LAB 3
z5115237

Exercise 1:

DNS record types

A - Address record, returns a 32-bit IPv4 address, most commonly used to map host names to an IP address of the host

CNAME - Canonical name record, Alias of one name to another. The DNS lookup will continue by retrying the lookup with the new name

MX - Mail exchange record, maps a domain name to a list of message transfer agents for that domain

NS - Name server record, Delegates a DNS zone to use the given authoritative name servers

PTR - Pointer record, pointer to a canonical name. Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing reverse DNS lookups.

SOA - Start of authority record, specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone

AAAA - IPv6 address record, returns a 128-bit IPv6 address, most commonly used to map host names to an IP address of the host

Exercise 2:

1. The IP address of cecs.anu.edu.au is 150.203.161.98. An 'A' query was sent to get this answer as this type of query maps host names to an IP address of the host.

2. The canonical name for the CECS ANU web server is www.cecs.anu.edu.au. This is evident from the CNAME query of rproxy.cecs.anu.edu.au. The IP address is also 150.203.161.98 as both names are connected to the same IP. A reason for having the alias www.cecs.anu.edu.au is that users may have trouble remembering rproxy as the prefix of the URL. Hence this is replaced with the well-known 'www' used in most URLs, in which most users know. This is done through 'NS' DNS queries

3. The Authority section on the response lists the authoritative servers in the domain. This means that ns1,ns2,ns3,ns4 are other servers used to help the host with other queries, etc. The Additional section gives the IP addresses of these authoritative servers in both IPv4 and IPv6 using 'A' and 'AAAA' DNS queries.

4. The IP address of the local name server is 129.94.208.3. This is found at the bottom of the dig response.

5. The DNS name servers for the 'cecs.anu.edu.au' domain are (ns1,ns2,ns3,ns4).cecs.anu.edu.au. There IP addresses are 150.203.161.(4,36,50,38). A 'NS' query is sent to obtain this information, which is the name server record.

```
; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61386
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 8

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    3503    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 1114    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        951     IN      NS      ns1.cecs.anu.edu.au.
cecs.anu.edu.au.        951     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        951     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        951     IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns1.cecs.anu.edu.au.    2516    IN      A       150.203.161.4
ns1.cecs.anu.edu.au.    2066    IN      AAAA    2001:388:1034:2905::4
ns2.cecs.anu.edu.au.    136     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    951     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    136     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    951     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    136     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    951     IN      AAAA    2001:388:1034:2905::26

;; Query time: 0 msec
;; SERVER: 129.94.208.3#53(129.94.208.3)
;; WHEN: Fri Aug 18 12:21:03 2017
;; MSG SIZE  rcvd: 322
```

6. The DNS name associated with the IP address 149.171.158.109 is engineering.unsw.edu.au. The 'PTR' DNS query is used to find this information, which is the reverse of the 'A' queries.

```
; <<>> DiG 9.7.3 <<>> -x 149.171.158.109
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53644
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;109.158.171.149.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
109.158.171.149.in-addr.arpa. 545 IN    PTR     engplws008.ad.unsw.edu.au.
109.158.171.149.in-addr.arpa. 545 IN    PTR     www.engineering.unsw.edu.au.

;; AUTHORITY SECTION:
158.171.149.in-addr.arpa. 7745  IN      NS      ns3.unsw.edu.au.
```

```
158.171.149.in-addr.arpa. 7745  IN      NS      ns2.unsw.edu.au.
158.171.149.in-addr.arpa. 7745  IN      NS      ns1.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        797     IN      A       129.94.0.192
ns1.unsw.edu.au.        165     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        797     IN      A       129.94.0.193
ns2.unsw.edu.au.        165     IN      AAAA    2001:388:c:35::2
ns3.unsw.edu.au.        797     IN      A       192.155.82.178
ns3.unsw.edu.au.        165     IN      AAAA    2600:3c01::f03c:91ff:fe73:5f10

;; Query time: 0 msec
;; SERVER: 129.94.208.3#53(129.94.208.3)
;; WHEN: Fri Aug 18 13:01:33 2017
;; MSG SIZE  rcvd: 301
```

7. The CSE name server (129.94.242.33) did not give us an authoritative answer for the Yahoo mail servers since there was not 'aa' flag in the dig response.

```
; <<>> DiG 9.7.3 <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56639
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              1150    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1150    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1150    IN      MX      1 mta5.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              71027   IN      NS      ns3.yahoo.com.
yahoo.com.              71027   IN      NS      ns4.yahoo.com.
yahoo.com.              71027   IN      NS      ns1.yahoo.com.
yahoo.com.              71027   IN      NS      ns5.yahoo.com.
yahoo.com.              71027   IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          331971  IN      A       68.180.131.16
ns1.yahoo.com.          2349    IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          13000   IN      A       68.142.255.16
ns2.yahoo.com.          5654    IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          597455  IN      A       203.84.221.53
ns3.yahoo.com.          65353   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          257208  IN      A       98.138.11.157
ns5.yahoo.com.          331971  IN      A       119.160.247.124

;; Query time: 0 msec
```

```
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Fri Aug 18 13:17:29 2017
;; MSG SIZE  rcvd: 360
```

8. When repeating the command using one of the cecs.anu.edu.au nameservers, there dig response provides no answer to the query. The key information given is the line "recursion requested but not available" which means that the server does not respond to recursive queries.

```
; <<>> DiG 9.7.3 <<>> @150.203.161.38 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 37096
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

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

;; Query time: 7 msec
;; SERVER: 150.203.161.38#53(150.203.161.38)
;; WHEN: Fri Aug 18 13:22:55 2017
;; MSG SIZE  rcvd: 27
```

9. This was achieved by quering one of the authoritative nameservers for the domain yahoo.com and also including the MX option for mail exchange records

```
; <<>> DiG 9.7.3 <<>> @ns1.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3916
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8
;; WARNING: recursion requested but not available

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

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

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.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.          1209600 IN      A       203.84.221.53
ns4.yahoo.com.          1209600 IN      A       98.138.11.157
ns5.yahoo.com.          1209600 IN      A       119.160.247.124
ns1.yahoo.com.          86400   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          86400   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          86400   IN      AAAA    2406:8600:b8:fe03::1003

;; Query time: 145 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Fri Aug 18 13:48:46 2017
;; MSG SIZE  rcvd: 360
```

10.

It took 5 DNS queries to obtain the IP address of my machine which was 129.94.209.12

```
z5115237@vx2:~$ dig NS .

; <<>> DiG 9.7.3 <<>> NS .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8152
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       156557          IN      NS      j.root-servers.net.
.                       156557          IN      NS      i.root-servers.net.
.                       156557          IN      NS      m.root-servers.net.
.                       156557          IN      NS      d.root-servers.net.
.                       156557          IN      NS      f.root-servers.net.
.                       156557          IN      NS      k.root-servers.net.
.                       156557          IN      NS      b.root-servers.net.
.                       156557          IN      NS      h.root-servers.net.
.                       156557          IN      NS      l.root-servers.net.
.                       156557          IN      NS      e.root-servers.net.
.                       156557          IN      NS      g.root-servers.net.
.                       156557          IN      NS      a.root-servers.net.
.                       156557          IN      NS      c.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     73568   IN      A       198.41.0.4
a.root-servers.net.     317485          IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     448412          IN      A       192.228.79.201
b.root-servers.net.     91191   IN      AAAA    2001:500:200::b
c.root-servers.net.     471792          IN      A       192.33.4.12
c.root-servers.net.     264824          IN      AAAA    2001:500:2::c
d.root-servers.net.     50381   IN      A       199.7.91.13
d.root-servers.net.     429433          IN      AAAA    2001:500:2d::d
```

```
e.root-servers.net.     437430      IN      A       192.203.230.10
e.root-servers.net.     539875      IN      AAAA    2001:500:a8::e
f.root-servers.net.     94184  IN   A       192.5.5.241
f.root-servers.net.     551028      IN      AAAA    2001:500:2f::f
g.root-servers.net.     94183  IN   A       192.112.36.4

;; Query time: 1 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Aug 21 13:06:05 2017
;; MSG SIZE  rcvd: 508

z5115237@vx2:~$ dig @198.41.0.4 au.

; <<>> DiG 9.7.3 <<>> @198.41.0.4 au.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20190
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 15
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;au.                            IN      A

;; AUTHORITY SECTION:
au.                     172800      IN      NS      a.au.
au.                     172800      IN      NS      b.au.
au.                     172800      IN      NS      u.au.
au.                     172800      IN      NS      v.au.
au.                     172800      IN      NS      w.au.
au.                     172800      IN      NS      x.au.
au.                     172800      IN      NS      y.au.
au.                     172800      IN      NS      z.au.

;; ADDITIONAL SECTION:
a.au.                   172800      IN      A       58.65.254.73
b.au.                   172800      IN      A       58.65.253.73
u.au.                   172800      IN      A       211.29.133.32
v.au.                   172800      IN      A       202.12.31.141
w.au.                   172800      IN      A       37.209.192.5
x.au.                   172800      IN      A       37.209.194.5
y.au.                   172800      IN      A       37.209.196.5
z.au.                   172800      IN      A       37.209.198.5
a.au.                   172800      IN      AAAA    2407:6e00:254:306::73
b.au.                   172800      IN      AAAA    2407:6e00:253:306::73
v.au.                   172800      IN      AAAA    2001:dc0:4001:1:0:1836:0:141
w.au.                   172800      IN      AAAA    2001:dcd:1::5
x.au.                   172800      IN      AAAA    2001:dcd:2::5
y.au.                   172800      IN      AAAA    2001:dcd:3::5
z.au.                   172800      IN      AAAA    2001:dcd:4::5

;; Query time: 171 msec
```

```
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Mon Aug 21 13:06:17 2017
;; MSG SIZE  rcvd: 472

z5115237@vx2:~$ dig @58.65.254.73 edu.au

; <<>> DiG 9.7.3 <<>> @58.65.254.73 edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 993
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;edu.au.                        IN      A

;; AUTHORITY SECTION:
edu.au.                 86400   IN      NS      w.au.
edu.au.                 86400   IN      NS      y.au.
edu.au.                 86400   IN      NS      x.au.
edu.au.                 86400   IN      NS      z.au.

;; ADDITIONAL SECTION:
w.au.                   86400   IN      A       37.209.192.5
x.au.                   86400   IN      A       37.209.194.5
y.au.                   86400   IN      A       37.209.196.5
z.au.                   86400   IN      A       37.209.198.5
w.au.                   86400   IN      AAAA    2001:dcd:1::5
x.au.                   86400   IN      AAAA    2001:dcd:2::5
y.au.                   86400   IN      AAAA    2001:dcd:3::5
z.au.                   86400   IN      AAAA    2001:dcd:4::5

;; Query time: 15 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Mon Aug 21 13:06:52 2017
;; MSG SIZE  rcvd: 264

z5115237@vx2:~$ dig @37.209.192.5 unsw.edu.au

; <<>> DiG 9.7.3 <<>> @37.209.192.5 unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47492
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;unsw.edu.au.                   IN      A

;; AUTHORITY SECTION:
```

```
unsw.edu.au.            14400  IN      NS      ns3.unsw.edu.au.
unsw.edu.au.            14400  IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            14400  IN      NS      ns1.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        14400  IN      A       129.94.0.192
ns2.unsw.edu.au.        14400  IN      A       129.94.0.193
ns3.unsw.edu.au.        14400  IN      A       192.155.82.178
ns1.unsw.edu.au.        14400  IN      AAAA2001:388:c:35::1
ns2.unsw.edu.au.        14400  IN      AAAA2001:388:c:35::2

;; Query time: 2 msec
;; SERVER: 37.209.192.5#53(37.209.192.5)
;; WHEN: Mon Aug 21 13:07:11 2017
;; MSG SIZE  rcvd: 187

z5115237@vx2:~$ dig @129.94.0.192 cse.unsw.edu.au

; <<>> DiG 9.7.3 <<>> @129.94.0.192 cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49145
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;cse.unsw.edu.au.               IN      A

;; AUTHORITY SECTION:
cse.unsw.edu.au.        10800  IN      NS      maestro.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        10800  IN      NS      beethoven.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.172.11
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.208.3
beethoven.orchestra.cse.unsw.edu.au. 10800 IN A   129.94.242.2
maestro.orchestra.cse.unsw.edu.au. 10800 IN A     129.94.242.33

;; Query time: 3 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Mon Aug 21 13:07:52 2017
;; MSG SIZE  rcvd: 153

z5115237@vx2:~$ dig @129.94.242.2 tabla12.cse.unsw.edu.au

; <<>> DiG 9.7.3 <<>> @129.94.242.2 tabla12.cse.unsw.edu.au
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41508
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
```

```
;; QUESTION SECTION:
;tabla12.cse.unsw.edu.au.       IN      A

;; ANSWER SECTION:
tabla12.cse.unsw.edu.au. 3600       IN      A       129.94.209.12

;; AUTHORITY SECTION:
cse.unsw.edu.au.        3600    IN      NS      beethoven.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        3600    IN      NS      maestro.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
maestro.orchestra.cse.unsw.edu.au. 3600     IN A    129.94.242.33
beethoven.orchestra.cse.unsw.edu.au. 3600 IN A      129.94.242.2

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Mon Aug 21 13:08:21 2017
;; MSG SIZE  rcvd: 145
```

11. A physical machine can have several names and/or IP addresses associated with it. A machine may have several network interfaces, in which each network interface can have several IP addresses associated with it. An example of this is aliases where multiple names are linked to an IP address.