Richard Boone, 8659963

CS 176B HW1

1)

```
[rboone@csil-13 ~]$ ifconfig -a
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 128.111.43.33  netmask 255.255.255.0  broadcast 128.111.43.255
        inet6 fe80::1a66:daff:fe23:3f8a  prefixlen 64  scopeid 0x20<link>
        ether 18:66:da:23:3f:8a  txqueuelen 1000  (Ethernet)
        RX packets 170296  bytes 22321188 (21.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 169136  bytes 120236427 (114.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xf7100000-f7120000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 30  bytes 1598 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 1598 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:62:ee:11  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0-nic: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 52:54:00:62:ee:11  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[rboone@csil-13 ~]$
```

a) The network interface is an ethernet interface listed as enp0s31f6. It gives it's own IP address (128.111.43.33), and the netmask and broadcast address for the computer. On the next line, it shows the IPV6 address with a prefixlength of 64, indicating that it's using the whole ipv6 address. The next line indicates the ethernet address on the local ethernet connection with the length of the transmit queue set to 1000. The next four lines indicate the packets and bytes sent and received, as well as the amount of errors and dropped packets. The most significant things to be noticed here are that the TX and RX packet numbers are very similar, but the computer is receiving many more bytes than it is transmitting. Additionally, there are no errors or dropped packets, indicating that we have a very stable connection. After the end of this interface, we see the other interfaces.

b) The same (or very similar) output can be generated with the command "ip addr" on most linux machines.

2) ARP

```
[rboone@csil-13 ~]$ arp -a
? (128.111.43.254) at <incomplete> on enp0s31f6
csworld43.cs.ucsb.edu (128.111.43.1) at 00:26:98:09:b6:41 [ether] on enp0s31f6
[rboone@csil-13 ~]$
```

a)

The first line indicates that my machine know's there's a machine at 128.111.43.254 but does not know the hardware address for said machine. The second line indicates that the machine with url "csworld43.cs.ucsb.edu is at IP address 128.111.43.1 and hardware address 00:26:98:09:b6:41 accessed through an ethernet connection.

b) When trying to delete pieces of the ARP table I get the error "SIOCDARP(dontpub): Operation not permitted" and when trying to add I get the error "SIOCSARP: Operation not permitted". Both these indicate that I do not have permissions to edit the ARP table. This makes sense because editing the ARP table can cause large security flaws.

```
[rboone@csil-13 ~]$ arp -a
csil-15.cs.ucsb.edu (128.111.43.35) at 18:66:da:23:6e:58 [ether] on enp0s31f6
csil-17.cs.ucsb.edu (128.111.43.37) at 18:66:da:23:49:63 [ether] on enp0s31f6
? (128.111.43.254) at <incomplete> on enp0s31f6
csworld43.cs.ucsb.edu (128.111.43.1) at 00:26:98:09:b6:41 [ether] on enp0s31f6
[rboone@csil-13 ~]$
```

c) You can affect the ARP table by connecting to other hosts that will be accessible to you by hardware address. In this case, I connected to csil-15 and csil-17 by using the ping command.

d) The simplest method to discover a timeout value is just to add the value in (either manually or by pinging as above) and then check the ARP cache with "ip neighbor" every few seconds or so to get an estimate. The default timeout can also be found by using the command "cat /proc/sys/net/ipv4/neigh/default/gc_stale_time". In my case, it's 60 seconds which fits well with the time at which ip neighbor marked the entry as "stale". However, the cache numbers do not disappear from the arp -a table. The reason for this is unclear.

e) Ip neighbor indicates which arp cache entries have been refreshed recently enough to be good and which are old enough that they should not be used.

```
[rboone@csil-13 ~]$ ip neighbor
128.111.43.35 dev enp0s31f6 lladdr 18:66:da:23:6e:58 STALE
128.111.43.37 dev enp0s31f6 lladdr 18:66:da:23:49:63 STALE
128.111.43.254 dev enp0s31f6  FAILED
128.111.43.1 dev enp0s31f6 lladdr 00:26:98:09:b6:41 REACHABLE
[rboone@csil-13 ~]$ arp -a
```

As you can see in the screenshot above, the connections I had previously pinged are not listed as "STALE" because they have not been used recently.

f) If the two hosts are not in the same subnet, likely no problems will occur. If the two hosts are in the same subnet, it will cause huge problems. Traffic going to either one of the two hosts will randomly go to one of them depending on whose address was last recognized by the switch. Neither will be able to effectively get an internet connection because packets will consistently be sent to the wrong machine.

3) Traceroute

a) Traceroute maps out a path to a location by sending packets with increasing TTL values, starting at a TTL value of 1 to get the closest path. In Linux, these packets are automatically UDP packets although this can be changed. When a router receives a packet, it automatically decrements its TTL value by 1 and if the TTL value is decremented to 0, the router discards the packet and (usually) return an ICMP Time Exceeded packet to the source. When the machine running the traceroute receives the ICMP Time Exceeded packet, it measures the time from sending the packet to receiving it and displays this time. Usually, 3 packets of each TTL value are sent and measured until traceroute gets values for the destination IP address.

```
[rboone@csil-13 ~]$ traceroute jnto.org.au
traceroute to jnto.org.au (45.32.191.118), 30 hops max, 60 byte packets
 1  csworld43.cs.ucsb.edu (128.111.43.1)  1.757 ms  1.869 ms  1.939 ms
 2  rl--535-c--1.commserv.ucsb.edu (128.111.252.148)  1.124 ms  1.059 ms  1.060 ms
 3  lax-agg8--ucsb-100g.cenic.net (137.164.23.90)  4.026 ms  4.666 ms  4.102 ms
 4  137.164.11.21 (137.164.11.21)  12.613 ms  12.554 ms dc-svl-agg8--lax-agg8-100ge-1.cenic.net (137.164.11.1)  12.
557 ms
 5  137.164.11.30 (137.164.11.30)  11.731 ms  11.730 ms  11.777 ms
 6  dc-paix-pxl--svl-agg4-10g.cenic.net (137.164.47.20)  11.674 ms  11.570 ms dc-paix-pxl--svl-agg4-10g.cenic.net (
137.164.47.172)  11.557 ms
 7  g5-0-0.plapx-drl.ix.singtel.com (198.32.176.50)  11.695 ms  17.375 ms  12.339 ms
 8  203.208.172.233 (203.208.172.233)  12.557 ms  11.800 ms  11.815 ms
 9  203.208.190.18 (203.208.190.18)  169.186 ms  169.240 ms  169.329 ms
10  59.154.18.30 (59.154.18.30)  168.723 ms 59.154.18.28 (59.154.18.28)  168.679 ms  168.561 ms
11  220.101.14.86 (220.101.14.86)  169.305 ms  169.362 ms  168.074 ms
12  * * *
13  * * 180.189.25.6 (180.189.25.6)  169.598 ms
14  * * *
15  * * *
16  45.32.191.118.vultr.com (45.32.191.118)  169.493 ms  169.439 ms  168.039 ms
[rboone@csil-13 ~]$
```

b) The above shows the path traceroute found from csil-13 to jnto.org.au. Lines 1-3 show the path the packets took out of the UCSB network. Lines 4-11 show the continuous path of the packets on their way to jnto.org.au. Notable are lines 4, 6, and 10 where some of the packets return different IP addresses indicating that they took different paths and did not all end at the same router. Lines 12-15 show mostly stars, indicating that traceroute did not receive the ICMP Time Exceeded packet for these numbers. This is usually because the router that received them did not send any packet back. At line 16, we reach jnto.org.au. However, it is not listed as jnto.org.au but as 45.32.191.118.vultr.com because this is the reverse DNS lookup address our computer has found.

c)

```
[rboone@csil-13 ~]$ traceroute sample.com
traceroute to sample.com (173.230.129.147), 30 hops max, 60 byte packets
 1  csworld43.cs.ucsb.edu (128.111.43.1)  1.264 ms  1.684 ms  1.663 ms
 2  rl--535-c--1.commserv.ucsb.edu (128.111.252.148)  1.071 ms  1.008 ms  1.006 ms
 3  lax-agg8--ucsb-100g.cenic.net (137.164.23.90)  4.024 ms  4.002 ms  4.671 ms
 4  137.164.11.26 (137.164.11.26)  3.915 ms 137.164.11.6 (137.164.11.6)  3.907 ms 137.164.11.36 (137.164.11.36)  3.
886 ms
 5  8-1-1-90.ear1.LosAngeles1.Level3.net (4.35.156.65)  3.651 ms  3.982 ms  4.287 ms
 6  * * *
 7  Cogent-level3-100G.LosAngeles1.Level3.net (4.68.73.210)  3.818 ms be3036.ccr41.lax04.atlas.cogentco.com (154.54
.14.129)  3.995 ms  4.085 ms

 8  be3360.ccr42.lax01.atlas.cogentco.com (154.54.25.149)  4.125 ms  3.945 ms  3.973 ms
 9  be2931.ccr31.phx01.atlas.cogentco.com (154.54.44.85)  15.841 ms be2932.ccr32.phx01.atlas.cogentco.com (154.54.4
5.161)  15.855 ms  15.980 ms
10  be2929.ccr21.elp01.atlas.cogentco.com (154.54.42.66)  23.961 ms be2930.ccr21.elp01.atlas.cogentco.com (154.54.4
2.78)  23.769 ms be2929.ccr21.elp01.atlas.cogentco.com (154.54.42.66)  23.821 ms
11  be2927.ccr41.iah01.atlas.cogentco.com (154.54.29.221)  39.969 ms be2928.ccr42.iah01.atlas.cogentco.com (154.54.
30.161)  40.273 ms  40.225 ms
12  be2687.ccr41.atl01.atlas.cogentco.com (154.54.28.69)  53.896 ms be2690.ccr42.atl01.atlas.cogentco.com (154.54.2
8.129)  54.267 ms  54.297 ms
13  be2847.ccr41.atl04.atlas.cogentco.com (154.54.6.102)  54.255 ms be2848.ccr41.atl04.atlas.cogentco.com (154.54.6
.118)  54.400 ms  54.342 ms
14  * * *
15  74.207.239.15 (74.207.239.15)  67.716 ms gw-h7.linode.com (74.207.239.1)  67.589 ms 74.207.239.13 (74.207.239.1
3)  67.411 ms
16  li169-147.members.linode.com (173.230.129.147)  67.469 ms  67.719 ms  67.610 ms
```

d) Machines can be configured to not respond to pings, so a lack of response to pinging a machine doesn't tell you anything about whether the machine exists or not. If we traceroute the machine and get all stars, or continuous stars after a point, we can know the machine does not exist.

e) I chose to use 73.0.0.22. I chose to start with the comcast IP range 73.0.0.0/8 and scan it using Angry IP Scanner. It found that many IPs that were inaccessible, so I chose one at random and tested it on my own machine using ping and traceroute. The traceroute was as follows.

```
[rboone@csil-13 ~]$ traceroute 73.0.0.22
traceroute to 73.0.0.22 (73.0.0.22), 30 hops max, 60 byte packets
 1  csworld43.cs.ucsb.edu (128.111.43.1)  1.676 ms  1.645 ms  1.921 ms
 2  rl--535-c--1.commserv.ucsb.edu (128.111.252.148)  1.129 ms  1.079 ms  1.061
ms
 3  lax-agg8--ucsb-100g.cenic.net (137.164.23.90)  4.271 ms  4.128 ms  4.247 ms
 4  et-1-0-2.0.rtsw.losa.net.internet2.edu (64.57.20.82)  3.627 ms  3.617 ms  3.
602 ms
 5  lo-0.8.rtsw.wilc.net.internet2.edu (64.57.20.254)  3.781 ms  3.779 ms  3.885
 ms
 6  te-0-0-0-0-8-pe01.losangeles.ca.ibone.comcast.net (66.208.233.137)  3.762 ms
  3.764 ms  3.666 ms
 7  be-11599-cr02.losangeles.ca.ibone.comcast.net (68.86.84.193)  5.638 ms  4.72
5 ms  5.622 ms
 8  be-11523-cr01.houston.tx.ibone.comcast.net (68.86.87.174)  40.868 ms  40.484
 ms  40.477 ms
 9  be-11423-cr02.56marietta.ga.ibone.comcast.net (68.86.85.21)  63.103 ms  63.0
75 ms  63.085 ms
10  be-7922-ar01.pompanobeach.fl.pompano.comcast.net (68.86.90.186)  63.238 ms
63.384 ms  63.361 ms
11  96.108.22.174 (96.108.22.174)  87.798 ms  87.803 ms  101.795 ms
12  ae2-acr09.ftlauderdale.fl.pompano.comcast.net (96.110.14.214)  63.290 ms  63
.467 ms  63.386 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[rboone@csil-13 ~]$
```

f)

```
[rboone@csil-13 ~]$ ping 12.1.2.36
PING 12.1.2.36 (12.1.2.36) 56(84) bytes of data.
^C
--- 12.1.2.36 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4120ms

[rboone@csil-13 ~]$ traceroute 12.1.2.36
traceroute to 12.1.2.36 (12.1.2.36), 30 hops max, 60 byte packets
 1  csworld43.cs.ucsb.edu (128.111.43.1)  3.430 ms  4.143 ms  3.802 ms
 2  rl--535-c--1.commserv.ucsb.edu (128.111.252.148)  2.348 ms  2.351 ms  2.413 ms
 3  lax-agg8--ucsb-100g.cenic.net (137.164.23.90)  3.925 ms  4.089 ms  4.861 ms
 4  137.164.11.26 (137.164.11.26)  3.496 ms 137.164.11.36 (137.164.11.36)  3.615 ms 137.164.11.6 (
137.164.11.6)  3.610 ms
 5  8-1-1-90.earl.LosAngeles1.Level3.net (4.35.156.65)  3.548 ms  4.092 ms  3.797 ms
 6  * * *
 7  192.205.37.145 (192.205.37.145)  12.614 ms  8.613 ms  13.971 ms
 8  cr1.la2ca.ip.att.net (12.122.128.102)  56.469 ms  57.694 ms  58.318 ms
 9  slkut21crs.ip.att.net (12.122.1.186)  68.853 ms  65.236 ms  56.846 ms
10  dvmco22crs.ip.att.net (12.122.28.45)  63.113 ms  63.021 ms  60.355 ms
11  cr1.kc9mo.ip.att.net (12.122.28.78)  63.256 ms  66.562 ms  63.217 ms
12  cr85.cgcil.ip.att.net (12.122.99.34)  63.380 ms  60.816 ms  64.434 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[rboone@csil-13 ~]$
```

g)

```
[rboone@csil-13 ~]$ traceroute 19.5.5.7
traceroute to 19.5.5.7 (19.5.5.7), 30 hops max, 60 byte packets
 1  csworld43.cs.ucsb.edu (128.111.43.1)  4.963 ms  1.258 ms  4.930 ms
 2  rl--535-c--1.commserv.ucsb.edu (128.111.252.148)  1.055 ms  1.032 ms  1.030 ms
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
[rboone@csil-13 ~]$
```

```
[rboone@csil-13 ~]$ traceroute 17.8.3.61
traceroute to 17.8.3.61 (17.8.3.61), 30 hops max, 60 byte packets
 1  csworld43.cs.ucsb.edu (128.111.43.1)  4.534 ms  4.566 ms  4.554 ms
 2  rl--535-c--1.commserv.ucsb.edu (128.111.252.148)  1.088 ms  1.089 ms  1.079 ms
 3  lax-agg8--ucsb-100g.cenic.net (137.164.23.90)  3.757 ms * *
 4  137.164.11.26 (137.164.11.26)  3.492 ms 137.164.11.6 (137.164.11.6)  3.563 ms  3.482 ms
 5  peering.kddi.com (198.32.146.36)  3.655 ms  3.643 ms  3.643 ms
 6  lacGCS002.int-gw.kddi.ne.jp (203.181.106.157)  3.633 ms lacGCS002.int-gw.kddi.ne.jp (203.181.1
06.153)  3.613 ms lacGCS002.int-gw.kddi.ne.jp (203.181.106.157)  3.650 ms
 7  106.187.12.17 (106.187.12.17)  109.666 ms 106.187.12.13 (106.187.12.13)  115.747 ms  115.729 m
s
 8  27.85.227.246 (27.85.227.246)  111.747 ms 27.85.227.234 (27.85.227.234)  119.491 ms  115.257 m
s
 9  cm-kot210.int-gw.kddi.ne.jp (125.29.22.174)  113.750 ms cm-kot210.int-gw.kddi.ne.jp (125.29.22
.170)  115.326 ms cm-kot210.int-gw.kddi.ne.jp (125.29.22.174)  113.793 ms
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

The routes all go some distance, then turn into complete stars. This happens because it is impossible for all the individual routers to know whether a machine exists, so each of the routers does their best to direct the packet towards its intended destination. At some point (likely when the packet reaches whatever subnet the computer should be contained in, the packets just get dropped because the host does not exist.

h) Tracepath is very similar to traceroute, but it does not show the IP of each individual router. It just shows the router name and a single TTL value.

4)

a)

Router: bourss-rbr1.ja.net
Query: (IPv4) traceroute host 23.185.0.2

```
 1  ae2-0.stonss-rbr1.ja.net (146.97.68.49)  1.315 ms  1.187 ms  1.185 ms
 2  ae1-0.aldess-rbr1.ja.net (146.97.68.46)  2.352 ms  2.246 ms  2.257 ms
 3  ae23.londpg-sbr2.ja.net (146.97.37.249)  3.984 ms  3.884 ms  3.659 ms
 4  ae30.londtw-sbr2.ja.net (146.97.33.6)  4.227 ms  4.262 ms  4.197 ms
 5  ae28.londtt-sbr1.ja.net (146.97.33.61)  5.071 ms  4.891 ms  5.406 ms
 6  ae0.londtn-ban1.ja.net (146.97.35.210)  4.242 ms  4.200 ms  4.288 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
```

All of the routers are within the ja.net domain, just like alice.ja.net. Line 1's location is not clear. Line 2 routes through Aldess in France. Lines 3-6 all route through London. Although the exact locations are not clear it is likely that the router for line 4 is in twickenham, and the router for line 6 is in Tunbridge. Because the route ends very early, and the IP address is not a UCSB IP address, it is clear that ucsb.net is not hosted in UCSB.

```
Router: bourss-rbr1.ja.net
Query:  (IPv4) traceroute host 128.111.1.1
```

```
 1  ae2-0.stonss-rbr1.ja.net (146.97.68.49)  1.848 ms  1.204 ms  1.193 ms
 2  ae1-0.aldess-rbr1.ja.net (146.97.68.46)  2.267 ms  2.242 ms  2.233 ms
 3  ae23.londpg-sbr2.ja.net (146.97.37.249)  3.666 ms  3.929 ms  3.723 ms
 4  ae29.londhx-sbr1.ja.net (146.97.33.1)  5.169 ms  4.179 ms  4.186 ms
 5  janet.mx1.lon.uk.geant.net (62.40.124.197)  4.754 ms  4.647 ms  4.183 ms
 6  internet2-gw.mx1.lon.uk.geant.net (62.40.124.45)  79.575 ms  79.353 ms  85.313 ms
 7  162.252.70.159 (162.252.70.159)  140.152 ms  139.219 ms  139.448 ms
 8  137.164.26.200 (137.164.26.200)  139.288 ms  139.704 ms  139.191 ms
 9  ucsb--lax-hpr3-100ge.cenic.net (137.164.26.238)  141.825 ms  142.292 ms  142.164 ms
10  535-c--r1--1.commserv.ucsb.edu (128.111.252.149)  178.343 ms  141.908 ms  142.382 ms
11  556-c-v1164.noc.ucsb.edu (128.111.4.117)  143.402 ms  142.560 ms  142.601 ms
12  ns1.ucsb.edu (128.111.1.1)  142.472 ms  142.391 ms  142.317 ms
```

b)

Unlike the last traceroute, this route actually finishes, and travels all the way to UCSB. Just as before, the first four lines are within ja.net with all four routers being the same as before. Lines 5 and 6 travel through London. Lines 7 and 8 are unclear because they only offer IP addresses. Lines 9 to 12 show the path of the packets through the UCSB network to the given machine.

5)

a) Netstat is a linux command that gives information about the network connections on your local machine. It is used to monitor network activity on a machine.

b) Netstat --tcp will show all tcp connections. The connections on the machine I used (csil-13 look as follows:

```
[rboone@csil-13 ~]$ netstat --tcp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 csil-13.cs.ucsb.edu:ssh ip98-185-241-2.sb:58355 ESTABLISHED
tcp        0      0 csil-13.cs.ucsb.edu:ssh ip98-185-241-2.sb:58939 ESTABLISHED
tcp        0      0 csil-13.cs.ucsb.edu:ssh ip184-187-185-149:56622 ESTABLISHED
tcp        0      0 csil-13.cs.ucsb.edu:789 tyr.engr.ucsb.edu:nfs   ESTABLISHED
tcp        0     85 csil-13.cs.ucsb.edu:ssh 164.ip-51-255-174:42180 FIN_WAIT1
tcp        0      0 csil-13.cs.ucsb.e:39486 syslog.engr.ucsb.:https TIME_WAIT
tcp        0    240 csil-13.cs.ucsb.edu:ssh ip184-189-222-14.:55719 ESTABLISHED
tcp        0    964 csil-13.cs.ucsb.edu:ssh ip184-189-224-175:43766 ESTABLISHED
tcp        0      0 csil-13.cs.ucsb.edu:ssh ip98-185-241-2.sb:58938 ESTABLISHED
```

c) Netstat -I displays interface status. There are 3 interfaces on my machine (csil-13). The loopback interface allows the machine to network with itself. Anything sent to this interface will loop back to the local machine. This can be used as an easy way to test web servers and other internet traffic without opening them to the public. The loopback interface is the same as using IPV4 address 127.0.0.0.

6) nslookup

a) Cs.princeton.edu is at 128.112.136.51

b) My computer uses 128.111.1.2. The computer is told by the local network what DNS server to use. Because both the host (csil-13) and the DNS server (128.111.1.1) are on the UCSB network, the local router probably gave this DNS address to the host on connection to the network.

c) Nslookup -type=mx hotmail.com gives the name of the mail exchanger: hotmail-com.olc.protection.outlook.com. By pinging this URL, we can get the IP 104.47.45.33.

7) whois
   a) Kevin Schmidt is the administrative contact for UCSB.
   b) 130.207.8.11 is the ip address for mortician.cc.gateway.edu
   c) Call Mark Silis at 617-324-5900
   d) Running nslookup -type=mx gmail.com gives the following mail exchangers:

```
Non-authoritative answer:
gmail.com       mail exchanger = 30 alt3.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 5 gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 10 alt1.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 20 alt2.gmail-smtp-in.l.google.com.
gmail.com       mail exchanger = 40 alt4.gmail-smtp-in.l.google.com.
```

   Checking this in a WhoiS database gives the following information.

Raw WHOIS Record

```
Domain Name: google.com
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2018-02-21T10:45:07-0800
Creation Date: 1997-09-15T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited
(https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited
(https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Name Server: ns3.google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
Name Server: ns1.google.com
DNSSEC: unsigned
```

   This shows that the gmail network is coordinated by MarkMonitor, a digital brand protection company.
   e) Innovative Logic Corp owns 198.182.196.56. Arin.net acts as the dns nameserver. 198.182.196.0 acts as DNS nameserver.
8) Misc
   a) 104.69.73.91 is returned. The browser returns this as an “invalid url”

b) I am redirected to www.whitehouse.gov. www.whitehouse.gov is at a different ip, and so is a different website. This means that the computer that hosts 104.69.73.91 is set up to redirect people who access by URL but not to redirect people who try to access it by IP.

c) Abuse complaints should be sent using any of the following information:

```
OrgAbuseHandle: NUS-ARIN
OrgAbuseName:   NOC United States
OrgAbusePhone:  +1-617-444-2535
OrgAbuseEmail:  abuse@akamai.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/NUS-ARIN
```

The domain is not a .gov, but a .com indicating that abuse complaints are received outside the government.

d) Abuse complaints should be sent to registrar-abuse@akamai.com. This is the same domain as above, once again indicating that abuse complaints are received outside the government.