Netwerken en systeembeveiliging
Assignment 2

Inge Becht

November 5, 2012

Task 1

1.ip from request: 192.168.2.10
ip from destination: 192.16.191.44

2. 2 packets. This because in the end twice a reply is sent by the destination host, and every time twice each intermediate host replies twice with an "TTL exceeded" message.

3. The computer sends out a ping request with Time To Live 1. When this message reaches a host (which is not the desired destination) the time to live decreases to 0 and the reached host sets out a "TTL exceeded message" which means the destination is not yet reached, and so another message needs to be send with an incremented Time To Live by 1. Now the request can make an extra hop towards the destination, but will be exceeded again if this second host is not yet the destination. This goes on until the destination is reached and a reply is sent. Each time a host sends back a "TTL exceeded" message the computer can calculate the length of the path so as to know the time to reach each hop.

4. 8 hops away in case hops consists of intermediate hosts and destination host.

5. The destination host is 147.102.222.213

6. UDP works the same way as ICMP but instead of sending a ping request it gives the possibility of choosing a source and destination port for the request.

7. After 19 hops the message is received from the destination host that the destination is not reachable.

Task 2

8. pingable:

www.facebook.com
www.cwi.nl
www.ntua.gr
www.twitter.com

Only www.mit.edu doens't respond. It could be the server does not respond to ping requests, or a proxy blocks the request.

9.

The last responding nodes is OC11-RTR-1-BACKBONE-2.MIT.EDU (18.168.1.41)

10. for facebook:

12.8ms
13.2ms
12.8ms

mean time 12.76 ms

for ntua.gr

51.7
51.5
51.5

mean time 51.56 ms

for cwi.nl:

0.855 ms
0.743 ms
0.731 ms

mean time 0.77 ms

There is quite a lot of difference between time for each host.
This could be explained by that the amount of hops for the ntua.gr is larger than the other two hosts, and thus more queueing delay could happen. This idea seems correct if you look at the nature of each host. ntua.gr takes longest as it is situated in greece, and facebook takes not as long because multiple ip adresses are available.

11.

For www.twitter.com a jump between 7 ms and 82 ms happen at:

```
xe-5-0-0.mpr1.lhr2.uk.above.net (64.125.24.77)  7.418 ms
xe-4-3-0.cr2.dca2.us.above.net (64.125.24.41)  82.134 ms
```

For www.mit.edu it is:

```
ae-48-48.ebr2.London1.Level3.net (4.69.143.82)  8.181 ms
ae-44-44.ebr1.NewYork1.Level3.net (4.69.137.78)  76.738 ms
```

So the increase starts when the router crosses from the UK to the US.
The jump in distance is quite big at that point until the next router which explains the sudden time increase.

12. The data:

```
ping -c 10 -s 8000 www.cwi.nl
PING www.cwi.nl (192.16.191.44) 8000(8028) bytes of data.
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=1 ttl=60 time=18.8 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=2 ttl=60 time=20.5 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=3 ttl=60 time=17.2 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=4 ttl=60 time=17.6 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=5 ttl=60 time=20.7 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=6 ttl=60 time=26.4 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=7 ttl=60 time=18.7 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=8 ttl=60 time=16.5 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=9 ttl=60 time=20.6 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=10 ttl=60 time=53.0 ms

--- www.cwi.nl ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 2.749/10.253/50.538/14.402 ms

ping -c 10 -s 8000 www.cwi.nl
PING www.cwi.nl (192.16.191.44) 8000(8028) bytes of data.
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=1 ttl=60 time=18.8 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=2 ttl=60 time=20.5 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=3 ttl=60 time=17.2 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=4 ttl=60 time=17.6 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=5 ttl=60 time=20.7 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=6 ttl=60 time=26.4 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=7 ttl=60 time=18.7 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=8 ttl=60 time=16.5 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=9 ttl=60 time=20.6 ms
8008 bytes from proxy2.cwi.nl (192.16.191.44): icmp_req=10 ttl=60 time=53.0 ms

--- www.cwi.nl ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 16.599/23.057/53.054/10.341 ms
```

In both cases there was no packet loss, but the average rtt difference is 10 ms. The propagation time for the second set of packets was higher.

task 3

13. The output for the traceroute from the Greece host to surfnet:

```
traceroute to www.surfnet.nl (145.0.2.10), 15 hops max, 52 byte packets
 1  * * *
 2  grnetRouter.ntua-primary.koletti-1.access-link.grnet.gr
         (194.177.209.117)  0.378 ms  0.369 ms  0.382 ms
 3  eie2-to-kol1.backbone.grnet.gr (195.251.27.54)  0.471 ms  0.579 ms  0.463 ms
 4  grnet.rt1.ath2.gr.geant.net (62.40.124.89)  0.525 ms  0.531 ms  0.538 ms
 5  so-4-2-0.rt1.mil.it.geant2.net (62.40.112.153)  28.986 ms  29.013 ms  28.994 ms
 6  as0.rt1.gen.ch.geant2.net (62.40.112.33)  36.396 ms  36.437 ms  36.406 ms
 7  so-4-0-0.rt1.fra.de.geant2.net (62.40.112.161)  44.194 ms  44.174 ms  44.188 ms
 8  so-4-0-0.rt1.ams.nl.geant2.net (62.40.112.10)  51.194 ms  51.190 ms  51.154 ms
 9  surfnet-gw.rt1.ams.nl.geant.net (62.40.124.158)  51.291 ms  51.295 ms  59.459 ms
10  AE2.500.JNR01.Asd001A.surf.net (145.145.80.78)  51.237 ms  51.222 ms  51.218 ms
11  V1131.sw4.amsterdam1.surf.net (145.145.19.170)  51.450 ms  51.392 ms  51.408 ms
12  www.surfnet.nl (145.0.2.10)  51.412 ms !Z  51.400 ms !Z  51.387 ms !Z
```

The traceroute link from Switzerland:

```
traceroute to www.surfnet.nl (145.0.2.10), 30 hops max, 60 byte packets
 1  swiCS5-V108.switch.ch (130.59.108.5)  0.306 ms  0.358 ms  0.430 ms
 2  swiZH2-10GE-3-1.switch.ch (130.59.36.138)  0.410 ms  0.503 ms  0.594 ms
 3  swiCE3-10GE-3-1.switch.ch (130.59.36.1)  36.782 ms * *
 4  switch-bckp.rt1.par.fr.geant.net (62.40.124.81)  12.878 ms  12.881 ms  12.873 ms
 5  as0.rt1.lon.uk.geant2.net (62.40.112.106)  20.365 ms  20.423 ms  20.465 ms
 6  as1.rt1.ams.nl.geant2.net (62.40.112.137)  28.365 ms  28.392 ms  28.360 ms
 7  surfnet-gw.rt1.ams.nl.geant.net (62.40.124.158)  31.192 ms  31.230 ms  31.275 ms
 8  AE2.500.JNR01.Asd001A.surf.net (145.145.80.78)  28.461 ms  28.482 ms  28.511 ms
 9  V1131.sw4.amsterdam1.surf.net (145.145.19.170)  28.629 ms  28.589 ms  28.640 ms
10  www.surfnet.nl (145.0.2.10)  28.577 ms !X  28.528 ms !X  28.512 ms !X
```

number of routes for the greek host: 1 route with 12 hops

number of Switzerland host: 1 route with 10 hops

average round trip delay to destination for Greece: 416.386 ms

average round trip delay to destination for Switzerland:216.19 ms

14. There are 3 links the same (4 in case you include de destination):

```
surfnet-gw.rt1.ams.nl.geant.net (62.40.124.158)
AE2.500.JNR01.Asd001A.surf.net (145.145.80.78)
V1131.sw4.amsterdam1.surf.net (145.145.19.170)
```

15. The biggest delay for the Greek host happens at the first contact with an Italian server. This is probably an important server spot that

handles a lot of packets.
The biggest delay for the Switzerland host happens at the first contact with ip 130.59.36.1. This is probably more because of a temporary malfunctioning server (as only 1 connection could be made instead of 3).

16. trace output from Australia to www.google.com:

```
 1  gigabitethernet3-3.exi1.melbourne.telstra.net (203.50.77.49)  0.440 ms  0.223 ms  0.24
 2  bundle-ether3.exi-core1.melbourne.telstra.net (203.50.80.1)  0.867 ms  2.362 ms  2.995
 3  bundle-ether12.chw-core2.sydney.telstra.net (203.50.11.74)  18.608 ms  23.474 ms  23.9
 4  bundle-ether1.chw48.sydney.telstra.net (203.50.6.154)  25.605 ms  23.476 ms  23.981 ms
 5  74.125.50.1 (74.125.50.1)  15.111 ms  15.105 ms  15.111 ms
 6  66.249.95.226 (66.249.95.226)  15.359 ms  15.355 ms  15.362 ms
 7  72.14.237.53 (72.14.237.53)  16.611 ms  16.603 ms  16.610 ms
 8  syd01s05-in-f19.1e100.net (74.125.237.51)  16.112 ms  16.104 ms  16.112 ms
```

    trace output from Switzerland to www.google.com:

```
traceroute to www.google.com (173.194.44.208), 30 hops max, 60 byte packets
 1  swiCS5-V108.switch.ch (130.59.108.5)  0.423 ms  0.507 ms  0.549 ms
 2  swiZH2-10GE-3-1.switch.ch (130.59.36.138)  4.292 ms  4.407 ms  4.494 ms
 3  swiIX1-10GE-3-3.switch.ch (130.59.36.129)  0.439 ms  0.437 ms  0.449 ms
 4  equinix-zurich.net.google.com (194.42.48.58)  62.291 ms  62.292 ms  62.284 ms
 5  209.85.243.127 (209.85.243.127)  1.183 ms  1.326 ms  1.469 ms
 6  173.194.44.208 (173.194.44.208)  0.720 ms  0.737 ms  0.724 ms
```

    There are no links the same. Google uses multiple ip addresses. Switzerland connects with Zurich and the Australian host ends up connecting to a router in Sydney

17. A packet is send 3 times by default when using traceroute. It seems that different routers were reached both times, which could be because of load-balancing.