Building a DNS cache

1. Configuring a Caching Server on a FreeBSD 5.3 Box.

1.1. FreeBSD 5.3 comes out of the box configured as a cache server, so you really do not need to configure it.

1.2.The named configuration file is /var/named/etc/namedb/named.conf and the entries for a caching nameserver are as follows.

```
options {
        directory       "/etc/namedb";
        pid-file        "/var/run/named/pid";
        dump-file       "/var/dump/named_dump.db";
        statistics-file "/var/stats/named.stats";

        listen-on { 127.0.0.1; 196.200.219.200; };
};

zone "." {
        type hint;
        file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
        type master;
        file "master/localhost.rev";
};
```

1.3. Change directory to /var/named/etc/namedb

```
# cd /var/named/etc/namedb
```

1.4. Run the following command to create the localhost.rev file.

```
# sh make-localhost
```

1.5. To set up the server to startup the named daemon (BIND) whenever the machine is started or rebooted, edit the /etc/rc.conf file and add the following line.

```
named_enable=”YES”
```

1.6. Start the caching nameserver with the following command.

```
# /etc/rc.d/named start
```

1.7. Check the log file to ensure that it started without any errors.

```
# tail /var/log/messages
```

2. Reconfigure your resolver to use your own cache only.

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

```
search e1.ws.afnog.org
nameserver 127.0.0.1    <--- This line is what you need to add
#nameserver 196.200.219.200
#nameserver 196.200.222.1
```

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

3. 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 yahoo.com.    Does it have the 'aa' flag?    ______
                    What is the TTL of the answer? ______ secs
                    How long is the Query Time?    ______ msecs

# dig yahoo.com.    Does it have the 'aa' flag?    ______
                    What is the TTL of the answer? ______ secs
                    How long is the Query Time?    ______ msecs
```

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

Try sending some queries to your neighbour's cache.

4. Watch the cache in operation

4.1. Dump the contents in cache:

```
# /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. **(Hint: use ifconfig to determine the name of your ethernet device and replace rl0 with yours).**

```
# tcpdump -n -s1500 -i rl0 udp port 53
```

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

```
# rndc flush
# dig yahoo.com.   -- and watch tcpdump output. What do you see?
# dig yahoo.com.   -- watch tcpdump again. This time?
```

5 Tightening up the configuration

(If you have extra time)

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:

```
acl mynetwork { 127.0.0.1; 196.200.219.20 };
options {
        directory       "/etc/namedb";
        pid-file        "/var/run/named/pid";
        dump-file       "/var/dump/named_dump.db";
        statistics-file "/var/stats/named.stats";

        listen-on       { 127.0.0.1; 196.200.219.200; };
        recursion       yes # this is the default
        allow-query     { mynetwork; };

# note: use 'allow-recursion' instead if your
# nameserver is both caching and authoritative
};
```

rndc reload

    to make your modified configuration active

tail /var/log/messages

    to check for errors in your configuration

6 Changing the default location of your log files

(If you have extra time)

Add the following lines to your /var/named/etc/namedb/named.conf file.

```
logging {
        channel default_log {
                file "/var/log/named.log" versions 3 size 10m;
                print-time yes;
                print-category yes;
                print-severity yes;
                severity info;
        };
        channel xfrs {
                file "/var/log/xfer.log" versions 5 size 5m;
                print-time yes;
                print-category yes;
                print-severity yes;
                severity info;
        };
        channel qrs {
                file "/var/log/queries.log" versions 5 size 5m;
                print-time yes;
                print-category yes;
                print-severity yes;
                severity info;
        };
        category default { default_log; };
        category xfer-in { xfrs; };
        category xfer-out { xfrs; };
        category queries { qrs; };
};
```

*****Remember:

rndc reload

to make your modified configuration active

tail /var/log/messages

to check for errors in your configuration

now tail /var/named/var/log/named.log

to check for errors in your configuration