

### **Vad är en auktoritativ namnserver?**

en auktoritativ namnserver är en dns server som ansvarar för uppslagningar(queries) i en domän.

### **Vad är alternativet till en auktoritativ namnserver**

Recursive resolvers, root namnserver, TLD namnserver är bland dem alternativa namnservrar.

### **Är det skillnad mellan en domän och en zon? Vilken skillnad isåfall?**

Ja, en domän är en mängd maskiner som tillhör en domän medan en zone är en samling av många domäner.

### **Vad innebär rekursiv slagning? Iterativ? Hur vet DNS-servern du frågar om det är en rekursivt ställd fråga?**

I rekursiv slagning en DNS server kommer att rekursivt leta efter klientens query till den hittar svaret. Om den inte själv vet svaret innebär det att den kommunicerar med andra DNS servrar. I andra hand iterativt uppslagning innebär att om dns servern inte vet själv svaret till uppslagningen kommer den att guida klienten till bäst dns server som den tror att har svaret.

### **I DNS delegerar vi ansvaret för olika zoner. Varför?**

Det är för att den gör DNS mer funktionellt då man kan utse administratör för varje zon vilket förbättrar dennes prestanda.

**Ovan beskriver vi hur man kommer fram till att liu.se har adressen 130.236.18.52 (och hela delegerings-hierarkin från root till auktoriteten för .se-domänen, till liu.se). Hur sker en uppslagning "åt andra hållet", där man vill slå upp om adressen 130.236.18.52 motsvarar någon webbadress (enligt din DNS-server)? Du kan vilja läsa om reverse DNS.**

Den använder sig av **reverse DNS lookup** vilket är ett slagning verktyg av DNS som kan avgöra domännamn som hör till en IP adress på baklänges sätt.

Kör dig **www.liu.se**, vilket bör ge outputen:

**1. Förklara kortfattat vad de olika delarna av utskriften innebär.**

Första delen innehåller information om vår uppslagning. Man kan se om den har lyckats hitta ett svar. I andra delen så ser man svaret. I vårt fall namnet på domänen som är "[www.liu.se](http://www.liu.se)" visas först. I andra kolumnen ser man TTL (time to live) som innebär hur länge den får spara svaret innan den skickar en ny uppslagning. I tredje kolumnen ser man klassen av uppslagningen som är IN (internet) och i fjärde kolumnen hittar man typen av uppslagningen "A" (som står för adress) och i sista kolumnen ser man ip adressen.

**2. När du gör en query som till exempel dig ANY liu.se @ns4.liu.se kan du få flera olika sorters resource records (RR) tillbaka. Vad ska A-, AAAA-, NS-, MX- och SOA-records innehålla?**

**A** är det DNS record som innehåller adressen som pekar på IP adress vilket använder IPv4 protocol.

**AAAA** är det DNS record som innehåller adressen som pekar på IP adress vilket använder IPv6 protocol.

**NS** är ett av de viktigaste DNS records som avgör namnservrar för en givet domän.

**MX** är också ett av de viktigaste DNS records som avgör de mailservrar som är ansvariga för mejlhantering för en given domän.

**SOA** är det DNS record som pekar på auktoritativ namnserver för en given domän.

**Kör dig `+trace www.google.com` och förklara kortfattat vad som står.**

Det visar en sökväg på hur det har lyckats hitta ip adressen för google.com. Den börjar från servrar som är ansvariga för root domänen “.”. I nästa steg frågar den servrar som har ansvar för “.com” och till slut hittar den servrar som kan ip adressen för [www.google.com](http://www.google.com).

## Konfiguration av er namnserver

### Hur sätter man önskad DNS-server på Linux:

Vi skriver både alternativen här då vi har tolkat frågan olika.

#### Alternativ 1:

För att sätta önskad DNS-server ändrar man följande fil med godtycklig namnserver:

```
nano /etc/resolv.conf
```

#### Alternativ 2:

Först och främst måste man ha DNS server (**bind9**) installerat i systemet. Det gör man med kommandot:

```
apt-get install bind9
```

Sedan behöver man installera DNS utilities också med kommandot:

```
apt install dnsutils
```

Nu för att konfigurera DNS öppnar vi filen *named.conf.options* och lägger till Googles DNS för klarhets skull vilket är **8.8.8.8**.

```
nano /etc/bind/named.conf.options
```

Efter att vi har sparat filen startar vi om DNS för att aktivera den nya konfigurationen.

```
systemctl restart bind9
```

Man kan även kontrollera statuset på DNS med följande kommando:

```
systemctl status bind9
```

Medan bind9 körs, kan vi testa Googles domain med dig kommandot:

```
dig google.com
```

Nu för exempel vill vi konfigurera "svt.se" vilket vi behöver korrigera filen "named.conf.local".

```
nano /etc/bind/named.conf.local
```

Och lägger till följande:

```
zone "svt.se" {  
type master;  
file "/etc/bind/db.svt.se";  
};
```

Nu kopierar vi innehållet av "db.local" till "db.svt.se"

```
cp /etc/bind/db.local /etc/bind/db.svt.se
```

Efter de här ändringarna startar vi om DNS igen:

```
systemctl restart bind9
```

För att vår nyskapade domän ska kunna kommunicera med IP adresser måste vi skapa en reverse zone fil. Först öppnar vi filen:

```
nano /etc/bind/named.conf.local
```

Sedan lägger vi till följande rader:

```
zone "192.168.18.in-addr.arpa" {  
type master;  
file "/etc/bind/db.10";  
};
```

Nu kopierar vi innehållet av "db.127" till "db.10"

```
cp /etc/bind/db.127 /etc/bind/db.10
```

Nu för att bekräfta våra konfigurationer kör vi följande kommando och se om vi får något felmeddelande eller inte.

```
$ named-checkzone svt.se /etc/bind/db.svt.se
$ named-checkzone 192.168.0.0 /32 /etc/bind/db.10
$ named-checkconf /etc/bind/named.conf.local
$ named-checkconf /etc/bind/named.conf
```

### Vad är en SOA post? Vad innebär dess olika fält?

SOA (start of authority) lagrar alla viktiga information om en domän eller zon, till exempel administratörens mejladress, när var domänen uppdaterades sist och så vidare. Nedan är ett exempel på SOA:

name	example.com
record type	SOA
MNAME	ns.primaryserver.com
RNAME	admin.example.com
SERIAL	111111111
REFRESH	86400
RETRY	7200
EXPIRE	4000000
TTL	11200

**MNAME:** namn på primärt namnserver.

**RNAME:** Mailadressen av ansvariga personen för denna zone

**SERIAL:** är versionsnumret på SOA record.

**REFRESH:** tiden (i sekunder) sekundärt namnservrar skulle vänta på primärt namnservrar om SOA record är uppdaterade eller inte.

**RETRY:** specificerar tiden (i sekunder) som en server ska vänta innan den kan fråga en primärt namnserver för en uppdatering igen

**EXPIRE:** Om sekundärt namnserver får inget svar från primärt namnserver under den här tiden då skulle den sluta med att svara på uppslagningar.

**TTL:** Representerar tiden (i sekunder) om hur lång tid de skulle behålla data i cache. Detta värde (TTL) är sparad i samtliga uppslagningar.

### Hur kan man spara “resolv.conf” på ett permanent sätt?

```
/etc/dhcp/dhclient.conf
```

Sedan:

```
prepend domain-name-servers 10.0.0.4;
```

1. Nu har ni kallat er zon för gruppnamn.example.com. Finns det något i DNS-protokollet som hindrar att ni istället sade att ni var google och hade alla deras domäner? I någon utökning av protokollet? Om ni satte upp en falsk tjänst och pekade adressen gmail.com till den via era DNS-server, är det något i DNS eller annat protokoll som skulle hjälpa en användare som använder er DNS-server att upptäcka bluffen?

Nej, för att man inte har auktoritet att registrera domänen med top nivå servrar. Det sättet att hitta en domän görs via hierarki av servrar. Rotservrar avgör top nivå domän till exempel “dot.com”. Nästa nivå av servrar till “dot.com” bestämmer var den ska kolla för en specifik domän. Endast auktoriserat registrar kan uppdatera de här “andra nivå servrar”.

2. Nu har ni skrivit zonfiler. Om ni skulle delegera auktoritet för users.gruppnamn.example.com hade ni behövt lägga till några rader i er zonfil. Vilka, och varför? (Ni kan fundera på delegering av delar av reverse-zon, men utöver att lösningen blir ful, är det inte obligatoriskt.)

Om vi skulle delegera auktoritet för en subdomän då skulle vi behöva definiera vart den ligger och vad dennes IP adress är. Till exempel om vi hade subdomän som heter “test.saysahadan.exmaple.com” då hade vi behövt lägga till följande rader i “saysahadan.example.com” zonfil:

```
test.saysahadan.example.com. IN NS ns1.test.saysahadan.example.com.
ns1.test.saysahadan.example.com. IN A 10.0.0.5
```

### Motivering för konfiguration:

Alla relevanta filer är bifogade i mejlet.

Configfil	Motivering
resolv.conf	Här definieras namnserver (den konfigureras i alla maskiner)
named.conf.local	Här lägger vi till vår zon och reverse zon.(den ligger i server)
saysahadan.example.com	Här sätter vi upp SOA post (med inställningar för forward uppslagningar)
0.0.10.in-addr.arpa	Här sätter vi upp SOA post (med inställningar för reverse uppslagningar)
dhclient.conf	Här gör vi ändringar för att spara "resolv.conf" på ett permanent sätt.