DNSSEC Training Course

Solution Booklet

November 2016

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

INTRODUCTION

Labs environment

The labs run on RIPE NCC's infrastructure, and consist of one server per participant. Every participant has access to a server with BIND running in a UNIX environment, with all the necessary software (shell, text editors, etc.).

For every exercise, please fill in your number (from the attendees' list) in the ovals to obtain the exact information for your environment.

For example, if your number on the list is 29, then:

www.domain⬭.workshop would be www.domain29.workshop.

If your number is 7, then:

www.domain⬭.workshop would be www.domain7.workshop.

To connect to the lab environment, use an SSH client (like Putty on windows), and adjust the port numbers like the following:

To connect to the lab environment, use an SSH client (like Putty on windows or terminal on OSX), with the following details:

Host: lab.dnssec-course.net
Username: user⬭
Port: 220⬭ (if your number is below 10, add a zero in front of it)
Password: user⬭_secret

An example for the OS X terminal is as follows:

ssh -p 220⬭ user⬭@lab.dnssec-course.net

The password for the lab is userX_secret

Exercise A: Creating a zone file

Task: Create a zone file on paper

In this exercise, you are going to create a zone file according to the requirements.

You have a domain, which is domain□.workshop.

You can use the form in the next page to fill in all the information!

A) Host www.domain.workshop has IPv4 address 10.□.0.80

B) Host www-test.domain□.workshop has IPv4 address 10.□.2.80

C) Mail servers for domain□.workshop are
mx1.domain□.workshop,
mx2.domain□.workshop. and
secondary.mail.workshop. These are in order of preference.
The two internal servers have respectively
10.□.0.25 and
10.□.3.25 as IPv4 addresses, and
2001:ff□:abcd::25 and
2001:ff□:cafe::25 as IPv6 addresses.

D) There is a development team that manages their own infrastructure, and would like to have a delegation for the domain dev.domain.workshop.

E) They have two nameservers:
ns1.dev.domain□.workshop and
dev-dns.domain□.workshop.
ns1.dev.domain□.workshop has IPv4 address 192.168.□.53 and IPv6 address 2001:ff□:de55::53.
dev-dns.domain□.workshop has IPv4 address 10.□.9.53 and IPv6 address 2001:ff□:9999::53.

F) The email address of the administrators of the zone file is admins@domain□.workshop

G) www.domain.workshop has IPv6 address 2001:ff□:abcd::80

H) www-test.domain□.workshop has IPv6 address 2001:ff□:cafe::80

I) The TTL for www-test.domain□.workshop should be 3600

J) support.domain⬭.workshop uses the same server as www.domain⬭.workshop

K) The general TTL for the zone is 300.

L) The serial should be 2015⬭0145 , where YYYY is the Year, MM is the month, DD is the day of the month, and XX is the number daily update. This should start from 00.

M) The name servers for the zone are
ns1.domain⬭.workshop and
ns1.secondary-dns.workshop.
ns1.domain⬭.workshop has IPv4 address 172.16.30.⬭ and IPv6 address 2001:ff⬭:abcd::53.

Notice the SOA record here is on the second page, because of formatting reasons
not at the beginning of the file, as it would be normally.

Host	Class/Type	Various	CDATA
www.domain**X**.workshop.	IN A		10.**X**.0.80
www-test.domain**X**.workshop. 3600	IN A		10.**X**.2.80
domain**X**.workshop.	IN MX	10	mx1.domain**X**.workshop.
domain**X**.workshop.	IN MX	20	mx2.domain**X**.workshop.
domain**XX**.workshop.	IN MX	30	secondary.mail.workshop.
mx1.domain**X**.workshop.	IN A		10.**X**.0.25
mx2.domain**X**.workshop.	IN A		10.**X**.2.25
mx1.domain**X**.workshop.	IN AAAA		2001:ff**X**:abcd::25
mx2.domain**X**.workshop.	IN AAAA		2001:ff**X**:cafe::25
dev.domain**X**.workshop.	IN NS		ns1.dev.domain**X**.workshop.
dev.domain**X**.workshop.	IN NS		dev-dns.domain**X**.workshop.

Host	Class/Type	Various	CDATA
ns1.dev.domainX.workshop.	IN A		192.168.X.53
ns1.dev.domainX.workshop.	IN AAAA		2001:ffX:de55::53
www.domainX.workshop.	IN AAAA		2001:ffX:abcd::80
www-test.domainX.workshop. 3600	IN AAAA		2001:ffX:cafe::80
domainX.workshop.	IN NS		ns1.domainX.workshop.
domainX.workshop.	IN NS		ns1.secondary-dns.workshop.
ns1.domainX.workshop	IN A		172.16.30.X
ns1.domainX.workshop	IN AAAA		2001:ffX:abcd::53
support.domainX.workshop	IN CNAME		www.domainX.workshop

$TTL __________

domain□.workshop.	IN SOA	ns1.domainX.workshop.
		admins.domainX.workshop.
		2016MMDDXX
		21600
		3600
		604800
		86400

Remember to either use the short name for the host, or to use the dot (.) at the end of the hostname.

Note: Instead of typing the whole domain, you can replace it with the @ sign.

Exercise B: New changes to the zone file

Task: Add/change records to the zone from the previous exercise

1) Connect to the lab environment following the instructions on page 2

```
nano domain/domain.conf or vim domain/domain.conf
```

2) Use a text editor to edit the domain file domain/domain.conf

3) Make the following modifications to the zone file:

A) Add a host called www-pre.domain□.workshop with IP address 10.□.0.88 and IPv6 address 2001:ff□:abcd::88

B) Increase the serial number by at least one;

C) Add two mail exchangers for the subdomain dev.domain□.workshop., which will be mx1.mail.workshop and mx2.mail.workshop.

D) Don't forget to add the dots at the end of host and domain names!

4) Once finished, you have to reload named in order for the changes to take effect:

```
sudo /usr/local/etc/rc.d/named reload
```

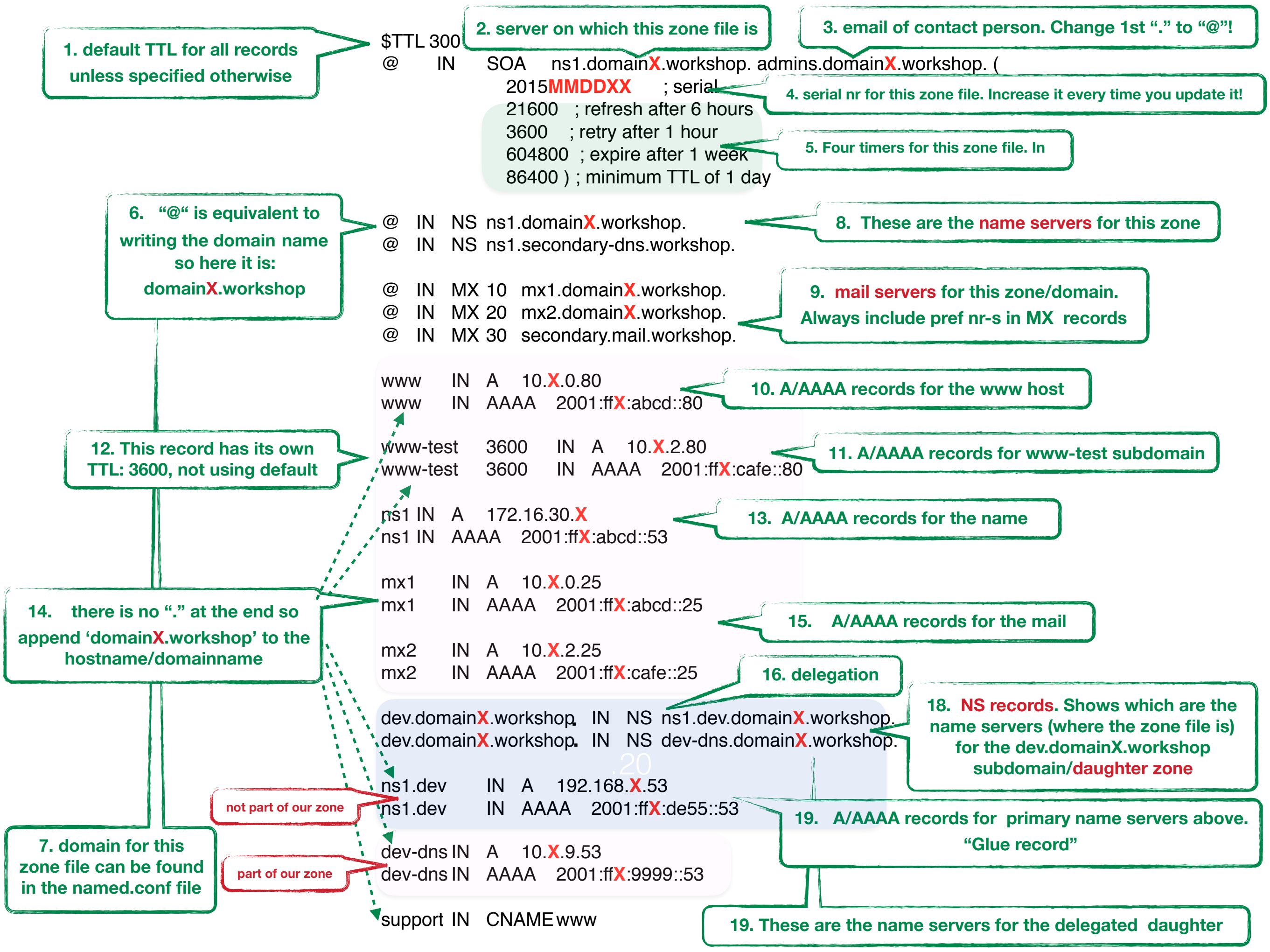
5) Once you are ready, you can proceed to check if your domain works by moving on to exercise C.

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

You can check if there have been problems loading the zone file by issuing:

and checking the log messages from BIND.

```
$TTL 300
@       IN      SOA     ns1.domainX.workshop. admins.domainX.workshop. (
                        2016MMDDXX      ; serial
                        21600   ; refresh after 6 hours
                        3600    ; retry after 1 hour
                        604800  ; expire after 1 week
                        86400 ) ; minimum TTL of 1 day

@       IN      NS      ns1.domainX.workshop.
@       IN      NS      ns1.secondary-dns.workshop.

@       IN      MX      10      mx1.domainX.workshop.
@       IN      MX      20      mx2.domainX.workshop.
@       IN      MX      30      secondary.mail.workshop.

www     IN      A       10.X.0.80
www     IN      AAAA    2001:ffX:abcd::80

www-test        3600    IN      A       10.X.2.80
www-test        3600    IN      AAAA    2001:ffX:cafe::80

ns1     IN      A       172.16.30.X
ns1     IN      AAAA    2001:ffX:abcd::53

mx1     IN      A       10.X.0.25
mx1     IN      AAAA    2001:ffX:abcd::25

mx2     IN      A       10.X.2.25
mx2     IN      AAAA    2001:ffX:cafe::25

dev.domainX.workshop IN NS      ns1.dev.domainX.workshop.
dev.domainX.workshop IN NS      dev-dns.domainX.workshop.

ns1.dev         IN      A       192.168.X.53
ns1.dev         IN      AAAA    2001:ffX:de55::53

dev-dns         IN      A       10.X.9.53
dev-dns         IN      AAAA    2001:ffX:9999::53

support         IN      CNAME           www
```



```
$TTL 300
@       IN      SOA     ns1.domainX.workshop. admins.domainX.workshop. (
                        2015MMDDXX      ; serial
                        21600   ; refresh after 6 hours
                        3600    ; retry after 1 hour
                        604800  ; expire after 1 week
                        86400 ) ; minimum TTL of 1 day

@   IN   NS  ns1.domainX.workshop.
@   IN   NS  ns1.secondary-dns.workshop.

@   IN   MX 10   mx1.domainX.workshop.
@   IN   MX 20   mx2.domainX.workshop.
@   IN   MX 30   secondary.mail.workshop.

www      IN   A      10.X.0.80
www      IN   AAAA   2001:ffX:abcd::80

www-test    3600    IN   A      10.X.2.80
www-test    3600    IN   AAAA   2001:ffX:cafe::80

ns1 IN   A      172.16.30.X
ns1 IN   AAAA   2001:ffX:abcd::53

mx1      IN   A      10.X.0.25
mx1      IN   AAAA   2001:ffX:abcd::25

mx2      IN   A      10.X.2.25
mx2      IN   AAAA   2001:ffX:cafe::25

dev.domainX.workshop.   IN   NS  ns1.dev.domainX.workshop.
dev.domainX.workshop.   IN   NS  dev-dns.domainX.workshop.

ns1.dev       IN   A      192.168.X.53
ns1.dev       IN   AAAA   2001:ffX:de55::53

dev-dns IN    A      10.X.9.53
dev-dns IN    AAAA   2001:ffX:9999::53

support IN    CNAME www
```

1. default TTL for all records unless specified otherwise

2. server on which this zone file is

3. email of contact person. Change 1st "." to "@"!

4. serial nr for this zone file. Increase it every time you update it!

5. Four timers for this zone file. In

6. "@" is equivalent to writing the domain name so here it is: domainX.workshop

7. domain for this zone file can be found in the named.conf file

8. These are the name servers for this zone

9. mail servers for this zone/domain. Always include pref nr-s in MX records

10. A/AAAA records for the www host

11. A/AAAA records for www-test subdomain

12. This record has its own TTL: 3600, not using default

13. A/AAAA records for the name

14. there is no "." at the end so append 'domainX.workshop' to the hostname/domainname

15. A/AAAA records for the mail

16. delegation

18. NS records. Shows which are the name servers (where the zone file is) for the dev.domainX.workshop subdomain/daughter zone

19. A/AAAA records for primary name servers above. "Glue record"

19. These are the name servers for the delegated daughter

not part of our zone

part of our zone

Exercise C: Using DIG to find information in DNS

Task: Use dig to find information in DNS and answer the questions

For this exercise, you have to still be logged in the lab environment.

1) Find out the root servers in the lab (type dig without any query)
a.root-servers.workshop, b.root-servers.workshop

2) Find out the name servers for the dns.workshop domain
(dig ns dns.workshop) ns1.dns.workshop, ns2.dns.workshop, ns-ext.domain.domain

3) Can you find out the IPv4 addresses for www.dns.workshop ?
172.16.18.29, 172.16.18.31, 172.16.18.30

4) Check if the secondary DNS server for your domain has updated its records (add @10.0.2.53 to the query for a SOA record)

```
dig @10.0.2.53  SOA domain29.workshop
```

5) If the data propagated, you can check if you can resolve the MX records for domain**X**.workshop directly from your secondary server

```
dig MX domain29.workshop @10.0.2.53
```

6) Check the SOA for the sync.workshop domain. (Use the +nssearch flag) Do you see anything strange?

The SOA are different, this means that the secondary DNS is not synchronised with the primary.

7) Check that a TCP query works and find the IPv6 address for www.mail.workshop (using the +tcp flag)

www.mail.workshop should be ffe0:9484:2344::80

Exercise D: Configure DNSSEC for the domain

Task: Generate the required keys, and configure your domain for DNSSEC and automatic key rollover

1) Connect to the lab environment following the instructions on page 2

2) Enter the directory where we will store the keys:

```
cd domain
```

3) Generate the Key Signing Key (KSK)

```
dnssec-keygen -a RSASHA256 -f KSK -b 4096 -n zone domainX.workshop
```

4) Generate the Zone Signing Key (ZSK)

```
dnssec-keygen -a RSASHA256 -b 4096 -n zone domainX.workshop
```

5) Change the ownership of the files so that Bind can read them, and use the keys to sign the zone:

```
sudo chown bind:bind K*
```

6) Configure bind to enable DNSSEC

```
cd ../
nano named.conf or vim named.conf
```

In the “options” section, we need to enable dnssec, adding these two lines:

```
dnssec-enable yes;
dnssec-validation auto;
```

With this change, we also enabled the server to be a DNSSEC-enabled resolver. This way we can perform DNSSEC queries through it to test if it is working.

7) In the section related to the zone “domainX.workshop”, modify it to look like this:

```
zone "domainX.workshop" {
        type master;
        file “/usr/local/etc/namedb/domain/domain.conf”;
        key-directory “/usr/local/etc/namedb/domain/”;
        allow-transfer { 10.0.2.53; };
        inline-signing yes;
        auto-dnssec maintain;
};
```

8) Restart/Reload Bind for the changes to take effect

```
sudo /usr/local/etc/rc.d/named reload
```

After this, you should try to check if the zone is signed by running this command:

```
$  dig RRSIG www.domainX.workshop @172.16.30.X
```

If the answer shows RRISG records, then it means the zone is being signed by Bind.

9) Generate the DS records and input them in the domain interface by connecting with a browser to http://lab.dnssec-course.net
Log in using the same user name and password you used for the lab.

You first have to identify which one is the Key Signing Key for your domain:

```
$ cd domain
$ grep "key-signing" K*
KdomainXX.workshop.+010+08763.key:; This is a key-signing key, keyid 8763, for
domainXX.workshop.
```

Then you can proceed to extract the DS records.
Copy the file name of the key, without the “.key” extension.

Copy and paste this part from the output:

KdomainX.workshop.+010+08763
(The numbers will be different for you, this is just an example)

Now paste it and use it to launch **dnssec-dsfromkey**:

```
$ dnssec-dsfromkey KdomainX.workshop.+010+08763

domainXX.workshop. IN DS 8763 10 1 DB8079B2D667C4A4F9D39C91C72548C1EC183965
domainXX.workshop. IN DS 8763 10 2
567797EDE2E1C305ABB8AAF490E76744A84763CB0B67FC08B753D4CB6ACBEB54
```

Just copy the text you got as an answer paste it into the web interface.

These are just the records to put in the web interface, as you would do with any domain registrar that supports DNSSEC.

Remember: Even if your zones are signed, DNSSEC will not be enabled until you supply the DS records to your registrar!

Exercise E: Check and troubleshoot DNSSEC

Task: Use dig, drill and delv to verify DNSSEC and troubleshoot broken implementations

For this exercise, you have to still be logged in the lab environment. For dig, remember to always use the +dnssec flag in every query.

1) Check the RRSIG records for nic.workshop

____

2) Launch “drill -S mx1.secondary-dns.workshop”. What do you see ?

You see the tree of DNSSEC records, keys and validation points.

3) What is the key ID for the keys of secondary-dns.workshop ?

____

4) And what is the algorithm used for them ?

Algorithm 8, RSASHA256

5) What type of RRSIG can you see for www.broken-dnssec.workshop ? If you can’t see it, try with the +cdflag

No RRSIGs, unless you use the +cdflag. DNSSEC is broken for this domain.

6) Why do we have to use that flag ? What is the problem ?

Because the CD flag disables DNSSEC checks. We don’t get any response because DNSSEC is broken. The DNSKEY does not match the DS Records. If we disable the checks, we see the RRSIGs.

7) Can you try running the same query with drill, using the -s flag ?

Drill tells you it can’t validate, and where the problem happened.

8) And what about with delv, with the vtrace flag ?

Delv has the same behaviour as Drill