Building a DNS cache

1. Check the version of BIND which is installed

```
# named -v
BIND 9.3.0
#
```

2. Start the cache and check it is running

```
Firstly, edit /etc/rc.conf and set
named_enable="YES"

Then run these commands:
# /etc/rc.d/named start
# ps auxwww | grep named
# tail /var/log/messages
Check for successful startup, no error messages.
```

> You may see errors about missing files "master/localhost.rev" and "master/localhost-v6.rev". You can fix this easily by running the following script which creates those files for you:
>
> ```
> # cd /etc/namedb
> # sh make-localhost
> ```
>
> This is something you only need to do once after installing your server.

---

3. Reconfigure your resolver to use your own cache only

Edit `/etc/resolv.conf` as follows:

```
search presanog.org.bt
nameserver 127.0.0.1
#nameserver 202.144.128.200
#nameserver 202.144.128.210
```

Remove any existing 'nameserver' lines, or comment them out by inserting '#' at the front as shown above.

4. Send some queries

Issue a query. Make a note of whether the response has the 'aa' flag set. Look at the answer section, note the TTL of the answer. Note how long the query took to process.

Then repeat the exact same query, and note the information again.

```
# dig www.tiscali.co.uk.    Does it have the 'aa' flag?    _______
                            What is the TTL of the answer? _______ seconds
                            How long is the Query Time?    _______ milliseconds

# dig www.tiscali.co.uk.    Does it have the 'aa' flag?    _______
                            What is the TTL of the answer? _______ seconds
                            How long is the Query Time?    _______ milliseconds
```

Repeat it a third time. Can you explain the differences?

5. Enable your cache to receive queries

The default configuration of bind under FreeBSD only accepts queries on the loopback interface (address 127.0.0.1). To enable queries from other addresses, edit `/etc/namedb/named.conf` and comment out this line:

```
    listen-on { 127.0.0.1; };

change this to:
//  listen-on { 127.0.0.1; };
```

Restart the name server. Get one of your neighbours to send some queries to your cache (remember dig @x.x.x.x hostname a)

6. Watch the cache in operation

You can take a snapshot of the cache contents like this:

```
# /usr/sbin/rndc dumpdb
# less /var/named/var/dump/named_dump.db
```

(Don't do this on a busy cache - you will generate a huge dump file!)

You can watch the cache making queries to the outside world using 'tcpdump' in a different window

```
# tcpdump -n -s1500 -i eth0 udp port 53
```

While this is running, in the first window flush your cache (so it forgets all existing data)

```
# rndc flush
# dig www.tiscali.co.uk.   -- and watch tcpdump output. What do you see?

# dig www.tiscali.co.uk.   -- watch tcpdump again. This time?
```

7. Tightening up the configuration

(If you have extra time)

Following the examples on the presentation, create zonefiles which map localhost to 127.0.0.1 and 127.0.0.1 to localhost, and test them.

Following the examples on the presentation, create an acl which restricts access to your cache to your machine only. Get someone else to try to resolve names using your cache. Remember:

rndc reload
    to make your modified configuration active
tail /var/log/messages
    to check for errors in your configuration