

z5147986

Lab3

Exercise 3: Digging into DNS

3.1

What is the IP address of www.cecs.anu.edu.au What type of DNS query is sent to get this answer?

The IP address is 150.203.161.98

The type of DNS query is a recursive query since there is a RD set in the dig query header



```
uxu_b ~/cs3331/lab3 P master
dig www.cecs.anu.edu.au

;; <<>> DiG 9.10.6 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36863
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.      3600    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au.   3600    IN      A       150.203.161.98

;; Query time: 89 msec
;; SERVER: 208.67.222.123#53(208.67.222.123)
;; WHEN: Thu Oct 10 20:52:15 AEDT 2019
;; MSG SIZE rcvd: 85
```

3.2

What is the canonical name for the CECS ANU web server? Suggest a reason for having an alias for this server.

The canonical name is rproxy.cecs.anu.edu.au.

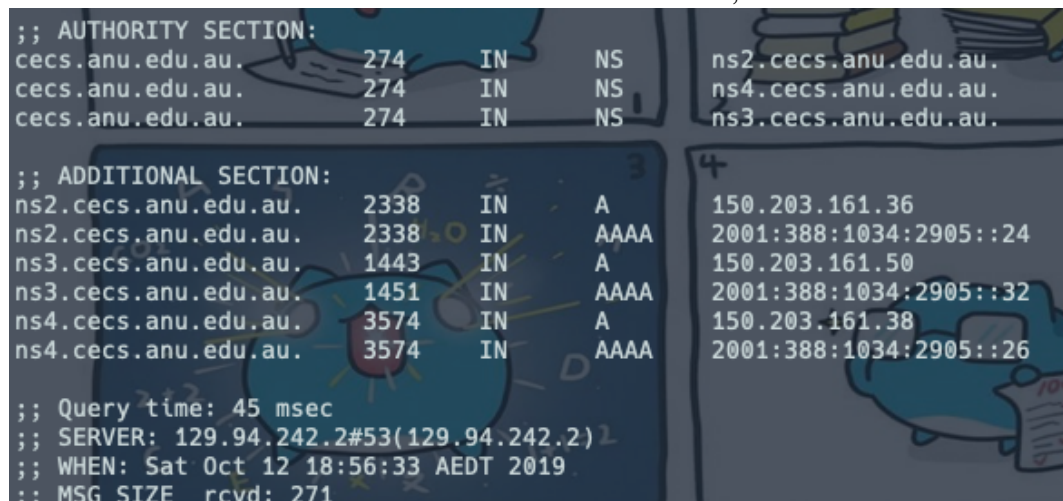
IP aliasing can be used to provide multiple network addresses on a single physical interface, it's like having multiple front doors to a location, can have more than one domain names that takes you to a single site.

3.3

What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

In the Authority section there are 3 DNS servers which are responsible for the domain.

In the Additional section contains A and AAAA records, which are IPv4 and IPv6 address.



```
;; AUTHORITY SECTION:
cecs.anu.edu.au.      274     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.      274     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.      274     IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.  2338    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.  2338    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.  1443    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.  1451    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.  3574    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.  3574    IN      AAAA    2001:388:1034:2905::26

;; Query time: 45 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sat Oct 12 18:56:33 AEDT 2019
;; MSG SIZE rcvd: 271
```

z5147986

Lab3

3.4

What is the IP address of the local nameserver for your machine?

*did not ssh to cse machine but my machine

```
;; Query time: 394 msec
;; SERVER: 208.67.222.123#53(208.67.222.123)
;; WHEN: Sat Oct 12 18:55:04 AEDT 2019
;; MSG SIZE rcvd: 85
```

3.5

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?

The DNS query is > dig www.cecs.anu.edu.au (I ssh into cse machine)

```
;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.      1832    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.      1832    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.      937     IN      A       150.203.161.50
ns3.cecs.anu.edu.au.      945     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.      3068    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.      3068    IN      AAAA    2001:388:1034:2905::26
```

3.6

What is the DNS name associated with the IP address 111.68.101.54? What type of DNS query is sent to obtain this information?

```
weill % dig -x 111.68.101.54 +short
webserver.seecs.nust.edu.pk.
```

3.7

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)

Non authoritative because there is no aa(authoritative answer) flag, and CSE nameserver has no authority on yahoo.com

```
weill % 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: 5291
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 9
```

z5147986

Lab3

3.8

Repeat the above (i.e. Question 7) but use one of the nameservers obtained in Question 5. What is the result?

```
weill % dig @150.203.161.36 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @150.203.161.36 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 54811
;; 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: 7 msec
;; SERVER: 150.203.161.36#53(150.203.161.36)
;; WHEN: Sat Oct 12 19:14:25 AEDT 2019
;; MSG SIZE  rcvd: 38
```

3.9

Obtain the authoritative answer for the mail servers for Yahoo! mail. What type of DNS query is sent to obtain this information?

```
weill % dig @68.180.131.16 yahoo.com MX

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @68.180.131.16 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35659
;; 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 mta7.am0.yahoodns.net.
yahoo.com. 1800 IN MX 1 mta6.am0.yahoodns.net.
yahoo.com. 1800 IN MX 1 mta5.am0.yahoodns.net.
```

z5147986

Lab3

3.10

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?
5 DNS servers to get an authoritative answer for lyre00.cse.unsw.edu.au

- a.root-servers.net.
- a.au.
- q.au.
- ns1.unsw.edu.au.
- beethoven.orchestra.cse.unsw.edu.au.

```
weill % dig NS

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9856
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
;; ADDITIONAL SECTION:
a.root-servers.net.      156988  IN      A        198.41.0.4
a.root-servers.net.      156988  IN      AAAA     2001:503:ba3e::2:30
b.root-servers.net.      261241  IN      A        199.9.14.201
b.root-servers.net.      247594  IN      AAAA     2001:500:200::b
c.root-servers.net.      183486  IN      A        192.33.4.12
c.root-servers.net.      247594  IN      AAAA     2001:500:2::c
;; ADDITIONAL SECTION:
a.au.                    172800  IN      A        58.65.254.73
c.au.                    172800  IN      A        162.159.24.179
d.au.                    172800  IN      A        162.159.25.38
q.au.                    172800  IN      A        65.22.196.1
;; ADDITIONAL SECTION:
q.au.                    86400   IN      A        65.22.196.1
r.au.                    86400   IN      A        65.22.197.1
s.au.                    86400   IN      A        65.22.198.1
t.au.                    86400   IN      A        65.22.199.1
;; ADDITIONAL SECTION:
ns1.unsw.edu.au.         900     IN      A        129.94.0.192
ns2.unsw.edu.au.         900     IN      A        129.94.0.193
ns3.unsw.edu.au.         900     IN      A        192.155.82.178
;; ADDITIONAL SECTION:
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
beethoven.orchestra.cse.unsw.edu.au. 10800  IN      A        129.94.172.11
maestro.orchestra.cse.unsw.edu.au. 10800  IN      A        129.94.242.33
;; ANSWER SECTION:
lyre00.cse.unsw.edu.au. 3600    IN      A        129.94.210.20
```


z5147986

Lab3

3.11

Can one physical machine have several names and/or IP addresses associated with it?

Yes, based on the evidences above an IP address can have multiple names(alias which refers to one canonical name) associated with it.