DNS-test

Patrik Fältström

paf@cisco.com

Ulf Vedenbrant

uffe@vedenbrant.se

Vad är dns-test?

- DNS-test är namnet på ett projekt som initierades av II-Stiftelsen
- dnscheck heter det programmet som Patrik skrev som (delvis) lösning på problemet
- I dagarna flyttas och installeras dnscheck hos NIC-SE för fast installation

Vad gör dnscheck?

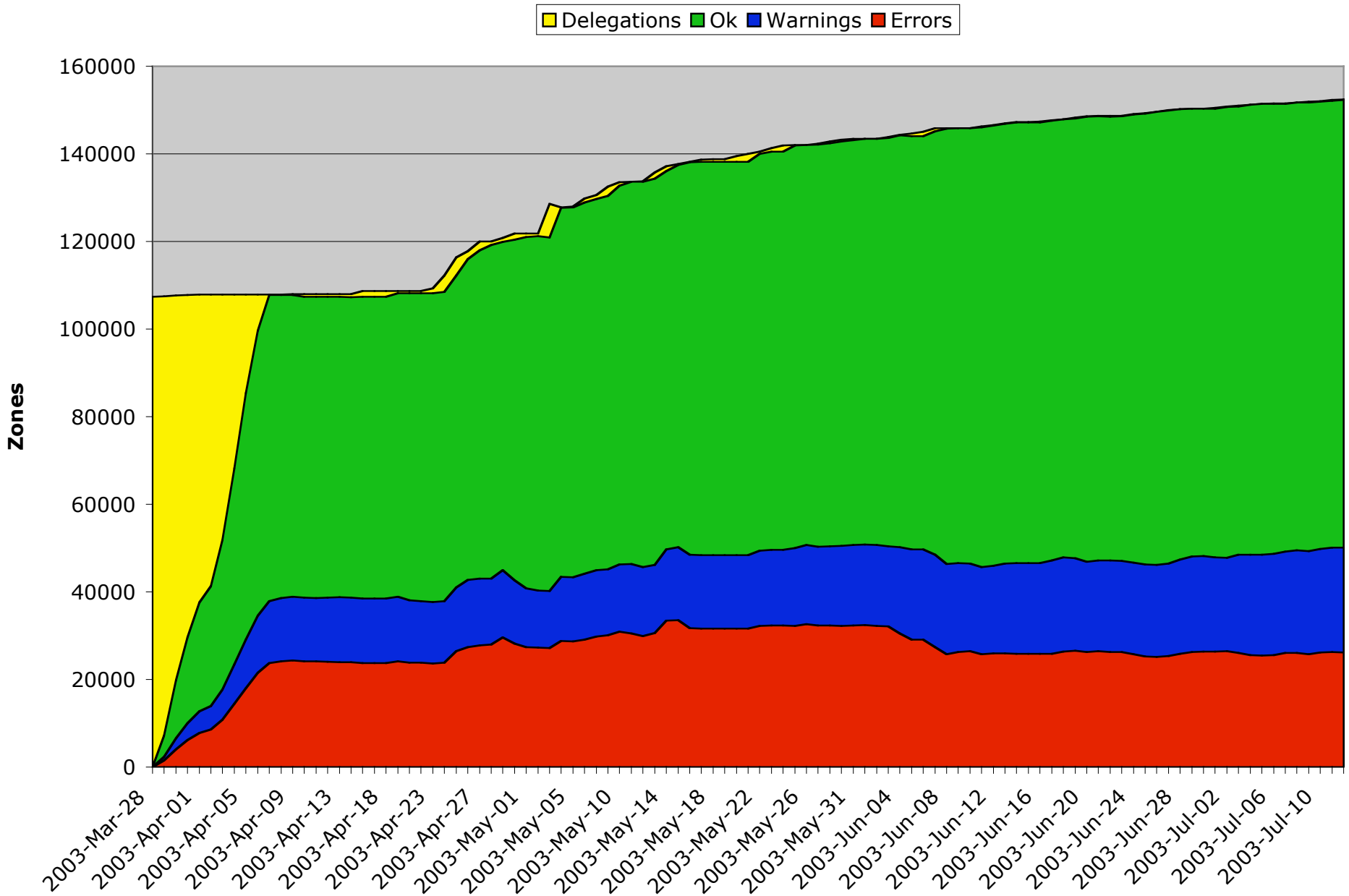
- Kontrollerar om en delegeringspunkt är korrekt konfigurerad
- I korthet, den ser om en zon är korrekt delegerad, dvs om information i parent- och child-zone stämmer med varandra
- Dessutom kontrolleras SOA

Andra verktyg?

- Det finns många andra verktyg på marknaden, tex i distributionen av Bind eller från Men&Mice på Island
- Dessa koncentrerar sig på att se att en zon är korrekt uppsatt, dvs att innehållet i zonen är rätt
- Därför utvecklade Patrik dnscheck som kontrollerar **andra** saker
- Dessa verktyg kompletterar varandra

En detalj…

- När vi pratar om ”ERROR” vad gäller ett domännamn, så betyder det tex att **någon** av de NS som finns för domänen är fel, **inte** att **alla** är fel
- En domän kan alltså i praktiken fungera, för 2 av 3 NS är rätt, men ändå loggas som ”ERROR” av dnscheck


Zone se
Delegations
Ok
Warnings
Errors
Zones
160000
140000
120000
100000
80000
60000
40000
20000
0
2003-Mar-28
2003-Apr-01
2003-Apr-05
2003-Apr-09
2003-Apr-13
2003-Apr-18
2003-Apr-23
2003-Apr-27
2003-May-01
2003-May-05
2003-May-10
2003-May-14
2003-May-18
2003-May-22
2003-May-26
2003-May-31
2003-Jun-04
2003-Jun-08
2003-Jun-12
2003-Jun-16
2003-Jun-20
2003-Jun-24
2003-Jun-28
2003-Jul-02
2003-Jul-06
2003-Jul-10

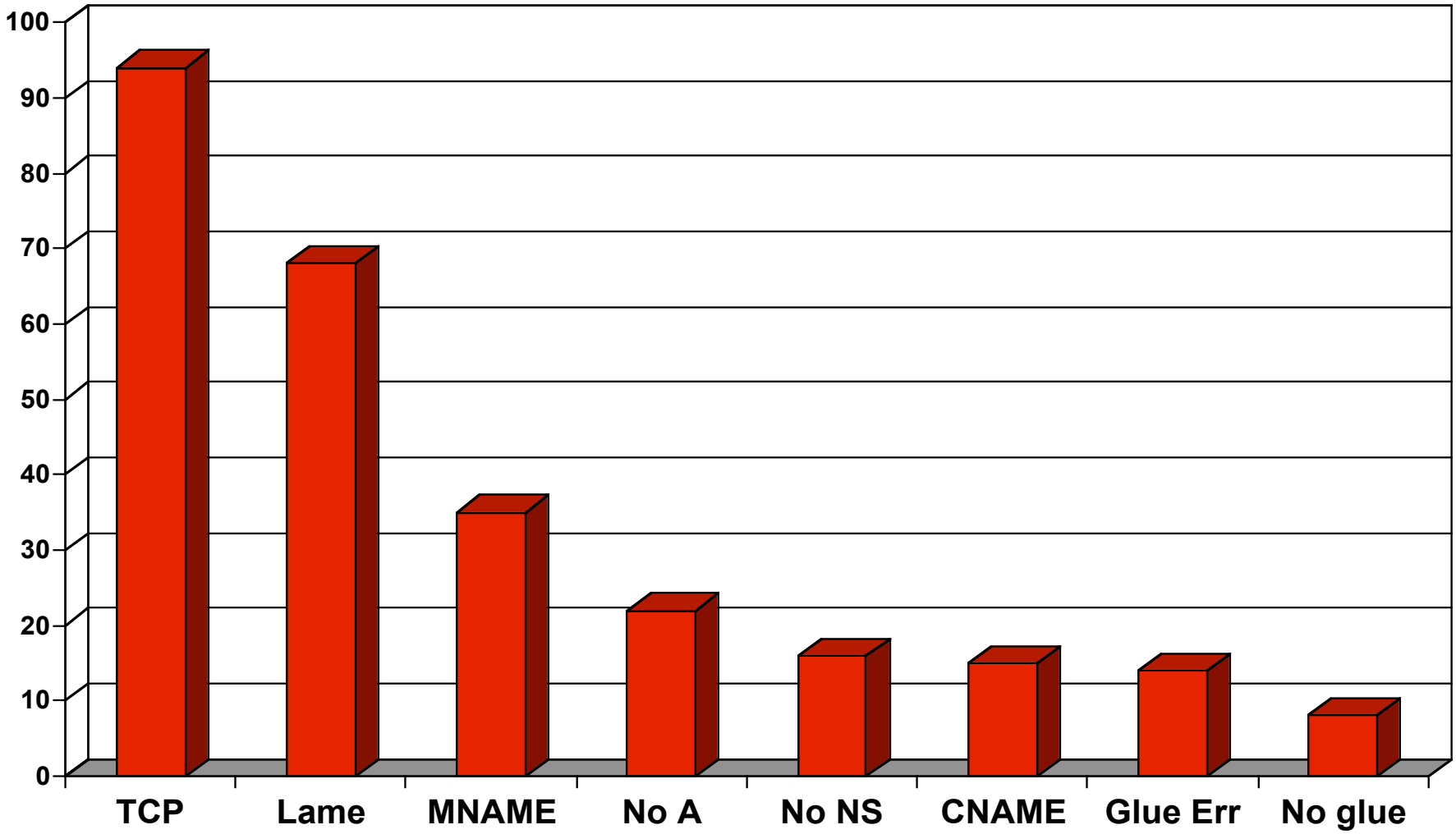
Vad testas 1(2)

- >1 namnserver för en zon?
- Är alla svar från auktoritativa servrar auktoritativa?
- Är serienummer från alla auktoritativa servrar samma?
- Är NS post i förälder och barn samma?
- Existerar A post för NS post?
- Finns det PTR för de IP-adresser man får när man slår upp A?
- Finns det A för alla domännamn?

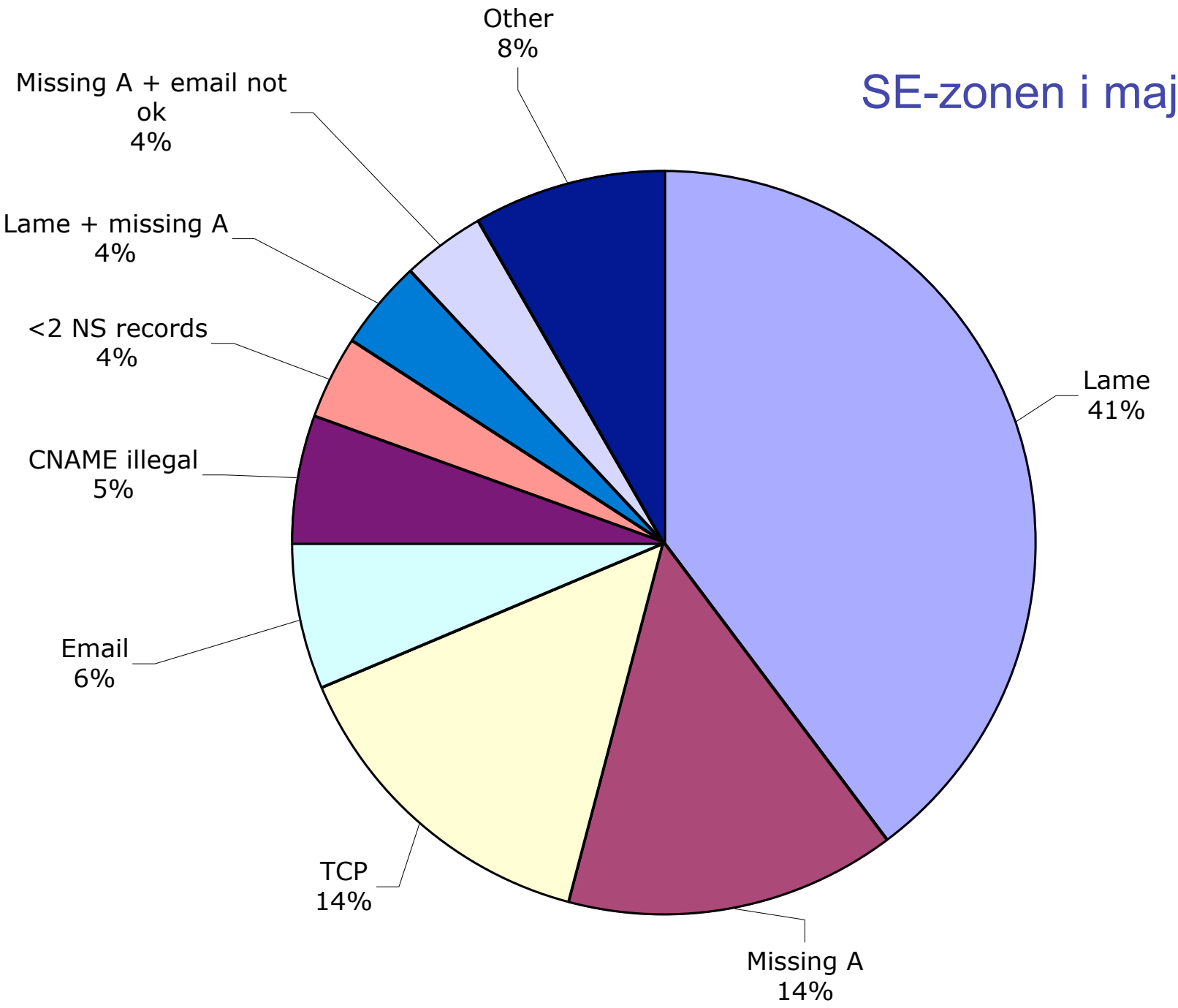
Vad testas 2(2)

- Svarar namnservrar över både UDP och TCP?
- Fungerar mailadressen som finns i SOA?
- Används CNAME (inte) för MX och NS?
- Kan SMTP-servern hantera EHLO och tom kuvertavsändare?
- Fungerar alla MX poster, eller bara en del av dem?
- Är det rätt “glue” som finns i förälder de gånger “glue” behövs?

Root-zon i juli



SE-zonen i maj



Vanliga fel?

- Man ska komma ihåg att DNS fungerar bra trots att någon server är trasig, men, till slut slutar det att fungera utan förvarning
- En zon ”ruttnar” gradvis, men DNS för zonen avtar inte gradvis utan abrupt
- En server som är trasig ger ofta följdfel
  - Om IP-adress är fel kommer den varken ge auktoritativa svar, eller svara över TCP
  - Man kan alltid vrida statistik dit man vill
- Faktum är att det kan vara bättre än 20% fel, och dsncheck ger långtidstrender

Lame

- Olika information i parent och child zone
- Vanligast är att man glömt prata med NIC-SE när man flyttat en namnserver
- Kan också hända om en namnserver helt enkelt gett upp, eller misslyckats med att göra zonetransfer ett tag

Exempel 1

- I zonen ”se”

```
example.se.      IN NS ns1.example.se.
example.se.      IN NS ns2.example.se.
ns1.example.se.  IN A  192.168.1.1
ns2.example.se.  IN A  192.168.2.1
```

- I zonen ”example.se”

```
example.se.      IN NS ns1.example.se.
example.se.      IN NS ns3.example.se.
ns1.example.se.  IN A  192.168.1.1
ns3.example.se.  IN A  192.168.3.1
```

Exempel 2

- I konfigurationen för slavserver

```
zone ”example.se” {
    Type slave;
    File ”slave/example.se”;
    Masters { 192.168.1.2; };
};
```

- Men, det finns ingen namnserver på 192.168.1.2 längre

A-record saknas

- I zonen ”example.se”

```
example.se. IN NS ns1.example.se.
example.se. IN NS ns3.example.se.
ns1.example.se. IN A 192.168.1.1
ns2.example.se. IN A 192.168.2.1
```

- Men, det finns inget A-record för ns3.example.se

TCP fungerar inte

- Det finns en brandvägg mellan DNS-server och Internet som enbart släpper igenom trafik mot port 53 över UDP
- Detta är dåligt, då det kan hända (och kommer hända oftare) att TCP behövs
- TCP behövs absolut för zonetransfer

CNAME

- I zonen ”example.se”

```
example.se.      IN NS ns4.example.se.
ns4.example.se.  IN CNAME ns1.example.se.
ns1.example.se.  IN A 192.168.1.1
```

NS

- I zonen ”example.se”

```
example.se. IN NS 192.168.1.1
```

SOA (email)

- I zonen ”example.se”:

```
$ORIGIN example.se.
   IN SOA ns1 hostmaster@example.se. (
          2003100200
          6h
          1h
          1w
          3h
)
```

- Det ovan ger ”**hostmaster@example@se**”

Summering

- Det är någon typ av fel i c:a 20% av domänerna i Sverige
- Procenttalet ökade **inte** när registreringen släpptes fri (det blev snarare bättre)
- DNS fungerar ändå
- Men, det kunde vara bättre (jag tror 10% fel är möjligt)

Patrik Fältström

paf@cisco.com

Ulf Vedenbrant

uffe@vedenbrant.se

http://dnscheck.se/