Exercise 2.3: Building a DNS cache

0. Become the Root User

For these exercises we will run as the root user. In order to become root
on your machine do:

```
$ sudo bash
```

and your prompt should change to a "#".

1. Check if BIND is installed

```
$ dpkg --get-selections | grep bind
```

If you do not see a _complete_ list like this:

```
bind9                                           install
bind9-host                                      install
bind9utils                                      install
libbind-confparser-perl                         install
libbind9-60                                     install
```

Then bind9 is not fully installed. The package "bind9" is the critical item.

For more details type about bind you can type:

```
$ aptitude show bind9
```

2. Install Bind version 9

```
# apt-get install bind9
```

Check the version of BIND which is installed

```
# named -v
BIND 9.7.0-P1
```

3. Check if BIND is running

Run these commands:

```
# ps aux | grep named
# grep bind /var/log/syslog
# service bind9 status
```

4. Update /etc/dhcp/dhclient.conf

At this time your machines are using dhcp to obtain an IP address. This would,
also, overwrite your /etc/resolv.conf file causing your resolver to no longer
query your machine by default.

But you can tell the DHCP client to automatically add the nameseervers you
choose by modifying the file /etc/dhcp/dhclient.conf:

To fix this edit the file:

```
# vi /etc/dhcp/dhclient.conf
```

Find the line that states:

```
#prepend domain-name-servers 127.0.0.1;
```

and change it to:

```
prepend domain-name-servers 127.0.0.1;
```

(remove the #)

let's manually shutdown then restart the DHCP client on your machine:

```
# ps auxwww | grep dhclient3
```

You should see a line similar to this:

```
root       531  0.0  0.1   2928   800 ?        Ss   Apr16   0:00
dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.pid -lf /var/
lib/dhcp/dhclient.eth0.leases -1 eth0
```

Note the Process ID (pid) of the dhclient process that is running. In this
case, it is 531. On your machine it will be different. You will need this in
order to shut down the client. To stop the client type:

```
# kill <ProcessID>
```

Now, restart the DHCP client (please copy this line - don't try and type it in!

```
# dhclient3 -e IF_METRIC=100 -pf /var/run/dhclient.eth0.pid
-lf /var/lib/dhcp/dhclient.eth0.leases -1 eth0
```

Finally, we need to make sure that your /etc/resolv.conf file has the correct entries.
Take a look at it.

It should look something like this now:

```
nameserver 127.0.0.1
nameserver 10.10.0.241
nameserver 10.10.0.242
```

5. Opening BIND to external requests

```
        # vi /etc/bind/named.conf.options
```

In the file add the following lines under the options

```
        recursion yes;
        allow-recursion { any; };
        listen-on       { any; };
```

Save the file and restart bind

```
        # service bind9 stop

        # service bind9 start
```

5. Send some queries

Issue a query. Make a note of whether the response has the 'aa' flag set.
Look at the answer section and note the TTL of the answer. Also 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?

If your neighbour has got their cache working, then try sending some queries
to their cache (remember `dig @x.x.x.x ...`)

6. Watch the cache in operation

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

```
# /usr/sbin/rndc dumpdb
# less /var/cache/bind/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 tcpdump is running, in the first window flush your cache (so it forgets all
existing data) and then issue some queries.

```
# 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. Using a Forwarding Name Server

Try querying the DNS for one of our workshop machines:

```
        # pc.ws.nsrc.org
```

You should receive an ANSWER: 0 response (i.e. it fails).

The Authoritative Name Server for our class DNS name space (ws.nsrc.org) is located
at 10.10.0.241. Since we have updated your /etc/resolv.conf file to no longer use
this name server queries for the domain ws.nsrc.org we need to tell our caching
name server to use 10.10.0.241 as a forwarding name server. This means we'll make
all our DNS requests to this server, but we'll still be caching the results locally.

To do this do:

```
        # vi /etc/bind/named.conf.options
```

And replace the section that looks like:

```
        // forwarders {
        //      0.0.0.0;
        // };
```

With:

```
        forwarders {
                10.10.0.241;
        };
```

Save the file and restart bind:

```
        # service bind9 restart
```

Now trying querying again:

```
        # dig pc1.ws.nsrc.org
```

And you should get a proper response.

8. Tightening up the configuration (optional)

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.

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/syslog      # to check for errors in your configuration
```