Question 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 query is needed is type A, which provides the name-value pairing that corresponds to the host name and the IP address.

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.

The canonical name for the CECS ANU web server is rproxy.cecs.anu.edu.au. Its IP address is 150.203.161.98 (same as above). The reason for having an alias is to abstract the hostname so that people wanting to access the IP address are able to use a simpler URL to access it.

Question 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 indicates the authoritative name server(s) that are the ultimate authority for answering DNS queries about that domain, as opposed to the local DNS server which occasionally answer queries about the domain if this information is in its cache. The response indicates that the the authoritative name servers are ns2.cecs.anu.edu.au, ns3.cecs.anu.edu.au, ns4.cecs.anu.edu.au (canonical names).

The additional section contains additional information regarding other servers that do not directly answer the original DNS query. This shows the IP addresses of ns2.cecs.anu.edu.au (in 32-bit and 128-bit), ns3.cecs.anu.edu.au and ns4.cecs.anu.edu.au.

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

The output below illustrates the the IP address of the local nameserver for my machine is 129.94.242.45. Priority is given to the first IP address in the list and DNS queries are sent only to the subsequent IP address listed if the prior one cannot resolve the query.

```
vx3 % cat /etc/resolv.conf
domain orchestra.cse.unsw.EDU.AU.
nameserver 129.94.242.45
nameserver 129.94.242.2
nameserver 129.94.242.33
options rotate
search orchestra.cse.unsw.EDU.AU. cse.unsw.EDU.AU. unsw.EDU.AU.
vx3 %
```

Question 5. What are the DNS nameservers for the “cecs.anu.edu.au” domain (note: the domain name is cecs.anu.edu.au and notwww.cecs.anu.edu.au)? Find out their IP addresses? What type of DNS query is sent to obtain this information?

The DNS nameservers for the “cecs.anu.edu.au” domain are the authoritative servers for the cecs.anu.edu.au domain listed under the authority section of the query below. These nameservers are ns4.cecs.anu.edu.au, ns2.cecs.anu.edu.au, ns3.cecs.anu.edu.au. Their IP addresses are contained in the additional section of the query - which are 150.203.161.38, 150.203.161.36, 150.203.161.50 respectively. Any type of query to any IP address within the “cecs.anu.edu.au” domain will show the authoritative name servers for the “cecs.anu.edu.au” domain under the authority section of the query. To find the corresponding IP addresses, we can use a A type query with the authoritative name server’s name if this information is not in the additional section.

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

;; ANSWER SECTION:
cecs.anu.edu.au.        3263    IN      A       150.203.161.98

;; AUTHORITY SECTION:
cecs.anu.edu.au.        804     IN      NS      ns4.cecs.anu.edu.au.
cecs.anu.edu.au.        804     IN      NS      ns2.cecs.anu.edu.au.
cecs.anu.edu.au.        804     IN      NS      ns3.cecs.anu.edu.au.

;; ADDITIONAL SECTION:
ns2.cecs.anu.edu.au.    805     IN      A       150.203.161.36
ns2.cecs.anu.edu.au.    805     IN      AAAA    2001:388:1034:2905::24
ns3.cecs.anu.edu.au.    2833    IN      A       150.203.161.50
ns3.cecs.anu.edu.au.    804     IN      AAAA    2001:388:1034:2905::32
ns4.cecs.anu.edu.au.    805     IN      A       150.203.161.38
ns4.cecs.anu.edu.au.    805     IN      AAAA    2001:388:1034:2905::26
```

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?

The DNS name(s) associated with the IP address above are:

www.engineering.unsw.edu.au, engplws008.ad.unsw.edu.au, engplws008.eng.unsw.edu.au. The type of DNS query sent to obtain this information is a ptr query, which returns a pointer to a canonical name.

```
; <<>> DiG 9.7.3 <<>> ptr 109.158.171.149.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30200
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;109.158.171.149.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
109.158.171.149.in-addr.arpa. 1387 IN   PTR     www.engineering.unsw.edu.au.
109.158.171.149.in-addr.arpa. 1387 IN   PTR     engplws008.ad.unsw.edu.au.
109.158.171.149.in-addr.arpa. 1387 IN   PTR     engplws008.eng.unsw.edu.au.

;; AUTHORITY SECTION:
158.171.149.in-addr.arpa. 8587  IN      NS      ns3.unsw.edu.au.
158.171.149.in-addr.arpa. 8587  IN      NS      ns1.unsw.edu.au.
158.171.149.in-addr.arpa. 8587  IN      NS      ns2.unsw.edu.au.

;; ADDITIONAL SECTION:
ns1.unsw.edu.au.        8981    IN      A       129.94.0.192
ns1.unsw.edu.au.        833     IN      AAAA    2001:388:c:35::1
ns2.unsw.edu.au.        8981    IN      A       129.94.0.193
ns2.unsw.edu.au.        833     IN      AAAA    2001:388:c:35::2
```

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)

We get the mailservers mta5.am0.yahoodns.net, mta6.am0.yahoodns.net, mta7.am0.yahoodns.net (also shown in the screenshot below)

The answer did not come directly from an authoritative server as the “aa” (authoritative answer) flag is missing from the DNS response header.

```
vx3 % 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: 52843
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 8

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

;; ANSWER SECTION:
yahoo.com.              1508    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              1508    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1508    IN      MX      1 mta5.am0.yahoodns.net.

;; AUTHORITY SECTION:
yahoo.com.              83161   IN      NS      ns3.yahoo.com.
yahoo.com.              83161   IN      NS      ns5.yahoo.com.
yahoo.com.              83161   IN      NS      ns4.yahoo.com.
yahoo.com.              83161   IN      NS      ns1.yahoo.com.
yahoo.com.              83161   IN      NS      ns2.yahoo.com.
```

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

There is an error resolving the DNS query because the recursion is requested but not available, as can be seen in the screenshot below. So the nameserver in Question 5 could potentially be blocking recursive DNS queries.

```
vx3 % dig @150.203.161.38 yahoo.com MX

; <<>> DiG 9.7.3 <<>> @150.203.161.38 yahoo.com MX
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 23537
;; 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: 7 msec
;; SERVER: 150.203.161.38#53(150.203.161.38)
;; WHEN: Tue Mar 12 11:17:24 2019
;; MSG SIZE  rcvd: 27
```

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

We query one of the authoritative servers of yahoo.com for the mail servers of yahoo.com (send a type MX query to yahoo.com). This obtains an authoritative answer.

```
Cvx3 dig @68.180.131.16 yahoo.com MX

 <<>> DiG 9.7.3 <<>> @68.180.131.16 yahoo.com MX
 (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39617
; 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:
ahoo.com.               1800    IN      MX      1 mta7.am0.yahoodns.net.
ahoo.com.               1800    IN      MX      1 mta5.am0.yahoodns.net.
ahoo.com.               1800    IN      MX      1 mta6.am0.yahoodns.net.

; AUTHORITY SECTION:
ahoo.com.               172800  IN      NS      ns5.yahoo.com.
ahoo.com.               172800  IN      NS      ns4.yahoo.com.
ahoo.com.               172800  IN      NS      ns2.yahoo.com.
```

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?

We use the name-server a.root-servers.net with IP address 198.41.0.4 (found through a DNS type A query) to find the authoritative name server for the “au” domain.

We use the name-server a.au with IP address 58.65.254.73 (found through the previous DNS query) to find the authoritative nameserver for the edu.au domain.

We use the name-server r.au (canonical name for edu.au) with IP address 65.22.197.1 (found through the previous DNS query) to find the authoritative nameserver for the unsw.edu.au.

We use the name-server ns1.unsw.edu.au (canonical name for unsw.edu.au) with IP address 129.94.0.192 (found through previous DNS query) to find the authoritative nameserver for cse.unsw.edu.au.

We use the name-server beethoven.orchestra.cse.unsw.edu.au (canonical name for cse.unsw.edu.au) with IP address 129.94.172.11 (found through previous DNS query) to find to find the IP address associated with our hostname (found through a simple hostname lookup).

This returns 129.94.242.117.

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

Many single physical machines have several names associated with it as many servers have a canonical name (real name) and an alias name (often a shorter and simpler alias for this canonical name).

It is possible for one physical machine to have multiple IP addresses on it. This is so that bottlenecks can be avoided. As a result, one physical machine can also have multiple canonical names associated with it.