**LAB 3**

**Exercise 1: Explore DNS records (Not marked, No need to submit)**

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Type id | Description | Function |
| A | 1 | Address record | Returns a 32-bit [IPv4](https://en.wikipedia.org/wiki/IPv4) address, most commonly used to map [hostnames](https://en.wikipedia.org/wiki/Hostname) to an IP address of the host, but it is also used for [DNSBLs](https://en.wikipedia.org/wiki/DNSBL), storing [subnet masks](https://en.wikipedia.org/wiki/Subnet_mask) in [RFC 1101](https://tools.ietf.org/html/rfc1101), etc. |
| CNAME | 5 | [Canonical name record](https://en.wikipedia.org/wiki/Canonical_name_record) | Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name. |
| MX | 15 | Mail exchange record | Maps a domain name to a list of [message transfer agents](https://en.wikipedia.org/wiki/Message_transfer_agent) for that domain |
| NS | 2 | Name server record | Delegates a [DNS zone](https://en.wikipedia.org/wiki/DNS_zone) to use the given [authoritative name servers](https://en.wikipedia.org/wiki/Authoritative_name_server) |
| PTR | 12 | [PTR Resource Record](https://en.wikipedia.org/w/index.php?title=PTR_Resource_Record&action=edit&redlink=1) [[de](https://de.wikipedia.org/wiki/PTR_Resource_Record)] | Pointer to a [canonical name](https://en.wikipedia.org/wiki/Canonical_name). Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing [reverse DNS lookups](https://en.wikipedia.org/wiki/Reverse_DNS_lookup), but other uses include such things as [DNS-SD](https://en.wikipedia.org/wiki/Zero_configuration_networking#Apple's_protocol:_Multicast_DNS/DNS-SD). |
| SOA | 6 | Start of  [a zone of] authority record | Specifies authoritative information about a [DNS zone](https://en.wikipedia.org/wiki/DNS_zone), including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone. |

### Exercise 2: Tracing DNS with Wireshark (Not marked, No need to submit)

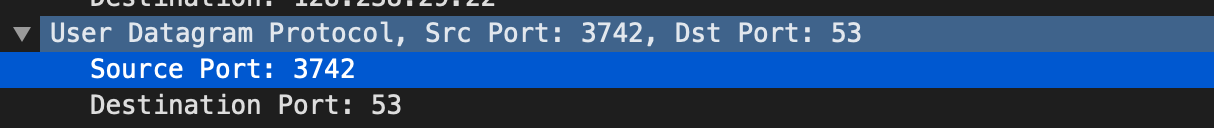
**Question 1: What transport layer protocol is being used by the DNS messages?**

UDP

A screenshot of a social media post

Description automatically generated

**Question 2: What is the source and destination port for the DNS query message and the corresponding response?**

****

**Question 3: To what IP address is the DNS query message sent? Is this the same as the default local DNS server?**

**A screenshot of a cell phone

Description automatically generated**

128.238.29.22. not the same.

**Question 4: How many “questions” are contained in the DNS query message? What “Type” of DNS queries are they? Does the query message also contain any “answers”?**

**A screenshot of a cell phone screen with text

Description automatically generated**

1 question in type A. It doesn’t contain any answers.

**Question 5: Examine the DNS response message. Provide details of the contents of the “Answers”, “Authority” and “Additional Information” fields. What can you infer from these?**

A screenshot of a cell phone

Description automatically generated

A close up of a sign

Description automatically generated

A close up of a sign

Description automatically generated

**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 records. And the Additional sections display IP address of these authoritative 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 address is 150.203.161.98. The type of query is A

**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 SOA. a.root-servers.net is the primary name server

**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)**

**A close up of text on a black background

Description automatically generated**

No, this is not a authoritative answer as the flags displayed are: qr, rd, ra. And they are respectively stand for:

qr --  Query?

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

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

And aa is not contained. ‘aa’ means 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 close up of text on a black background

Description automatically generated**

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

**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?**