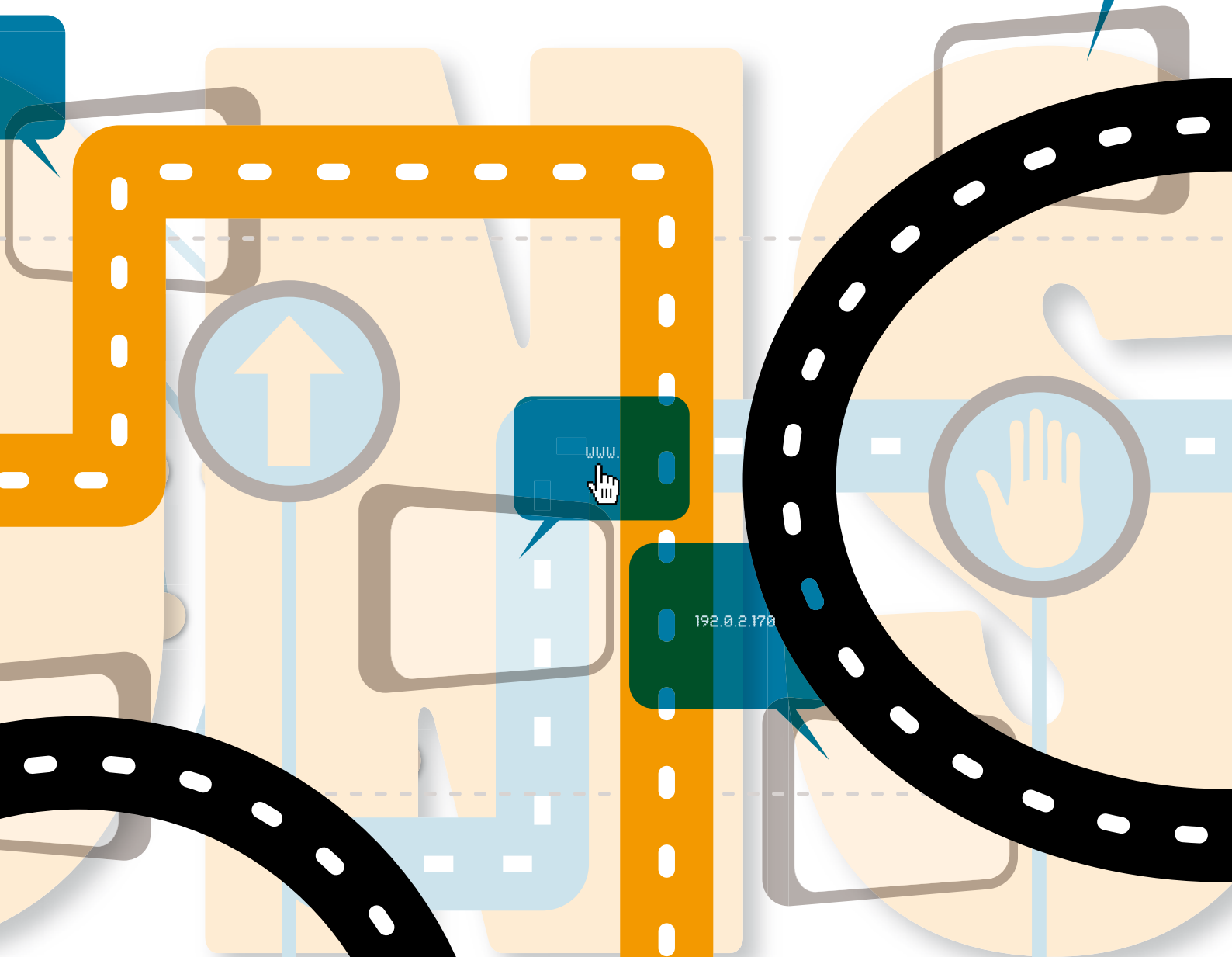
Björn Raunio

DNS – Internets vägvisare

Tekniken som leder dig rätt på nätet



DNS – Internets vägvisare

.SE:s Internetguide, nr 12
Version 1.0 2009

Författare: Björn Raunio
Redaktör: Lennart Bonnevier
Formgivning, layout och redigering: Gunnel Olausson/FGO AB
Illustrationer: © Camilla Laghammar
Tryck: Livonia Print, Riga, maj 2009
ISBN: 978-91-977908-7-1

.SE (Stiftelsen för Internetinfrastruktur) ansvarar för Internets svenska toppdomän. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige.

Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00
Fax: +46 8 452 35 02
E-post: info@iis.se
Organisationsnummer: 802405-0190
www.iis.se

Förord

Om någon nu tror det, så ska jag redan från början slå fast att författaren till guiden du håller i din hand (eller läser på din skärm) inte är någon tekniker. Innan jag för drygt ett år sedan började hjälpa .SE att ta fram texter av olika slag hade jag bara en vag idé om vad DNS var och hur det funkade. Å andra sidan är tanken med den här guiden just att berätta om domännamnssystemet ur en icke-teknikers synvinkel, så därför var jag en lämplig kandidat att skriva den.

Under arbetet med denna guide har jag dock lärt mig en del om DNS och jag hoppas att det visar sig vara tillräckligt för att kunna förklara det på ett bra sätt för dig som läsare. Det som fascinerar mig mest med detta ämne är nog att Internet är ett sådant tydligt exempel på att decentralisering och ansvarsfördelning kan fungera mycket väl, även om det finns ett inneboende dilemma i att det distribuerade ansvaret också tycks ge upphov till de hot som finns mot Internetinfrastrukturen.

När jag berättat för kollegor och bekanta att jag jobbar med en guide om DNS har en vanlig reaktion varit att det knappast kan bli någon kioskvältare. Men jag hoppas ändå att denna Internetguide kan finna sin publik. Med tanke på att Internet har blivit en så viktig och naturlig del av vår vardag borde vi bli fler som har ett hum om hur det egentligen funkar. Förhoppningsvis kan jag bidra något lite till att sprida denna förståelse!

De skriftliga källor som jag har använt mig av under arbetet med denna guide är PTS-dokumentet *Beskrivning av infrastrukturen för Internet i Sverige*, boken *DNS and Bind* av Paul Albitz & Cricket Liu (Förlag: O'Reilly, 2006), webbplatsen http://www.dnssec.net, skriften *Introduktion till DNS* av Erik Geijer, boken *Pro DNS and BIND* av Ronald Aitchison tillgänglig på www.zytrax.com samt Wikipedia på www.wikipedia.org.

Stockholm i maj 2009
Björn Raunio

Hjälp oss att förbättra
Om du hittat fel eller har synpunkter på denna guide kan du sända dem till publikationer@iis.se

Inledning

I dag har Internet blivit en självklarhet i de flesta svenskars liv. Vi använder det både privat, i skolan och i arbetslivet, från fasta nät och mobila. Tack vare Internet har vi vant oss vid att ständigt ha tillgång till en uppsjö av information, underhållning och tjänster av alla möjliga slag. Många av oss lever också delar av vårt sociala liv med hjälp av nätet, i synnerhet de yngre.

En hel del av dem som glatt använder Internet till både det ena och det andra har aldrig ens reflekterat över vad som egentligen händer när de har skrivit in en adress i sin webbläsare och tryckt ned Enter-tangenten. Eller hur ett e-postmeddelande kan nå den tilltänkta mottagaren. Nätet har blivit något vi tar för givet, som bara funkar, så där alldeles av sig själv.

I själva verket är det ju inte så. Det finns en hel infrastruktur på plats bakom kulisserna och den måste fungera som tänkt för att du ska kunna surfa in på en webbplats eller skicka ett mejl. Den här guiden handlar om en av de mer grundläggande delarna av denna infrastruktur: den hierarkiska och distribuerade databasen DNS (förkortning för domännamnssystemet). Idén här är att försöka förklara vad detta är för något och hur det fungerar, helt enkelt lyfta lite på kulisserna och försöka svara på vad som egentligen händer där bakom, utan att grotta ned oss för mycket i de tekniska detaljerna.

Med tanke på det samhälle som har växt fram under de senaste 15 åren, där mer och mer kommunikation, handel och affärer sker på eller med hjälp av Internet, är det nyttigt om fler av oss får ett hum om den infrastruktur som är själva grunden för nätet. Internetinfrastrukturen blir en alltmer vital del av hela samhällsstrukturen. I dag skulle väldigt lite bli gjort i Sverige om .se-domänen plötsligt slutade fungera och inga webb- eller e-postadresser som slutar på .se längre gick att nå. Därför kan det ur ett rent allmänbildningsperspektiv vara nyttigt att förstå i varje fall lite grann kring hur det fungerar.

Som redan nämnts är DNS en hierarkisk och distribuerad data-

bas. Redan vid dessa ord kanske många läsare skyggar tillbaka och tycker att det blir för krångligt. Känner du så, bör du ändå inte sluta läsa redan nu. Exakt vad detta begrepp innebär kommer att förklaras längre fram. Att vi beskriver DNS på just detta sätt beror på att det lyfter fram de nyckelegenskaper som har gjort Internet till en sådan framgångssaga med global spridning.

Den hierarkiska strukturen innebär att nätverket inte slutar att fungera bara för att det finns problem på en lägre belägen nivå, vilket gör Internetinfrastrukturen mycket robust. Det kan liknas vid ett träd, där det inte spelar någon roll för trädets livskraft i sin helhet om några kvistar längst ut bryts av, eller till och med om hela grenar försvinner.

Det distribuerade ansvaret för domänerna inom DNS har å sin sida gjort Internets enorma spridning möjlig. I och med att var och en ansvarar för sin beskärda del av DNS finns väldigt få inbyggda administrativa begränsningar för nätverkets spridning.

När DNS skapades 1984 var det just för att råda bot på de administrativa problem som Internets föregångare Arpanet drogs med. Nätverket hade helt enkelt blivit för stort för att kunna hanteras centralt på ett smidigt sätt. Den hierarkiska och distribuerade strukturen var en genialisk lösning på problemet som öppnade vägen för den fenomenala utveckling som Internet sedan fick.

Innan vi går in på hur DNS är uppbyggt och fungerar ska vi dock titta på något som kan sägas vara ännu mer grundläggande för Internet, nämligen datakommunikationen.

Datakommunikationen på Internet

- Vi behöver IP-adresser för att kunna identifiera varje dator på nätet och för att e-post och annan datatrafik ska hitta rätt.
- Domännamnen har kommit till för att vi lättare ska komma ihåg adressen, IP-adressens alla siffror kan vara svåra att memorera.

I grund och botten är Internet ett jättelikt nätverk som kopplar samman en enorm mängd datorer så att de kan kommunicera med varandra. För att denna kommunikation ska fungera så måste datorerna använda samma uppsättning regler när de skickar och tar emot information. Dessa regelverk kallas protokoll och det mest grundläggande protokollet som används på Internet kallas Internetprotokollet och förkortas IP.

Som namnet antyder så skapades Internetprotokollet för att nätverk av olika typ skulle kunna kommunicera med varandra (jämför ordet Internet med till exempel internationell, interregional eller interplanetär). I dag används dock IP i väldigt många lokala nätverk likaväl som för kommunikationen dem emellan över Internet.

När information skickas med hjälp av IP, så bryts den ned i små beståndsdelar som kallas IP-paket. IP-paketens information delas upp i ett antal skikt. Den information som ska överföras ”kapslas in” och är oväsentlig i själva dataöverföringen. Här är det i stället bara informationen om vilken dator som har skickat paketet och vilken dator som ska ta emot det som spelar roll. Baserat på denna information transporteras IP-paketen från en punkt i nätverket till en annan.

IP-adressen leder rätt

Det som gör att IP-paketen kan hitta fram till rätt dator är att alla datorer som är uppkopplade på Internet har en så kallad IP-adress.

Det är en unik nummerserie som identifierar datorn i nätverket, ungefär på samma sätt som alla telefoner har ett eget nummer i telenätet.

I den version av IP som har använts mest fram till i dag, IPv4, består adressen av 32 bitar (det vill säga ettor och nollor) eller 4 byte (1 byte = 8 bit). Vanligtvis skriver man ut de fyra byten i decimal form med punkter emellan, där varje siffergrupp (som kan bestå av numren 0–255) motsvarar en byte, så här:

192.0.2.170

Med IPv4 är antalet möjliga IP-adresser på Internet begränsat. När antalet Internetanslutna datorer ökade explosionsartat under 1990-talet utvecklades därför olika tekniker som gör det möjligt för flera datorer att dela på samma IP-adress när de ansluter till Internet. På så vis behöver inte varenda dator ha en världsunik IP-adress. Den IP-adress som en dator använder på Internet skiftar därför i många fall över tiden.

Inom de närmaste åren beräknas dock adressbristen trots allt bli så akut att det blir nödvändigt att inleda ett skifte till en ny version av IP, IPv6 (vilket du kan läsa mer om i kapitlet IPv6 och DNS). I denna version består en IP-adress av 128 bitar och är alltså avsevärt mycket längre än IPv4-adressen ovan. Denna övergång kan komma att göra tekniken där man delar på samma IP-adress onödig.

Varför finns domännamn?

Kommunikationen över Internet sker alltså med hjälp av unika IP-adresser. Vad behöver vi då domännamnen till? Är det inte bara att använda adresserna? Det hade nog funkat fint om det bara vore datorer inblandade. Men domännamnen är ett hjälpmedel för oss människor, som har mycket lättare för att lägga ord och namn på minnet än långa nummerserier.

Det kan vara svårt nog att hålla några få telefonnummer, kort- och portkoder i huvudet, tänk dig då att försöka komma ihåg långa

nummer för alla webbplatser du vill gå in på eller alla e-postadresser du vill e-posta till! Domännamnssystemet DNS har helt enkelt skapats för att översätta IP-adresserna till namn som vi människor enkelt kan komma ihåg. Likt en telefonkatalog som översätter namn till telefonnummer så är databasen DNS en katalogtjänst som (bland annat) översätter domännamn till IP-adresser. Tack vare DNS kan IP-paketen skickas rätt när vi e-postar och surfar utan att vi behöver lära oss några otympliga nummerserier. Och dessutom gör DNS att man inte behöver byta webb- eller e-postadress bara för att en server byter IP-adress.

”Domännamnssystemet DNS har helt enkelt skapats för att översätta IP-adresserna till namn som vi människor enkelt kan komma ihåg.”

Så fungerar DNS

DNS är en hierarkisk databas vilket innebär att informationen är lagrad i en trädstruktur, som gör att det går snabbt att hitta fram till den information som man är intresserad av.

I detta kapitel får du bland annat veta hur strukturen är uppbyggd, och hur den delas upp i domäner, underdomäner, zoner, etcetera.

Vi har tidigare slagit fast att DNS är en hierarkisk och distribuerad databas, men vad betyder egentligen detta?

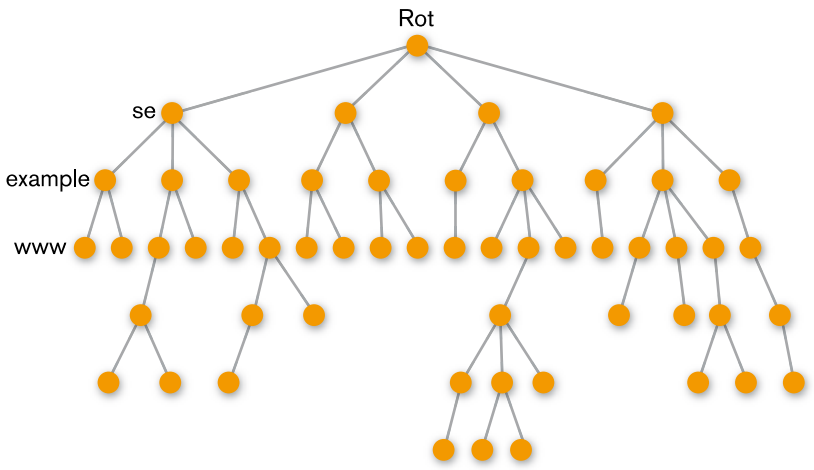
För den som inte vet vad en databas är, så är det helt enkelt en samling information – eller data – som är organiserad så att det, med hjälp av rätt programvara, är lätt att hitta och hämta enskilda delar av informationen. I fallet med DNS är systemet uppbyggt så att det ska gå snabbt att få fram vilken IP-adress som är kopplad till ett visst domännamn med hjälp av program som kallas namnservrar. (Det finns även annan information än IP-adressen kopplad till ett domännamn, men för tydlighetens skull begränsar vi oss här till att tala om IP-adressen.)

Att DNS är en hierarkisk databas innebär att informationen är lagrad i en trädstruktur, vilket gör att det går snabbt att hitta fram till den information som man är intresserad av. Och att databasen är distribuerad betyder att informationen är utspridd på många olika datorer som är sammankopplade i ett nätverk, i det här fallet på servrar som finns spridda över hela Internet. Båda dessa egenskaper gör det möjligt att fördela ansvaret för olika delar av databasen på olika händer. På så vis förblir systemet stabilt och robust i sin helhet även om problem uppstår i någon enskild del av databasen.

DNS-trädet

För att förklara hur informationen är organiserad i DNS liknar man alltså systemet vid ett träd som förgrenar sig från roten. Till skill-

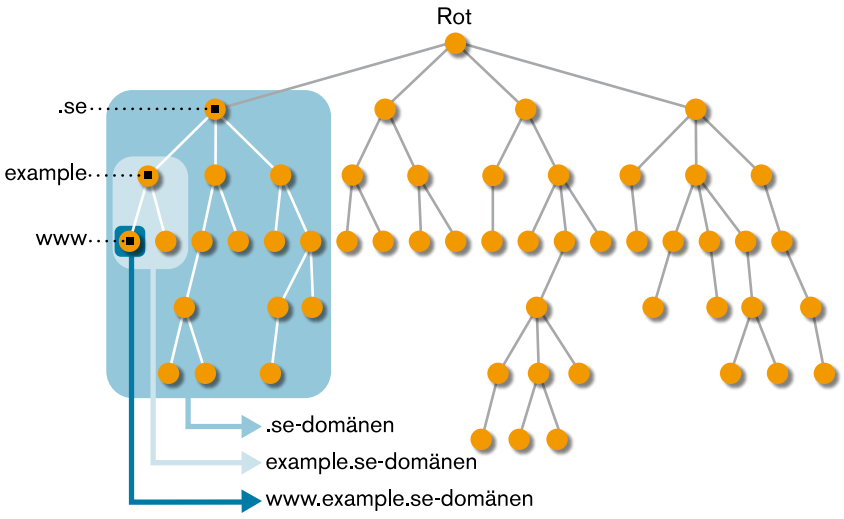
nad från ett riktigt träd brukar roten dock sättas högst upp i DNS-trädet.



Figur 1. Trädstrukturen i DNS.

Ett domännamn är helt enkelt en märkning som pekar ut var i trädstrukturen det går att hitta informationen om vilken IP-adress som är kopplad till det. Varje nod i trädstrukturen kan anges med ett domännamn. Noden längst ut till vänster i figur 1 härintill benämns till exempel med domännamnet *www.example.se*, där punkterna skiljer åt namnen på de noder som passeras på vägen upp till trädets rot. Roten hamnar alltid sist i domännamnet och får inte någon egen benämning. På detta vis skapas en sökväg som leder rätt i trädet.

En domän är en delmängd av hela DNS-trädet och ett domännamn är detsamma som benämningen på noden i toppen av en domän. Domänen kan därför ingå i en annan domän. Till exempel är domänen *www.example.se* en del av domänen *example.se*, vilken i sin tur är en del av domänen *.se*. Man säger att *www.example.se* är en underdomän till *example.se* och denna i sin tur är en underdomän till *.se*-domänen (se figur 2). Det maximala antalet nivåer i DNS är 127, vilket innebär att ett domännamn skulle kunna ha 127 delar med punkter emellan sig.



Figur 2. Domäner och underdomäner.

Auktoritativa namnservrar

Trädstrukturen för ett system[1] i sin helhet brukar kallas för dess domännamnrymd (*domain name space*). I fallet Internet innefattar domännamnrymden alltså alla domäner på hela Internet och är jättelik. Trots detta är grundidén med en trädstruktur så genialisk att det oftast går blixtsnabbt att hitta fram till rätt information.

För varje domän i domännamnrymden finns en namnserver, eller för att vara mer exakt, en auktoritativ namnserver (som ibland också kallas svarande namnserver). Och i praktiken finns det oftast flera namnservrar med identisk information.

Namnservrar, eller DNS-servrar som de också kallas, är de programvaror som används för att få fram information i DNS. Det finns ett antal olika namnserverprogram att välja mellan, men det absolut vanligaste för större installationer är BIND, ett program med öppen

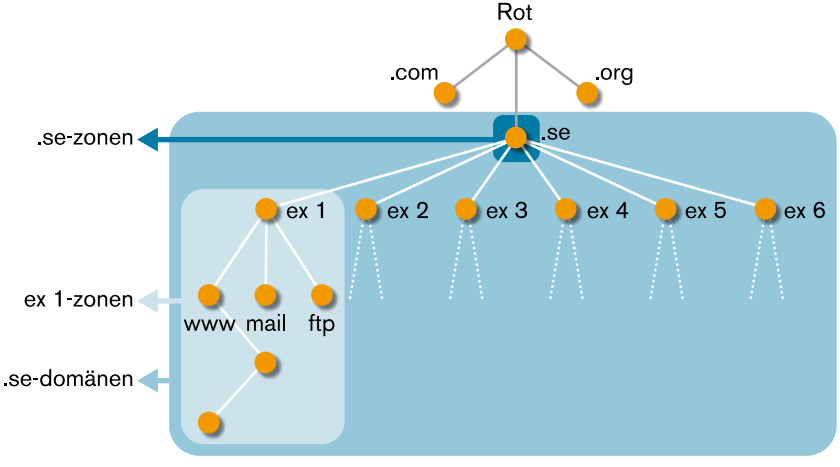
1 Som tidigare nämnts kan ju DNS även användas i nätverk som inte är uppkopplade till Internet.

källkod som från början utvecklades vid universitet Berkley i Kalifornien. Andra vanliga program är Microsoft DNS, vilket ingår i Windows Server, samt Unbound och djbdns, båda med öppen källkod.

Delegering och zoner

Varje fungerande domännamn på Internet måste ha (minst) en utpekad auktoritativ namnserver som kan översätta domännamnet till en IP-adress. Detta kan låta som att vissa namnservrar måste innehålla väldigt mycket information – till exempel finns det över trekvarts miljon domännamn som slutar på .se. Måste då inte den auktoritativa namnservern för .se ha koll på IP-adresserna för alla dessa domännamn?

Svaret är nej. Tack vare att DNS är hierarkiskt uppbyggt behöver den utpekade namnservern för .se inte ha informationen om alla sina underdomäner. Det ansvaret kan i stället delegeras till andra auktoritativa namnservrar. Varje namnserver har bara komplett information om en del av sin domän och denna del kallas för en



Figur 3. Domäner och zoner.

zon. Det går alltså att tala om både *.se*-domänen och *.se*-zonen. Vad zonen består av beror på vad den som ansvarar för den aktuella domänen väljer att delegera. De underdomäner som får ansvar för sina egna zoner kan sedan i sin tur välja att delegera ytterligare underdomäner.

Det är på detta vis man i praktiken delar upp ansvaret för Internets olika delar på flera händer. Var och en har ansvar för DNS-informationen för sin zon. Det för med sig att domänerna längre ned i hierarkin är beroende av att de högre nivåerna fungerar, så att delegeringen verkligen sker och det går att hitta fram till den IP-adress som är knuten till ett visst domännamn. Däremot är de högre nivåerna i hierarkin inte beroende av sina underdomäner. Denna ansvarsfördelning gör infrastrukturen mindre känslig. Samtidigt blir ansvaret tyngre ju närmare man kommer roten i trädstrukturen.

Roten och toppdomänerna

Vem är det då som ansvarar för att de auktoritativa namnservrarna på de högre nivåerna i Internets DNS-träd fungerar och innehåller den nödvändiga informationen (och därigenom ser till att Internet fungerar)? Om vi börjar med själva roten, vilken resten av Internet är helt beroende av, så finns det 13 IP-adresser på Internet där man hittar rotnamnservrar. Det innebär inte att det bara finns 13 stycken servrar, bakom de enskilda adresserna döljer det sig i vissa fall utspridda kluster av servrar, så det totala antalet är närmare 200. I dag är det ICANN (*The Internet Corporation for Assigned Names and Numbers*) som har ansvaret för innehållet i rotnamnservrarna.

Trots att det är otroligt kritiskt att de fungerar så behöver rotnamnservrarna i praktiken inte innehålla så mycket information, eftersom närapå allt ansvar för DNS-informationen har delegerats ned till nästa nivå i hierarkin. Här finns de så kallade toppdomänerna, ofta förkortade TLD (*top-level domains*). Då toppdomänerna utgör nivån närmast roten i DNS-trädet och ett domännamn indikerar sökvägen till roten i omvänd ordning, så slutar alla domännamn

med en toppdomän. Detta är grundläggande för att det ska gå att hitta fram till informationen om vilken IP-adress som domännamnet korresponderar till.

Man skiljer på generiska toppdomäner som .com för kommersiella syften, .org för icke-kommersiella organisationer, .net för domäner som har anknytning till nätverket Internet och så vidare, och på nationella toppdomäner som .se, .fi, .dk, .no med flera.[2] Det finns ett 20-tal generiska toppdomäner och knappt 300 nationella toppdomäner som i olika grad är kopplade till stater, territorier och i ett fall (.eu) till en överstatlig union. Landskoderna med två bokstäver följer standarden ISO 3166 (förutom vad gäller Storbritannien, där man valt att använda .uk i stället för .gb i syfte att inkludera Nordirland).

Vem som har ansvaret för att administrera toppdomänerna bestäms av ICANN. Som en följd av att Internet växte fram gradvis och på informella vägar är det en rätt vildvuxen blandning aktörer som i dag har detta ansvar för de olika toppdomänerna. Två av de populäraste generiska toppdomänerna, .com och .net, administreras till exempel av det börsnoterade amerikanska företaget VeriSign. Vad gäller de olika nationella toppdomänerna är det i vissa fall också privata, vinstdrivande företag som administrerar dem, ibland utan någon som helst koppling till landet i fråga (ett i Sverige välkänt fall är den lilla önationen Niues toppdomän .nu).

Hur det ser ut för respektive toppdomän hänger ofta ihop med historien kring Internet i det specifika landet. Från början var det ofta små grupper i den akademiska världen som sysslade med Internet. I Sverige var det exempelvis under lång tid en enda person, Björn Eriksen på ENEA och sedan KTH, som ansvarade för den nationella toppdomänen .se. Vad som sedan hände när Internetutvecklingen tog fart på allvar på 1990-talet skiljde sig åt i olika länder. Läs faktarutan härintill om hur det ser ut i de olika nordiska länderna, så förstår du vilken mångfald som råder.

2 Se appendix B för en fullständig lista över alla toppdomäner.

Ansvaret för den nationella toppdomänen i de nordiska länderna

- I **Danmark** står den ideella föreningen DIFO (Dansk Internet Forum) bakom det bolag som administrerar .dk-domänen, DK Hostmaster. Bland föreningens medlemmar finns till exempel olika branschorganisationer inom IT och annat näringsliv, Danmarks advokatsamfund och den unix-användarförening som var involverad i den danska delen av Internet under dess tidiga år.
- I **Sverige** är det .SE (Stiftelsen för Internetinfrastruktur) som sedan mer än ett årtionde har ansvarat för .se-domänen, sedan några år tillbaka reglerat av en särskild lag och med Post- och telestyrelsen (PTS) som tillsynsansvarig myndighet. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige, bland annat genom att överskottet från registreringen av domännamn finansierar olika initiativ för att främja Internetutvecklingen i landet.
- I **Norge** är det vare sig en ideell förening eller en stiftelse som står bakom den nationella toppdomänen, utan den norska staten. Norid, som har till uppgift att administrera .no-domänen, är ett dotterbolag till det statsägda företaget Uninett, vilket i sin tur levererar nätverk och nätverkstjänster till de norska universiteten och högskolorna.
- I **Finland** är toppdomänen i än högre grad en del av staten. Där är det Kommunikationsverket, det vill säga motsvarigheten till PTS i Sverige, som administrerar .fi-domänen. Ålands toppdomän .ax administreras av Ålands landskapsregering.
- På **Island**, slutligen, ägs företaget ISNIC som administrerar .is-domänen numera av privata investerare, efter det att Islands universitet och isländska staten sålt sin aktiemajoritet i bolaget år 2001.

Registrering av domännamn

Den som vill starta en domän på Internet måste vända sig till någon av dem som administrerar en toppdomän för att registrera sitt domännamn, annars går det inte att hitta fram till domänen via DNS. I och med den mångfald som råder kan regler och priser för detta skilja sig mycket mellan olika toppdomäner.

För vissa nationella toppdomäner måste man höra hemma i landet för att registrera ett domännamn, för andra godtas bara företag eller andra juridiska personer. En del nationella toppdomäner använder egna generiska underdomäner för olika kategorier av kunder, till exempel går det inte att registrera domännamn direkt under den brittiska .uk-domänen, utan kommersiella företag är hänvisade till .co.uk, privatpersoner till .me.uk och så vidare. Reglerna för registrering kan förstås också ändras över tiden, som till exempel när privatpersoner år 2003 fick börja registrera domännamn direkt under .se.

IDNA ger stöd för fler språk

Genom ansvarsfördelningen på Internet råder det alltså stor mångfald kring såväl vem som administrerar toppdomänerna och hur man kan registrera domännamn under dem. Men vissa regler för hur domännamn får se ut är gemensamma för alla toppdomäner. DNS begränsar varje led i ett domännamn till max 63 tecken. Och vill du att ditt domännamn ska fungera bör det bara innehålla tecknen a–z, 0–9 eller bindestreck, ”-”[3]. Även om DNS i sig inte förbjuder att andra tecken används är det av andra orsaker mer eller mindre garanterat att domännamnet inte fungerar om man gör det.

Det är därför nordbor och andra från början fick vänja sig av med att använda våra bokstävers prickar, ringar, streck, krokar och andra fnuttar när det gällde webb- och e-postadresser. Internet startade ju i USA och engelska råkar vara ett språk som saknar sådana inslag (förutom vad gäller enstaka lånord). När Internet spreds över världen upplevdes det hela dock som ett problem på många håll utanför

3 Domännamnet får dock inte börja eller sluta med ett bindestreck.

den anglosaxiska språksfären. Och i länder där man använder helt andra skriftsystem än det latinska alfabetet var det här förstås en ännu större fråga.

I stället för att designa om hela den befintliga DNS-infrastrukturen har man valt att utveckla ett system som kallas IDNA (*Internationalized Domain Names in Applications*) för att jobba runt problemet. IDNA översätter tecken som används i andra språk än engelska till koder som fungerar i DNS. Systemet har i dag anammats av de flesta webbläsare, så skriver du till exempel in *www.båtfärdsgröt.se* i adressfältet i din Firefox så letar webbläsaren automatiskt efter *www.xn--btfrdsgrt-x2ai6s.se* i DNS. Det blir resultatet när å:et, ä:et och ö:et i domännamnet översätts till andra koder med hjälp av IDNA. Du slipper dock se den något svårläsliga översättningen i ditt webbläsarfönster och märker egentligen inte av översättningen.

Många nationella toppdomäner erbjuder numera registrering av dessa så kallade internationaliserade domännamn (IDN). Under .se-domänen kan man till exempel registrera domännamn som innehåller å, ä, ö, é och ü samt de tecken som förekommer i de officiella minoritetsspråken i Sverige: finska, jiddisch, meänkieli (tornedalsfinska), romani och samiska. Men även om det går problemfritt att använda IDN för webbplatser så fungerar det fortfarande inte tillfredsställande för e-post, så vi kan ännu inte bli helt blågula i vårt Internetutnyttjande.

”Men även om det går problemfritt att använda IDN för webbplatser så fungerar det fortfarande inte tillfredsställande för e-post, så vi kan ännu inte bli helt blågula i vårt Internetutnyttjande.”

Det pågår även testverksamhet för att skapa IDN-toppdomäner som skrivs med andra skriftsystem än det latinska alfabetet. På så vis skulle kineser, indier, ryssar, greker, iranier, araber och så vidare kunna skriva in hela domännamnen med sin egen skrift, inte bara underdomänerna.

Toppdomänernas delegering

De auktoritativa namnservrarna för en toppdomän ger alltså information om sin zon. Namnservrarna för .se-domänen informerar till exempel om .se-zonen. Den närmaste nivån under toppdomänerna brukar kallas huvuddomäner. De allra flesta huvuddomäner delegeras

och blir någon annan auktoritativ namnservers ansvar. Därför handlar informationen på toppdomänernas namnservrar framför allt om vilka delegeringar som gäller för olika huvuddomäner. Annorlunda uttryckt pekar toppdomänens namnservrar ut vilka namnservrar som har information om respektive huvuddomän.

För att detta ska vara möjligt måste den som administrerar toppdomänen få information om vilken delegering som ska gälla för varje huvuddomän som registreras under toppdomänen. Den som registrerar ett domännamn måste peka ut minst en auktoritativ namnserver för domännamnet. Antingen kan det vara en namnserver som innehavaren av domännamnet själv gör tillgänglig på Internet eller också drivs den av någon annan, ofta en Internetoperatör eller ett webbhotell.

När du registrerar ett .se-domännamn hos någon av de så kallade registrarer som .SE har auktoriserat för att sköta försäljning och administration av domännamn – i många fall just Internetoperatörer eller webbhotell – så sköter de oftast utpekningen av namnservrar åt dig. Eller också får du instruktioner från dem som berättar hur du gör det själv.

Zonfiler

Den DNS-information för en zon som tillhandahålls av en auktoritativ namnserver på Internet finns i en textfil som kallas zonfil. Där finns information om alla domännamn som ingår i den aktuella domänen. Hur fullständig denna information är för ett visst domännamn beror på om ansvaret för domännamnet i fråga har delegerats till en underordnad zon eller ej.

Informationen om varje domännamn bryts i zonfilen ned i ett antal så kallade DNS-poster (*resource records*) som gör att namnservrarna kan svara på ett antal olika frågor om varje domän. De viktigaste av de DNS-poster som kan anges för respektive domännamn hittar du i faktarutan härintill.

De viktigaste DNS-posterna

- **A: Address (IPv4)**
  Anger den IP-adress som motsvarar ett visst domännamn när protokollet IPv4 används. Till exempel efterfrågas den av webbläsaren när en användare har skrivit in en webbadress.
- **AAAA: Address (IPv6)**
  Anger den IP-adress som motsvarar ett visst domännamn när protokollet IPv6 används. Till exempel efterfrågas den av webbläsare när en användare har skrivit in en webbadress.
- **PTR: Pointer**
  Denna domännamnspekare anger vilket domännamn som motsvarar en viss IP-adress. Den kan användas vid så kallade omvända DNS-uppslagningar (se kapitlet Så går en DNS-uppslagning till).
- **MX: Mail Exchanger**
  Anger en e-postserver för domänen, så att det går att få reda på vart e-post till adresser som slutar på domännamnet ska skickas.
- **NS: Name Server**
  Specificerar en namnserver som är auktoritativ för en viss zon. Normalt finns som sagt flera auktoritativa namnservrar – och alltså flera NS-poster – för varje zon. I de fall en underdomän har delegerats är detta ofta allt som anges i zonfilen för den överordnade zonen. Har exempelvis example.se delegerats så finns NS-poster för example.se i .se-zonfilen, men för att få fram mer information är man sedan hänvisad till zonfilen som finns på de auktoritativa namnservrar som NS-posterna pekar ut.
- **CNAME: Canonical Name**
  Posten anger ett alias. Flera domännamn kan nämligen kopplas till samma IP-adress, men alla utom det verkliga namnet kan anges som alias med hjälp av denna post.
- **SOA: Start of Authority**
  I denna post anges ett antal uppgifter om zonen:
  – kontaktuppgifter (e-post) till den som är ansvarig för zonen
  – versionsnummer för zonfilen
  – hur ofta de sekundära namnservrarna ska kontrollera om zonen har uppdaterats (se avsnittet Zonöverföring härintill)

  - hur länge de ska vänta om de inte genast lyckas nå fram till den primära namnservern
  - hur länge information ska anses som giltig om det inte går att nå den primära namnservern
  - hur länge svar från zonen ska sparas (så kallad TTL = *time to live*, se vidare avsnittet Cachning i kapitlet Så går en DNS-uppslagning till)
  - domännamn för zonens primära namnserver
- **TXT: Text**
  Används bland annat för att lägga in kommentarer i klartext.

Zonöverföring

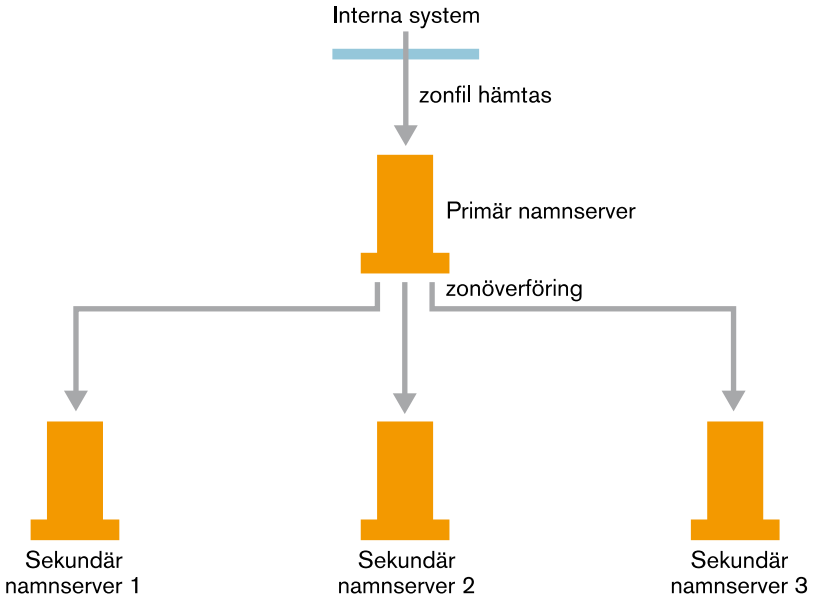
Den som är ansvarig för en zon ska se till att en uppdaterad zonfil finns tillgänglig på zonens auktoritativa namnserver. För att Internet ska fungera är detta av särskilt stor vikt för toppdomänerna. Till exempel uppdaterar .SE zonfilen för .se-zonen varannan timme, dygnet runt. Processen när de auktoritativa namnservrarna uppdateras kallas zonöverföring.

Om vi fortsätter med .se-zonen som exempel så går det till så att varje gång ett .se-domännamn registreras, pekas om till en ny namnserver eller avregistreras så förs de nya uppgifterna in i .SE:s domännamnsregister. Detta sker oftast via någon av .SE:s registrarer som för in förändringarna via ett särskilt gränssnitt. Informationen för samtliga .se-domännamn samlas i en zonfil som sedan överförs[4] till de auktoritativa namnservrarna för .se-zonen. På liknande sätt fungerar alla toppdomäner.

Genom zonöverföringen hålls informationen på namnservrarna hela tiden uppdaterad. För att DNS-tjänsten ska bli tillräckligt robust används oftast fler än en auktoritativ namnserver för att informera om en och samma zon. Eftersom det är viktigt att mini-

4 I praktiken är det endast förändringarna som överförs.

mera felkällor finns det då en primär namnserver som är den enda som hämtar zonfilen direkt från de interna systemen hos den institution som har ansvaret för zonen. De övriga namnservrarna är sekundära och hämtar zonfilen antingen från den primära namnservern eller från en annan sekundär namnserver.



Figur 4. Zonöverföring till primära och sekundära namnservrar.

Så går en DNS-uppslagning till

I elva steg kan du läsa om hur en DNS-uppslagning går till – om du vill veta vilken IP-adress ett speciellt domännamn har.

I föregående kapitel har vi förklarat att de auktoritativa namnservrarna gör DNS-information om olika domännamn tillgänglig på Internet. Vidare kunde du läsa att denna information finns uppdelad i DNS-poster i så kallade zonfiler som den som har ansvaret för respektive zon måste hålla uppdaterade.

Men hur går det till när någon vill ta reda på vilken IP-adress som motsvarar ett visst domännamn, exempelvis för att surfa in på en webbplats eller skicka ett e-postmeddelande? Då får denna någon, eller snarare hans/hennes dator, göra en DNS-uppslagning. Det kallas så eftersom DNS ju är ett slags katalog över domännamn och IP-adresser.

Programvaran som används för DNS-uppslagningar kallas för en resolver, eftersom den hittar lösningen på frågan vilken IP-adress ett domännamn motsvarar[5] (ibland kallas det också för frågande namnserver). Resolver-programmen ingår ofta i samma DNS-programvaror som de auktoritativa namnservrarna, det vill säga BIND, Microsoft DNS och så vidare.

Varje gång ett domännamn ska översättas till en IP-adress måste datorn ta hjälp av en resolver. Man skiljer på så kallade rekursiva resolvrar och stubb-resolvrar. När en rekursiv resolver genomför en DNS-uppslagning ställer den frågan om det aktuella domännamnet om och om igen tills den får svar.

En rekursiv resolver kan finnas installerad på den lokala klienten (det vill säga den Internetuppkopplade datorn som begär DNS-uppslagningen), men det är betydligt vanligare att ha en stubb-resolver installerad på sin dator. En stubb-resolver ställer frågan om domännamnet en enda gång till en rekursiv resolver som finns hos

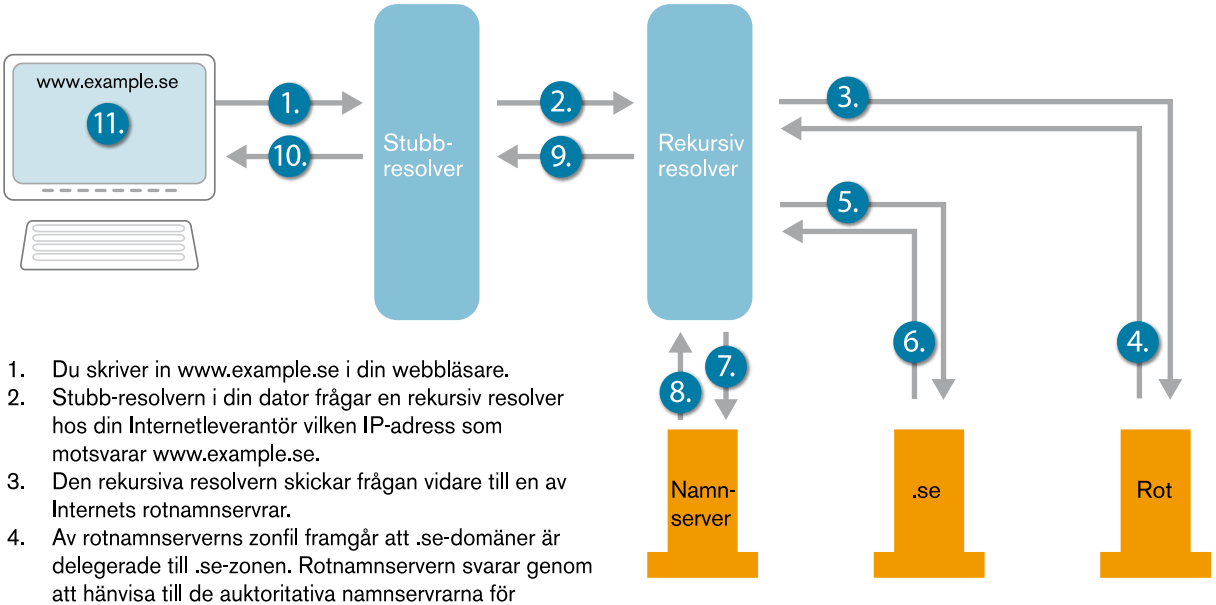
5 Engelskans *to resolve* = att lösa.

exempelvis Internetleverantören. Sedan är det denna rekursiva resolver som ställer frågan ut på Internet. På så vis behöver datorn inte befatta sig vidare med DNS-uppslagningen utan kan bara invänta svaret från den rekursiva resolvern.

Så hittar din dator rätt IP-adress

Vad händer då vid en DNS-uppslagning? Vi kan exemplifiera med vad som måste hända för att rätt webbplats ska dyka upp i ditt webbläsarfönster när du skriver in en viss webbadress:

1. **Du skriver in webbaddressen www.example.se i din webbläsare.**
   Som vi tidigare förklarat måste domännamnet översättas till en IP-adress. Det är först då din dator kan hitta rätt webbserver på Internet, ansluta till den och ladda hem innehållet på webbplatsen *www.example.se*. Det är detta DNS-uppslagningen handlar om.
2. **Stubb-resolvern i din dator frågar en rekursiv resolver om IP-adressen.**
   Den rekursiva resolver som stubb-resolvern är konfigurerad att vända sig till finns troligen hos din Internetleverantör. Det är den som får ställa DNS-frågan om vilken IP-adress som motsvarar *www.example.se* till de berörda auktoritativa namnservrarna på Internet. Din dator behöver inte befatta sig med resten av proceduren utan kan helt enkelt invänta svaret från den rekursiva resolvern.
3. **Den rekursiva resolvern skickar frågan vidare till en av Internets rotnamnservrar.**
   I detta exempel finns ingenting om domännamnet lagrat på den rekursiva resolvern (mer om detta följer avsnittet Cachning). Därför måste den börja sin undersökning från toppen av DNS-trädet. Resolvern ställer frågan om *www.example.se* till en av Internets rotnamnservrar.



1. Du skriver in www.example.se i din webbläsare.
2. Stubb-resolvern i din dator frågar en rekursiv resolver hos din Internetleverantör vilken IP-adress som motsvarar www.example.se.
3. Den rekursiva resolvern skickar frågan vidare till en av Internets rotnamnservrar.
4. Av rotnamnserverns zonfil framgår att .se-domäner är delegerade till .se-zonen. Rotnamnservern svarar genom att hänvisa till de auktoritativa namnservrarna för .se-zonen.
5. Resolvern ställer frågan igen, till en av de auktoritativa namnservrarna för .se-zonen.
6. Av .se-namnserverns zonfil framgår att example.se har delegerats och .se-namnservern svarar med att hänvisa till de auktoritativa namnservrar som pekats ut för domännamnet.
7. Resolvern ställer frågan igen till en av de utpekade auktoritativa namnservrarna för example.se.
8. Den auktoritativa namnservern för example.se svarar med IP-adressen som motsvarar www.example.se.
9. Den rekursiva resolvern vidarebefordrar IP-adressen till stubb-resolvern på din dator.
10. Stubb-resolvern vidarebefordrar IP-adressen till din webbläsare.
11. Webbläsaren ansluter till webbservern som finns på datorn som har den angivna IP-adressen och laddar ner webbsidan till din dator.

Figur 5. Alla steg i en DNS-uppslagning (när ingen information finns lagrad).

4. Rotnamnservern hänvisar till de auktoritativa namnservrarna för .se-zonen.
Av rotnamnserverns zonfil framgår att alla *.se*-domäner har delegerats till *.se*-zonen. Alltså kan rotnamnservern inte svara på frågan vilken IP-adress som motsvarar *www.example.se.* Däremot har rotnamnservern ständigt uppdaterad information om vilka namnservrar som är auktoritativa för *.se*-zonen och svarar därför med en hänvisning till dem.

5. **Resolvern ställer om frågan till en av .se-zonens auktoritativa namnservrar.**
   Svaret från rotnamnservern innebär att den rekursiva resolvern kan begränsa sin vidare sökning efter rätt IP-adress till *.se*-zonen. DNS-frågan ställs nu till en av de auktoritativa namnservrarna som rotnamnservern hänvisade till.

6. **Namnservern för .se-zonen hänvisar till de auktoritativa namnservrarna för example.se**
   Av *.se*-namnserverns zonfil framgår att *example.se* har delegerats till en underordnad zon. Alltså kan *.se*-namnservern inte heller svara på frågan vilken IP-adress som motsvarar *www.example.se.* Däremot finns i zonfilen alltid uppdaterad information om vilka auktoritativa namnservrar som har pekats ut för domännamnet *example.se.* Därför svarar *.se*-namnservern med en hänvisning till dem.

7. **Resolvern ställer om frågan till en av de utpekade auktoritativa namnservrarna.**
   Svaret från *.se*-namnservern innebär att den rekursiva resolvern nu kan vända sig till en av de namnservrar som har pekats ut som auktoritativ för domännamnet *example.se.* I vissa fall är det domäninnehavaren själv som gör dessa namnservrar tillgängliga på Internet, fast ofta drivs de av ett webbhotell eller en Internet-leverantör.

8. **Den auktoritativa namnservern för example.se svarar med IP-adressen.**
   Zonfilen på den auktoritativa namnservern för *example.se* har uppdaterad information om vilken IP-adress som motsvarar *www.example.se.* Ibland är domännamnet ett alias vilket gör att det kan finnas flera domännamn knutna till samma IP-adress. Endast ett av domännamnen är då det ”äkta” domännamnet för IP-adressen. Hur som helst behövs nu inga fler hänvisningar, utan namnservern kan svara på frågan med den aktuella IP-adressen.

9. **Den rekursiva resolvern vidarebefordrar IP-adressen till stubb-resolvern på din dator.**
   Nu är den rekursiva resolverns arbete över för denna gång.
10. **Stubb-resolvern vidarebefordrar IP-adressen till din webbläsare.**
11. **Webbläsaren ansluter till datorn som finns på IP-adressen.**
    När webbläsaren fått reda på IP-adressen som motsvarar *www.example.se* kan den ansluta till webbservern som finns ansluten till Internet på denna adress. Sedan laddas webbsidan i fråga ned till din dator så att du kan titta på den i webbläsaren.

Så ser en DNS-uppslagning ut

Med verktyget *dig,* som ingår i programvaran BIND, kan man låtsas vara resolver i dialogen som förs mellan den rekursiva resolvern och de auktoritativa namnservrarna vid en DNS-uppslagning. Dialogen ser ut så här (efter att det mesta av informationen har klippts bort för överskådlighetens skull):

```
1.   FRÅGA   dig @h.root-servers.net www.pts.se
2.   SVAR    se.     172800  IN      NS      d.ns.se.
             d.ns.se.172800  IN      A       81.228.8.16
4.   FRÅGA   dig @81.228.8.16 www.pts.se
5.   SVAR    pts.se.86400    IN      NS      b.dns.songnetworks.se.
             b.dns.songnetworks.se.86400    IN      A       213.50.29.195
6.   FRÅGA   dig @213.50.29.195     www.pts.se
7.   SVAR    www.pts.se.7200         IN      A       192.121.211.200
8.   FRAMME!
-----------------------------------------------------------------
```

Hela DNS-uppslagningen går oftast på bråkdelen av en sekund. Den snabbas dessutom på av att den rekursiva resolvern kan korttidslagra information och varifrån den kom. Det är detta som kallas cachning.

Cachning (mellanlagring)

För att hindra DNS-uppslagningarna från att ta för lång tid och orsaka onödigt mycket nätverkstrafik, så kan en rekursiv resolver tillfälligt lagra svar som den får från namnservrar i sitt så kallade cacheminne. När en fråga kommer in till resolvern så kontrollerar den först om det finns några uppgifter i cacheminnet som kan hjälpa till att svara på den.

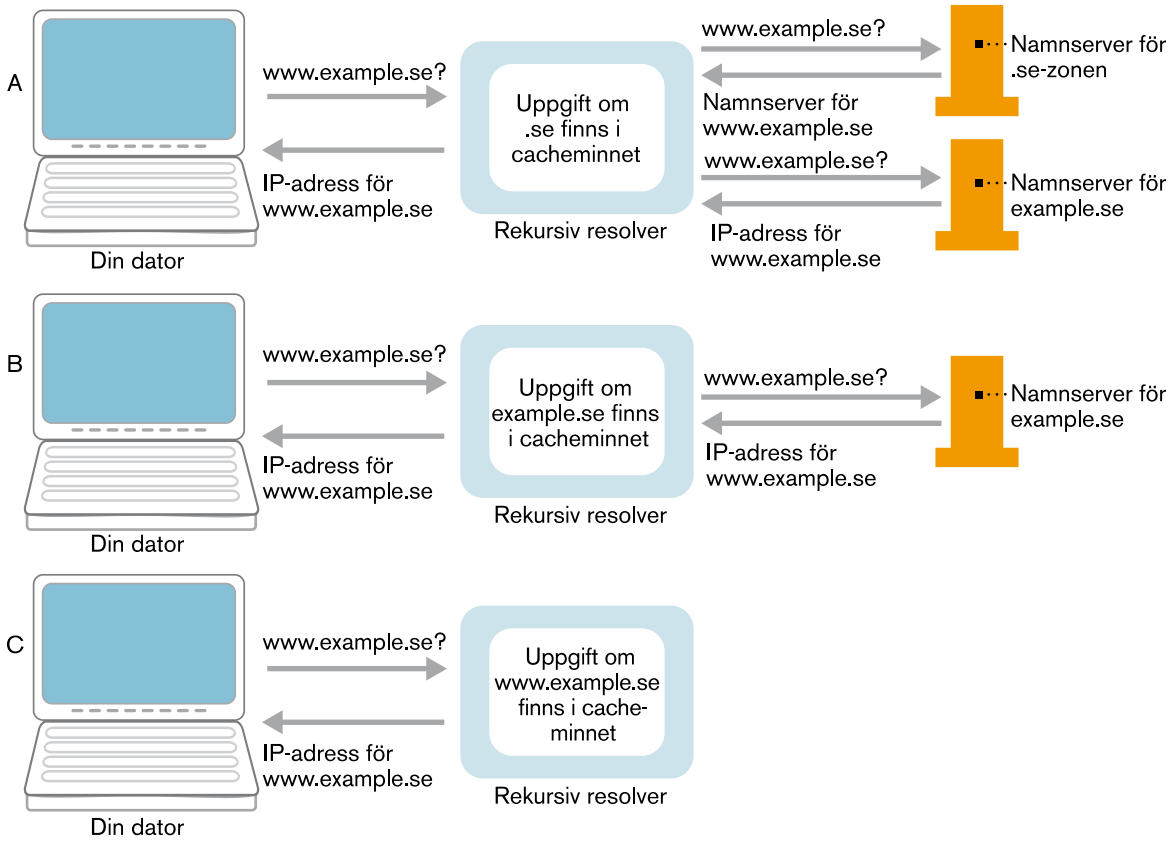
Om vi använder samma exempel som tidigare, www.example.se, så kanske resolvern nyligen har svarat på en fråga om ett annat domännamn som slutar på .se. I så fall finns svaret som resolvern den gången fick från rotnamnservern fortfarande lagrat i cacheminnet. Av det sparade svaret framgår vilka namnservrar som är auktoritativa för .se-zonen och resolvern kan därför hoppa över steget att fråga rotnamnservern. I stället ställs frågan om *www.example.se* direkt till en av *.se*-namnservrarna (se exempel A i Figur 6 här bredvid).

Det kan också vara så att resolvern nyligen har svarat på en fråga om ett annat domänamn som slutar på *example.se*. Exempelvis kanske en annan användare har laddat upp filer till *ftp.example.se* med hjälp av samma resolver. Då finns svaret som resolvern fick från *.se*-zonens namnserver lagrat i cacheminnet och resolvern kan hoppa över även detta steg och gå direkt till en av de auktoritativa namnservrarna för *example.se* (se exempel B i Figur 6 här bredvid).

Slutligen kanske resolvern har svarat på en fråga om just *www.example.se*. I så fall finns svaret som den fick från den auktoritativa namnservern för detta domännamn lagrat i cacheminnet och resolvern kan svara din dator direkt med vilken IP-adress som motsvarar *www.example.se* (se exempel C i Figur 6 här bredvid).

Hur länge svaren lagras av den rekursiva resolvern bestäms av ett värde som anges av den som är ansvarig för zonen, en så kallad TTL (*time to live*). När denna tidsperiod är slut sparas uppgiften inte längre och då måste den rekursiva resolvern kontakta någon av zonens auktoritativa namnservrar nästa gång en uppslagning görs.

Det finns argument både för och emot en lång TTL. Eftersom trafiklasten minskar och uppslagningarna blir snabbare genom



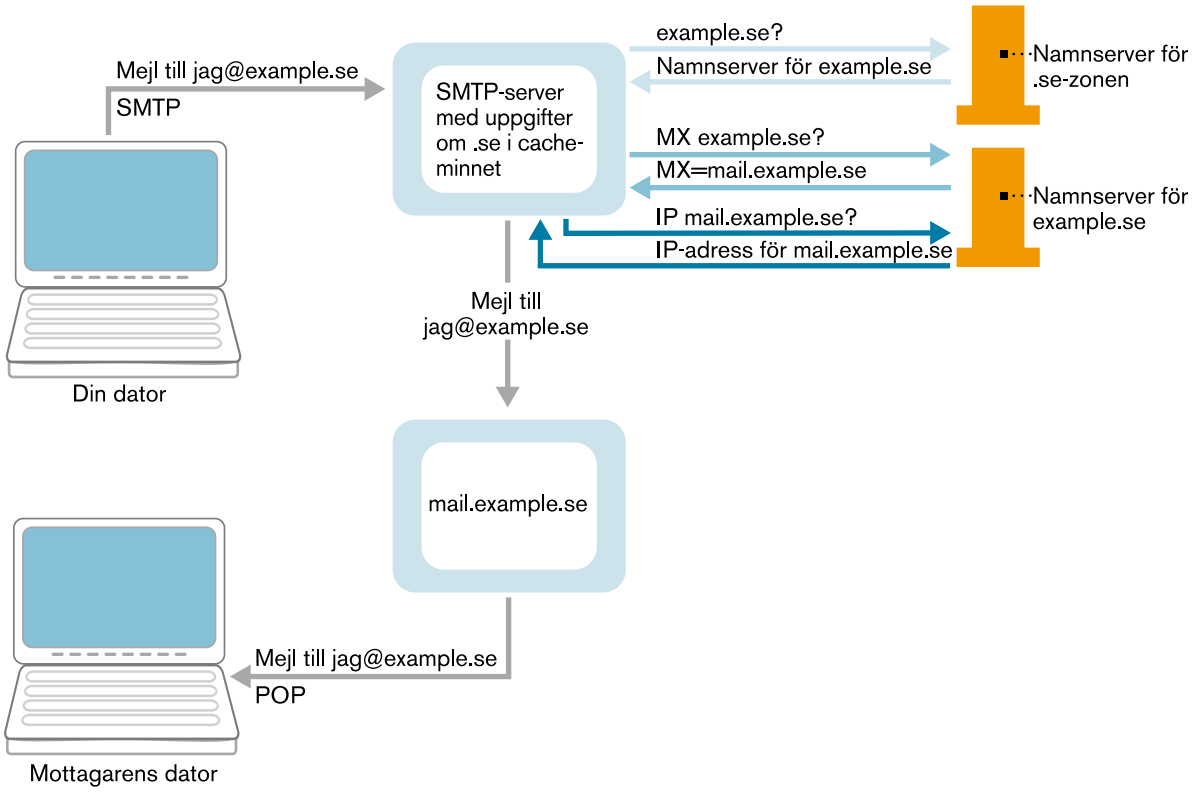
Figur 6. DNS-uppslagningar där information finns lagrad i resolverns cacheminne.

mellanlagring kan man tycka att det vore bra att använda en så lång TTL som möjligt. Men samtidigt tar det då längre tid för förändringar i zonfilen att slå igenom. Det kan leda till problem att till exempel nå fram till webbsidor när domännamn tillkommer eller pekas om till nya namnservrar. TTL för domäner under .se är som standard 24 timmar, vilket kan ses som en lagom kompromiss för en toppdomän.

E-postservrars DNS-uppslagningar

Från din dator skickas e-postmeddelanden via en e-postserver för utgående post, oftast med ett protokoll som heter SMTP (*Simple Mail Transfer Protocol*). Alla e-postadresser, till exempel *jag@example.se*, slutar med ett domännamn. När du skickar iväg ett mejl till denna adress från din dator så kommer det först till den SMTP-server som du har ställt in i ditt e-postprogram. Vanligtvis tillhandahålls denna av din Internetoperatör eller ditt webbhotell.

För att SMTP-servern ska veta vart mejlet sedan ska, så måste



Figur 7. E-postöverföring med DNS-uppslagningar.

den först få fram IP-adressen till den mottagande e-postservern för domännamnet *example.se*. Därför gör den en DNS-uppslagning på domännamnet *example.se* på samma sätt som den rekursiva resolvern i exemplet här bredvid. Vad den tar fasta på i svaret från den auktoritativa namnservern för example.se är vilken e-postserver som pekas ut för domänen i DNS-posten MX (*Mail Exchanger*), i det här fallet säger vi att servern heter *mail.example.se*.

SMTP-servern slår då upp domännamnet *mail.example.se* i DNS och namnservern för *example.se* svarar på frågan med den IP-adress som motsvarar detta domännamn. Nu kan den avsändande e-postservern ansluta till den mottagande över Internet och mejlet överföras. När användaren som har e-postadressen *jag@example.se* sedan laddar hem sina nya meddelanden från den mottagande e-postservern, oftast med hjälp av något av protokollen POP (Post Office Protocol) eller IMAP (*Internet Message Access Protocol*), så kommer ditt mejl fram.

E-post behöver inte fungera på exakt detta vis, i synnerhet inte i respektive ände, eftersom man till exempel kan använda webbmejl och då loggar in direkt till sin e-postserver. Men så länge e-postmeddelanden skickas över Internet och inte internt inom ett företagsnätverk måste DNS-uppslagningar alltid genomföras för att meddelandena ska hamna rätt.

Omvänd DNS-uppslagning

Det som beskrivits ovan är den vanligaste sortens DNS-uppslagning, när man har ett domännamn och vill få fram en IP-adress för att kommunicera med en dator över Internet. Men det finns också tillfällen då det är användbart att ta reda på vilket domännamn som motsvarar en viss IP-adress. Därför går det även att göra omvända uppslagningar i DNS.

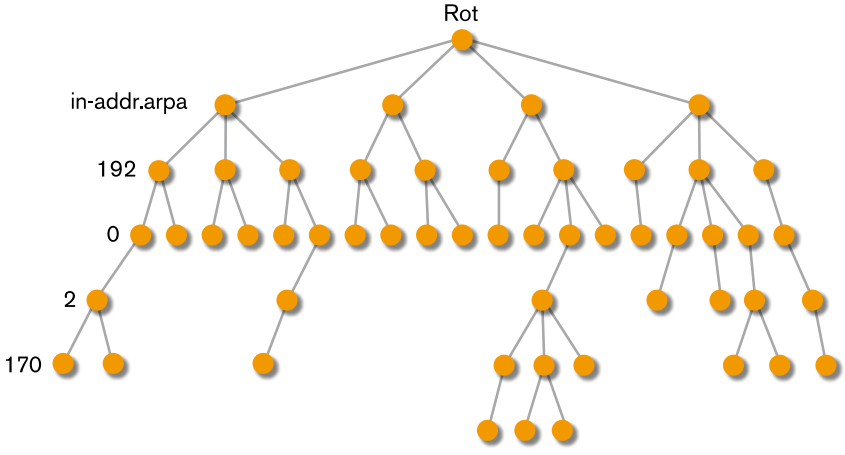
Många moderna e-postsystem gör DNS-uppslagningar både på domännamn och på IP-nummer för att se att de stämmer överens och på så vis upptäcka när till exempel spammare använder falska avsändaradresser när de skickar sin skräppost.

Praktiskt är det möjligt att göra en omvänd DNS-uppslagning

genom att en del av domännamnrymden på Internet avspeglar alla använda publika IP-adresser i en trädstruktur, på samma sätt som resten av domännamnrymden kartlägger domännamn. När det gäller IPv4-adresser heter domänen för detta in-addr.arpa. Den utgår från det gängse sättet att skriva IPv4-adresser, som fyra siffergrupper av nummer mellan 0–255 med punkter mellan sig, exempelvis 192.0.2.170.

Eftersom numren i IP-adresser blir mer specifika ju längre åt höger de står i adressen är det denna ordning som bestämmer hierarkin i in-addr.arpa-domänen. I vårt exempel hamnar därför 192 som den högst placerade underdomänen i *in-addr.arpa*-domänen, 0 på nästa nivå, följt av 2 och 170.

DNS-uppslagning kan enkelt göras med hjälp av verktyg som finns tillgängliga på olika webbplatser (till exempel www.lookup-server.com). För att ta reda på vilket domännamn som motsvarar IP-adressen 192.0.2.170 så gör dessa verktyg helt enkelt en DNS-uppslagning på domännamnet *170.2.0.192.in-addr.arpa*. På grund av sättet trädstrukturen är uppbyggd på bakvänds alltså IP-adressen. Genom DNS-posten PTR (*Pointer*) för domännamnet



Figur 8. IP-adressen 192.0.2.170 i in-addr.arpa-domänen.

170.2.0.192.in-addr.arpa får man sedan fram vilket domännamn som motsvarar IP-adressen i fråga.

För IPv6-adresser finns en motsvarande domän som heter ip6.arpa. Proceduren där är densamma som för IPv4, fast adresserna är längre – och därmed blir nivåerna i DNS-trädet fler.

Det finns också programvaror med öppen källkod som kan användas såväl för att göra omvända DNS-uppslagningar som för att få fram alla möjliga andra DNS-uppgifter om Internetanslutna datorer. Ett sådant program heter *nslookup* och ett nyare är verktyget *dig* som ingår i programvaran BIND.

Det främsta hotet mot DNS – och lösningen

I det här kapitlet kan du läsa om hoten mot DNS och de risker som dåligt uppdaterade namnservrar utgör. Men vi berättar också om olika sätt att hindra angriparna från att ställa till med skador, eller åtminstone försvåra för dem.

Ända sedan människor i stor skala började utnyttja Internet för affärstransaktioner, bankärenden och så vidare har illasinnade krafter på olika sätt försökt exploatera det för egen vinning. Dessa brottslingar kan bland annat försöka utnyttja brister i DNS för att lura intet ont anande Internetanvändare.

DNS-programvarorna utvecklas förstås hela tiden och man täpper till säkerhetshål allt eftersom dessa upptäcks. Men samtidigt som DNS distribuerade karaktär och frånvaron av centralstyrning har varit nyckeln till Internets framgång och stora spridning, får just dessa egenskaper som konsekvens att det är svårt att driva igenom verkligt heltäckande förändringar i systemet. Ingen har överblick över samtliga auktoritativa namnservrar och rekursiva resolvrar som används vid DNS-uppslagningar på Internet, så det finns risk att råka ut för dåligt uppdaterade namnservrar och resolvrar som är känsliga för attacker av olika slag.

Ett knep som de kriminella har använt är så kallat nätfiske (*phishing*), vilket i sin ursprungliga form egentligen inte kräver att man utnyttjar några tekniska brister i DNS. Vid nätfiske lockar man – ofta via länkar i ett falskt mejl som utnyttjar välkända varumärken, logotyper och liknande – in användare på en falsk webbplats som utger sig för att vara till exempel en Internetbank. På den falska sajten försöker man få användarna att uppge känsliga uppgifter, exempelvis kreditkortsnummer och lösenord.

Ibland har nätfiskarna gjort en så kallad felstavningsregistrering och använder ett domännamn som ligger nära namnet på det före-

tag vars kunder man vill blåsa. Denna typ av missbruk motarbetas oftast av toppdomänerna genom att företag kan hävda sin rätt till sådana domännamn i kraft av till exempel registrerade varumärken.

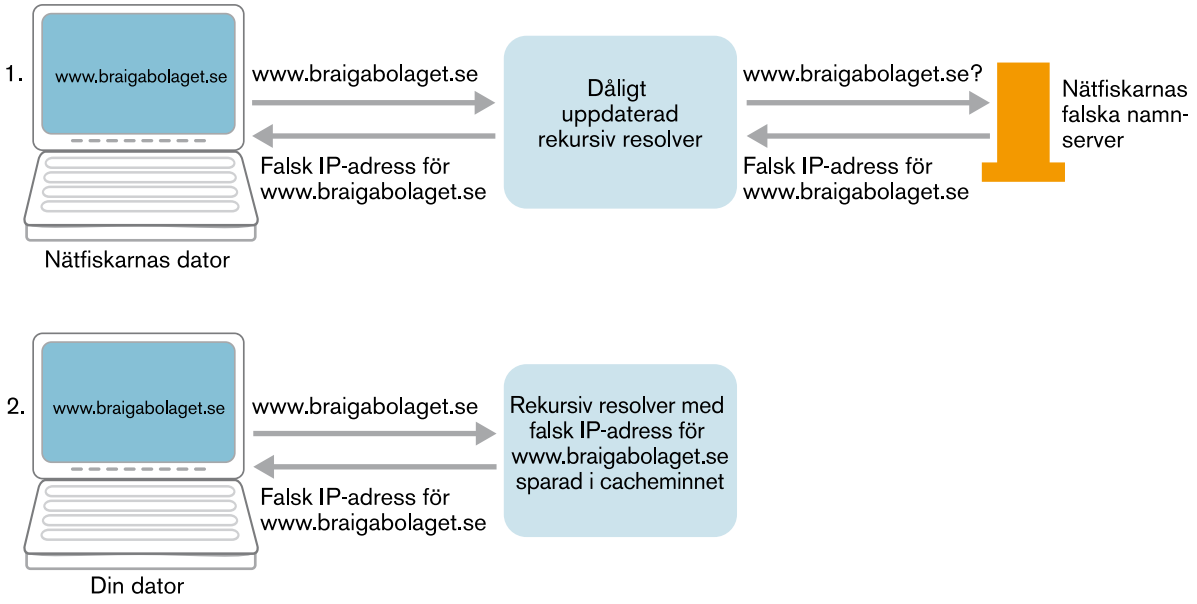
I Sverige har flera bankers kunder utsatts för nätfiskeangrepp, men det har oftast varit ganska lätt att inse att mejlet varit falskt, inte minst på grund av lurendrejarnas bristande kunskaper i svenska språket. De flesta användare har inte låtit sig luras vid sådana attacker.

Cacheförgiftning och ”Kaminskybuggen”

Det kan vara svårare att lista ut att man blir lurad när de fula nätfiskarna utnyttjar domännamnssystemets öppna arkitektur genom så kallad cacheförgiftning. Då behöver angriparna inte lura användaren att själv klicka på en länk till deras falska webbplats. I stället hittar de en rekursiv resolver som är dåligt uppdaterad. Tack vare brister i DNS-programvaran kan angriparna förse resolvern med ett falskt svar som uppger en felaktig IP-adress för det efterfrågade domännamnet.

Eftersom svaret sparas i resolverns cacheminne, med ett TTL-värde som anges av angriparen, så kommer alla användare som sedan ställer frågan om det aktuella domännamnet att få det falska svaret och därmed ledas in på angriparens falska webbplats som finns på en server med den felaktiga IP-adressen. Om sajten är välgjord har man ingen anledning att tro att något är fel. Det går inte att se på webbadressen i webbläsaren att informationen på en sajt kommer från en falsk server

Låt oss säga att du ska logga in och göra affärer på adressen *www.braigabolaget.se*. Om då din Internetoperatör har slarvat med att uppdatera sina rekursiva resolvrar så kan en eller flera av dem ha cacheförgiftats för att ge fel svar på just domännamnet *www.braigabolaget.se.* Har du otur svarar en förgiftad resolver på din DNS-fråga och du leds via en felaktig IP-adress intet ont anande in på en kopia av Braiga bolagets webbplats som ligger på skurkarnas server. Väl där kan du luras att till exempel uppge inloggningsuppgifter eller



Figur 9. Cacheförgiftning där användaren får ett falskt svar på sin DNS-uppslagning.

ditt kreditkortsnummer som de sedan använder för att handla med själva.

En annan variant är att angriparen lägger sig emellan användaren och den besökta webbplatsen och bara byter ut delar av informationen på sajten. Syftet är förstås detsamma, att snappa upp intressant information som kan missbrukas på olika sätt.

Sommaren 2008 väckte datasäkerhetsforskaren Dan Kaminsky stor uppmärksamhet då han upptäckte en allvarlig brist i DNS som sedermera ofta har kallats Kaminskybuggen. Vad han visade var ett enkelt sätt att utföra en cacheförgiftning. Dan Kaminsky förvarnade alla leverantörer av DNS-programvaror om buggen innan han gick ut offentligt med sin upptäckt. Därför kunde de utveckla uppgraderingar som försvårar genomförandet av denna sorts cacheförgiftning.

Möjligheten att genomföra cacheförgiftningar beror dock på en

brist i själva DNS-arkitekturen, så uppgraderingarna löser inte problemet slutgiltigt. Dessutom stöter man på problemet att alla måste uppdatera sina rekursiva resolvrar för att de ska vara säkra.

Även om uppgraderingarna av DNS-programmen gör att denna form av cacheförgiftning tar längre tid och blir svårare att genomföra, så finns bristerna i domännamnssystemet kvar. Så länge problemen kvarstår kommer skurkar att kunna utveckla nya metoder att utnyttja dem. Grundproblemet är att DNS inte från början byggdes upp med tanke på säkerheten. Vägen till att långsiktigt klara av säkerhetshoten är därför de säkerhetstillägg till DNS som har tagits fram och som går under beteckningen DNSSEC (*DNS Security Extensions*).

DNSSEC

Säkerhetstilläggen DNSSEC har utvecklats i syfte att säkra domännamnssystemet från missbruk som cacheförgiftning. För att råda bot på problemet med att det går att lura rekursiva resolvrar med falsk information används kryptografiska signaturer. Genom så kallad asymmetrisk kryptering säkerställer DNSSEC både att DNS-svaret kommer från rätt källa och att innehållet i det – viktigast av allt då vilken IP-adress som motsvarar ett visst domännamn – inte har ändrats under överföringen.

När en domän signeras med DNSSEC så flaggas detta i zonfilen för den överordnade zonen. Om domänen braigabolaget.se har signerats finns det i .se-zonfilen, utöver NS-posten som pekar ut vilken namnserver som är auktoritativ för domänen, även en så kallad DS-post (DS = *Delegation Signer*) för den. När en resolver gör en DNS-uppslagning på domännamnet braigabolaget.se kan den ur DS-posten utläsa att domänen är signerad och vem som publicerar nycklar för den. Då kommer resolvern att leta efter extra DNS-

poster även i svaret från den auktoritativa namnservern för braigabolaget.se. Försöker en nätfiskare lura resolvern med ett falskt svar som inte innehåller några sådana extraposter så kommer det inte att fungera.

DNSSEC-posterna i zonfilen på braigabolaget.se-domänens auktoritativa namnserver innehåller den digitala signaturen och information om vem som utfärdat den. När en rekursiv resolver får ett svar på en DNS-uppslagning så följer alltså DNSSEC-posterna med IP-adressen och övrig information. Resolvern kan då kontrollera signaturen, eftersom publika DNSSEC-nycklar görs tillgängliga på Internet av den som utfärdat en signatur.

Genom att följa en så kallad *"chain of trust"* kan resolvern även kontrollera att signaturen som följer med DNS-svaret om braigabolaget.se har skapats av rätt nyckel, så att ingen information kan ha ändrats på vägen från den auktoritativa namnservern till resolvern. En chain of trust slutar hos vad som kallas ett *"trust anchor"*, eller tillitsankare, en slutgiltig instans som garanterar att rätt nyckel har använts. I nuläget är .SE trust anchor för signerade .se-zoner. I en inte alltför avlägsen framtid kommer Internets rot förhoppningsvis att signeras och då börjar roten fungera som en sådan garant för hela DNS-trädet.

Genom chain of trust elimineras risken för att nätfiskaren ska kunna förfalska DNSSEC-posterna och leda resolvern till en falsk nyckel. Först när allt har säkerställts skickar resolvern vidare IP-adressen till den stubb-resolver som har bett om DNS-uppslagningen.

Införandet av DNSSEC

Ett allmänt införande av DNSSEC ses av många som en nödvändighet för att Internet ska fortsätta att blomstra och utvecklas. Problemet är detsamma som med de dåligt uppdaterade resolvrarna: det är svårt att genomdriva omfattande förändringar i hela systemet. Inte bara för att de som är innehavare av domännamn måste signera

sina domäner. För att DNSSEC ska fungera för alla Internetanvändare krävs också att alla resolvrar uppdateras och konfigureras så att de får stöd för tekniken.

Trots att själva DNSSEC-standarden har funnits i många år har tekniken hittills inte slagit igenom på bred front. Den svenska toppdomänen .SE har legat i framkant och var först i världen om att erbjuda en fullständig DNSSEC-tjänst i februari 2007 och sedan dess har några ytterligare toppdomäner följt efter. I och med Dan Kaminskys upptäckt 2008 ökade intresset avsevärt för DNSSEC och den svenska tjänsten rönte mycket uppmärksamhet internationellt.

Uppmärksamheten gjorde att allt fler domäninnehavare faktiskt också började signera sina domäner och nu kan snöbollen vara i rullning. Ytterligare ett steg för att underlätta DNSSEC-införandet är att ICANN, i väntan på att roten signeras, har upprättat ett särskilt register där toppdomänerna kan publicera sina DNSSEC-nycklar, vilket gör DNSSEC heltäckande genom att domännamn kan signeras ända upp till den högsta nivån i DNS. Även här var .SE först bland toppdomänerna när man publicerade nycklarna för .se-domänen där i januari 2009.

Ytterligare en fördel med DNSSEC är att om DNS-strukturen säkras mot missbruk och förfalskningar så kan samma katalog även användas till att publicera annan information som ställer högre krav på säkerhet.

IPv6 och DNS

Redan i det första kapitlet såg vi att dagens IPv4-adresser håller på att ta slut, och att Internet på sikt måste använda sig av nya, längre IPv6-adresser. DNS fungerar i princip likadant för IPv6 som för IPv4, men skiftet innebär ändå vissa omställningar.

I det första kapitlet (Datakommunikation på Internet) kunde du läsa att det i dag finns ett växande behov att gå över till en ny version av Internetprotokollet IP på grund av att IP-adresserna håller på att ta slut. Den nya versionen betecknas IPv6 och löser problemet genom att IP-adresserna blir på 128 bitar i stället för 32. Det innebär att antalet möjliga adresser blir i praktiken obegränsat, exempelvis skulle varje nu levande individ kunna ha 5×10^{28} IPv6-adresser var.

Eftersom övergången ännu inte riktigt har kommit i gång trots att adressbristen i IPv4 snart beräknas bli akut så kommer de två standarderna troligtvis leva vidare sida vid sida under ganska lång tid framöver. I länder som Sverige, där de flesta företag redan är uppkopplade och det finns relativt gott om IP-adresser, kommer övergången troligen bli en utdragen historia eftersom det inte är här bristen kommer att märkas mest. På andra håll, som i de stora tillväxtekonomierna i Asien, lär IPv6 komma att införas snabbare.

Däremot så kommer många svenska företag behöva se till att deras webbplatser, e-postservrar och andra Internetresurser går att nås över IPv6. Annars kan det hända att till exempel kunder, leverantörer och affärskontakter som enbart använder IPv6 inte kommer att kunna komma åt dessa.

För att det ska gå att nå webbplatser, e-postservrar och så vidare via IPv6 så måste de ha en IPv6-adress. DNS-drift och uppslagningar fungerar i princip på samma sätt oavsett vilket protokoll man använder. Den DNS-post i zonfilen som anger IPv6-adressen kallas dock AAAA eller quad-A i stället för A (eftersom IPv6-adresserna är fyra gånger längre än IPv4-adresserna).

Men det räcker inte att skaffa en IPv6-adress för att surfare som använder det nya protokollet ska kunna hitta fram till din webbplats. De namnservrar som är auktoritativa för domännamnet måste själva vara åtkomliga över IPv6, hela vägen från roten till det sista ledet i domännamnet. I dag finns redan namnservrarna på rotnivån och hos de flesta toppdomänerna tillgängliga via IPv6, men för underdomänerna är det de som har ansvaret för respektive namnserver, till exempel Internetoperatörer och webbhotell, som måste ordna med detta. Det handlar inte om någon större åtgärd men måste genomföras för att det ska gå att få fram en IPv6-adress genom DNS-uppslagningar över IPv6.

Avslutande ord

Syftet med denna guide har varit att ge en idé om hur DNS fungerar, utan att bli alltför teknisk. Förhoppningen är att du som läsare har fått ett begrepp om domännamnssystemet och vad som egentligen händer bakom kulisserna när du surfar på nätet.

Bilden som ges av DNS här är förstås ytterst förenklad och det finns mycket mer att lära sig för den som är intresserad. Vill du läsa mer och kanske själv lära dig använda DNS-programvara finns det en uppsjö av litteratur på engelska, både i tryckt form och på olika webbplatser. Nedan hittar du ett axplock.

Lästips för den som vill lära sig mer

DNS and BIND av Paul Albitz & Cricket Liu
(Förlag: O'Reilly, 2006)

DNS and BIND Cookbook av Cricket Liu
(Förlag: O'Reilly, 2002)

DNS for Dummies av Blair Rampling & David Dalan
(Förlag: For Dummies, 2003)

Alternative DNS Servers av Jan-Piet Mens
(Förlag: UIT Cambridge, 2008)

DNS on Windows Server 2003 av Cricket Liu, Matt Larson & Robbie Allen (Förlag: O'Reilly, 2003)

Pro DNS and BIND av Ron Aitchison
(Förlag: Apress, 2005)

http://www.dnssec.net/

Appendix A – Typfall för en ompekning av ett domännamn

Här förklaras hur en ”ompekning” av ett domännamn under .se ska göras för att minimera nödvändig nedtid för både DNS-tjänsten och kringtjänster som webb och e-post. Ompekning är detsamma som att byta auktoritativ namnserver för domännamnet. Det sker till exempel när domäninnehavaren byter registrar. Men det händer också att en innehavare bara byter namnserveroperatör och leverantör av kringtjänster, utan att för den skull byta registrar.

Det finns en inneboende tröghet i DNS-tjänsten på grund av att de rekursiva resolvrarna mellanlagrar DNS-svar enligt det TTL-värde som den zonansvariga har satt. Därför är det viktigt att göra flytten i två steg för att webb- och e-posttjänster ska hållas i drift under hela processen. När man byter från tjänsteleverantör 1 (TL1) till tjänsteleverantör 2 (TL2) ska man:

1. Flytta DNS-tjänsten från TL1 till TL2.
2. När ompekningen slagit igenom på Internet (det vill säga när TTL har gått ut – vilket är 24 timmar för domäner under .se) flytta alla eventuella övriga tjänster (som webb och e-post) från TL1 till TL2.

Flödet nedan minimerar nedtiden för webb- och e-posttjänster till någon minut. (För tydlighetens skull antas det här att det bara finns en auktoritativ namnserver för domännamnet, fast det i verkligheten nästan alltid finns fler än en. Vid varje steg där namnserver anges, ska samtliga namnservrar anges.)

Typfall 1 – Domännamn utan DNSSEC-signering

1. **TTL minskas**
   Om tjänsteleverantören tillåter det, ska TTL för tjänsterna hos TL1 minskas till en väldigt kort period, 1–5 minuter. På detta vis kommer flytten av webb- och e-posttjänster att gå snabbt när den genomförs. Det ska göras först av allt för att förändringen ska hinna slå igenom innan flytten sker. Om befintlig TTL hos TL1 bedöms som tillräckligt kort kan detta steg hoppas över.

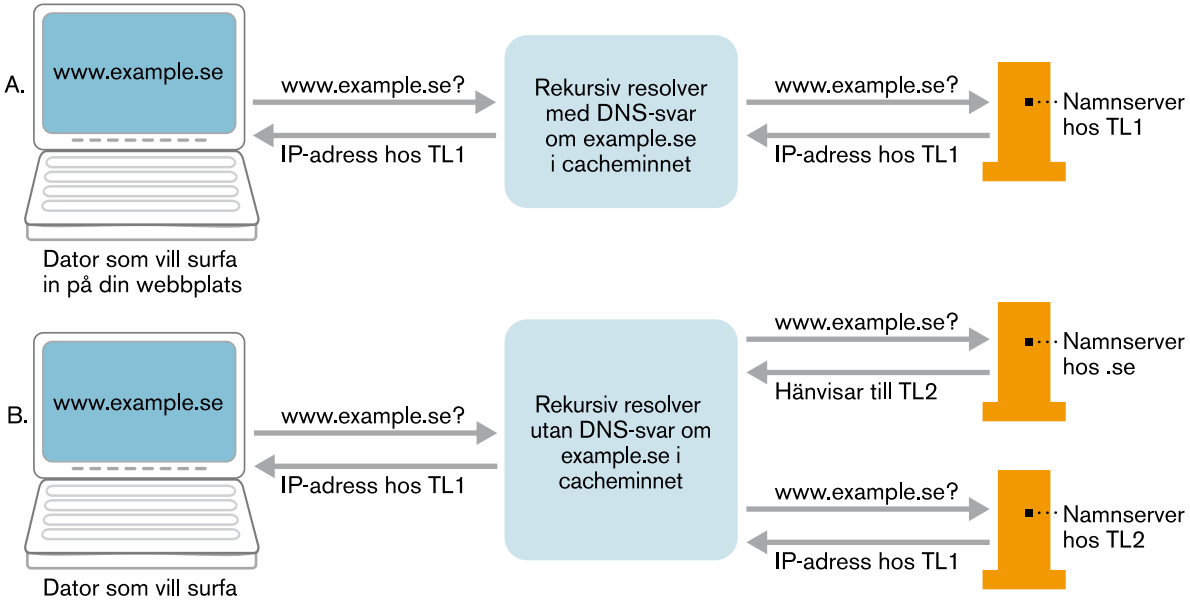
2. **Den nya DNS-tjänsten konfigureras med bibehållna tjänster**
   All DNS-data för domännamnet begärs ut från TL1. Går det inte att få ut uppgifterna från TL1 kan man också få fram dem med hjälp av verktyget *dig*. Sedan konfigureras DNS-tjänsten hos TL2 med samma uppgifter, förutom vad gäller den auktoritativa namnservern (NS-posten) som ska vara TL2:s. Denna namnserver kommer då under övergången att peka till IP-adresserna för webb- och e-postservrarna hos TL1. På så vis kommer tjänsterna att fungera även under den tid det tar för alla rekursiva resolvrar att få de nya DNS-uppgifterna, vilket är beroende av de TTL-värden som .SE och TL1 har satt för sina respektive zoner.

3. **Test av den nya DNS-tjänsten**
   Ett så kallat ”odelegerat domäntest” med .SE:s tjänst DNSCheck (som finns på http://dnscheck.iis.se) säkerställer att den auktoritativa namnservern hos TL2 är redo att svara på DNS-frågor om domännamnet.

4. **Registrering av ny auktoritativ namnserver hos .SE**
   Ska man byta registrar för domännamnet görs detta genom att en särskild kod begärs ut från TL1 (ifall detta är den gamla registraren) och ges till TL2 (den nya registraren). TL2 ser då till att registrera den nya auktoritativa namnservern för domännamnet hos .SE, alternativt ger instruktioner kring hur detta ska göras. När det har genomförts inleds övergången till den nya auktoritativa namnservern. Om man inte ska byta registrar,

utan har .SE Direkt som registrar och endast vill byta namnserveroperatör, så används i stället .SE Direkts domänhanterare för att ange ny namnserver.

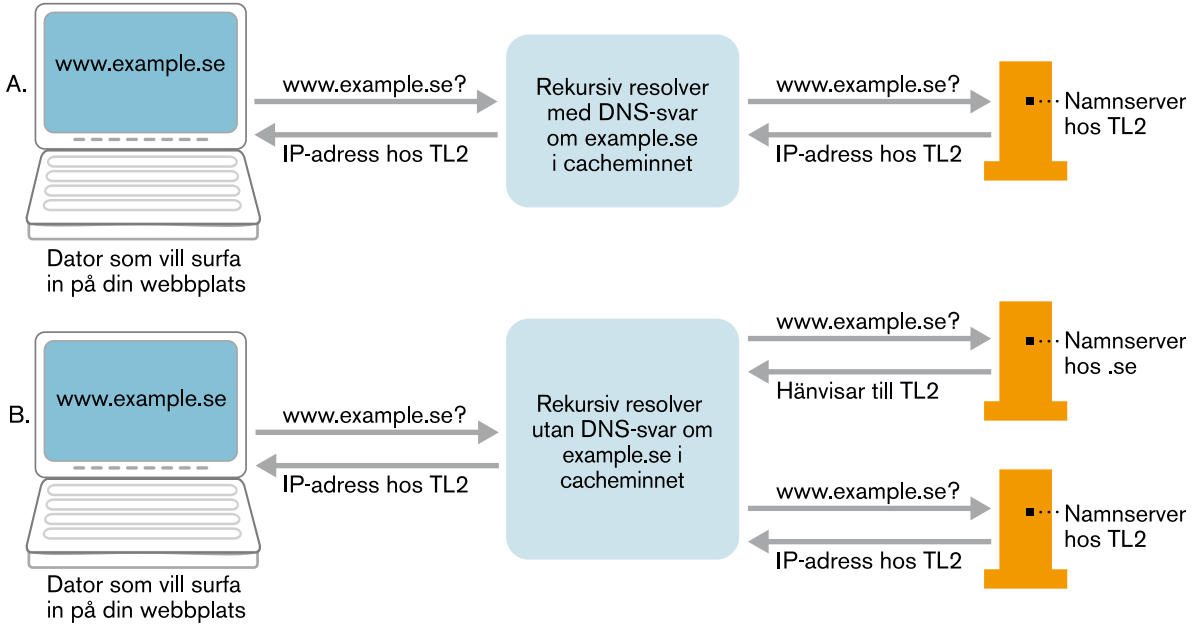
5. **Test av att .SE har rätt information**
Efter tre timmar har .se-zonen uppdateras. Då kan man med hjälp av .SE:s tjänst DNSCheck (som finns på http://dnscheck.iis.se) kontrollera att DNS-svaren innehåller rätt information. Förutom vad gäller NS-posten ska den auktoritativa namnservern hos TL2 tills vidare tillhandahålla exakt samma uppgifter som namnservern hos TL1. Om så ej är fallet, ska TL2 rätta till felaktigheterna.



Figur 10. DNS-uppslagning under ompekning. Resolvrar med mellanlagrade DNS-svar (Fall A) ställer frågan till den auktoritativa namnservern hos TL1. Andra resolvrar (Fall B) frågar .SE:s namnserver och hänvisas då till TL2. För minimal nedtid ska både TL1 och TL2 svara med IP-adresser hos TL1 under övergången.

6. TTL ska ta slut

Under övergången kommer den auktoritativa namnservern hos TL1 att fortsätta svara på DNS-uppslagningar från rekursiva resolvrar som har lagrat tidigare DNS-svar i sitt cacheminne. Allt eftersom tiden går kommer dock de mellanlagrade uppgifternas TTL att ta slut. Då begär den rekursiva resolvern ett nytt svar om domännamnet från en av .SE:s auktoritativa namnservrar som hänvisar frågan till namnservern hos TL2. TTL för .se-zonen är 24 timmar och om TL1 inte har längre TTL än så (vilket är föga troligt) så kommer samtliga rekursiva resolvrar att hänvisa till TL2 efter 24 timmar.



Figur 11. DNS-uppslagning när ompekningen är slutförd. Både resolvrar med mellanlagrade DNS-svar (Fall A) och andra resolvrar (Fall B) hänvisas till den auktoritativa namnservern hos TL2 som svarar med de nya IP-adresserna hos TL2.

7. **Webb- och e-posttjänster flyttas till TL2**
   Nu kan DNS-tjänsten hos TL2 konfigureras om så att den pekar ut IP-adresser för webb- och e-postservrar hos TL2 i stället för TL1. Den enda nedtid som då krävs för webbplats och e-post är den TTL som ställdes in innan ompekningen startades, det vill säga 1–5 minuter.

8. **Samtliga tjänster hos TL1 stängs ned**
   När TTL har tagit slut hamnar alla DNS-förfrågningar hos TL2 och därför kan nu alla tjänster hos TL1 avslutas.

9. **TTL återställs**
   När flytten är klar återställs TTL för tjänsterna hos TL2 till det tidigare värdet. Nu har ompekningen genomförts med minimal nedtid.

Typfall 2 – Domännamn med DNSSEC-signering

1. **TTL minskas**
   Om tjänsteleverantören tillåter det, ska TTL för tjänsterna hos TL1 minskas till en väldigt kort period, 1–5 minuter. På detta vis kommer flytten av webb- och e-posttjänster att gå snabbt när den genomförs. Det ska göras först av allt för att förändringen ska hinna slå igenom innan flytten sker. Om befintlig TTL hos TL1 bedöms som tillräckligt kort kan detta steg hoppas över.

2. **DS-nycklar tas bort**
   Registraren för domännamnet (TL1 eller .SE Direkt) ska ta bort den DS-nyckel som är producerad hos .SE. Om detta inte görs kommer ompekningen att få till följd att DNSSEC-svaren från TL2 går sönder. Signeringen av zonen behöver däremot inte stängas av. Zonen blir dock oskyddad under själva ompekningen. Utvecklingsarbete pågår för att detta ska kunna undvikas i framtiden.

3. **Den nya DNS-tjänsten konfigureras med bibehållna tjänster**
   All DNS-data för domännamnet begärs ut från TL1. Går det inte att få ut uppgifterna från TL1 kan man också få fram dem med hjälp av verktyget *dig*. Sedan konfigureras DNS-tjänsten hos TL2 med samma uppgifter, förutom vad gäller den auktoritativa namnservern (NS-posten) som ska vara TL2:s. Denna namnserver kommer då under övergången att peka till IP-adresserna för webb- och e-postservrarna hos TL1. På så vis kommer tjänsterna att fungera även under den tid det tar för alla rekursiva resolvrar att få de nya DNS-uppgifterna, vilket är beroende av de TTL-värden som .SE och TL1 har satt för sina respektive zoner.

4. **Zonen signeras hos TL2**
   När DNS-tjänsten etableras hos TL2 ska zonen signeras med DNSSEC även här.

5. **Test av den nya DNS-tjänsten**
   Ett så kallat ”odelegerat domäntest” med .SE:s tjänst DNSCheck (som finns på http://dnscheck.iis.se) säkerställer att den auktoritativa namnservern hos TL2 är redo att svara på DNS-frågor om domännamnet.

6. **Registrering av ny auktoritativ namnserver hos .SE**
   Ska man byta registrar för domännamnet görs detta genom att en särskild kod begärs ut från TL1 (ifall detta är den gamla registraren) och ges till TL2 (den nya registraren). TL2 ser då till att registrera den nya auktoritativa namnservern för domännamnet hos .SE, alternativt ger instruktioner kring hur detta ska göras. När det har genomförts inleds övergången till den nya auktoritativa namnservern. Om man inte ska byta registrar, utan har .SE Direkt som registrar och endast vill byta namnserveroperatör, så används i stället .SE Direkts domänhanterare för att ange ny namnserver.

7. **Test av att .SE har rätt information**
   Efter tre timmar har .se-zonen uppdateras. Då kan man med hjälp av .SE:s tjänst DNSCheck (som finns på http://dnscheck.iis.se)

kontrollera att DNS-svaren innehåller rätt information. Förutom vad gäller NS-posten ska den auktoritativa namnservern hos TL2 tills vidare tillhandahålla exakt samma uppgifter som namnservern hos TL1. Om så ej är fallet, ska TL2 rätta till felaktigheterna.

8. **TTL ska ta slut**
   Under övergången kommer den auktoritativa namnservern hos TL1 att fortsätta svara på DNS-uppslagningar från rekursiva resolvrar som har lagrat tidigare DNS-svar i sitt cacheminne. Allt eftersom tiden går kommer dock de mellanlagrade uppgifternas TTL att ta slut. Då begär den rekursiva resolvern ett nytt svar om domännamnet från en av .SE:s auktoritativa namnservrar som hänvisar frågan till namnservern hos TL2. TTL för .se-zonen är 24 timmar och om TL1 inte har längre TTL än så (vilket är föga troligt) så kommer samtliga rekursiva resolvrar att hänvisa till TL2 efter 24 timmar.

9. **Webb- och e-posttjänster flyttas till TL2**
   Nu kan DNS-tjänsten hos TL2 konfigureras om så att den pekar ut IP-adresser för webb- och e-postservrar hos TL2 i stället för TL1. Den enda nedtid som då krävs för webbplats och e-post är den TTL som ställdes in innan ompekningen startades, det vill säga 1–5 minuter.

10. **Samtliga tjänster hos TL1 stängs ned**
    När TTL har tagit slut hamnar alla DNS-förfrågningar hos TL2 och därför kan nu alla tjänster hos TL1 avslutas.

11. **Den nya DS-posten skickas till .SE**
    Den DS-post som skapats genom signeringen av zonen hos TL2 skickas till .SE. Då produceras en ny DS-nyckel hos .SE och zonen är återigen skyddad.

12. **TTL återställs**
    När flytten är klar återställs TTL för tjänsterna hos TL2 till det tidigare värdet. Nu har ompekningen genomförts med minimal nedtid.

13. **Gör en sista kontroll**

Efter ett par timmar, när samtliga TTL:er hos TL2 har återgått till det normala och den nya DS-posten har publicerats, kan det vara lönt att en sista gång testa att allt står rätt till med hjälp av DNSCheck (http://dnscheck.iis.se).

Appendix B – Samtliga (aktiva) toppdomäner på Internet

Generiska toppdomäner

aero	Avsett för flygbolag (begränsad registrering)
arpa	Avsett för infrastruktur på Internet (begränsad registrering)
asia	Avsett för webbplatser i Asien (begränsad registrering)
biz	Avsett för affärsverksamheter
cat	Avsett för webbplatser på katalanska eller som har att göra med katalansk kultur
com	Avsett för kommersiella syften
coop	Avsett för kooperativ verksamhet (begränsad registrering)
edu	Avsett för utbildningsinstitutioner (begränsad registrering)
gov	Avsett för USAs federala och delstatliga regeringar och myndigheter (begränsad registrering)
info	Avsett för informationssajter
int	Avsett för internationella organisationer (begränsad registrering)
jobs	Avsett för platsannonser
mil	Avsett för USAs väpnade styrkor (begränsad registrering)
mobi	Avsett för mobilt anpassade webbplatser (begränsad registrering)
museum	Avsett för museer (begränsad registrering)
name	Avsett för privatpersoner
net	Avsett för nätverksorganisationer
org	Avsett för organisationer
pro	Avsett för läkare, avokater och revisorer (begränsad registrering)
tel	Avsett för webbplatser för Internetkommunikation (begränsad registrering)
travel	Avsett för rese- och turistindustrin (begränsad registrering)

Toppdomäner för IDN-tester

xn--0zwm56d	IDN-toppdomän för tester med förenklad kinesiska
xn--11b5bs3a9aj6g	IDN-toppdomän för tester med hindi
xn--80akhbyknj4f	IDN-toppdomän för tester med ryska
xn--9t4b11yi5a	IDN-toppdomän för tester med koreanska
xn--deba0ad	IDN-toppdomän för tester med jiddisch
xn--g6w251d	IDN-toppdomän för tester med traditionell kinesiska
xn--hgbk6aj7f53bba	IDN-toppdomän för tester med persiska
xn--hlcj6aya9esc7a	IDN-toppdomän för tester med tamilska
xn--jxalpdlp	IDN-toppdomän för tester med grekiska
xn--kgbechtv	IDN-toppdomän för tester med arabiska
xn--zckzah	IDN-toppdomän för tester med japanska

Nationella toppdomäner

ac	Ascension
ad	Andorra
ae	Förenade Arabemiraten
af	Afghanistan
ag	Antigua & Barbuda
ai	Anguilla
al	Albanien
am	Armenien
an	Nederländska Antillerna
ao	Angola
aq	Antarktis
ar	Argentina
as	Amerikanska Samoa
at	Österrike
au	Australien
aw	Aruba
ax	Åland
az	Azerbajdzjan
ba	Bosnien & Hercegovina
bb	Barbados
bd	Bangladesh
be	Belgien
bf	Burkina Faso
bg	Bulgarien
bh	Bahrain
bi	Burundi
bj	Benin
bm	Bermuda
bn	Brunei
bo	Bolivia
br	Brasilien
bs	Bahamas
bt	Bhutan
bv	Bouvetön (oanvänd)
bw	Botswana
by	Vitryssland
bz	Belize
ca	Kanada
cc	Kokosöarna
cd	Kongo-Kinshasa (Demokratiska republiken Kongo)
cf	Centralafrikanska republiken
cg	Kongo-Brazzaville (Republiken Kongo)
ch	Schweiz
ci	Elfenbenskusten
ck	Cooköarna
cl	Chile
cm	Kamerun
cn	Kina
cr	Costa Rica
cs	Serbien och Montenegro (inaktuell efter landets splittring)
cu	Kuba
cv	Kap Verde
cx	Julön
cy	Cypern
cz	Tjeckien
de	Tyskland
dj	Djibouti
dk	Danmark
dm	Dominica
do	Dominikanska republiken
dz	Algeriet
ec	Ecuador
ee	Estland
eg	Egypten
er	Eritrea
es	Spanien
et	Etiopien
eu	Europeiska unionen
fi	Finland
fj	Fiji
fk	Falklandsöarna
fm	Mikronesiska federationen
fo	Färöarna
fr	Frankrike
ga	Gabon
gb	Storbritannien (oanvänd, i stället används uk)
gd	Grenada
ge	Georgien

gf	Franska Guyana
gg	Guernsey
gh	Ghana
gi	Gibraltar
gl	Grönland
gm	Gambia
gn	Guinea
gp	Guadelope
gq	Ekvatorialguinea
gr	Grekland
gs	Sydgeorgien
gt	Guatemala
gu	Guam
gw	Guinea-Bissau
gy	Guyana
hk	Hongkong
hm	Heard- & McDonaldsöarna
hn	Honduras
hr	Kroatien
ht	Haiti
hu	Ungern
id	Indonesien
ie	Irland
il	Israel
im	Isle of Man
in	Indien
io	Brittiska territoriet i Indiska oceanen
iq	Irak
ir	Iran

is	Island
it	Italien
je	Jersey
jm	Jamaica
jo	Jordanien
jp	Japan
ke	Kenya
kg	Kirgizistan
kh	Kambodja
ki	Kiribati
km	Komorerna
kn	Saint Kitts & Nevis
kp	Nordkorea
kr	Sydkorea
kw	Kuwait
ky	Caymanöarna
kz	Kazakstan
la	Laos
lb	Libanon
lc	Saint Lucia
li	Liechtenstein
lk	Sri Lanka
lr	Liberia
ls	Lesotho
lt	Litauen
lu	Luxemburg
lv	Lettland
ly	Libyen
ma	Marocko
mc	Monaco

md	Moldavien
me	Montenegro
mg	Madagaskar
mh	Marshallöarna
mk	Makedonien
ml	Mali
mm	Myanmar (Burma)
mn	Mongoliet
mo	Macao
mp	Nordmarianerna
mq	Martinique
mr	Mauretanien
ms	Montserrat
mt	Malta
mu	Mauritius
mv	Maldiverna
mw	Malawi
mx	Mexiko
my	Malaysia
mz	Moçambique
na	Namibia
nc	Nya Kaledonien
ne	Niger
nf	Norfolkön
ng	Nigeria
ni	Nicaragua
nl	Nederländerna
no	Norge
np	Nepal
nr	Nauru

nu	Niue
nz	Nya Zeeland
om	Oman
pa	Panama
pe	Peru
pf	Franska Polynesien
pg	Papua Nya Guinea
ph	Filippinerna
pk	Pakistan
pl	Polen
pm	Saint Pierre & Miquelon (oanvänt)
pn	Pitcairnöarna
pr	Puerto Rico
ps	Palestina
pt	Portugal
pw	Palau
py	Paraguay
qa	Qatar
re	Réunion
ro	Rumänien
rs	Serbien
ru	Ryssland
rw	Rwanda
sa	Saudiarabien
sb	Salomonöarna
sc	Seychellerna
sd	Sudan
se	Sverige
sg	Singapore
sh	Sankt Helena
si	Slovenien
sj	Svalbard (oanvänt)
sk	Slovakien
sl	Sierra Leone
sm	San Marino
sn	Senegal
so	Somalia (oanvänt)
sr	Surinam
st	São Tomé & Príncipe
su	Sovjetunionen (finns kvar trots att landet inte gör det)
sv	El Salvador
sy	Syrien
sz	Swaziland
tc	Turks & Caicosöarna
td	Tchad
tf	Franska sydterritorierna
tg	Togo
th	Thailand
tj	Tadzjikistan
tk	Tokelauöarna
tl	Östtimor
tm	Turkmenistan
tn	Tunisien
to	Tonga
tp	Östtimor (landets tidigare toppdomän)
tr	Turkiet
tt	Trinidad & Tobago
tv	Tuvalu
tw	Taiwan
tz	Tanzania
ua	Ukraina
ug	Uganda
uk	Storbritannien
us	USA
uy	Uruguay
uz	Uzbekistan
va	Vatikanstaten
vc	Saint Vincent & Grenadinerna
ve	Venezuela
vg	Brittiska Jungfruöarna
vi	Amerikanska Jungfruöarna
vn	Vietnam
vu	Vanuatu
wf	Wallis- & Futunaöarna (oanvänt)
ws	Samoa
ye	Jemen
yt	Mayotte (oanvänt)
yu	Jugoslavien (finns kvar trots att landet inte gör det)
za	Sydafrika
zm	Zambia
zw	zimbabwe

Appendix C – Ordlista

A-post – A = *Address* – DNS-post som anger den IPv4-adress som motsvarar ett visst domännamn.

AAAA-post – AAAA = *Address* x 4 – DNS-post som anger den IPv6-adress som motsvarar ett visst domännamn.

Auktoritativ namnserver – Namnserver som tillhandahåller DNS-information om en viss zon.

BIND – BIND = *Berkeley Internet Name Domain* – Den vanligaste namnserverprogramvaran som används för både auktoritativa namnservrar och resolvrar.

Cacheförgiftning – Angrepp där en cachande namnserver förmås spara ett felaktigt svar på en DNS-uppslagning i sitt cacheminne och sedan lämnar falska svar på DNS-frågor.

Cachning – När en namnserver tillfälligt lagrar svar som den får från en annan namnservrar i ett cacheminne.

Chain of trust – En tillitskedja som om man följer den gör det möjligt att kontrollera att den digitala signatur som följer med ett DNS-svar när DNSSEC används har skapats av rätt nyckel.

Delegering – När ansvaret för att tillhandahålla DNS-information kring en underdomän läggs på någon annan och zonfilen hänvisar till denna andra auktoritativa namnserver angående den underdomänen.

dig – Ett programverktyg genom vilket man kan låtsas vara resolver, ställa frågor om DNS och få fram DNS-informationen för en domän i klartext.

Djbdns – En namnserverprogramvara som används för både auktoritativa namnservrar och resolvrar.

DNS – DNS = *Domain Name System* – Internets domännamnssystem, en hierarkisk och distribuerad databas som gör det möjligt att snabbt hitta information om vilken IP-adress (och annan information) som är kopplad till ett domännamn.

DNSSEC – DNS = *Domain Name System Security Extensions* – Säkerhetstillägg till DNS som säkrar systemet mot missbruk som cacheförgiftning genom att DNS-data signeras digitalt.

DNS-poster – Informationen om varje domännamn bryts i zonfilen ned i ett antal DNS-poster som utgör svar på olika frågor om domännamnet.

DNS-träd – Modell som används för att förklara hur informationen i DNS är organiserad, som ett omvänt träd som förgrenar sig nedåt från roten.

DNS-uppslagning – Process genom vilken man i DNS når fram till informationen om vilken IP-adress som motsvarar ett domännamn (samt annan information).

Domän – En delmängd av DNS-trädet, benämns med ett domännamn.

Domännamn – Benämningen av en nod i domännamnrymden.

Domännamnrymden – Trädstrukturen för ett domännamnssystem i sin helhet, i fallet Internet innefattar den alla domäner på hela Internet.

DS-post – DS = *Delegation Signer* – DNS-post som finns om en domän har signerats med DNSSEC och som talar om att domänen är signerad och vilken nyckel som signerar den.

Frågande namnserver – Se *Rekursiv resolver*.

Fulregistrering – Registrering i ond tro av ett domännamn som till exempel ligger nära ett varumärke, företagsnamn eller dylikt.

Fully qualified domain name (FQDN) – Ett domännamn som namnger en unik nod i domänträdet. Ett exempel är www.example.se. som anger både rot (.), toppdomän (se), huvuddomän (example) och nodnamn (www).

Generisk toppdomän – Toppdomän som (ursprungligen) inte är kopplad till en nation eller geografisk region, utan i stället sammankopplas med specifika aktiviteter eller typer av organisationer (till exempel .com, .net och .org).

Huvuddomän – Vanlig benämning på den domän som ligger närmast under toppdomänen (exempelvis example i example.se).

ICANN – ICANN = *Internet Corporation for Assigned Names and Numbers* – Den institution som har det övergripande ansvaret för DNS. Bland annat ansvarar man för innehållet på Internets rotnamnservrar och för att delegera ansvaret för toppdomänerna.

IDN – IDN = *Internationalized Domain Name* – Domännamn som innehåller tecken utöver a–z, 0–9 och ”-”).

IDNA – IDNA = *Internationalized Domain Names in Applications* – System som gör det möjligt att använda tecken utöver a–z, 0–9 och ”-” i domännamn.

IMAP – IMAP = *Internet Message Access Protocol* – Protokoll som används för att hämta meddelanden från en e-postserver.

in-addr.arpa – Domän som kartlägger alla använda publika IPv4-adresser i en trädstruktur så att det går att göra omvända DNS-uppslagningar i IPv4.

IP – IP = *Internet Protocol* – Det mest grundläggande protokollet som används för datakommunikationen på Internet och som delar upp och kapslar in informationen i IP-paket.

ip6.arpa – Domän som kartlägger alla använda IPv6-adresser i en trädstruktur så att det går att göra omvända DNS-uppslagningar i IPv6.

IP-adress – Unik nummerserie som identifierar varje dator på Internet (eller i vilket IP-nätverk som helst) så att IP-paketen som skickas över nätet hamnar rätt.

IP-paket – De beståndsdelar som information bryts ned i när den skickas över ett IP-nätverk.

IPv4 – IPv4 = *Internet Protocol version 4* – Den version av IP som använts mest fram till i dag, där IP-adresserna består av 32 bitar och det därför kan finnas max drygt fyra miljarder adresser.

IPv6 – IPv6 = *Internet Protocol version 6* – En ny version av IP, där IP-adresserna består av 128 bitar och antalet möjliga adresser blir oerhört stort.

Kaminskybuggen – En brist i DNS som gör det enkelt att utföra en cacheförgiftning.

Microsoft DNS – En namnserverprogramvara som används för både auktoritativa namnservrar och resolvrar.

MX-post – MX = *Mail Exchanger* – DNS-post som anger en e-postserver för en domän.

Namnserver – Programvara som används för att göra information tillgänglig i DNS samt för att få fram denna information, både auktoritativa namnservrar och rekursiva resolvrar kallas ibland bara namnservrar.

Nationell toppdomän – Toppdomän som (ursprungligen) är kopplad till en nation eller geografisk region (till exempel .se, .dk och .eu).

Nod – Punkt i DNS-trädet som anges med ett domännamn.

nslookup – Ett programverktyg som ställer frågor om DNS och får fram DNS-informationen för en domän i klartext.

NS-post – DNS-post som specificerar en namnserver som är auktoritativ för en zon, annorlunda uttryckt pekar den ut vilken auktoritativ namnserver zonen är delegerad till.

Nätfiske – När man lockar in nätanvändare på en falsk webbplats som utger sig för att vara något annat i syfte att få användaren att uppge känsliga uppgifter som kreditkortsnummer eller lösenord.

Omvänd DNS-uppslagning – När man gör en uppslagning på en IP-adress för att få fram vilket domännamn den motsvarar.

Phishing – Se Nätfiske.

POP – POP = *Post Office Protocol* – Protokoll som används för att hämta meddelanden från en e-postserver.

Primär namnserver – Auktoritativ namnserver som hämtar zonfilen direkt från de interna systemen hos den institution som har ansvaret för zonen.

PTR-post – DNS-post som anger vilket domännamn som motsvarar en viss IP-adress och som används vid omvända DNS-uppslagningar.

Registrar – Auktoriserade återförsäljare av domännamn som även sköter administrationen av domännamnen.

Rekursiv resolver – Namnserver som används för att göra DNS-uppslagningar på Internet och därigenom (bland annat) få fram vilken IP-adress ett domännamn motsvarar.

Rotnamnserver – Auktoritativ namnserver för Internets rotzon, som tillhandahåller DNS-information om alla de olika toppdomänerna.

Sekundär namnserver – Auktoritativ namnserver som hämtar zonfilen från den primära namnservern eller en annan sekundär namnserver för zonen.

SMTP – SMTP = *Simple Mail Transfer Protocol* – Protokoll som används för att överföra e-post mellan datorer.

SOA-post – DNS-post som anger ett antal uppgifter om en zon och vem som ansvarar för den.

Stubb-resolver – Ett enkelt program som finns installerat på en dator och konfigureras för att ställa DNS-frågor till en rekursiv resolver som sedan i sin tur gör en DNS-uppslagning på Internet.

Svarande namnserver – Se *Auktoritativ namnserver*.

TLD – Top-Level Domain, se *Toppdomän*.

Toppdomän – En domän som hör till nivån närmast roten i DNS-trädet. Alla domännamn slutar på en toppdomän och vem som administrerar respektive toppdomän bestäms av ICANN.

TTL – TTL = *Time to live* – Värde som anges av den som ansvarar för en zon och som bestämmer hur länge ett DNS-svar ska sparas i resolverns cacheminne.

Unbound – En namnserverprogramvara som används för resolvrar.

Underdomän – Domän som ligger under en annan domän i trädstrukturen, till exempel är example.se en underdomän till .se-domänen.

Zon – Den del av en domän som inte har delegerats och som den auktoritativa namnservern för domänen måste tillhandahålla fullständig DNS-information om.

Zonfil – Textfil som innehåller all den DNS-information som finns om en zon. Zonfilen görs tillgänglig på Internet av zonens auktoritativa namnserver.

Zonöverföring – Processen genom vilken en zon överförs mellan auktoritativa namnservrar.

.SE (Stiftelsen för Internetinfrastruktur) är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige. Utöver att ansvara för Internets svenska toppdomän bedriver .SE ett omfattande utvecklingsarbete:

- **.SE:s Internetguider** är en skriftserie som riktar sig till intresserade lekmannaanvändare och behandlar olika Internetfrågor. Denna publikation ingår i serien. Läs mer: iis.se/se-ar-mer/ses-publikationer.
- **Webbstjärnan** är en tävling i webbpublicering för skolan. Syftet är att dra nytta av Internets möjligheter i skolarbetet, genom att bygga en webbplats kring ett valfritt skolarbete. Läs mer: webbstjärnan.se och stjärnkikarna.se.
- **Internet för alla.** .SE bidrar till olika åtgärder för att förbättra tillgängligheten till Internet för de grupper som idag inte är anslutna till nätet.
- **Pålitlig e-post**. .SE undersöker vad som kan göras för att öka säkerheten och förtroendet för e-post för både företag och privatpersoner.
- **IPv6 och DNSSEC** är två viktiga teknikprojekt som ska säkerställa att Internets infrastruktur även i fortsättningen kan vidareutvecklas och fungera säkert. Läs mer: ipv6forum.se respektive iis.se/domaner/dnssec/.
- **Bredbandskollen** är ett konsumentverktyg som hjälper bredbandskunder att utvärdera sin bredbandsuppkoppling. Läs mer: bredbandskollen.se
- **Internetstatistik** .SE har tagit initiativ för att etablera ett samarbete kring statistik och fakta om Internet, vilket bland annat resulterat i den tryckta rapporten Svenskarna och Internet. Läs mer: iis.se/se-ar-mer/ses-publikationer och internetstatistik.se.
- **Internetfonden** bidrar till Internetutvecklingen genom att finansiera fristående projekt. Bland uppdragstagarna finns organisationer, privatpersoner och akademiska institutioner. Läs mer: iis.se/se-ar-mer/internetfonden.
- **Internetdagarna** är .SE:s årligen återkommande konferens för alla som arbetar med Internet. Läs mer: internetdagarna.se

.se

Som en del i .SE:s arbete med Internetutveckling producerar .SE ett antal skrifter under produktnamnet .SE:s Internetguider. Guiderna behandlar olika Internetrelaterade områden och riktar sig i första hand till intresserade lekmannaanvändare. En guide kan vara såväl en praktisk handbok som en mer beskrivande rapport.

.se

Stiftelsen för Internetinfrastruktur