Chapter 1

Conclusion

1.1 Conclusion

The DNS system is a cleaver solution to the original problem; connecting millions of computers through the internet. In many aspects the system is brilliant resolving human friendly logical names into IP address meanwhile being very fast and does not need user interference. Although there is no assurance that the requested data is not corrupted as the name servers can be cheated with altered DNS responses as outcome. Currently it can be guaranteed that DNS query/response transactions is secure if the digital signature-based DNSSEC is being used. Unfortunately the DNSSEC does not cover mail servers, web browsers or web servers.

There is a lot of ways of finding a solution for the school used as case in the prototype-development. To retrieve the caching functionality, BIND is simple and easy to set up and use. If wanted, it can furthermore be specialized in the way of setting up a filter or forwarding requests to a public DNS server.
BIND is a simple solution, but if better security or caching is wanted, a custom solution is needed. However, for a small school this might not be needed, and therefore BIND would be the suggested choice.

1.2 Discussion

The internet is a great system used by millions of computers every day and DNS servers are one of the main factors for its accessibility. Due to this fact it is necessary that no politic organization can shut down the servers to prevent the citizens access to the internet.

Security measures has been taken but a country like China has found loopholes to censor part of the internet, setting up *Deep Packet Inspection* near all international gateways and searching for certain keyword, they return bad IP-addresses before the correct is returned [**?**]. If it was "only" China's population who could not access certain websites it would be a relatively controlled problem, but if a computer in South Korea request a website and the location of the root DNS server is in China, South Korea is suddenly also affected.

Also it is significant that the security of the DNS query/response transaction is limited to the caching name servers as it can not be guaranteed that a web server is not attacked. Also the DNSSEC developers can not require implementation of the DNSSEC. As a result the users have to rely on their ISPs filters or they can use BIND with customized filtering.