COMP3331

Lab 2

Dean So (z5204873)

Exercise 3: Digging into DNS

1. *What is the IP address of www.eecs.berkeley.edu . What type of DNS query is sent to get this answer?*

The ip address of www.eecs.berkeley.edu is 23.185.0.1. Address type dns query is sent

Command: dig www.eecs.berkeley.edu A

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> www.eecs.berkeley.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30498
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.eecs.berkeley.edu.         IN      A

;; ANSWER SECTION:
www.eecs.berkeley.edu.  14758   IN      CNAME   live-eecs.pantheonsite.io.
live-eecs.pantheonsite.io. 13   IN      CNAME   fe1.edge.pantheon.io.
fe1.edge.pantheon.io.   275     IN      A       23.185.0.1

;; AUTHORITY SECTION:
edge.pantheon.io.       121     IN      NS      ns-1213.awsdns-23.org.
edge.pantheon.io.       121     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       121     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       121     IN      NS      ns-644.awsdns-16.net.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   102881  IN      A       205.251.192.233
ns-233.awsdns-29.com.   102881  IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   98820   IN      A       205.251.194.132
ns-644.awsdns-16.net.   95172   IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  99983   IN      A       205.251.196.189
ns-1213.awsdns-23.org.  99983   IN      AAAA    2600:9000:5304:bd00::1
ns-2013.awsdns-59.co.uk. 101158 IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 101158 IN      AAAA    2600:9000:5307:dd00::1

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 16 09:52:28 AEDT 2021
;; MSG SIZE  rcvd: 453
```

2. *What is the canonical name for the eecs.berkeley web server (i.e. www.eecs.berkeley.edu)? Suggest a reason for having an alias for this server.*

The CNAME for the webserver is live-eecs.pantheonsite.io using the command dig www.eecs.berkeley.edu CNAME.

An alias could be useful for this server as people are typically used to the "www" format of website names rather than directly using the server name. Also the owner may be running multiple services that point to the same address.

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> www.eecs.berkeley.edu CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46163
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 11

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.eecs.berkeley.edu.         IN      CNAME

;; ANSWER SECTION:
www.eecs.berkeley.edu.  14545   IN      CNAME   live-eecs.pantheonsite.io.

;; AUTHORITY SECTION:
eecs.berkeley.edu.      6327    IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      6327    IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      6327    IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      6327    IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      6327    IN      NS      ns.eecs.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     24196   IN      A       169.229.60.61
ns.CS.berkeley.edu.     14545   IN      AAAA    2607:f140:f000:1260::30
ns.eecs.berkeley.edu.   26091   IN      A       169.229.60.153
ns.eecs.berkeley.edu.   8408    IN      AAAA    2607:f140:f000:2160::30
adns1.berkeley.edu.     1212    IN      A       128.32.136.3
adns1.berkeley.edu.     9636    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     7243    IN      A       128.32.136.14
adns2.berkeley.edu.     1212    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     7242    IN      A       192.107.102.142
adns3.berkeley.edu.     1212    IN      AAAA    2607:f140:a000:d::abc

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 16 09:56:01 AEDT 2021
;; MSG SIZE  rcvd: 406
```

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

The Authority section lists the DNS servers that are able to provide an authoritative answer to queries and the Additional section lists the ip addresses of each authoritative server with ipv4 and ipv6 both listed.

```
;; AUTHORITY SECTION:
edge.pantheon.io.       121     IN      NS      ns-1213.awsdns-23.org.
edge.pantheon.io.       121     IN      NS      ns-233.awsdns-29.com.
edge.pantheon.io.       121     IN      NS      ns-2013.awsdns-59.co.uk.
edge.pantheon.io.       121     IN      NS      ns-644.awsdns-16.net.

;; ADDITIONAL SECTION:
ns-233.awsdns-29.com.   102881  IN      A       205.251.192.233
ns-233.awsdns-29.com.   102881  IN      AAAA    2600:9000:5300:e900::1
ns-644.awsdns-16.net.   98820   IN      A       205.251.194.132
ns-644.awsdns-16.net.   95172   IN      AAAA    2600:9000:5302:8400::1
ns-1213.awsdns-23.org.  99983   IN      A       205.251.196.189
ns-1213.awsdns-23.org.  99983   IN      AAAA    2600:9000:5304:bd00::1
ns-2013.awsdns-59.co.uk. 101158 IN      A       205.251.199.221
ns-2013.awsdns-59.co.uk. 101158 IN      AAAA    2600:9000:5307:dd00::1
```

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

IP address of local DNS nameserver is 129.94.242.2

```
;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 16 10:13:19 AEDT 2021
;; MSG SIZE  rcvd: 453
```

5. *What are the DNS nameservers for the "eecs.berkeley.edu." domain (note: the domain name is eecs.berkeley.edu and not www.eecs.berkeley.edu . This is an example of what is referred to as the apex/naked domain)? Find out their IP addresses? What type of DNS query is sent to obtain this information?*

DNS name servers:

- ns.CS.berkeley.edu. – IP of 169.229.60.61
- ns.eecs.berkeley.edu. – IP of 169.229.60.153
- adns1.berkeley.edu. – IP of 128.32.136.3
- adns2.berkeley.edu. – IP of 128.32.136.14
- adns3.berkeley.edu. – IP of 192.107.102.142

```
;; ANSWER SECTION:
eecs.berkeley.edu.      5198    IN      NS      adns1.berkeley.edu.
eecs.berkeley.edu.      5198    IN      NS      adns3.berkeley.edu.
eecs.berkeley.edu.      5198    IN      NS      ns.CS.berkeley.edu.
eecs.berkeley.edu.      5198    IN      NS      adns2.berkeley.edu.
eecs.berkeley.edu.      5198    IN      NS      ns.eecs.berkeley.edu.

;; ADDITIONAL SECTION:
ns.CS.berkeley.edu.     23067   IN      A       169.229.60.61
ns.CS.berkeley.edu.     13416   IN      AAAA    2607:f140:f000:1260::30
ns.eecs.berkeley.edu.   24962   IN      A       169.229.60.153
ns.eecs.berkeley.edu.   7279    IN      AAAA    2607:f140:f000:2160::30
adns1.berkeley.edu.     83      IN      A       128.32.136.3
adns1.berkeley.edu.     8507    IN      AAAA    2607:f140:ffff:fffe::3
adns2.berkeley.edu.     6114    IN      A       128.32.136.14
adns2.berkeley.edu.     8507    IN      AAAA    2607:f140:ffff:fffe::e
adns3.berkeley.edu.     6113    IN      A       192.107.102.142
adns3.berkeley.edu.     83      IN      AAAA    2607:f140:a000:d::abc
```

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?*

REVERSE LOOKUP DNS query is sent with command dig –x 111.68.101.54.

The DNS name associated with the above IP address is webserver.seecs.nust.edu.pk.

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23191
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;54.101.68.111.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
54.101.68.111.in-addr.arpa. 667 IN      PTR     webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 26914  IN      NS      ns2.hec.gov.pk.
101.68.111.in-addr.arpa. 26914  IN      NS      ns1.hec.gov.pk.

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Tue Mar 16 10:20:17 AEDT 2021
;; MSG SIZE  rcvd: 140
```

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)*

CSE UNSW nameservers don't have the authority for yahoo authority records notice in the DNS Header Flags – there is no AA in the header.

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @129.94.242.33 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7636
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10

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

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

;; AUTHORITY SECTION:
yahoo.com.              85602   IN      NS      ns1.yahoo.com.
yahoo.com.              85602   IN      NS      ns4.yahoo.com.
yahoo.com.              85602   IN      NS      ns5.yahoo.com.
yahoo.com.              85602   IN      NS      ns2.yahoo.com.
yahoo.com.              85602   IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          532485  IN      A       68.180.131.16
ns1.yahoo.com.          47500   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          4523    IN      A       68.142.255.16
ns2.yahoo.com.          33754   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          1773    IN      A       27.123.42.42
ns3.yahoo.com.          818     IN      AAAA    2406:8600:f03f:1f8::1003
ns4.yahoo.com.          10004   IN      A       98.138.11.157
ns5.yahoo.com.          50145   IN      A       202.165.97.53
ns5.yahoo.com.          50145   IN      AAAA    2406:2000:ff60::53

;; Query time: 101 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Mar 16 10:22:56 AEDT 2021
;; MSG SIZE  rcvd: 399
```

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

Upon using the IP address of the DNS nameserver from Berkeley 169.229.60.61.

The result is a refused DNS query which occurs because of security reasons as you are not a part of the Berkeley network to access the Berkeley DNS servers.

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @169.229.60.61 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 44253
;; 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: 166 msec
;; SERVER: 169.229.60.61#53(169.229.60.61)
;; WHEN: Tue Mar 16 10:26:51 AEDT 2021
;; MSG SIZE  rcvd: 38
```

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

An MX DNS query is sent for the authoritative nameservers of Yahoo.com. I obtained one of the Yahoo authoritative DNS nameservers and queried that server specifically.

```
; <<>> DiG 9.9.5-9+deb8u19-Debian <<>> @68.180.131.16 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59232
;; flags: qr aa rd; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
;; 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 mta5.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1800    IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              172800  IN      NS      ns3.yahoo.com.
yahoo.com.              172800  IN      NS      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.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.          86400   IN      A       202.165.97.53
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
ns5.yahoo.com.          86400   IN      AAAA    2406:2000:ff60::53

;; Query time: 146 msec
;; SERVER: 68.180.131.16#53(68.180.131.16)
;; WHEN: Tue Mar 16 10:32:50 AEDT 2021
;; MSG SIZE  rcvd: 399
```

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). If you are using VLAB Then find the IP address of one of the following: lyre00.cse.unsw.edu.au, lyre01.cse.unsw.edu.au, drum00.cse.unsw.edu.au or drum01.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?

Using this nameserver, we start the queries;

```
;; ADDITIONAL SECTION:
a.root-servers.net.     209759  IN      A       198.41.0.4
```

- 1st Query: dig @198.41.0.4 lyre00.cse.unsw.edu.au NS (a.root-servers.net.)
  - `a.au.  172800  IN  A  58.65.254.73`
- 2nd Query: dig @58.65.254.73 lyre00.cse.unsw.edu.au NS (a.au.)
  - `q.au.  86400  IN  A  65.22.196.1`
- 3rd Query: dig @65.22.196.1 lyre00.cse.unsw.edu.au NS (q.au.)
  - `ns1.unsw.edu.au.  900  IN  A  129.94.0.192`
- 4th Query: dig @129.94.0.192 lyre00.cse.unsw.edu.au NS (ns1.unsw.edu.au.)
  - `beethoven.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.208.3`
- 5th Query: dig @129.94.208.3 lyre00.cse.unsw.edu.au A (beethoven.orchestra.cse.unsw.edu.au.)
  - `lyre00.cse.unsw.EDU.AU. 3600  IN  A  129.94.210.20`

IP address of my VLAB machine is 129.94.210.20

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

Yes one physical machine can indeed have several names and/or IP addresses associated with it (multiple interfaces with different incoming and outgoing packet interfaces).