DNS Exercise - Delegation

In this exercise, we will create a new TLD in our root.
for example: MYTLD

You will create a master nameservice on your own machine, and you will get secondary service from the instructor, provided by "auth1.grpYYY.dns.nsrc.org" (YYY is the group of the instructor, which will be communicated in class).

Then you will ask the administrator for the domain above you (the root) to delegate your domain to you - this is also the instructor.

Note: the following should be done as the "root" superuser - use sudo -s

Firstly, note that your hostname is configured correctly on your machine. Check that it is configured correctly by using the 'hostname' command - e.g. on auth1.grpXX.dns.nsrc.org, if you type:

```
 # hostname
```

You should see:

```
  auth1.grpXX.dns.nsrc.org
```

If not, then configure your server with its name: e.g. for auth1.grp25.dns.nsrc.org, type:

```
 # hostname auth1.grp25.dns.nsrc.org
```

Remember to replace "grpXX" with the the proper group number!

Edit the file /etc/rc.conf (using "vi" or "ee", i.e.: ee /etc/rc.conf), and update the "hostname":

```
  hostname="auth1.grpXX.dns.nsrc.org"
```

In the file /etc/hosts, you should see a line:

```
  10.20.X.1   auth1.grpXX auth1.grpXX.dns.nsrc.org
```

Exercise

* Choose a new domain, write it down somewhere

  i.e.: "MYTLD" or "EARTH" - whatever you feel like.

  (Do NOT choose any of the PC names, e.g. `auth1.grpXX`, as your subdomain)

  This could for example be the name of your country code, country name, company name, etc... but REMEMBER that someone might pick the same name! First come, first serve.

* If we are using the web interface for registration (RZM):

  Register your new domain using the classroom root zone manager at https://rzm.dnssek.org/

Username is your MYTLD
Password is up to you but you must remember it for later exercises.
Click the "Signup" button.

The next page is an example of a two-factor security system. Unless told by instructor, leave the "verification code" field blank and simply click "Proceed". You will be able to return to this page later to configure your security token (e.g. Google Authenticator) if desired.

Click logout on the next page. You will fill the information in later.

* Create your zone file in `/etc/namedb/master/MYTLD`
(where MYTLD is your chosen domain) -- you can pretty much "copy and paste" the section below -- but remember to update the XXX with your IP:

*** Remember, you will need to become root to create this file,
*** so, e.g.
***
*** $ cd /etc/namedb/master
*** $ sudo vi MYTLD
***
*** (feel free to use another editor instead of vi, e.g. joe, ee)

```
- - - - - - - - - - - - - cut below - - - - - - - - - - - - -

$TTL 2m
@       IN      SOA     auth1.grpXX.dns.nsrc.org. your.email.address. (
                        2012022301    ; Serial - replace 20120223 with the date
                        10m           ; Refresh
                        5m            ; Retry
                        4w            ; Expire
                        2m )          ; Negative

        IN      NS      auth1.grpXXX.dns.nsrc.org.   ; master
        IN      NS      auth1.grpYYY.dns.nsrc.org.   ; slave at instructor

www     IN      A       10.20.XXX.1             ; your own IP

- - - - - - - - - - - - - cut above - - - - - - - - - - - - -
```

Replace `your.email.address.` with your home E-mail address, so that user@domain.name becomes user.domain.name

XXX and YYY are the IP of your group, and your slave's, respectively.

We have chosen purposely low values for TTL, refresh, and retry to make it easier to fix problems in the classroom. For a production domain you might use higher values.

* Edit `/etc/namedb/named.conf` and do the following:

*** Remember, you will need to become root to edit this file,
*** so, e.g.
***
*** $ cd /etc/namedb
*** $ sudo vi named.conf

```
  ***
  ***   (feel free to use another editor instead of vi, e.g. joe, ee)

    - If it is still there, REMOVE the following line:

         listen-on { 127.0.0.1; };

    ... and add another line in the options section:

        allow-query { any; };

    ... so that your nameserver will now answer queries from the network

    - Add a section to configure your machine as master for
      your domain, by adding something like this at the end
      (the bottom) of the file:

      zone "MYTLD" {
        type master;
        file "/etc/namedb/master/MYTLD";
      };

    Pay attention to the ';' and '}' !

*   Check that your config file and zone file are valid:

        # named-checkconf
        # named-checkzone MYTLD /etc/namedb/master/MYTLD

    * If there are any errors, correct them ! *

*   If we are not using the web interface for registration of domain names:

    Tell the instructor managing grpYYY that you need secondary service for
    your domain - tell them the domain and tell them what your group number is.

    For instance, if the domain is "COCONUT", and you are Group 5, you
    should write on a piece of paper

COCONUT. NS  auth1.grp5.dns.nsrc.org.
COCONUT. NS  auth1.grpYYY.dns.nsrc.org.   (YYY = the group of the instructor)

    And give this to the instructor managing grpYYY

*   If this is not already done, enable named in your server's configuration,
    by editing the file /etc/rc.conf and adding, if this is not already done:

     ** Remember, again, you need to be root to edit this file

        named_chrootdir=""
        named_enable="YES"

    - Then start/restart named with

        # service named restart

    Check the result with

        # tail /var/log/messages
```

Verify with dig that MYTLD is now configured on your host:

```
# dig @10.20.XX.1 MYTLD. NS
```

Where "XX" is the group number of your machine.

You can also check the nameserver status using rndc:

```
# rndc status
```

- If there are any errors, correct them. Some configuration errors can cause the daemon to die completely, in which case you may have to start it again after correcting the problem:

```
# service named restart
```

* Check that you and the instructor slave at grpYYY are giving authoritative answers for your domain:

```
# dig +norec @10.20.XXX.1 MYTLD. SOA
# dig +norec @10.20.YYY.1 MYTLD. SOA
```

Check that you get an AA (authoritative answer) from both, and that the serial numbers match.

* Now you are ready to request delegation:

a) if using the RZM:

Go to https://rzm.dnssek.org/

Login using the Username/Password you used at the begining of the exercise. Click "Proceed"

Enter your nameserver, e.g., auth1.grpXX.dns.nsrc.org and IP address for it, e.g., 10.20.X.1

Click "Update". If all goes well, your entry should show up with a document icon next to it indicating it checked out and has been inserted into the root zone file.

You should also see and entry with an "eye" icon indicating that another server, your slave server, was noticed. If the slave entry looks correct,e.g., it is auth2.grpYY.dns.nsrc.org, click on the "eye" to get a "check" mark and then click "Update" to also send this to the root.

b) if not using the RZM:

Indicate to the instructor, on a piece of paper:

```
Domain name:          _____________________

Master nameserver:    auth1.grp___.dns.nsrc.org

Slave nameserver:     auth1.grp___.dns.nsrc.org
```

*   You will not get delegation until the instructor has checked:

    - Your nameservers are all authoritative for your domain
    - They all have the same SOA serial number
    - The NS records within the zone match the list of servers you are
      requesting delegation for
    - The slave(s) are across the room from you :)

    => This is called policy!

*   Once you have delegation, try to resolve www.MYTLD:

    - On your own machine
    - On someone else's machine (who is not slave for you):

  # dig @10.20.XXX.230 www.MYTLD   (where MYTLD is your domain)

*   Add a new resource record to your zone file. Remember to update the
    serial number. Check that your slaves have updated. Try resolving this
    new name.