

[Resources](#) / [Lab Exercises \(/COMP3331/21T1/resources/57481\)](#) / [Lab Exercise 3: Solutions](#)

# Lab Exercise 3: Solutions

## Exercise 1 (Not Marked)

Here is a short summary.

A = Internet address of the host (in IPv4 format); hostname to IP address mapping.

CNAME = canonical name of an alias; a machine may have several names (aliases) associated with it, but only one of them is the "real" one.

MX = mail exchanger; mail server for the domain. This is used by SMTP.

NS = nameserver; which nameserver is responsible for the domain.

PTR = pointer to a canonical name; IP address to hostname mapping.

SOA = domain's start-of-authority information; who is in charge for the administration of the domain.

## Exercise 2 (Not Marked)

Question 1. DNS uses UDP.

Question 2. Source port is 3742 and destination port is 53 for the query. For the response it is reversed, i.e. source port is 53 and destination port is 3742.

Question 3. The DNS query is sent to the IP address 128.238.29.22, which is the default local DNS server.

Question 4. There is only one "question" in the query message. It is of type A and is requesting for the IPv4 address for www.mit.edu (<http://www.mit.edu/>) .

Question 5. The response message contains one "Answer" which is the RR (resource record) for www.mit.edu (<http://www.mit.edu/>) . The RR is as follows:

```
www.mit.edu: type A, class inet, addr 18.7.22.83
```

In addition, there are three authoritative records which are the RRs for the authoritative name servers for mit.edu domain. These RRs are as follows:

```
mit.edu: type NS, class inet, ns BITSY.mit.edu mit.edu: type NS, class inet, ns STRAWB.mit.edu
```

Finally, there are also three additional RRs, which contain the type A records for the above three name servers. They are as follows:

```
BITSY.mit.edu: type A, class inet, addr 18.72.0.3 STRAWB.mit.edu: type A, class inet, addr 18.7
```

## Exercise 3.

Question 1.

The IP address of [www.eecs.berkeley.edu](https://eecs.berkeley.edu/) (<https://eecs.berkeley.edu/>) is 23.185.0.1 To get this answer we make a type A query.

```
192-168-1-109:~ z3116703$ dig www.eecs.berkeley.edu ; <<>> DiG 9.10.6 <<>> www.eecs.berkeley.edu
```

#### Question 2.

The CNAME is [live-eecs.pantheonsite.io](https://live-eecs.pantheonsite.io/). Canonical names are usually very long and hard to remember. An alias such as [www.eecs.berkeley.edu](https://eecs.berkeley.edu/) (<https://eecs.berkeley.edu/>) is more mnemonic and easy to remember. Aliasing is also useful when running multiple services (e.g. an email server and web server) from a single IP address.

#### Question 3.

The authority section contains NS resource records for the [eecs.berkeley.edu](https://eecs.berkeley.edu/) (<https://eecs.berkeley.edu/>) domain name. In other words, it indicates the four authoritative name servers for this particular domain name which are ns.1213.awsdns-23.org, ns.233.awsdns-29.com and ns.2013.awsdns-59.co.uk and ns.644.awsdns-16.net.

The additional section contains IP addresses for these four authoritative name servers (i.e. the type A resource records for the name servers). The AAAA records are for IPv6 addresses.

#### Question 4.

The information about the local nameserver is included at the bottom of the output, 129.94.242.2# 53 This is the local DNS server for the CSE network. The above query was made by connecting the CSE login servers via SSH.

#### Question 5.

We issue the following query, which is for an NS record.

```
-bash-4.2$ dig eecs.berkeley.edu.au NS ;;ANSWER SECTION: eecs.berkeley.edu. 72630 IN NS adns2.b
```

The name servers are adns2, adns1, ns.eecs, ans.CS and adns3. .berkeley.edu and their IP addresses are: 169.229.60.61, 169.229.60.153, 2607:f140:fff:ffe::3 and 1607:f140:a000;d:abc respectively. Note that, AAAA records are for IPv6 addresses.

#### Question 6.

For this, we use reverse DNS, i.e. we make a type PTR query for 125.158.171.149.in-addr.arpa. (note the reverse ordering of the IP address)

```
<>> DiG 9.10.6 <>>> -x 111.68.101.54 ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- op
```

The hostname corresponding to 111.68.101.54 is [webserver.seecs.nust.edu.pk](https://webserver.seecs.nust.edu.pk).

#### Question 7.

```
bash-4.1$ dig @129.94.208.3 yahoo.com MX ; <<>> DiG 9.8.3-P1 <<>> @129.94.208.3 yahoo.com MX ;
```

We see that the server we queried (orchestra.cse.unsw.edu.au) cannot give us an authoritative answer since the flags do not contain aa. This is because it has authority for only the cse.unsw.edu.au domain and not for the Yahoo domain.

#### Question No 8.

When we try with the ANU nameservers we do not get a response. This can be inferred from the fact that the status of the reply is REFUSED. The reason could be that these name servers do not reply to DNS queries that are sent from devices that are not part of the ANU network as a security measure.

```
-bash-4.2$ dig @ns1.anu.edu.au yahoo.com MX ; <<>> DiG 9.7.3 <<>> @ns1.anu.edu.au yahoo.com MX
```

#### Question 9.

For this we query one of the authoritative nameservers for the domain yahoo.com (which can be obtained from the response in Question 7), e.g. ns2.yahoo.com.

```
-bash-4.2$ dig @ns2.yahoo.com yahoo.com MX ; <<>> DiG 9.7.3 <<>> @ns2.yahoo.com yahoo.com MX ;
```

#### Question 10:

Assuming that current hostname is drum01.cse.unsw.edu.au. First query for the IP address of the root nameservers.

```
-bash-4.1$ dig . NS ; <<>> DiG 9.7.3 <<>> . NS ;; global options: +cmd ;; Got answer: ;; ->>HEA
```

Next query one of the root nameservers as follows:

```
-bash-4.1$ dig @198.41.0.4 drum01.cse.unsw.edu.au NS ; <<>> DiG 9.7.3 <<>> @198.41.0.4 drum01.c
```

We are being referred to the .au nameservers, so query one of them as follows:

```
-bash-4.1$ dig @58.65.254.73 drum01.cse.unsw.edu.au NS ; <<>> DiG 9.7.3 <<>> @58.65.254.73 drum
```

We are being referred to the edu.au. nameservers, so query one of them as follows:

```
-bash-4.1$ dig @37.209.192.5 drum01.cse.unsw.edu.au NS ; <<>> DiG 9.7.3 <<>> @37.209.192.5 drum
```

Now we are being referred to the UNSW nameservers, so query one of them as follows:

```
-bash-4.1$ dig @129.94.0.192 drum01.cse.unsw.edu.au NS ; <<>> DiG 9.7.3 <<>> @129.94.0.192 drum
```

We are now being referred to the CSE nameservers, so we query one of them as follows. However, note that this time the query should be for a type A address (all previous queries were for type NS).

```
-bash-4.1$ dig @129.94.242.33 drum01.cse.unsw.edu.au A ; <<>> DiG 9.7.3 <<>> @129.94.242.33 dru
```


The IP address for drum01.cse.unsw.edu.au is 129.94.209.31. Following the iterative query process starting at the root nameserver, we had to query 5 DNS servers (a.root-servers.net, a.au, x.au, unsw.edu.au, maestro.orchestra.cse.unsw.edu.au).

Question 11.

Yes, a machine may have several network interfaces. Moreover, a network interface can have several IP addresses associated with it at any given time. An IP address may have been associated with several hostnames (additional hostnames are known as "aliases").

Resource created [3 months ago \(Monday 08 February 2021, 02:38:33 PM\)](#), last modified [2 months ago \(Thursday 25 March 2021, 09:42:10 AM\)](#).

### Comments





 Add a comment

There are no comments yet.