Aalto University

School of Electrical Engineering
Department of Communications and Networking

ELEC-E7330 Laboratory Course in Internet Technologies

33 – Domain Name System (DNS)

Student edition

Juha Järvinen, 20.9.2006
Matias Elo & Antti Kajander, 9.8.2010
Jitendra Kumar Pandit & Sunny Dutta, 30.7.2014
Abbas Waqar & Ogenda Dancun 27.6.2019

Contents

1. Preliminary Theory Exercise 3
2. Pre-Laboratory Exercise 4
   2.1. NS1 Configuration 4
   2.4. Pre Report 5
3. Laboratory Exercise A (Slave NS and Adding a Subdomain) 6
   3.1. Network Topology and IP Addressing Scheme 6
   3.2. Environment 6
   3.3. Instructions 7
      3.3.1. Bind files and ones to edit 7
      3.3.2. NS1 and NS2 Configuration (comnet.lab) 7
      3.3.3. NS Configuration (research.comnet.lab) 8
      3.3.4. TSIG Configuration 8
      3.3.5. Checking your configuration 9
4. Laboratory Exercise B (DSN configuration using views) 10
   4.1. Network Topology 10
   4.2. Instructions 10
   4.3. Configuring an Intranet DNS 11
   4.4. Hints 11
5. Laboratory Exercise C (DNS-R and DNS-NS) 11
   5.1. Topology 12
   5.2. Configuring an DNS-R 12
   5.3. Configuring an DNS-NS 12
   5.4. Testing the configuration 12
6. Final Report 13

Appendix A 14

Appendix B 15

Appendix C 15

1. Preliminary Theory Exercise

Answer the following questions to get a good and clear understanding of Domain Name System (DNS). The questions can be answered in Finnish or Swedish or English. Try and provide the answers to the questions as clearly and concisely as possible.

[P01] (2 points)

a) What is DNS and what is generally used for?
b) Differentiate between reverse and forward DNS mapping

[P02] (2 points)

Differentiate between static and dynamic DNS.

[P03] (3 points)

Briefly explain the following terms and their function in DNS:

a) Master and slave servers.
b) Primary, secondary and tertiary DNS servers.
c) Mail Exchange (MX).
d) DNS Security (DNSSEC).
e) TSIG.
f) Reverse Zone File.

[P04] (2 points)

A client makes a query: it wants to know IP address related to address www.netlab.hut.fi. Draw a picture about the name resolution process and explain it. Assume you are now in fool.com domain and your nameserver's DNS cache is now empty.

[P05] (1 point)

You have a new domain with nameservers 130.200.56.1 and 130.200.56.2 running in your office. There is something wrong or something is not considered as a good practice in this setup. Identify the problem.

[P06] (1 point)

Your company decides to buy a new domain name – company.fi. What are the different processes/steps that have to be followed before the name (company.fi) can be publicly used?

[P07] (1 point)

Provide at least two ways that you would use to share keys between DNSSEC servers.

Additionally, familiarize yourself with the laboratory work and the BIND configuration instructions, for example, Red Hat's Guide [2]. Read it carefully. Pay attention to the meaning of different files namely, named.conf, zone and reverse zone files together with information that they contain, the meaning of the different zone file resource record types (A, MX, NS, SOA, CNAME)

2. Pre-Laboratory Exercise

You have complete this exercise at home before coming to the Lab for Laboratory exercises. The concept is to make DNS nameserver NS1 and configure it for domain comnet.lab.

The network topology of the task is as shown in figure 1.

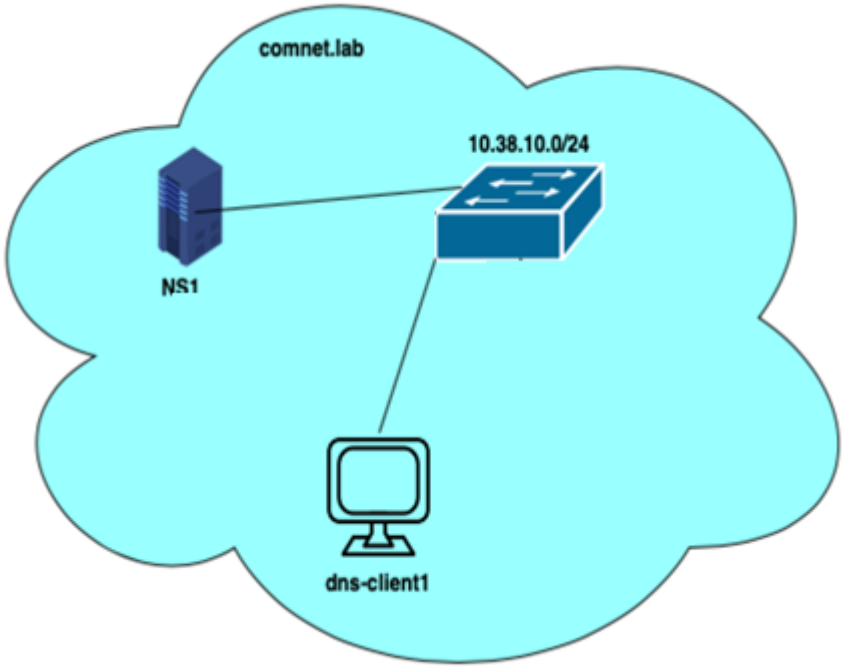

Fig. 1. Preliminary Exercise Network Topology

NS1 and client can be configured on Debian running Bind9 DSN software. For this purpose, there is a virtual box image (debian with Bind) available on course Mycourses page, which has the required software installed.

NAME	IP ADDRESS
NS1	10.38.10.1/24
dns-client1	10.38.10.10/24

2.1. NS1 Configuration

Add the necessary configuration on NS1 to make it: -

- Work as a master for the comnet.lab domain
- Do both forward and reverse queries (domain to IP address and vice versa)
- Allow recursion only from 10.38.10.0/24 network
- Allow queries only from 10.38.10.0/24 and not from anywhere else
- Create an alias www.comnet.lab for ns1.comnet.lab
- Create a mail server with a priority of 10 for ns1.comnet.lab

[P08] (2 points)

You have to show that the DNS server is running correctly. Use nslookup to show that your client can find:

- The IP address of www.comnet.lab
- The domain name of 10.38.10.1 from dns-client1

If you have problems getting DNS to work on the clients. Check that their name servers are configured correctly, dns-clien t1 should use 10.38.10.1. Name servers are configured in the `/etc/resolv.conf` file.

[P09] (2 points)

Familiarize yourself with dig and do some inquiries, for example www.finnair.fi and so on. Set +trace parameter on and do some more inquiries. Study the captured messages and give a very short report on what kind of information you can see in the inquiries and what is the function of +trace parameter.

[P10] (2 points)

Take a copy of named.conf, reverse zone and zone files from the name server. Include the files in the pre-report. Do not copy and paste the whole files, just take the useful and important parts as snippets. Explain briefly exactly what you have done.

2.4. Pre Report

Answer the questions from P01 to P10 in Pre-report.

NOTE: Preliminary exercise must be completed, and the report returned before coming to for the laboratory exercise as you will use those configuration files for further tasks.

3. Laboratory Exercise A (Slave NS and Adding a Subdomain)

In the laboratory, you will take your solution configuration and add a slave NS2 in the comnet.lab domain. Then you will configure a subdomain research.comnet.lab with its own local nameserver NS. The configurations for the machines (name servers and the clients) have already been done in the Lab. All the necessary networking and needed software has been installed. Do not try and install any software.

3.1. Network Topology and IP Addressing Scheme

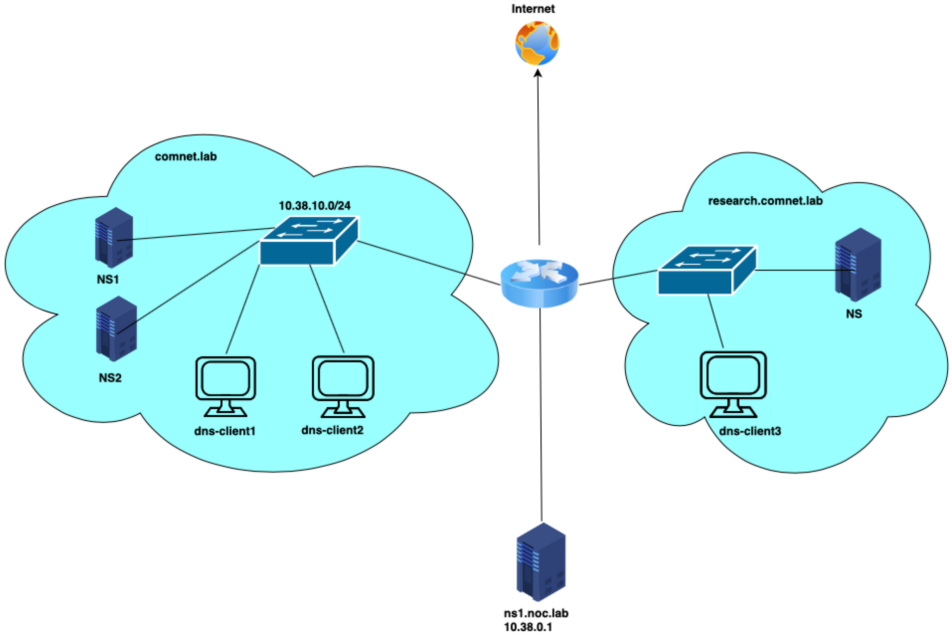

Fig. 2. Laboratory Network Topology

3.2. Environment

You will be configuring three DNS servers: **ns1.comnet.lab** (Copy your configuration files from Pre-report)**, ns2.comnet.lab** and **ns.research.comnet.lab**. The servers are running ISC's BIND name server software on Debian GNU/Linux. NS1 and NS2 are also running Monkey web servers. All servers are running automatic clock synchronization, as required by TSIG.

The web servers are preconfigured, you are not allowed to change any of their settings! You only need to configure BIND.

You can reach the servers via SSH. The username and password are both **lab.**

NAME	IP ADDRESS	BIND	HTTPD
NS1	10.38.10.1/24	INSTALLED	INSTALLED
NS2	10.38.10.2/24	INSTALLED	INSTALLED
NS	10.38.20.1/24	INSTALLED	
dns-client1	10.38.10.10/24		
dns-client2	10.38.10.11/24		
dns-client3	10.38.20.20/24		

Table 1. IP Addressing Scheme and Installed Software

For testing purposes there are three client machines running Debian. You can reach them via SSH. The username and password are both **lab.**

3.3. Instructions

The assignment is done on the workstation named PC2. Username is **lab** as well as the password. Log into the name servers using SSH as the **root** user. The password is **lab**.

3.3.1. Bind files and ones to edit

These are the files that you must edit in order to ensure that you place your configurations in the right place.

- Named.conf

A sample named.conf file is given in the appendices. In this file, you need to configure the properties of the DNS servers as defined in previous section (NS1 Configuration)

- Zone Files

Zone files go to */etc/bind/*. Zone file examples can be found from the DNS RFC and BIND Reference manual. Feel free to use any resource that you can find on the internet.

When naming zone files, use the following format:

- Master zone files: master.<DOMAIN> (e.g. master.comnet.lab)
- Slave zone files: slave.<DOMAIN> (e.g. slave.comnet.lab)
- Reverse master zone files: master.<IP> (e.g. master.10.38.10)
- Reverse slave zone files: slave.<IP> (e.g. slave.10.38.10)

There is a serial number in every zone file. Use the format YYYYMMDDNN, where YYYY is the year, MM the month, DD the day and NN a number between 00 and 99, e.g., 2010071700. Remember to increase this number every time after changing zone files. Otherwise the slave server won't notice the new zone configurations.

Some common zone files such as the forward and reverse zone files for localhost and the root zone file are included in the BIND package. These files are used in the sample named.conf. You should not make any modifications to them.

3.3.2. NS1 and NS2 Configuration (comnet.lab)

Copy your Configuration of NS1 from Pre-Lab work and modify it as per following:

- Use transaction signatures (TSIG) between NS1 and NS2 when transferring zone files.
- Forward other inquiries than for comnet.lab and research.comnet.lab to 10.38.0.1 and 10.38.0.2.
- Send all the queries related to research.comnet.lab domain to be resolved at ns.research.comnet.lab
- Allow recursion only from 10.38.10.0/24 and 10.38.20.0/24 networks
- Allow queries only from 10.38.10.0/24 and 10.38.20.0/24. Allow anyone to query comnet.lab.

Make NS2 to be able to: -

- Work as a slave for the comnet.lab domain
- Allow zone files to be copied automatically from the master (NS1) automatically. Do not create any zone files for NS2 as they should be transferred from the master.
- Be able to do forward and reverse queries
- Use TSIG when transferring zone files from the master (ns1.comnet.lab)
- Allow recursion only from 10.38.10.0/24 network
- Allow queries only from the 10.38.10.0/24 network

3.3.3. NS Configuration (research.comnet.lab)

Your NS configuration has to make the server:

- Work as a master server for research.comnet.lab domain
- Forward other inquiries than for research.comnet.lab both to ns1.comnet.lab and to ns2.comnet.lab
- Be able to do the transformation from name to IP and the reverse transformation from IP to name.
- Deny zone transfers
- Allow recursion only from 10.38.10.0/24 and 10.38.20.0/24
- Allow queries only from 10.38.10.0/24 and 10.38.20.0/24, but allow anyone to query research.comnet.lab zone
- Create an alias fool.research.comnet.lab for ns.research.comnet.lab

3.3.4. TSIG Configuration

TSIG is a mechanism used to provide authenticated server-to-server communication. It uses shared secrets and a one-way hash function to authenticate DNS messages. TSIG can protect the following type of transactions between servers: zone transfer, notify, recursive query messages, dynamic updates.

Run `ntpdate 10.38.0.1` in NS1 and NS2 to make sure the clocks are synchronized. Otherwise TSIG will fail.

Next you must create shared keys. Use HMAC-MD5 algorithm with 128-bit key length, key type is HOST. You can choose the key ID yourself. Keys are generated with dnssec-keygen:

```
dnssec-keygen -a <ALGORITHM_NAME> -b <N> -n <TYPE> -r </dev/urandom> <KEY_ID>
```

Now you have two key files, one with *.private* and one with *.key* extension. Copy the string preceded by "*Key*:" from the *.private* file to *named.conf* of ns1.comnet.lab and ns2.comnet.lab servers. The key statement in *named.conf* has the following syntax:

```
key <KEY_ID > {
        algorithm <ALGORITHM_NAME >;
            secret "<KEY >";
};
```

Add the next statement to the options section of your *named.conf* on the master server:

```
allow-transfer { key <KEY_ID>; };
```

Finally add the following to your *named.conf* file on the slave server:

```
server <IP > { keys <KEY_ID >; };
```

3.3.5. Checking your configuration

To check that your /etc/bind/named.conf is configured correctly, run the named-checkconf command. When the program prints nothing then it means your configuration is fine. However, if it prints something, which will show that you have errors. It will show the error and offer tips on how to correct them.

As for the zone files, run the named-checkzone <ZONENAME> <FILENAME >. The last line of the program output is supposed to print "OK". If the files are incorrectly configured, the servers will not work properly.

[Q01] (2 points)

Use tcpdump on NS1, interface eth0 for capturing. Then restart bind9 service in NS1 and NS2 machines. Capture DNS messages between the hosts when starting BIND in the slave server. What kind of information can you see in the captured messages?

Note: If the servers are not working, check /var/log/syslog to see what's wrong, fix it and try again. You don't have time to get stuck here, ask the assistant for help.

[Q02] (2 points)

In the named.conf of the master, alter the key and start capturing packets. Change the serial number at the server by incrementing it from the previous value. From the log messages, how can you prove that zone files can no longer be transferred from the master to the slave?
NOTE: After this part, make the keys in the master and slave match again.

[Q03] (2 points)

Then make an inquiry in dns-client1. Ask dns-client3's IP address with host, and capture messages between ns.media.dns.lab and ns1.dns.lab. Use the same capture settings as in Q1. How do the messages differ from Q1?

If you have problems getting DNS to work on the clients. Check that their name servers are configured correctly. dns-client1 should use 10.38.10.1, dns-client2 10.38.10.2 and dns-client3 10.38.20.1. Name servers are configured in the /etc/resolv.conf file.

You have to show to the lab assistant that the servers are running correctly. Use nslookup to show that your clients can find:

- The IP address of www.aalto.fi from all clients.
- The domain name of 10.38.10.1 from dns-client1 and dns-client3.
- The domain name of 10.38.20.1 from dns-client1.
- The IP address of ns.media.dns.lab from dns-client1 and dns-client3.
- The IP address of ns2.dns.lab from dns-client3.

[Q04] (3 points)

Take a copy of named.conf, reverse zone and zone files from all the name servers, Include the files in the final report. Do not simply copy and paste the whole files, just the most important and interesting parts. In the final report you have to explain briefly, what you have done in the configuration files.

4. Laboratory Exercise B (DSN configuration using views)

4.1. Network Topology

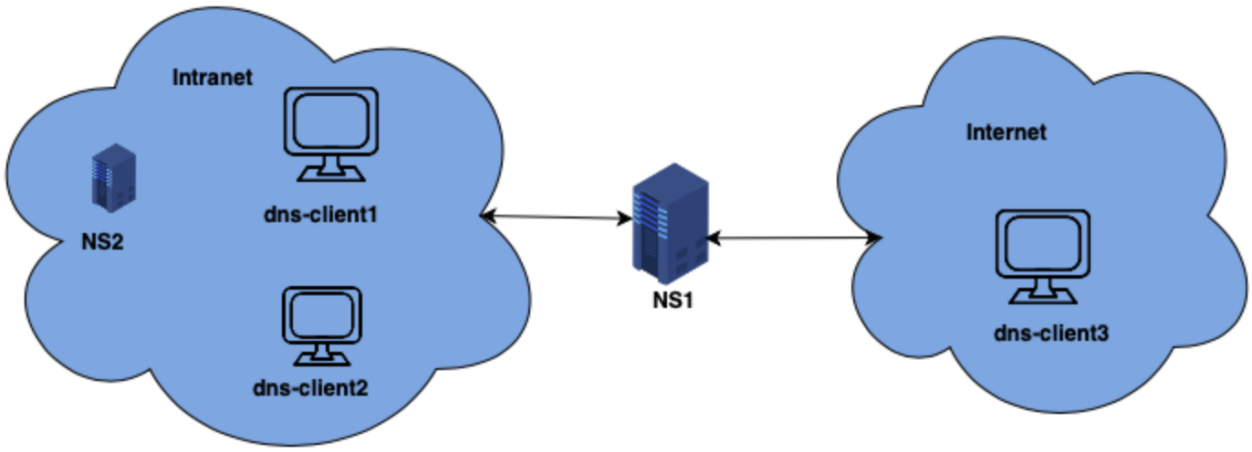

Fig. 3. Intranet DNS Topology

Before moving on from laboratory exercise A, backup your configurations of NS1, NS2 and NS. In this Lab you will learn to implement the concepts of "views" in BIND. BIND 9 introduced views, that's very useful in firewalled environments. Views allow you to present one name server configuration to one community of hosts and a different configuration to another community.

4.2. Instructions

The idea behind this laboratory exercise is to use view when configuring the different zone files. Views in bind allows you to create different version of same zones intended for different class of users. This means you can create zones for various views. For example, in this case, you are going to configure an intranet view that deals with IPs in the network 10.38.10.0/24 and an internet view that deals with the 10.38.20.0/0 network. As both NS1 and NS2 are working as High availability pair I.e. master and slave, views must be matched on both sides i.e. a view on a name server A should have a corresponding view on a name server B. You can create different zone files for each view.

The idea is to further through the use of views enable the viewing of webpages at NS1 and NS2 by configuring the subdomain (www.comnet.lab). Depending on the origin of the DNS query that needs to be resolved, then one of the webpages should be shown either using curl or through a web browser.

The web configuration has already been done. On NS1, when everything has been configured correctly, www.comnet.lab query from intranet network should display "***Welcome to NS1***" and "***Welcome to NS2***" for external network. The following part describes the tasks that have to be fulfilled for the web pages to be displayed.

4.3. Configuring an Intranet DNS

In the NS1 name server, edit the two files (named.conf and the zone file). Do not implement an additional reverse zone file as it is really not needed for this assignment.

Your task is to configure a domain name server in ns1.comnet.lab. It has to have the following: -

- Give the IP address of NS1 in case the name query for www.comnet.lab comes from the 10.38.20.0/24 network (internet). An example is a request that comes from dns-client3
- Give the IP address of NS2 in the name query for www.comnet.lab comes from the 10.38.10.0/24 network (intranet). An example is a query that comes from dns-client1 or dns-client2
- Deny the access from the internet to NS2 and to the intranet.
- Enable access to all the computers from the intranet with their own names
- Forward queries that are not related to comnet.lab to 10.38.0.1

4.4. Hints

Try to use different forward zone files: one for the internet and the other for the intranet. Create access control lists (ACLs) in the named.conf for defining the internet. Then by using views sections, create multiple zone configuration in the same configuration file.

The intranet is in the **10.38.10.0/24** network and the intranet is in the **10.38.20.0/24** network

[Q05] (3 points)

Prove that when you query www.comnet.lab from dns.client1, you are able to view the message "**Welcome to NS2**". Do the same from dns-client3 and show that the message is "**Welcome to NS1**"

[Q06] (3 points)

Include the important configurations that you made on NS1 and NS2 in your final report and explain exactly what they do.

5. Laboratory Exercise C (DNS-R and DNS-NS)

The idea behind this task is to configure one DNS-R (Resolver) that will act as an intermediary between the clients and the nameserver. The purpose of DNS-R is to determine whether the DNS query is destined for its local domain or not. If the query is for the local domain, it will forward it to the nameserver to be resolved there. In case the query is not for the local domain DNS-R will forward it to the root server. It can beneficial as it can relieve the burden from the Nameserver.

For this task, you have to remove the master and slave configurations for NS1 and NS2. Here NS2 will act as DNS-R and NS1 will be the DNS-NS.

5.1. Topology

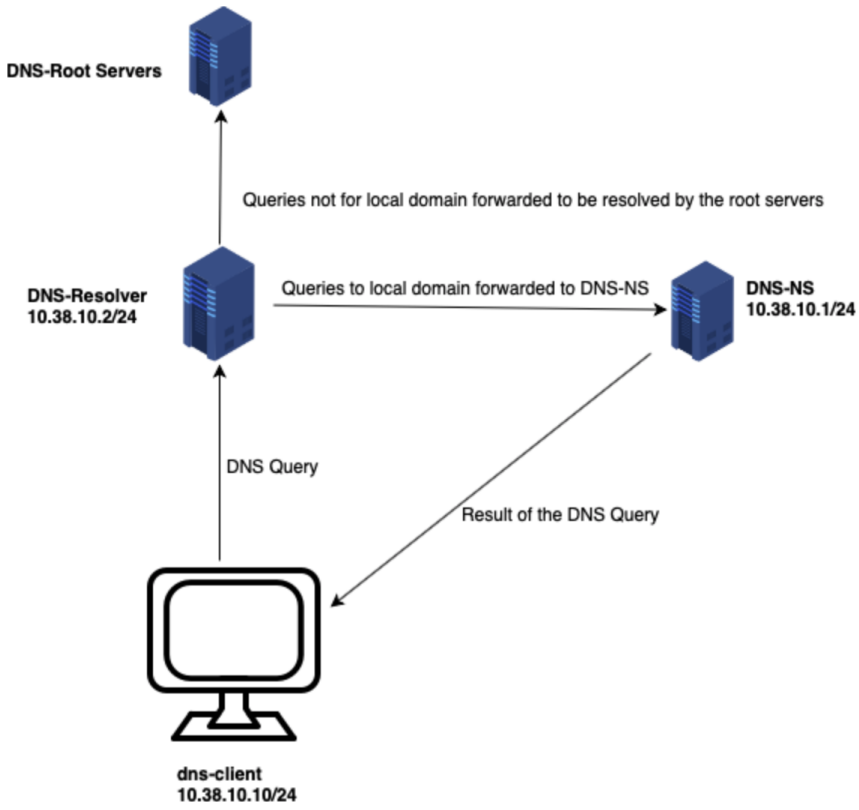

Fig. 4. Resolving queries (DNS-R)

5.2. Configuring an DNS-R

- Allow queries and recursion only from networks that are trusted
- Allow recursion
- Make it a forward only name server
- Make it forward queries to the DNS-NS
- Does not need its own zone files as it is only a forwarding name server

5.3. Configuring an DNS-NS

- Acts as a master and contains a zone file for the comnet.lab domain
- Allow queries from anywhere
- Allow transfers from the DNS-NS
- Do not allow recursion

5.4. Testing the configuration

Now that you have configured the domain comnet.lab (ns.comnet.lab), from the dns-client, try resolving the ns.comnet.lab and see the results

[Q07] (2 points)

Use tcpdump on DNS-R eth0 interface for capturing. Query www.comnet.lab and view the log messages between DNS-R and DNS-NS and explain briefly what is happening. (client should have nameserver configured as 10.38.10.2). Repeat the same process for another query of www.aalto.fi.

[Q08] (3 points)

Take sample parts of the configurations that you made in the DNS-NS and DNS-R. Try to give a short explanation of what you did.

6. Final Report

In the final report answer the following questions marked with Q and the following final report questions. Stay to be point and present concise answers to the questions.

[F1] (2 points)

Your network has two name servers (a master and a slave). You do not have any limitation on zone transfers and recursive queries in master's named.conf file. What harm can a malicious person do with the master server?

[F2] (1 point)

What is DNSSEC and why should it be used?

[F3] (1 point)

What is catching in the concept of name servers? Why it used and what is are its benefits?

[F4] (3 points)

You did an intranet configuration with help of DNS in the lab. Why isn't our configuration a good solution, if you also think of security aspects? What ways can the configuration be made safer?

[F5] (3 points)

What are the roles of the five numeric values configured in the start of authority (SOA) part of the zone and reverse zone files? What would the most optimal values be? Why?

[F6] (2 points)

Big operators' advice against the use of recursive queries. Provide explanations for this and why it is considered a bad idea

Appendix A

Sample configuration file for BIND

```
include "/ etc/ bind / rndc . key ";

options {
        directory "/ var/ cache / bind ";
        auth - nxdomain no;             # conform to RFC1035

//      forwarders {
//                      0.0.0.0;
//      };
};

//   prime the server with knowledge of the root servers
zone "." {
        type hint ;
        file "/ etc/ bind /db. root ";
};
//  be authoritative for the localhost forward and reverse zones ,
//  and for broadcast zones as per RFC 1912

zone " localhost " {
        type master ;
        file "/ etc/ bind /db. local ";
};

zone "127. in - addr . arpa " {
        type master ;
        file "/ etc/ bind /db .127";
};

zone "0.in - addr . arpa " {
        type master ;
        file "/ etc/ bind /db .0";
};

zone "255. in - addr . arpa " {
        type master ;
        file "/ etc/ bind /db .255";
};

//
//  Do any local configuration here
//
```

Appendix B

Sample zone file for BIND

```
$TTL 1h

@       IN  SOA    <NAMESERVER_DOMAINNAME >. <EMAIL_DOTTED >. (
        <SERIAL >
        1d
        1d
        4w
        1h
)
@                           NS              <NS_NAME >
<NS_NAME >                  A               <NS_IP >
<ALIAS >                     CNAME          <REAL >
```

Appendix C

Sample zone file for BIND

```
$TTL 1h

@       IN  SOA    <NAMESERVER_DOMAINNAME >. <EMAIL_DOTTED >. (
        <SERIAL >
        1d
        1d
        4w
        1h
)
                            NS              <NS_NAME >
<IP_LAST_PART >             PTR             <DOMAIN_NAME >.
```