

Kvalitet i DNS

Lars-Johan Liman
Autonomica AB



Vad är dålig kvalitet i DNS?

- "Det funkar inte."
- Man når inte sin motpart alls!
- Det blir irriterande fördröjningar.
- Man hamnar rent av *fel!*?
- Men också: det går inte att få tag på den ansvarige när något har slutat funka.



Kvalitetens beståndsdelar

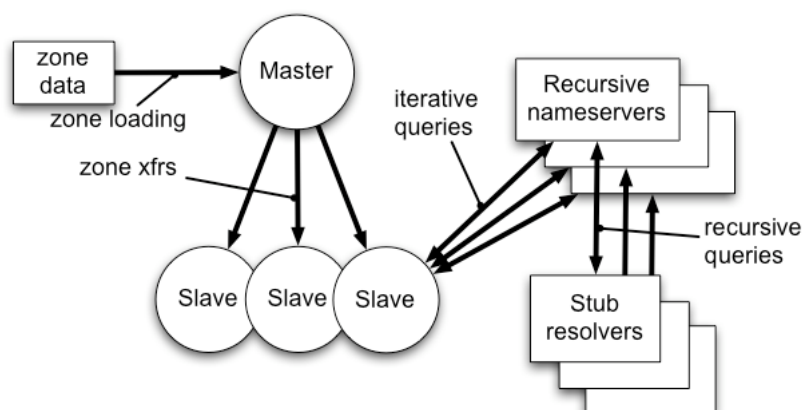
- Stabilitet
 - Det skall funka – jämt!
- Säkerhet
 - Jag skall få den information jag tror att jag får.
- Akualitet
 - Jag skall inte få gammal information.

2007-09-12



3

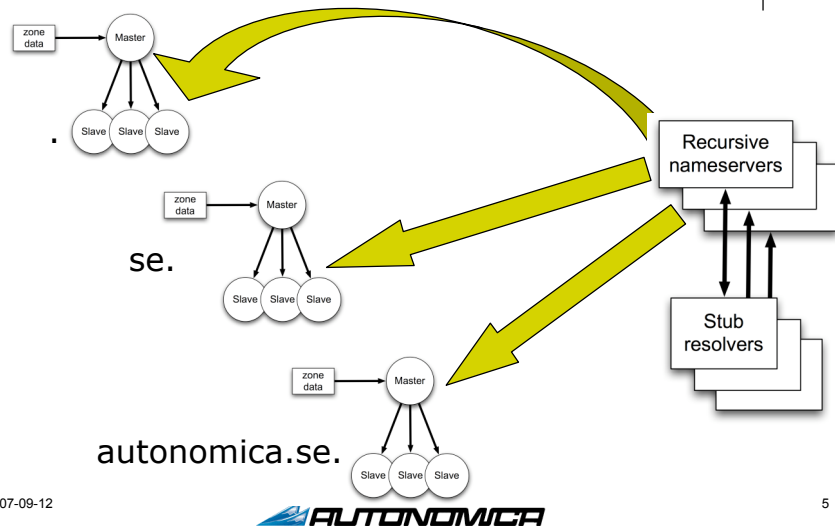
DNS-transaktioner ...



20

4

... sker i flera nivåer!



2007-09-12

5

Masterservrar

- Stabil maskin
- Duglig konnektivitet
 - Behöver inte vara lysande om inte också publik server.
- Säkerhet
- TSIG
 - Men kom då ihåg att köra NTP!
- Fräsch programvara

2007-09-12

AUTONOMICA

6

Vad är det för fel på min gamla BIND?



- Jo, det var just det ... den är **GAMMAL!**
- Säkerhetshål
 - <http://www.isc.org/index.pl?/sw/bind/bind-security.php#matrix>
- Prestandaproblem
- Klarar inte moderna tillägg till DNS
- Rena buggar
 - Ex: elaka DNSSEC-"buggar" i tidiga BIND9-versioner som även påverkar drift *utan* DNSSEC!

2007-09-12



7

BIND 8 är DÖD!



To: bind-announce@isc.org
Subject: **BIND8 entering end of life**
From: Paul Vixie <Paul_Vixie@isc.org>
Date: 09 Aug 2007 22:54:47 +0000

whereas BIND9 is now 8 years old,
and BIND9 is performance-competitive against BIND8,
and BIND9 conforms to more of the DNS protocol than
BIND8,
and BIND9 is more secure and more portable than BIND8,
we are declaring BIND8 to be in "end of life" (like BIND4).
[snip]

--
Paul Vixie

2007-09-12



8

Slavervrar

- Stabil maskin
- Övervakning
- **Utmärkt** konnektivitet till Internet
- Säkerhet
- TSIG
 - Men kom då ihåg att köra NTP!
- Fräsch programvara

2007-09-12



9

BIND 8 är DÖD!

To: bind-announce@isc.org
Subject: **BIND8 entering end of life**
From: Paul Vixie <Paul_Vixie@isc.org>
Date: 09 Aug 2007 22:54:47 +0000

whereas BIND9 is now 8 years old,
and BIND9 is performance-competitive against BIND8,
and BIND9 conforms to more of the DNS protocol than
BIND8,
and BIND9 is more secure and more portable than BIND8,
we are declaring BIND8 to be in "end of life" (like BIND4).
[snip]

--
Paul Vixie

2007-09-12



10

Resolvrar

- Stabil maskin
- God konnektivitet till Internet
- **Utmärkt** konnektivitet till klienter
- DNSSEC?
 - Om man vill.
 - "Klart om 6 månader ..." :-)
- TSIG?
 - Inte klart ännu. "Kommer i nästa release".
- Fräsch programvara

2007-09-12



11

BIND 8 är DÖD!

To: bind-announce@isc.org
Subject: **BIND8 entering end of life**
From: Paul Vixie <Paul_Vixie@isc.org>
Date: 09 Aug 2007 22:54:47 +0000

whereas BIND9 is now 8 years old,
and BIND9 is performance-competitive against BIND8,
and BIND9 conforms to more of the DNS protocol than
BIND8,
and BIND9 is more secure and more portable than BIND8,
we are declaring BIND8 to be in "end of life" (like BIND4).
[snip]

--
Paul Vixie

2007-09-12



12

DNSSEC – är det kvalitet?



- "Ni bör nog lära er hur det funkar."
- Egen ny administration
 - Nyckelgenerering
 - ... med periodiska byten.
 - Signering
 - ... periodiskt.
 - Nyckelutbyte med förälder.
 - ... med periodiska byten
- Ny administration gentemot andra
 - Ankarnycklar (.SE, .RO, .NL, root ...)
 - ... med periodiska byten

Övervakning



- BIND producerar frågestatistik
 - ... men det räcker inte!
- Ställ frågor till egna servrar!
 - Är alla slavar vakna?
 - Svarar de rätt?
 - Stämmer serienumren överens mellan slavarerna?
- Måste också övervaka nätverket!

Vanliga fel

- Glömda punkter
- Felaktiga delegeringar
- Övergivna servrar
- Glue records
- Gammal kontaktinformation

Glömda punkter

- Måste man hitta själv.
- Den vane kollar alltid det **FÖRST**. :-)
- Gör manuell zone transfer.
dig @master.server zone.se AXFR
 - ... då sticker namnet ut tydligt.
- ... eller så kör man utan punkter, men det har också nackdelar.
 - Saker hamnar i fel zon.

Felaktiga delegeringar



- Föräldern har en uppsättning NS-poster och barnet en annan.
- Inträffar oftast när barnet byter nameservrar.
- Kom ihåg att alltid prata med **ALLA** föräldrar när ni byter nameserver. Framlänges, baklänges, alla toppdomäner m.m.
 - Ja, det är förb-nat jobbigt att få ihop det.
- Kör <http://dnscheck.se/>

Övergivna servrar



- Uppträder oftast när man har varit slav åt någon, och de har bytt slavar utan att tala om det.
- Kolla med jämna mellanrum att er server är med bland NS-posterna för alla zoner.
 - Men kolla det från en **ANNAN** resolver!

Glue records



- Bastarder på fel plats.
- Måste letas upp av resolvern.
- Samspelet auktoritativ server – resolver underlättas av "in bailiwick glue".
`autonomica.se. IN NS ns.autonomica.se.`
`ns.autonomica.se. IN A 192.71.80.99`
- Dock lurigt i baklängeszoner. Tekniskt sett funkar det, men inte alla gillar
`ns.80.71.192.in-addr.arpa. IN A 192.71.80.99`

2007-09-12



19

Gammal kontaktinformation



- Ett gammalt kärt problem ...
- Den hårda vägen:
 - Gör tjänsten beroende av att "kunderna" med jämna mellanrum verifierar sin kontaktinformation.
- Den mjuka vägen:
 - Kolla själv med jämna mellanrum att saker stämmer.
- Försök koppla det till annan periodisk händelse.

2007-09-12



20

DNS i stordrift



- Ju högre upp i DNS-trädet, desto högre krav på tjänsten.
- Root, TLD har väldigt höga krav.
- Dock:
 - Redundans på "applikationsnivå" (där DNS är applikationen).

Anycast



- Annonsera *samma* prefix från flera ställen med samma AS-nummer.
- Lurar BGP-systemet.
- Om en site försvinner kommer BGP att routa om till andra.
- Om en site DDoS:as, drabbar det bara den siten.

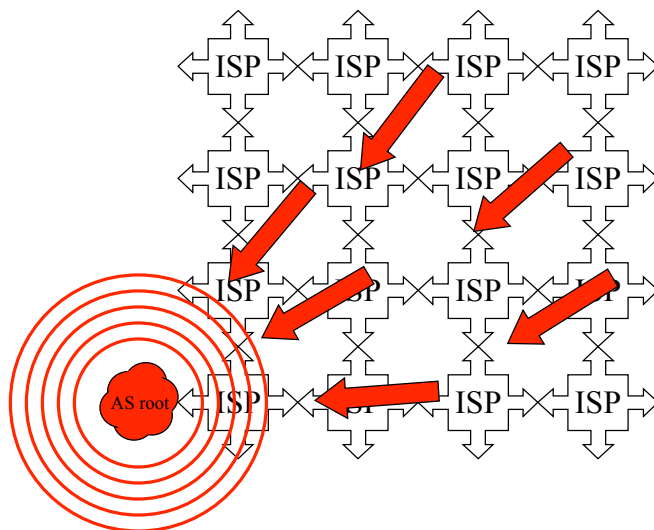
Anycast

- Varje site har
 - 2 routrar
 - 2+ servrar
- Routrarna ansluts till Internet
 - Ofta knutpunkt – direkt eller via knutpunkts-AS.
 - Ibland stor operatör.
- "Bakväg" in för administration.
 - Måste ha unicast.

2007-09-12



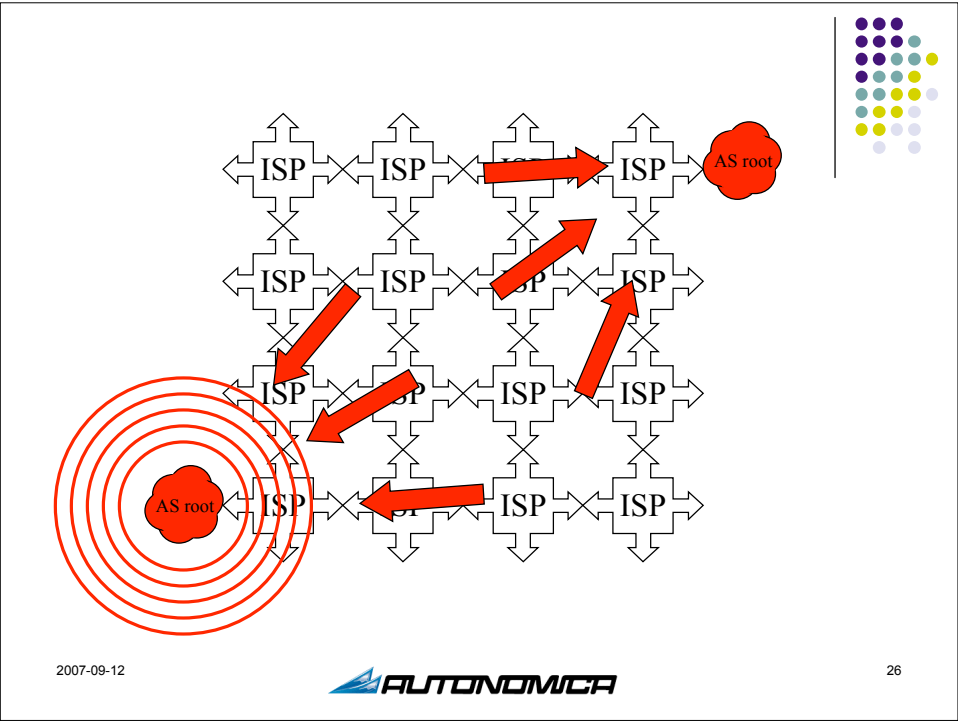
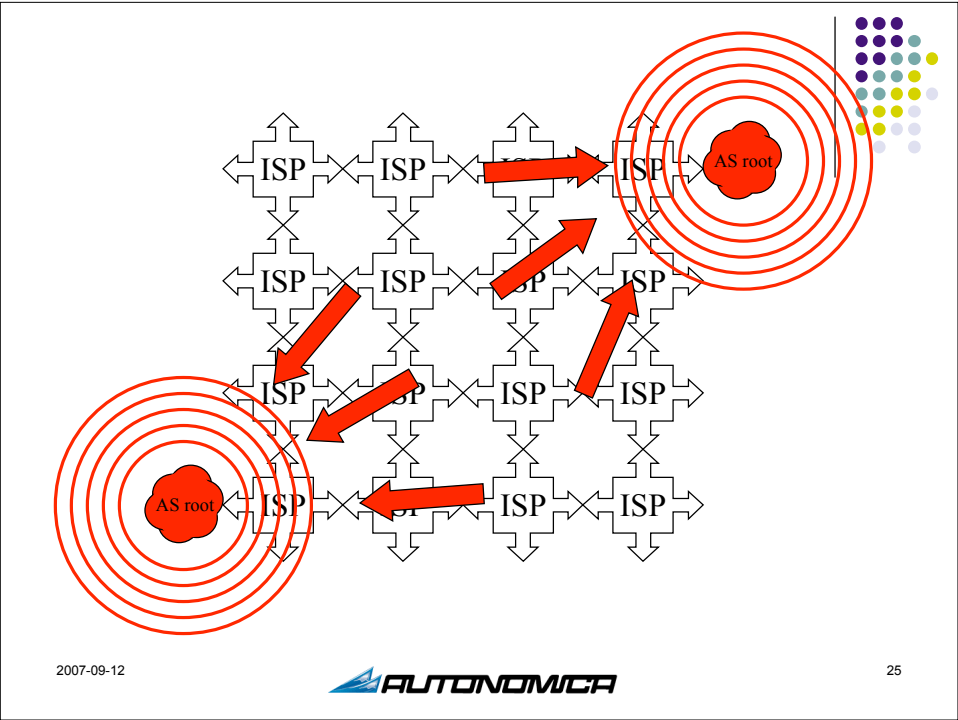
23

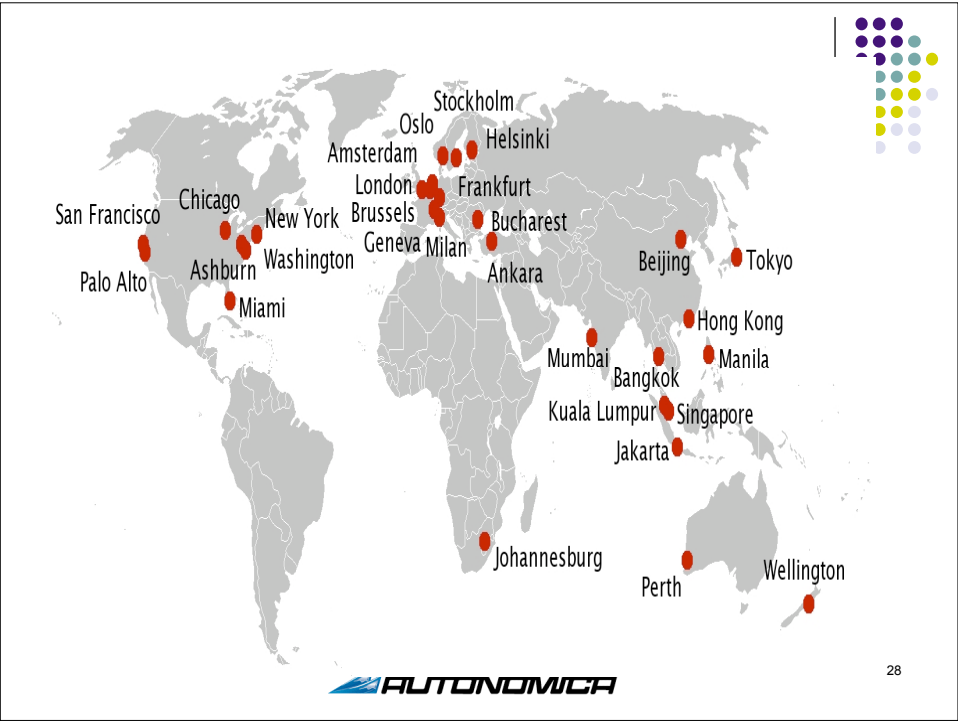
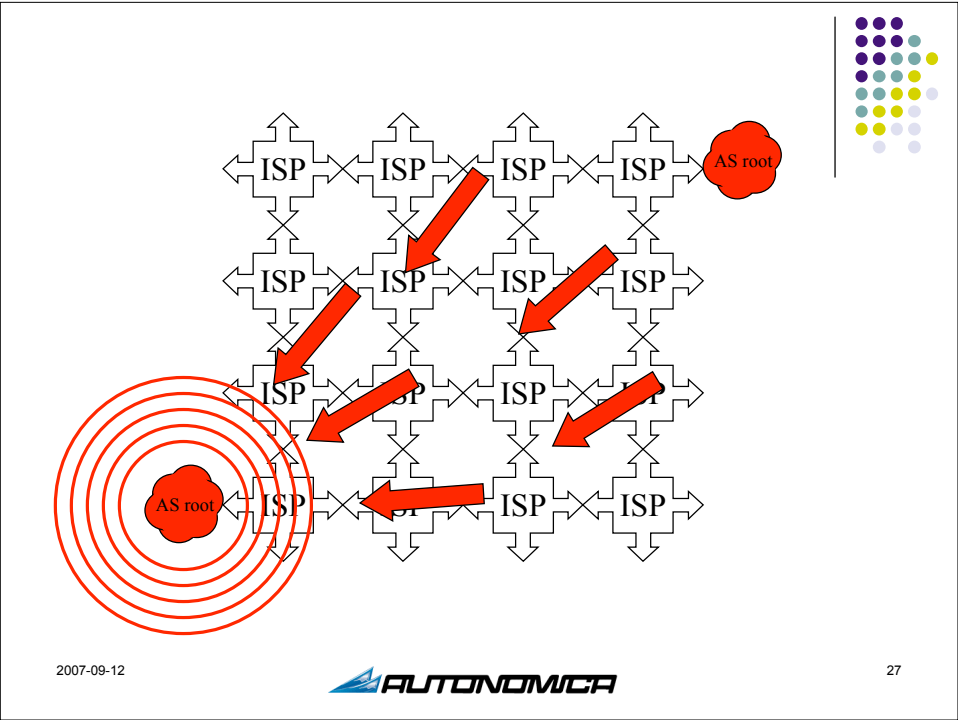


2007-09-12



24





Zondistribution



- 2 distributionsmastrar i olika bergrum
- Matar alla anycastinstanser och andra servrar.
- All överföring sker med TSIG.
- Serienummer övervakas.

Övervakning



- DNS-grafer
- Trafikgrafer
- Nagios med egna DNS-moduler
 - Nåbarhet – svarstider: egna och mastrar.
 - Överensstämmelse serienummer: egna och mastrar.
- RIPE NCC: DNSMON
 - <http://dnsmon.ripe.net/>

Prober



- Pyttedatorer vi delar ut över hela världen.
- Målet: 50 st.
- Går igång av sig själva.
- Frågar i sakta mak våra DNS-servrar.
- Ger oss en bild av hur vår tjänst upplevs runt om i världen.
- "Vår egen DNSMON"

Denna presentation finns på URL:

<http://www.autonomica.se/liman/presentations/sunet/optosunet-DNS-kvalitet-2007.pdf>

Autonomica AB
Bellmansgatan 30
SE-118 47 Stockholm
Sweden
Tel: +46-8-6158570
Fax: +46-8-4420967
E-mail: info@autonomica.se
<http://www.autonomica.se/>

