report.md

Lab03 Report - z5117408

Exercise 3

Q1

- 150.203.161.98, it was a request for an address record ('A' record query type)

Q2

- rproxy.cecs.anu.edu.au. is the CNAME given. If they need to change the underlying IP address then they need only do it for this one address. All other CNAMES will still resolve down to this one address and wont need to be changed.

Q3

```
$ dig www.cecs.anu.edu.au

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43626
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    1467    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1467    IN      A       150.203.161.98

;; AUTHORITY SECTION:
edu.au.                 72071   IN      NS      t.au.
edu.au.                 72071   IN      NS      s.au.
edu.au.                 72071   IN      NS      r.au.
edu.au.                 72071   IN      NS      q.au.

;; ADDITIONAL SECTION:
q.au.                   12642   IN      A       65.22.196.1
q.au.                   18686   IN      AAAA    2a01:8840:be::1
r.au.                   7374    IN      A       65.22.197.1
r.au.                   12909   IN      AAAA    2a01:8840:bf::1
s.au.                   588     IN      A       65.22.198.1
s.au.                   4982    IN      AAAA    2a01:8840:c0::1
t.au.                   16109   IN      A       65.22.199.1
t.au.                   6950    IN      AAAA    2a01:8840:c1::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Oct 13 13:51:30 AEDT 2019
;; MSG SIZE  rcvd: 325
```

- the authority section seems to be listing the authority name servers for this request, the additional section is then showing the ipv4/v6 addresses for these name servers

Q4

- SERVER: 127.0.0.53#53(127.0.0.53)

Q5

```
cecs.anu.edu.au.        3431    IN      NS      ns3.cecs.anu.edu.au. (ip address = 150.203.161.50)
cecs.anu.edu.au.        3431    IN      NS      ns2.cecs.anu.edu.au. (ip address = 150.203.161.36)
cecs.anu.edu.au.        3431    IN      NS      ns4.cecs.anu.edu.au. (ip address = 150.203.161.38)
```

- NS (name server) query for getting the nameservers, A (address) for the ip addresses

Q6

```
54.101.68.111.in-addr.arpa. 3600 IN     PTR     webserver.seecs.nust.edu.pk.
```

- this webserver name. The query type is PTR.

Q7

```
dig @129.94.242.33 yahoo.com MX

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 6374
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; Query time: 20 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Oct 13 13:45:43 AEDT 2019
;; MSG SIZE  rcvd: 38
```

- the request is refused when using the CSE nameserver at home?

```
dig @129.94.242.33 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40773
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1111    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1111    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1111    IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              1094    IN      NS      ns5.yahoo.com.
yahoo.com.              1094    IN      NS      ns1.yahoo.com.
yahoo.com.              1094    IN      NS      ns4.yahoo.com.
yahoo.com.              1094    IN      NS      ns3.yahoo.com.
yahoo.com.              1094    IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          336007  IN      A       68.180.131.16
ns1.yahoo.com.          15639   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          100642  IN      A       68.142.255.16
ns2.yahoo.com.          9157    IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          105     IN      A       27.123.42.42
```

```
ns3.yahoo.com.          105     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          160083  IN      A       98.138.11.157
ns5.yahoo.com.          163281  IN      A       119.160.253.83

;; Query time: 1 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Oct 13 13:48:54 AEDT 2019
;; MSG SIZE  rcvd: 371
```

- I'm assuming the response i got back did not come from one of the authoritative name servers listed, but instead the local (to cse) DNS cache server because of the instant query time;

```
;; Query time: 0 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
```

- also, the flags do not contain "aa" which would indicate a authoritative response

Q8

- the query is refused both on my local machine and the cse machine. I'm assuming this is because they are authoritative for the web server provieded in q5 and NOT authoratative for these yahoo mail servers.

```
dig @150.203.161.50 yahoo.com MX

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>> @150.203.161.50 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 65308
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: f5cd626f99fd019c613a2ca15da29b3d44e9d145e6232187 (good)
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; Query time: 23 msec
;; SERVER: 150.203.161.50#53(150.203.161.50)
;; WHEN: Sun Oct 13 14:34:20 AEDT 2019
;; MSG SIZE  rcvd: 66
```

Q9

- first I obtained the authoritative NS for yahoo.com with "dig yahoo.com NS". This gave ns[1/2/3/4].yahoo.com.
- then I just specified to use #4 for the look-up

```
dig @ns4.yahoo.com. yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @ns4.yahoo.com. yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26893
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1272
;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta5.am0.yahoodns.net.
```

```
;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          1209600 IN      A       68.180.131.16
ns2.yahoo.com.          1209600 IN      A       68.142.255.16
ns3.yahoo.com.          1800    IN      A       27.123.42.42
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          1209600 IN      A       119.160.253.83
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1800    IN      AAAA    2406:8600:f03f:1f8::1003

;; Query time: 197 msec
;; SERVER: 98.138.11.157#53(98.138.11.157)
;; WHEN: Sun Oct 13 14:41:13 AEDT 2019
;; MSG SIZE  rcvd: 371
```

- it is an MX query

Q10

- wagner.cse.unsw.edu.au. 3600 IN A 129.94.242.19
- the amount of names in the dot.separate.name, + 1 for root (.) and then possibly +1 to get an uncached final answer. In my case it took me 6

Q11

- Yes, network cards are able to have multiple ip addresses associated with them. This is helpful for virtualising servers (i.e. more than one server on the one physical machine). Furthermore, you could argue that ipv4 and ipv6 is two for the one machine anyways without the above fact. It is of course possible to have multiple names for the same machine as well, either by adding multiple A type records for it, or by adding CNAMEs for existing A records.

Exercise 4

- using python3