CS433

Lab2

Bo Song

Part2

**2a.**

1. When send/receive packages to/from network. Set the ByteBuffer to Bigendian order.
2. According to the packet pair theory

where and are the arrival times of the first and second packets respectively at the destination, and are the transmission times of the first and second packets respectively, is the size of the second packet, and is the bandwidth of the bottleneck link.

My plan is to let client shoot two packages with client timestamp quickly. Under this circumstance, is neglectable. Bandwidth is

1. Yes.
   1. Client stamps current local time on the request packet and sends to server.
   2. Upon receipt by server, server stamps server-time and returns.
   3. Upon receipt by client, client subtracts current time from sent time and divides by two to compute latency. It subtracts current time from server time to determine client-server time delta and adds in the half-latency to get the correct clock delta.

Reference: <http://www.mine-control.com/zack/timesync/timesync.html>

* 1. Repeat for several times, pick up the median delay time to do the synchronization.

Accuracy may be range -150~150ms

**2b**

1. It doesn’t work because the server must use different identification number to differentiate and pair request and response.
2. request coming rate (number of coming requests per second). N is the buffer size.
3. First search d, then search c, then search b, finally search a

**2c**

1. Flood attack the local DNS server of the target country, so that the local DNS server of the country can’t response to normal requests. Or we can pollute DNS server to let it return wrong IP address.

**3a**

dig +norecurse @a.root-servers.net cicada.cs.yale.edu A

dig +norecurse @a.edu-servers.net cicada.cs.yale.edu A

dig +norecurse @serv1.net.yale.edu cicada.cs.yale.edu A

Yes. Server yale-server.uchicago.edu is a backup DNS server for Yale in University of Chicago

cicada.zoo.cs.yale.edu.

128.36.232.5

-bash-4.2$ dig +norecurse @a.root-servers.net cicada.cs.yale.edu A

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7\_2.2 <<>> +norecurse @a.root-servers.net cicada.cs.yale.edu A

; (2 servers found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37047

;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 8

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 1472

;; QUESTION SECTION:

;cicada.cs.yale.edu. IN A

;; AUTHORITY SECTION:

edu. 172800 IN NS a.edu-servers.net.

edu. 172800 IN NS c.edu-servers.net.

edu. 172800 IN NS d.edu-servers.net.

edu. 172800 IN NS f.edu-servers.net.

edu. 172800 IN NS g.edu-servers.net.

edu. 172800 IN NS l.edu-servers.net.

;; ADDITIONAL SECTION:

a.edu-servers.net. 172800 IN A 192.5.6.30

c.edu-servers.net. 172800 IN A 192.26.92.30

d.edu-servers.net. 172800 IN A 192.31.80.30

f.edu-servers.net. 172800 IN A 192.35.51.30

g.edu-servers.net. 172800 IN A 192.42.93.30

l.edu-servers.net. 172800 IN A 192.41.162.30

g.edu-servers.net. 172800 IN AAAA 2001:503:cc2c::2:36

;; Query time: 14 msec

;; SERVER: 198.41.0.4#53(198.41.0.4)

;; WHEN: Sun Feb 14 20:56:43 EST 2016

;; MSG SIZE rcvd: 282

-bash-4.2$ dig +norecurse @a.edu-servers.net cicada.cs.yale.edu A

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7\_2.2 <<>> +norecurse @a.edu-servers.net cicada.cs.yale.edu A

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2759

;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 5, ADDITIONAL: 6

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;cicada.cs.yale.edu. IN A

;; AUTHORITY SECTION:

yale.edu. 172800 IN NS serv1.net.yale.edu.

yale.edu. 172800 IN NS serv2.net.yale.edu.

yale.edu. 172800 IN NS serv4.net.yale.edu.

yale.edu. 172800 IN NS serv3.net.yale.edu.

yale.edu. 172800 IN NS yale-server.uchicago.edu.

;; ADDITIONAL SECTION:

serv1.net.yale.edu. 172800 IN A 130.132.1.9

serv2.net.yale.edu. 172800 IN A 130.132.1.10

serv4.net.yale.edu. 172800 IN A 130.132.89.9

serv3.net.yale.edu. 172800 IN A 130.132.1.11

yale-server.uchicago.edu. 172800 IN A 128.135.249.140

;; Query time: 33 msec

;; SERVER: 192.5.6.30#53(192.5.6.30)

;; WHEN: Sun Feb 14 20:59:55 EST 2016

;; MSG SIZE rcvd: 246

-bash-4.2$ dig +norecurse @serv1.net.yale.edu cicada.cs.yale.edu A

; <<>> DiG 9.9.4-RedHat-9.9.4-29.el7\_2.2 <<>> +norecurse @serv1.net.yale.edu cicada.cs.yale.edu A

; (1 server found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38508

;; flags: qr aa ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;cicada.cs.yale.edu. IN A

;; ANSWER SECTION:

cicada.cs.yale.edu. 10800 IN CNAME cicada.zoo.cs.yale.edu.

cicada.zoo.cs.yale.edu. 10800 IN A 128.36.232.5

;; AUTHORITY SECTION:

zoo.cs.yale.edu. 10800 IN NS serv1.net.yale.edu.

zoo.cs.yale.edu. 10800 IN NS serv2.net.yale.edu.

zoo.cs.yale.edu. 10800 IN NS serv3.net.yale.edu.

zoo.cs.yale.edu. 10800 IN NS serv4.net.yale.edu.

;; ADDITIONAL SECTION:

serv1.net.yale.edu. 10800 IN A 130.132.1.9

serv2.net.yale.edu. 10800 IN A 130.132.1.10

serv3.net.yale.edu. 10800 IN A 130.132.1.11

serv4.net.yale.edu. 10800 IN A 130.132.89.9

;; Query time: 0 msec

;; SERVER: 130.132.1.9#53(130.132.1.9)

;; WHEN: Sun Feb 14 21:01:07 EST 2016

;; MSG SIZE rcvd: 236

**3b**

dig MX gmail.com +short

40 alt4.gmail-smtp-in.l.google.com.

5 gmail-smtp-in.l.google.com.

10 alt1.gmail-smtp-in.l.google.com.

20 alt2.gmail-smtp-in.l.google.com.

30 alt3.gmail-smtp-in.l.google.com.

dig A alt4.gmail-smtp-in.l.google.com +short

173.194.65.27

Dig A gmail-smtp-in.l.google.com +short

173.194.68.27

Dig A alt1.gmail-smtp-in.l.google.com +short

64.233.190.27

**3c**

Dig txt gmail.com +short

Dig txt \_spf.google.com +short

Dig txt \_netblocks.gmail.com +short

"v=spf1 ip4:64.18.0.0/20 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20 ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:207.126.144.0/20 ip4:209.85.128.0/17 ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all"

173.194.1.1 is within the subnet 173.194.0.0/16

So it is an authorized mail transfer agent for gmail.