COMP9331 LAB3 – DNS

Changfeng LI(z5137858)

Exercise 1,2: (not needed in the report)

Exercise 3: Digging into DNS

Qs3-1: What is the IP address of www.cecs.anu.edu.au . What type of DNS query is sent to get this answer?
Qs3-2: What is the canonical name for the CECS ANU web server? What is its IP address? Suggest a reason for having an alias for this server.
Qs3-3: What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?
Qs3-4: What is the IP address of the local nameserver for your machine?
Qs3-5: What are the DNS nameservers for the "cecs.anu.edu.au" domain (note: the domain name is cecs.anu.edu.au and not www.cecs.anu.edu.au)? Find out their IP addresses? What type of DNS query is sent to obtain this information?
Qs3-6: What is the DNS name associated with the IP address 149.171.158.109? What type of DNS query is sent to obtain this information?
Qs3-7: Run dig and query the CSE nameserver (129.94.242.33) for the mail servers for Yahoo! Mail (again the domain name is yahoo.com, not www.yahoo.com). Did you get an authoritative answer? Why? (HINT: Just because a response contains information in the authoritative part of the DNS response message does not mean it came from an authoritative name server. You should examine the flags in the response to determine the answer)
Qs3-8: Repeat the above (i.e. Question 7) but use one of the nameservers obtained in 3-5, What is the result?
Qs3-9: Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?
Qs3-10: In this exercise you simulate the iterative DNS query process to find the IP address of your machine (e.g. lyre00.cse.unsw.edu.au). First, find the name server (query type NS) of the "." domain (root domain). Query this nameserver to find the authoritative name server for the "au." domain. Query this second server to find the authoritative nameserver for the "edu.au." domain. Now query this nameserver to find the authoritative nameserver for "unsw.edu.au". Next query the nameserver of unsw.edu.au to find the authoritative name server of cse.unsw.edu.au. Now query the nameserver of cse.unsw.edu.au to find the IP address of your host. How many DNS servers do you have to query to get the authoritative answer?
Qs3-11: Can one physical machine have several names and/or IP addresses associated with it?

As3-1:

```
lichangfengdeMacBook-Pro:lab3 windfall$ dig www.cecs.anu.edu.au

; <<>> DiG 9.8.3-P1 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53729
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;www.cecs.anu.edu.au.           IN      A

;; ANSWER SECTION:
www.cecs.anu.edu.au.    2920    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1921    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        1120    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        1120    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        1120    IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    1120    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    1120    IN      AAAA    2001:388:1034:2905::24
ns4.cecs.anu.edu.au.    1276    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    1120    IN      AAAA    2001:388:1034:2905::26
ns3.cecs.anu.edu.au.    1120    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    1120    IN      AAAA    2001:388:1034:2905::32

;; Query time: 25 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 17:29:10 2018
;; MSG SIZE  rcvd: 260
```

The IP Address is 150.203.161.98, and of Type A.

As3-2: We can find info from CNAME area that it is “rproxy.cecs.anu.edu.au”.

```
;; ANSWER SECTION:
rproxy.cecs.anu.edu.au. 368     IN      A       150.203.161.98
```

The IP address is 150.203.161.98 the same.
The main reason why this server has an alias is that it is the website for university, so the alias can help people remember it.

As3-3:
The Authority section indicates the server(s) that are the ultimate authority for answering DNS queries about that domain.
The Additional sections give the information of which DNS servers provide this authoritative answers and shows their IP.

As3-4:
129.94.0.196

As3-5:

The DNS server are listed below:
ns2.cecs.anu.edu.au. => 150.203.161.36
ns4.cecs.anu.edu.au. => 150.203.161.38
ns3.cecs.anu.edu.au. => 150.203.161.50
Type: NS

As3-6:

As3-7:

```
lichangfengdeMacBook-Pro:lab3 windfall$ dig 129.94.242.33 yahoo.com MX

; <<>> DiG 9.8.3-P1 <<>> 129.94.242.33 yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 14366
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;129.94.242.33.                 IN      A

;; AUTHORITY SECTION:
.                       10689   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2018080900 1800 900 604800 86400

;; Query time: 46 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:09:52 2018
;; MSG SIZE  rcvd: 106

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10582
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1258    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1258    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1258    IN      MX      1 mta7.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              154966  IN      NS      ns2.yahoo.com.
yahoo.com.              154966  IN      NS      ns3.yahoo.com.
yahoo.com.              154966  IN      NS      ns4.yahoo.com.
yahoo.com.              154966  IN      NS      ns1.yahoo.com.
yahoo.com.              154966  IN      NS      ns5.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          395906  IN      A       68.180.131.16
ns1.yahoo.com.          145224  IN      AAAA    2001:4998:130::1001
ns4.yahoo.com.          68346   IN      A       98.138.11.157
ns3.yahoo.com.          143826  IN      A       203.84.221.53
ns3.yahoo.com.          68858   IN      AAAA    2406:8600:b8:fe03::1003
ns2.yahoo.com.          474580  IN      A       68.142.255.16
ns2.yahoo.com.          135222  IN      AAAA    2001:4998:140::1002
ns5.yahoo.com.          68346   IN      A       119.160.253.83

;; Query time: 15 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:09:52 2018
;; MSG SIZE  rcvd: 360
```

No, because I don’t find AA section, which means authoritative answers.

As3-8:

```
lichangfengdeMacBook-Pro:lab3 windfall$ dig 150.203.161.36 yahoo.com MX

; <<>> DiG 9.8.3-P1 <<>> 150.203.161.36 yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 35850
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;150.203.161.36.                        IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2018080900 1800 900 604800 86400

;; Query time: 68 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:17:36 2018
;; MSG SIZE  rcvd: 107

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57626
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              1679    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1679    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1679    IN      MX      1 mta7.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              76934   IN      NS      ns1.yahoo.com.
yahoo.com.              76934   IN      NS      ns5.yahoo.com.
yahoo.com.              76934   IN      NS      ns4.yahoo.com.
yahoo.com.              76934   IN      NS      ns2.yahoo.com.
yahoo.com.              76934   IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns4.yahoo.com.          59838   IN      A       98.138.11.157
ns3.yahoo.com.          419922  IN      A       203.84.221.53
ns3.yahoo.com.          66267   IN      AAAA    2406:8600:b8:fe03::1003
ns5.yahoo.com.          45902   IN      A       119.160.253.83
ns1.yahoo.com.          76873   IN      A       68.180.131.16
ns1.yahoo.com.          76934   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          148779  IN      A       68.142.255.16
ns2.yahoo.com.          55081   IN      AAAA    2001:4998:140::1002

;; Query time: 17 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:17:36 2018
;; MSG SIZE  rcvd: 360
```

As3-9:

Firstly, we dig yahoo.com, we get

```
lichangfengdeMacBook-Pro:lab3 windfall$ dig yahoo.com

; <<>> DiG 9.8.3-P1 <<>> yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27702
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      A

;; ANSWER SECTION:
yahoo.com.              300     IN      A       98.137.246.8
yahoo.com.              300     IN      A       72.30.35.10
yahoo.com.              300     IN      A       72.30.35.9
yahoo.com.              300     IN      A       98.137.246.7
yahoo.com.              300     IN      A       98.138.219.231
yahoo.com.              300     IN      A       98.138.219.232

;; AUTHORITY SECTION:
yahoo.com.              76775   IN      NS      ns1.yahoo.com.
yahoo.com.              76775   IN      NS      ns5.yahoo.com.
yahoo.com.              76775   IN      NS      ns2.yahoo.com.
yahoo.com.              76775   IN      NS      ns3.yahoo.com.
yahoo.com.              76775   IN      NS      ns4.yahoo.com.

;; ADDITIONAL SECTION:
ns4.yahoo.com.          59679   IN      A       98.138.11.157
ns3.yahoo.com.          419763  IN      A       203.84.221.53
ns3.yahoo.com.          66108   IN      AAAA    2406:8600:b8:fe03::1003
ns5.yahoo.com.          45743   IN      A       119.160.253.83
ns1.yahoo.com.          76714   IN      A       68.180.131.16
ns1.yahoo.com.          76775   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          148620  IN      A       68.142.255.16
ns2.yahoo.com.          54922   IN      AAAA    2001:4998:140::1002

;; Query time: 67 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:20:15 2018
;; MSG SIZE  rcvd: 377
```

Then we send MX query, we get

```
lichangfengdeMacBook-Pro:lab3 windfall$ dig 68.180.131.16 yahoo.com MX

; <<>> DiG 9.8.3-P1 <<>> 68.180.131.16 yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 62861
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;68.180.131.16.                 IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2018080900 1800 900 604800 86400

;; Query time: 39 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:22:08 2018
;; MSG SIZE  rcvd: 106

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7264
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

;; QUESTION SECTION:
;yahoo.com.                     IN      MX

;; ANSWER SECTION:
yahoo.com.              522     IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              522     IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              522     IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              154230  IN      NS      ns2.yahoo.com.
yahoo.com.              154230  IN      NS      ns1.yahoo.com.
yahoo.com.              154230  IN      NS      ns4.yahoo.com.
yahoo.com.              154230  IN      NS      ns5.yahoo.com.
yahoo.com.              154230  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          395170  IN      A       68.180.131.16
ns1.yahoo.com.          144488  IN      AAAA    2001:4998:130::1001
ns4.yahoo.com.          67610   IN      A       98.138.11.157
ns3.yahoo.com.          143090  IN      A       203.84.221.53
ns3.yahoo.com.          68122   IN      AAAA    2406:8600:b8:fe03::1003
ns2.yahoo.com.          473844  IN      A       68.142.255.16
ns2.yahoo.com.          134486  IN      AAAA    2001:4998:140::1002
ns5.yahoo.com.          67610   IN      A       119.160.253.83

;; Query time: 17 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:22:08 2018
;; MSG SIZE  rcvd: 360
```

As3-10:

```
lichangfengdeMacBook-Pro:lab3 windfall$ dig . NS

; <<>> DiG 9.8.3-P1 <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20492
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       153807  IN      NS      m.root-servers.net.
.                       153807  IN      NS      c.root-servers.net.
.                       153807  IN      NS      g.root-servers.net.
.                       153807  IN      NS      f.root-servers.net.
.                       153807  IN      NS      b.root-servers.net.
.                       153807  IN      NS      j.root-servers.net.
.                       153807  IN      NS      i.root-servers.net.
.                       153807  IN      NS      a.root-servers.net.
.                       153807  IN      NS      d.root-servers.net.
.                       153807  IN      NS      k.root-servers.net.
.                       153807  IN      NS      h.root-servers.net.
.                       153807  IN      NS      e.root-servers.net.
.                       153807  IN      NS      l.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     67433   IN      A       198.41.0.4
a.root-servers.net.     117537  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     502558  IN      A       199.9.14.201
b.root-servers.net.     54890   IN      AAAA    2001:500:200::b
c.root-servers.net.     486890  IN      A       192.33.4.12
c.root-servers.net.     54890   IN      AAAA    2001:500:2::c
d.root-servers.net.     312571  IN      A       199.7.91.13
d.root-servers.net.     54890   IN      AAAA    2001:500:2d::d
e.root-servers.net.     504927  IN      A       192.203.230.10
e.root-servers.net.     54890   IN      AAAA    2001:500:a8::e
f.root-servers.net.     586840  IN      A       192.5.5.241
f.root-servers.net.     54890   IN      AAAA    2001:500:2f::f
g.root-servers.net.     593465  IN      A       192.112.36.4

;; Query time: 60 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Aug  9 20:25:53 2018
;; MSG SIZE  rcvd: 508
```

1. dig @198.41.0.4 lyre00.cse.unsw.edu.au .au Authoritative NS
2. dig @58.65.254.73 lyre00.cse.unsw.edu.au .edu.au Authoritative NS
3. dig @37.209.192.5 lyre00.cse.unsw.edu.au .unsw.edu.au Authoritative NS
4. dig @129.94.0.192 lyre00.cse.unsw.edu.au .cse.unsw.edu.au Authoritative NS
5. dig @129.94.242.2 lyre00.cse.unsw.edu.au lyre100.cse.unsw.edu.au A record

IP of my machine: 129.94.210.20

As3-11:

In most cases, a physical device have a corresponding name and a corresponding IP address, but we can configure so that it will have multiple name and address. To some extent, an IP always has multiple name for different usages, that's "alias".

Exercise 4: (Code only)