CSE 473 – Introduction to Computer Networks

Review Questions 7

Your Name:

Please print out this form (two-sided, if you can) and write your answers *legibly* in the spaces provided. If you can't write legibly, type.

1. Run `traceroute` network towards a handful of different destinations, preferably geographically distributed. (On Linux, the `traceroute` utility should be natively available. On Windows you should use `tracert`, on MAC OSX it should be available under Network Utility (usually in the utilities folder of the Applications folder).

   a) Carry out the experiment first from a computer connected to the university's network. What do you notice and what do the results imply?

   Performing `traceroute` to www.yahoo.com from guerin-Inspiron-530 yields

   guerin@guerin-Inspiron-530:~$ traceroute www.yahoo.com

   traceroute to atsv2-fp.wg1.b.yahoo.com (98.139.180.149), 64 hops max

   1 128.252.20.198 1.034ms 0.701ms 0.690ms

   2 128.252.1.137 1.206ms 0.911ms 0.992ms

   3 128.252.1.44 0.818ms 0.681ms 0.680ms

   4 128.252.100.126 1.446ms 1.292ms 1.256ms

   *5 * * **

   *6 * * **

   *7 * * **

   *8 * * **

   *9 * * **

   *10 * * **

   The subnet 128.252.0.0/16 belongs to Wash.U., and so the first four replies are from internal Wash. U. routers. There are no further replies beyond that, which seems to indicate filtering of ICMP messages by the WUSTL gateway/firewall. Similar outcomes can be observed for pretty much all external destinations.

   b) Repeat the experiment for the same set of destinations but now connected to your home network. How are the results different and what do they tell you?

```
$ tracert www.yahoo.com

Tracing route to ds-any-fp3-real.wa1.b.yahoo.com [98.139.183.24]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
```

```
  2     *        *        *     Request timed out.
  3    11 ms    10 ms     9 ms  dtr01ovldmo-tge-0-3-0-21.ovld.mo.charter.com
[96.34.52.121]
  4    11 ms    15 ms    15 ms  bbr01olvemo-bue-4.olve.mo.charter.com [96.34.2.18]
  5    19 ms    23 ms    23 ms  bbr02chcgil-bue-2.chcg.il.charter.com [96.34.0.12]
  6    18 ms    18 ms    20 ms  prr01chcgil-bue-4.chcg.il.charter.com [96.34.3.11]
  7    20 ms    24 ms    18 ms  ge-0-3-5.pat2.pao.yahoo.com [216.115.100.77]
  8    42 ms    42 ms    99 ms  ae-9.pat1.bfz.yahoo.com [216.115.101.159]
  9    44 ms    43 ms    44 ms  ae-3.msr1.bf1.yahoo.com [216.115.100.29]
 10    49 ms    46 ms    49 ms  xe-1-1-1.clr1-a-gdc.bf1.yahoo.com [98.139.128.9]
 11    49 ms    53 ms    55 ms  et-17-1.fab3-1-gdc.bf1.yahoo.com [98.139.128.41]
 12    52 ms    46 ms    49 ms  po-11.bas2-7-prd.bf1.yahoo.com [98.139.129.179]
 13    43 ms    45 ms    43 ms  ir2.fp.vip.bf1.yahoo.com [98.139.183.24]
```

```
$ tracert wwww.baidu.com

Tracing route to ps_other.a.shifen.com [123.125.114.144]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2     *        *        *     Request timed out.
  3    12 ms    10 ms    38 ms  dtr01ovldmo-tge-0-3-0-21.ovld.mo.charter.com
[96.34.52.121]
  4    11 ms    13 ms    19 ms  bbr01olvemo-bue-4.olve.mo.charter.com [96.34.2.18]
  5    12 ms    15 ms    15 ms  bbr01blvlil-bue-3.blvl.il.charter.com [96.34.0.15]
  6    30 ms    31 ms    31 ms  206.181.23.181
  7    57 ms    64 ms    59 ms  ae1d0.mcr2.marylandheights-mo.us.xo.net [216.156.1.90]
  8    70 ms    59 ms    64 ms  vb1721.rar3.denver-co.us.xo.net [216.156.0.181]
  9    66 ms    60 ms    62 ms  te0-13-0-0.rar3.la-ca.us.xo.net [207.88.12.86]
 10    58 ms     *      117 ms  207.88.13.81.ptr.us.xo.net [207.88.13.81]
 11    58 ms    59 ms    59 ms  219.158.39.45
 12   246 ms   239 ms   241 ms  219.158.102.101
 13   263 ms   269 ms   305 ms  219.158.19.197
 14   331 ms   331 ms   329 ms  219.158.23.21
 15   307 ms   277 ms   265 ms  219.158.101.117
 16   275 ms   256 ms   252 ms  123.126.0.10
 17   233 ms   231 ms   233 ms  123.126.6.114
 18   231 ms   254 ms   289 ms  202.106.43.38
 19     *        *        *     Request timed out.
 20   230 ms   235 ms     *     123.125.114.144
 21   260 ms   345 ms   349 ms  123.125.114.144
```

Note the time-out for the second hop, which probably indicates that this Charter router is filtering ICMP packets.

c) Finally, repeat the experiment but now using one of the `traceroute` servers that you can find listed at traceroute.org. Choose one located on a different continent and observe the differences.

From Global Crossing router in Kansas City

```
traceroute to www.yahoo.com (98.139.183.24), 30 hops max, 60 byte packets
 1  vl99.mag01.mci01.atlas.cogentco.com (66.250.250.17)  0.426 ms  0.434 ms
 2  te0-0-0-29.ccr22.mci01.atlas.cogentco.com (154.54.28.49)  0.569 ms  0.592
ms
 3  be2010.ccr22.dfw01.atlas.cogentco.com (154.54.46.218)  10.931 ms
be2012.ccr21.dfw01.atlas.cogentco.com (154.54.2.114)  11.048 ms
 4  be2031.ccr21.dfw03.atlas.cogentco.com (154.54.7.46)  11.238 ms  11.419 ms
 5  te2-1.mag01.dfw03.atlas.cogentco.com (154.54.83.178)  11.072 ms te2-
4.mag01.dfw03.atlas.cogentco.com (154.54.3.146)  11.069 ms
 6  yahoo.dfw03.atlas.cogentco.com (154.54.10.122)  11.091 ms  11.072 ms
 7  ae-5.pat2.che.yahoo.com (216.115.96.61)  43.034 ms *
```

```
 8  ae-9.pat2.bfz.yahoo.com (216.115.101.199)  51.722 ms ae-
8.pat1.bfz.yahoo.com (216.115.101.231)  45.096 ms
 9  ae-4.msr1.bf1.yahoo.com (216.115.100.25)  47.534 ms *
10  * *
11  et-17-1.fab1-1-gdc.bf1.yahoo.com (98.139.128.37)  46.127 ms et18-25.fab5-
1-sat.bf1.yahoo.com (98.139.128.101)  45.929 ms
12  po-16.bas2-7-prd.bf1.yahoo.com (98.139.130.3)  48.229 ms po-14.bas2-7-
prd.bf1.yahoo.com (98.139.129.227)  48.944 ms
13  * *
14  * *
```

Some information, but incomplete. Again because some of the routers on the path do ICMP filtering.

Trace route to www.baidu.com

```
Target IP address: 180.76.3.151
Source address:
Numeric display [n]: n
Timeout in seconds [3]: 1
Probe count [3]: 2
Minimum Time to Live [1]: 1
Maximum Time to Live [30]: 30
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 180.76.3.151
VRF info: (vrf in name/id, vrf out name/id)
  1 ae8-0-40G.scr4.LAX1.gblx.net (67.16.164.29) 44 msec 44 msec
  2 e5-2-70G.ar6.LAX1.gblx.net (67.16.132.214) 44 msec 44 msec
  3 HUTCHISON-GLOBAL-COMMUNICA.Port-channel2.469.ar4.LAX1.gblx.net (67.17.160.102) 44
msec 44 msec
  4 218.189.5.138 [AS 9304] 48 msec
    218.189.5.179 [AS 9304] 48 msec
  5 d1-45-224-143-118-on-nets.com (118.143.224.45) [AS 9304] 200 msec
    d1-49-224-143-118-on-nets.com (118.143.224.49) [AS 9304] 204 msec
  6 218.189.5.52 [AS 9304] 204 msec
    218.189.5.20 [AS 9304] 192 msec
  7 218.189.31.102 [AS 9304] 220 msec 216 msec
  8  *  *
  9  *  *
 10  *  *
```

Same comment as above.

From HiNet (Taiwan)

```
Translating "www.yahoo.com"...domain server (168.95.192.1) [OK]

Type escape sequence to abort.
Tracing the route to ds-tw-fp3.wg1.b.yahoo.com (202.43.192.109)

  1 TPDB-3516.hinet.net (210.65.161.22) 4 msec 0 msec 4 msec
  2 TPDT-3011.hinet.net (220.128.1.146) 4 msec 0 msec 0 msec
  3 TPDT-3301.hinet.net (220.128.3.149) 4 msec 0 msec 0 msec
  4 211.22.41.45 8 msec 0 msec 0 msec
  5 te-8-1.bas1-1-prd.tw1.yahoo.com (119.160.240.1) 4 msec
    te-8-1.bas2-1-prd.tw1.yahoo.com (119.160.240.3) 4 msec 0 msec
  6  *  *  *
  7  *  *  *
```

Traceroute Result (www.baidu.com) :

```
Type escape sequence to abort.
Tracing the route to www.a.shifen.com (180.76.3.151)

  1 TPDB-3516.hinet.net (210.65.161.22) 0 msec 0 msec 0 msec
  2 TPDT-3011.hinet.net (220.128.1.146) 0 msec 8 msec 0 msec
  3 r4104-s2.tp.hinet.net (220.128.3.97) 4 msec 0 msec 0 msec
  4 220-128-4-157.HINET-IP.hinet.net (220.128.4.157) 0 msec 0 msec
    r4004-s2.tp.hinet.net (220.128.4.37) 0 msec
  5 p16-3-3-1.r21.tkokhk01.hk.bb.gin.ntt.net (129.250.9.137) 24 msec 24 msec
24 msec
  6 as-1.r21.newthk02.hk.bb.gin.ntt.net (129.250.6.125) 24 msec 24 msec 28
msec
  7 ae-2.r02.newthk02.hk.bb.gin.ntt.net (129.250.3.11) 28 msec 24 msec 24
msec
  8 203.131.246.146 28 msec 28 msec 24 msec
  9  *  *  *
 10  *  *  *
```

2. Under what circumstances is the DHCP discover message required? In what common situation is it *not* required?

   A discover message is required when a host connects to a new network. It is not required when the host only seeks to renew its lease on its current IP address.

3. Consider the network on slide entitled "A Closer Look At NAT" (slide 21), and assume that a webserver is running on the host with address 10.0.0.2.

   What would be an appropriate entry in the NAT table at the router to facilitate external connectivity to the webserver?

   Given that webservers are expected to run on port 80, a reasonable choice would be an entry of the form <10.0.0.2,80:80>

   Suppose a remote host sent a packet intended for the web server? What would it use as the destination address and port number?

   The remote host would send its packet to <138.76.29.7,80>, assuming this is the first packet of a request for the server. If this is a subsequent packet, then the TCP connection setup would have specified another port at the server, which would then correspond to a different port number mapping in the NAT. For example, if the TCP connection was associated with <10.0.0.2:49567> on the server, then the NAT would have created a new mapping of the form <10.0.0.2,49567:uvwxy>, so that the (destination) port number specified in the incoming packet would have been uvwxy.

What destination address and port number would the router substitute when forwarding the packet on the local network?

Upon receiving the packet, the router would substitute 138.76.29.7 with 10.0.0.2, and keep the port number as 80 (assuming this the first packet and the webserver is indeed listening on port 80). If the packet was a subsequent packet after the establishment of the TCP connection, the port number would have been mapped to the value specified in the NAT's mapping table, i.e., the incoming port would have been uvwxy as per the previous example, and mapped to 49567.