Chapter 1

Prototype: School DNS

A school want to use a DNS server to filter certain internet sites from students and also have the opportunity to get a faster response from the name server.

1.1 Solution

To achieve the school's request, a BIND server could be set up. BIND is a open source implementation of the DNS protocol and is the most used DNS server software. One of the advantages with BIND, is that it supports both Windows, Mac and Linux. BIND acts like a caching server, where it stores answers to name queries which results in reduced response time of future queries to the same server.

When a requested hostname needs to be looked up the local cache is the first place to be checked. If the hostname is not found there a DNS server is asked. This might be your ISP or even a server on a "higher" level. It is also possible via BIND to forward your requests to a public DNS server, meaning it will be asked, if no other server before that (e.g. your ISPs DNS server) has the hostname in its cache. An overview of this system is showed in Figure 1.1:

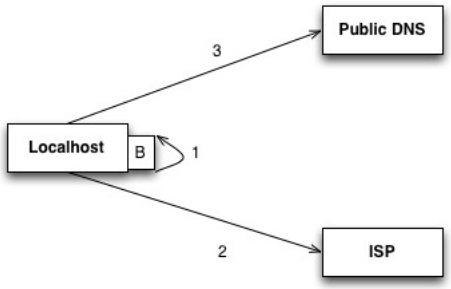

Figure 1.1: System overview

1.1.1 Setup BIND Server

To install a BIND server on Linux type in `sudo apt-get install bind[9]`. This will install version 9 of the BIND server software. To check if the installation is successful type `named -v` where – if successful, `BIND 9.8.1-P1` will be responded. For testing purpose, *dnsutils* have been used, because it can be used to see response time for the DNS lookup with the command `dig -x [IP-address]`.

1.1.2 Caching name server

A caching name server will find the answer to name queries and remember the answer the next time you need it. To set up the caching name server the configuration file /ect/resolv.conf needs to contain the following:
`nameserver 127.0.0.1`
To test the caching name server type `dig ubuntu.com` twice to see that the response time is a lot faster the second time:

```
;; Query time: 79 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Apr 25 17:33:03 2013
;; MSG SIZE  rcvd: 255
```

Figure 1.2: Use of the command `dig ubuntu.com` the first time

```
;; Query time: 5 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Apr 25 17:33:07 2013
;; MSG SIZE  rcvd: 255
```

Figure 1.3: Use of the command `dig ubuntu.com` the second time

1.1.3 Forward to public DNS

If the school wants to forward their requests to a public DNS, e.g. OpenDNS, they have to do a bit of research on finding the optimal solution for them. There is a lot of public DNS servers, where some of them are good at filtering bad hostnames, but are in the same time not always the fastest. In this section tests are made to find the fastest response time.

To find an optimal solution, Google's Test Bench (GTB) have been used. In this case GTB looked up around 4500 servers and tested them all to find the fastest server in average.

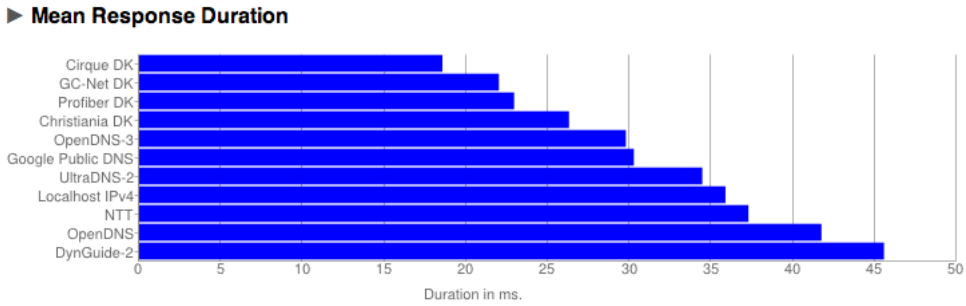

Figure 1.4: Output from Google Test Bench test

The test in Figure 1.2 and Table 1.1 shows, that Cirque DK have the lowest mean response time with 18 ms, and the default DNS have a mean response time on 36 ms. One of the more popular public DNS is openDNS, which is a little faster than the default DNS with 29 ms.

In a way of verifying the results of GTB, a manual test with `dig -x` have been made with 5 different internet sites and their given response time. To test the servers, the file located at */etc/bind/named* have to be edited with the address of the DNS server it shall forward to.

Forwarding - Cirquie.DK

Site	First test (ms)	Second test (ms)
Ubuntu.com	391	381
Bt.dk	356	906
Iha.dk	375	240
Facebook.com	354	207
Wikipedia.org	375	442

Forwarding - OpenDNS

Site	First test (ms)	Second test (ms)
Ubuntu.com	355	352
Bt.dk	792	436
Iha.dk	334	117
Facebook.com	184	279
Wikipedia.org	153	115

Table 1.1: Forwarding with Cirquie.DK and OpenDNS

It is hard to make a final conclusion based on our test, since the response times are unstable

(e.g. even though bt.dk was tested via Cirquie.DK two times under the same conditions; first test resulted in 356 ms and second in 906 ms), which is why GTB is a good tool to use. However, we can conclude that even if you forward to the one tested to be the fastest public DNS, you cannot be sure it is the fastest every single time, since the server might be busy.

1.1.4 Filtering

A DNS server can also be used as a simple filter, in the way of not providing the IP for harmful or illegal hostnames. Some public DNS servers, like OpenDNS, have this filter build-in, which means that you in a simple way can archive a bit of security.

In the same way, it is also possible to block specific hostnames with BIND, which can be useful if you want your filter to be more specialized. This can be used if a school wants to block for e.g. Facebook or Ekstrabladet.dk.

The problem about this way of filtering is if the users look up the IP directly. In that case, the DNS server will not be used and the filter will therefore not be used either and other methods have to be used.