DNS prestanda

YOUNES BENTAHAR

KTH Information and Communication Technology

Examensarbete inom
Kommunikationssystem
Grundnivå, 15 hp
Stockholm, Sweden

DNS prestanda

(DNS performance)

Younes Bentahar

2013-01-31

Kandidatexamensarbete

Examinator och handledare
Professor Gerald Q. Maguire Jr.

Skolan för informations- och kommunikationsteknik (ICT)
Kungliga Tekniska Högskolan (KTH)
Stockholm, Sverige

Abstrakt

Dator- och nätverksanvändandet är idag en del av vardagen. Användandet sker inte enbart när man sitter hemma, utan det kan ske hela tiden och överallt. Det kan handla om allt från att surfa in på någon webbsida när man är hemma, till att kolla sin e-post i mobilen när man är på väg till jobbet. De flesta funderar inte på hur det egentligen går till när man försöker ansluta till en webbsida genom att skriva in adressen i webbläsaren. Däremot något som de flesta nog lagt märke till är hur lång tid det ibland kan ta att komma åt någon webbsida.

Alla objekt som är direkt uppkopplade till IP-nätverket, har en unik IP-adress som används för att kunna kommunicera med varandra. IP-adressen är antingen en punktskild sifferföljd som består av 32 bitar eller en semikolonskild sifferföljd som består av 128 bitar, beroende på om det är IPv4 eller IPv6. Denna sifferföljd är ofta svår för oss människor att komma ihåg och av den orsaken konstruerades domännamnsystemet (DNS) som tillåter oss att genom adresser i textformat komma åt det sökta objektet på nätverket. DNS kan ses som ett uppslagsverk för nätverket och kan liknas vid en telefonkatalog, där om man vet namnet på en person kan hitta dennes telefonnummer.

I detta examensarbete kommer det att beskrivas hur olika adressöversättningar sker med hjälp av DNS. Det kommer även utredas hur stor påverkan DNS har på den upplevda fördröjningen från det att man skrivit in webbsidans adress i adressfältet i webbläsaren tills det att man faktiskt kommer fram till webbsidan. En undersökning av DNS prestandan kommer att presenteras som utreder hur mycket tid man kan tjäna på att använda någon av Sveriges två mest kända alternativa DNS-servrar (Google Public DNS och OpenDNS) istället för den normalt förinställda DNS-servern som fås av ens internetleverantör (ISP).

Undersökningen kommer även visa hur DNS uppslagningarnas väntetid förändras vid olika tidpunkter på dygnet samt vid olika veckodagar. Syftet med detta arbete är att ge en grundläggande förklaring av vad DNS är för något samt att öka förståelsen för hur en vardaglig nätverksanvändare på ett enkelt sätt kan effektivisera sitt nätverksanvändande genom att få sina DNS uppslagningar att gå fortare.

Slutsatsen från denna avhandling är att den alternativa DNS-servern Google Public DNS har snabbast DNS uppslagningstid för just denna dator som mätningarna genomförts på. Men detta säger oss ingenting om huruvida fallet är för andra nätverksanvändare eftersom den observerade DNS prestandan är till stor grad beroende av den ISP man är ansluten till samt vilken plats man befinner sig på.

Nyckelord: DNS, DNSSEC, prestanda, mätningar, Google Public DNS, OpenDNS

Abstract

Use of computers and computer networks is nowadays a part of everyday life. You do not use them only at home when you sit at you computer, but you can use them all the time everywhere. This can involve everything from surf to any website when you are at home, to checking your email on your mobile when you are on your way to work. Most people do not think about how it really works when they try to access a web page by typing the address into their browser, but something that most people probably notice is how long it can sometimes take to access a web page.

All items which are directly connected to the IP network have a unique IP address that is used to make it possible to communicate. The IP address is either a period separated sequence of digits representing 32 bits or a colon separated sequence of digits representing 128 bits, depending on whether the address is an IPv4 or IPv6 address. Such numeric sequences are often difficult for us humans to remember therefore, the domain name system (DNS) was constructed. DNS makes it possible for us to write addresses in a textual format to access an item stored in a device connected to the network. DNS can be seen as a directory for the network and can be compared to a telephone directory, where if you know the name of a person can find his or her phone number.

This thesis will describe how the various address translations are done by using DNS. It will also examine how much impact DNS has on the experienced delay from the time you type a web page address in the address bar of your browser to the actual time you reach the website. A survey of DNS performance will be presented to investigate how much delay can be reduced by using one of Sweden's two most well-known public DNS servers (Google Public DNS and OpenDNS) instead of the normal default DNS server provided by one's Internet service provider (ISP).

The survey will also show how the DNS lookup waiting time changes at different times of day and different days of the week. The purpose of this work is to provide a basic explanation of what DNS is and increase the understanding of how an everyday user in a simple way can make their network usage more effective by getting their DNS lookups to occur faster.

The conclusion from this thesis is that the alternative DNS server, Google Public DNS has the fastest DNS lookup time for this particular computer which the measurement was carried on. But this tells us nothing about whether the case for any other network users because the observed DNS performance has a large extent dependent on the ISP you are connected to, and what place you are at.

Keywords: DNS, DNSSEC, performance, measurements, Google Public DNS, OpenDNS

Innehållsförteckning

Figurförteckning

Tabellförteckning

Akronymer och förkortningar

Akronym	Förkortning	Svensk översättning
BBB	(A Swedish broadband company)	Bredbandsbolaget
CCN	Content-Centric Networking	Innehållscentrisk nätverkande
CDN	Content Distribution Networks	Innehållsdistribuerande nätverk
CPU	Central Processing Unit	Centrala processorenheten
CSV	Comma Separated Values	Kommaavgränsande värden
DNS	Domain Name System	Domännamnssystem
DNSSEC	Domain Name System Security Extension	Domännamnssystem säkerhetsutvidgning
DoS	Denial of Service	Förnekande av tjänst
DDoS	Distributed Denial of Service	Distribuerat förnekande av tjänst
DHCP	Dynamic Host Configuration Protocol	Dynamisk värd konfigureringsprotokoll
DPT	DNS Performance Test	DNS prestanda test
FTP	File Transfer Protocol	Filöverföringsprotokoll
HTTP	Hypertext Transfer Protocol	Hypertext överföringsprotokoll
IP	Internet Protocol	Internetprotokoll
ISP	Internet Service Provider	Internetleverantör
LAN	Local Area Network	Lokal area nätverk
OSI	Open Systems Interconnection	Förbindelse mellan öppna system
PCAP	Packet Capture	Paket fångande
RFC	Request For Comments	Begäran om kommentarer
RR(s)	Resource Record(s)	Resurspost(er)
RTT	Round Trip Time	Tur och Returtid
SMTP	Simpel Mail Transfer Protocol	Simpelt postöverföringsprotokoll
SRI	Stanford Research Institute	Stanford forskningsinstitut
TCP	Transmission Control Protocol	Transmissionskontrollprotokoll
TTL	Time To Live	Tid att leva
UDP	User Datagram Protocol	Användare datagramsprotokoll

Förord

Majoriteten av den information som finns inom informations- och kommunikationsteknik är skriven på engelska och därmed finns det flera termer och uttryck endast beskrivna på engelska. Denna avhandling är skriven på svenska och av den orsaken har de termer och uttryck som inte hittats på svenska, efter bästa möjliga förmåga översatts av mig personligen. Vid användning av svenska termer eller uttryck som inte är så vanliga så finns vid första tillfället, termen eller uttrycket används, en engelsk översättning i parantes.

Jag vill tillägna ett stort tack till Professor Gerald Q. Maguire Jr. som varit både min examinator samt handledare. Jag vill tacka honom för att ha introducerat mig till det ämne som behandlats i denna avhandling och för att alltid ha fått snabb och bra respons vid behov. En annan sak som jag är tacksam för är de rekommendationer jag fått om att delta på intressanta presentationer som varit relevanta för mitt arbete.

1 Inledning

Efter att ha skrivit in en webbadress i webbläsaren och tryckt på enter-knappen kommer man vanligtvis till webbsidan man söker. Det enda som en vardaglig internetanvändare lägger märke till efter att ha tryckt på enter-knappen och fram till dess att hela webbsidan visas är oftast en liten väntetid. Denna väntetid beror främst på fyra olika faktorer: (1) adressöversättningen från textformat som vi människor föredrar till IP-adressen som nätverket och routrar använder sig av, (2) tiden det tar att inrätta en TCP anslutning, (3) den väntetid det tar för att ta emot den första byte data efter att anslutningen inrättats, (4) nedladdningstiden det tar för att ladda ned objekt från hemsidan. Största delen av denna avhandling kommer att fokusera på adressöversättningar och hur dessa adressöversättningar sker med hjälp av domännamnsystemet (DNS) som kommer utredas närmare i kapitel 2.

1.1 Syfte

Syftet med denna avhandling är att ge en grundläggande förklaring av vad DNS är för något samt att öka förståelsen för hur man som vardaglig nätverksanvändare kan effektivisera sitt nätverksanvändande genom att få sina DNS uppslagningar att gå fortare. En undersökning av DNS prestandan kommer att göras för att se hur DNS uppslagningarnas väntetid förändras vid olika dagar och tidpunkter på dygnet samtidigt som en jämförelse kommer att göras av den lokala DNS-servern och de två mest kända alternativa DNS-servrar, *Google Public DNS* och *OpenDNS*.

1.2 Målgrupp

Målgruppen för denna rapport är främst elever som läser samma utbildning som mig, Civilingenjörsutbildningen med inriktning på Informationsteknik. Men den vänder sig även till andra elever på KTH:s ICT skola, samt till allmänheten som har ett intresse att få reda på hur de kan effektivisera sitt nätverksanvändande med hjälp av DNS. Det är tänkt att en person utan allt för stora nätverkskunskaper ska kunna läsa och förstå denna rapport och av den orsaken har ett flertal grundläggande begrepp förklarats grundligt.

1.3 Introduktion till DNS

Innan DNS uppfanns fick varje nätverkskoppladdator en handskriven textfil (HOST.TXT) från en dator på SRI. Textfilen innehöll en mappning mellan olika namn och numeriska adresser. Nätverkets snabba tillväxt hade till följd att detta tillvägagångssätt blev ineffektivt och man behövde alltså ett system som automatiskt kunde sköta om denna mappning. Detta var anledning till varför DNS uppfanns och konstruerades år 1983 av Paul Mockapetris.

Målet med domännamn finns beskrivet i *RFC 1035* som *"The goal of domain names is to provide a mechanism for naming resources in such a way that the names are usable in different hosts, networks, protocol families, internets, and administrative organizations."* [1] och DNS, som finns introducerat i *RFC 1034* [2], är systemet som sköter denna mekanism. DNS är ett distribuerat databassystem som bygger på klient/server-modellen och består av ett flertal domännamnsservrar (DNS-servrar) som innehåller och lagrar information. Dessa DNS-servrar tar bland annat emot förfrågningar från klientsidan av DNS applikationen eller andra DNS-servrar och svarar med information om det sökta värddatornamnet eller den sökta IP-adressen. DNS är ett protokoll som tillhör applikationslagret i OSI-modellen, men kan ses som ett protokoll som är anställt av andra protokoll i samma lager. Detta eftersom DNS inte är ett protokoll som användaren direkt kommer i kontakt med utan är ett protokoll som körs i bakgrunden och används av applikationer såsom FTP, webbläsare, e-postklient, osv. [3]

1.4 Problemdefinition

Moderna webbsidor kräver idag ett flertal DNS uppslagningar eftersom de i många fall har ett ökat innehåll kommandes från externa webbsidor som till exempel vid fall då kommenteringssystem finns, integration av sociala medier förekommer, osv. och därför har det visat sig att ände-mot-ände (English: end-to-end) DNS prestandan har fått en allt viktigare roll för den tid det tar att hämta en webbsida [4]. För att få en uppskattning om hur stor faktor DNS har på väntetiden det tar för att hämta en webbsida kan en titt tas på en mätning som gjorts av Google Developers [5]. Den totala tiden för att hämta en webbsida var 11 sekunder och hela 13 DNS uppslagningar gjordes och trots att flera av dessa 13 DNS uppslagningar skedde parallellt krävdes ändå 5 seriella DNS uppslagningar som totalt stod för flera sekunder av den totala tid det tog för att hämta webbsidan.

1.5 Omfattning

Detta arbete kommer att fokusera på DNS prestanda och därmed kommer ett flertal mätningar att göras. Mätningar och en jämförelse kommer att göras av:

- den DNS-servern som automatiskt fås av ISP:n *(BBB);*
- den alternativa DNS-servern *Googles Public DNS; och*
- den alternativa DNS-servern *OpenDNS.*

Just dessa DNS-servrar valdes eftersom det är intressant att se hur stor skillnad det är på DNS prestandan av den DNS-server som fås av ISP:n (i detta fall DNS-servern för Bredbandsbolaget - BBB) jämfört med de två största alternativa DNS-servrarna (Google Public DNS och OpenDNS). En analys kommer att göras om hur DNS prestandan påverkas med användning av dessa två tekniker:

- DNS cache och
- DNSSEC.

Efter att dessa mätningar och analys är genomförda kommer en slutsats att presenteras som har i syfte att hjälpa vardagliga användare att få en bättre inblick i hur de kan effektivisera sitt nätverksanvändande med hjälp av DNS.

2 Domännamnsystemet (DNS)

I det här avsnittet kommer domännamnsystemet (DNS) att utredas närmare. Vi kommer att göra en närmare granskning och beskriva saker som: funktioner som tillhandahålls, ställning inom nätverksanvändandet, hierarki, namnuppslagningsprocess, cache lagring, meddelande och poster, sårbarheter, DNSSEC, och alternativa DNS servrar. En stor del av informationen om DNS grundar sig på det som skrivs i J. Kurose och K. Ross, *Computer Networking,* (2009*)* [3].

2.1 Funktioner som tillhandahålls

Huvuduppgift för DNS är adressöversättningen från ett namn som vi människor är vana att se den som till exempel *www.kth.se* till en IP-adress som nätverk och routrar använder sig av som till exempel *130.237.72.246*. Men detta är inte DNS enda uppgift utan man kan även med hjälp av DNS binda ett flertal namn till en eller flera IP-adresser. Sedan kan man med hjälp av antingen ett namn eller en IP-adress få reda på alla namn som är bundna till en viss IP-adress. DNS medför även att man kan få korta e-postadresser som är enkla att komma ihåg och att företag kan ha samma adress till både sin e-postserver och webbserver. Ytterligare en funktion som DNS tillhandahåller är lastfördelning som är praktiskt för stora webbplatser med miljontals användare. Dessa webbplatser med miljontals användare har oftast flera servrar med olika ändsystem som tar hand om de besökande klienterna. Alla dessa servrar har olika IP-adresser och alla dessa IP-adresser finns sparade i DNS databasen. När en förfrågan fås av en sådan adress skickas en lista med alla IP-adresser ut, men det lastfördelningen gör är att den skiftar ordningen i listan. Eftersom den skickat förfrågningen oftast använder den första tillgängliga adressen medför detta att en jämn fördelning på de olika servrarna sker och det minskar risken att en server överbelastas.

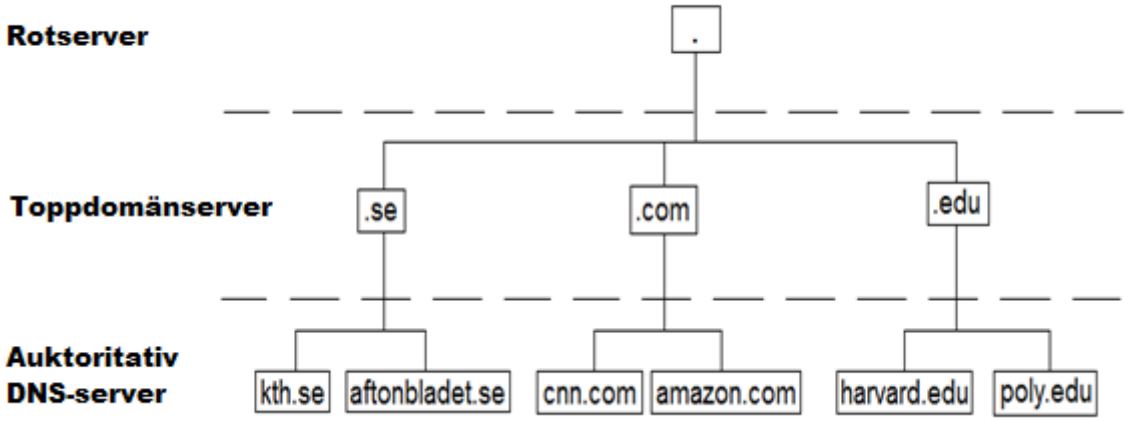
2.2 Ställning inom nätverksanvändandet

DNS har en enormt viktig ställning inom dagens nätverksanvändande och med hjälp av ett antagande kommer denna ställning att försöka framhävas. Om man antar att DNS helt plötsligt slutar fungera en dag så skulle man vara tvungen att kunna IP-adressen till servern man vill ansluta sig till. Förutom att IP-adressen är mycket svårare för oss människor att minnas än ett namn, stöter vi även på stora problem då dessa IP-adresser ofta uppdateras vilket gör det omöjligt för oss människor att kunna nå servern utan att ha den rätta IP-adressen. DNS-servrar finns utspridda över hela världen och varför man valt att inte ha alla på ett och samma ställe kopplat till en och samma server finns det flera anledningar till. Först och främst hade en situation som ovan beskrivits inträffat ifall en brand eller liknande hade uppstått och DNS-servern hade kraschat. Förutom att det hade krävts en väldigt stor DNS-server för att få plats med all information i en och samma databas hade det även vart servern än placerats, funnits nätverksanvändare som fått skicka sina förfrågningar runt halva jordklotet för att nå fram till servern. Även trafikproblem hade uppstått då alla världens nätverksanslutningar försöker nå samt få hjälp från en och samma plats. Det hade även krävts konstanta uppdateringar för varje ny klient som ansluter till servern.

2.3 Hierarki

DNS servrarna är uppdelade i en tre nivås hierarki där den högsta nivån är rotservrar som det finns 13 stycken utav. Rotservrarna ger ut information om toppdomänservrarna som är den andra nivån i hierarkin. Toppdomänservrarna är ansvariga för alla länders toppdomäner som *se, fi, fr, uk, jp,* osv, men även för alla toppdomäner som *com, net, org, edu,* och *gov*. Längst ner i hierarkin har varje myndighet, företag, eller organisation sin egen auktoritativa DNS-

server (se Figur 1). Observera att många enheter som har ett tilldelat domännamn utnyttjar en tredje part som tar ansvaret för tillhandahållande av en auktoritativ DNS-server för dem.



Figur 1: DNS-server hierarki

Förutom de nämnda servrarna i DNS-server hierarkin har även varje ISP, företag, universitet, osv. även en lokal DNS-server. Denna lokala DNS-server är vanligtvis placerad i samma LAN eller högst ett par routrar från klienten och har bland annat i uppgift att oftast med hjälp av en DHCP-server dela ut IP-adresser till nya klienter som ansluter sig till nätverket samtidigt som DHCP-servern rapporterar varje klients IP-adress till den lokala DNS-servern. Det är även denna DNS-server som klientsidan av DNS applikationen först skickar iväg en förfrågan till. Den lokala DNS-servern agerar sedan som en proxy och skickar vidare förfrågningen till resten av DNS hierarkin.

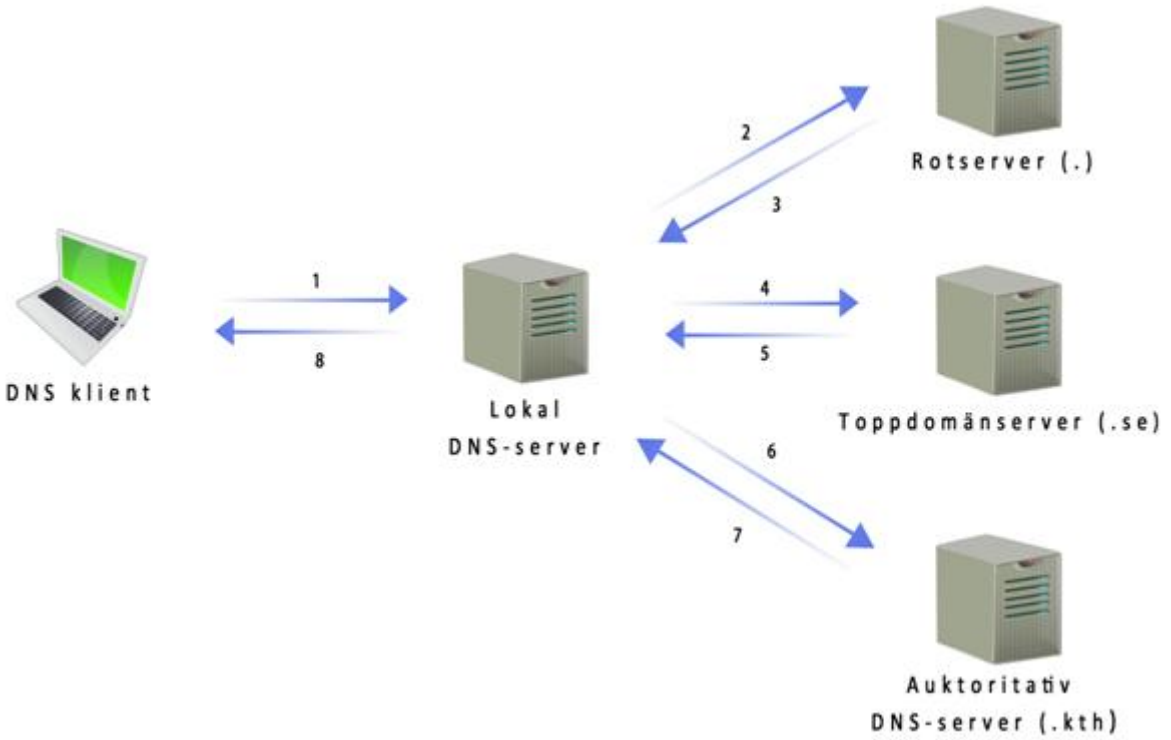
2.4 Namnuppslagningsprocess

Det går till på följande sätt när en användare försöker ansluta till en webbadress. Först skriver användaren in webbadressen som till exempel *www.kth.se* i webbläsaren och det denna gör är att den skickar domännamndelen av webbadressen vidare till klientsidan av DNS applikationen som är igång i bakgrunden på samma maskin. Klientsidan skickar därefter vidare en förfrågan innehållandes detta namn till en DNS-server och inväntar sedan ett svar innehållandes en IP-adress. När klientsidan mottagit IP-adressen skickas den vidare till webbläsaren som sedan kan hitta webbservern och upprätta en anslutning. Det är från dess att klientsidan av DNS applikationen skickat iväg en förfrågan till dess att den får tillbaka ett svar som den största fördröjningen som orsakas av DNS uppstår.

Namnuppslagningsprocessen kan se ut på följande sätt (se Figur 2) när man vill få reda på IP-adressen till en webbadress som man för första gången ska besöka:

1. Klienten skickar en förfrågan innehållandes det sökta värddatornamnet som till exempel *www.kth.se* till dess lokala DNS-server.
2. Den lokala DNS-servern känner inte till detta namn och inte heller IP-adressen till toppdomänservern som är ansvarig för den noterade ändelsen *(.se)*. Förfrågan om värddatornamnet *(www.kth.se)* skickas vidare till rotservern.
3. Rotservern noterar ändelsen på domännamnet som i detta fall är (*.se)* och svarar med en lista innehållandes adress till toppdomänservrar som är ansvariga för (*.se).*
4. Den lokala DNS-servern skickar vidare förfrågan om värddatornamnet *(www.kth.se)* till en av de ansvariga toppdomänservrarna.

5. Toppdomänservern känner inte till det sökta värddatornamnet men noterar (*.kth)* från domännamnet och svarar med en adress till den auktoritativa DNS-servern.
6. Den lokala DNS-servern skickar vidare förfrågan om värddatornamnet *(www.kth.se)* till den auktoritativa DNS-servern.
7. Den auktoritativa DNS-servern känner till det sökta värddatornamnet och svarar med information om den sökta IP-adressen.
8. Den lokala DNS-servern skickar det sökta värddatornamnets IP-adress tillbaka till klienten.



Figur 2: Exempel på hur en namnuppslagningsprocess kan gå till

Som det framgår i processen ovan så måste ett flertal steg utföras innan klienten kan få det sökta värddatornamnets IP-adress och varenda en av dessa steg medför en viss fördröjning. Flertalet av dessa steg går emellertid ofta att slippa med hjälp av en cache lagringsteknik *(se avsnitt 2.5)* som finns implementerad i DNS systemet. I processen ovan kan vi även se att förfrågningarna sker både rekursivt och iterativt. DNS-servrar som tar emot en förfrågning och sedan själv skickar förfrågningen vidare står för de rekursiva anropen medan DNS-servrar som endast ger ett så bra svar som möjligt utan att själv fråga vidare står för de iterativa anropen. I figuren ovan kan vi se att den lokala DNS-server står för de rekursiva anropen medan de andra DNS-servrarna står för de iterativa anropen. I allmänhet är oftast alla rotservrar och toppdomänservrar iterativa eftersom de redan har tillräckligt mycket arbete. De rekursiva servrarna använder sig ofta av cache lagring som gör att många DNS förfrågningar redan finns sparade på servern och därmed minskar DNS förfrågningarna som behöver göras på resten av nätverket.

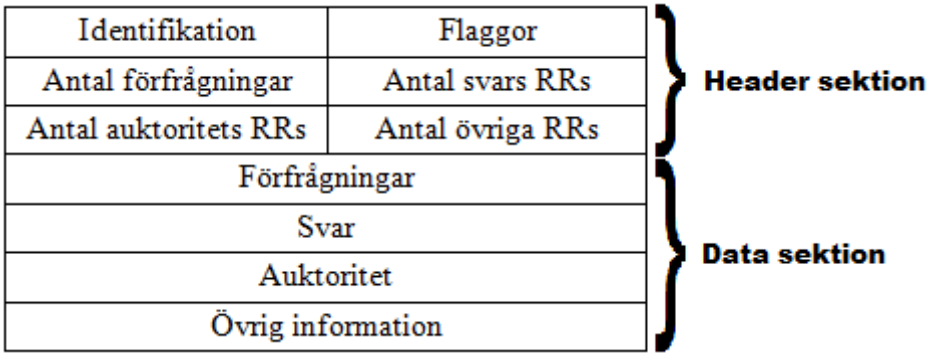
2.5 Cache lagring

Det cache lagringstekniken gör är att efter att en server fått en förfrågan och sedan även ett svar från en annan server, sparas denna information på servern. Om en ny förfrågan om samma namn inkommer till servern så finns denna information redan sparad på servern och

därmed kan servern snabbare ge ett svar till klienten eftersom man slipper ett antal steg i namnuppslagningsprocessen som beskrivs ovan. Om exempelvis den lokala DNS-servern får en förfrågan om ett namn som den redan finns lagrat i serverns cacheminne, slipper man utföra steg 3 till 7 i namnuppslagningsprocessen och behöver alltså bara utföra 3 steg vilket medför att uppslagningstiden kraftigt minskar. Informationen sparas endast en begränsad tid på servern eftersom IP-adresser ofta uppdateras och en ny hämtning krävs för att man ska ha rätt information om det sökta namnet. DNS-servern inkluderar i sitt svar den maximala tid som detta svar kan vara cache lagrat.

2.6 Meddelande och poster

Vanligtvis sänds DNS-meddelandena från klienten och mellan de olika DNS-servrarna över UDP på portnummer 53 [1]. DNS förfrågningar består oftast av endast en UDP förfrågan från klienten följt av endast ett UDP svar från servern. Men när ett DNS-svarsmeddelande är större än standardstorleken (512 bytes) svarar servern med ett UDP datagram innehållandes så mycket data som tillåts och markerar det med en flagga som talar om att det är ofullständigt och tillåter därmed avsändaren att skicka förfrågningen igen och denna gång över TCP på portnummer 53. Andra fall då TCP används är bland annat vid zonöverförningar men det finns även vissa klienttillämpningar som använder TCP för alla förfrågningar. Det finns endast två sorters DNS-meddelanden (förfrågningar och svarsmeddelanden) båda dessa har samma format och semantiken ser ut på följande sätt (se Figur 3).



Figur 3: DNS-meddelandeformat

DNS-meddelandets första 12 bytes utgör dess *header sektion* som är indelad i 6 lika stora fält: *Identifikation, Flaggor, Antal förfrågningar, Antal svars RRs, Antal auktoritets RRs,* och *Antal övriga RRs*. Första fältet *Identifikation* används för att matcha rätt svar med rätt förfrågan. Fältet *Flaggor* har flera 1 bits flaggor som beroende på ifall biten innehåller en etta (1) eller en nolla (0) talar om olika saker såsom ifall: meddelandet är ett svar eller en förfrågan, svarsmeddelandet är från en auktoritativ DNS-server eller inte, DNS-servern stöder rekursiva anrop eller inte, etc. De fyra resterade fälten i meddelandets header sektion talar om antalet förekomster och hur de följande fyra fälten i data sektionen av DNS-meddelandet används.

I *data sektionen* finns det fyra fält: *Förfrågningar, Svar, Auktoritet,* och *Övrig information*. *Förfrågningsfältet* innehåller ett varierande antal förfrågningar där det finns information om förfrågningen som ska göras. Förfrågningarna är uppdelade på följande sätt (se Figur 4) där det finns en del som innehåller förfrågningsnamnen och sedan finns två ytterligare delar, var den ena anger vad det är för typ av förfrågan (om det man söker t.ex. är e-post servern eller värddatornamnet) och den andra anger vad det är för klass (som oftast är klassen IN som står för internet). De tre efterföljande fälten i data sektionen innehåller ett varierande antal poster (English: Resource Records - RRs). *Svarsfältet* innehåller poster för

det ursprungligt förfrågade namnet, *Auktoritetsfältet* talar om vad det finns för andra auktoritativa servrar och det sista fältet *Övrig information* ger annan nyttig information (som till exempel ett alternativt värddatornamn eller en alternativ e-post server).

Förfrågningsnamn	
Förfrågningstyp	Förfrågningsklass

Figur 4: Formatet på förfrågningsfältet i ett DNS-meddelande

Posterna är så kallade *Resource Records (RRs)* och består av en fyrtupel som ser ut på följande sätt: (Namn, Värde, Typ, Tid att leva (TTL)). Där fälten *Namn* och *Värde* betyder olika saker beroende på vad posten är för *Typ*. Det finns ungefär 50 olika posttyper. I Tabell 1 kan ni se exempel på några vanligt förekommande typer samt en beskrivning på vad fälten *Namn* och *Värde* får för betydelse vid dessa posttyper. Fältet TTL innehåller den tid som anger hur länge en post kan vara cache lagrad.

Tabell 1: Beskrivning på några vanligt förekommande posttyper (RRs)

Typ	**Beskrivning**
A	En normal värddatornamn till IP-adress mappning. Fältet *Namn* innehåller värddatornamnet och fältet *Värde* innehåller dess IP-adress.
NS	Specificerar auktoritativa servrar för en viss domän. Fältet *Namn* innehåller en domän och fältet *Värde* innehåller värddatornamnet för auktoritativa DNS-servrar.
CNAME	Den här typen anger ett alternativt värddatornamn till det sökta värddatornamnet. Fältet *Namn* innehåller alias värddatornamnet och fältet *Värde* innehåller det alternativa värddatornamnet.
MX	Medför att värddatornamn för e-post servrar kan få korta alias som är enkla att komma ihåg. Typen MX gör det även möjligt för företag att till exempel ha samma adress för både en webbserver och en e-post server. Fältet *Namn* innehåller ett alias värddatornamn och fältet *Värde* innehåller ett alternativt namn till en e-post server.

2.7 Sårbarheter

Trots DNS viktiga roll inom användandet av IP-nätverk finns ett par sårbarheter. Detta beror främst på DNS öppna distribuerade design och användningen av det osäkra UDP protokollet. De vanligaste två attackerna är cache förgiftningsattacker (English: Cache poisoning attacks) och förnekande av tjänst (English: Denial of Service - DoS) attacker [6]. Cache förgiftningsattackerna går ut på att felaktig information placeras i DNS cachen som ofta leder till att en användare blir omdirigerad från en förlitlig webbplats till en skadlig webbplats som till exempel kan försöka lura en användare till att ge ut personlig information, kontonummer, lösenord, mm. DoS attackers ändamål är att förhindra ett system från normal användning. De vanligaste DoS attacken är överbelastningsangrepp där ett system som blir attackerat lägger alla sina resurser på att hantera det inkommande data som attackerna orsakat och därmed finns inga resurser kvar till att hantera systemets relevanta data. DNS-servrar har ofta många adresser sparade i cacheminnet, vilket DoS attackerna utnyttjar för att antingen utföra distribuerade förnekande av tjänst (English: Distributed Denial of Service - DDoS) attacker på klienterna själva eller utnyttja klienterna för att utföra DoS attacker på andra system. DDoS attacker innebär att en stor mängd anrop görs med en relativt liten mängd data, attackerna kommer från ett stort antal olika datorer som gör det svårt för systemet att avvärja attacken genom att blockera specifika IP-adresser.

2.8 DNSSEC

Domännamnssystem säkerhetsutvidgning (English: DNS Security Extension - DNSSEC) är en utvidgning av DNS med syfte att täppa igen dess sårbarheter genom att skapa integritet och autentisering av informationen som sänds mellan klienten och de olika DNS-servrarna [7]. Detta sker genom asymmetrisk kryptografi som går ut på att man har två olika nycklar, en allmän nyckel som används för att kryptera informationen som ska sändas och en privat som används för att dekryptera informationen. Observera att i fallet med DNSSEC används den privata nyckeln för att signera ett meddelande och den allmänna nyckeln används för att verifiera att meddelandet inte har ändrats och att avsändaren är som de påstår sig vara. DNSSEC försöker skapa en kedja av tillit som börjar i rotservrarna och sedan rör sig vidare nedåt i hierarkin.

Meningen är att försöka få så många som möjligt att gå över till DNSSEC och därmed öka sannolikheten att det man söker har blivit digitalt undertecknat så att man kan vara säker på att inga ändringar gjorts i meddelandet. DNSSEC är även bakåtkompatibel med vanlig DNS, vilket gör det fortfarande möjligt för klienter som inte gått över till DNSSEC att få tag i meddelandet utan att det blivit digitalt undertecknat [8]. En viktig dag för DNSSEC var 15 juli 2010 då rotservrarna blev signerade och införde DNSSEC [9].

Det finns ett par nackdelar med DNSSEC. En nackdel är att trots DNSSEC är en säkerhetsåtgärd åt DNS, inte skyddar mot DDoS attacker som är en vanligt förekommande attack mot DNS-servrar. Den största nackdelen med DNSSEC är att den medför att man förutom de steg som tidigare nämndes i samband med en adressöversättning med hjälp av DNS, nu även blir tvungen att vänta på att autentiseringen och integriteten utförs och att extra information kopplat till DNSSEC sänds [10]. Dessa extra åtgärder medför att väntetiden ökar för slutanvändaren.

2.9 Alternativa DNS-servrar

Förutom den lokala DNS-servern som erbjuds av en nätverksanvändares ISP finns ett antal alternativa DNS-servrar som nätverksanvändare kan använda sig av istället. Exempel på dem två största tredjepartens DNS-servrar är *Google Public DNS* [11] och *OpenDNS* [12], båda är gratis och enkla att konfigurera. Syftet hos dessa alternativa DNS-servrar är att snabba upp DNS användningen genom att ha en stor databas med vanligt förekommande adresser så att dessa kan fås direkt utan att behöva kontakta andra servrar. Många alternativa DNS-servrar ger förutom en möjligen förbättrad hastighet även en extra säkerhet för användaren, genom att bland annat blockera kända webbplatser som exempelvis utnyttjas av hackare för att komma åt en användare, används för nätfiske eller innehåller sabotageprogram [13].

3 Bakgrund

I detta avsnitt kommer nödvändig information erhållas om olika relaterade arbeten samt information om vilka olika program som använts för mätningar och analys av de olika testerna som genomförs i denna avhandling.

3.1 Relaterade arbeten

En intressant undersökning är "*Comparing DNS Resolvers in the Wild"* som gjordes i Berlin år 2010 och som undersöker 50 lokala DNS-servrar som fåtts av ISP:n gentemot de två största alternativa DNS-servrarna *Google Public DNS* och *OpenDNS* [14]. Denna undersökning har ett par likheter med mitt arbete, vilket är anledningen till att den ligger i mitt intresse. Det framgår från undersökningen att två aspekter utgör den mest betydelsefulla delen av DNS uppslagningstiden. Dessa är (1) fördröjningen av servern och (2) innehållet i DNS cachen när förfrågningen görs. Slutsatsen av denna undersökning är att slutanvändare som använder den lokala DNS-servern som fås av ISP:n upplever väldigt små fördröjningar på grund av DNS-servern. Det existerar även fall då tredjepartens DNS-servrar som *Google Public DNS* och *OpenDNS* överträffar den lokala DNS-servern om man granskar antalet svar. Flertalet DNS-servrar som fås av ISP:n och tredjeparten förlitar sig på en lastbalanseringsinstallation av trafiken utan en gemensam cache, vilket leder till dålig effektivitet. Ett annat stort problem som påträffades var att slutanvändare med tredjepartens DNS-servrar inte lyckades att komma åt innehåll som fanns inom ISP:n, vilket de lokala DNS-servrar som fåtts av ISP:n klarade av.

Ett annat intressant arbete är "*Economical and Political Implications of DNSSEC Deployment"* som är skrivet av A. Fant-Eldh och M. Kirvesniemi och som ger en bra inblick i hur DNSSEC fungerar samt vad den stött på för implikationer vid försök av införandet [10]. Detta arbete ger oss en bra beskrivning av DNSSEC samtidigt som den även ger en bra överblick över hur långt världen kommit i införandet av DNSSEC.

Tester på prestandan av rekursiv DNS kunde hittas i arbetet *"DNS-TEST-RESULT"* skrivet av J. Zhang, L. Ren och L. Li [15]. Testerna är utförda i laborationsmiljö i en testbädd bestående av fyra DNS-servrar varav en är rekursiv och tre är iterativa. De tre iterativa servrarna implementerar rollen som rotserver, toppdomänserver, respektive auktoritativ server. Förutom dessa DNS-servrar finns även en switch och en förfrågningsgenerator som simulerar massor med olika klienter med olika IP-adresser. Testerna utfördes med tre olika implementeringar; (1) vanlig rekursiv DNS, (2) rekursiv DNS med DNSSEC och (3) rekursiv DNS med sortlist. Det vi är intresserade av från detta arbete är resultatet från de två första implementeringarna (1) och (2). Statistik och forskningsarbete på DNS i nätverket China Mobile (Kinas största telekommunikationsföretag) föreslår att det borde vara ungefär 75-80 % DNS förfrågningar av den rekursiva DNS-servern som träffar cachen per sekund. I det här arbetet testas både den övre och lägre gränsen. Resultatet för den övre gränsen (80 %) visar att vid 30 % utnyttjande av CPU:n så utförde implementeringen med vanlig rekursiv DNS hela 19800 förfrågningar per sekund medan implementeringen med rekursiv DNS med DNSSEC endast utförde 9800 förfrågningar per sekund. Resultatet för den undre gränsen (75 %) visar att vid 30 % utnyttjande av CPU:n så utförde implementeringen med vanlig rekursiv DNS hela 18000 förfrågningar medan implementeringen med rekursiv DNS med DNSSEC endast utförde 8200 förfrågningar.

En undersökning över hur mönstret för den dagliga nätverkstrafiken ser ut kunde hittas i avhandlingen *"Locality of Internet Traffic: An analysis based upon traffic in an IP access network"* skrivet av Jie Sun [16]. Denna avhandling presenterar en slutsats om att

nätverkstrafiken är relativt liknande både på helger och vardagar. Avhandlingen visar också att det är högtrafik mellan tiderna 18.00 - 23.00 och att trafiken därefter snabbt minskar efter midnatt.

Arbetet *"Content Based Addressing: The case for multiple Internet service providers"* som är skrivet av Robert Mört presenterar en undersökning om hur innehållsdistribuerande nätverk (English: Content Distribution Networks – CDN) kan minimera mängden av nätverkstrafik mellan olika internetleverantörer [17]. Detta uppnås med hjälp av cachning av innehåll i internetleverantörernas nätverk. Undersökningen utfördes i laborationsmiljö med en testbädd implementerad med CCNx 0.6.0 (en implementering av Content-Centric Networking – CCN) och jämfört med HTTP så innehåller dessa paket en extra header vilket gör att mer information måste skickas och därför kan vi se en 16 procents reducering av prestandan vid hämtning av nya paket. Innehållet sparas därefter i cacheminnet och behöver inte hämtas igen vid förfrågning av samma innehåll och därför har det visat sig finnas en vinst i att använda CCNx istället för HTTP.

3.2 Program som använts

Det finns ett flertal olika program som kan utföra mätningar och jämför olika DNS-servrar för att på så sätt hjälpa en användare att ta reda på vilken DNS-server är bäst för just den specifika användaren. Nedan följer en beskrivning på tre olika program som vid denna avhandling använts för mätningar och analys; *(1) DNS Performance Test (DPT)* [18], *(2) namebench* [19] och *(3) Wireshark* [20].

DPT är ett simpelt och litet gratisprogram som gör det möjligt att undersöka prestandan av sin DNS-server. Med programmet följer en textfil *(domains.txt)*, som innehåller 10000 olika domännamn, som programmet använder sig av för att i slumpmässig ordning göra DNS uppslagningar ifrån. Uppslagningarna väljs slumpmässigt från listan och så fort en uppslagning är avslutad så påbörjas nästa. Programmet presenterar resultatet från en körning både i ett diagram och som en lista med statistik. Listan med statistik innehåller information såsom: antal lyckade uppslagningar, bäst uppslagningstid, sämst uppslagningstid, genomsnittlig uppslagningstid, antalet tidsgränser (som inte räknats med i statistiken), osv. Varje DNS uppslagning har fem sekunder på sig att få ett responsmeddelande och ifall inget meddelande inkommer så noterade programmet det och räknar det som en tidsgräns (English: timeout) som inte tas med i statistiken och alltså inte heller påverkar den genomsnittliga uppslagningstiden.

Programmet namebench som är utvecklat av Google Developers ger bland annat användaren möjligheten att använda sig utav webbhistorik för att avgöra vad som är bäst för just denne. Med hjälp av namebench kan många DNS uppslagningar ske på samma gång och till olika DNS-servrar. Det finns en möjlighet att själv skriva in adresserna till DNS-servrarna man vill testa eller så kan man också låta programmet inkludera både alternativa DNS-servrar och de bästa regionala DNS-servrarna som finns tillgängliga. Antingen utförs DNS uppslagningarna grundade på adresserna från webbhistoriken eller från en lista bestående av topp 2000 webbsidor som är utfärdat av *Alexa* [21].

Med hjälp av programmet Wireshark kunde nätverkstrafiken analyseras. Det finns möjlighet att ställa in olika filter om vad för paket man vill fånga upp och visa. I detta fall användes filtret för att se vad för DNS paket som färdades till och från testdator. Wireshark användes också för att se hur programmen DPT och namebench hanterade tidsgränser och fall då namnuppslagningstiden på DNS-meddelandena var väldigt långa.

4 Metod

I följande avsnitt kommer metoden för de två olika testerna att beskrivas. Först beskrivs Test A – Med DPT och sedan beskrivs Test B – Med namebench.

4.1 Test A - Med DPT

Innan mätningarna påbörjades sågs det till att DNS cachen blev rensad och därmed var tom. Eftersom mätningarna utfördes på en dator med operativsystemet Microsoft Windows, gjordes detta genom att skriva in kommandot ”ipconfig /flushdns” i kommandotolken. Därefter startades programmet Wireshark som kördes igång för att senare göra det möjligt att kunna analysera all inkommande och utgående nätverkstrafik. När dessa förberedelser var klara började själva mätningarna.

Med programmet *DNS Performance Test (DPT)* utfördes 1000 olika DNS uppslagningar som var slumpmässigt valda från en lista innehållandes 10000 stycken olika webbadresser placerade runt om i världen. Det tog cirka 12-20 minuter för programmet att utföra dessa 1000 olika DNS uppslagningarna och när detta var gjort, ändrades DNS-server till en annan. Därefter började det om från början med att rensa DNS cachen och köra igång mätningarna igen. För att utföra mätningarna med de tre olika DNS-servrarna (BBB:s DNS-server, Google Public DNS och OpenDNS) tog det ungefär en timme. Ett schema sattes upp där mätningarna pågick flera gånger varje dag under en hel vecka.

Mätningarna pågick mellan nedanstående tider och påbörjades på en måndag och avslutades på en söndag: 09.00 - 10.00, 12.00 - 13.00, 15.00 - 16.00, 18.00 - 19.00, och 21.00 - 22.00. Dessa tider valdes eftersom en så stor del av dagen som möjligt ville täckas in och det kändes därför relevant att göra mätningarna med två timmars mellanrum mellan varje omgång. För varje DNS-server så utfördes det alltså 1000 DNS uppslagningar (som pågick i cirka 15 minuter) fem gånger varje dag under en hel vecka. Mätningen av de olika DNS-servrarna utfördes i skiftande ordning. Under måndagen var det BBB:s server som testades först, därefter Google’s server och sist ut var OpenDNS. Nästa dag testades Google’s server först, OpenDNS sedan och sist BBB:s server. På detta sätt skiftades ordningen varje ny veckodag.

All information som samlats om nätverkstrafiken sparades med hjälp av Wireshark i PCAP filer som sedan exporterades till CSV filer som därmed kunde läsas och hanteras av programmet Microsoft Excel. Med hjälp av Microsoft Excel kunde mätningarna hanteras och viktig samt relevant information om DNS uppslagningar kunde tas fram.

4.2 Test B – Med namebench

Programmet namebench användes för att utföra mätningar på samma DNS-servrar som vid Test A. De tre DNS-servrarnas IP-adresser skrevs in och sedan valdes det att namnuppslagningarna skulle ske från listan bestående av topp 2000 webbsidor. Därefter ställdes det in att antalet förfrågningar till var och en av dessa servrar skulle vara 1000 stycken. Efter ett antal körningar av programmet observerades att namnuppslagningstiden minskade en hel del. Enligt Google Code [22] är det normalt att resultatet man får skiljer sig mellan de olika testerna. Detta eftersom ju fler gånger man kör programmet desto större risk blir det att man gör en förfrågning på ett namn som nyligen gjorts och på så sätt ligger kvar i någon av de närstående cacheminnena, vilket resulterar i att den DNS-server som är närmast placerad testdatorn får bäst resultat. Detta är anledningen till varför vi i resultatdelen av denna avhandling endast presenterar resultatet från första mätningen.

5 Resultat

I detta avsnitt presenteras först resultatet från Test A därefter presenteras resultatet från Test B. Figurer och diagram används för att ge en bra överblick.

5.1 Test A - Med DPT

Nedan syns tre olika tabeller som visar det genomsnittliga värdet för hur lång tid en DNS namnuppslagning tagit samt medianen och standardavvikelsen för dessa värden. Tabellerna visar en hel veckas information med fem olika tidpunkter varje dag. Första tabellen visar information om BBB:s DNS-server medan andra och tredje tabellen visar information om de alternativa DNS-servrarna *Google Public DNS* samt *OpenDNS*. Varje medelvärde är framtaget från ~1000 lyckade DNS uppslagningar och i tabellen är dessa beskrivna i millisekunder och de visas i förhållande till en angiven tidpunkt och dag.

Tabell 2: Namnuppslagningstid i millisekunder för BBB:s DNS-server

BBB	Dag 1	Dag 2	Dag 3	Dag 4	Dag 5	Dag 6	Dag 7	Median	Std
09.00 - 10.00	231	245	226	243	229	222	213	229	10,45
12.00 - 13.00	222	219	234	218	215	208	217	218	7,32
15.00 - 16.00	235	241	215	230	214	190	212	215	15,99
18.00 - 19.00	244	232	261	235	225	238	218	235	12,84
21.00 - 22.00	260	266	226	269	202	222	220	226	24,64
Median	235	241	226	235	215	222	217		
Std	12,91	15,53	15,53	17,05	9,44	16,10	3,03		

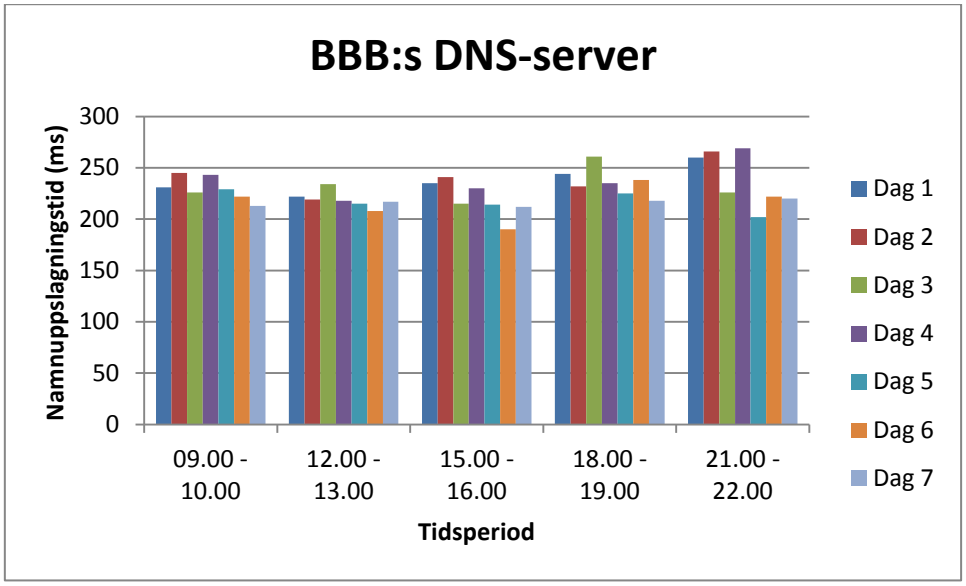
Tabell 3: Namnuppslagningstid i millisekunder för Google Public DNS

Google	Dag 1	Dag 2	Dag 3	Dag 4	Dag 5	Dag 6	Dag 7	Median	Std
09.00 - 10.00	140	140	136	135	146	159	155	140	8,67
12.00 - 13.00	132	138	125	130	127	135	149	132	7,48
15.00 - 16.00	152	136	139	133	134	141	142	139	5,97
18.00 - 19.00	149	157	148	144	145	145	151	148	4,20
21.00 - 22.00	147	139	137	171	149	135	145	145	11,26
Median	147	139	137	135	145	141	149		
Std	7,18	7,62	7,35	14,95	8,33	8,85	4,54		

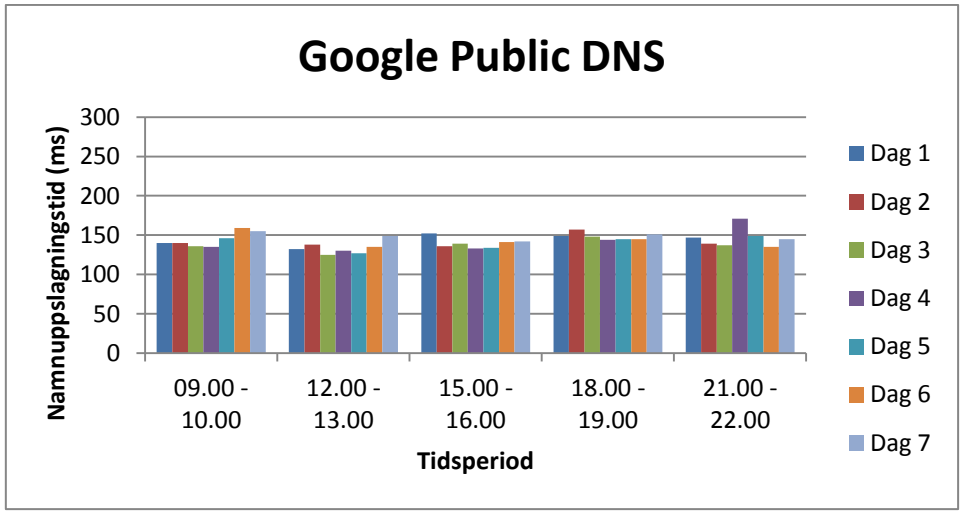
Tabell 4: Namnuppslagningstid i millisekunder för OpenDNS

OpenDNS	Dag 1	Dag 2	Dag 3	Dag 4	Dag 5	Dag 6	Dag 7	Median	Std
09.00 - 10.00	203	175	186	211	219	202	228	203	16,98
12.00 - 13.00	186	179	175	215	207	187	208	187	14,66
15.00 - 16.00	210	168	176	198	218	212	209	209	17,89
18.00 - 19.00	202	182	180	245	200	200	211	200	20,06
21.00 - 22.00	172	166	189	236	187	201	204	189	21,56
Median	202	175	180	215	207	201	209		
Std	13,76	6,16	5,49	17,12	11,92	7,96	8,32		

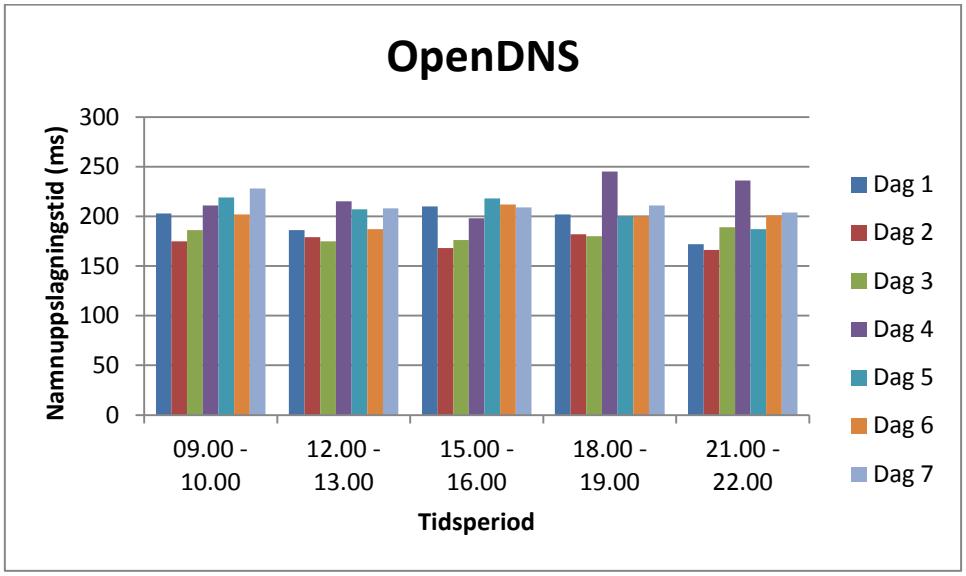
Antalet tidsgränser per ~1000 lyckade DNS namnuppslagningar för de olika DNS-servrarna (BBB, Google och OpenDNS) var i snitt 54, 56 respektive 25 stycken. Figurerna 5, 6 och 7 på nästa sida innehåller samma data som tabellerna ovan men visar inte medianen eller standardavvikelsen. Figurerna presenterar resultatet i diagramform vilket kan ge läsaren en bättre överblick över resultatet.



Figur 5: Namnuppslagningstid i millisekunder för BBB:s DNS-server



Figur 6: Namnuppslagningstid i millisekunder för Google Public DNS



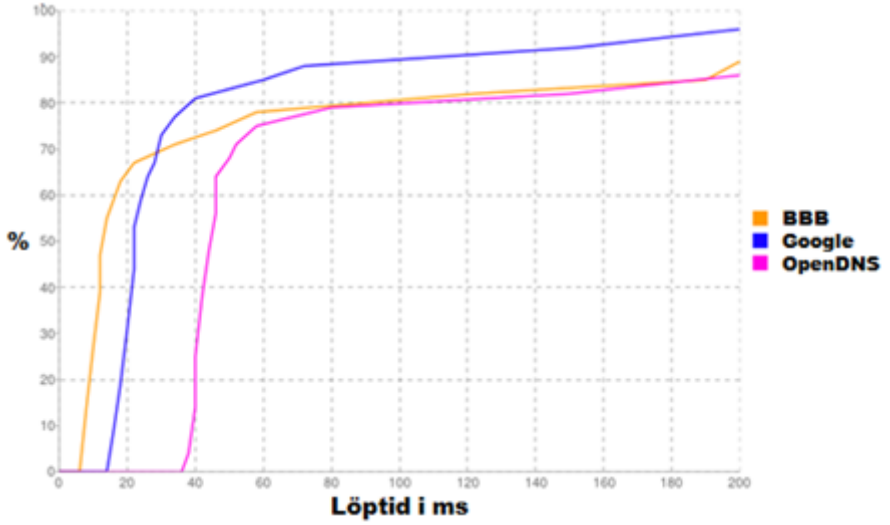
Figur 7: Namnuppslagningstid i millisekunder för OpenDNS

5.2 Test B – Med namebench

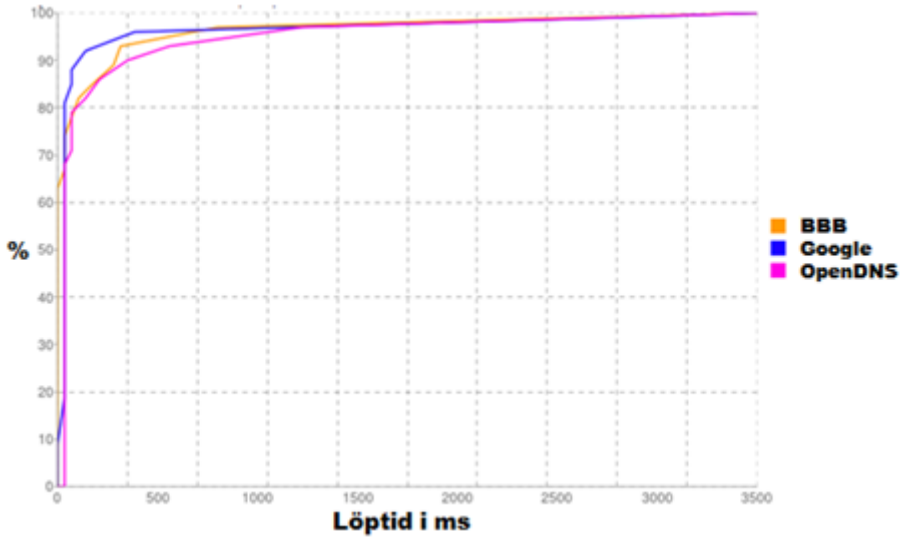
Resultatet från mätningen med namebench visas i webbläsaren där den snabbaste DNS-servern presenteras först och en rekommenderad konfiguration föreslås. Efter det visas en tabell som innehåller information av resultatet av de testade DNS-servrarna. Därefter finns det ett par diagram som visar den genomsnittlig namnuppslagningstid, den snabbaste individuella namnuppslagningstid, namnuppslagnings distributionsdiagram (över de första 200 ms), namnuppslagnings distributionsdiagram (över hela körningen). Nedan visas en tabell med information om de delar som är relevanta för denna mätning, samt de två olika distributionsdiagrammen som fåtts från körningen av programmet.

Tabell 5: Resultat från körning med programmet namebench

DNS-server	Medel (ms)	Min (ms)	Max (ms)	Tidsgränser
BBB	145	5,1	3500	18
Google	96	13,7	3500	7
OpenDNS	187	36,2	3500	14



Figur 8: Namnuppslagnings distributionsdiagram (första 200 ms)



Figur 9: Namnuppslagnings distributionsdiagram (hela körningen)

6 Analys

I det här avsnittet kommer resultatet från Test A och Test B att analyseras separat. Sedan presenteras en analys om hur DNS cache och DNSSEC påverkar DNS prestandan. Därefter presenteras både en jämförelse mellan resultatet från Test A och Test B samt en felanalys.

6.1 Test A – Med DPT

En klar skillnad finns mellan DNS-servrarna och detta presenteras bäst nedanför i Tabell 6 som visar medelvärdet av hela veckans reslutat för de olika DNS-servrarna och är en sammanställning av Tabell 2, 3 och 4 från resultatdelen. I tabellen kan man tydligt se att den genomsnittliga namnuppslagningstiden var endast 142 ms för *Google Public DNS*, medan den var 198 ms för *OpenDNS* och 228 ms för BBB:s DNS-server. *Google Public DNS* hade alltså kortast DNS uppslagningstid och fick därmed bäst resultat i testet trots att man skulle kunna tänka sig att DNS-servern som fås av ISP:n (BBB) borde vara snabbast på att utföra DNS uppslagningar, eftersom den med störst sannolikhet är fysiskt närmast placerad testdatorn och därmed även borde kunna ge ett snabbt svar. Men mätningarna visar att detta inte stämmer eftersom båda de alternativa DNS-servrarna visade sig vara snabbare än BBB:s. Standardavvikelserna för dessa tre värden är 17,62, 9,61 respektive 19,14 ms.

Tabell 6: Medelvärdet av namnuppslagningstiden hos de tre olika DNS-servrarna

BBB:s DNS-server	Google Public DNS	OpenDNS
228 ms	142 ms	198 ms

Med hjälp av *traceroute* undersöktes ifall det verkligen är så att den DNS-server som förses av ISP:n ligger fysiskt närmast till den berörda datorn. I Microsoft Windows utförs detta i kommandotolken med kommandot *tracert* följt av IP-adressen till den sökta DNS-servern. Nedan i tabell 7 syns antal hopp samt den tur och returtid (English: round trip time – RTT) i millisekunder det tar att nå de olika DNS-servrarna.

Tabell 7: Antal hopp samt RTT att nå de tre olika DNS-servrarna

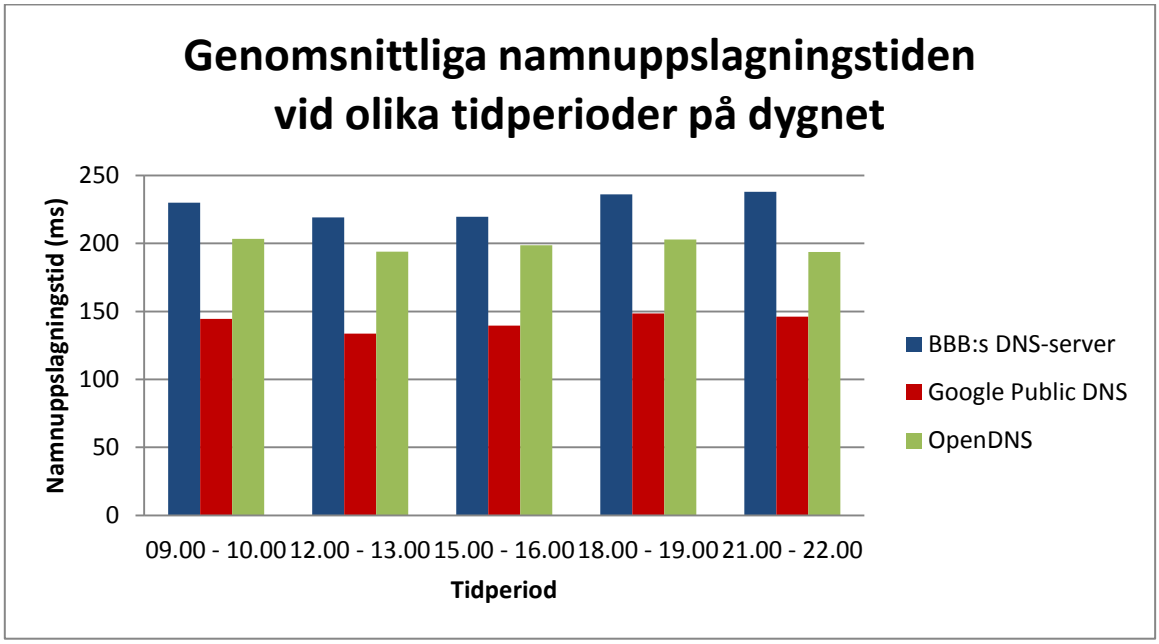
BBB:s DNS-server	Google Public DNS	OpenDNS
5 hopp, 4 ms	11 hopp, 11 ms	11 hopp, 35 ms

Precis som det antagits låg BBB:s DNS-server (som erhållits av ISP:n) fysiskt närmast den testdatorn. I Tabell 7 kan man se att den ligger endast 5 hopp ifrån testdatorn och har en RTT på 4 ms, medan de två alternativa DNS-servrarna *Google Public DNS* och *OpenDNS* båda ligger 11 hopp ifrån datorn och har en RTT på 11 respektive 35 ms. Men trots detta tog DNS uppslagningarna längst tid för BBB:s DNS-server och detta beror på att det finns ett flertal saker som har en påverkan på hur lång tid en DNS uppslagning tar och antalet hopp och RTT endast utgör en liten del av den totala uppslagningstiden (ISP:n 1,75 %, Google Public DNS 7,74 % och OpenDNS 17,68 %).

BBB har inte endast en DNS-server, utan har flera olika DNS-servrar som är placerade runt om i Sverige och dessa tar vanligtvis hand om de kunder som befinner sig närmast. Liksom BBB har även de alternativa DNS-servrarna (Google Public DNS och OpenDNS) flera olika servrar. OpenDNS har 12 stycken olika servrar eller rättare sagt 12 stycken olika datacenter som är strategiskt placerade runt om i världen [23]. Google Public DNS har över 40 olika servrar som är placerade runt om i världen [24]. Skillnaden mellan de DNS-servrar som vanligtvis fås av ISP:n och de alternativa DNS-servrarna är att hos de alternativa DNS-servrarna så är IP-adressen densamma för alla de olika servrarna medan ISP:ns har olika IP-adresser för varje server. DNS använder sig av så kallad *anycast routing* för att bestämma vilken server som ligger närmast och vart pakterna därmed ska skickas. Om vi undersöker den observerade RTT till de olika DNS-servrarna kan vi för BBB se att den hade en RTT på 4

ms och eftersom det är ett svenskt företag kan man anta att deras DNS-servrar ligger i Sverige och med tanke på den korta RTT så verkar det stämma. Den DNS-server tillhörande OpenDNS som ligger närmast Stockholm är antingen servern som är placerad i Frankfurt (Tyskland) eller den som är placerad i Amsterdam (Holland). Vilken av dessa som vi kontaktat är svårt att veta men en RTT på 36 sekunder säger oss att det är troligt att det är någon av dessa. Google Public DNS hade en RTT på 11 sekunder och här är det väldigt svårt att veta vilken av de olika servrarna som vi kontaktat eftersom det inte finns någon bra karta över de olika servrarna utan endast en lista med deras IP-adress och flygplatskod [24], men med tanke på dess RTT är mer än BBB:s och mindre än OpenDNS så antas det att servern ligger någonstans i Skandinavien.

För att få reda på hur tiden hos DNS uppslagningarna varierade vid olika tidpunkter av dygnet samt vid veckans olika veckodagar, kombinerades information från *Tabell 2 – 4* och sammanställdes i Figur 10 och Figur 11. I *Figur 10* visas de genomsnittliga DNS uppslagningstiden hos de tre olika DNS-servrarna vid olika tidperioder på dygnet. Vi kan här observera en marginell sänkning på alla tre DNS-servrar under tidsperioden 12.00 - 13.00 om man jämför med den tidigare tidsperioden. Under tidsperioden 15.00 – 16.00 är DNS uppslagningstiden ungefär samma som vid tidsperioden 12.00 – 13.00. En liten ökning för alla tre DNS-servrar syns vid tidsperioden 18.00 - 19.00 och den håller sig kvar även i sista perioden 21.00 – 22.00. De två sista tidsperioderna har alltså en förhållandevis hög DNS uppslagningstid om man jämför med de andra tidsperioderna.

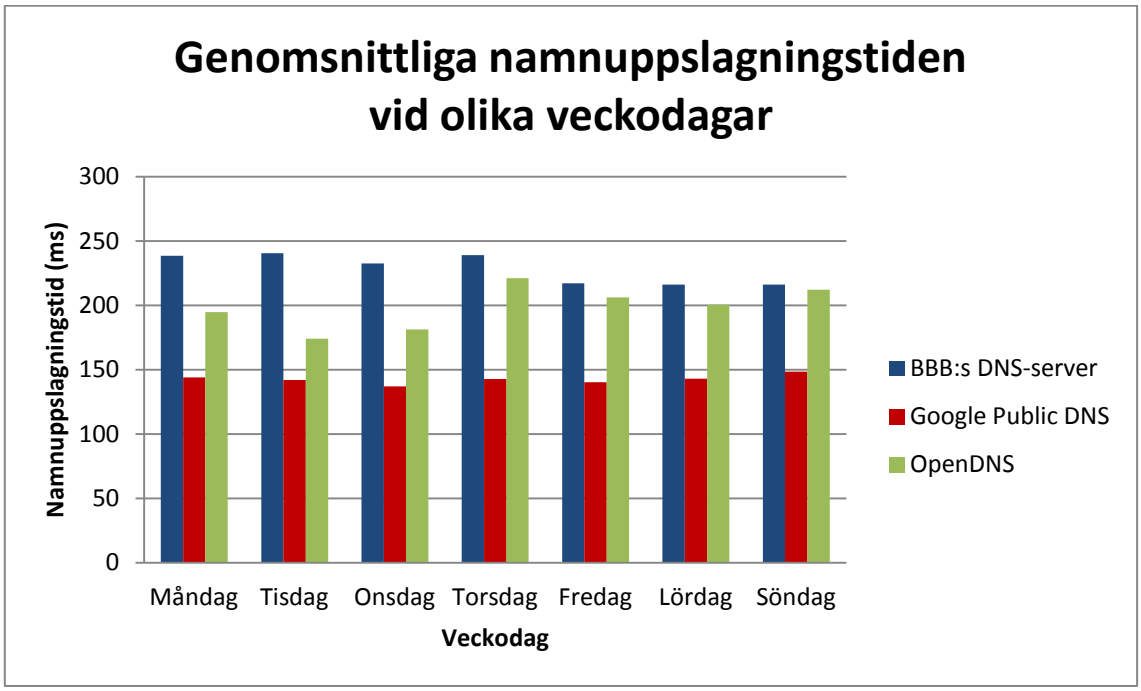


Figur 10: Genomsnittliga namnuppslagningstiden vid olika tidperioder på dygnet

Det är svårt att reflektera kring vad sänkningen under tidsperioden 12.00 – 13.00 beror på. Att det sedan var en ökning under de två sista tidsperioderna 18.00 – 19.00 och 21.00 – 22.00 kan man se ett samband till ifall man betraktar resultatet från den tidigare nämnda avhandlingen *”Locality of Internet Traffic: An analysis based upon traffic in an IP access network”* som presenterade att det var högtrafik just under dessa tidsperioder. I tabell 7 kan vi se att det krävdes 5 hopp att nå till BBB:s DNS-server och 11 hopp till de båda alternativa DNS-servrarna och detta säger oss att DNS uppslagningstiden borde påverkas av den korsande nätverkstrafiken. Ifall man betraktar antalet hopp så skulle man kunna reflektera om att de båda alternativa DNS-servrarna som är 6 hopp längre bort än BBB:s DNS-server borde därmed även påverkas mer av den korsade nätverkstrafiken och därför få en större ökning på

DNS uppslagningstiden än BBB:s DNS-server. Men Figur 10 visar att resultatet i denna avhandling inte stödjer denna reflektion, eftersom vi kan se att BBB:s namnuppslagningstid ökat mest.

Figur 11 visar den genomsnittliga DNS uppslagningstiden hos de tre olika DNS-servrarna vid olika veckodagar. Vi kan även här se att uppslagningstiderna inte varierar särskilt kraftigt vid veckans olika veckodagar, men en liten ökning förekommer under torsdagen. Det är svårt att veta vad dessa avvikelser beror på och ifall detta är ett mönster som uppkommer varje vecka eller ifall det var unikt för just den vecka mätningarna genomfördes på.



Figur 11: Genomsnittliga namnuppslagningstiden vid olika veckodagar

För ~1000 lyckade DNS namnuppslagningar var antalet observerade tidsgränser för de olika DNS-servrarna i snitt 54 stycken för BBB, 56 stycken för Google och 25 stycken för OpenDNS. Detta säger oss att OpenDNS är den server som nådde minst tidsgränser och kan därmed ses som den server som fick bäst resultat i mätningarna med avseende på tidsgränser.

6.2 Test B – Med namebench

Resultatet från mätningen med namebench visar också att Google Public DNS är den snabbaste DNS-servern om man jämför med OpenDNS och BBB:s DNS-server. Google hade en genomsnittlig DNS uppslagningstid på 96 ms medan BBB hade 145 ms och OpenDNS hade 187 ms. Snabbast individuella DNS uppslagningstid hade BBB vilket var precis som förväntat eftersom det är den DNS-server som fåtts av vår ISP och är även den DNS-server som ligger närmast vår testdator. Den snabbaste individuella DNS uppslagningstiden för BBB låg på 5,1 ms medan den för Google och OpenDNS låg på 13,7 respektive 36,2 ms.

På Figur 8 och Figur 9 på sida 15 visas hur stor andel av namnuppslagningarna från de olika DNS-servrarna var fördelade med avseende på löptiden. Figur 8 visar de första 200 ms från hela mätningen och här kan vi se att BBB står för störst del av namnuppslagningar fram tills cirka 28 ms av löptiden har passerat, därefter är det Google Public DNS som står för störst andel av namnuppslagningar fram till slutet av de första 200 ms. OpenDNS som hade högst individuella namnuppslagningstid kan vi precis som förväntat se att den startar sist i diagrammet och vi kan även se att dess graf i diagrammet efter cirka 80 ms av löptiden hamnar på samma nivå som BBB:s och ligger på ungefär samma nivå som BBB fram tills

cirka 193 ms av löptiden, då vi kan se att BBB gör en liten ökning. På Figur 9 som är en fortsättning av Figur 8 kan vi se att BBB:s graf går ihop med den från Google vid ungefär 650 ms av den totala löptiden. Därefter vid cirka 1200 ms av den totala löptiden ansluter sig även OpenDNS graf till de andra och ligger på samma nivå som de andra fram till slutet av mätningen.

Antalet uppnådda tidsgränser vid en mätning med 1000 namnuppslagningar var för BBB 18 stycken, för Google Public DNS 7 stycken och för OpenDNS 14 stycken. Google Public DNS nådde därmed minst antal tidsgränser samtidigt som den hade överlägset bäst medeltid på namnuppslagningarna samt bäst individuell uppslagningstid. Google Public DNS kan därför överlägset ses som den mest passande DNS-servern med hänsyn till testet som gjorts med namebench.

6.3 DNS cache och DNSSEC

DNS cache lagring finns beskrivet i avsnitt 2.5 och som tidigare nämnts så är det en teknik som medför att DNS uppslagningstiderna kraftigt minskar. DNS cache lagring är idag brett använt och i mätningarna som utförts har flera av namnuppslagningarna varit cache lagrade i någon av de mellanliggande DNS-servrarna men på grund av DNS transparens är det svårt att kontrollera och styra vad som finns i de olika DNS-servrarna. Hur mycket uppslagningstiderna minskar med på grund DNS cache lagring varierar från fall till fall men en uppfattning kan fås om vi till exempel granskar namnuppslagningstiden för BBB i Test B med namebench. Snabbast individuella namnuppslagningstid som observerades var 5,1 ms medan den längsta var 3500 ms. Med tanke på att snabbaste namnuppslagningstiden endast var 5,1 ms och BBB:s DNS-servern hade en RTT på 4 ms så kan vi anta att denna post måste varit cache lagrad i denna DNS-server, till skillnad från den längsta observerade namnuppslagningstiden som var 3500 ms och som vi kan anta inte var cache lagrad. Utifrån detta kan vi dra slutsatsen att cache lagringstekniken kan bidra med flera sekunders förbättring av namnuppslagningstiden.

DNSSEC finns beskrivet i avsnitt 2.8 och som det nämnts tidigare så är detta en säkerhetsutvidgning av DNS med syfte att täppa igen DNS sårbarheter genom att skapa integritet och autentisering av information som sänds mellan klienter och de olika DNS-servrarna. Det har även påpekats att DNSSEC medför en fördröjning av den upplevda väntetiden som det tar för att utföra en adressöversättning. Exakt hur mycket DNSSEC påverkar den verkliga DNS prestandan är svårt att spekulera kring. En granskning av resultatet som presenteras i arbetet ”DNS-TEST-RESULT” som grundar sig på en testbädd visar skillnaden mellan hur många förfrågningar per sekund som utfördes med vanlig rekursiv DNS respektive rekursiv DNS med DNSSEC. Resultatet visar att för både den övre och undre gränsen så var antalet förfrågningar per sekund ungefär dubbelt så många för vanlig rekursiv DNS jämfört med rekursiv DNS med DNSSEC. Detta bevisar att DNSSEC har en stor negativ inverkan på DNS prestandan om man granskar adressöversättningstiden.

6.4 Jämförelse mellan Test A och Test B samt felanalys

Det observerades att testet med namebench gav märkbart kortare genomsnittliga DNS uppslagningstider. Anledningen till detta är att testet med DPT väntar på ett responsmeddelande i 5 sekunder innan den hanterar meddelandet som en tidsgräns, till skillnad från namebench som endast väntar i 3,5 sekunder. Längden för hur länge ett program väntar på ett responsmeddelande har alltså en stor påverkan på den genomsnittliga DNS uppslagningstiden som presenteras.

En annan stor skillnad från mätningarna med DPT är att BBB i fallet med namebench var betydligt snabbare än vad den var i fallet med DPT. En anledning som det kan bero på är den

stora skillnaden på vilken period de olika testerna utfördes på. Test A utfördes under hela vecka 33 (mellan datumen 13 – 19 augusti) år 2012 och Test B utfördes 27 december 2012.

Antalet tidsgränser skiljde sig också mycket mellan de olika testerna. Med tanke på att namebench endast väntade i 3,5 sekunder till skillnad från DPT som väntade i 5 sekunder på ett responsmeddelande, skulle man kunna tro att antalet tidsgränser för namebench skulle vara betydligt fler än vad det var för DPT. Men det observerade resultatet visade något helt annat. Antalet nådda tidgränser var istället cirka en tredjedel för namebench än vad det var för DPT. Vad detta oväntade resultat beror på är svårt att spekulera omkring, men en gissnings skulle kunna vara att även detta beror på den stora skillnaden på vilken period de olika testerna utfördes på.

En stor skillnad mellan hur de olika programmen utför namnuppslagningarna observerades. Med DPT skedde namnuppslagningarna en efter en och inte parallellt som de gjorde med namebench. Det visade sig vara ineffektivt att utföra namnuppslagningarna en efter en och mycket tid hade kunnat sparas ifall de skett parallellt istället. Det är möjligt att detta även kunnat påverka resultatet eftersom vid varje mätningsomgång med DPT så började en mätning cirka 40 minuter innan den tredje DNS-servern testades. Val av testprogram är därför viktigt och borde tänkas igenom innan testerna startas.

Att i testet med DPT utföra mätningarna utifrån cirka 1000 slumpmässigt valda adresser från en större lista istället för att använda samma uppsättning av adresser för var och en av mätningarna, kan man ifrågasätta ifall det verkligen var den mest optimala metoden för denna typ av undersökning. Anledningen till varför just denna metod användes var för att ju fler slumpmässiga adresser som används desto närmare kommer man ett verklighetsbaserat värde och en varierande uppsättning av adresser användes eftersom det skulle minska risken för att fler adresser hamnar i cacheminnet och på så sätt påverkar resultatet.

7 Slutsats

I det här avsnittet kommer en slutsats att presenteras, sedan kommer det att ges förslag på eventuella framtida forskningar inom ämnet och därefter avslutas allt med lite obligatoriska reflektioner.

7.1 Slutsats

Den här undersökningen visar att vid jämförandet av den DNS-server som fås av ISP:n (BBB) och de två största alternativa DNS-servrarna (Google Public DNS och OpenDNS) så är det Google Public DNS som fått bäst resultat och borde vara det självklara valet av DNS-server för just denna dator. Huruvida det är för andra nätverksanvändare är ingenting som man kan uttala sig om efter enbart denna undersökning. Istället rekommenderas det att varje användare som vill utvärdera vilken DNS-server som är bäst för just denne, borde göra en egen undersökning från den berörda datorn. Detta eftersom resultatet från undersökningarna är väldigt beroende på den ISP man är ansluten till samt den plats man befinner sig på.

Det finns massor med olika verktyg och program tillgängligt gratis på internet som kan hjälpa en vardaglig nätverksanvändare att ta reda på vilken DNS-server är bäst för just denne. Exempel på ett bra och enkelt sådant är namebench som på enbart ett fåtal minuter kan hjälpa en användare att få reda på vilka olika DNS-servrar som finns tillgängliga och vilken av dessa som är bäst för just den specifika användaren.

Någonting som man kan undra över är varför DNS-servrar som fås av ISP:n egentligen finns kvar och varför de inte ersatts helt av de alternativa DNS-servrarna som i många fall visat sig ha en bättre prestanda. Anledningen till detta är främst att de som fås av ISP:n oftast ligger fysiskt närmare än de alternativa DNS-servrarna och ger därför snabbast svar ifall det handlar om en förfrågning som redan finns i serverns cacheminne. Sedan är det också så att de som har samma ISP också ofta besöker liknande webbsidor och därmed ökar chansen till att en webbsida man vill besöka redan finns i cacheminnet och kan fås direkt utan att kontakta de andra DNS-servrarna som finns i hierarkin. Storleken på både ISP:n och cacheminnet har också en betydelse för hur effektiv en DNS-server är. Ifall till exempel en stor ISP med många anslutna användare har ett litet cacheminne som inte rymmer många poster, så kommer cacheminnet ofta att uppdateras och poster som skulle behövas kan försvinna.

Någonting som borde tänkas på vid val av DNS-server är att trots att en DNS-server får bra resultat vid test av DNS prestandan, behöver det inte alltid betyda att denna DNS-server som ger bäst slutresultat för användaren ifall man tittar på nätverksanvändandet. Detta eftersom själva nätverksanvändandet i sig beror på flera faktorer som bland annat diskuterats i inledningen. Exempel på ett problem som kan uppstå vid val av en alternativ DNS-server istället för den som fås av ISP:n är att vid användning av CDN så kan det vara svårt att veta vart värddatorn är placerad. Det kan därmed bli så att innehåll färdas en onödigt lång väg i nätverket eftersom den hämtas från en server som ligger långt bort från värddatorn istället för någon närliggande server som har samma innehåll. Detta kan medföra att väntetiden som slutanvändaren upplever ökar istället för minskar fast DNS uppslagningen går fortare.

Cache lagringstekniken har en stor betydelse för DNS prestandan och som det framgår i analysdelen av denna avhandling, kan cache lagringstekniken bidra med flera sekunder kortare namnuppslagningstid. DNSSEC är en behövande säkerhetsutvidgning av DNS men anledningen till att DNS inte helt bytts ut helt till DNSSEC är att det fortfarande finns brister i DNSSEC och en viktig sådan är dess negativa inverkan på DNS prestandan som vi kan se i avsnitt 6.4.

7.2 Framtida forskning

Utifrån de mätningar som gjorts i denna avhandling är det svårt att dra någon slutsats angående hur DNS prestandan förändras vid olika tidpunkter och veckodagar. Förslag på framtida forskning är att ungefär liknande mätningar som denna avhandlig behandlat borde göras i en större utsträckning och gärna med mätningar under även nattiden. För att detta ska göras på ett effektivt sätt rekommenderas att ett skript skapas som automatiskt utför mätningar i regelbundna tider och håller på i flera veckor eller månader med att utföra mätningar och samla information om flera olika DNS-servrar. Om detta görs skulle mer data samlats och det skulle kunna utredas ifall det är någon skillnad på DNS prestandan vid olika tidpunkter på dygnet samt vid olika veckodagar.

Vid användning av en alternativ DNS-server har det tidigare påpekats i denna avhandling att det kan vara svårt att då CDN används veta vilken server som är närmast och därmed finns det en risk att innehåll hämtas från en server placerad längre bort än nödvändigt. Detta gäller inte bara då CDN används utan kan gälla för vilken webbserver som helst. En undersökning som skulle kunna göras är att ta reda på hur stor skillnad det i verkligheten kan bli på tiden det tar att hämta ett visst innehåll från en server vid användning av en alternativ DNS-server istället för den som fås utav ISP:n.

7.3 Obligatoriska reflektioner

Denna avhandling utreder DNS prestandan och hjälper oss vardagliga nätverksanvändare att få en större inblick i hur DNS egentligen fungerar och vilka olika alternativ som finns tillgängliga för oss för att effektivisera vår DNS prestanda. I följd av att DNS prestandan effektiviseras kommer även den upplevda nätverksanvändningen av slutanvändaren att effektiviseras. Den tid miljontals människor här i Sverige bara sitter framför datorn och väntar på att en DNS uppslagning ska ske, kan därmed förkortas och användas för att göra någon nytta istället för att bara sitta och vänta på att DNS uppslagningen ska bli färdig.

En ökad insikt i hur DNS fungerar leder till att vardagliga nätverksanvändare själva kan avgöra vad som är bäst för just denna istället för att automatiskt acceptera den DNS-server som fås av deras ISP. Det kan bli så att användare bestämmer sig för att välja en viss ISP bara för att de vet att de har en bättre DNS-server. Ifall olika företag och ISP känner till detta kan det leda till att de anstränger sig mer för att utveckla sina DNS-servrar vilket i sin tur leder till att bättre DNS-servrar utvecklas och fler alternativ dyker upp.

Litteraturförteckning

[1] P. Mockapetris, ”Domain Names - Implementation and Specification,” RFC 1035, Internet Engineering Task Force, November 1987.

[2] P. Mockapetris, ”Domain Names - Concepts and Facilities,” RFC 1034, Internet Engineering Task Force, November 1987.

[3] J. F. Kurose och K. W. Ross, Computer Networking: A Top-Down Approach, USA. Upper Saddle River: Pearson Education, 2009, pp. 158-172.

[4] T. Daly, ”The Impact Of DNS Round Trips On Website Performance,” Dyn, 6 Mars 2012. [Online]. Available: http://dyn.com/the-impact-of-dns-round-trips-on-website-performance/. [Använd 19 September 2012].

[5] Google Developers, ”Public DNS: Performance,” 19 April 2012. [Online]. Available: http://code.google.com/speed/public-dns/docs/performance.html. [Använd 23 Maj 2012].

[6] Google Developers, ”Security Benefits,” 28 Mars 2012. [Online]. Available: https://developers.google.com/speed/public-dns/docs/security?hl=sv-SE. [Använd 22 Maj 2012].

[7] R. Arends, R. Austein, M. Larson, D. Massey och S. Rose, ”DNS Security Introduction and Requirements,” RFC 4033, Internet Engineering Task Force, March 2005.

[8] DNSSEC @ ICANN, ”Signing the root zone: A way forward toward operational readiness,” 15 July 2008. [Online]. Available: http://www.icann.org/en/announcements/dnssec-paper-15jul08-en.pdf. [Använd 22 05 2012].

[9] ICANN & VeriSign Inc, ”Enhancements to DNSSEC validation for the DNS Root Zone change requests,” 16 July 2010. [Online]. Available: http://www.root-dnssec.org/2011/01/27/rrsig-checking/. [Använd 22 Maj 2012].

[10] A. Fant-Eldh och M. Kirvesniemi, ”Economical and Political Implications of DNSSEC Deployment,” Kungliga Tekniska Högskolan, Stockholm, Sverige, 2010.

[11] Google Developers, ”Public DNS,” [Online]. Available: https://developers.google.com/speed/public-dns/. [Använd 23 Maj 2012].

[12] OpenDNS, ”OpenDNS vs. Google Public DNS,” [Online]. Available: http://www.opendns.com/technology/opendns-vs-google-public-dns/. [Använd 23 Maj 2012].

[13] D. Strom, ”Improve Network Security with DNS Servers,” eSecurity Planet: Internet security for IT pros, 10 February 2010. [Online]. Available:

http://www.esecurityplanet.com/views/article.php/3864181/Improve-Network-Security-with-DNS-Servers.htm. [Använd 12 December 2012].

[14] Bernhard Ager, Wolfgang Mühlbauer, Georgios Smaragdakis, och Steve Uhlig, ”Comparing DNS Resolvers in the Wild,” Proceeding IMC ’10 Proceedings of the 10th annual conference on Internet measurement, 2010, pp. 15–21, DOI:10.1145/1879141.1879144, [Online]. Available: http://portal.acm.org/citation.cfm?doid=1879141.1879144.

[15] J. Zhang, L. Ren och L. Li, ”DNS-Test-Result,” Internet-Draft, Internet Engineering Task Force, draft-zhang-dnsext-test-result-00, March 2012, Expires: September 2, 2012.

[16] J. Sun, ”Locality of Internet Traffic: An analysis based upon traffic in an IP access network,” School of Information and Communication Technology, KTH Royal Institute of Technology, Stockholm, Sweden, 2012.

[17] R. Mört, ”Content Based Addressing: The case for multiple Internet service providers,” School of Information and Communication Technology, KTH Royal Institute of Technology, Stockholm, Sweden, 2012.

[18] ”Silverwolf Software,” [Online]. Available: http://swmirror.zapto.org/cms/index.php/software-download/dns-performance-test/. [Använd 15 September 2012].

[19] Google Developers, ”namebench: Open-source DNS Benchmark Utility,” [Online]. Available: http://code.google.com/p/namebench/. [Använd 12 December 2012].

[20] ”Wireshark · Go deep.,” [Online]. Available: http://www.wireshark.org/. [Använd 18 September 2012].

[21] ”Alexa: The Web Information Company,” [Online]. Available: http://www.alexa.com/.

[22] ”namebench: FAQ,” Google Code, [Online]. Available: http://code.google.com/p/namebench/wiki/FAQ. [Använd 28 12 2012].

[23] OpenDNS, ”OpenDNS: Premium DNS,” [Online]. Available: http://www.opendns.com/business-solutions/premium-dns/benefits. [Använd 28 12 2012].

[24] Google Developers, ”Google Developers: FAQ,” [Online]. Available: https://developers.google.com/speed/public-dns/faq#locations. [Använd 28 12 2012].

TRITA-ICT-EX-2013:2

www.kth.se