Helsinki University of Technology

Department of Electrical and Communications Engineering
Networking Laboratory

S-38.3133 - Networking Technology, laboratory course
Autumn 2006 - Spring 2007
Work number 33: Domain Name System (DNS)

Preliminary exercises, laboratory assignment and questions for final report

29.6.2005
Juha Järvinen
Juha.Jarvinen@netlab.tkk.fi

Updated 20.9.2006
Juha Järvinen
Juha.Jarvinen@netlab.tkk.fi

Domain Name System (DNS) Laboratory Work

Preliminary Exercises

Add a cover page for your answers according to the example. Answer the following questions briefly **but clearly**. Language of the reports is Finnish or Swedish for Finns, English for others! Make sure you understand the basics of DNS before entering the lab. It may also be a good idea to examine the laboratory assignment beforehand. Return the preliminary report three days before coming to the laboratory.

Any comments and questions concerning this work should be addressed to juha.jarvinen@netlab.tkk.fi in the autumn 2006 and spring 2007.

1. Tell about differences between static DNS and dynamic DNS. Why is DNS generally used?

2. Explain the following terms briefly. Explain their tasks in DNS.
    - Primary DNS
    - Secondary DNS
    - MX
    - DNSSEC
    - CNAME
    - Reverse Zone Data File

3. A client makes an inquiry: it wants to know the IP address related to the address *www.netlab.tkk.fi*. Draw a picture about the name resolution process and explain it. Assume that you are in *fool.com* domain and your name server's DNS cache is empty.
    a) When recursive name resolution process is used (from name server *fool.com* on)
    b) When iterative name resolution process is used (from name server of *fool.com* on)

4. You have a new domain with name servers *130.200.56.1* and *130.200.56.2*. There's something wrong (or rather, something contrary to good practice) in this setup. What is it?

5. Your company decides to buy a new domain name – *company.fi*. What do you have to do before you can use that name publicly?

6. You have DNSSEC servers. How should you share keys between parents and children in a secure way? Give at least two different methods.

In addition familiarize yourself with some Bind configuration instructions, for example: *http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/ch-bind.html*. Read it carefully. You should understand at least:

- Meaning of different files: *named.conf*, zone file and reverse zone file what information they contain
- Meaning of different types of zone file resource records

Domain Name System (DNS) Laboratory Assignment

1. Introduction

DNS is a very important part of IP network from users' point of view. With the help of DNS you don't have to remember any numerical IP addresses when you want to connect to computers around the world. As you will notice during this lab work, DNS is very useful in the intranet/internet interface, too.

This laboratory work is quite easy, if you have understood a couple of basic features of the DNS system. If you have done the VPN/NAT laboratory work before this, you should already have a little bit of touch with DNS.

You have three hours to do this lab work and this time should be sufficient. The written documents play a big role in grading, so make the final report carefully. If you have any appendices, remember to refer to them in your text!

2. Goals of this laboratory work

After this laboratory work you will understand the basic features of DNS, the importance of SSL feature in the future and how to configure a domain name server for different situations.

3. Environment

In this laboratory work you will use a part of the laboratory network, which is also connected to the Internet. The structure of the network is shown below in *Figure 1*.
The lab room has five DNS servers, three for this work and two for the *.lab* domain. These three servers have the Debian Testing operating system[1] and the Bind 9.1[2] program with SSL feature for resolving names and IP addresses. NS1 and NS2 servers also have Apache HTTP servers. They both have been configured to *www.dns.lab* domain name. You are not allowed to make any changes to the HTTP server settings! NTP should be running all the time in domain name servers, but sometimes there might be some problems in the automatic running. There is a guideline how to get 'the official time'. This is necessary only in the exercise 5.2 (DNSSEC).

NS1 and NS2 servers are in *10.38.10.0/24* space and NS is *10.38.20.0/24* space. For testing purposes there are two client PCs (*zyskowicz* at *10.38.10.10* and *uusipaavalniemi* at *10.38.20.20*). They are both running a FreeBSD[3] 5.4 operating system.

The DNS-networks' physical topology is shown in *Figure 1*.

[1] www.debian.org
[2] www.isc.org/products/BIND/
[3] www.freebsd.org

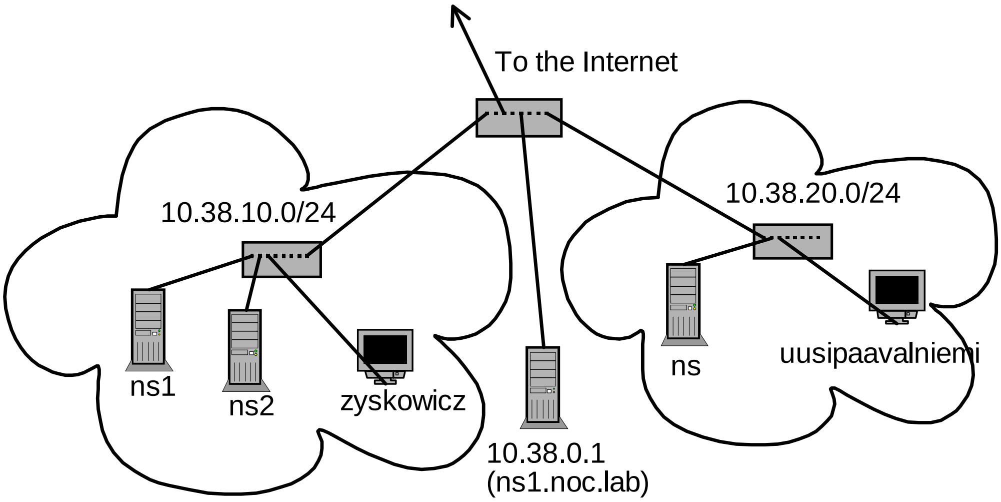

Figure 1 *Physical topology of the network*

4. Instructions

Log in to name servers as the *root* user. The assistant will tell you the password. There is a sample configuration file for *named.conf* in every three computers. It is named *named.conf.sample* and its location is in */etc/* directory. Before starting copy this file to *named.conf.* There is no sample file of zone files, but it is recommended to locate them to a */var/named/* directory.

When creating zone configuration files, name them as followed:

- Primary zone files: named.+domain (e.g. *named.dns.lab*)
- Secondary zone files: slave.+domain (e.g. *slave.dns.lab*)
- Reverse primary zone files: named.+IP (e.g. *named.10.38.10*)
- Reverse secondary zone files: slave+IP (e.g. *slave.10.38.10*)

Apache and Bind do not start in reboot; you have to start them manually:

- Bind: */etc/init.d/bind9 start*
- Apache: */etc/init.d/apache start* (Do not start this before the final section)

Starting Bind also starts an *rndc* program. The *rndc* (Remote Name Daemon Control) program allows the system administrator to control the operation of name servers. If you make any changes to your zone files after starting the Bind program, you'll have to run *rndc reload*. If you make any changes to your *named.conf* file, you'll have to run */etc/init.d/named restart.*

There is a serial number in every zone file. Create it by using date + two digits, e.g. 2005071709. Remember to increase this number every time when you have made changes to zone files. Otherwise, *rndc* won't notice the new zone configurations.

There are some good programs to check syntax of the zone and *named.conf* files.
For *named.conf* files run:

```
named-checkconf /etc/named.conf
```

and for zone files run

named-checkzone domain-name-here /var/named/named.domain-name

If *named.conf* file is not ok, the *rndc* program will not work properly.

Make sure that routing between networks *10.38.10.0/24* and *10.38.20.0/24* works properly.

Use *Ohmi* to configure the name servers. *Zyskowicz* and *uusipalvalniemi* have no displays, so you'll have to connect to them using SSH.

With appendices [4] and [5] you can familiarize yourself with Bind configuration commands. Appendices [1] – [3] are sample configuration files for *named.conf*, zone and reverse zone.

5. Exercises

5.1 Configuring a regular Domain Name Server

Now the goal is to configure a regular Domain Name Server; this includes a primary DNS, a secondary DNS and a DNS for a sub-domain. The network structure is shown in *Figure 2*.

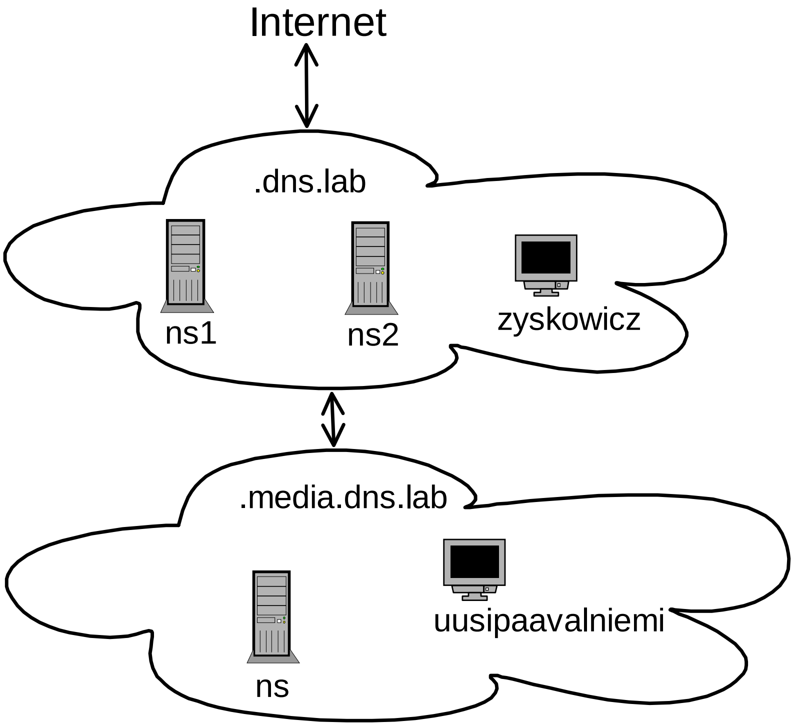

Figure 2 *Domain name service topology*

Table 1 shows the IP addresses needed in this exercise.

Table 1. *IP addresses for fig. 2.*

Hostname	**IP**
ns1.dns.lab	10.38.10.1
ns2.dns.lab	10.38.10.2
zyskowicz.dns.lab	10.38.10.10
ns.media.dns.lab	10.38.20.1
uusipaalvalniemi.media.dns.lab	10.38.20.20

In every nameserver you have to edit three files: *named.conf*, zone file and reverse zone file.

Ns1.dns.lab

First let's configure ns1. Your configuration has to make the server:

- Work as a primary server
- Forward other inquiries than for *dns.lab* and *media.dns.lab* to *10.38.0.1*
- Be able to do the transformation from name to IP and the reverse transformation from IP to name.
- Send all the inquiries related to *media.dns.lab* domain to *ns.media.dns.lab* domain name server to resolve there.
- Create a canonical name *www.dns.lab* for *ns2.dns.lab*
- Create a mail server entry with priority 10 *for ns1.dns.lab*

Ns2.dns.lab

Your ns2 configuration has to make the server:

- Work as a secondary server
- Make ns2 to copy ns1's zones automatically from ns1. You aren't allowed to create any zone files to ns2 by yourself.
- Be able to do the transformation from name to IP and the reverse transformation from IP to name.
- Send all the inquiries related to *media.dns.l*ab domain to *ns.media.dns.lab* domain name server to resolve there.

Ns.media.dns.lab

Your ns configuration has to make the server:

- Work as a primary server for *media.dns.lab* domain
- Forward other inquiries than for *media.dns.lab* both to *ns1.dns.lab* and to *ns2.dns.lab*
- Be able to do the transformation from name to IP and the reverse transformation from IP to name.
- Create canonical name *fool.media.dns.lab* for *ns.media.dns.lab*

Now the configuration is ready.

Q1: First restart *named* service in *ns1* and *ns2* machines. Capture messages between the hosts when starting *named* in the slave server. What kind of information can you see in the captured messages? Use "`tcpdump –w <filename> -s 0`" on *zyskowicz* to capture messages in the network. You can then use SCP to transfer the file to *Ohmi* and then use *Ethereal* to view the captured traffic. Use "`scp <filename> ohmi.noc.lab:`" to transfer the file to *Ohmi*.

Q2: Then make an inquiry in *zyskowicz*. Ask *uusipaavalniemi*'s IP address, and capture messages between *ns.media.dns.lab* and *ns1.dns.lab* on *zyskowicz*. How do the messages differ from Q1?

Checking

You have to show the running servers to your lab assistant. Use *dig* program.

If you get a correct response when searching for example *www.ba.com* or *www.yle.fi*, your configuration works.

If everything isn't running properly after you have checked the configurations, you have to fix the bugs.

Q3: Familiarize yourself with *dig*. Set all parameters on and recursive inquiries on. Do some inquiries, for example *www.finnair.fi* and so on. Study the captured messages and give a very short report on what kind of information you can see in the inquiries. **Do this exercise at home**. You can find the *dig* program at least at TKK's Computer Centre's Linux machines. There is a version for Windows OS in the Internet.

Q4: Take a copy of *named.conf* files and zones files of name servers and include them in the final report. Do not include the whole file, just the most important and interesting parts. In the final report you have to explain briefly what you have done.

Don't remove any files yet!

5.2 DNSSEC

DNSSEC [RFC2535] is on the IETF standards track and has been implemented in the 'BIND' name server software (versions 9.0 to 9.2).[4]

Name server is unfortunately very vulnerable to different net attacks. By using different features it's very easy to disturb the action of DNSs and therefore slow down the whole network, because hosts have to wait for a response from DNSs. The purpose of using DNSSEC is to reduce this kind of disturbance in networks.

5.2.1 Securing Zone Transfer

In name servers *ns1* and *ns2* you have to edit only one file: *named.conf*. *ns.media* can be running on the background.

By securing zone transfers we can ensure that our secondary server is an identical copy of our primary name server and nobody has changed zone data.

First synchronize clocks in our three name servers. They should already be synchronized, but if not, run:

[4] Kolkman, Olaf M.,: DNSSEC Operational HOWTO

```
ntpdate 10.38.0.1
```

Next you have to create shared keys. Use a *dnssec-keygen* command. Use HMAC-MD5 algorithm and 128 bits. For example, you can run the next command:

```
dnssec-keygen –a algorithm_name –b bits –n HOST key_id
```

Now you have two keys (they are same) with *.private* and *.key* extensions. Copy the key part of a file to *named.conf* file of the *ns1.dns.lab* and *ns2.dns.lab* servers. The key statement has the following syntax:

```
key key_id. {
     algorithm string;
     secret "string";
}
```

Add the next statement to your *dns.lab* and its reverse zones:

```
allow-transfer { key key_id. ;};
```

And finally add the next command to your *named.conf* file of the slave server:

```
server ip {
     keys {key_id. ;};
```

IP is the address, where you want to transfer traffic from.

Now the configuration is ready. Restart *named* service in the both machines. Capture messages between the hosts when starting *named* in the slave server.

Q5: How does the zone transfer differ in regular and DNSSEC server when analysing captured messages?

Then, change the key in the primary server and restart *named* in the both hosts and start capturing messages.

Q6: How can you see from the captured messages that you can't transfer zone files from the primary server?

Q7: Take a copy of *named.conf* files and zones files of *ns1* name server and include them in the final report. Do not include whole file, just the most important and interesting parts. In the final report you have to explain briefly what you have done.

5.3 Configuring an Intranet and a DNS

The goal now is to configure a regular domain name server for Intranet and Internet. This is situated in the same name server. The network structure is shown in *Figure 3*.

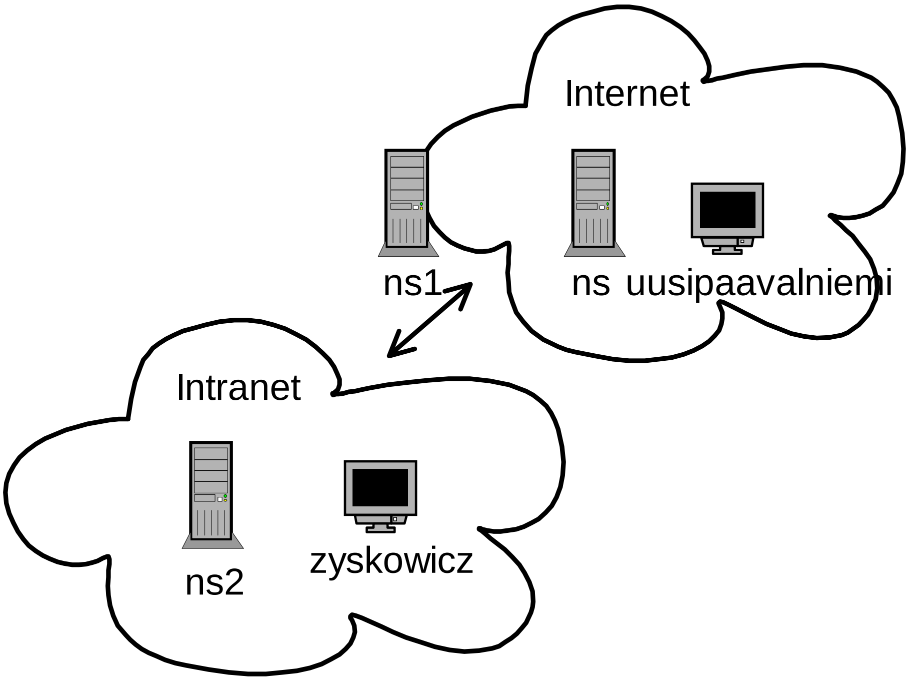

Figure 3 *Network structure*

In the name server *ns1* you have to edit two files: *named.conf*, zone file. No reverse zone file is needed. This time *ns2* and *ns.media* are not acting as name servers.

First make sure an HTTP server is running in both *ns1* and *ns2*. Change the network settings of *uusipaavalniemi* and *zyskowicz*: the name server is now *ns1*. Stop Bind in *ns2*.

Now your task is to configure a domain name server in *ns1.dns.lab*. It has to:

- Give the IP address of *ns1* if the name query for *www.dns.lab* comes from the Internet (for example from *uusipaavalniemi)*
- Give the IP address of *ns2* if the name query for *www.dns.lab* comes from the Intranet (for example from *zyskowicz*)
- Deny the access from Internet to *ns2* and to the Intranet
- Have access to all the computers from Intranet with their own names.
- Forward another enquiries as for *dns.lab* to *10.38.0.1*

The network address of the Intranet is *10.38.10.0/24.*

Hints: You can e.g. create different zones for the Internet and the Intranet. In *named.conf* you can create an access control list (ACL) for defining a trusted subnet.

If you have configured Bind correctly, you'll see different web pages, when viewing *www.dns.lab* pages from z*yskowicz* and *uusipaavalniemi*.

Q8: Take a copy of *named.conf* files and zones files of *ns1* name server and include them in the final report. Do not include the whole file, just the most important and interesting parts. In the final report you have to explain briefly what you have done.

6. Before leaving the lab room

Be sure you have all the necessary zone, reverse zone and *named.conf* files with you.

Remove all the configuration files (or clean them) you have made today. **Do not remove *named.conf.sample* files!** Backup the network configurations of the PCs. Reboot all three name servers.

7. Final Report

You have to include:

- Answers to the questions shown in this lab work in your final report.
- Answers to the following questions (see below), in your final report

Q9: Your network has two name servers (a primary and a secondary). You don't have any connection limitation to primary's *named.conf* file. What can a malicious person do with data of the primary server?

Q10: Why should DNSSEC be used?

Q11: You are working at networking lab. A DHCP service is available and you have to use it. How should the lab's name server be configured? Write a configuration file and explain it briefly.

Q12: Why is caching usually used in name servers? Why is it better than a regular name server?

Q13: You did an intranet configuration with help of DNS in the exercise 5.3. Why isn't our configuration a good solution, if you also think of security aspects? How can you make a safer configuration?

Q14: What is the role of the 5 number sequences in zone and reverse zone files? What would the most optimal numbers be? Why?

Q15: Big operators don't allow doing recursive inquiries. Why not?

8. Appendices

[1] Sample configuration for *named.conf*
[2] Sample configuration for zone file
[3] Sample configuration for reverse zone file
[4] Look: *http://www.tml.hut.fi/~jii/bind82/config.html* for configuration commands.
[5] Look: *http://www.bind9.net/Bv9ARM.ch06.html* for configuration commands.

APPENDIX 1 Sample configuration for named.conf

```
// named.conf for an authorative name server 19990917 JM
//    authorative in the local net (X.Y.Z.0/24)
//    assuming public IP address X.Y.Z.W
//    we want to do recursing in the local net

// declare friendly networks with address match list
acl homenets {
                X.Y.Z/24;
}
options {
        directory "/var/named";
        dump-file "/var/named/tmp/named.dump";
        named-xfer "/usr/sbin/named-xfer";
        // We listen to our loopback and ethernet interface
        listen-on {
                X.Y.Z.W;
                127.0.0.1;
        };
        // Permit zone transfers to secondary
        // servers:
        //   ISP:s secondary server A.A.A.A
        //   friendly organization's server B.B.B.B
        allow-transfer {
                127.0.0.1;
               X.Y.Z.W;
               A.A.A.A;
               B.B.B.B;
        };
};

// Hint file for Internet root servers
zone "." {
        type hint;
        file "named.cache";
};
// Loopback net
zone "0.0.127.in-addr.arpa" {
        type master;
        file "0.0.127.in-addr.arpa";
};
// Master nets
zone "localnet.org" {
        type master;
        file "localnet.org";
        allow-query { any; }
};
zone "Z.Y.X.in-addr.arpa" {
        type master;
        file "Z.Y.X.in-adddr.arpa";
        allow-query { any; }
};
```

APPENDIX 2 Sample configuration for zone file

```
@       IN      SOA     land-5.com. root.land-5.com. (
                        199609206       ;
                        10800           ;
                        7200            ;
                        10800           ;
                        86400 )         ;
                NS      land-5.com.
                NS      ns2.psi.net.
                MX      10 land-5.com.

ns       A       156.56.2.4
www      A       156.56.2.1
gw       A       156.56.2.5
```

APPENDIX 3. Sample configuration for reverse zone file

```
@       IN      SOA     tehdas.fi. jtjarvi3.dns.lab. (
                        2003071103
                        28800
                        7200
                        604800
                        86400 )
                NS      ns1.dns.lab.


12              PTR     ns.tehdas.fi.
1               PTR     www.tehdas.fi
```