DNS Exercise 3.1: Setting up a domain
=====================================

In this exercise, you will create a new domain,
something.afnog.guru.
You will create master nameservice on your own machine, and someone
else
will setup their machine to be a slave server for your domain. Then
you
will ask the administrator for the domain above you (afnog.guru) to
delegate
your domain to you.

* IMPORTANT! Yesterday we configured unbound as a cache that would
* respond to DNS requests from other clients in the AfNOG network.
*
* In this exercise we want to configure an authoritative server for
* clients throughout the world to send queries to, using BIND9.
*
* We can't have both unbound and BIND9 listening on the same port on
* the same addresses. So we will restrict unbound just to listen to
* localhost, and BIND9 just to live on other interfaces.

Recall that the default behaviour of unbound was just to listen on
localhost -- we had to add configuration to make it listen to other
interfaces, which we will now remove:

>   # rm /etc/unbound/unbound.conf.d/clients.conf

Then we will restart unbound:

>   # service unbound restart

And check that it is still running:

>   # unbound-control status

We are now ready to start!

Exercise
----

*   Choose a new domain, write it here:
`_____________________.afnog.guru.`
    (Do not choose any of the pc names, e.g. `pc23`, as your
subdomain,
    because that would be confusing)

*   Install BIND9:

        # apt-get install bind9

*   Find someone who will agree to be slave for your domain. You

must choose
    someone on a DIFFERENT table to you. (Remember RFC2182:
secondaries must
    be on remote networks). You can have more than one slave if you
wish.

*   Create your zone file in `/var/cache/bind/master/
xxxxx.afnog.guru`
    (where xxxxxx is your chosen domain). You will need to be root
for
    this to work. You will also need to create the directory
    /var/cache/bind/master (/var/cache/bind is already there).

    > $TTL 10m
    >   @   IN   SOA   pcXX.sse.ws.afnog.org.
yourname.example.com. (
    >   2009051200   ; Serial
    >   10m   ; Refresh
    >   10m   ; Retry
    >   4w   ; Expire
    >   10m)   ; Negative
    >
    >   IN   NS   pcXX.sse.ws.afnog.org.   ;
master
    >   IN   NS   pcYY.sse.ws.afnog.org.   ; slave
    >
    >   www   IN   A   196.200.219.X   ; your
own IP

    Replace `yourname.example.com.` with your home E-mail address,
changing
    "@" in the e-mail address to "." and adding a "." to the end.

    Don't just copy and paste the text above! If your zone file
contains spaces
    and ">" characters at the beginning of each line, you will have
problems!

    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
    would use higher values, e.g. `$TTL 1d`

*   Edit `/etc/bind/named.conf.local` to configure your machine as
    master for your domain (see slides for information how to do
this).

*   Check that your config file and zone file are valid, and then
reload
    the nameserver daemon:

        # named-checkconf
        # named-checkzone xxxxx.afnog.guru. \

/var/cache/bind/master/xxxxx.afnog.guru.

*   If there are any errors, correct them*

```
# rndc reload
# tail /var/log/syslog
```

*   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:

```
# 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.
    Again, the instructions for how to do this are on the slides. If you
    have changed your `named.conf` so that you are a slave for someone
    else, make sure there are no errors in `/var/log/syslog` after you
    do `rndc reload`.

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

```
# dig +norec @pcXX.sse.ws.afnog.org xxxxx.afnog.guru. soa
# dig +norec @pcYY.sse.ws.afnog.org xxxxx.afnog.guru. soa
```

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

*   Now you are ready to request delegation. Bring the following information to
    the classroom instructor:

```
Domain name:          _____________________.afnog.guru.

Master nameserver:    pc____.sse.ws.afnog.org

Slave nameserver:     pc____.sse.ws.afnog.org

Slave nameserver:     pc____.sse.ws.afnog.org (optional)

Slave nameserver:     pc____.sse.ws.afnog.org (optional)
```

*   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 desk as you

*   Once you have delegation, try to resolve www.xxxxx.afnog.guru.:

    - On your own machine
    - On someone else's machine (who is not slave for you)
    - On a machine elsewhere on the Internet, if you have access to
one
    - Using Google Public DNS, 8.8.8.8 8.8.4.4

*   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 from elsewhere.