# ***Lab3: DNS and Socket programming***

## ***EXERCISE 3***

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

IP address: 150.203.161.98
Query sent: dig www.cecs.anu.edu.au A

**Question 2. What is the canonical name for the CECS ANU web server? Suggest a reason for having an alias for this server.**

CNAME: rproxy.cecs.anu.edu.au
Alias names are very useful because the owner will be able to run multiple services to the same address but just using different domain names. Eg. Mail.google.com and maps.google.com

**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 details the servers that have ultimate authority for answering DNS queries about the domain. The three servers are:

| | | | | |
|---|---|---|---|---|
| anu.edu.au. | 632 | IN | NS | ns1.anu.edu.au. |
| anu.edu.au. | 632 | IN | NS | una.anu.edu.au. |
| anu.edu.au. | 632 | IN | NS | ns.adelaide.edu.au. |

The additional section details data that relates to the query but does no strictly answer the question. There is one server in the additional section:

| | | | | |
|---|---|---|---|---|
| ns.adelaide.edu.au. | 8754 | IN | A | 129.127.40.3 |

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

Local name server: 129.94.0.196

**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 are: (found using dig cecs.anu.edu.au NS)

| | | | | | |
|---|---|---|---|---|---|
| cecs.anu.edu.au. | 300 | IN | NS | ns2.cecs.anu.edu.au. | IP: 150.203.161.36 |
| cecs.anu.edu.au. | 300 | IN | NS | ns3.cecs.anu.edu.au. | IP: 150.203.161.50 |
| cecs.anu.edu.au. | 300 | IN | NS | ns4.cecs.anu.edu.au. | IP: 150.203.161.38 |

I then used dig @hostname A on all of them to get their respective IP

**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?**

Name: webserver.seecs.nust.edu.pk.
Command: dig -x 111.68.101.54

**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)**

No authoritative answer was given. In the flags section, there was no AA, meaning that there was no authoritative answer.
flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
This is because the CSE server is not connected to Yahoo.

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

Using ns2.cecs.anu.edu.au. IP: 150.203.161.36, there was also no answer. This is probably because ANU and yahoo mail aren't connected.
flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

Command: dig @ns1.yahoo.com yahoo.com MX

| | | | | |
|---|---|---|---|---|
| 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. |

There are 3 Authoritative Answers.

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?

| | |
|---|---|
| Query 1: dig @198.41.0.4 flute16.cse.unsw.edu.au | .au Authoritative NS |
| Query 2: dig @162.159.25.38 flute16.cse.unsw.edu.au | .edu.au |
| Query 3: dig @65.22.196.1 flute16.cse.unsw.edu.au | .unsw.edu.au |
| Query 4: dig @129.94.0.192 flute16.cse.unsw.edu.au | .cse.unsw.edu.au |
| Query 5: dig @129.94.208.3 flute16.cse.unsw.edu.au | Flute16.cse.unsw.edu.au |

IP Address is: 129.94.210.106
It took 5 queries to get the IP of my machine

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

Yes, a machine can have multiple names are IP addresses associated with it. Those extra names and IPs are aliases.