5090209351 杜溪

PART 1

1. d = 56b / (500 kb/s) + 2ms +56b / (64kb/s) = (56/500 + 56/64 + 2)ms = 2.987ms

2. a. n = (1Mb/s)/(100kb/s) = 10
   b. p = 10% = 0.1
   c. $C(40,n) * p^n * (1-p)^{40-n} = 40!/(n!(40-n)!)*0.1^n*0.9^{40-n}$
   d. 1.4697224972242656e-3
      in GHCi:
      ```
      let ce n k = div (foldl (*) 1 [k+1..n]) (foldl (*) 1 [1..n-k])
      let pn n = (fromIntegral (ce 40 n)) * 0.1^n * 0.9^(40-n)
      foldl (+) 0 ( map pn [11..40] )
      ```

3. Intra-continent: 61.135.181.175

time	1	2	3
average RTD (ms)	131.17424999999997	140.19119999999998	125.57480769230769
std. dev. of RTD (ms)	6.8064126224492885	20.16631230269072	3.599442834875763
number of routers	19	18 or 19	19 or 22

~6 ISPs

Inter-continent: 128.2.10.162

time	1	2	3
average RTD (ms)	403.5662500000001	442.10939130434787	402.00776
std. dev. of RTD (ms)	67.25053034557325	125.26268099795111	54.38134497944433
number of routers	27 or 28	26,27 or 28	27 or 28

~8 ISPs

The paths change in all the hours. The largest delays do occur at ISP peering interfaces.
Inter-continent routing has longer and less stable round-trip delays, experiences more hops
and more frequent path changes, and goes through more ISPs than intra-continent routing.

The data and code are packed in a1p1p3.rar

4. WiFi is a wireless local area network technology, where user devices directly connects to access points within a few tens of meters which connects to the internet. 3G is a wireless wide are a network technology based on mobile phone networks, where user device directly connects to mobile communication broadcast towers. IMT-2000 specification (3G) requires peak data rates of at least 200 kbps. Bit rates in IEEE 802.11 standards (WiFi)

ranges from 1Mbps to 150Mbps, 54Mbps being the most frequent case as I observe. But since WiFi is a LAN technology the actual bit rate of internet access is further limited by the connection of the access point to the internet and how many users shares this internet connection, which makes the internet access bit rate for one user lower than the bit rate of her WiFi connection. WiFi access are often provided free of charge as a convenience because of its locality, but the internet access for the wireless access points is still charged for by ISPs, though not directly to the end users. A 3G internet connection is charged by the ISP, often at a higher price than wired connections of similar capacity. The hardware costs for the end users should be similar, for they are both widely adopted by today's consumer electronics. Of course, using 3G from a personal computer often requires a separately purchased mobile modem, since 3G is mainly a mobile phone technology. As for set-up costs, a 3G broadcast tower is obviously orders of magnitude more costly to set up than a WiFi access point, but the tower also covers much larger area and connects to much more users, so it's hard to compare. Because WiFi is one system (IEEE 802.11) with different versions, while 3G is actually two systems (UMTS and CDMA2000), roaming of 3G devices should be more problematic than that of WiFi devices. Also WiFi is just a LAN technology, as long as the devices are compatible, switching networks is not an issue and incurs no additional costs. Generally speaking 3G is more ubiquitous as it's rare to encounter a situation where you have a wireless LAN access but your cellphone fails to connect to the network, while the reversed situation is common.

5.

1) FTP. By capturing all ftp packets during logging (using known username and password) and searching for the password (“public”) in captured packets.

```
11  140.302619  59.78.18.58  202.120.2.2  FTP 67  Request: PASS public
```

2) Discuz! web forum system. By capturing all http packets during logging with known username and password, and then searching for the password (“afduaawey”) in captured packets.

```
formhash=096ac7ee&referer=http%3A%2F%2Fbbs.3dmgame.com
%2Findex.php&loginfield=username&username=aertasawrjf&password=afduaawey&questionid=0&answer=
```

3) Horde Web Email (mail.sjtu.edu.cn). By capturing all http packets during logging with known username and password(temporarily changed to “1111qqqq” for privacy), and subsequent searching in captured packets.

```
97  3.206920 59.78.18.58  202.112.26.39    HTTP 1124 POST /mail/login.php?nocache=2ttnnx6gjrgg
HTTP/1.1  (application/x-www-form-urlencoded)
url=&ie_version=8%2C0%2C6001%2C18702&horde_user=sdiyazg&horde_pass=1111qqqq&new_lang=zh_CN
```

This also exposes a problem that while jAccount logging info is encrypted, the same username and password is passed in plain text in SJTU mail service, which defeats the security measure taken in jAccount.

PART 2

1.

1.

```
eth0      Link encap:Ethernet  HWaddr 00:1E:4F:98:79:C2
          inet addr:192.168.1.14  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fec0::c:21e:4fff:fe98:79c2/64 Scope:Site
          inet6 addr: 2002:3ac4:9b29:c:21e:4fff:fe98:79c2/64 Scope:Global
          inet6 addr: fe80::21e:4fff:fe98:79c2/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:24646130 errors:0 dropped:115 overruns:0 frame:0
          TX packets:9195839 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2657934688 (2.4 GiB)  TX bytes:1331548007 (1.2 GiB)
          Memory:80200000-80220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2153061 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2153061 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:531194187 (506.5 MiB)  TX bytes:531194187 (506.5 MiB)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Link encap : link-layer interfaces exposed to implementations of network-layer protocols. Field values are self-explanatory.
HWaddr : Ethernet address of the network adapter.
inet addr : private network IPv4 address.
Bcast : subnet broadcast address.
Mask : subnet bitmask.
inet6 addr : IPv6 addresses.
Scope:Site : site-local IPv6 address
Scope:Link : link-local IPv6 address
Scope:Global : global IPv6 address
UP BROADCAST RUNNING MULTICAST LOOPBACK NOARP : state flags
MTU : the size of the largest packet that a network protocol can transmit.
Metric : a heuristic to help the IP protocol implementation decide which link-layer interface to use, which in this case is effectively disabled.
RX/TX packets : accumulated numbers of packets received/sent.
errors : number of checksum errors.
dropped : number of discarded packets.
overruns : number of buffer overruns.
txqueuelen : upper limit of numbers of queuing transmission packets.
RX/TX bytes : accumulated numbers of bytes received/sent.

2.

1.

/sbin/arp -a

```
node1 (192.168.1.15) at 00:1E:4F:98:9C:9F [ether] on eth0
node4 (192.168.1.18) at 00:1E:4F:98:9C:77 [ether] on eth0
```

```
? (192.168.1.100) at <incomplete> on eth0
? (192.168.1.1) at 00:0F:E2:3B:1C:49 [ether] on eth0
? (192.168.1.19) at 00:21:70:26:2E:7F [ether] on eth0
node2 (192.168.1.16) at 00:1E:4F:98:97:4E [ether] on eth0
node3 (192.168.1.17) at 00:1E:4F:97:45:CD [ether] on eth0

format:
    <hostname> (<IP address>) at <link-layer address> [<interface type>] on <interface name>
```

2. The shell returns:
   SIOCSARP: Operation not permitted
   That's because I haven't logged in as an administrator.
3. By sending packets to other hosts with new (private network) IP addresses, for example using traceroute.

```
node1 (192.168.1.15) at 00:1E:4F:98:9C:9F [ether] on eth0
? (192.168.1.3) at <incomplete> on eth0
? (192.168.1.2) at D8:5D:4C:36:B8:DA [ether] on eth0
? (192.168.1.4) at <incomplete> on eth0
? (192.168.1.10) at <incomplete> on eth0
node4 (192.168.1.18) at 00:1E:4F:98:9C:77 [ether] on eth0
? (192.168.1.1) at 00:0F:E2:3B:1C:49 [ether] on eth0
? (192.168.1.19) at 00:21:70:26:2E:7F [ether] on eth0
node2 (192.168.1.16) at 00:1E:4F:98:97:4E [ether] on eth0
? (192.168.1.13) at <incomplete> on eth0
node3 (192.168.1.17) at 00:1E:4F:97:45:CD [ether] on eth0
```

4. About 6 minutes.
   We need an unreachable private network IP.
   1) Ensure that such IP does not exist in the ARP table
   2) Ping the IP
   3) Check the ARP table, now the unreachable IP should be in the table
   4) Continuously query the ARP table until the unreachable IP disappears. We can also use bisection to find the timeout.
5. Since the destination IP is contained in the IP datagram, this should be a non-issue. In such situation the two hosts share a network adapter and both receive the packets sent to either one of them, just to discard packets with the destination IP of the other host. The source host simply sends packets with different destination IP fields to the same Ethernet address.

3. 1.

```
traceroute to tourism.at.ru (188.138.50.13), 100 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  4.730 ms  4.791 ms  4.842 ms
 2  202.120.40.126 (202.120.40.126)  3.670 ms  3.964 ms  4.332 ms
 3  10.22.1.253 (10.22.1.253)  3.334 ms  3.482 ms  3.788 ms
 4  10.3.2.77 (10.3.2.77)  4.027 ms  4.141 ms  4.399 ms
 5  10.3.0.46 (10.3.0.46)  4.513 ms  6.919 ms  7.025 ms
 6  10.3.0.50 (10.3.0.50)  132.299 ms  206.091 ms *
 7  * 202.120.201.198 (202.120.201.198)  72.701 ms  72.461 ms
 8  202.112.6.69 (202.112.6.69)  71.171 ms * *
 9  202.112.53.137 (202.112.53.137)  71.285 ms  70.900 ms  66.619 ms
10  202.112.36.37 (202.112.36.37)  72.670 ms * 202.112.36.37 (202.112.36.37)  72.379 ms
11  bj-11-p11-1.cernet.net (202.112.46.5)  89.592 ms  73.871 ms  73.492 ms
12  202.112.61.158 (202.112.61.158)  78.298 ms  86.220 ms  85.443 ms
13  202.112.61.14 (202.112.61.14)  86.150 ms  74.302 ms  73.684 ms
14  so-0-0-0.gw4.hkg3.asianetcom.net (203.192.137.197)  155.582 ms  202.355 ms  251.254 ms
15  * gi3-0-0.cr3.hkg3.asianetcom.net (203.192.134.65)  246.760 ms  299.494 ms
```

```
16  te0-2-2-0.wr2.hkg0.asianetcom.net (61.14.157.137)  167.432 ms  166.853 ms  166.490 ms
17  te0-1-0-0.wr2.osa0.asianetcom.net (61.14.157.5)  232.636 ms  191.551 ms  201.005 ms
18  te0-0-0-0.wr2.nrt0.asianetcom.net (61.14.157.1)  243.937 ms * te0-0-0-
0.wr2.nrt0.asianetcom.net (61.14.157.1)  243.829 ms
19  * gi14-0-0.gw3.lax1.asianetcom.net (61.14.157.94)  346.098 ms  345.529 ms
20  te0-0-0-0.gw1.lax3.asianetcom.net (202.147.61.154)  362.410 ms  362.393 ms  302.151 ms
21  * * *
22  te0-0-0-2.ccr22.lax01.atlas.cogentco.com (154.54.30.193)  496.891 ms * te0-0-0-
2.ccr22.lax01.atlas.cogentco.com (154.54.30.193)  577.005 ms
23  te0-3-0-6.ccr22.iah01.atlas.cogentco.com (154.54.3.185)  486.766 ms  486.765 ms te0-1-0-
3.ccr22.iah01.atlas.cogentco.com (154.54.44.253)  511.902 ms
24  te0-0-0-7.ccr22.atl01.atlas.cogentco.com (154.54.24.21)  519.019 ms te0-2-0-
2.ccr22.atl01.atlas.cogentco.com (154.54.42.214)  456.805 ms te0-0-0-
2.ccr22.atl01.atlas.cogentco.com (154.54.5.93)  525.662 ms
25  te0-0-0-7.ccr22.dca01.atlas.cogentco.com (154.54.28.221)  520.846 ms te0-4-0-
7.ccr22.dca01.atlas.cogentco.com (154.54.42.197)  541.993 ms te0-0-0-
7.ccr22.dca01.atlas.cogentco.com (154.54.28.221)  533.813 ms
26  te0-2-0-4.ccr22.fra03.atlas.cogentco.com (154.54.31.242)  456.237 ms  446.949 ms  485.787 ms
27  te1-1.ccr01.sxb01.atlas.cogentco.com (130.117.51.238)  479.952 ms  460.902 ms  459.759 ms
28  149.11.26.10 (149.11.26.10)  588.884 ms  540.931 ms  491.674 ms
29  static-ip-62-75-135-102.inaddr.ip-pool.com (62.75.135.102)  469.961 ms * static-ip-62-75-135-
102.inaddr.ip-pool.com (62.75.135.102)  505.806 ms
30  mail.j-vista.ru (188.138.50.13)  479.888 ms  406.943 ms  440.947 ms
```

Every packet has a TTL field which means after how many hops the router should refuse forwarding the packet and send an error message to the source. The traceroute utility sends packets with successively increased TTL field, starting from TTL = 1, and gets information about how packets are routed from the error messages received. The traceroute actually sends 3 packets for each TTL value. The first line of the output is the configuration of the tool, which says the tool is configured to send 40-byte long packets to the host 188.138.50.13, the domain name of which being tourism.at.ru, and stop sending packets if the packets it sends have reached 100 hops. The remaining lines each describes information collected from a 3-packet group sent with a particular TTL. The first field is the TTL, the second field is the IP address or domain name of the router which has sent the error message, the third field (in the parentheses) is the IP address of said router, the remaining three time values are the time from sending a packet to receiving the error message, in milliseconds, which becomes an asterisk in case the error message is not received in time.

2.

The trick is to traceroute to some reserved special IP address. Pinging random IP does not work because 1) the IPv4 address space is close to exhaustion and we are unlikely to hit an unallocated global IP, and 2) an IP being unreachable does not ensure the non-existence of an host with such IP since we could have simply hit some blocking mechanism like the GFW.

3.

```
traceroute to 198.18.0.14 (198.18.0.14), 30 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  4.373 ms  4.399 ms  4.461 ms
 2  202.120.40.126 (202.120.40.126)  3.610 ms  3.849 ms  4.099 ms
 3  10.22.1.253 (10.22.1.253)  3.202 ms  3.267 ms  3.421 ms
 4  10.3.2.77 (10.3.2.77)  3.671 ms  3.916 ms  4.162 ms
 5  10.3.0.46 (10.3.0.46)  6.197 ms  6.298 ms  6.424 ms
 6  10.3.0.50 (10.3.0.50)  95.865 ms  92.830 ms  92.871 ms
 7  202.120.201.198 (202.120.201.198)  51.755 ms  51.739 ms  51.271 ms
 8  202.112.6.69 (202.112.6.69)  45.696 ms  45.682 ms  45.776 ms
```

```
 9  sh0.cernet.net (202.112.53.89)  51.978 ms  48.247 ms  47.286 ms
10  202.112.36.37 (202.112.36.37)  54.433 ms  46.591 ms  54.283 ms
11  202.112.62.57 (202.112.62.57)  72.010 ms  85.590 ms  28.821 ms
12  202.112.61.158 (202.112.61.158)  49.071 ms  91.441 ms  91.351 ms
13  202.112.61.10 (202.112.61.10)  134.728 ms  133.586 ms  133.607 ms
14  202.112.61.18 (202.112.61.18)  130.691 ms  125.139 ms  137.464 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

4.

```
traceroute to 203.0.113.255 (203.0.113.255), 30 hops max, 40 byte packets
 1  192.168.1.1 (192.168.1.1)  4.501 ms  4.540 ms  4.591 ms
 2  202.120.40.126 (202.120.40.126)  3.598 ms  3.846 ms  4.230 ms
 3  10.22.1.253 (10.22.1.253)  3.306 ms  3.430 ms  3.680 ms
 4  10.3.2.77 (10.3.2.77)  3.928 ms  4.045 ms  4.289 ms
 5  10.3.0.46 (10.3.0.46)  6.413 ms  6.516 ms  6.640 ms
 6  10.3.0.50 (10.3.0.50)  123.017 ms  177.876 ms  247.614 ms
 7  202.120.201.198 (202.120.201.198)  53.631 ms  53.577 ms *
 8  * * *
 9  202.112.53.137 (202.112.53.137)  53.272 ms  49.223 ms  58.028 ms
10  202.112.36.37 (202.112.36.37)  56.915 ms * 202.112.36.37 (202.112.36.37)  57.014 ms
11  202.112.62.57 (202.112.62.57)  74.823 ms * *
12  * * 202.112.61.158 (202.112.61.158)  94.736 ms
13  202.112.61.10 (202.112.61.10)  90.151 ms  89.956 ms  90.906 ms
14  * 202.112.61.18 (202.112.61.18)  116.256 ms  115.468 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

5.

They all hit 202.112.61.18 and were unable to proceed further. Web search shows that the host 202.112.61.18 may be the host linking CERNET and the rest of the Internet.

4.

1.

Netstat prints information about the Linux networking subsystem, including network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

2.

--tcp -n

(to show only ESTABLISHED ones we need:

netstat --tcp -n | grep "ESTABLISHED"

but grep is not part of netstat)

printout:

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 192.168.1.14:703           192.168.1.14:636            TIME_WAIT
tcp        0      0 192.168.1.14:42968         192.168.1.14:111            TIME_WAIT
tcp        0      0 ::ffff:192.168.1.14:9001   ::ffff:192.168.1.15:34338   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.116:16259   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.187:4936    ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:116.237.245.14:15391 ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9001   ::ffff:192.168.1.17:57098   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9000   ::ffff:192.168.1.15:36637   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:202.120.40.69:24304  ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9001   ::ffff:192.168.1.18:43127   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.47:2712     ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:58.212.6.58:8223     ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:116.234.204.34:64254 ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.35:5050     ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:111.186.60.85:4379   ESTABLISHED
tcp        0   2144 ::ffff:192.168.1.14:22     ::ffff:111.186.60.85:2816   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9000   ::ffff:192.168.1.18:42816   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:222.70.39.109:3885   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.199:57521   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9001   ::ffff:192.168.1.16:55466   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:114.95.121.205:4820  ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.72:2091     ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.6:18256     ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.23:49744    ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:114.95.101.139:4269  ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9000   ::ffff:192.168.1.16:41205   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:58.37.106.145:27562  ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.26.137:52398   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:9000   ::ffff:192.168.1.17:51435   ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:58.25.4.87:1543      ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:202.120.40.69:24651  ESTABLISHED
tcp        0      0 ::ffff:192.168.1.14:22     ::ffff:59.78.23.143:5773    ESTABLISHED
```

Also the output has a self-explanatory header. “Proto” means the network protocol used, which are all TCP. “Recv-Q” and “Send-Q” refers to the number of packets queued up in buffers. “Local Address” and “Foreign Address” actually shows both IP addresses, which are IPv4-mapped IPv6 addresses here, and port numbers at the two ends of connections. “State” is just the state of the TCP connections.

3.

Display the kernel routing tables.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     *               255.255.255.0   U         0 0          0 eth0
169.254.0.0     *               255.255.0.0     U         0 0          0 eth0
default         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
```

4.

-i

printout: (2 Interfaces)

```
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
```

```
eth0      1500   0 24442148      0    115      0  9059035      0      0      0 BMRU
lo       16436   0  2136786      0      0      0  2136786      0      0      0 LRU
```

"lo" is used to emulate network connections between processes running on the local host. With the loopback interface, a process can communicate with another process using a unified interface (socket) no matter whether the two processes are running on the same computer or different ones.

5.

1.
   128.32.37.213
2.
   202.120.2.100
   It's a DNS server in SJTU.("上海交通大学 网络中心")
3.
   nslookup -type=mx hotmail.com ns1.msft.net
   It returns 4 (mx1.hotmail.com to mx4.hotmail.com) domain names, but nslookup to the 4 domain names returns the same result, which is:
   65.54.188.110
   65.54.188.126
   65.54.188.72
   65.54.188.94
   65.55.37.104
   65.55.37.120
   65.55.37.72
   65.55.37.88
   65.55.92.136
   65.55.92.152
   65.55.92.168
   65.55.92.184

   These IPs are of the mail exchangers of hotmail.com

6.

1.
   Shilie Weng
2.
   IST Communication and Network Services
3.
   Name: America Online Inc
   Phone: +1-703-265-4462
   Email: domains@aol.net

```
[5090209351@head ~]$ nslookup -type=mx aol.com
Server:         202.120.2.100
Address:        202.120.2.100#53

Non-authoritative answer:
aol.com mail exchanger = 15 mailin-02.mx.aol.com.
aol.com mail exchanger = 15 mailin-03.mx.aol.com.
aol.com mail exchanger = 15 mailin-04.mx.aol.com.
aol.com mail exchanger = 15 mailin-01.mx.aol.com.

Authoritative answers can be found from:
aol.com nameserver = dns-01.ns.aol.com.
aol.com nameserver = dns-02.ns.aol.com.
```

```
aol.com nameserver = dns-07.ns.aol.com.
aol.com nameserver = dns-06.ns.aol.com.
mailin-01.mx.aol.com    internet address = 205.188.159.42
mailin-01.mx.aol.com    internet address = 64.12.90.1
mailin-01.mx.aol.com    internet address = 64.12.90.98
mailin-01.mx.aol.com    internet address = 205.188.59.194
mailin-01.mx.aol.com    internet address = 205.188.146.193
mailin-02.mx.aol.com    internet address = 205.188.103.1
mailin-02.mx.aol.com    internet address = 205.188.190.1
mailin-02.mx.aol.com    internet address = 64.12.90.65
mailin-02.mx.aol.com    internet address = 64.12.139.193
mailin-03.mx.aol.com    internet address = 205.188.59.193
mailin-03.mx.aol.com    internet address = 205.188.156.193
mailin-03.mx.aol.com    internet address = 205.188.190.2
mailin-03.mx.aol.com    internet address = 64.12.90.33
mailin-03.mx.aol.com    internet address = 64.12.90.97

[5090209351@head ~]$ nslookup -type=mx aol.com dns-01.ns.aol.com
Server:         dns-01.ns.aol.com
Address:        64.12.51.132#53

aol.com mail exchanger = 15 mailin-01.mx.aol.com.
aol.com mail exchanger = 15 mailin-02.mx.aol.com.
aol.com mail exchanger = 15 mailin-03.mx.aol.com.
aol.com mail exchanger = 15 mailin-04.mx.aol.com.

[5090209351@head ~]$ nslookup mailin-01.mx.aol.com dns-01.ns.aol.com
Server:         dns-01.ns.aol.com
Address:        64.12.51.132#53

Name:   mailin-01.mx.aol.com
Address: 205.188.159.42
Name:   mailin-01.mx.aol.com
Address: 64.12.90.1
Name:   mailin-01.mx.aol.com
Address: 64.12.90.98
Name:   mailin-01.mx.aol.com
Address: 205.188.59.194
Name:   mailin-01.mx.aol.com
Address: 205.188.146.193

[5090209351@head ~]$ nslookup mailin-01.mx.aol.com dns-02.ns.aol.com
Server:         dns-02.ns.aol.com
Address:        205.188.157.232#53

Name:   mailin-01.mx.aol.com
Address: 205.188.59.194
Name:   mailin-01.mx.aol.com
Address: 205.188.146.193
Name:   mailin-01.mx.aol.com
Address: 205.188.159.42
Name:   mailin-01.mx.aol.com
Address: 64.12.90.1
Name:   mailin-01.mx.aol.com
Address: 64.12.90.98

[5090209351@head ~]$ nslookup mailin-02.mx.aol.com dns-02.ns.aol.com
Server:         dns-02.ns.aol.com
Address:        205.188.157.232#53

Name:   mailin-02.mx.aol.com
Address: 205.188.190.1
Name:   mailin-02.mx.aol.com
Address: 64.12.90.65
Name:   mailin-02.mx.aol.com
Address: 64.12.139.193
Name:   mailin-02.mx.aol.com
Address: 205.188.103.1
```

```
[5090209351@head ~]$ nslookup mailin-03.mx.aol.com dns-02.ns.aol.com
Server:         dns-02.ns.aol.com
Address:        205.188.157.232#53

Name:   mailin-03.mx.aol.com
Address: 64.12.90.97
Name:   mailin-03.mx.aol.com
Address: 205.188.59.193
Name:   mailin-03.mx.aol.com
Address: 205.188.156.193
Name:   mailin-03.mx.aol.com
Address: 205.188.190.2
Name:   mailin-03.mx.aol.com
Address: 64.12.90.33

[5090209351@head ~]$ nslookup mailin-04.mx.aol.com dns-02.ns.aol.com
Server:         dns-02.ns.aol.com
Address:        205.188.157.232#53

Name:   mailin-04.mx.aol.com
Address: 64.12.138.161
Name:   mailin-04.mx.aol.com
Address: 205.188.103.2
Name:   mailin-04.mx.aol.com
Address: 205.188.146.194
Name:   mailin-04.mx.aol.com
Address: 64.12.90.34
Name:   mailin-04.mx.aol.com
Address: 64.12.90.66

[5090209351@head ~]$ jwhois -h whois.arin.net 64.12.138.161
[Querying whois.arin.net]
[whois.arin.net]
#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 64.12.138.161"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=64.12.138.161?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       64.12.0.0 - 64.12.255.255
CIDR:           64.12.0.0/16
OriginAS:
NetName:        AOL-MTC
NetHandle:      NET-64-12-0-0-1
Parent:         NET-64-0-0-0-0
NetType:        Direct Assignment
RegDate:        1999-12-13
Updated:        1999-12-16
Ref:            http://whois.arin.net/rest/net/NET-64-12-0-0-1

OrgName:        America Online, Inc.
OrgId:          AMERIC-158
Address:        10600 Infantry Ridge Road
City:           Manassas
StateProv:      VA
PostalCode:     20109
Country:        US
RegDate:        1999-12-13
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/AMERIC-158

OrgTechHandle: CKN23-ARIN
OrgTechName:   No, Contact Known
```

```
OrgTechPhone:  +1-800-555-1234
OrgTechEmail:  nobody@example.com
OrgTechRef:    http://whois.arin.net/rest/poc/CKN23-ARIN

OrgAbuseHandle: AOL-NOC-ARIN
OrgAbuseName:   America Online Inc
OrgAbusePhone:  +1-703-265-4462
OrgAbuseEmail:  domains@aol.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/AOL-NOC-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#

[5090209351@head ~]$ jwhois -h whois.arin.net 205.188.103.2
[Querying whois.arin.net]
[whois.arin.net]
#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 205.188.103.2"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=205.188.103.2?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       205.188.0.0 - 205.188.255.255
CIDR:           205.188.0.0/16
OriginAS:
NetName:        AOL-DTC
NetHandle:      NET-205-188-0-0-1
Parent:         NET-205-0-0-0-0
NetType:        Direct Assignment
RegDate:        1998-04-18
Updated:        1998-04-27
Ref:            http://whois.arin.net/rest/net/NET-205-188-0-0-1

OrgName:        America Online, Inc
OrgId:          AMERIC-59
Address:        22080 Pacific Blvd
City:           Sterling
StateProv:      VA
PostalCode:     20166
Country:        US
RegDate:        1998-04-18
Updated:        2011-09-24
Ref:            http://whois.arin.net/rest/org/AMERIC-59

OrgTechHandle: CKN23-ARIN
OrgTechName:   No, Contact Known
OrgTechPhone:  +1-800-555-1234
OrgTechEmail:  nobody@example.com
OrgTechRef:    http://whois.arin.net/rest/poc/CKN23-ARIN

OrgAbuseHandle: AOL-NOC-ARIN
OrgAbuseName:   America Online Inc
OrgAbusePhone:  +1-703-265-4462
OrgAbuseEmail:  domains@aol.net
OrgAbuseRef:    http://whois.arin.net/rest/poc/AOL-NOC-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
```

The only valid contact information I can get is (America Online Inc,+1-703-265-4462,domains@aol.net). Although it is not clearly shown to be the coordinator, its name and email address imply so.

4.

It's some machine belonging to Innovative Logic Corp, but doesn't seem to have a domain name. Reverse DNS lookup returned empty result.