Z5146286

Exercise 3: Digging into DNS

Question 1. What is the IP address of www.cecs.anu.edu.au . What type of DNS query is sent to get this answer?

Answer:

150.203.161.98

```
z5146286@vx4:/tmp_amd/cage/export/cage/3/z5146286$ ping www.cecs.anu.edu.au
PING rproxy.cecs.anu.edu.au (150.203.161.98) 56(84) bytes of data.
64 bytes from 150.203.161.98: icmp_req=1 ttl=53 time=5.73 ms
64 bytes from 150.203.161.98: icmp_req=2 ttl=53 time=5.71 ms
```

Type of DNS query :A

```
;; ANSWER SECTION:
www.cecs.anu.edu.au.    3264    IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 146     IN      A       150.203.161.98
```

Question 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.

Answer:

Canonical name :rproxy.cecs.anu.edu.au.

```
;; ANSWER SECTION:
www.cecs.anu.edu.au.    1459    IN      CNAME   rproxy.cecs.anu.edu.au.
```

IP address: 150.203.161.98

```
rproxy.cecs.anu.edu.au. 906     IN      A       150.203.161.98
```

Reason: A domain alias is an additional/alternate domain name created for the primary domain of the website. if CNAME changes, it is not necessary for users to remember extra domain name. Because alias can map to any canonical name for web server.

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

```
;; AUTHORITY SECTION:
cecs.anu.edu.au.        3599    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        3599    IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        3599    IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    1702    IN      A       150.203.161.36
ns3.cecs.anu.edu.au.    1741    IN      A       150.203.161.50
ns4.cecs.anu.edu.au.    3599    IN      A       150.203.161.38
ns2.cecs.anu.edu.au.    3599    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    3599    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    3599    IN      AAAA    2001:388:1034:2905::26
```

Answer:

Authority section shows NS record，and which servers mange DNS record of “cecs.au.edu.au.”.

Additional section shows IP address of nameservers above.

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

```
;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 17 22:33:59 2019
;; MSG SIZE  rcvd: 204
```

Answer:129.94.242.2

Question 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?

```
z5146286@vx4:/tmp_amd/cage/export/cage/3/z5146286$ r
Server:         129.94.242.2
Address:        129.94.242.2#53

Non-authoritative answer:
Name:   cecs.anu.edu.au
Address: 150.203.161.98
```

Nameserver:129.94.242.2

IP Address:150.203.161.98

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

;; ANSWER SECTION:
cecs.anu.edu.au.        597     IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        949     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        949     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        949     IN      NS      ns4.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    2285    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    2285    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    2626    IN      A       150.203.161.50
ns4.cecs.anu.edu.au.    1298    IN      A       150.203.161.38

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 17 22:43:10 2019
;; MSG SIZE  rcvd: 179
```

Type of DNS query: NS

Question 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?

```
192-168-1-130:~ zhangpei$ dig -x 149.171.158.109
```

```
;; ANSWER SECTION:
109.158.171.149.in-addr.arpa. 1972 IN   PTR     engplws008.eng.unsw.edu.au.
109.158.171.149.in-addr.arpa. 1972 IN   PTR     engplws008.ad.unsw.edu.au.
```

DNS name: engplws008.eng.unsw.edu.au
engplws008.ad.unsw.edu.au
Type of DNS query: PTR

Question 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)

```
z5146286@vx4:/tmp_amd/cage/export/cage/3/z5146286$ dig @129.94.242.33 yahoo.com mx

; <<>> 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: 3854
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              599     IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              599     IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              599     IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              126772  IN      NS      ns3.yahoo.com.
yahoo.com.              126772  IN      NS      ns1.yahoo.com.
yahoo.com.              126772  IN      NS      ns5.yahoo.com.
yahoo.com.              126772  IN      NS      ns4.yahoo.com.
yahoo.com.              126772  IN      NS      ns2.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          160316  IN      A       68.180.131.16
ns1.yahoo.com.          40444   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          170205  IN      A       68.142.255.16
ns2.yahoo.com.          49017   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          54609   IN      A       203.84.221.53
ns3.yahoo.com.          40548   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          85551   IN      A       98.138.11.157
ns5.yahoo.com.          63132   IN      A       119.160.253.83

;; Query time: 0 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Sun Mar 17 23:01:22 2019
;; MSG SIZE  rcvd: 360
```

Answer: No

a “aa” in flags means it is an Authoritative Answer, which ensure the query result comes from Authoritative nameserver ,not catching nameserver.

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

```
z5146286@vx4:/tmp_amd/cage/export/cage/3/z5146286$ dig @129.94.242.2 yahoo.com mx

; <<>> DiG 9.7.3 <<>> @129.94.242.2 yahoo.com mx
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 416
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              305     IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              305     IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              305     IN      MX      1 mta7.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              122161  IN      NS      ns2.yahoo.com.
yahoo.com.              122161  IN      NS      ns1.yahoo.com.
yahoo.com.              122161  IN      NS      ns4.yahoo.com.
yahoo.com.              122161  IN      NS      ns5.yahoo.com.
yahoo.com.              122161  IN      NS      ns3.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          59102   IN      A       68.180.131.16
ns1.yahoo.com.          40374   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          63061   IN      A       68.142.255.16
ns2.yahoo.com.          77874   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          54539   IN      A       203.84.221.53
ns3.yahoo.com.          40478   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          85481   IN      A       98.138.11.157
ns5.yahoo.com.          63062   IN      A       119.160.253.83

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Sun Mar 17 23:02:32 2019
;; MSG SIZE  rcvd: 360
```

No, Non-authoritative Answer.

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

Answer:

Type of DNS query: NS

Question 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?

Step1:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       108982  IN      NS      j.root-servers.net.
.                       108982  IN      NS      a.root-servers.net.
.                       108982  IN      NS      h.root-servers.net.
.                       108982  IN      NS      i.root-servers.net.
.                       108982  IN      NS      m.root-servers.net.
.                       108982  IN      NS      k.root-servers.net.
.                       108982  IN      NS      c.root-servers.net.
.                       108982  IN      NS      b.root-servers.net.
.                       108982  IN      NS      l.root-servers.net.
.                       108982  IN      NS      e.root-servers.net.
.                       108982  IN      NS      f.root-servers.net.
.                       108982  IN      NS      d.root-servers.net.
.                       108982  IN      NS      g.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     3536182 IN      A       198.41.0.4
b.root-servers.net.     3547665 IN      A       199.9.14.201
c.root-servers.net.     3545435 IN      A       192.33.4.12
d.root-servers.net.     3548754 IN      A       199.7.91.13
e.root-servers.net.     3551967 IN      A       192.203.230.10
f.root-servers.net.     3543104 IN      A       192.5.5.241
g.root-servers.net.     3536831 IN      A       192.112.36.4
h.root-servers.net.     3536898 IN      A       198.97.190.53
i.root-servers.net.     3536898 IN      A       192.36.148.17
j.root-servers.net.     3536898 IN      A       192.58.128.30
k.root-servers.net.     3536899 IN      A       193.0.14.129
l.root-servers.net.     3536899 IN      A       199.7.83.42
m.root-servers.net.     3536301 IN      A       202.12.27.33
a.root-servers.net.     3536182 IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     3536367 IN      AAAA    2001:500:200::b
c.root-servers.net.     3549041 IN      AAAA    2001:500:2::c
d.root-servers.net.     3545437 IN      AAAA    2001:500:2d::d
e.root-servers.net.     3545978 IN      AAAA    2001:500:a8::e
f.root-servers.net.     3574880 IN      AAAA    2001:500:2f::f
g.root-servers.net.     3545978 IN      AAAA    2001:500:12::d0d
h.root-servers.net.     3536182 IN      AAAA    2001:500:1::53
i.root-servers.net.     3536182 IN      AAAA    2001:7fe::53
j.root-servers.net.     3597937 IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     3536182 IN      AAAA    2001:7fd::1
l.root-servers.net.     3536182 IN      AAAA    2001:500:9f::42
m.root-servers.net.     3537406 IN      AAAA    2001:dc3::35
```

Step2:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;au.                            IN      NS

;; ANSWER SECTION:
au.                     26343   IN      NS      b.au.
au.                     26343   IN      NS      q.au.
au.                     26343   IN      NS      t.au.
au.                     26343   IN      NS      c.au.
au.                     26343   IN      NS      d.au.
au.                     26343   IN      NS      u.au.
au.                     26343   IN      NS      v.au.
au.                     26343   IN      NS      r.au.
au.                     26343   IN      NS      s.au.
au.                     26343   IN      NS      a.au.
```

Step3:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;edu.au.                                IN      NS

;; ANSWER SECTION:
edu.au.                 900     IN      NS      t.au.
edu.au.                 900     IN      NS      r.au.
edu.au.                 900     IN      NS      s.au.
edu.au.                 900     IN      NS      q.au.
```

Step4:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;unsw.edu.au.                   IN      NS

;; ANSWER SECTION:
unsw.edu.au.            4486    IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            4486    IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            4486    IN      NS      ns3.unsw.edu.au.

;; ADDITIONAL SECTION:
ns3.unsw.edu.au.        5011    IN      A       192.155.82.178
ns3.unsw.edu.au.        3148    IN      AAAA    2600:3c01::f03c:91ff:fe73:5f10
ns2.unsw.edu.au.        8777    IN      A       129.94.0.193
ns2.unsw.edu.au.        8777    IN      AAAA    2001:388:c:35::2
ns1.unsw.edu.au.        5011    IN      A       129.94.0.192
ns1.unsw.edu.au.        3148    IN      AAAA    2001:388:c:35::1
```

Step5:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cse.unsw.edu.au.               IN      NS

;; ANSWER 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. 2770 IN A    129.94.242.33
beethoven.orchestra.cse.unsw.edu.au. 3349 IN A  129.94.242.2
```

Step6:

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;cse.unsw.edu.au.               IN      NS

;; ANSWER SECTION:
cse.unsw.edu.au.        3537    IN      NS      beethoven.orchestra.cse.unsw.edu.au.
cse.unsw.edu.au.        3537    IN      NS      maestro.orchestra.cse.unsw.edu.au.

;; ADDITIONAL SECTION:
maestro.orchestra.cse.unsw.edu.au. 2707 IN A    129.94.242.33
beethoven.orchestra.cse.unsw.edu.au. 3286 IN A  129.94.242.2
```

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

Answer: Yes

A single physical machine can have multiple IP addresses. This is almost essential when implementing server virtualization with multiple virtual servers running on the same physical hardware, each needs its own IP address.