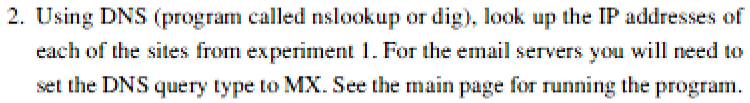
1. Develop a list of at least five web sites and five email servers that you think are geographically dispersed across the Internet.

List of websites:

1. www.google.com
2. www.facebook.com
3. www.twitter.com
4. www.microsoft.com
5. www.wikipedia.org

List of Email servers:

1. www.gmail.com
2. www.yahoomail.com
3. www.rediff.com
4. James.apache.org
5. Hotmail.com



2. Using DNS (program called nslookup or dig), 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.

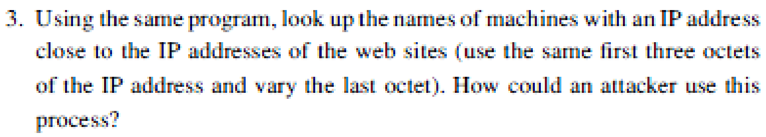
IP addresses of websites:

1. 74.125.225.80/84
2. 63.69.189.16
3. 199.59.149.198

4. 207.46.232.182
5. 208.80.152.2

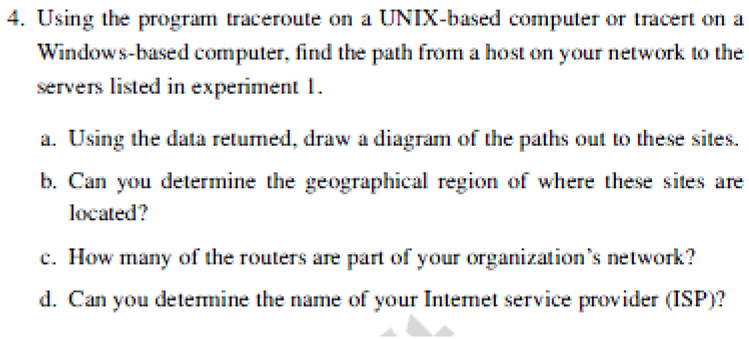
IP addresses of email servers:

1. 209.85.225.26
2. 68.180.131.16
3. 213.155.153.132
4. 192.87.106.230
5. 65.54.188.110



3. Using the same program, look up the names of machines with an IP address close to the IP addresses of the web sites (use the same first three octets of the IP address and vary the last octet). How could an attacker use this process?

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.



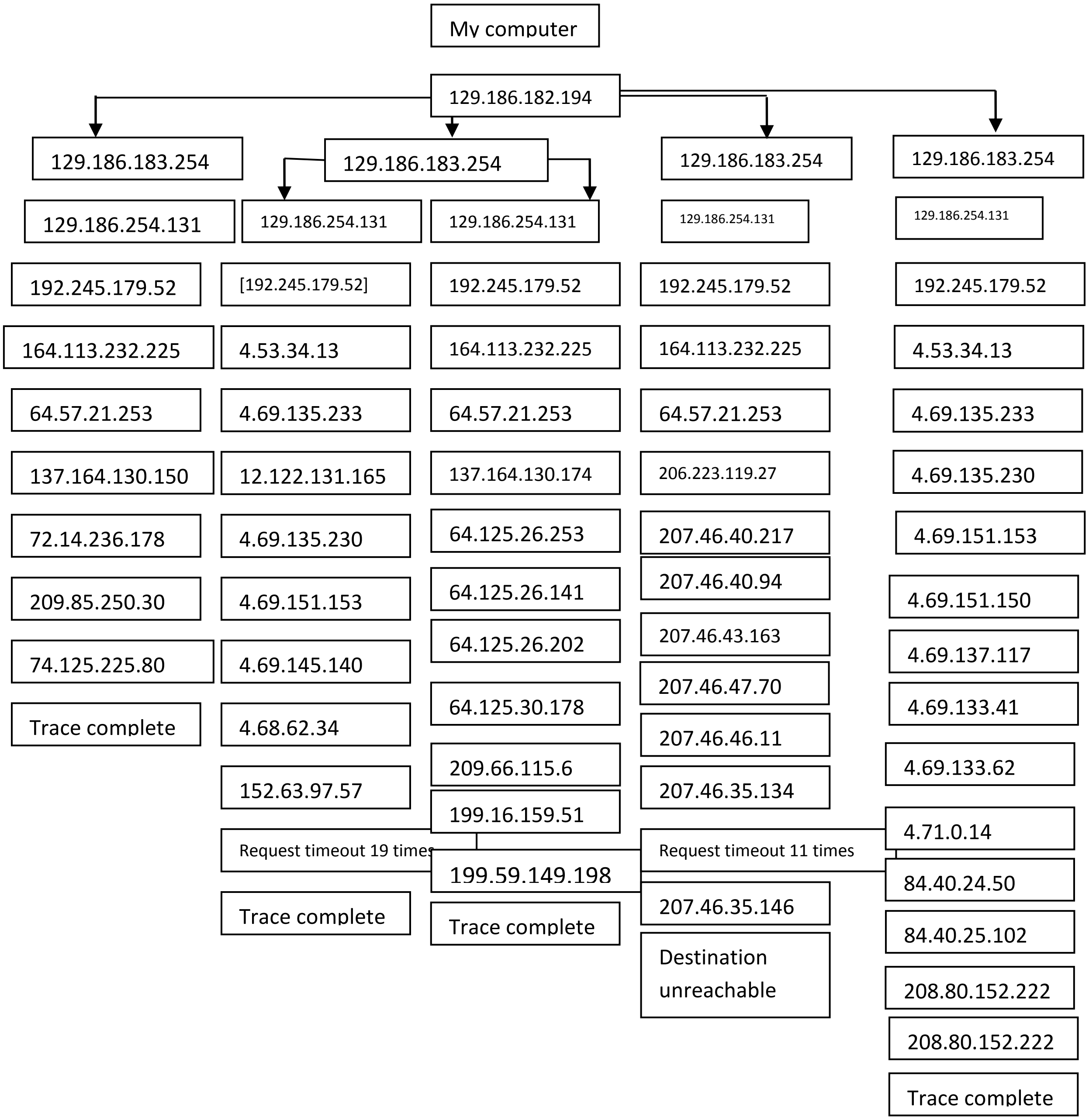
4. Using the program traceroute on a UNIX-based computer or tracert on a Windows-based computer, find the path from a host on your network to the servers listed in experiment 1.

   a. Using the data returned, draw a diagram of the paths out to these sites.

   b. Can you determine the geographical region of where these sites are located?

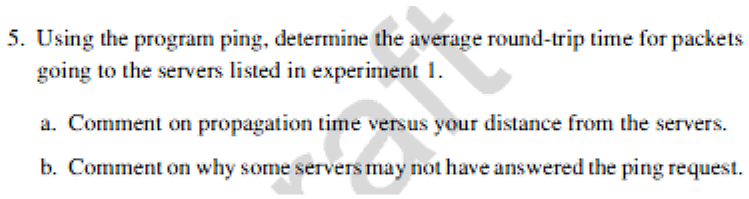
   c. How many of the routers are part of your organization's network?

   d. Can you determine the name of your Internet service provider (ISP)?


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
Trace complete
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
152.63.97.57
Request timeout 19 times
Trace complete
129.186.254.131
192.245.179.52
164.113.232.225
64.57.21.253
137.164.130.174
64.125.26.253
64.125.26.141
64.125.26.202
64.125.30.178
209.66.115.6
199.16.159.51
199.59.149.198
Trace complete
129.186.183.254
129.186.254.131
192.245.179.52
164.113.232.225
64.57.21.253
206.223.119.27
207.46.40.217
207.46.40.94
207.46.43.163
207.46.47.70
207.46.46.11
207.46.35.134
Request timeout 11 times
207.46.35.146
Destination unreachable
129.186.183.254
129.186.254.131
192.245.179.52
4.53.34.13
4.69.135.233
4.69.135.230
4.69.151.153
4.69.151.150
4.69.137.117
4.69.133.41
4.69.133.62
4.71.0.14
84.40.24.50
84.40.25.102
208.80.152.222
208.80.152.222
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.



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 your distance from the servers.
    b. Comment on why some servers may not have answered the ping request.

Average round trip time for:

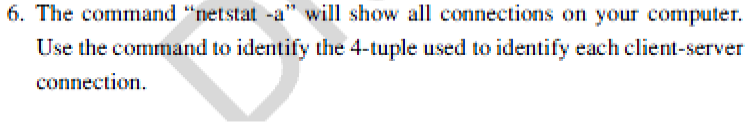
IP addresses of websites:

1. www.google.com – 15ms
2. www.facebook.com – 39ms
3. www.twitter.com – 61ms
4. www.microsoft.com – 63ms
5. www.wikipedia.org – 55ms

IP addresses of email servers:

1. www.gmail.com – 15ms
2. www.yahoomail.com – 40ms
3. www.rediff.com – 1ms
4. James.apache.org – 51ms
5. Hotmail.com – 49ms

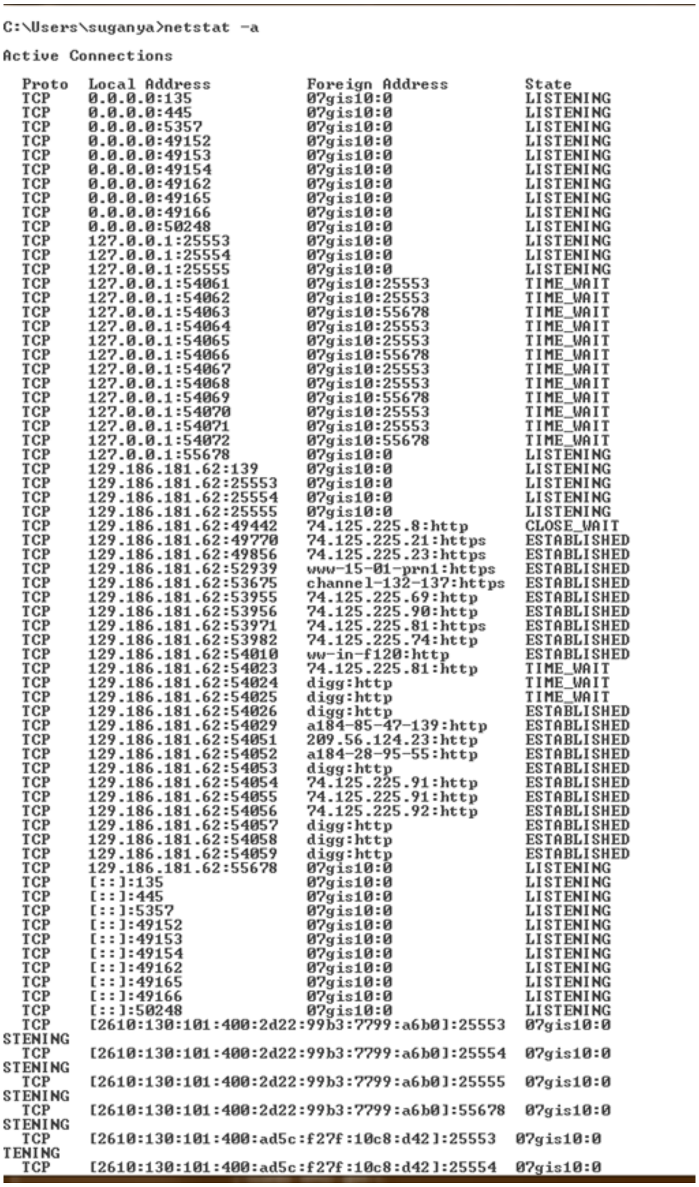
Propagation time: The propagation time is directly proportional to the geographical distance of the server.
Ping request time out: The reason for the time out could be because there is no reply from the host, or the packet is lost on its way back.



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

"netstat –a" returns Protocol, Local Address, Foreign Address and State

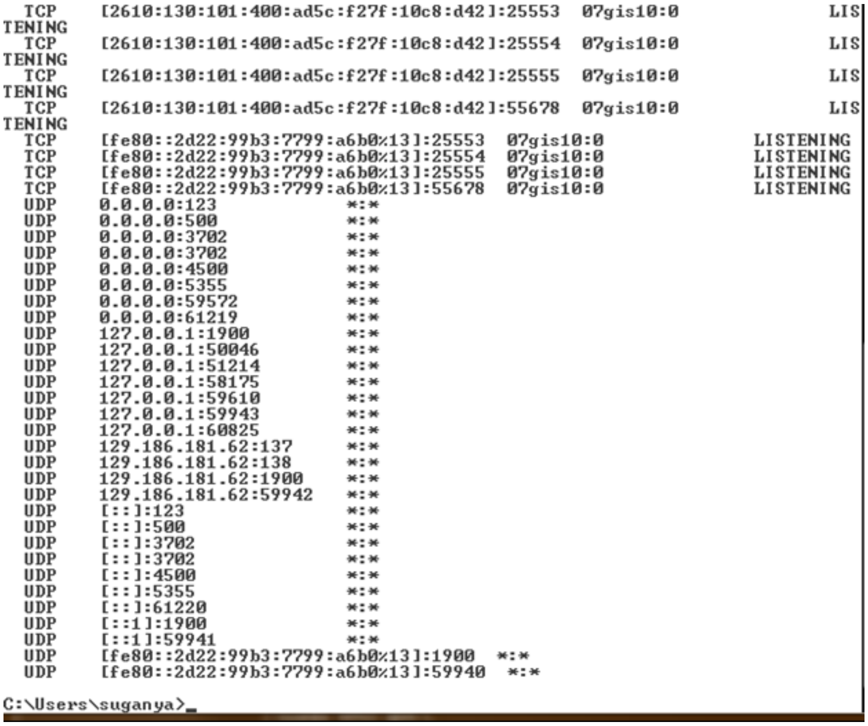
Below is the list of those connections:



```
C:\Users\suganya>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            07gis10:0              LISTENING
  TCP    0.0.0.0:445            07gis10:0              LISTENING
  TCP    0.0.0.0:5357           07gis10:0              LISTENING
  TCP    0.0.0.0:49152          07gis10:0              LISTENING
  TCP    0.0.0.0:49153          07gis10:0              LISTENING
  TCP    0.0.0.0:49154          07gis10:0              LISTENING
  TCP    0.0.0.0:49162          07gis10:0              LISTENING
  TCP    0.0.0.0:49165          07gis10:0              LISTENING
  TCP    0.0.0.0:49166          07gis10:0              LISTENING
  TCP    0.0.0.0:50248          07gis10:0              LISTENING
  TCP    127.0.0.1:25553        07gis10:0              LISTENING
  TCP    127.0.0.1:25554        07gis10:0              LISTENING
  TCP    127.0.0.1:25555        07gis10:0              LISTENING
  TCP    127.0.0.1:54061        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54062        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54063        07gis10:55678          TIME_WAIT
  TCP    127.0.0.1:54064        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54065        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54066        07gis10:55678          TIME_WAIT
  TCP    127.0.0.1:54067        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54068        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54069        07gis10:55678          TIME_WAIT
  TCP    127.0.0.1:54070        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54071        07gis10:25553          TIME_WAIT
  TCP    127.0.0.1:54072        07gis10:55678          TIME_WAIT
  TCP    127.0.0.1:55678        07gis10:0              LISTENING
  TCP    129.186.181.62:139     07gis10:0              LISTENING
  TCP    129.186.181.62:25553   07gis10:0              LISTENING
  TCP    129.186.181.62:25554   07gis10:0              LISTENING
  TCP    129.186.181.62:25555   07gis10:0              LISTENING
  TCP    129.186.181.62:49442   74.125.225.8:http      CLOSE_WAIT
  TCP    129.186.181.62:49770   74.125.225.21:https    ESTABLISHED
  TCP    129.186.181.62:49856   74.125.225.23:https    ESTABLISHED
  TCP    129.186.181.62:52939   www-15-01-prn1:https   ESTABLISHED
  TCP    129.186.181.62:53675   channel-132-137:https  ESTABLISHED
  TCP    129.186.181.62:53955   74.125.225.69:http     ESTABLISHED
  TCP    129.186.181.62:53956   74.125.225.90:http     ESTABLISHED
  TCP    129.186.181.62:53971   74.125.225.81:https    ESTABLISHED
  TCP    129.186.181.62:53982   74.125.225.74:http     ESTABLISHED
  TCP    129.186.181.62:54010   ww-in-f120:http        ESTABLISHED
  TCP    129.186.181.62:54023   74.125.225.81:http     TIME_WAIT
  TCP    129.186.181.62:54024   digg:http              TIME_WAIT
  TCP    129.186.181.62:54025   digg:http              TIME_WAIT
  TCP    129.186.181.62:54026   digg:http              ESTABLISHED
  TCP    129.186.181.62:54029   a184-85-47-139:http    ESTABLISHED
  TCP    129.186.181.62:54051   209.56.124.23:http     ESTABLISHED
  TCP    129.186.181.62:54052   a184-28-95-55:http     ESTABLISHED
  TCP    129.186.181.62:54053   digg:http              ESTABLISHED
  TCP    129.186.181.62:54054   74.125.225.91:http     ESTABLISHED
  TCP    129.186.181.62:54055   74.125.225.91:http     ESTABLISHED
  TCP    129.186.181.62:54056   74.125.225.92:http     ESTABLISHED
  TCP    129.186.181.62:54057   digg:http              ESTABLISHED
  TCP    129.186.181.62:54058   digg:http              ESTABLISHED
  TCP    129.186.181.62:54059   digg:http              ESTABLISHED
  TCP    129.186.181.62:55678   07gis10:0              LISTENING
  TCP    [::]:135               07gis10:0              LISTENING
  TCP    [::]:445               07gis10:0              LISTENING
  TCP    [::]:5357              07gis10:0              LISTENING
  TCP    [::]:49152             07gis10:0              LISTENING
  TCP    [::]:49153             07gis10:0              LISTENING
  TCP    [::]:49154             07gis10:0              LISTENING
  TCP    [::]:49162             07gis10:0              LISTENING
  TCP    [::]:49165             07gis10:0              LISTENING
  TCP    [::]:49166             07gis10:0              LISTENING
  TCP    [::]:50248             07gis10:0              LISTENING
  TCP    [2610:130:101:400:2d22:99b3:7799:a6b0]:25553  07gis10:0
STENING
  TCP    [2610:130:101:400:2d22:99b3:7799:a6b0]:25554  07gis10:0
STENING
  TCP    [2610:130:101:400:2d22:99b3:7799:a6b0]:25555  07gis10:0
STENING
  TCP    [2610:130:101:400:2d22:99b3:7799:a6b0]:55678  07gis10:0
STENING
  TCP    [2610:130:101:400:ad5c:f27f:10c8:d42]:25553  07gis10:0
TENING
  TCP    [2610:130:101:400:ad5c:f27f:10c8:d42]:25554  07gis10:0
```



```
  TCP    [2610:130:101:400:ad5c:f27f:10c8:d42]:25553  07gis10:0              LIS
TENING
  TCP    [2610:130:101:400:ad5c:f27f:10c8:d42]:25554  07gis10:0              LIS
TENING
  TCP    [2610:130:101:400:ad5c:f27f:10c8:d42]:25555  07gis10:0              LIS
TENING
  TCP    [2610:130:101:400:ad5c:f27f:10c8:d42]:55678  07gis10:0              LIS
TENING
  TCP    [fe80::2d22:99b3:7799:a6b0%13]:25553  07gis10:0              LISTENING
  TCP    [fe80::2d22:99b3:7799:a6b0%13]:25554  07gis10:0              LISTENING
  TCP    [fe80::2d22:99b3:7799:a6b0%13]:25555  07gis10:0              LISTENING
  TCP    [fe80::2d22:99b3:7799:a6b0%13]:55678  07gis10:0              LISTENING
  UDP    0.0.0.0:123            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:3702           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:59572          *:*
  UDP    0.0.0.0:61219          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:50046        *:*
  UDP    127.0.0.1:51214        *:*
  UDP    127.0.0.1:58175        *:*
  UDP    127.0.0.1:59610        *:*
  UDP    127.0.0.1:59943        *:*
  UDP    127.0.0.1:60825        *:*
  UDP    129.186.181.62:137     *:*
  UDP    129.186.181.62:138     *:*
  UDP    129.186.181.62:1900    *:*
  UDP    129.186.181.62:59942   *:*
  UDP    [::]:123               *:*
  UDP    [::]:500               *:*
  UDP    [::]:3702              *:*
  UDP    [::]:3702              *:*
  UDP    [::]:4500              *:*
  UDP    [::]:5355              *:*
  UDP    [::]:61220             *:*
  UDP    [::1]:1900             *:*
  UDP    [::1]:59941            *:*
  UDP    [fe80::2d22:99b3:7799:a6b0%13]:1900  *:*
  UDP    [fe80::2d22:99b3:7799:a6b0%13]:59940  *:*

C:\Users\suganya>_
```

<u>Reference:</u>

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