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 someone else will provide slave service. Then you will ask the administrator for the domain above you (dns) to delegate your domain to you.

Note: the following should be done as the "root" superuser.

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 pc18.dns.nsrc.org, if you type:

```
 # hostname
```

You should see:

```
  pc18.dns.nsrc.org
```

If not, then configure your server with its name: e.g. for pc18.dns.nsrc.org, type:

```
 # hostname pc18.dns.nsrc.org
```

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

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

```
      pc18.dns.nsrc.org
```

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

```
  10.20.X.18      pc18.dns.nsrc.org pc18
```

Exercise

* Choose a new domain, write it down somewhere

    i.e.: "MYNAME.dns.nsrc.org" or "KANGURU.dns.nsrc.org" - whatever you feel like.

    (Do *NOT* choose any of the PC names, e.g. `pc18.dns.nsrc.org`, 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 - and it must be a subdomain of ".dns.nsrc.org".

* Find someone who will agree to be slave for your domain. Please find someone on a different table than you (Remember RFC2182: secondaries must be on remote networks but here we work on a flat net). You can have more than one slave if you wish.

*   If required, installed bind9:

    Ubuntu: apt-get install bind9

*   Create your zone file in `/etc/bind/db.MYNAME.dns.nsrc.org`
    (where MYNAME 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/bind/
  *** $ sudo vi db.MYNAME.dns.nsrc.org
  ***
  ***   (feel free to use another editor instead of vi, e.g. joe, ee)

- - - - - - - - - - - - - cut below - - - - - - - - - - - -

```
$TTL 10m
@       IN      SOA     pcXX.dns.nsrc.org. sysadm@pcXX.dns.nsrc.org. (
                        2011112301    ; Serial
                        10m           ; Refresh
                        5m            ; Retry
                        4w            ; Expire
                        10m )         ; Negative

        IN      NS      pcXX.dns.nsrc.org.   ; master
        IN      NS      pxYY.dns.nsrc.org.   ; slave

www     IN      A       10.20.0.XX             ; your own IP
```

- - - - - - - - - - - - - cut above - - - - - - - - - - - -

      You can replace `sysadm@pcXX.dns.nsrc.org..` with your home E-mail address
      if you want.

      XX and YY are the IP of your PC and your slave's.

    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/bind/named.conf.options`

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

    ... add another line in the options section, so it becomes:

```
        listen-on-v6 { any; };

        allow-query { any; };      // <- this is a new line!
```

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

      Save & quit the editor.

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

    - 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 "MYNAME.dns.nsrc.org" {
        type master;
        file "/etc/bind/db.MYNAME.dns.nsrc.org";
      };

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

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

        $ named-checkconf
        $ named-checkzone MYNAME.dns.nsrc.org /etc/bind/db.MYNAME.dns.nsrc.org

    * If there are any errors, correct them ! *

*   Restart named (the BIND nameserver):

        $ sudo service bind9 restart

    Check the result with

        $ tail /var/log/messages

      Verify with dig that MYNAME.dns.nsrc.org. is now configured on your host:

            $ dig @localhost MYNAME.dns.nsrc.org. NS

        You can also check the nameserver status using rndc:

        $ sudo 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:

        $ sudo service bind9 restart

*   Assist your slaves to configure themselves as slave for your domain, and
    configure yourself as a slave if asked to do so by another table.

    The instructions for how to do this are on the slides, but here's a hint
    on what to put in /etc/bind/named.conf.local

      zone "MYNAME.dns.nsrc.org" {
         type slave;
         masters { 10.20.0.XX; };
         file "/var/cache/bind/db.MYNAME.dns.nsrc.org";
      };
```

... where XX is the IP of the MASTER PC for the zone.

Remember, you will also need to be a slave for someone else's zone!

When you have changed your `named.conf.local` so that you are a slave for someone else, make sure there are no errors in `/var/log/messages` after you restart your nameserver.

* Check that you and your slaves are giving authoritative answers for your domain:

```
# dig +norec @10.20.0.XX MYNAME.dns.nsrc.org. SOA
# dig +norec @10.20.0.YY MYNAME.dns.nsrc.org. SOA
```

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

* Now you are ready to request delegation – indicate to the instructor, on a piece of paper:

Domain name: _____

Master nameserver: pcX.dns.nsrc.org

Slave nameserver: pcY.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 not on the same side of the room as you :)

=> This is called policy!

* Once you have delegation, try to resolve www.MYNAME.dns.nsrc.org

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

```
# dig @10.20.0.XX www.MYNAME.dns.nsrc.org       (where MYNAME 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.