lab3.md

CS3331 Lab 3: Digging deeper in DNS and TCP sockets

Exercise 2: Digging into DNS

Question 1

Answer

The IP address of `www.cecs.anu.edu.au` is 150.203.161.98 and an A record type query was sent to retrieve this answer.

Dig Command Output

I ran `dig www.cecs.anu.edu.au` and obtained the following output:

```
; <<>> DiG 9.7.3 <<>> www.cecs.anu.edu.au
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25691
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

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

;; ANSWER SECTION:
www.cecs.anu.edu.au.    147     IN      CNAME   rproxy.cecs.anu.edu.au.
rproxy.cecs.anu.edu.au. 147     IN      A       150.203.161.98
```

```
;; AUTHORITY SECTION:
cecs.anu.edu.au.        253     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        253     IN      NS      ns1.cecs.anu.edu.au.
cecs.anu.edu.au.        253     IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        253     IN      NS      ns2.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns1.cecs.anu.edu.au.    2348    IN      A       150.203.161.4
ns1.cecs.anu.edu.au.    1912    IN      AAAA    2001:388:1034:2905::4
ns2.cecs.anu.edu.au.    1259    IN      A       150.203.161.36
ns3.cecs.anu.edu.au.    2363    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    253     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    150     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    253     IN      AAAA    2001:388:1034:2905::26

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Aug 16 15:01:02 2017
;; MSG SIZE  rcvd: 294
```

Question 2

Answer

The canonical name of the CECS ANU web server is `rproxy.cecs.anu.edu.au` . A CNAME type query was sent to retrieve this answer. An alias is used for this server most likely for simplicity reasons since it's canonical name is longer and harder to remember than it's alias URL.

Question 3

Answer

In the Authority section are some NS records which show other available name servers for `anu.edu.au` including:

- una.anu.edu.au

- ns1.anu.edu.au
- ns.adelaide.edu.au

In the Additional section are extra A records the query returned, which displays the IP addresses of these alternative available name servers:

Alternative nameserver	IP address
una.anu.edu.au	150.203.22.28
ns.adelaide.edu.au	129.127.40.3
ns1.anu.edu.au	150.203.1.10

Question 4

Answer

The IP address of the local nameserver on my machine is 129.94.242.2. I discovered this from the stats section of the dig command output where below the query output is a printed field for the server the query was sent from which can be seen at the bottom of the dig command output from Question 1.

Question 5

Answer

I found the following DNS nameservers for `cecs.anu.edu.au` in the Answers section of a DNS NS record query:

```
cecs.anu.edu.au.        1800    IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        1800    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        1800    IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        1800    IN      NS      ns1.cecs.anu.edu.au.
```

Also listed was their corresponding IP addresses in IPv4 (A record) and IPv6 (AAAA) format.

```
ns1.cecs.anu.edu.au.    814     IN      A       150.203.161.4
ns1.cecs.anu.edu.au.    1800    IN      AAAA    2001:388:1034:2905::4
ns2.cecs.anu.edu.au.    814     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    1800    IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    2354    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    2354    IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    1644    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    1800    IN      AAAA    2001:388:1034:2905::26
```

Dig Command Output

I ran the following command `dig cecs.anu.edu.au NS` and obtained the following output:

```
; <<>> DiG 9.7.3 <<>> cecs.anu.edu.au NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49356
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 8

;; QUESTION SECTION:
;cecs.anu.edu.au.               IN      NS

;; ANSWER SECTION:
cecs.anu.edu.au.        1598    IN      NS      ns1.cecs.anu.edu.au.
cecs.anu.edu.au.        1598    IN      NS      ns3.cecs.anu.edu.au.
cecs.anu.edu.au.        1598    IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        1598    IN      NS      ns4.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns1.cecs.anu.edu.au.    2127    IN      A       150.203.161.4
ns1.cecs.anu.edu.au.    1691    IN      AAAA    2001:388:1034:2905::4
ns2.cecs.anu.edu.au.    1038    IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    249     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    2142    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    32      IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    3534    IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    3162    IN      AAAA    2001:388:1034:2905::26
```

```
;; Query time: 6 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Aug 16 15:04:43 2017
;; MSG SIZE  rcvd: 281
```

Question 6

Answer

`www.engineering.unsw.edu.au` and `engplws008.ad.unsw.edu.au` appear to be associated with the IP address 149.171.158.109. A PTR type DNS query was sent to retrieve this information.

Dig Command Output

I ran the command `dig -x 149.171.158.109` to obtain the following output:

```
; <<>> DiG 9.7.3 <<>> -x 149.171.158.109
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45854
;; 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. 2742 IN   PTR     www.engineering.unsw.edu.au.
109.158.171.149.in-addr.arpa. 2742 IN   PTR     engplws008.ad.unsw.edu.au.

;; AUTHORITY SECTION:
158.171.149.in-addr.arpa. 9942  IN      NS      ns3.unsw.edu.au.
158.171.149.in-addr.arpa. 9942  IN      NS      ns2.unsw.edu.au.
158.171.149.in-addr.arpa. 9942  IN      NS      ns1.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        8905    IN      A       129.94.0.192
```

```
ns1.unsw.edu.au.        8905    IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        8905    IN      A       129.94.0.193
ns2.unsw.edu.au.        3992    IN      AAAA    2001:388:c:35::2
ns3.unsw.edu.au.        8905    IN      A       192.155.82.178
ns3.unsw.edu.au.        3992    IN      AAAA    2600:3c01::f03c:91ff:fe73:5f10

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Aug 16 15:06:38 2017
;; MSG SIZE  rcvd: 301
```

Question 7

Answer

I obtained the following mail servers for `yahoo.com` in the Answer section when I completed a DNS query for MX records:

```
;; ANSWER SECTION:
yahoo.com.              1730    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1730    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1730    IN      MX      1 mta7.am0.yahoodns.net.
```

I didn't receive an authoritative answer as the query didn't send back the 'AA' flag for 'authoritative answer'.

Dig Command Output

I ran the command `dig yahoo.com MX` to obtain the following output:

```
; <<>> DiG 9.7.3 <<>> yahoo.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41191
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8
```

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

;; ANSWER SECTION:
yahoo.com.              915     IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              915     IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              915     IN      MX      1 mta6.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              148016  IN      NS      ns2.yahoo.com.
yahoo.com.              148016  IN      NS      ns5.yahoo.com.
yahoo.com.              148016  IN      NS      ns3.yahoo.com.
yahoo.com.              148016  IN      NS      ns4.yahoo.com.
yahoo.com.              148016  IN      NS      ns1.yahoo.com.

;; ADDITIONAL SECTION:
ns1.yahoo.com.          59112   IN      A       68.180.131.16
ns1.yahoo.com.          12174   IN      AAAA    2001:4998:130::1001
ns2.yahoo.com.          85414   IN      A       68.142.255.16
ns2.yahoo.com.          11184   IN      AAAA    2001:4998:140::1002
ns3.yahoo.com.          58165   IN      A       203.84.221.53
ns3.yahoo.com.          22719   IN      AAAA    2406:8600:b8:fe03::1003
ns4.yahoo.com.          153540  IN      A       98.138.11.157
ns5.yahoo.com.          324684  IN      A       119.160.247.124

;; Query time: 0 msec
;; SERVER: 129.94.242.2#53(129.94.242.2)
;; WHEN: Wed Aug 16 15:07:59 2017
;; MSG SIZE  rcvd: 360
```

Question 8

I repeated the query for the mail servers of `yahoo.com` using the command `dig yahoo.com ns3.cecs.anu.edu.au mx +noall +answer` and received only A records in the following answer:

```
yahoo.com.              1096    IN      A       206.190.36.45
yahoo.com.              1096    IN      A       98.138.253.109
yahoo.com.              1096    IN      A       98.139.180.149
```

Once again the answer wasn't authoritative either as the query answer didn't contain an 'AA' flag.

Question 9

I obtained an authoritative answer for the mail servers for Yahoo! mail by querying one of the servers listed in the Authority section of `yahoo.com` I found in Question 7, by calling dig with the first parameter of `@nameserver` to query `ns4.yahoo.com` directly for `yahoo.com` 's MX records.

Dig Command Output

I ran `dig @ns4.yahoo.com yahoo.com MX` to obtain the following dig output:

```
; <<>> DiG 9.7.3 <<>> @ns4.yahoo.com yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43663
;; 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 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      ns2.yahoo.com.
yahoo.com.              172800  IN      NS      ns3.yahoo.com.
yahoo.com.              172800  IN      NS      ns5.yahoo.com.
yahoo.com.              172800  IN      NS      ns4.yahoo.com.
yahoo.com.              172800  IN      NS      ns1.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: 188 msec
;; SERVER: 98.138.11.157#53(98.138.11.157)
;; WHEN: Wed Aug 16 17:54:26 2017
;; MSG SIZE  rcvd: 360
```

Question 10

Answer

I queried 5 DNS servers to obtain the final IP address of my host.

Dig Command Output

Ran `dig . NS +noall +answer` to get:

```
; <<>> DiG 9.7.3 <<>> . NS +noall +answer
;; global options: +cmd
.                       51998   IN      NS      j.root-servers.net.
.                       51998   IN      NS      l.root-servers.net.
.                       51998   IN      NS      f.root-servers.net.
.                       51998   IN      NS      e.root-servers.net.
.                       51998   IN      NS      g.root-servers.net.
.                       51998   IN      NS      c.root-servers.net.
.                       51998   IN      NS      k.root-servers.net.
.                       51998   IN      NS      i.root-servers.net.
.                       51998   IN      NS      a.root-servers.net.
.                       51998   IN      NS      d.root-servers.net.
.                       51998   IN      NS      b.root-servers.net.
```

```
.                       51998   IN      NS      m.root-servers.net.
.                       51998   IN      NS      h.root-servers.net.
```

Ran `dig @j.root-servers.net. au. +noall +authority` to get:

```
; <<>> DiG 9.7.3 <<>> @j.root-servers.net. au. +noall +authority
; (1 server found)
;; global options: +cmd
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.
```

Ran `dig @a.au. edu.au. NS +noall +authority` to get:

```
; <<>> DiG 9.7.3 <<>> @a.au. edu.au. NS +noall +authority
; (1 server found)
;; global options: +cmd
edu.au.                 86400   IN      NS      z.au.
edu.au.                 86400   IN      NS      x.au.
edu.au.                 86400   IN      NS      w.au.
edu.au.                 86400   IN      NS      y.au.
```

Ran `dig @z.au. unsw.edu.au NS +noall +authority` to get:

```
; <<>> DiG 9.7.3 <<>> @z.au. unsw.edu.au NS +noall +authority
; (1 server found)
;; global options: +cmd
unsw.edu.au.            14400   IN      NS      ns1.unsw.edu.au.
unsw.edu.au.            14400   IN      NS      ns2.unsw.edu.au.
unsw.edu.au.            14400   IN      NS      ns3.unsw.edu.au.
```

Ran `dig @ns1.unsw.edu.au. cse.unsw.edu.au NS +noall +authority` to get:

```
; <<>> DiG 9.7.3 <<>> @ns1.unsw.edu.au. cse.unsw.edu.au NS +noall +authority
; (1 server found)
;; global options: +cmd
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.
```

Ran `dig maestro.orchestra.cse.unsw.edu.au. A +noall +answer` to get:

```
maestro.orchestra.cse.unsw.edu.au. 3600 IN A
```

Question 11

Answer

Yes - one physical machine can have several names (aliases) setup or IP addresses associated with it.

Exercise 3: Implementing a simple Web Server

```
# Retrieve command line args library.
import sys
# Socket programming library.
import socket
# Regex and string operations library.
import string
import re

# Retrieve server port from command line input args.
# port = sys.argv[1]
port = int (sys.argv[1])
host = ''
```

```
# Store default buffer size (max amount of data to receive at once).
bufferSize = 1024

# Create a TCP socket (SOCK_STREAM) and bind it to the input port
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.bind((host, port))
s.listen(1)

while True:
    conn, address = s.accept()
    # Retrieve the request object.
    data = conn.recv(bufferSize)
    # Split the GET request by new lines.
    lines = string.split(data, '\n')
    # Retrieve the file name in the GET request using regex matching.
    match = re.findall('/\w+.\w+', data)[0]
    fileName = re.findall('\w+.\w+', match)[0]
    try:
        # Open the file and send it over the connection socket if successful.
        f = open(fileName, 'rb')
        l = f.read(bufferSize)
        # Send HTTP header.
        conn.send('HTTP/1.0 200 OK\n')
        conn.send('Content-Type: text/html\n')
        conn.send('\n')
        conn.send('"""')
        while l:
            conn.send(l)
            print "Sent: %s" % l
            l = f.read(bufferSize)
        conn.send('"""')
        f.close()
    except IOError:
        # If opening the file was unsuccessful, return a 404 error.
        conn.send("HTTP/1.1 404 Not Found\r\n\r\n")

conn.close()
```