CIA Lab Assignment: Domain Name System (2)

I DID THE DELEGATION IN THIS ASSIGNMENT FOR 3 TIMES and the LAST ONE WITH CHRIS SO YOU WILL SEE THE WIKI PAGE NOT THAT CLEAR BECAUSE I ONLY DOING THE REMAINING PARTS WITH CHRIS INSTEAD TO START FROM ZERO.

I need to give credits to FOUAD and CHRIS to help me in this (especially in the trip in order to finalize my feedbacks)

Question 1. Why is that useful?

First, lets define what is reverse DNS ? It is IP address to domain name mapping - the opposite of forward (normal) DNS which maps domain names to IP addresses. It is mostly used for tracking where a website visitor came from, or where an e-mail message originated. In addition to that many e-mail servers on the Internet are configured to reject incoming e-mails from any IP address which does not have reverse DNS. So if you run your own e-mail server, reverse DNS must exist for the IP address that outgoing e-mail is sent from.

Simple Figure to clarify the differences:

Source:

1- http://support.simpledns.com/kb/a45/what-is-reverse-dns-and-do-i-need-it.aspx

2- https://www.ripe.net/manage-ips-and-asns/db/support/forwardreversedns.png

Question 2. (a) Set up your own reverse zone for your IPv4 subnet.

Address allocated for me 145.100.104.160/27

Now, in /local/usr/etc/nsd/nsd.conf I change the zone section:

```
zone:
    name: "105.100.145.in-addr.arpa"
    zonefile: "105.100.145.zone"
```

Then, create zone file:

```
kotaiba@bristol:/usr/local/etc/nsd$ cat 145.100.105.zone
$ORIGIN 105.100.145.in-addr.arpa.
$TTL 1800
@       IN      SOA     ns1.bristol.prac.os3.nl.
admin.bristol.prac.os3.nl. (
                        2017092605        ; serial number
                        3600                    ; refresh
                        900                     ; retry
                        1209600                 ; expire
                        1800                    ; ttl
                        )
    IN    NS      ns1.bristol.prac.os3.nl.
```

```
    IN    NS      ns2.bristol.prac.os3.nl.
1   IN    PTR     bristol.prac.os3.nl.
2   IN    PTR     bristol.prac.os3.nl.
3   IN    PTR     bristol.prac.os3.nl.
4   IN    PTR     bristol.prac.os3.nl.
5   IN    PTR     bristol.prac.os3.nl.
6   IN    PTR     bristol.prac.os3.nl.
7   IN    PTR     bristol.prac.os3.nl.
8   IN    PTR     bristol.prac.os3.nl.
9   IN    PTR     bristol.prac.os3.nl.
10  IN    PTR     bristol.prac.os3.nl.
11  IN    PTR     bristol.prac.os3.nl.
12  IN    PTR     bristol.prac.os3.nl.
13  IN    PTR     bristol.prac.os3.nl.
14  IN    PTR     bristol.prac.os3.nl.
15  IN    PTR     bristol.prac.os3.nl.
```

Question 2. (b) Show that a reverse lookup works.

```
kotaiba@bristol:~$ dig -x 145.100.104.163

; <<>> DiG 9.10.6 <<>> -x 145.100.104.163
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62298
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;163.104.100.145.in-addr.arpa.  IN    PTR

;; ANSWER SECTION:
163.104.100.145.in-addr.arpa. 156202 IN PTR    bristol.studlab.os3.nl.

;; AUTHORITY SECTION:
104.100.145.in-addr.arpa. 145101 IN NS    ns1.os3.nl.
104.100.145.in-addr.arpa. 145101 IN NS    ns3.surfnet.nl.
104.100.145.in-addr.arpa. 145101 IN NS    ns2.os3.nl.

;; ADDITIONAL SECTION:
ns3.surfnet.nl.     1150    IN    A    195.169.124.71
ns3.surfnet.nl.     1150    IN    AAAA    2001:610:0:800c:195:169:124:71

;; Query time: 0 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Tue Sep 26 21:55:14 CEST 2017
;; MSG SIZE  rcvd: 199
```

Question 3. If Niels had been here and he had not yet implemented the reverse zone delegation,

what information would you need to give him so that he can implement it?

1- DNS zone 104.100.145.in-addr.arpa.

2- NS (NameServer) records, which will be used to delegate the reverse DNS queries. e.g. : 104.100.145.in-addr.arpa. 145101 IN NS ns1.os3.nl.

3- CNAME records, one for each IP address in my block. e.g. : 163.104.100.145.in-addr.arpa name = bristol.studlab.os3.nl.

Source:

1- https://help.dyn.com/standard-dns/configuring-a-reverse-dns-zone-with-standard-dns/

Question 4. How did you set up the subdomains and their delegation?

Question 4. (a) How did you set up the subdomains in your zone file?

I will work with Chris “avignon.prac.os3.nl”:

```
kotaiba@bristol:/usr/local/etc/nsd$ host avignon.prac.os3.nl
avignon.prac.os3.nl has address 145.100.104.103
avignon.prac.os3.nl has IPv6 address 2001:610:158:1043:145:100:104:103
avignon.prac.os3.nl mail is handled by 30 toulouse.prac.os3.nl.
avignon.prac.os3.nl mail is handled by 20 rouen.prac.os3.nl.
avignon.prac.os3.nl mail is handled by 10 avignon.prac.os3.nl.
```

I will work Chris to set up delegation. He already will delegated a domain zone to me. We decided that we will use bristol

Since Chris already added his changes in his zone file of the delegation,I need to add zone delegation now to him. So I will change my zone file to:

I added in my bristol.prac.os3.nl:

```
; Delegation to Chris
$ORIGIN chris.bristol.prac.os3.nl.
$TTL 3000
@       IN    NS    ns1
ns1     IN    A    145.100.104.103
ns1     IN    AAAA    2001:610:158:1046:145:100:104:103
```

Now, for the delegation from Chris:

I created a new zone file “kotaiba.avignon.prac.os3.nl” and added the following:

```
kotaiba@bristol:/usr/local/etc/nsd$ cat kotaiba.avignon.prac.os3.nl
;; OPT PSEUDOSECTION:
$ORIGIN kotaiba.avignon.prac.os3.nl.
; EDNS: version: 0, flags:; udp: 4096
$ORIGIN kotaiba.avignon.prac.os3.nl.
$TTL 300
```

```
@       IN      SOA     kotaiba.avignon.prac.os3.nl.
kotaiba.bristol.studlab.os3.nl (
                        2               ;Serienummer
                        300             ;Refresh TTL
                        300             ;Retry TTL
                        300             ;Expire TTL
                        300             ;neg-cache TTL
                        )
;Nameservers
@               IN      NS      ns1
;A record for NS
ns1             IN      A       145.100.104.163
ns1             IN      AAAA    2001:610:158:1043:145:100:104:163
google          IN      A       8.8.8.8
ripe            IN      AAAA    2001:67c:2e8:22::c100:68b
xkcd            IN      AAAA    2a04:4e42::67
mail            IN      A       145.100.104.163
mail2           IN      A       145.100.104.163

; Additional records
chris           IN      CNAME   chriskuipers.com.
isitsecure      IN      CNAME   letsencrypt.org.

; MX records
@               IN      MX      10      mail
@               IN      MX      20      mail2
```

Question 4. (b) What named.conf/nsd.conf options did you add or change?

I added to my nsd.conf file:

```
   zone:
        name: kotaiba.avignon.prac.os3.nl
        zonefile: "/usr/local/etc/nsd/kotaiba.avignon.prac.os3.nl"
```

Question 4. © Show the results of the tests that you performed.

```
kotaiba@bristol:/usr/local/etc/nsd$ dig chris.kotaiba.avignon.prac.os3.nl
@145.100.104.163

; <<>> DiG 9.10.6 <<>> chris.kotaiba.avignon.prac.os3.nl @145.100.104.163
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36534
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;chris.kotaiba.avignon.prac.os3.nl. IN  A
```

```
;; ANSWER SECTION:
chris.kotaiba.avignon.prac.os3.nl. 300 IN CNAME chriskuipers.com.

;; Query time: 0 msec
;; SERVER: 145.100.104.163#53(145.100.104.163)
;; WHEN: Sat Oct 28 18:35:48 CEST 2017
;; MSG SIZE  rcvd: 92
```

Question 5. (a) How did you set up the slave nameserver? + (b) Show the changes to the configuration files that you made.

My server will be slave for Chris, so I added in the nsd.conf file:

```
# 145.100.104.103 Chris Server is the master.
pattern:
        name: "fromchris"
        allow-notify: 145.100.104.103 NOKEY
        request-xfr: AXFR 145.100.104.103@53 NOKEY

# Zone to receive from chris
zone:
        name: chris.bristol.prac.os3.nl.
        include-pattern: "fromchris"
        zonefile: /usr/local/etc/nsd/chris.bristol.prac.os3.nl.zone
```

Check the log with Chris:

```
Oct 28 19:25:44 bristol nsd[17149]: notify for chris.bristol.prac.os3.nl.
from 145.100.104.103
```

To show that the notify from Chris works, check log:

```
Oct 28 19:28:15 bristol nsd[17149]: notify for chris.bristol.prac.os3.nl.
from 145.100.104.103 serial 3
Oct 28 19:28:15 bristol nsd[17145]: xfrd: zone chris.bristol.prac.os3.nl.
written received XFR packet from 145.100.104.103@53 with serial 3 to disk
Oct 28 19:28:15 bristol nsd[17145]: xfrd: zone chris.bristol.prac.os3.nl.
committed "received update to serial 3 at 2017-10-28T19:28:15 from
145.100.104.103@53"
Oct 28 19:28:15 bristol nsd[17146]: zone chris.bristol.prac.os3.nl. received
update to serial 3 at 2017-10-28T19:28:15 from 145.100.104.103@53 of 470
bytes in 0.000109 seconds
Oct 28 19:28:15 bristol nsd[17145]: zone chris.bristol.prac.os3.nl. serial 2
is updated to 3.
```

Question 6. What happens if the primary nameserver for the subdomain fails? And for how long?

The applications will still use the cache until the TTL expires. But after that, the slave server handle it. The slave server will continue to answer queries until the expire time has finished.

example from my configuration file:

```
                        1209600                 ; expire
                        1800                    ; ttl
```

Question 7. Considering that the slave nameserver is also the delegating nameserver, explain why this is essentially a bad setup?

In this case if the delegating nameserver fails, a resolver will no longer be able to do the delegation.

Question 8. Show the output of the DNS tool.

```
kotaiba@bristol:/usr/local/etc/nsd$ dig AXFR chris.bristol.prac.os3.nl
@145.100.104.103

; <<>> DiG 9.10.6 <<>> AXFR chris.bristol.prac.os3.nl @145.100.104.103
;; global options: +cmd
chris.bristol.prac.os3.nl. 300  IN    SOA    chris.bristol.prac.os3.nl.
chris.avignon.studlab.os3.nl.chris.bristol.prac.os3.nl. 2 300 300 300 300
chris.bristol.prac.os3.nl. 300  IN    NS    ns1.chris.bristol.prac.os3.nl.
chris.bristol.prac.os3.nl. 300  IN    MX    10
mail.chris.bristol.prac.os3.nl.
chris.bristol.prac.os3.nl. 300  IN    MX    20
mail2.chris.bristol.prac.os3.nl.
chris.chris.bristol.prac.os3.nl. 300 IN CNAME    chriskuipers.com.
google.chris.bristol.prac.os3.nl. 300 IN A  8.8.8.8
isitsecure.chris.bristol.prac.os3.nl. 300 IN CNAME letsencrypt.org.
mail.chris.bristol.prac.os3.nl. 300 IN    A    145.100.104.103
mail2.chris.bristol.prac.os3.nl. 300 IN A    145.100.104.103
ns1.chris.bristol.prac.os3.nl. 300 IN   A    145.100.104.103
ns1.chris.bristol.prac.os3.nl. 300 IN   AAAA
2001:610:158:1043:145:100:104:103
ripe.chris.bristol.prac.os3.nl. 300 IN    AAAA    2001:67c:2e8:22::c100:68b
xkcd.chris.bristol.prac.os3.nl. 300 IN    AAAA    2a04:4e42::67
chris.bristol.prac.os3.nl. 300  IN    SOA    chris.bristol.prac.os3.nl.
chris.avignon.studlab.os3.nl.chris.bristol.prac.os3.nl. 2 300 300 300 300
;; Query time: 0 msec
;; SERVER: 145.100.104.103#53(145.100.104.103)
;; WHEN: Sat Oct 28 19:27:50 CEST 2017
;; XFR size: 14 records (messages 1, bytes 457)
```

Question 9. Describe the steps in the transfer process.

the following process:

1- The secondary server for the zone waits a certain amount of time (specified in the Refresh field of the SOA resource record), and then polls the master server for its SOA.

2- The master server for the zone responds with the SOA resource record.

3- The secondary server for the zone compares the returned serial number to its own serial number. If the serial number sent by the master server for the zone is higher than its own serial number, that means its zone database is out of date, and it sends an AXFR request (a request for a full zone

transfer).

4- The master server for the zone sends the full zone database to the secondary server.

To simplify it more:

Source:

1- https://technet.microsoft.com/en-us/library/cc958966.aspx

2- http://images.slideplayer.com/36/10620169/slides/slide_15.jpg

Question 10. What information did the slave server receive? In what format?

The slave receives all information that the master server has about the zone.

The Format described in the RFC 1034 (help from colleague):

```
        +---------------------------------------------------+
Header  | OPCODE=SQUERY, RESPONSE, AA                       |
        +---------------------------------------------------+
Question| QNAME=USC-ISIC.ARPA., QCLASS=IN, QTYPE=A          |
        +---------------------------------------------------+
Answer  | USC-ISIC.ARPA.   86400 IN CNAME   C.ISI.EDU.      |
        +---------------------------------------------------+
Authority| ISI.EDU.        172800 IN NS      VAXA.ISI.EDU.  |
        |                        NS      A.ISI.EDU.        |
        |                        NS      VENERA.ISI.EDU.   |
        +---------------------------------------------------+
Additional| VAXA.ISI.EDU.  172800    A       10.2.0.27      |
        |                172800    A       128.9.0.33      |
        | VENERA.ISI.EDU.172800    A       10.1.0.52       |
        |                172800    A       128.9.0.32      |
        | A.ISI.EDU.     172800    A       26.3.0.103      |
        +---------------------------------------------------+
```