**LAB 3**

**Exercise 3: Digging into DNS (marked, include in the lab report)**

**Question 1. What is the IP address of**[**www.cecs.anu.edu.au**](http://www.cecs.anu.edu.au/)**. What type of DNS query is sent to get this answer?**

A screenshot of text

Description automatically generated

query of type A is sent to get the IP address of [www.cecs.anu.edu.au](http://www.cecs.anu.edu.au/). The IP address is

150.203.161.98

**Question 2. What is the canonical name for the CECS ANU web server? 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. The IP address of is 150.203.161.98. The reason for having an alias is that it can be easily remembered and identified.

**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 sections show details of the authoritative server. There are 3 NS records, in which the TTL is 300.

And the Additional sections display IP address of these authoritative server. The type AAAA is the IPv6 address for this domain server.

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

The IP address of the local nameserver is showed at the bottom. That is 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**](http://www.cecs.anu.edu.au/)**)? Find out their IP addresses? What type of DNS query is sent to obtain this information?**

**A screenshot of text

Description automatically generated**

Their IP addresses are 150.203.161.36, 150.203.161.50, 150.203.161.38. The type of query is NS

**Question 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?**

**A screenshot of a cell phone

Description automatically generated**

The type of DNS query is PTR. The DNS name associated with 111.68.101.54 is webserver.seecs.nust.edu.pk.**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**](http://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)**

the first step is to query the nameserver for the authoritative hostname of mail server of Yahoo! Mail. the response is shown below.

**A close up of text on a black background

Description automatically generated**

the flags include:

qr – Query?

rd – [Recursion Desired](https://serverfault.com/a/373017/218198)

ra -- [Recursion Available](https://serverfault.com/a/373017/218198)

and aa (authoritative answer) is not included, so this is not an authoritative answer

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

**A screenshot of a cell phone

Description automatically generated**

The query is refused

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

A close up of text on a black background

Description automatically generated

there are 3 mail servers: mta5.am0.yahoodns.net, mta7.am0.yahoodns.net and mta6.am0.yahoodns.net. The type of query is MX

**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?**

**(1) find the name server of “.” domain**

**A screenshot of a cell phone

Description automatically generated**

(2) find the authoritative name server for the “au.” domain

A screenshot of a cell phone

Description automatically generated

(3) find the authoritative name server for the “edu.au.” domain

A screenshot of a cell phone

Description automatically generated

(4) find the authoritative name server for the “unsw.edu.au.” domain

A screenshot of text

Description automatically generated

(5) find the authoritative name server for the “cse.unsw.edu.au.” domain

A screenshot of a cell phone

Description automatically generated

(5) find the authoritative name server for the “**lyre00.cse.unsw.edu.au**” domain

A screenshot of a cell phone

Description automatically generated

the IP address of my machine is 129.94.242.20. I query 6 servers to get the answer

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

yes, a machine may have multiple names as well as IP addresses associated. Actually, this is also a common fact. For example, a machine may be both connected to Internet by Wifi and Lan. Then it may has 2 IP addresses. Also, for a server, it’s essential to have multiple IP addresses, especially when there is need implement server virtualization.

.