# UppLYSning om DNS

**Måns Nilsson, KTHNOC/SUNET**

`mansaxel@sunet.se`

**20 mars, 2001**

# Underavdelningar

1. **DNS-systemet, en snabb översikt.**
2. **Drift av DNS, några goda råd.**
3. **Ny funktionalitet i DNS.**
4. **Organisation och politik runt domäner.**

# 1 DNS-systemet, en snabb översikt.

Vad är DNS?

- DNS är världens största distribuerade databas.
- Internet Standard, RFC1034 och 1035.
- En unik namnrymd.
- Tillåter uppslagning men inte sökningar.
- Distribuerad administration.

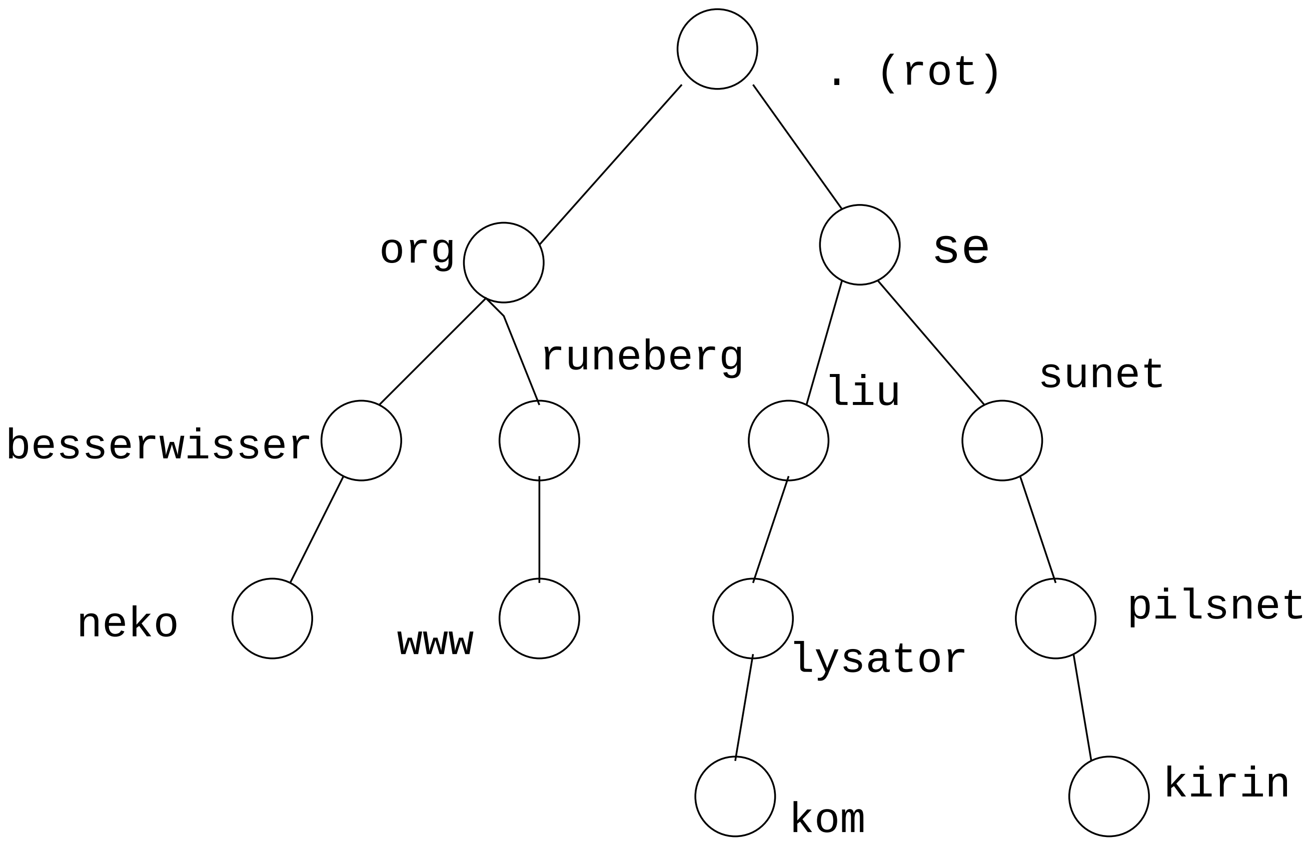
## 1.1 Historia

- I begynnelsen var `HOSTS.TXT`. Den hämtades med FTP en gång i veckan, och underhölls av en enda organisation.
- Detta skalade så klart inte. Man började designa ett distribuerat system, och kom fram till DNS.
- Systemet som det designades har visat sig skala mycket bra, och används alltjämt med mycket små ändringar.

## 1.2 Protokollet

- DNS pratar TCP och UDP på port 53.
- Blocka inte TCP/53 i eventuella filterburkar.
- TCP tar man till om man behöver stora datamängder, t e x zontransfer.
- Ett DNS-meddelande innehåller en header med statusdata och eller flera svarsdelar.

## 1.3 Ett exempelträd:



## 1.4 Posttyper i DNS

Data i DNS är uppställt i olika poster.

- SOA Start Of Authority. "Här börjar zonen". Nödvändig.
- NS Name Server. "Denna dator har zonen". Minst en.
- A Adress. Pekar namn till IP-adress.
- PTR PoinTeR. Pekar IP-adress till namn.
- CNAME Canonical NAME Alias, pekar till en annan nod.

## 1.5 Posttyper i DNS, forts..

- MX Mail eXchanger Postlåda för en nod.
- TXT TeXT Fritext om en nod.
- HINFO Host INFOrmation Beskriver OS och HW.
- SRV SeRVice Pekar ut var viss tjänst finns för en nod.
- KEY Nyckel Innehåller en nyckel, i samband med DNSSec.
- SIG SIGnature En signatur på en annan post.

## 1.6 Begrepp

- rot: Toppen på DNS-systemet.
- nod: En specifik punkt i trädet.
- label: Namndel – tex “sunic” i sunic.sunet.se.
- domän: Allt under en viss nod.
- delegering: Överlämning av ansvar nedåt.
- zon: En domän minus det som är delegerat vidare.

## Begrepp, forts..

- FQDN: Fully Qualified Domain Name, absolut namn; t ex `www.sunet.se.`
- rekursion: Iterativ uppslagningprocess i DNS-trädet.
- master: Den namnserver där uppdateringar görs för en zon.
- slav: En namnserver som svarar m h a data hämtat från master.
- cachning: Proceduren att spara allt man får reda på i en definerad tid.

## Begrepp, forts..

- namnserver: En server konfigurerad att svara på frågor om en eller flera zoner.
- uppslagsserver: En server konfigurerad att hjälpa till med uppslag åt dem som inte kan göra egen rekursion.
- auktoritet: Svar om en zon från en server som är konfigurerad med data från disk eller zontransfer.

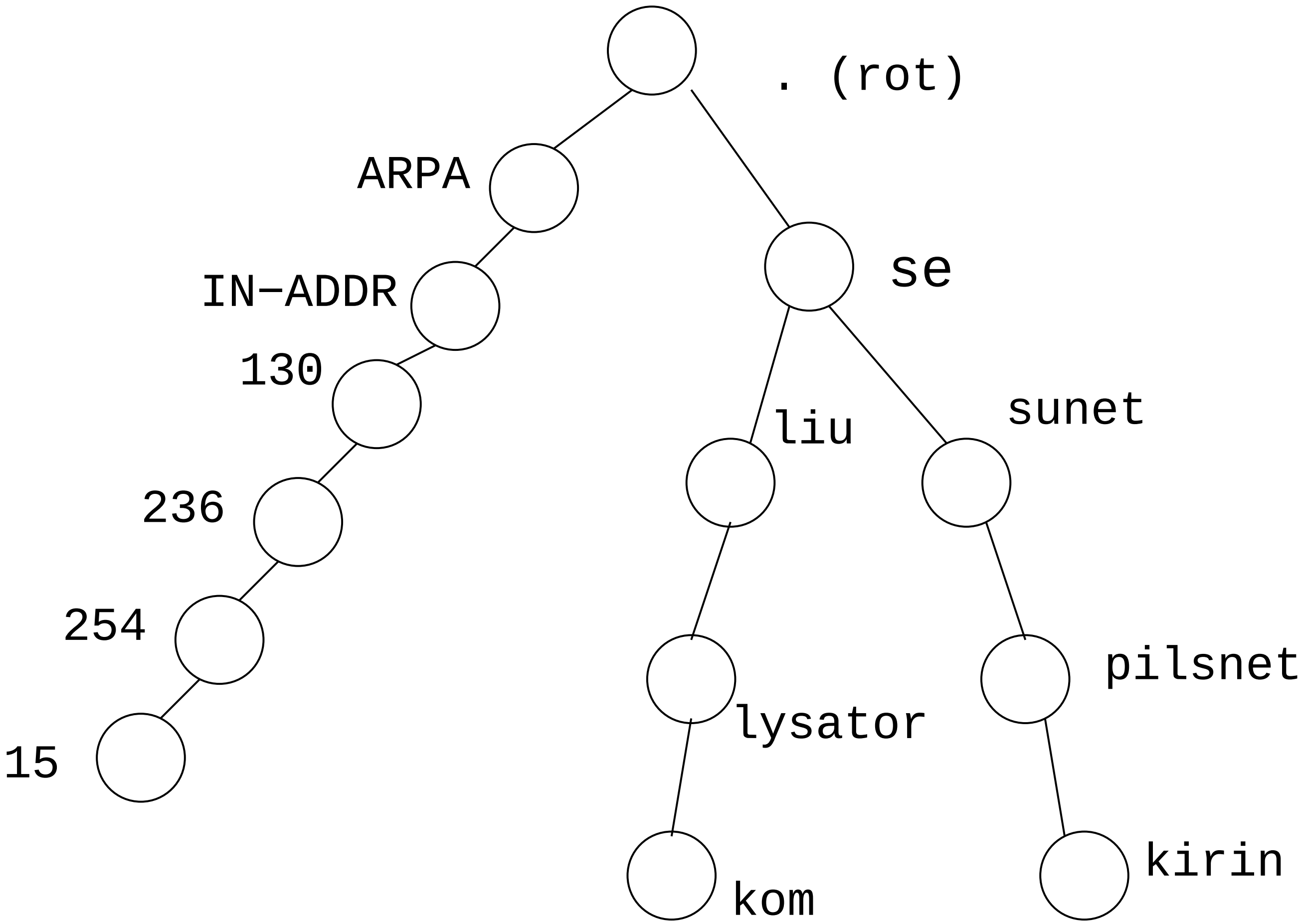
## 1.7 Delegeringsprocessen

- För varje zon måste det finnas en eller flera namnservrar.
- Namnservrar pekas på från moderzonen, och utgör en sammanbindande väg mellan zonerna.
- Om man pekar på servrar nere i den utpekade zonen måste man bootstrappa uppslagningen med *glue records*, för att kunna nå fram.
- NS och glue är det *enda* ur dotterzonen som får finnas i moderzonen.

## 1.8 Bakåtuppslag, kusinen från landet?

- Bakåtuppslag hjälper oss att hitta namnet när vi har IP-adressen.
- Vanligare att program använder bakåtuppslag i bakgrunden än direkt interaktivt bruk.
- Ofta styvmoderligt behandlat. Det är dumt. Bakåtuppslag är bra.
- Implementerat som en egen domänhierarki, IN-ADDR.ARPA.

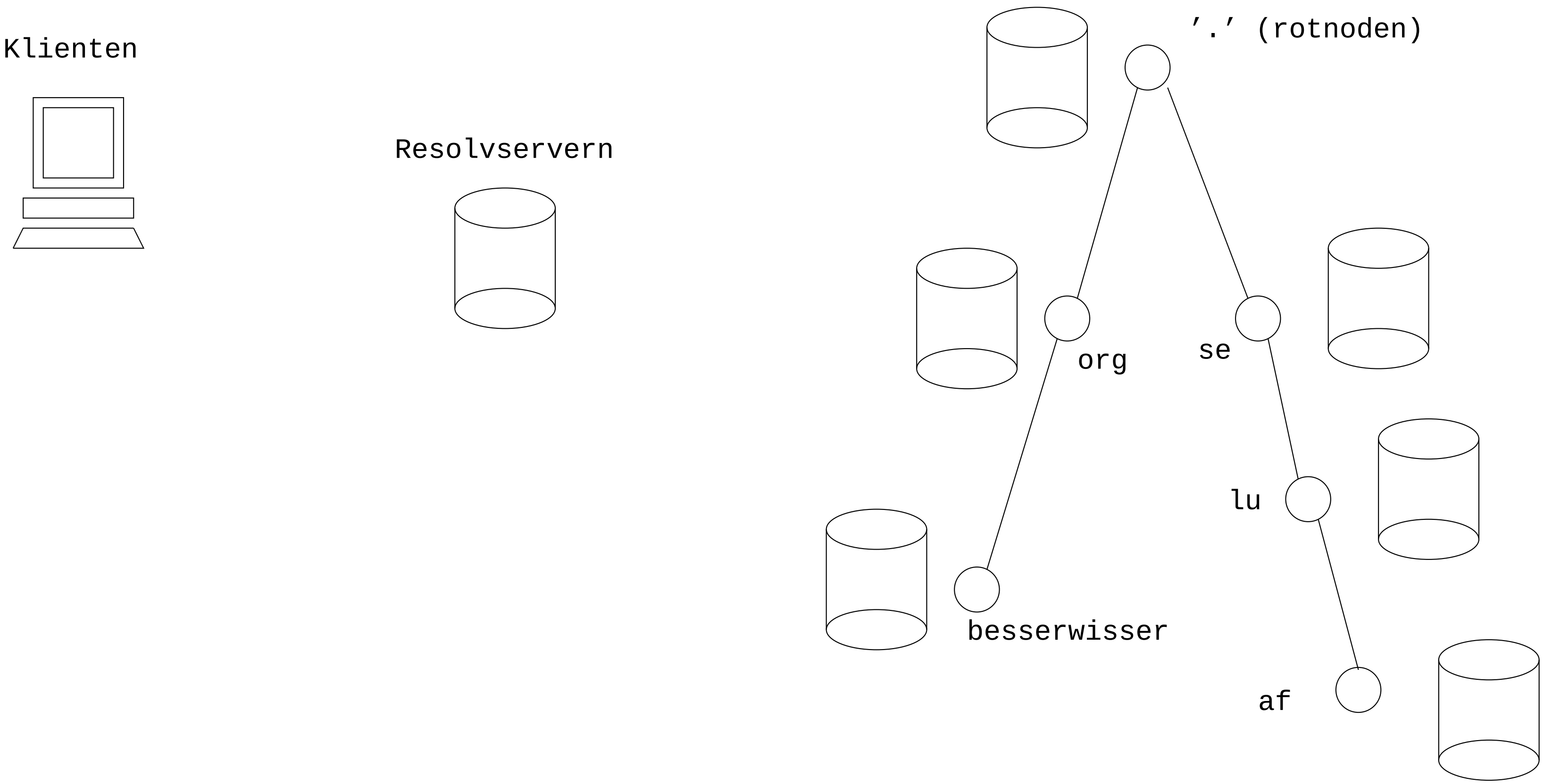
# Ett träd med IN-ADDR.ARPA



## 1.9 Rekursion

- Uppslagning i DNS sker nästan alltid med rekursion. Antingen gör man den själv, eller så ber man någon annan.
- För att kunna rekursera måste man först veta var toppen på DNS-trädet finns.
- Därför konfigurerar man i varje namnserver som ska kunna rekursera statiskt in listan över de namnservers som håller rot-zonen.

# Rekursiv uppslagsprocess



## 1.10 Programvara

- BIND Klart vanligast.
  <http://www.isc.org/products/BIND/>
- djbdns Uppstickare. Ovanlig.
  <http://cr.yp.to/djbdns.html>
- MS DNS Alltför vanlig :-)
  <http://www.microsoft.com/windows2000/library/howitworks/communications/nameadrmgmt/dnsover.asp?bPrint=True>

## 1.11 Debugprogram.

- `nslookup`: Använd inte nslookup! Det är alldeles för optimistiskt och hurtigt. Det kommer dessutom att försvinna från BIND-distributionen.
- `host`: Betydligt bättre som snabbverktyg.
- `dig`: DNS-teknikerns Hiltihammare. Berättar precis hur saker hänger ihop.

# 2 DNS-drift, ett par goda råd

- Namntjänst
- Uppslagstjänst
- Redundans, inte ögontjäneri

## 2.1 Vad blir fel?

Det vanligaste felet är att blanda ihop uppslags– och namntjänst.

Det är *mycket* olämpligt annat än för mycket små kontrollerade miljöer.

## Vad blir fel? – forts

Det näst vanligaste felet är att inte skapa system som är verkligt redundanta.

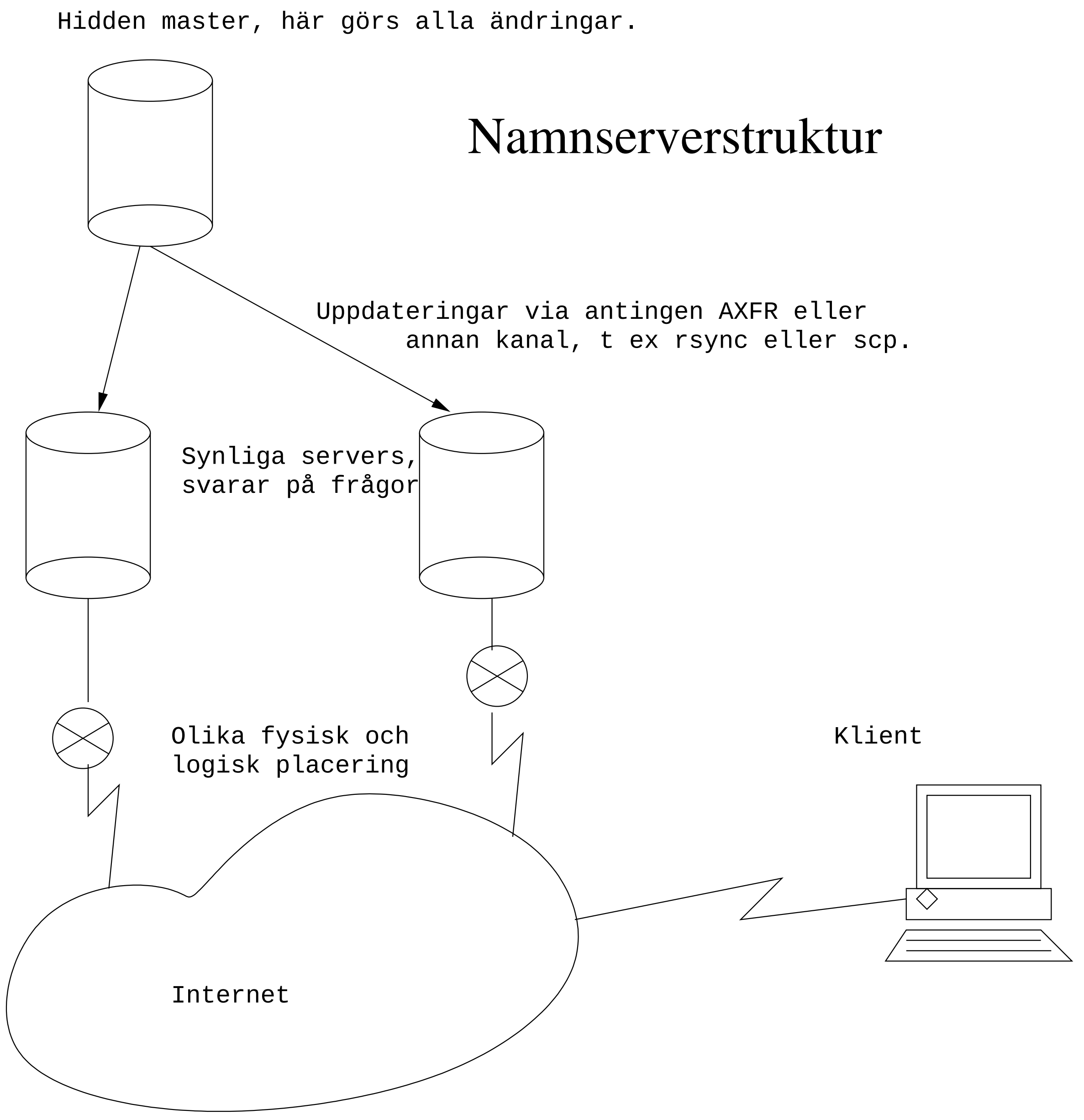
DNS är så lätt att göra redundant att man inte ska låta bli.

## 2.2 Namntjänst

Hur bygger man en skalbar och stabil namntjänst?

- Läs RFC1591, den är en bra vägvisare.
- Flera servers.
- Olika nät.
- Hidden master.
- Snabba uppdateringar med Notify (RFC1996).

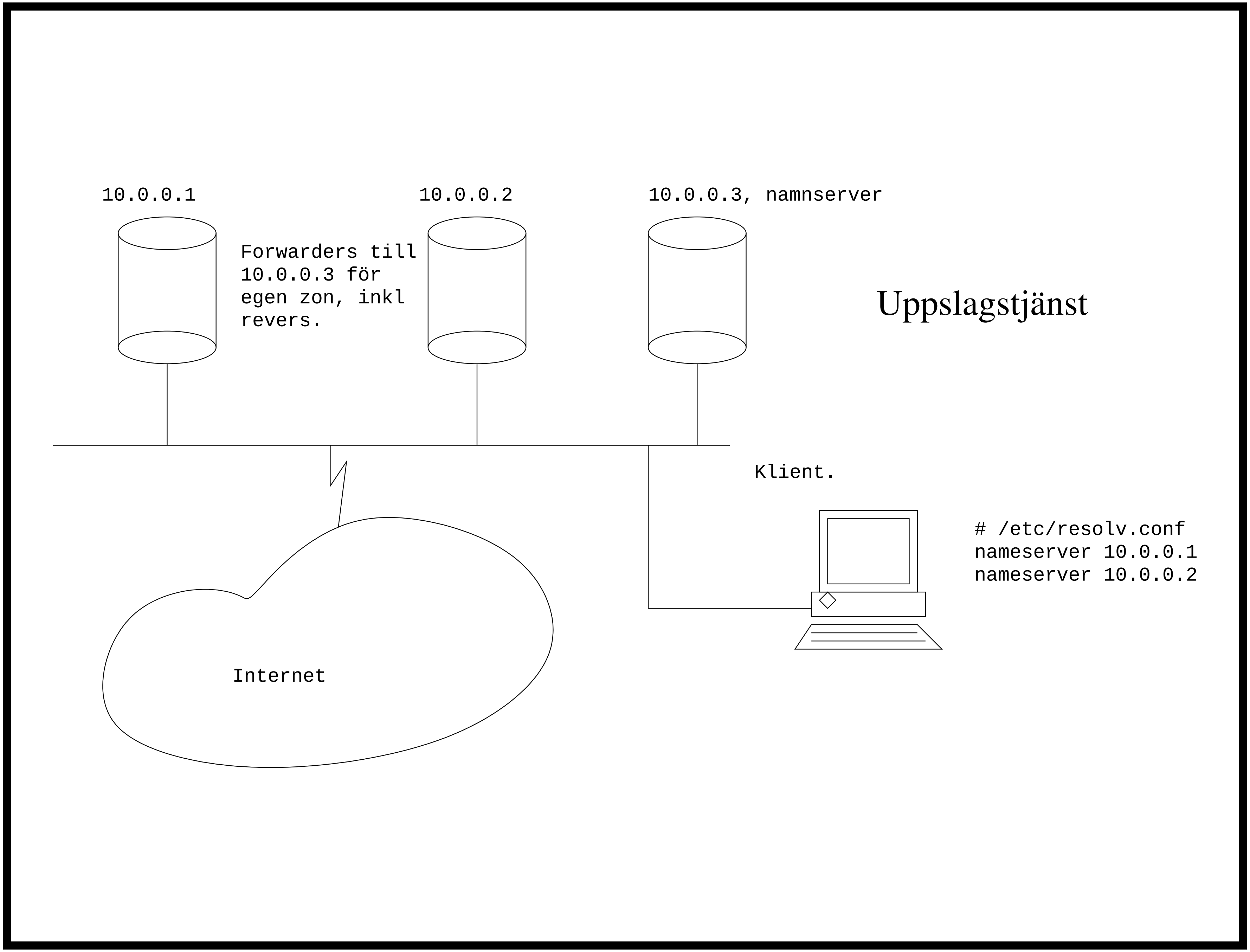
# Namnserverstruktur



## 2.3 Uppslagstjänst

Hur bygger man en pålitlig och korrekt resolvtjänst?

- Blanda *inte* ihop namn- och uppslagstjänst!
- Men man kan vilja ha stubzon till vissa saker.
- Lokala maskiner, gärna med forwarders om Internetförbindelsen är tunn.
- 127.0.0.1 är ju standard!


10.0.0.1
10.0.0.2
10.0.0.3, namnserver
Forwarders till
10.0.0.3 för
egen zon, inkl
revers.
Uppslagstjänst
Klient.
# /etc/resolv.conf
nameserver 10.0.0.1
nameserver 10.0.0.2
Internet

# 3 Ny funktionalitet i DNS

- DNSSec – Pålitliga data
- Internationella tecken – “åäö”

## 3.1 DNSSec

- Ett system för att sätta kryptografiska signaturer på DNS-data så att man kan verifiera dess korrekta ursprung.
- Data blir inte hemligt, bara validerbart!
- Definieras f n i RFC 2535, men är än så länge ett mycket rörligt mål.
- Något ytterligare lär (de)stabiliseras i och med IETF 50 som pågår denna vecka.

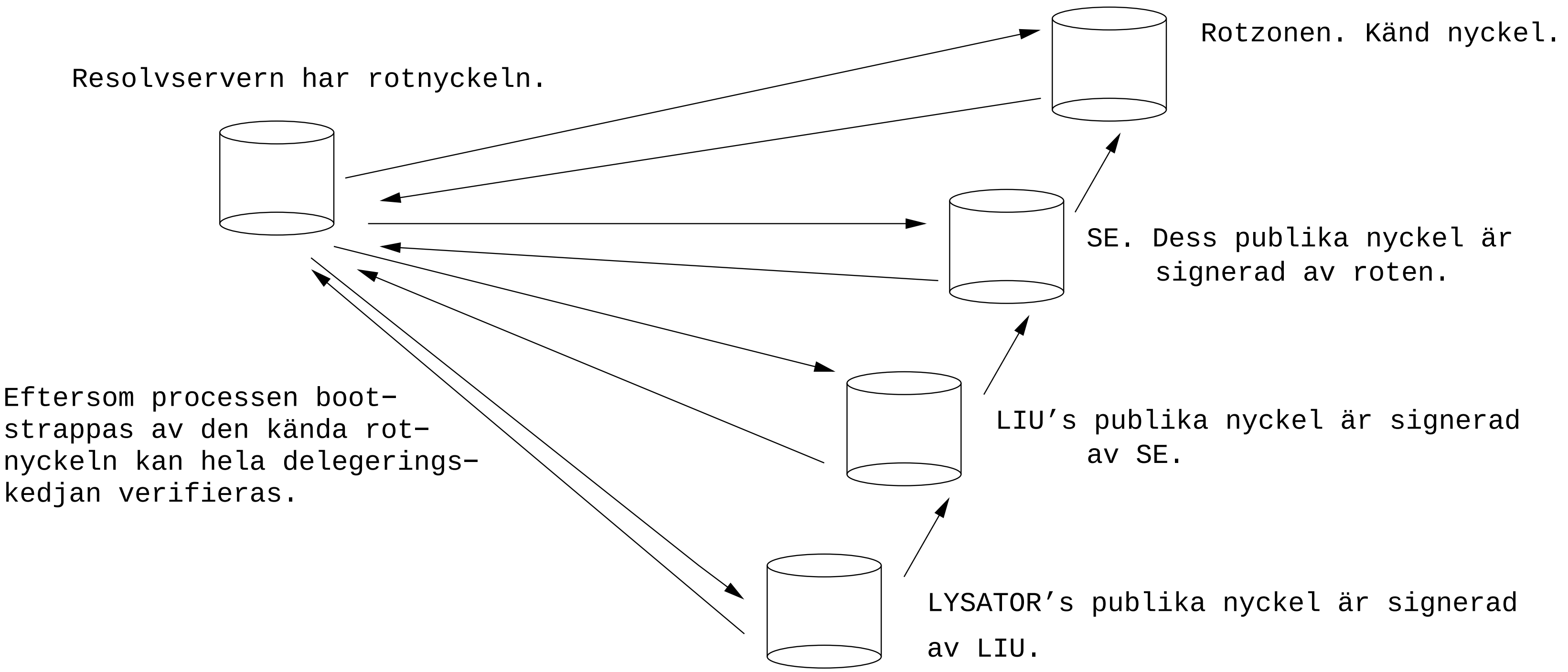
## Hur fungerar det?

- Bygger på privat/publik nyckel.
- Moderzon signerar dotterzons publika nyckel.
- Alla lagrar rotzonens publika nyckel (spridd out-of-band) och kan således verifiera svar eftersom varje rekurssionssteg åtföljs av signerade nycklar vilkas privata halvor signerat svaret.
- Man kan också lagra varandras nycklar för att kunna göra värd-till-värd-validering utan att behöva lita på roten.

## Hur sätter man upp det?

- Skapa ett nyckelpar.
- Signera ditt data med den privata nyckeln.
- Sänd den publika nyckeln uppåt i trädet, så att din moderzon kan signera den med sin privata nyckel.
- När din moderzon har signerat nyckeln så läggs den in i din egen zon (och eventuellt i moderzonen) så att den som frågar kan verifiera dina signaturer med hjälp av moderns signatur på din publika nyckel.
- Detta fungerar bara om det finns en obruten kedja!

# Resolverns verifiering



# Problem och fällor i DNSSec

Många nya hanteringsfrågor dyker upp i samband med DNSSec. Helt plötsligt måste man ha sekretess och kontroll på nycklar och system.

Både nycklar och deras signaturer har bästföre-datum; man måste göra nyckelbyten och omsigneringar med jämna mellanrum.

Allt detta har direkt inverkan på informations-integriteten. Minsta slarv leder till komprometterad integritet.

Givet hur DNS sköts idag är många pessimister.

## Men man vill ha det ändå! Varför?

I dag är det väldigt lätt att förfalska data i DNS.

DNS är ett väldigt väl fungerande system för distribution av små datamängder. Man kan lätt lösa många andra nyckeldistributionsproblem om man kan lita på data från DNS. Exempelvis PGP– eller IPSecnycklar är lätta att dela med sig av.

## Jag vill prova! Hur gör jag?

BIND 9 har full support för DNSSec som standarden ser ut i dag.

Det finns en laboratoriezon, `sigz.net`, som man kan få sin zon inlagd under. Se `<http://www.sigz.net/>`

Det pågår arbete för att anpassa applikationer och system. Bl a. har IIS sponsrat arbete med IPSec-nyckelhämtning och en simpel vävbläddrare som verifierar sina uppslag.

## 3.2 IDN, a k a “ÅÄÖ”

- “Bara ASCII är orättvist!”
- Störst problem för Asien.
- Drivande kraft är förstås trenden att alla namn ska finnas i DNS, inte bara namn på datorer, som det var tänkt från början.
- Mycket dynamiskt och rörligt område, många olika idéer.
- Bakvänt arbete i IETF, man arbetar för att förekomma lokala standarder. Hot om babylonisering måste undanröjas!

# IDN, forts

Många problem med att bygga ut teckenrymden:

- DNS är egentligen 8-bitrent, i alla namnsträngar. Det har fått folk att hitta på en massa olika lösningar, som baseras på Latin-1 (NuNames) eller UTF-8 (många asiatiska system).
- Men många applikationer som använder DNS är långt ifrån 8-bitrena. Man kan alltså inte utan vidare stoppa in oktetter med sista biten satt, det kan leda till konstigheter högre upp.

## IDN, forts

Vad är då planen med tanke på bakåtkompatibilitet?

- Det lutar fn. åt ACE, Ascii Compatible Encoding, som finns i två varianter, RACE och LACE.
- Principen är ytligen enkel, man kodar om en sträng som innehåller tecken utanför {a-z,0-9} till en "godkänd" sträng så att t ex. **`‘‘räksmörgås’’`** blir **`‘‘bq--abzoi23tnx3hez7fom’’`**

## IDN, forts

- Prefixet

  ``bq--''

  indikerar att strängen är {R,L}ACE. Detta kommer att bytas.

- Därefter är det applikationernas uppgift att konvertera mellan det som syns och det som skickas på tråden.

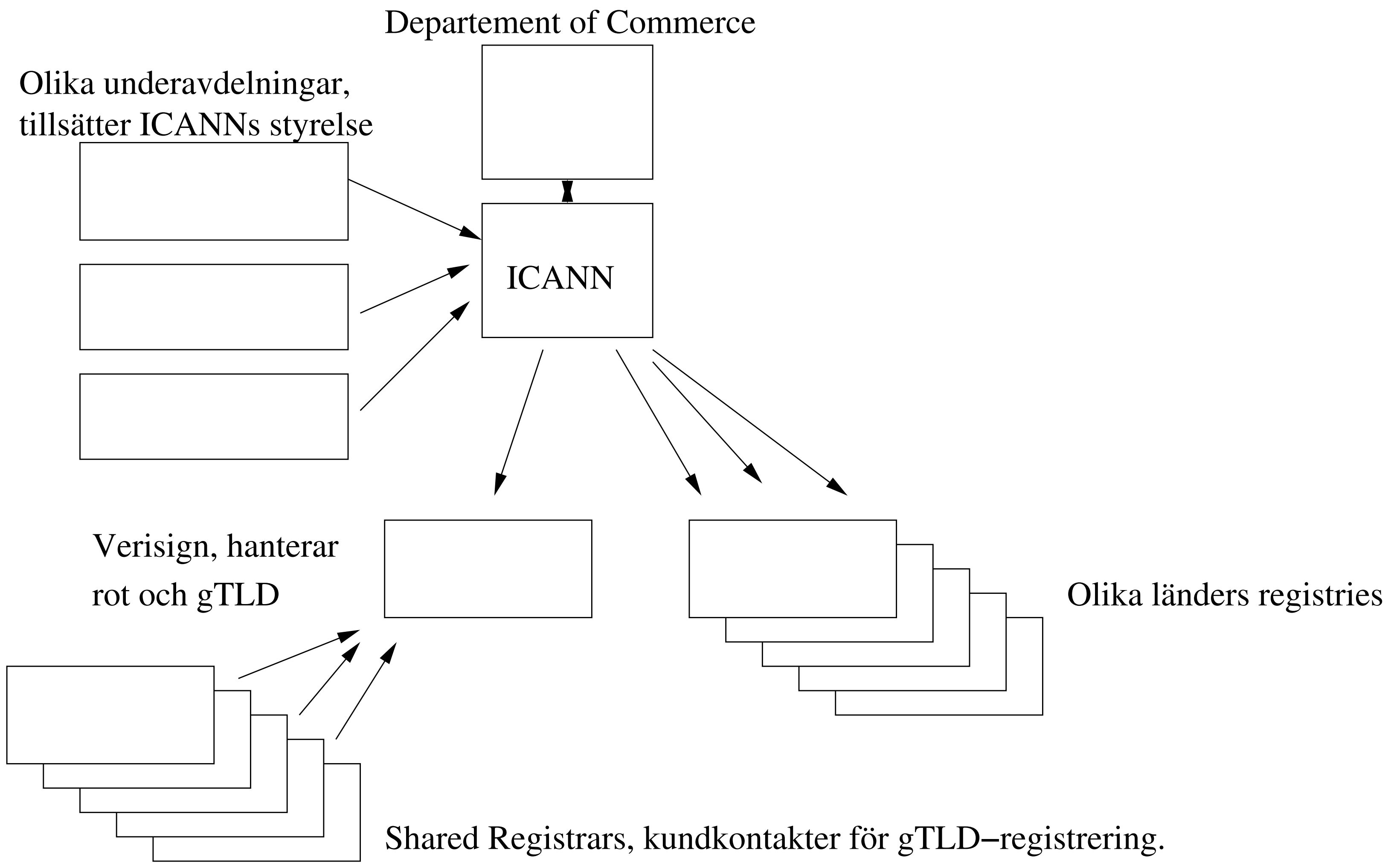
- Inga ändringar görs i DNS-protokollet.

- Detta är i kontrast till olika inkompatibla lösningar.

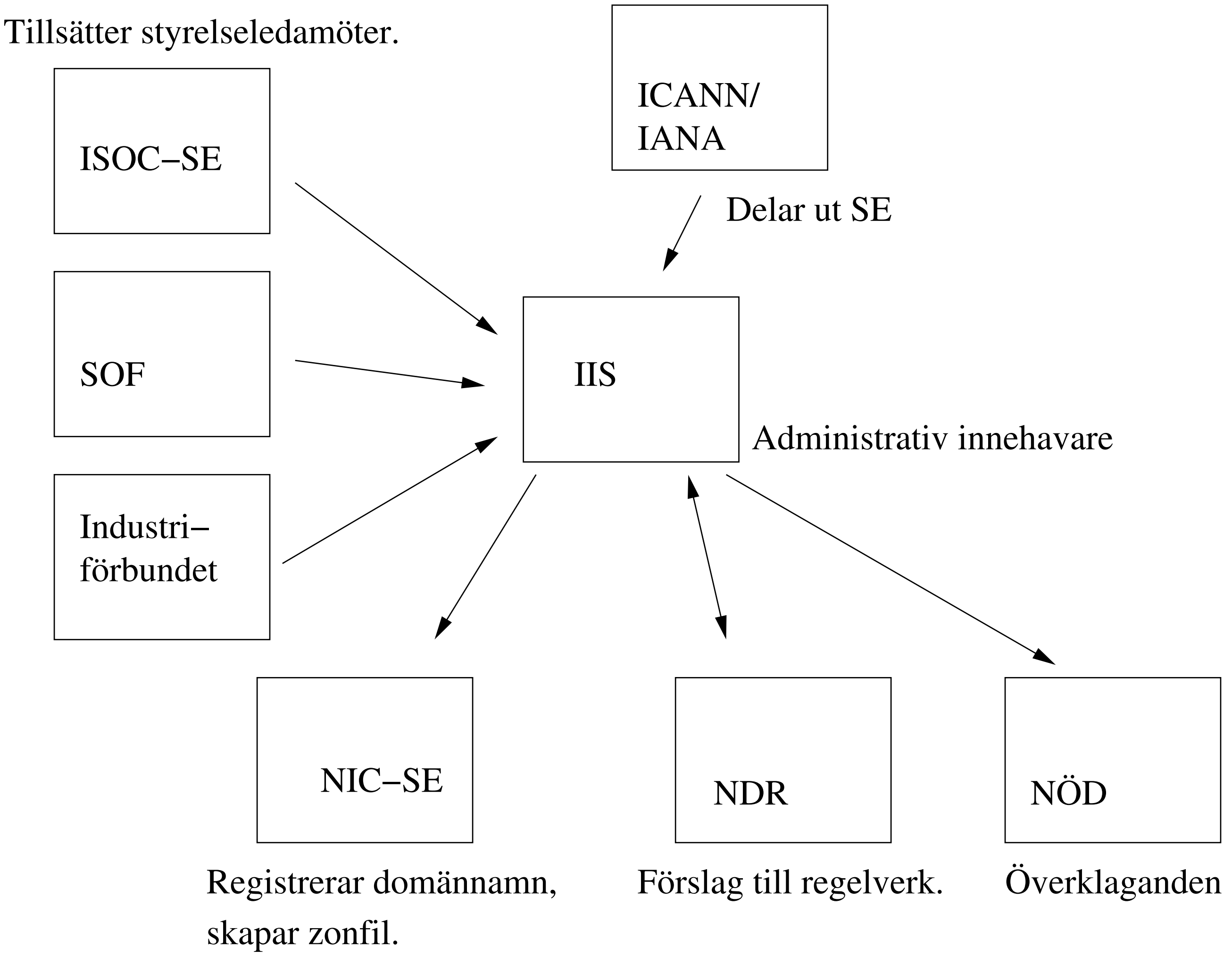
# 4 Organisation och politik runt domäner

- Från början enskilda personer som var personligt bekanta.
- Nu har domännamn som politisk och organisatorisk företeelse växt ur den kostymen.
- Många olika intressenter vill vara med och bestämma.
- Nationalstaterna håller på att vakna.

# Organisation internationellt



# Organisation i Sverige



# 5 Resurser

- RFC'er
  RFC 1034, Domain names - concepts and facilities.
  RFC 1035, Domain names - implementation and specification.
  RFC 1591, Domain Name System Structure and Delegation.
  RFC 2535, Domain Name System Security Extensions.
- Litteratur
  Albitz & Liu, "DNS & BIND, 4th ed." O'Reilly & Associates, Cambridge, Mass. ISBN 0-596-00158-4

# Nyttiga WWW-platser:

ICANN, ansvariga för rootzonen:

`<http://www.icann.org/>`

IIS, administrativ innehavare av SE:

`<http://www.iis.se/>`

NIC-SE, ansvariga för .SE:

`<http://www.nic-se.se/>`

DNS Resources Directory, bra länksamling:

`<http://www.dns.net/dnsrd/>`

# SLUT, Tack så mycket!

## Frågor?

Presentationen kommer att finnas som `<http://vvv.besserwisser.org/upplysning.ps>` så snart jag har fått nät igen..