Domain Name System – DNS

- Det här kapitlet behandlar DNS översiktligt. Det är ett utdrag ur ett mer omfattande kapitel i boken. Hur vi klarade oss innan DNS behandlas. Namnstrukturer och toppdomäner gås igenom. Hur DNS-frågor görs och hur svaren mellanlagras och behandlas.
- Kapitlet är tänkt att kunna läsas fristående men fungerar bäst om du vet hur TCP/IP fungerar.

DNS är ett protokoll för att i ett globalt nätverk av DNS-servers kunna ställa frågor och få svar. Om den aktuella servern inte känner till svaret så kan den svara med en hänvisning till en annan server istället. Program för DNS och protokollet har funnits i tjugo år och fungerar enligt samma principer. Två saker krånglar till det om du vill förstå DNS:

- användningen och begreppen har ändrats med tiden. Eftersom DNS fungerar väl globalt så finns det grupper som vill lägga in fler och fler funktioner i strukturen.
- I Windows används också begreppet domäner. Från början hade Windows-domäner ingenting med DNS att göra, men med Windows Server 2000 och senare 2003 används DNS även för detta. Tanken är att förenkla men eftersom de flesta organisationer inte vill visa sin interna struktur externt så blir det i alla fall komplext. (Tanken med DNS var från början att alla DNS:er ska kunna fråga varandra.)

I det här kapitlet utgår vi från dagens begrepp och hur grundfunktionerna i DNS används. DNS kan även användas för lastdelning och det kan användas för dynamiska uppdateringar då en nod byter IP-adress (Dynamic DNS enligt RFC 2136). Det finns även ett tillägg DNSSEC med vars hjälp man kan upptäcka förfalskade DNS-data. Dessa funktioner behandlas dock inte i detta kapitel.

Så här långt har guiden mest handlat om IP-adresser. Men de flesta användare använder inte IP-adresser utan kommer bara i kontakt med nodnamn. I den här guiden används benämningen nodnamn, på engelska används ofta begreppen ”host name”. I DNS används begreppet domännamn (domain name) vilket även omfattar namn som www.bolag.se. Ett mer exakt begrepp är det engelska FQDN, Fully Qualified Domain Name. Jag har använt begreppet komplett domännamn eller FQDN nedan för att sär-

Nodnamn (host name) och domännamn (domain name) är två olika saker. FQDN är ett namn som fungerar i DNS-strukturen och kan närmast översättas med komplett domännamn.

skilja det från nodnamn (det är inte ovanligt att en dator har FQDN som www.bolag.se medan nodnamnet speglar maskinens uppbyggnad som 2GXeonDuo).

Hosts-filen

Internet och TCP/IP har en gång fungerat utan DNS men i praktiken kan vi inte vara utan det idag. I stort sett alla TCP/IP-implementationer har kvar den tidiga metoden i form av en hosts-fil. I Windows XP nås den under C:\WINDOWS\system32\drivers\etc. I filen finns i princip två kolumner, den högra är nyckeln till det vi letar med. När vi får träff så kontrolleras vad som står till vänster. Om vi till exempel skriver in sekvensen ”x.acme.com” i en webbläsare så fungerar i stort sett alla program så att de använder proceduren ”gethostbyname”. Och från hosts-filen kan vi då erhålla resultatet 38.25.63.10.

```
102.54.94.97     rhino.acme.com          # source server
38.25.63.10      x.acme.com              # x client host

127.0.0.1        localhost
```

Du kan enkelt testa hur hosts-filen fungerar. I de flesta Linux-varianter kan man välja om DNS ska användas i första hand eller om hosts-filen ska användas. I Windows används hosts-filen i första hand.


Testa själv

Ta reda på en IP-adress som används och styr ett komplett domännamn som www.kth.se till denna IP-adress via ett tillägg till hosts-filen. Mata sedan in domännamnet i en webbläsare. Du kommer att styras enligt hosts-filen. Även efter att denna ändring tas bort ur hosts-filen ligger denna information kvar ett tag, detta beror på att man mellanlagrar DNS-information (alltså även i en vanlig arbetsstations resolver).

Namnstrukturer

DNS inför två stora förändringar jämfört med hosts-filer. För det första blir det svårt att genomföra globala förändringar om varje dator har en lokal fil. Under Internets tidiga år gjorde man så att det fanns en masterfil som användare kunde hämta regelbundet.

Men den här modellen håller inte om vi kräver att ändringar ska slå igenom fort och kunna hantera miljontals användare. DNS hämtar istället bara den information som behövs, och den hämtas när den behövs. En nyckel till att hantera informationen effektivt är sedan att svar mellanlagras (cachas).

DNS hämtar bara den information som behövs och informationen mellanlagras.

DNS införde dessutom en namnstruktur. Tidigare hade varje nod ofta ett enkelt namn som rhino eller alma. Men om det nu fanns två servers med samma namn. Vem är mest alma om två universitet hade samma datornamn? Och hur ska vi hantera alla maskiner som har namn som anknyter till funktioner, typ mailserver, postman, webserver och nameserver?

Ett komplett domännamn innehåller normalt minst tre nivåer. Två exempel är www.firma.se och mail.bolag.com. Detta kallas som sagt ett FQDN och utläses i det första fallet som noden ”www” i domänen ”firma.se”. Ett komplett domännamn går hela vägen från den enstaka noden ända upp till roten (ibland understryker man detta genom att lägga till en extra punkt som refererar till roten, till exempel ”www.firma.se.”). Ett komplett domännamn går ofta att översätta till en IP-adress, men det är ofta intressant att ställa andra frågor än bara IP-adresser. Vi kan till exempel fråga vilken nod som är ansvarig för domänen, vi kan fråga om det finns en e-post server med mera.

Toppdomäner

Sedan länge har toppdomänerna funnits i två varianter. Nationella toppdomäner som se, no och de samt generiska som com och net. De generiska utökades under 2000 till 2002 och omfattar idag:

Nationella toppdomäner betcknas ofta ccTLD’s: Country Coded Top Level Domains. De generiska betecknas gTLD’s: Generic Top Level Domains.

Toppdomän	Tillkom	Anm
.aero	2002	Flygfartsindustri
.arpa		För infrastruktur och fanns i princip innan DNS. Används bland annat för baklänges-uppslagning.
.biz	2001	Jämför med .com
.com	1985	Kommersiella bolag (den mest använda toppdomänen)
.coop	2002	
.edu	1985	Utbildningsväsende
.gov	1985	Amerikansk statsförvaltning (governmental)
.info	2001	
.int	1988. Stängdes 2000.	Internationella organisationer, bland annat drivet av önskemål från NATO.
.mil	1985	Amerikansk militär
.museum	2001	För museer
.name	2002	Individer
.net	1985	"Network support Centers". Tillsammans med "com" en av de toppdomäner som det varit lättast att registrerar namn på.
.org	1985	Övriga organisationer. Tillsammans med "com" en av de toppdomäner som det varit lättast att registrera namn på.
.pro	2004	Professionals. Am begrepp som bland annat omfattar läkare och advokater.

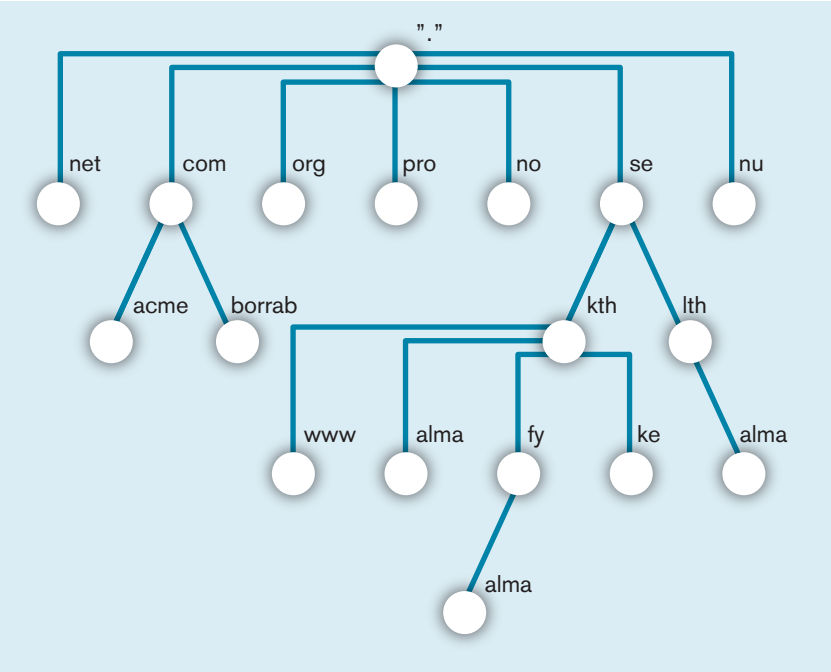
Toppdomännamn.

Under 2007 är fler nya domäner på gång som cat, jobs, mobi, travel. Andra förslag är mail och tel.

Generiska toppdomäner styrs av ICANN. Hur de används har styrts av riktlinjer för respektive domän. De nationella subdomänerna har fungerat olika i olika länder. I England har de till exempel ofta använt subdomäner som co och ac under sin toppdomän uk. Amerikanska bolag använde sällan domänen us utan de generiska. I Sverige var man under 1990-talet väldigt restriktiv men utdelning under ".se" och krävde registrerade varumärken, föreningar eller aktiebolag. Enskilda firmor registrerades under länsbokstäver (detta harmonierar med hur bolagsnamnen hanteras). Från 2003 gäller dock principen först till kvarn under .se-domänen och konflikter löses i efterhand.

Eftersom det under 90-talet var enklare att registrera com, net och org-domäner så blev de ofta populära och till och med svenska statliga utredningar dök upp under com-domänen. Under 1990-talet började även namnpirater att registrera organisatoriska domäner eller vanliga felslagningar av populära domäner för att sälja dem vidare. Den praktiska lösningen på detta blev att sökmotorer används oftare eftersom vi inte vet om vi ska söka på "bolag.com"

eller ”bolag.net” eller ”bolagab.se”. Och i princip kan den som administrerar en domän bara styra hur subdomäner till just den domänen delas ut.

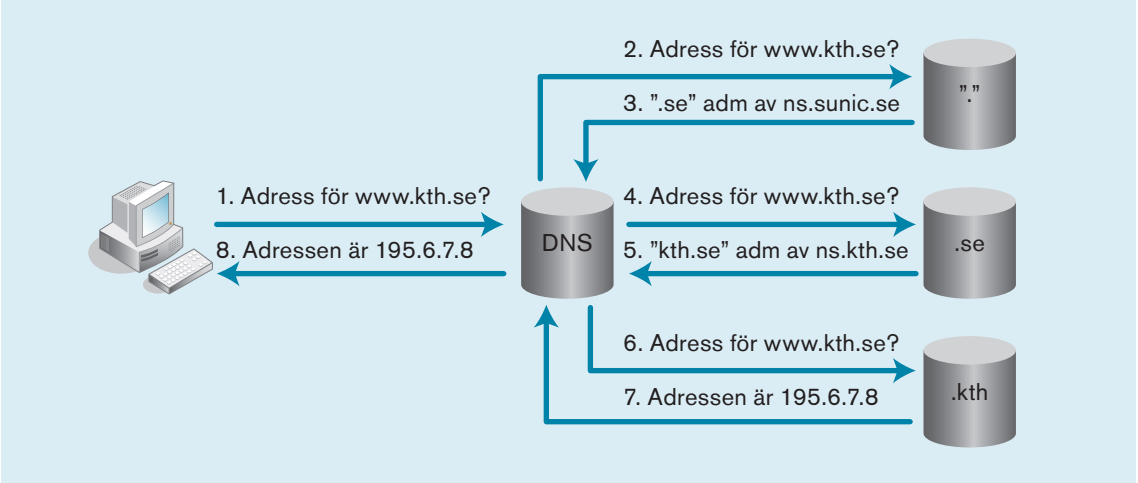


Toppdomäner högst upp följs av subdomäner.

Med toppdomäner och en namnstruktur får vi ordning på namnen så att de blir unika. Vi kan skilja på alma.kth.se och alma.lth.se. Högst upp (det vi kallar roten ologiskt nog) har vi alla namn. De så kallade rotservrarna känner sedan till de knappt 300 toppdomänerna och vilka namnservrar som har vidare information. Poängen är sedan att de hänvisar till dessa servrar för mer information. På samma sätt kan ett par maskiner vara ansvariga för se-domänen, men de innehåller främst information om varje subdomän som registreras och vilken namnserver som har informationen. Om vi granskar domänen kth.se så ser vi att det finns två noder vid namn www och alma. Däremot är fy och troligen även ke subdomäner som delegeras vidare. I DNS-strukturen hanteras enkla nodnamn och domäner på samma sätt. Från namnen i sig kan vi inte se att www är en nod och ke är en subdomän. (Det finns dock ett antal konventioner som till exempel www för en server som svarar på port 80 och ns för den nod som hanterar domäner.) Därför skulle vi få meddelandet ”Non Existing Domain” förkortat som NXDOMAIN om vi frågade efter det felaktiga ww.kth.se.

Resolvers

En vanlig arbetsstation eller PC innehåller en liten DNS-resolver. Applikationer skickar som sagt en uppkopplingsbegäran med kommandot gethostbyname. DNS-resolvern på din PC löser detta men den tar hjälp av en fullödig DNS. Denna skiljer sig från din PC:s enkla på så sätt att den kan ställa rekursiva frågor. Ur PC:ns synpunkt ställs frågan till en DNS (1) och strax efter kommer svaret (8).



Stora DNS:er kan ställa rekursiva frågor.

En DNS har en tabell med IP-adresser till de 13 rotservrar som finns globalt. Frågan skickas till en av dessa. Rotservern svarar (3) med att den är just rotserver, men den här frågan avseende se-domänen är delegerad till en (eller fler) servrar. Till DNS-protokollet hör också möjligheten att lägga till extra information för att minska antalet frågor, så ett fält "additional information" innehåller information om IP-adressen till ns.sunic.se. Vår DNS skickar nu frågan till ns.sunic.se (4) som svarar att information om kth.se har delegerats vidare. Eventuellt sker liknande delegering en eller två gånger till men tillslut hamnar vi hos en DNS som är ansvarig för denna domän. Denna svarar med IP-adressen för www.kth.se (7). Vår DNS kan nu leverera svaret till vår PC-klient (8). Hemligheten med DNS är alltså att servrarna hela tiden delegerar frågan till någon som vet. Gott ledarskap alltså.

Svaren från en DNS innehåller även tidsvärden (Time To Live). Detta gör att svaren kan mellanlagras och här ligger mycket av effektiviteten. Nästa gång vår DNS behöver fråga om något som avser hela se-domänen så vet den att den kan skicka frågan till ns.sunic.se. Rotservern behöver inte belastas igen. Om en annan klient skickar samma fråga till vår DNS så kan den direkt svara

med IP-adressen. Hur länge svaren ska sparas kan variera. Typiska värden kan vara 8 till 24 timmar. Kortare och längre värden förekommer, till exempel brukar rotservrarna meddela att svar vad gäller toppdomäner kan mellanlagras i sju dygn.

Eftersom svar mellanlagras tar det tid innan ändringar slår igenom. Vill man byta IP-adress på en maskin bör man först ställa ner tidsvärdet så den lagras kort tid och sedan genomföra förändringen. Har man sin DNS utlagd till en operatör tar det även tid innan de genomför förändringen, speciellt om man ska byta vilken server som är ansvarig för en domän, en så kallad domain transfer. Felaktiga ändringar får stort genomslag och säkerhetsmässigt vill operatörerna vara säkra på att den som begär flytt och ändringar är behörig. Ändringar kompliceras också ofta av att fler servrar blandas in.

Eftersom DNS är en viktig del av Internet behövs redundans. Om du försökt registrera en ny domän så har du säkert fått frågan om vilka maskiner som ansvarar för domänen. Det räcker inte med att ange en adress utan två. Förr användes begreppen primary och secondary DNS dessa har idag ersatts av master och slave. En master-DNS kan ha flera slave-DNS. Det är master-DNS som innehåller informationen i original och slave-DNS kollar regelbundet efter förändringar och hämtar vid behov uppdaterad information. Överliggande domän har normalt vetskap om två eller fler servers så DNS-frågorna kan besvaras utan att vara beroende av enstaka servrar.

Fråga och svar

Nedan visas en inspelning av ett paket till och från en DNS-server. UDP och port 53 används som väntat.

För att kunna matcha svar med fråga används en identitet (2 byte). Sedan följer 16 bitar som används för flaggor, här kan vi se att det är en standardfråga och DNS-servern förväntas använda en rekursiv sökning. I övrigt består en DNS-fråga av fyra delar: question (fråga), answer (svar), authority (behörighet) och additional (tillägg). Efter flaggorna följer information om huruvida dessa delar används och deras antal. I detta fall följer en fråga och den byggs upp. Frågan innehåller vår söknyckel samt två fält: typ och klass. Klassen är enkel då den i praktiken alltid är IN, det vill säga Internet. Typen av fråga varierar. Det finns cirka 50 olika posttyper (type) definierade varav några av de vanligaste är:

Typ	Förklaring	Anm
A	Host Adress	IP-adress
NS	Name Server	Namn på authoritative server
PTR	Pointer	För baklängesuppslagning
SOA	Start Of Authority	Administrativ information för en domän
CNAME	Canonical Name	Alias, används för att t ex styra www.bolag.se till 2GXeon.bolag.se
MX	Mail eX-changer	Används för e-post. Namnservrar frågar om det finns en MX-server för en viss domän.

Några vanliga post-typer.

Paket 158

Ethernet II, Src: Fujitsu_c3:2f:98, Dst: 3comEuro_9f:4a:fa
Internet Protocol, Src: 192.168.3.245, Dst: 192.168.3.1
User Datagram Protocol, Src Port: 1633 (1633), Dst Port: domain (53)
  Source port: 1633 (1633)
  Destination port: domain (53)
  Length: 46
  Checksum: 0x2217 [correct]
Domain Name System (query)
  Transaction ID: 0x0006
  Flags: 0x0100 (Standard query)
    0... .... = Response: **Message is a query**
    .000 0... .... = Opcode: **Standard query** (0)
    .... ..0. .... = Truncated: Message is not truncated
    ....1 .... = Recursion desired: Do query recursively
    .... .0.. .... = Z: reserved (0)
    ....0 .... = Non-authenticated data OK
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
      Name: www.mittbolag.se
      Type: A (Host address)
      Class: IN (0x0001)

I svaret ser vi inte bara själva IP-adressen utan också information om hur länge svaret kan mellanlagras (TTL Time To Live). Vi ser också att den server som svarat inte är ansvarig (authority) för domänen. Servern svarar också med att den tillåter rekursiva frågor.

Paket 159
Ethernet II, Src: 3comEuro_9f:4a:fa, Dst: Fujitsu_c3:2f:98
Internet Protocol, Src: 192.168.3.1, Dst: 192.168.3.245
User Datagram Protocol, Src Port: domain (53), Dst Port: 1633 (1633)
Domain Name System (response)
[Request In: 148]
[Time: 0.029266000 seconds]
Transaction ID: 0x0006
Flags: 0x8180 (Standard query response, No error)
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative:
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available:
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 0
Queries
www.mittbolag.se: type A, class IN
Name: www.mittbolag.se
Type: A (Host address)
Class: IN (0x0001)
Answers
www.mittbolag.se: type A, class IN, addr 130.239.8.25
Name: www.mittbolag.se
Type: A (Host address)
Class: IN (0x0001)
Time to live: 9 hours, 21 minutes, 58 seconds
Data length: 4
Addr: 130.239.8.25

Om man använder kommandot ”dig” i Unix för att felsöka i DNS får man svar som stämmer väl med hur DNS-frågor och svar ser ut. Om allt går bra erhålls svaret NOERROR, vid problem får man ofta meddelandet NXDOMAIN samt information om från vilken DNS som svarat detta. På detta sätt kan man se hur långt namnupplösningen fungerade.

Baklängesuppslagning

DNS-strukturen kan användas åt andra hållet. Vi kan allstå få svar på frågan ”Om vi har en IP-adress vad motsvarar det för domännamn?” Baklängesuppslagning görs av flera applikationer i samband med loggning, felsökning och verifiering. DNS bygger på att den mest signifikanta delen finns till höger (med början i toppdomänen). IP-adresser har den mest signifikanta delen till vänster så man löser upp adresser från vänster till höger. En konvention är att man har reserverat domänen ”in-addr.arpa” för baklängesuppslagning. Normalt tar DNS och även verktyg som nslookup och dig hand om detta själv. Vill vi veta domännamnet för exempelvis 192.3.4.5 så kommer själva frågan ha formen ”5.4.3.192.in-addr.arpa” men det slipper vi som användare oftast tänka på.

Säkerhet och DNS

DNS är en vital del av Internet och strukturen har utsatts för flera attacker, främst mot rotservrarna. Hittills har angriparna inte lyckats och Internet skulle inte sluta fungera om en rotserver slogs ut. (De flesta frågorna till rotservrarna är fel delvis beroende på manuella felstavningar.)

Men DNS är känsligt och med ett lite mindre perspektiv kan en angripare ställa till med mycket. I en dåligt skyddad DNS kan någon ändra informationen så att frågor efter till exempel www.internetbank.se styrs till fel ställe. På samma sätt kan ett virus ändra i hosts-filen. Dessa metoder har använts historiskt för angrepp. Ytterligare ett sätt är att bygga ett litet program som lyssnar efter DNS-frågor och sedan skickar ett snabbt felaktigt DNS-svar. Det spelar då ingen roll att rätt svar kommer senare, DNS-klienten tar det första svaret.

För att förbättra situationen med DNS så finns en förbättrad variant som heter DNSsec. I DNSsec används digitala signaturer för att verifiera svaren.

Information från DNS-servrar har också kunnat användas vid attacker. Angripare hämtar information från en DNS och ser vilka servrar som har intressanta namn och får direkt information om dess IP-adress. Den mest använda programvaran för DNS-servrar, BIND, har historiskt sett haft flera brister som har rättats till.

Referenser

RFC 1034 och 1035	DNS
www.iis.se	Information .se-domänen Här finns även viss information om DNSsec.
www.isc.org	ISC utvecklar programmet BIND, en populär DNS-server. Manualen till BIND ger en bra bild av modern DNS.