Student Name: Luyang Ye
Student zID: z5280537

Lab Exercise 3: DNS & Socket Programming

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

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 of www.cecs.anu.edu.au is 150.203.161.98.
The type of DNS query sent to get this answer is Type A.

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.
Maybe having an alias for this server is easier for users to remember it.

Question 3. What can you make of the rest of the response (i.e. the details available in the Authority and Additional sections)?

In the authority section, it shows that q.au, r.au, t.au and s.au are the authority for answer DNS queries about the queried domain.

In the additional section, it shows eight IP addresses for q.au, r.au, s.au and t. au. Because it shows both IPv4 IP address and IPv6 IP address, so there are 8 IP addres here.

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

The IP address of the local nameserver for my machine is 129.94.208.2.

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)? 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 ns2.cecs.anu.edu.au, ns3.cecs.anu.edu.au, ns4.cecs.anu.edu.au.

Their corresponding IPv4 addresses are 150.203.161.36, 150.203.161.50, 150.203.161.38.

Their corresponding IPv6 addresses are 2001:388:1034:2905::24, 2001:388:1034:2905::32, 2001:388:1034:2905::26.

The type of DNS query sent to obtain this information 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?

The DNS name asociated with the IP address 111.68.101.54 is webserver.seecs.nust.edu.pk

The type of DNS query sent to obtain this information is PTR

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)

Although the response contains information in the authoritative part, I still didn't get an autoritative answer. The reason is that the flags of the response does not contain aa, which is the flag for 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?

I didn't get an response when I use ns2.cecs.anu.edu.au. The status of the message shows "REFUSED", I think that means the nameserver refused to reply DNS query from me.

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

The type of DNS query sent to obtain this information 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?

I have to query 6 DNS servers to get the authoritative answer. (All the screenshot of these 6 DNS servers are saved in another folder within the lab2.tar file.)

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

I think one physical machine can have several names an/or IP addresses associated with it. For example, if some virtual servers running on the same physical machine, then each of them will have an IP addresses. Also, another instance is that a host can have both name and alias.