IP priset 2011
Vem, DNSEC och IPv6

Tobbe Eklöv – torbjorn.eklov@interlan.se

Swedish Network Users' Society
En ideell förening för svenska nätverksanvändare.

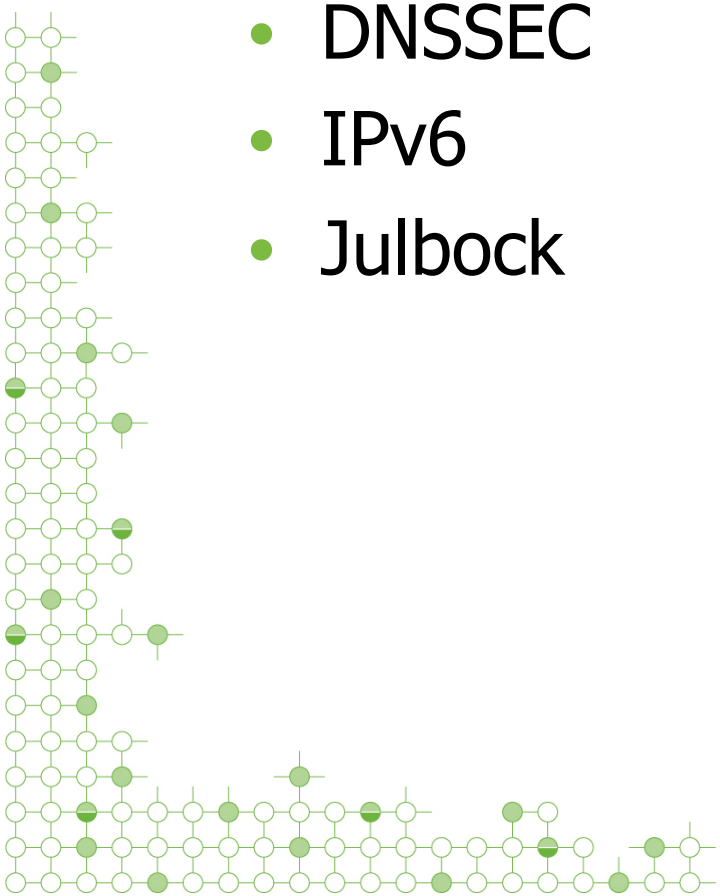
NYHETER | OM SNUS | STYRELSEN | STADGAR | BLI MEDLEM! | IP-PRISET | VERKSAMHET | REMISSVAR | KONTAKT | SNUS JUNIOR AWARD

IP-priset 2011 går till Torbjörn Eklöv

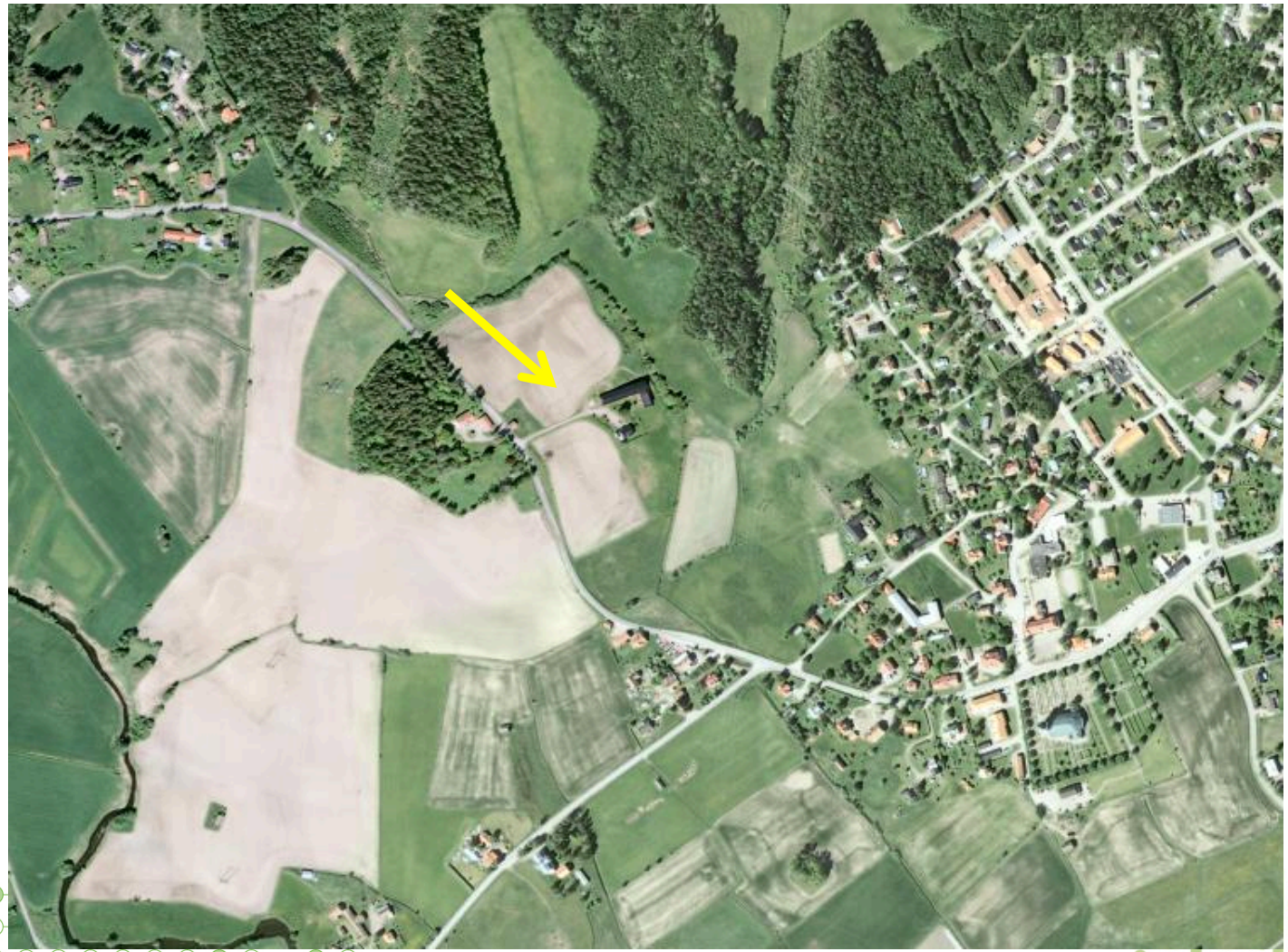
interlan

Agenda

- Historik
- DNSSEC
- IPv6
- Julbock



interlan



Historik

- 1986-1987 Elektromontage
- 1987-1989 HIGS
- Owell 1989
- 1991 – IP på lg.se
  "*Jag brukar använda de här adresserna*"
- 1992 – Ädelreformen
  Sune – 192.71.65.1
- 1996 (?) WM-data köper Owell
- 1997 Interlan grundas

interlan

Historik

- 1997 – Hjälper Sandnet igång
- 2001 – RIPE-kurs i Köpenhamn
- 2001 – AS-path prepend
- 2003 – Tittar på v6 första gången
- 2007 - .SE börjar med DNSSEC
- 2007 – Signerar gavle.se och ockelbo.se v6 på DNS och MX
- 2008-2009 kommuner och myndighetermed….
- 2009 – Interlans webbhotell + kontor är v6 och DNSSEC'at
- 2011 – IP-priset!!!!!!!!!

IPv6 och DNSSEC

- Tänkte inte prata så mycket om varför utan mer om status och problem som finns och som kommer att uppstå
- Och mest ur ett företags/ myndighetsperspektiv

IPv6 och DNSSEC

- **Varken DNSSEC eller IPv6 är dyrt eller svårt att komma igång med!**
- Om man använder rätt kompetens dvs….

Sverige ska verka för ett tillgängligt, öppet och robust internet i Sverige och globalt. För att få en säkrare kommunikation för myndigheter behövs underlag till en internetspecifikation som kan användas vid myndigheters upphandling av internetanslutning. Senast 2013 ska det därför finnas en gemensam internetspecifikation med olika robust- och säkerhetskrav (typfall) framtagen för myndigheter. Dessutom bör alla myndigheter senast 2013 använda sig av DNSSEC och vara nåbara med IPv6.

Varför DNSSEC?

The Kaminsky bug

What is the Kaminsky bug?

In the summer of 2008, researcher Dan Kaminsky discovered how flaws in the Internet's Domain Name System, DNS, can be exploited for an attack. Through the so-called Kaminsky bug an attacker can, by simple means, trick Internet users by temporarily taking over a domain name and redirecting queries to another server.

This method can simplify so-called "phishing", when users believe that they are communicating with for example their online bank, but are actually being tricked into sending sensitive information such as account numbers and passwords to the attacker's server.

The film here shows how an attack is carried out technically. With software that has been upgraded the attack is more difficult to carry out, but is still feasible. The long-term solution is to use the security extensions to DNS called DNSSEC.

http://www.youtube.com/watch?v=29IhLOhnclY

interlan

Varför DNSSEC?

NYHETER Säkerhetsexperter dömer ut hela systemet för säkra webbplatser, sedan hundratals förfalskade certifikat spridits den senaste veckan. "Det här förutspådde vi redan för 15 år sedan", säger Anne-Marie Eklund Löwinder på Punkt SE.

Ett hänglås i webbläsaren betyder inte längre att du besöker en webbplats via en säker förbindelse.

Flera hundra välkända webbplatsers säkerhet ifrågasätts efter ett intrång mot säkerhetsföretaget Diginotar. Efter attacken spreds förfalskade certifikat som används som garantier för att webbplatserna är äkta. Flera av de stulna certifikaten gäller google.com, och i veckan har Google tvingats meddela 300 000 Gmailanvändare att någon kan ha brutit sig in i deras e-postkonton.

Att certifikat förfalskas sänker förtroendet för hela systemet.

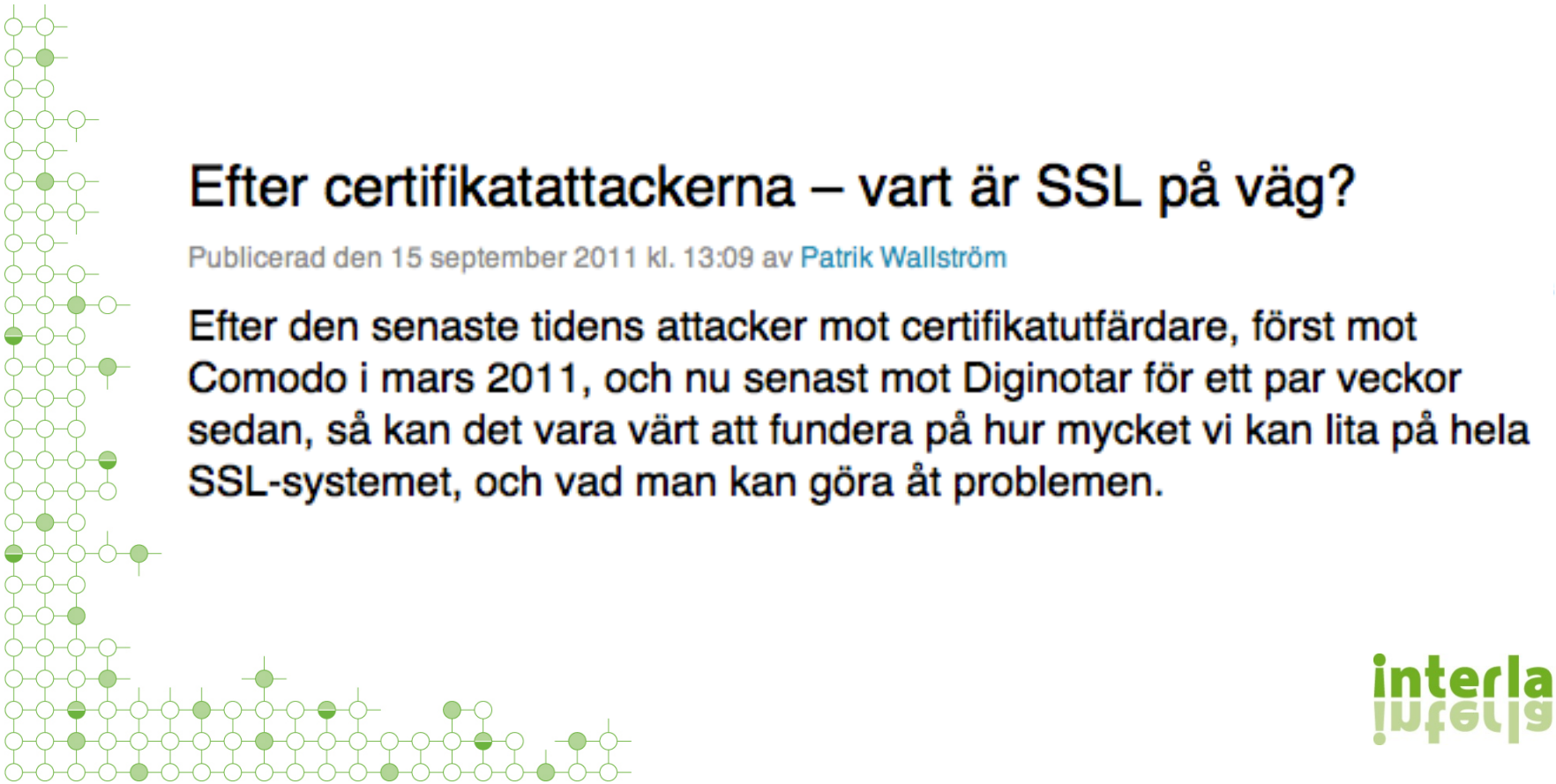
– Infrastrukturen är inte tillräckligt bra. Tyvärr, det här är inte alls oväntat, säger Anne-Marie Eklund Löwinder, informationssäkerhetsansvarig på Punkt SE och en av Sveriges främsta säkerhetsexperter.

interlan

Varför DNSSEC?

- DNS är som protokoll osäkert
- DNSSEC gör att svaren valideras av tredjepart
- .SE igång sedan 2007
- Roten signerad sedan sommaren 2010
- För första gången i Internets historia har vi en global PKI-infrastruktur

DANE - DNS-based Authentication of Named Entities



Efter certifikatattackerna – vart är SSL på väg?

Publicerad den 15 september 2011 kl. 13:09 av Patrik Wallström

Efter den senaste tidens attacker mot certifikatutfärdare, först mot Comodo i mars 2011, och nu senast mot Diginotar för ett par veckor sedan, så kan det vara värt att fundera på hur mycket vi kan lita på hela SSL-systemet, och vad man kan göra åt problemen.

interlan

Hur väljer jag DNS-operatör?

- Om du kör själv => bra registrar
- IPv6 glue
- DNSSEC med valfria DNS'er
- Vid många domäner är ett API bra

- Extern DNS-operatör => Minst två DNS'er i Sverige – v6 och DNSSEC

DNS1.EASYDNS.COM

✓IPv6 enabled

- Ashburn
- Chicago
- San Jose
- Amsterdam
- Tokyo

DNS2.EASYDNS.NET

(Deployed via **Prolexic** as follows:)

- Miami
- Phoenix
- London, UK
- Hong Kong

DNS3.EASYDNS.CA

✓IPv6 enabled
(**DNS Hosting** level domains use DNS1, DNS2 & this one)

- Seattle
- Chicago
- Washington
- Singapore
- Frankfurt

DNS3.EASYDNS.ORG

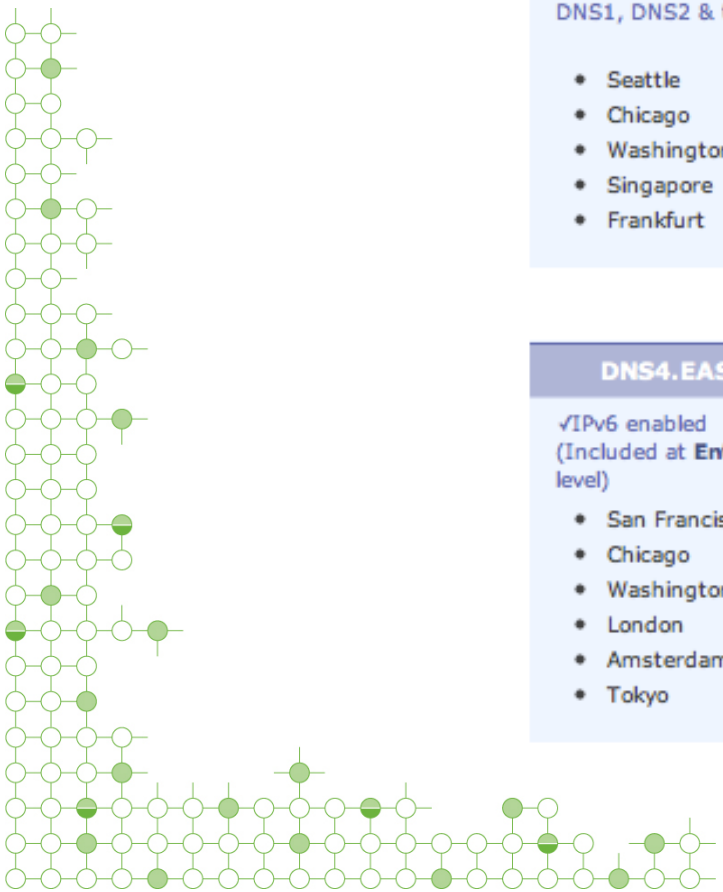
✓IPv6 enabled
(**DNS Pro** and **Enterprise DNS** use this one. This nameserver *includes* all the dns3.easydns.ca nodes **plus:**)

- Palo Alto
- Paris
- Hong Kong
- London
- Los Angeles

DNS4.EASYDNS.INFO

✓IPv6 enabled
(Included at **Enterprise DNS** level)

- San Francisco
- Chicago
- Washington
- London
- Amsterdam
- Tokyo



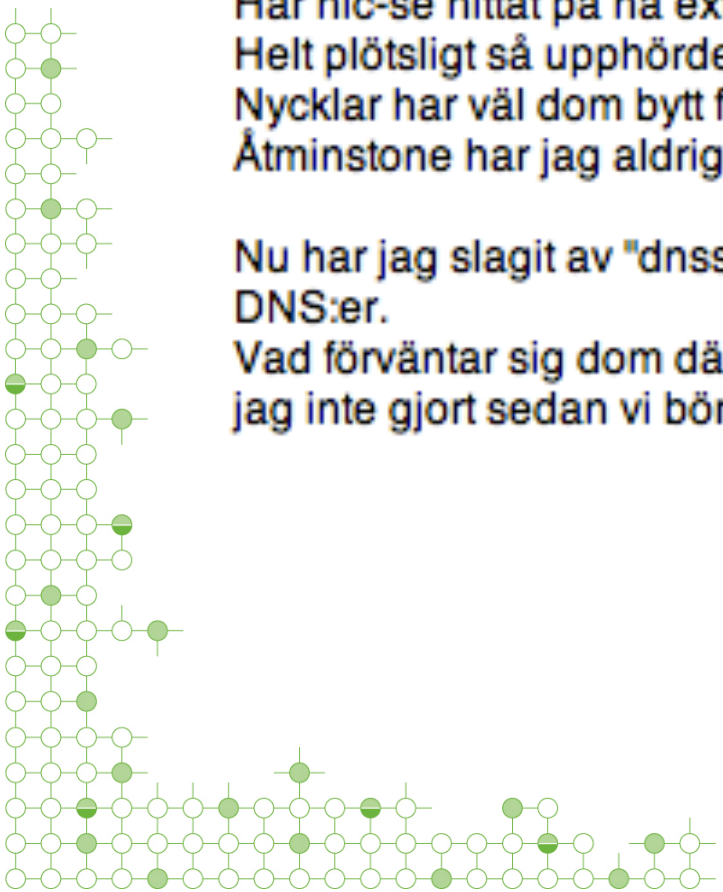
Signering ⇔ Validering

- Utan validering är signering onödig
- Microsoft server 2008 R2 kan DNSSEC på papperet men inte i praktiken
- Nästa version ska bli bättre
- Validering idag => IPAM-system, Linux/ *BSD resolvrar med stub-zone mot AD

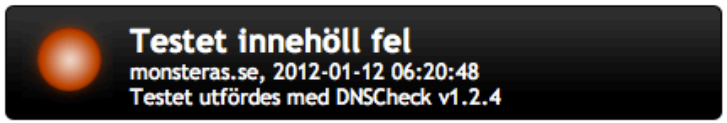
Problem

God morgon,
Har nic-se hittat på nå extra jävelskap vid nyckelbytet i natt?
Helt plötsligt så upphörde alla uppslag mot .se-domäner?!?!
Nycklar har väl dom bytt förr och det har aldrig varit några problem.
Åtminstone har jag aldrig behövt göra något.

Nu har jag slagit av "dnssec-validation" så att vi åtminstone har fungerande DNS:er.
Vad förväntar sig dom där figurerna att jag skall göra den här gången som jag inte gjort sedan vi började i juni 2010??



Problem – jag kan själv



Förenklat resultat | Avancerat resultat

- Delegering
- DNS-server
  - DNS-server ns01.monsteras.se
  - DNS-server ns02.monsteras.se
- Konsekvent uppsättning
- SOA
- Konnektivitet
- DNSSEC
  - Hittade ej tillräckligt med godkända signaturer över SOA RRset hittade för monsteras.se.

Länk till det här testresultatet:
http://dnscheck.iis.se/?time=1326345648&id=2120325&view=basic&test=standard

Tidigare test

- 2012-01-12 08:03:33
- 2012-01-12 06:20:48
- 2012-01-11 14:06:11
- 2011-12-21 22:33:32
- 2011-12-21 22:23:21
- 2011-12-21 22:05:11
- 2011-12-21 21:58:47
- 2011-12-21 21:48:19
- 2011-12-21 21:12:49
- 2011-12-21 12:18:16

Sida 1/15

Förklaring

- Testet var ok
- Testet innehöll varningar
- Testet innehöll fel

Problem

- Vi validerar DNSSEC =>

Torbjorn Eklov Ny kommun, någon som känner någon på Mönsterås kommun, deras #DNSSEC är trasig... http://bit.ly/zpQFN6

bit.ly bit.ly

Like • Comment • Share • 1 second ago

To webmaster@monsteras.se, drift@monsteras.se

Add Cc Add Bcc

Subject Trasig DNSSEC

Attach a file Insert: Invitation

« Plain Text

Hej, jag måste maila från Gmail då vi validerar DNSSEC, er DNSSEC är trasig så ni är onåbara från många ställen för tillfället.

--

/Tobbe

Testa din DNS-server och upptäck fel

Domännamn: soderhamn.se

Ange ditt domännamn ovan för att testa dess DNS-servrar.

Testa nu

Testet innehöll fel
soderhamn.se, 2012-01-19 07:50:43
Testet utfördes med DNSCheck v1.2.4

Förenklat resultat | Avancerat resultat

Delegering

- Extra DNS-server listad hos förälder: ns1.ascio.net
- Extra DNS-server listad hos förälder: ns4.ascio.net
- Ingen likhet mellan förälderns och barnets glue.

DNS-server

- DNS-server a4.nstld.com
- DNS-server f4.nstld.com
- DNS-server g4.nstld.com
- DNS-server l4.nstld.com

Konsekvent uppsättning

SOA

Konnektivitet

DNSSEC

Länk till det här testresultatet:
http://dnscheck.iis.se/?time=1326955843&id=2129877&view=basic&test=standard

Tidigare test

- 2012-01-19 07:50:43
- 2012-01-19 07:30:39
- 2012-01-19 07:21:56
- 2012-01-18 23:19:30
- 2012-01-18 20:43:14
- 2012-01-18 20:32:02
- 2012-01-18 20:02:14
- 2012-01-18 19:51:45
- 2012-01-18 19:12:19
- 2012-01-18 18:50:55

Sida 1/8

Förklaring

- Testet var ok
- Testet innehöll varningar
- Testet innehöll fel
- Testet utfördes inte

www.kommunermeddnssec.se

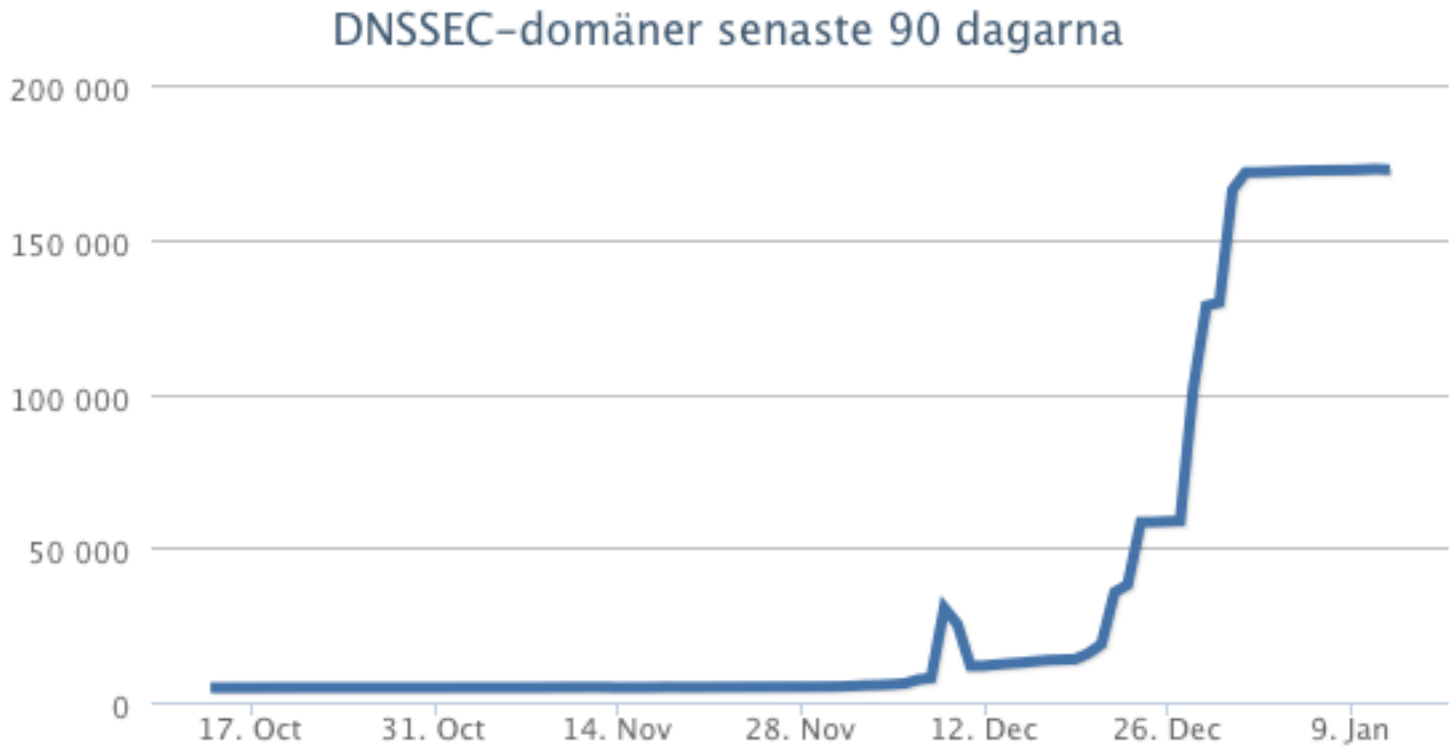
ale.se	alingsas.se	alvesta.se	aneby.se	arboga.se
arjeplog.se	arvidsjaur.se	arvika.se	askersund.se	avesta.se
bengtsfors.se	berg.se	bjurholm.se	bjuv.se	boden.se
bollebygd.se	✓ bollnas.se	borgholm.se	borlange.se	boras.se
botkyrka.se	boxholm.se	bromolla.se	bracke.se	burlov.se
bastad.se	dalsed.se	danderyd.se	degerfors.se	dorotea.se
✓ eda.se	ekero.se	eksjo.se	emmaboda.se	✓ enkoping.se
eskilstuna.se	eslov.se	essunga.se	fagersta.se	falkenberg.se
falkoping.se	falun.se	filipstad.se	finspong.se	flen.se
forshaga.se	fargelanda.se	gagnef.se	✓ gislaved.se	✓ gnesta.se
gnosjo.se	gotland.se	grums.se	grastorp.se	gullspang.se
gellivare.se	✓ gavle.se	goteborg.se	gotene.se	habokommun.se
✓ hagfors.se	hallsberg.se	hallstahammar.se	halmstad.se	hammaro.se
haninge.se	✓ haparanda.se	heby.se	hedemora.se	helsingborg.se
herrljunga.se	hjo.se	hofors.se	huddinge.se	hudiksvall.se
hultsfred.se	hylte.se	habo.se	hellefors.se	herjedalen.se
harnosand.se	harryda.se	hassleholm.se	hoganas.se	hogsby.se
horby.se	hoor.se	jokkmokk.se	jarfalla.se	jonkoping.se
kalix.se	kalmar.se	karlsborg.se	karlshamn.se	karlskoga.se
karlskrona.se	karlstad.se	katrineholm.se	kil.se	kinda.se
kiruna.se	klippan.se	knivsta.se	kramfors.se	kristianstad.se
kristinehamn.se	krokom.se	kumla.se	kungsbacka.se	kungsor.se
kungalv.se	kavlinge.se	koping.se	laholm.se	landskrona.se
laxa.se	lekeberg.se	✓ leksand.se	lerum.se	lessebo.se
lidingo.se	lidkoping.se	lilaedet.se	lindesberg.se	linkoping.se
ljungby.se	ljusdal.se	ljusnarsberg.se	lomma.se	ludvika.se
lulea.se	lund.se	lycksele.se	lysekil.se	malmo.se
malung-salen.se	mala.se	mariestad.se	markaryd.se	mark.se
mellerud.se	mjolby.se	mora.se	✓ motala.se	mullsjo.se
munkedal.se	munkfors.se	molndal.se	✓ monsteras.se	morbylanga.se
nacka.se	nora.se	norberg.se	nordanstig.se	nordmaling.se
norrkoping.se	✓ norrtalje.se	norsjo.se	nybro.se	nykvarn.se
nykoping.se	nynashamn.se	nassjo.se	✓ ockelbo.se	✓ olofstrom.se
orsa.se	orust.se	osby.se	oskarshamn.se	✓ ovanaker.se

interlan

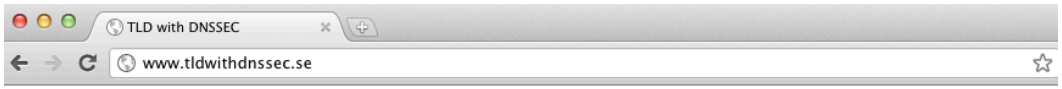
Registrarer

100procent.com	NameISP.com	ab.se	admax.se	aitos.se
aname.net	atellus.se	attendit.se	ballou.se	bgpm.se
bikab.com	binero.se	birdname.se	bluerange.se	buildit.net
cedel.se	citynetwork.se	communique.se	crossnet.se	dgc.se
domaininfo.com	domanregister.se	driftbolaget.se	egensajt.se	ember.se
euroitsolutions.se	fagerlind.com	forss.se	✓ frobbit.se	griffel.se
groth.se	hogia.se	ilait.se	imegasystem.se	infracom.se
internet.se	internetbolaget.se	internetsrs.com	✓ intron.net	iten.se
itkoncept.se	itproductions.se	jamtport.se	julian.se	kontorsspecial.se
✓ leissner.se	levonline.com	loopia.se	lopnet.se	mailbox.se
melbourneitcbs.com	natdesign.m.se	neware.se	nictrade.se	nmugroup.com
nordreg.se	oderland.com	odibo.se	patrafee.com	praktit.se
premiumregistrations.se	proteamity.se	quicknet.se	rackfish.com	registrera-doman.se
riktad.se	rymdweb.se	sbbs.se	✓ sedirekt.se	servercentralen.se
smelink.se	softnetwork.se	solidparkductus.se	solutions.se	space2u.com
standardbolaginternet.se	sveabyran.se	svenskadomaner.se	svenskaexportmedia.com	swip.net
t5.se	✓ tdc.se	telia.com	venabler.com	vikab.com
vildmarksdata.se	vmi.se	webbhosting.nu	webbnamn.nu	webcows.se
webhotellet.net	winstart.se	wk.se	wopsa.se	wpsyd.com
wwwgbg.se	yamito.se	yask.se	ymex.se	

Är det nå drag i DNSSEC då?



Finns det fler än .SE som gör det?

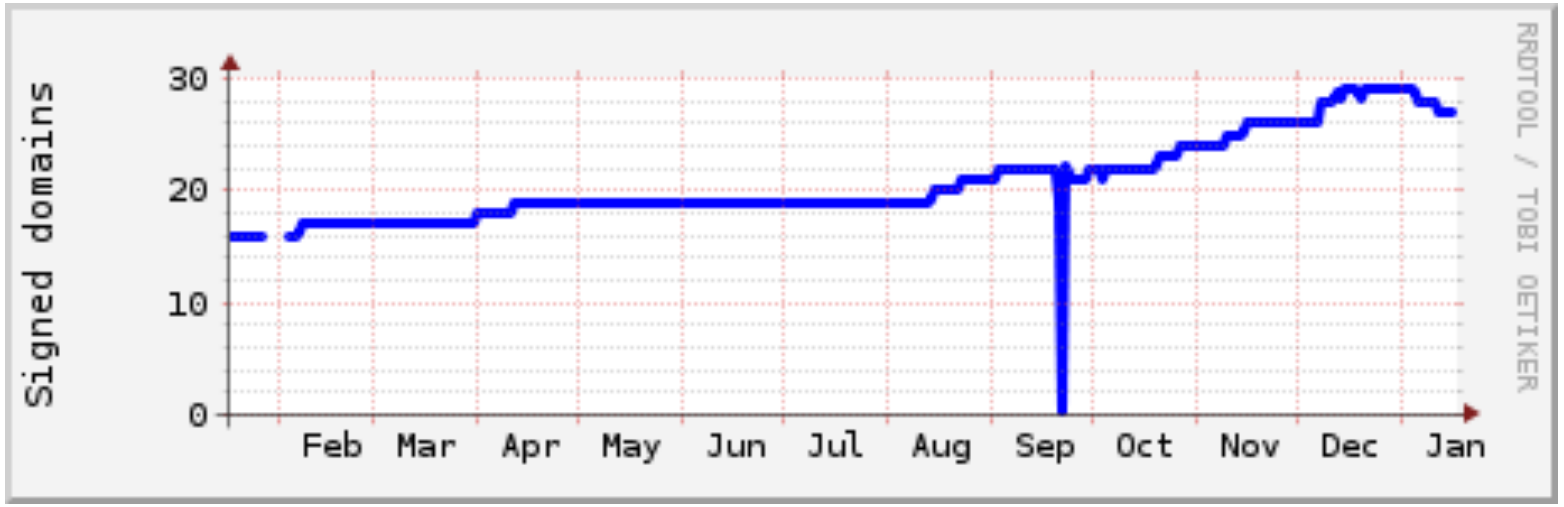


TLD with DNSSEC

www.tldwithdnssec.se just list TLD's who have signed the TLD and if they have published DS in the root..
Contact: tobbe (at) interlan punkt se
Some contribution from Stephan Lagerholm and Jakob Schlyter

TLD	Key Algo	Key Len	DS Algo	Denial
AC.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 5 021d
AG.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
AM.	RSASHA1NSEC3	2048	SHA2	NSEC3 1 0 10 76931f
ARPA.	RSASHA256	2048	SHA1SHA2	NSEC
ASIA.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
AT.	RSASHA256	2048	NOT-IN-ROOT	NSEC3 1 0 5 4a9f8b7e2671e561
BE.	RSASHA256	2048	SHA1SHA2	NSEC3 1 0 5 1a4e9b6c
BG.	RSASHA1	4096	SHA1SHA2	NSEC
BIZ.	RSASHA256	2048	SHA1SHA2	NSEC
BR.	RSASHA1	1280	SHA1	NSEC
BZ.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
CAT.	RSASHA512	2048	SHA2	NSEC3 1 0 12 ae7a5f02adac6f45
CH.	RSASHA1NSEC3	1024	SHA2	NSEC3 1 0 2 fed8
CL.	RSASHA256	2048	SHA2	NSEC3 1 0 2 a45f80464bbaefba483973a43b8f78cb
CO.	RSASHA256	2048	SHA1SHA2	NSEC
COM.	RSASHA256	2048	SHA2	NSEC3 1 0 0 -
CZ.	RSASHA512	2048	SHA2	NSEC3 1 0 10 04a65146089adc2a
DE.	RSASHA256	2048	SHA2	NSEC3 1 0 15 ba5eba11
DK.	RSASHA256	2048	SHA2	NSEC3 1 0 17 d62599df241f8204
EDU.	RSASHA256	2048	SHA2	NSEC3 1 0 0 -
EU.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 5ca1ab1e
FI.	RSASHA256	2048	SHA2	NSEC3 1 0 5 d9945ce53b53a52d
FR.	RSASHA256	2048	SHA2	NSEC3 1 0 1 badfe11a
GI.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
GL.	RSASHA256	2048	SHA2	NSEC3 1 0 10 6cd13fb2
GOV.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 8 4c44934802d3
GR.	RSASHA1NSEC3	2048	SHA2	NSEC3 1 0 10 beef
HN.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
IN.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
INFO.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
IO.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 5 021d
JP.	RSASHA256	2048	SHA1SHA2	NSEC3 1 0 8 731ea38c88
KG.	RSASHA1	1024	SHA1SHA2	NSEC
KR.	RSASHA1NSEC3	2048	SHA2	NSEC3 1 0 10 96e920
LA.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 150 46a94223
LC.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
LI.	RSASHA1NSEC3	1024	SHA2	NSEC3 1 0 2 44a3
LK.	RSASHA1	2048	SHA1SHA2	NSEC
LU.	RSASHA256	2048	SHA2	NSEC3 1 0 3 e780d40a
ME.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
MIL.	RSASHA256	2048	NOT-IN-ROOT	NSEC3 1 0 10 fdee
MM.	RSASHA256	2048	SHA1	NSEC
MN.	RSASHA1NSEC3	2048	SHA1SHA2	NSEC3 1 0 1 d399eaab
MUSEUM.	RSASHA512	2048	SHA2	NSEC3 1 0 12 3b616ccef9d86adc
MY.	RSASHA256	2048	SHA1SHA2	NSEC3 1 0 10 a97693
NA.	RSASHA1	4096	SHA1	NSEC
NC.	RSASHA256	2048	SHA2	NSEC3 1 0 10 140238c4

Problem


Signed domains
30
20
10
0
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
RRDTOOL / TOBI OETIKER

Testet innehöll fel

stockholm.se, 2012-01-23 21:25:07
Testet utfördes med DNSCheck v1.2.4

Förenklat resultat | Avancerat resultat

Delegering

DNS-server

- **DNS-server ns1.stockholm.se**
  - Kunde inte hitta baklängesadress för 2a03:c780:12:2400:0:0:0:10 (0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.2.2.1.0.0.0.8.7.c.3.0.a.2.ip6.arpa.).
  - DNS-servern ns1.stockholm.se (2a03:c780:12:2400:0:0:0:10) svarar inte på anrop via UDP.
  - DNS-servern ns1.stockholm.se (2a03:c780:12:2400:0:0:0:10) svarar inte på anrop via TCP.
- **DNS-server ns2.stockholm.se**
  - Kunde inte hitta baklängesadress för 2a03:c780:13:2400:0:0:0:10 (0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.2.3.1.0.0.0.8.7.c.3.0.a.2.ip6.arpa.).

Konsekvent uppsättning

SOA

- Kunde inte hitta baklängesadress för 2a03:c780:12:2400:0:0:0:10 (0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.2.2.1.0.0.0.8.7.c.3.0.a.2.ip6.arpa.).

Konnektivitet

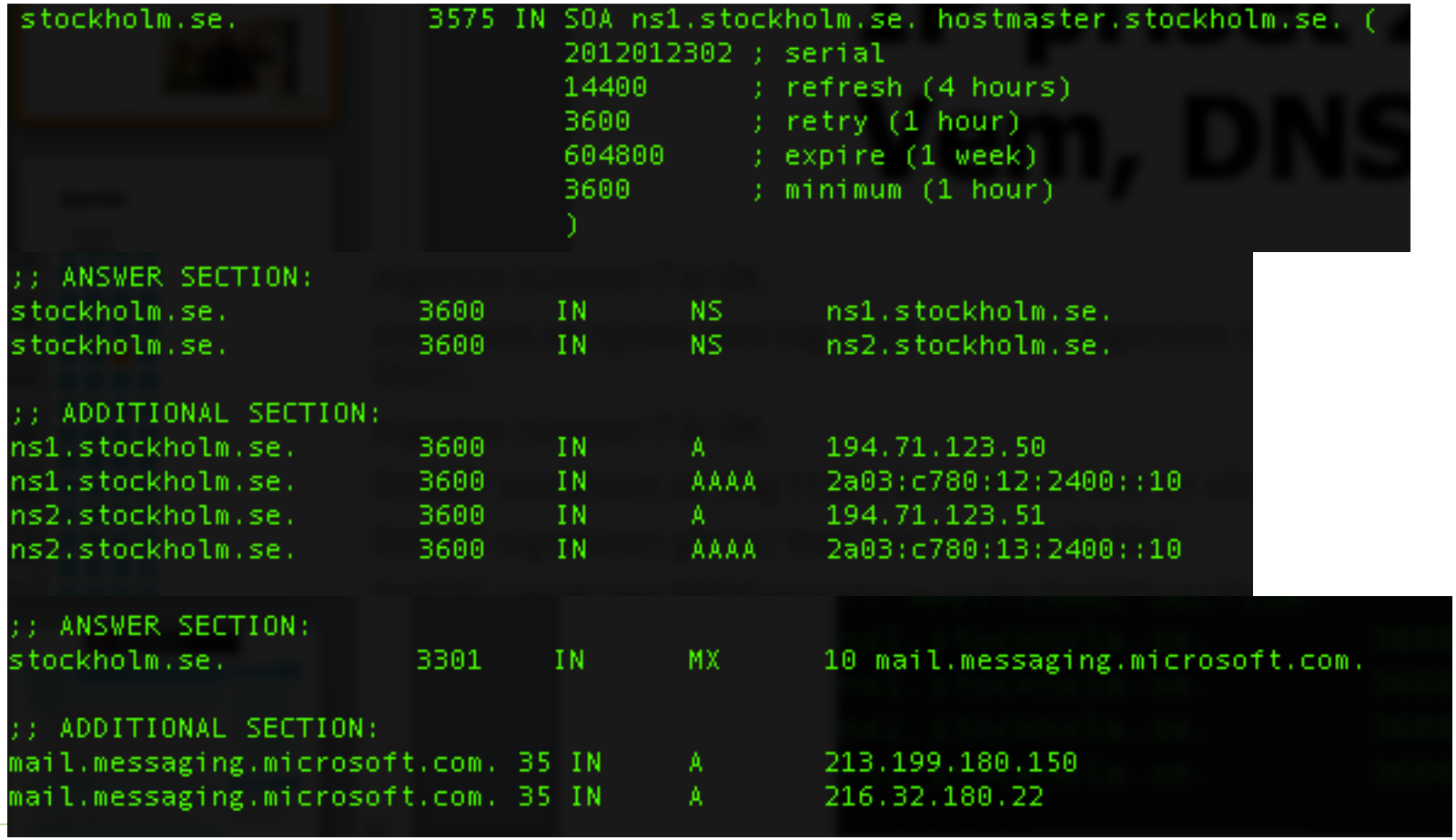
Tidigare test

- 2012-01-23 21:25:07
- 2011-10-06 13:24:36
- 2011-10-03 14:18:16
- 2011-09-26 09:41:48
- 2011-09-23 14:39:51
- 2011-09-23 13:49:36
- 2011-09-23 13:20:29
- 2011-09-23 12:19:11
- 2011-09-23 12:04:59
- 2011-09-23 10:48:57

Sida 1/12

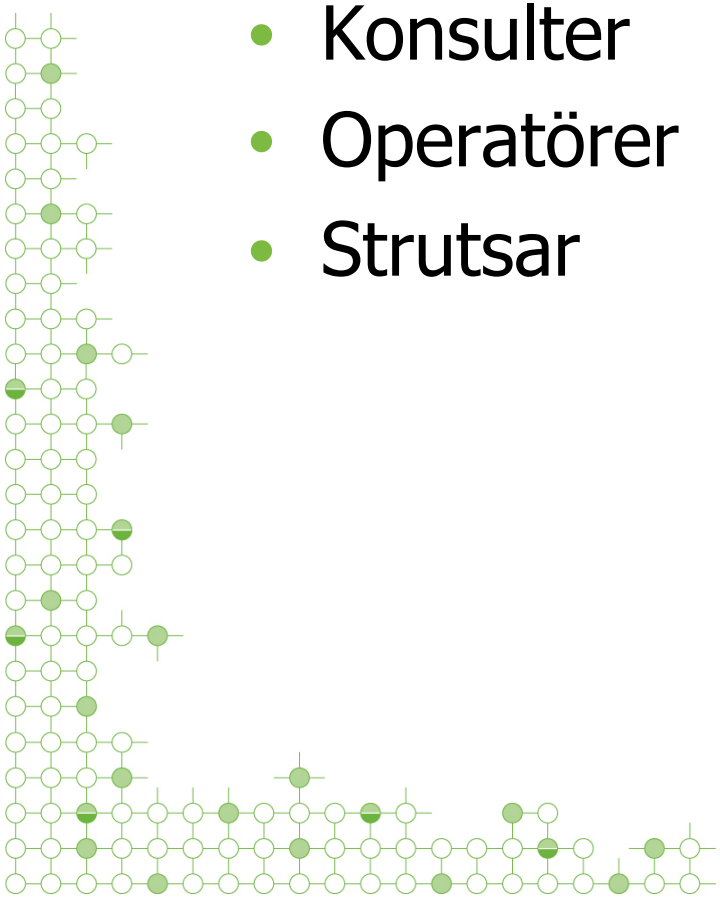
Förklaring

- Testet var ok
- Testet innehöll varningar
- Testet innehöll fel
- Testet utfördes inte


stockholm.se. 3575 IN SOA ns1.stockholm.se. hostmaster.stockholm.se. (
2012012302 ; serial
14400 ; refresh (4 hours)
3600 ; retry (1 hour)
604800 ; expire (1 week)
3600 ; minimum (1 hour)
)
;; ANSWER SECTION:
stockholm.se. 3600 IN NS ns1.stockholm.se.
stockholm.se. 3600 IN NS ns2.stockholm.se.
;; ADDITIONAL SECTION:
ns1.stockholm.se. 3600 IN A 194.71.123.50
ns1.stockholm.se. 3600 IN AAAA 2a03:c780:12:2400::10
ns2.stockholm.se. 3600 IN A 194.71.123.51
ns2.stockholm.se. 3600 IN AAAA 2a03:c780:13:2400::10
;; ANSWER SECTION:
stockholm.se. 3301 IN MX 10 mail.messaging.microsoft.com.
;; ADDITIONAL SECTION:
mail.messaging.microsoft.com. 35 IN A 213.199.180.150
mail.messaging.microsoft.com. 35 IN A 216.32.180.22

Problem

- Outsourcing
- Konsulter
- Operatörer
- Strutsar



Varför IPv6?


The 5th Wave
By Rich Tennant
©RICHTENNANT
NO INTERNET ADDRESS
PLEASE

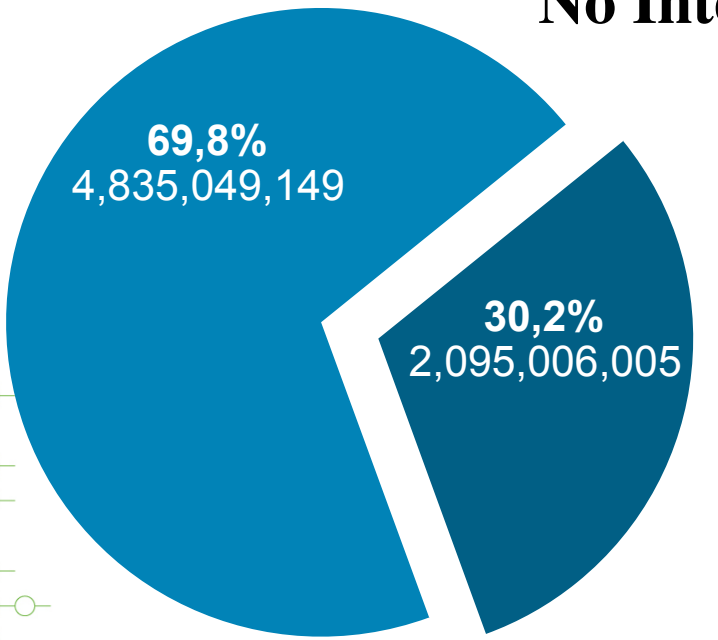
THE FUTURE IS FOREVER

6 JUNE 2012

Major Internet service providers (ISPs), home networking equipment manufacturers, and web companies around the world are coming together to permanently enable IPv6 for their products and services by 6 June 2012.

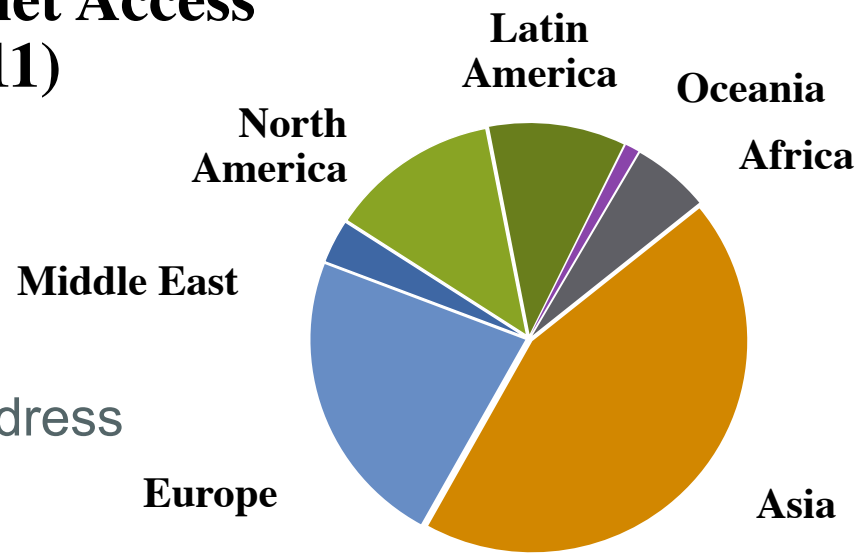
Organized by the Internet Society, and building on the successful one-day World IPv6 Day event held on 8 June 2011, World IPv6 Launch represents a major milestone in the global deployment of IPv6. As the successor to the current Internet Protocol, IPv4, IPv6 is critical to the Internet's continued growth as a platform for innovation and economic development.

Most of the World has NO Internet Access



No Internet Access (Mar11)

Internet Access (Mar11)



- The world majority still needs an IP address

….and clean water, vaccinations etc…

interlan

Varför IPv6 ?

Topp 10 som gör IPv6 ’bättre' än IPv4

1. **Större adressrymd**
2. **Bättre end-to-end connectivity**
3. **Autokonfigurering av adresser**
4. **Enklare header**
5. **Bättre säkerhet (IPSEC – ESP, AH)**
6. **Bättre quality of services**
7. **Bättre multicast och anycast funktionalitet**
8. **Mobila funktioner**
9. **Enklare administration**
10. **Enkel övergång från IPv4**

interlan

Why IPv6 ?

Top 10 som gör IPv6 ’bättre' än IPv4

- ✓ Större adressrymd
- ✓ Bättre end-to-end connectivity
- ✗ Autokonfigurering av adresser
- ~ Enklare header
- ~ Bättre säkerhet (IPSEC – ESP, AH)
- ~ Bättre quality of services
- ~ Bättre multicast och anycast funktioner
- ~ Mobila funktioner
- ✗ Enklare administration
- ✗ .Enkel övergång från IPv4

interlan

Problem kommer att uppstå

- **Kända problem med IPv6**
  Vad ser vi för risker med Ipv6? En risk är att man ställs inför en ny teknik och att man inte riktigt vet vad som kan hända vid införandet för att man saknar praktisk erfarenhet. Kända problem som t.ex. tunnlar som automatkonfigureras och trafik som går andra vägar än vad som är tänkt är bara exempel på problem man kan tänkas ställas inför.

  Vi har pratat med kollegor i branschen som har haft problem vid användning av Teredo tunnlar. Kollegorna har beskrivit hur plötsligt företagets lokala nätverk stannade upp och blev långsamt. Alla inblandade var tekniskt intresserade och laborerade på sin fritid hemma med IPv6 för att lära sig att första□ vilka problem man kan tänkas ställas inför. När dessa inblandade använde sina bärbara datorer hemma och på kontoret med IPv6 konfigurerat sa□ började datorerna som var anslutna på kontoret att automatiskt konfigurera sig och hitta en Teredo tunnel hem till en av medarbetarnas hemmaserver som satt kopplad på en långsam DSL förbindelse som därmed blev default gateway för hela kontoret.

- Men INTE det som beskrivs ovan!!!!

IPv6ready.org

Details of Logo 02-C-000430

TOP > 02-C-000430

IN-2-C-20091202-000118

Management Application Form Extended Test Categories

Logo ID	02-C-000430
Approved Date	2010/01/22
Application ID	IN-2-C-20091202-000118
Applied Date	2009/12/02
Usage Agreement	Agreed
OEM Licensor's Logo ID	-
Note	-

Management Application Form Extended Test Categories

Target Information	**Application Phase**	Phase-2
	Test Category	Core Protocols
	Vendor Name	Elitecore Technologies Ltd.
	Country	IN
	Product Name	Cyberoam UTM Appliances
	Product Version	10_00_0045
	Product Classification	Router

~~IPv6ready.org~~

Worldwide Partner

Cyberoam Securing You

Solutions | Products | Partners | Training & Events | Support | Company

Home > Products > IPv6 Ready

IPv6 Ready

Ready for the new Internet

Cyberoam is "IPv6 Ready" Gold logo certified, making it future-ready when the current IPv4 Internet addressing system moves to IPv6 to meet the high demand for IP addresses.

Cyberoam supports organizations' preparedness for the transition, with its IPv6-ready security solutions.

- Cyberoam has been certified with "IPv6 Ready" Gold logo by the IPv6 Forum.
- The Gold logo assures organizations of a smooth transition to IPv6 with Cyberoam's ability to identify and process IPv6 traffic.
- Cyberoam's Gold logo is a result of 3000+ rigorous test cases which are part of an International Testing Program by the IPv6 Forum.

interlan

Some interesting aspects of IPv6 security

- There is much less experience with IPv6 than with IPv4
- IPv6 implementations are less mature than their IPv4 counterparts
- Security products (firewalls, NIDS, etc.) have less support for IPv6 than for IPv4
- The complexity of the resulting network will increase during the transition/co-existance period:
  - Two internetworking protocols (IPv4 and IPv6)
  - Increased use of NATs
  - Increased use of tunnels
  - Use of other transition/co-existance technologies
- Lack of well-trained human resources

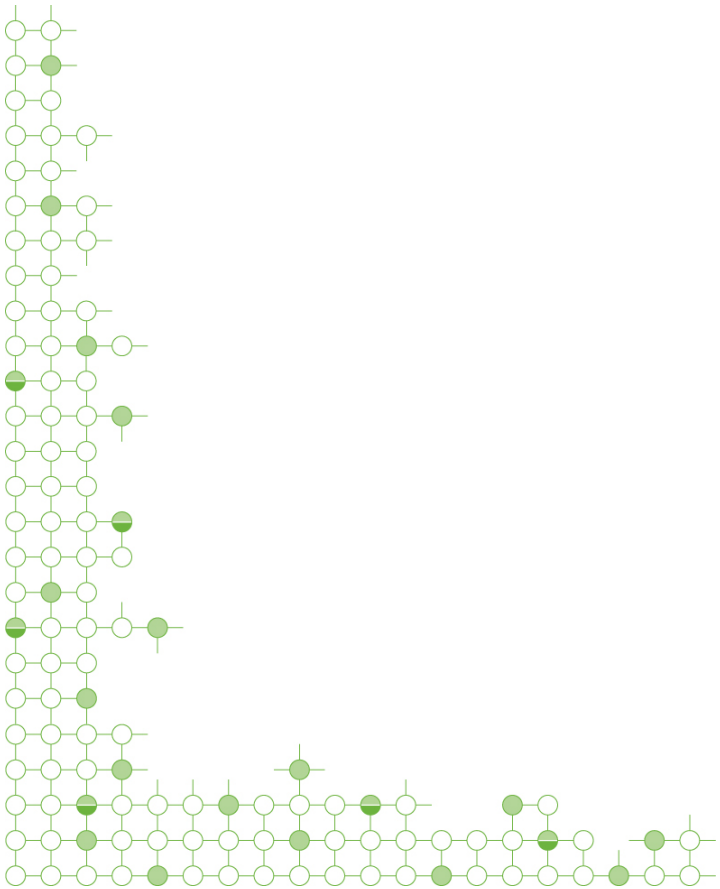
…and even then, in many cases IPv6 will be the only option to remain in this business

Ett problem

- Sk. 192.168.1.0-konsulter
  Har gjort nästan samma installation hela arbetslivet

- Med IPv6 kommer det in mer komplexitet då alla adresser är globala och t.ex kan omnumrering ske när som helst om t.ex prefix delegation/6RD används

IPv6 var ju inte säkrare....



Autoconfiguration IPv4 x IPv6

- IPv4 – DHCP, ARP

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:c
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

Autoconfiguration – IPv4

- IPv4 autoconfiguration = DHCP
- Protection mechanisms on L2 devices

  DHCP snooping
  - **Blocking DHCP responses on access ports**
  - **Prevents against fake DHCP servers**

  Dynamic ARP protection
  - **MAC-IP address database based on DHCP leases**
  - **Checking content of ARP packets on client access port**
  - **Prevents against ARP spoofing**

  Dynamic lock down
  - **The MAC-IP database is used for inspection of client source MAC and IP address.**
  - **Prevents against source address spoofing**

Possible solutions for IPv6

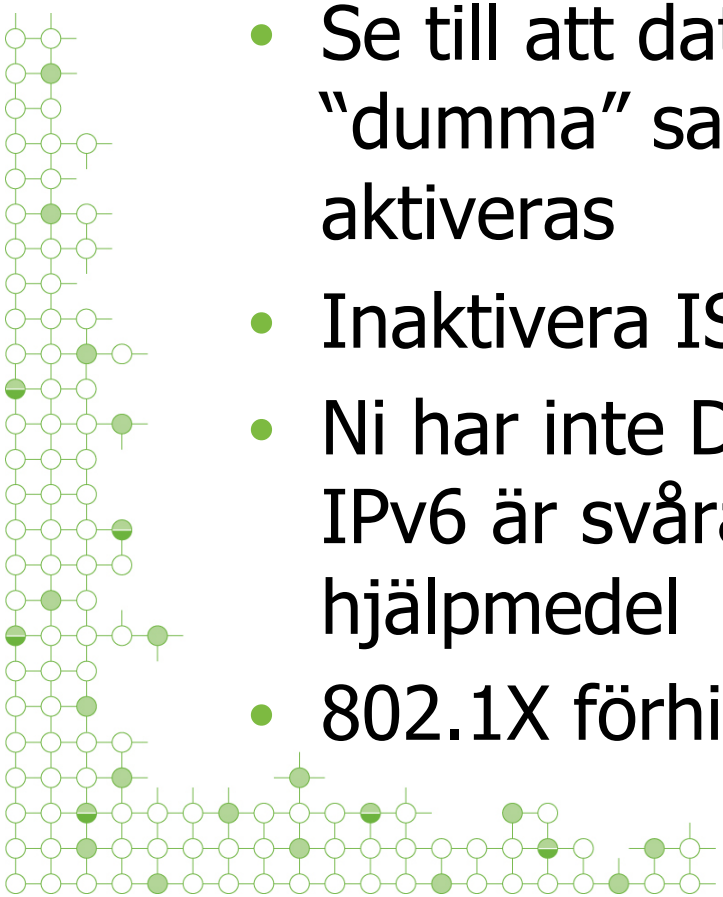
- SeND (RFC 3971, March 2005)
  - ***Based on cryptography CGA keys***
  - ***Requires PKI infrastructure***
  - ***Can not work with***
    - **Manually configured, EUI 64 and Privacy Extension addresses**
- RA-Guard (RFC 6105, February 2011)
  - ***Dropping fake RA messages on access port (RA Snooping)***
  - ***Cooperation with SeND (send proxy) – learning mode***
- SAVI (draft-ietf-savi-*, divided into more drafts)

Possible solutions for IPv6

- No support in devices
  - ***Only few vendors support some of that features***
  - ***You probably will have to replace all access switches***
- There is a easy way how to bypass such protection
  - ***CVE-2011-2395 (http://seclists.org/fulldisclosure/2011/May/446)***
  - ***Using extension headers***
  - ***ICMPv6/ND Packet fragmentation***

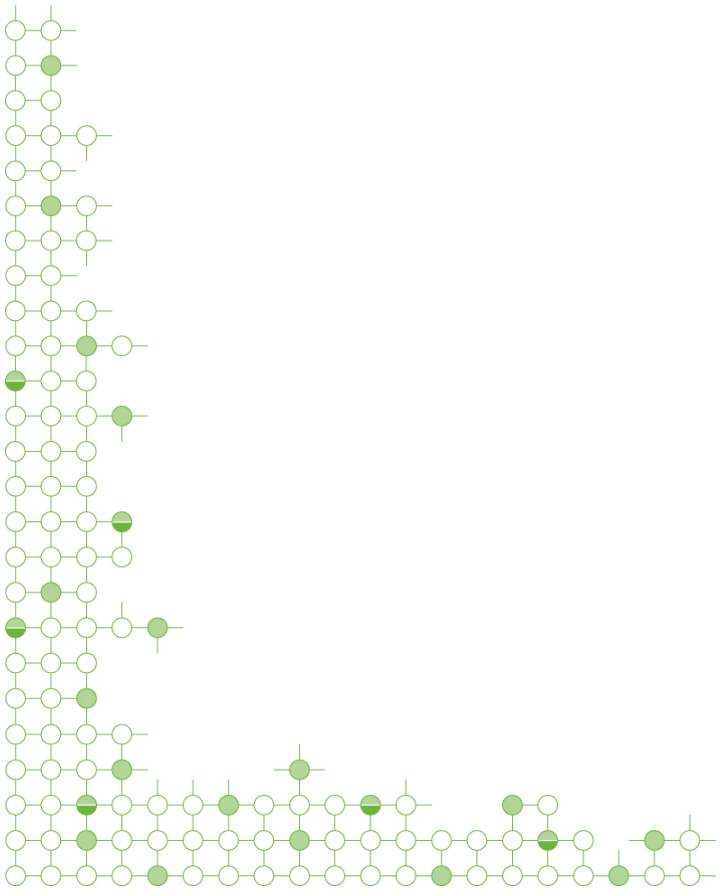
Är det farlig att köra igång v6 på företaget?

- Nej!
- Se till att datorerna är nedlåsta så inte "dumma" saker kan installeras och aktiveras
- Inaktivera ISATAP, Teredo och 6to4
- Ni har inte DAI aktiverat idag och MIM med IPv6 är svårare, för v4 finns det fina hjälpmedel
- 802.1X förhindrar okända saker nätet



Är inte Teredo, 6to4 mm. farliga????

- NEJ!



BYOD – både v4 och v6

- Med BYOD kan vi inte designa nät på traditionellt sätt - bygg de näten som bredbandsnät
- Isolera konferensrum med vlan/brandvägg
- 802.1X på det trådade
- Force forward

Bredbandsnät

- Force Forward, ett vlan/kund – Isolering mm.
- 6RD!!!

Andra problem

- Kloningsprogram

DHCPv6 – DUID

Ett problem som jag stött på några gånger är att när man aktiverar DHCPv6 så uppstår det adresskonflikter för v6-adresserna.
Problemet har alltid varit klonade Windowsburkar där DHCP Unique IDentifier varit samma för datorerna som klonats ur samma batch.
Ett sätt att lösa det är att ta bort registernyckeln för DUID med kommandot

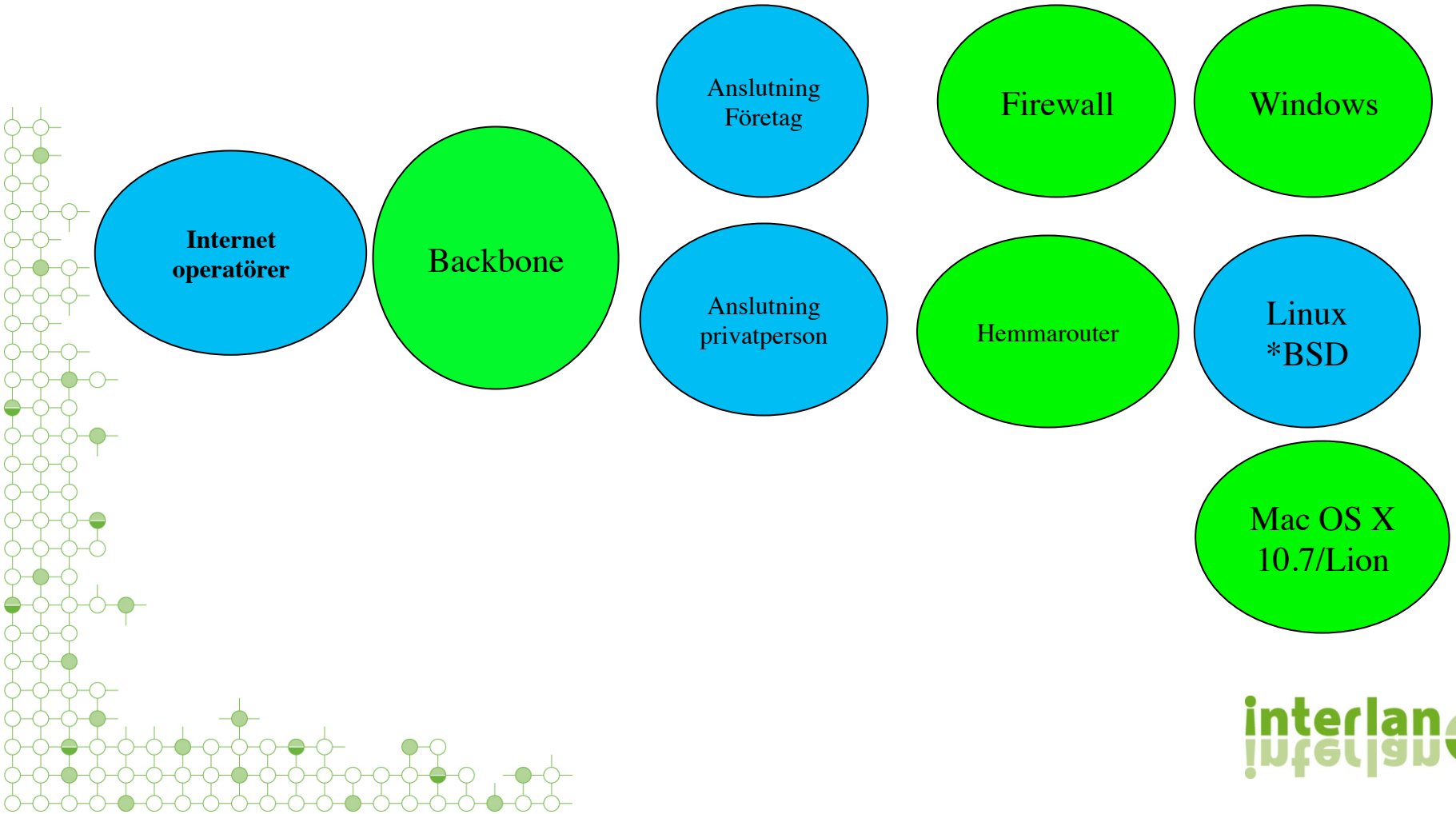
```
reg delete HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters /f /v Dhcpv6DUID
```

och starta om datorn.
Detta är en temporär lösning och kloningsprogrammet ska så klart fixa det här default.

Läs mer om DHCPv6 på RFC 3315 och IPv6friday

Vad fattas?

Grön Ok
Blå Nja
Röd Nej



interlan

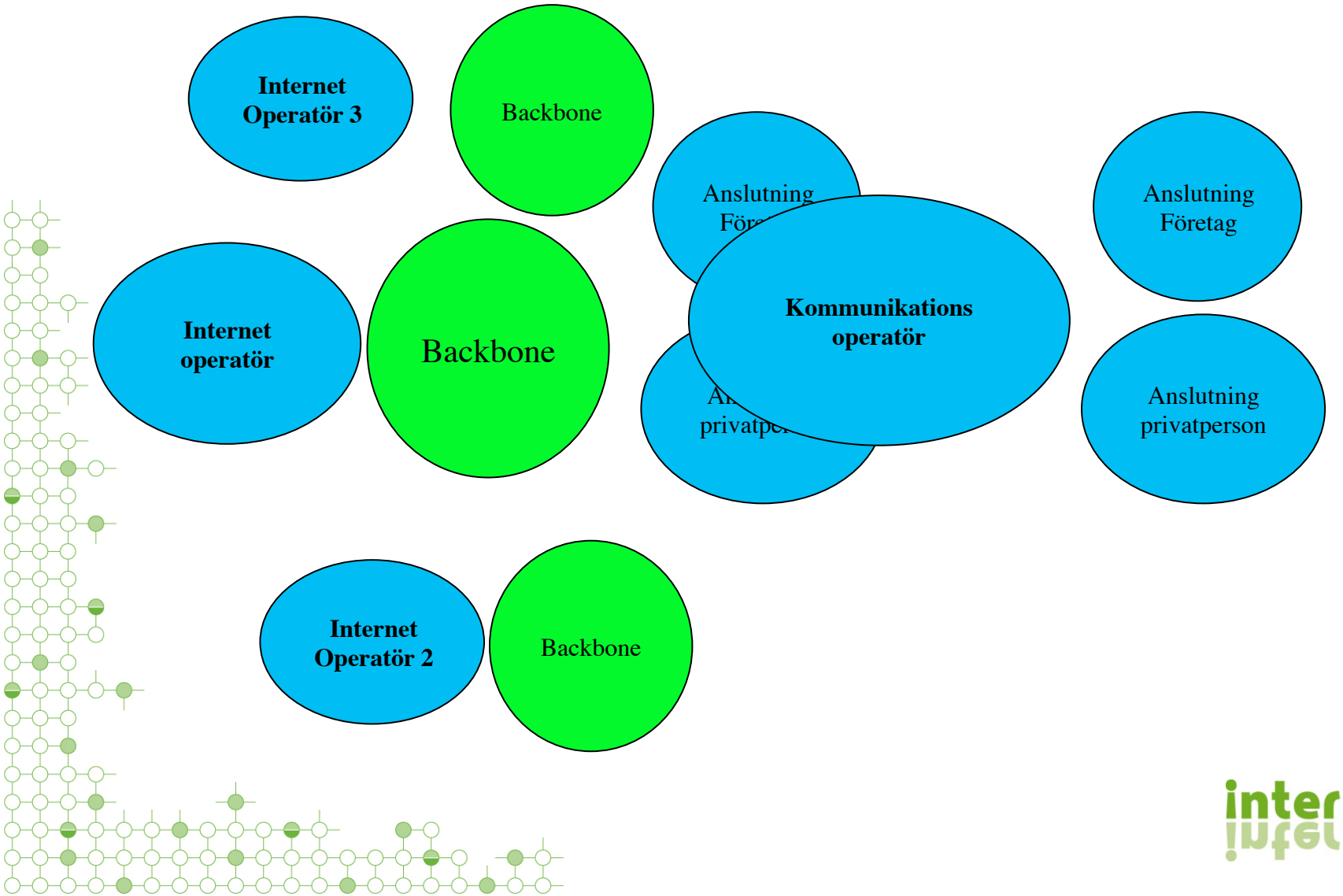
Microsoft är grön men….

- Hur är det med Lync, TMG…
- Installerar man DA enligt skolboken spärrar man v6 helt…

- (Och Office 365…)

Vad fattas?

Grön Ok
Blå Nja
Röd Nej



Operatörer

- Stora som små
- "Öppna" nät med kommunikationsoperatörer

interlan

Hur mycket IPv6 tål en julbock? Andra säsongen

Hur mycket IPv6 tål en julbock? Andra säsongen

Hur mycket IPv6 tål en julbock? Andra säsongen

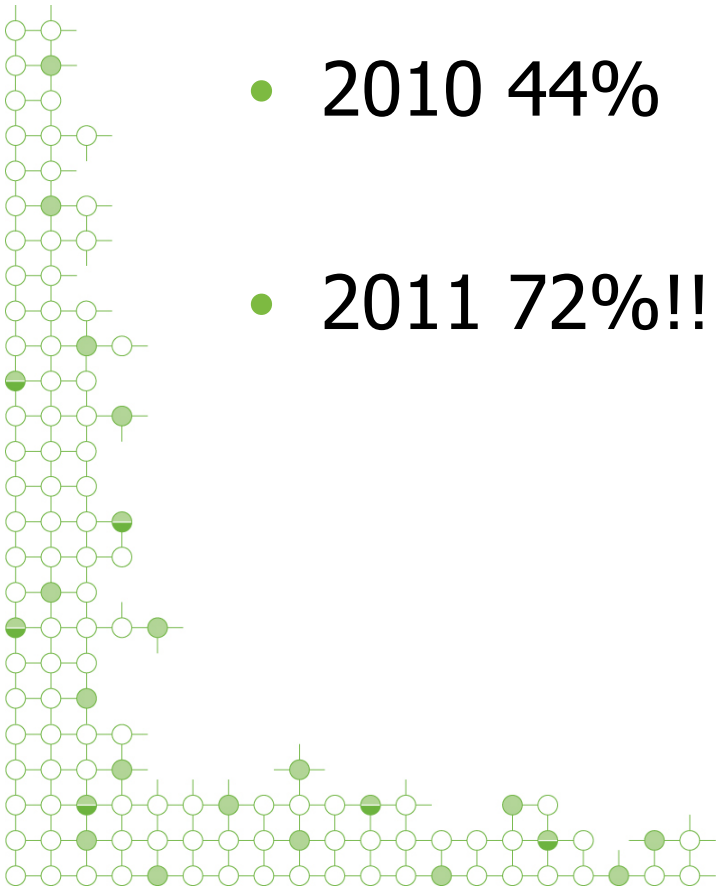
IPv6

- Native IPv6 0.5%!!! (2010 0.1%)
- 52% kunde nå ipv6.jpg med native, 6to4 eller Teredo (2010 26%)
- Av total IPv6
  74% Teredo
  25% 6to4
  1% Native

Validering av DNSSEC?

- `<img src="pic.try2readme.se/dnssec.jpg" width=0 height=0 />`

- 2010 44%
- 2011 72%!!



interlan

DNSSEC and IPv6

www.dnssecandipv6.se

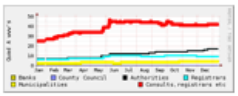
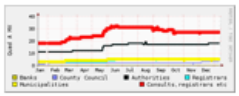
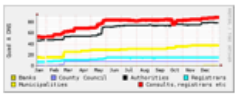
DNSSEC and IPv6

Home | My CV (Swedish Only) | Open Source Firewall with IPv6 Support | Vinter | World IPv6 day | Digitaliseringsrådet | Bredbandsforum

DNSSEC and IPv6

Posted on April 11, 2011 by admin

This website is a collection page of my geeksites with information about IPv6 and DNSSEC usage in Swedish municipalities and authorities
Sites about DNSSEC and IPv6, updated daily and everyone except tldwithdnssec now have graphs.

IPv6

IPv6akuten – Swedish only
Municipalities with IPv6
Authorities with IPv6
Swedish registrars and IPv6
County council and IPv6
Swedish banks and IPv6
Is your domain IPv6-ready?
Are you ready for IPv6?
Swedish OMX30 and IPv6
www.ipv6.tk, test if you have IPv6

DNSSEC and DNS health

Municipalities with DNSSEC
Swedish banks and DNSSEC
Swedish registrars and DNSSEC
County council with DNSSEC
Authorities with DNSSEC
TLD with DNSSEC

Search

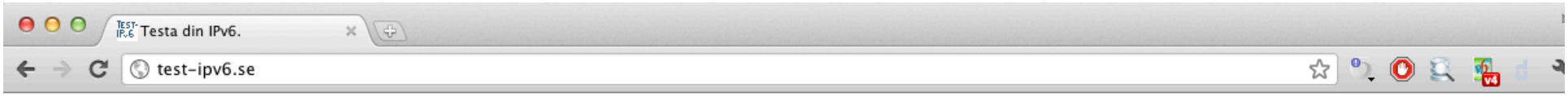
Search

Pages

- Bredbandsforum
- Digitaliseringsrådet
- My CV (Swedish Only)
- Open Source Firewall with IPv6 Support
- Vinter
- World IPv6 day

Recent Posts

- DNSSEC and IPv6



Testa IPv6 | FAQ | Global lansering av IPv6 | Lokala klockslag | Spegelsidor

Testa din IPv6-anslutning

Summering | Tester körda | Teknisk information | Dela resultat / Kontakt

Din publika IPv4-adress ser ut att vara 192.71.21.2

Din publika IPv6 adress ser ut att vara 2001:67c:2448:15:5cd1:3184:47de:ab0a

Dagen för global lansering av IPv6 är 6 Juni, 2012. **Goda nyheter!** Din nuvarande webbläsare på denna dator och på denna plats förväntas fortsätta fungera efter lanseringen. *[mer information]*

Gratulerar! Det ser ut som du har fungerande IPv4 och IPv6. Om en webbsida publiceras med IPv6 kommer du kunna nå den över IPv6. Din webbläsare föredrar IPv6 framför IPv4 (detta är det förväntade resultatet).

Din DNS (förmodligen hos din Internetleverantör) ser ut att ha IPv6-anslutning.

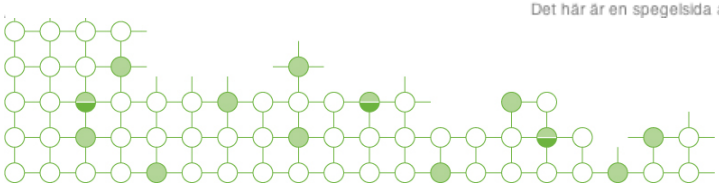
Dina poäng är

10/10	för IPv4 stabilitet och beredskap, om både IPv4 och IPv6 används för publicering
10/10	för IPv6 stabilitet och beredskap, om bara IPv6 används för publicering

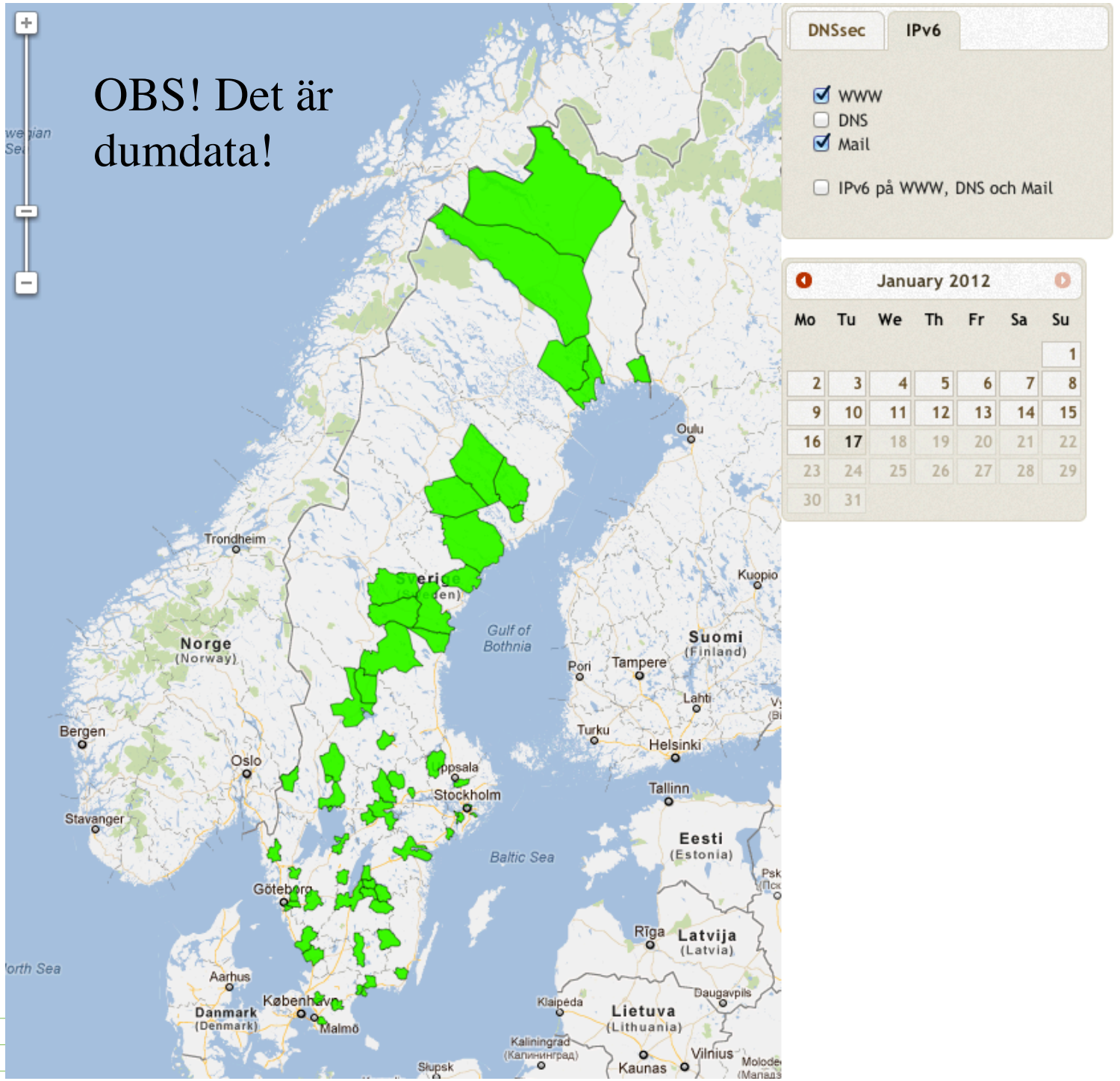
Klicka för att se testresultat

Need something simpler? http://omgipv6day.com Spread the word!

Copyright (C) 2010, 2012 Jason Fesler. All rights reserved. -- r692
Mirrors | Mission | Source | Email - - Attributions | Debug
Det här är en spegelsida av test-ipv6.com. Åsikter uttryckta här kanske inte överensstämmer med ägaren av denna sidan.



interlan


OBS! Det är dumdata!
DNSsec
IPv6
WWW
DNS
Mail
IPv6 på WWW, DNS och Mail
January 2012
Mo Tu We Th Fr Sa Su
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31
Oulu
Kuopio
Trondheim
Norge
(Norway)
Gulf of Bothnia
Suomi
(Finland)
Pori
Tampere
Lahti
Turku
Helsinki
Bergen
Oslo
Stockholm
Tallinn
Stavanger
Eesti
(Estonia)
Baltic Sea
Göteborg
Rīga
Latvija
(Latvia)
Aarhus
København
Danmark
(Denmark)
Malmö
Klaipėda
Lietuva
(Lithuania)
Daugavpils
Kaliningrad
Vilnius
Kaunas
Słupsk

Summering – problem DNSSEC – IPv6

- Konsulter
- Strutsar
- Operatörer
- "Öppna" nät
- Outsoursing


IPv6
IPv6
CAN'T LIVE
WITHOUT YOU