Lab Exercise 3: Solutions

Exercise 1 (Not Marked)

Here is a short summary.

A = Internet address of the host (in IPv4 format); hostname to IP address mapping.

CNAME = canonical name of an alias; a machine may have several names (aliases) associated with it, but only one of them is the "real" one.

MX = mail exchanger; mail server for the domain. This is used by SMTP.

NS = nameserver; which nameserver is responsible for the domain.

PTR = pointer to a canonical name; IP address to hostname mapping.

SOA = domain's start-of-authority information; who is in charge for the administration of the domain.

Exercise 2 (Not Marked)

Question 1. DNS uses UDP.

Question 2. Source port is 3742 and destination port is 53 for the query. For the response it is reversed, i.e. source port is 53 and destination port is 3742.

Question 3. The DNS query is sent to the IP address 128.238.29.22, which is the default local DNS server.

Question 4. There is only one "question" in the query message. It is of type A and is requesting for the IPv4 address for www.mit.edu (http://www.mit.edu) .

Question 5. The response message contains one "Answer" which is the RR (resource record) for www.mit.edu (http://www.mit.edu) . The RR is as follows:

```
www.mit.edu: type A, class inet, addr 18.7.22.83
```

In addition, there are three authoritative records which are the RRs for the authoritative name servers for mit.edu domain. These RRs are as follows:

```
mit.edu: type NS, class inet, ns BITSY.mit.edu
mit.edu: type NS, class inet, ns STRAWB.mit.edu
mit.edu: type NS, class inet, ns W20NS.mit.edu
```

Finally, there are also three additional RRs, which contain the type A records for the above three name servers. They are as follows:

```
BITSY.mit.edu: type A, class inet, addr 18.72.0.3
STRAWB.mit.edu: type A, class inet, addr 18.71.0.151
W20NS.mit.edu: type A, class inet, addr 18.70.0.160
```

Exercise 3.

Question 1.

The IP address of www.eecs.berkeley.edu (https://eecs.berkeley.edu/) is 23.185.0.1 To get this answer we make a type A query.

Question 2.

The CNAME is live-eecs.pantheonsite.io. Canonical names are usually very long and hard to remember. An alias such as www.eecs.berkeley.edu (https://eecs.berkeley.edu/) is more mnemonic and easy to remember. Aliasing is also useful when running multiple services (e.g. an email server and web server) from a single IP address.

Question 3.

The authority section contains NS resource records for the eecs.berkeley.edu (https://eecs.berkeley.edu/) domain name. In other words, it indicates the four authoritative name servers for this particular domain name which are ns.1213.awsdns-23.org, ns.233.awsdns-29.com and ns.2013-awsdns-59.co.uk and ns-644-awsdns-16.net.

The additional section contains IP addresses for these four authoritative name servers (i.e. the type A resource records for the name servers). The AAAA records are for IPv6 addresses.

Question 4.

The information about the local nameserver is included at the bottom of the output, 129.94.242.2# 53 This is the local DNS server for the CSE network. The above query was made by connecting the CSE login servers via SSH.

Question 5.

We issue the following query, which is for an NS record.

```
-bash-4.2$ dig eecs.berkeley.edu.au NS


<span class="redactor-invisible-space">
<span class="redactor-invisible-space">
</span></span> ;; ANSWER SECTION:
 eecs.berkeley.edu. 72630 IN  NS  adns2.berkeley.edu
 eecs.berkeley.edu. 72630 IN  NS  adns1.berkeley.edu
 eecs.berkeley.edu. 72630 IN  NS  ns.eecs.berkeley.edu
 eecs.berkeley.edu. 72630 IN  NS  ns.CS.berkeley.edu
 eecs.berkeley.edu. 72630 IN  NS  adns3.berkeley.edu

 ;; ADDITIONAL SECTION:
adns2.berkeley.edu    72649  IN  A    169.229.60.61
adns1.berkeley.edu    72649  IN  A    169.229.60.153
ns.eecs.berkeley.edu  158907 IN  AAAA 2607.f140.fff:fffe::3
adns3.berkeley.edu     1015  IN  AAAA 2607:f140;a000;d:abc


 ;; Query time: 0 msec
 ;; SERVER: 129.94.242.2#53(129.94.242.2)
 ;; WHEN: Tue Jun 24 14:53:10 2020
 ;; MSG SIZE rcvd: 231
```

The name servers are adns2, adns1, ns.eecs, ans.CS and adns3. .berkeley.edu and their IP addresses are: 169.229.60.61, 169.229.60.153, 2607.f140.fff:fffe::3 and 1607:f140;a000;d:abc respectively. Note that, AAAA records are for IPv6 addresses.

Question 6.

For this, we use reverse DNS, i.e. we make a type PTR query for 125.158.171.149.in-addr.arpa. (note the reverse ordering of the IP address)

```
<>> DiG 9.10.6 <<>> -x 111.68.101.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37588
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; 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. 3600 IN    PTR    webserver.seecs.nust.edu.pk.

;; AUTHORITY SECTION:
101.68.111.in-addr.arpa. 77827    IN    NS    ns1.hec.gov.pk.
101.68.111.in-addr.arpa. 77827    IN    NS    ns2.hec.gov.pk.

;; ADDITIONAL SECTION:
ns2.hec.gov.pk.        2763    IN    A    103.4.93.6
ns1.hec.gov.pk.        2763    IN    A    103.4.93.5

;; Query time: 417 msec
;; SERVER: 129.94.0.196#53(129.94.0.196)
;; WHEN: Thu Oct 10 17:03:08 AEDT 2019
;; MSG SIZE  rcvd: 172
```

The hostname corresponding to 111.68.101.54 is webserver.seecs.nust.edu.pk.

Question 7.

```
bash-4.1$ dig @129.94.208.3 yahoo.com MX
; <<>> DiG 9.8.3-P1 <<>> @129.94.208.3 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32279
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 6, ADDITIONAL: 6

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

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

;; AUTHORITY SECTION:
yahoo.com. 154972 IN NS ns2.yahoo.com.
yahoo.com. 154972 IN NS ns6.yahoo.com.
yahoo.com. 154972 IN NS ns3.yahoo.com.
yahoo.com. 154972 IN NS ns4.yahoo.com.
yahoo.com. 154972 IN NS ns5.yahoo.com.
yahoo.com. 154972 IN NS ns1.yahoo.com.

;; ADDITIONAL SECTION:
ns2.yahoo.com. 5620   IN A 68.142.255.16
ns3.yahoo.com. 179224 IN A 203.84.221.53
ns4.yahoo.com. 405802 IN A 98.138.11.157
ns5.yahoo.com. 434523 IN A 119.160.247.124
ns6.yahoo.com. 154972 IN A 121.101.144.139
ns6.yahoo.com. 1199 IN AAAA 2406:2000:108:4::1006

;; Query time: 169 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Mar 8 15:04:37 2016
;; MSG SIZE rcvd: 322
```

We see that the server we queried (orchestra.cse.unsw.edu.au) cannot give us an authoritative answer since the flags do not contain aa. This is because it has authority for only the cse.unsw.edu.au domain and not for the Yahoo domain.

Question No 8.

When we try with the ANU nameservers we do not get a response. This can be inferred from the fact that the status of the reply is REFUSED. The reason could be that these name servers do not reply to DNS queries that are sent from devices that are not part of the ANU network as a security measure.

```
-bash-4.2$ dig @ns1.anu.edu.au yahoo.com MX

 ; <<>> DiG 9.7.3 <<>> @ns1.anu.edu.au yahoo.com MX
 ; (1 server found)
 ;; global options: +cmd

 ;; Got answer:
 ;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 23813
 ;; 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: 9 msec
 ;; SERVER: 150.203.1.10#53(150.203.1.10)
 ;; WHEN: Sat Mar 11 13:06:21 2017
 ;; MSG SIZE rcvd: 27
```

Question 9.

For this we query one of the authoritative nameservers for the domain yahoo.com (which can be obtained from the response in Question 7), e.g. ns2.yahoo.com.

```
-bash-4.2$ dig @ns2.yahoo.com yahoo.com MX

 ; <<>> DiG 9.7.3 <<>> @ns2.yahoo.com yahoo.com MX
 ; (2 servers found)
 ;; global options: +cmd
 ;; Got answer:
 ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34867
 ;; 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 ns5.yahoo.com.
 yahoo.com. 172800 IN NS ns4.yahoo.com.
 yahoo.com. 172800 IN NS ns1.yahoo.com.
 yahoo.com. 172800 IN NS ns3.yahoo.com.
 yahoo.com. 172800 IN NS ns2.yahoo.com.

 ;; ADDITIONAL SECTION:
 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
 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

 ;; Query time: 342 msec
 ;; SERVER: 2001:4998:140::1002#53(2001:4998:140::1002)
 ;; WHEN: Sat Mar 11 13:10:30 2017
 ;; MSG SIZE rcvd: 360
```

Question 10:

Assuming that current hostname is drum01.cse.unsw.edu.au. First query for the IP address of the root nameservers.

```
-bash-4.1$ dig . NS
; <<>> DiG 9.7.3 <<>> . NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42845
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;. IN NS

;; ANSWER SECTION:
. 2305 IN NS b.root-servers.net.
. 2305 IN NS c.root-servers.net.
. 2305 IN NS h.root-servers.net.
. 2305 IN NS f.root-servers.net.
. 2305 IN NS i.root-servers.net.
. 2305 IN NS e.root-servers.net.
. 2305 IN NS a.root-servers.net.
. 2305 IN NS g.root-servers.net.
. 2305 IN NS d.root-servers.net.
. 2305 IN NS k.root-servers.net.
. 2305 IN NS m.root-servers.net.
. 2305 IN NS j.root-servers.net.
. 2305 IN NS l.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 63431 IN A 198.41.0.4
a.root-servers.net. 83017 IN AAAA 2001:503:ba3e::2:30
b.root-servers.net. 174722 IN A 192.228.79.201
b.root-servers.net. 149835 IN AAAA 2001:500:84::b
c.root-servers.net. 148572 IN A 192.33.4.12
c.root-servers.net. 174722 IN AAAA 2001:500:2::c
d.root-servers.net. 400286 IN A 199.7.91.13
d.root-servers.net. 124000 IN AAAA 2001:500:2d::d
e.root-servers.net. 66037 IN A 192.203.230.10
f.root-servers.net. 4330 IN A 192.5.5.241
f.root-servers.net. 149835 IN AAAA 2001:500:2f::f
g.root-servers.net. 54415 IN A 192.112.36.4
h.root-servers.net. 391257 IN A 198.97.190.53

;; Query time: 1 msec
;; SERVER: 129.94.208.3#53(129.94.208.3)
;; WHEN: Tue Mar 8 15:51:07 2016
;; MSG SIZE rcvd: 496
```

Next query one of the root nameservers as follows:

```
-bash-4.1$ dig @198.41.0.4 drum01.cse.unsw.edu.au NS
; <<>> DiG 9.7.3 <<>> @198.41.0.4 drum01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47294
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 15
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;drum01.cse.unsw.edu.au. IN NS

;; 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: 170 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Mar 8 15:54:18 2016
;; MSG SIZE rcvd: 492
```

We are being referred to the .au nameservers, so query one of them as follows:

```
-bash-4.1$ dig @58.65.254.73 drum01.cse.unsw.edu.au NS
; <<>> DiG 9.7.3 <<>> @58.65.254.73 drum01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56009
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 8
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;drum01.cse.unsw.edu.au. IN NS

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

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

;; Query time: 15 msec
;; SERVER: 58.65.254.73#53(58.65.254.73)
;; WHEN: Tue Mar 8 15:57:50 2016
;; MSG SIZE rcvd: 280
```

We are being referred to the edu.au. nameservers, so query one of them as follows:

```
-bash-4.1$ dig @37.209.192.5 drum01.cse.unsw.edu.au NS

; <<>> DiG 9.7.3 <<>> @37.209.192.5 drum01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38088
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 5
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;drum01.cse.unsw.edu.au. IN NS
;; AUTHORITY SECTION:
unsw.edu.au. 14400 IN NS ns2.unsw.edu.au.
unsw.edu.au. 14400 IN NS ns1.unsw.edu.au.
unsw.edu.au. 14400 IN NS ns3.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au. 14400 IN A 129.94.0.192
ns1.unsw.edu.au. 14400 IN AAAA 2001:388:c:35::1
ns2.unsw.edu.au. 14400 IN A 129.94.0.193
ns2.unsw.edu.au. 14400 IN AAAA 2001:388:c:35::2
ns3.unsw.edu.au. 14400 IN A 192.155.82.178

;; Query time: 2 msec
;; SERVER: 37.209.192.5#53(37.209.192.5)
;; WHEN: Tue Mar 8 16:08:30 2016
;; MSG SIZE rcvd: 198
```

Now we are being referred to the UNSW nameservers, so query one of them as follows:

```
-bash-4.1$ dig @129.94.0.192 drum01.cse.unsw.edu.au NS

; <<>> DiG 9.7.3 <<>> @129.94.0.192 drum01.cse.unsw.edu.au NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55902
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;drum01.cse.unsw.edu.au. IN NS

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

;; ADDITIONAL SECTION:
maestro.orchestra.cse.unsw.edu.au. 10800 IN A 129.94.242.33
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

;; Query time: 3 msec
;; SERVER: 129.94.0.192#53(129.94.0.192)
;; WHEN: Tue Mar 8 16:10:18 2016
;; MSG SIZE rcvd: 160
```

We are now being referred to the CSE nameservers, so we query one of them as follows. However, note that this time the query should be for a type A address (all previous queries were for type NS).

```
-bash-4.1$ dig @129.94.242.33 drum01.cse.unsw.edu.au A

; <<>> DiG 9.7.3 <<>> @129.94.242.33 drum01.cse.unsw.edu.au A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25158
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;drum01.cse.unsw.edu.au. IN A

;; ANSWER SECTION:
drum01.cse.unsw.edu.au. 3600 IN A 129.94.209.31

;; 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 129.94.208.3

;; Query time: 0 msec
;; SERVER: 129.94.242.33#53(129.94.242.33)
;; WHEN: Tue Mar 8 16:14:09 2016
;; MSG SIZE rcvd: 144
```

The IP address for drum01.cse.unsw.edu.au is 129.94.209.31. Following the iterative query process starting at the root nameserver, we had to query 5 DNS servers (a.root-servers.net, a.au, x.au, unsw.edu.au, maestro.orchestra.cse.unsw.edu.au).

Question 11.

Yes, a machine may have several network interfaces. Moreover, a network interface can have several IP addresses associated with it at any given time. An IP address may have been associated with several hostnames (additional hostnames are known as "aliases").

Resource created 4 months ago (Wednesday 29 April 2020, 03:56:57 PM), last modified about a month ago (Monday 13 July 2020, 03:34:14 PM).

Comments

(/COMP3331/20T2/forums/search?forum_choice=resource/44914)

(/COMP3331/20T2/forums/resource/44914)

Add a comment

There are no comments yet.