IPv6 and security

Myth or reality?

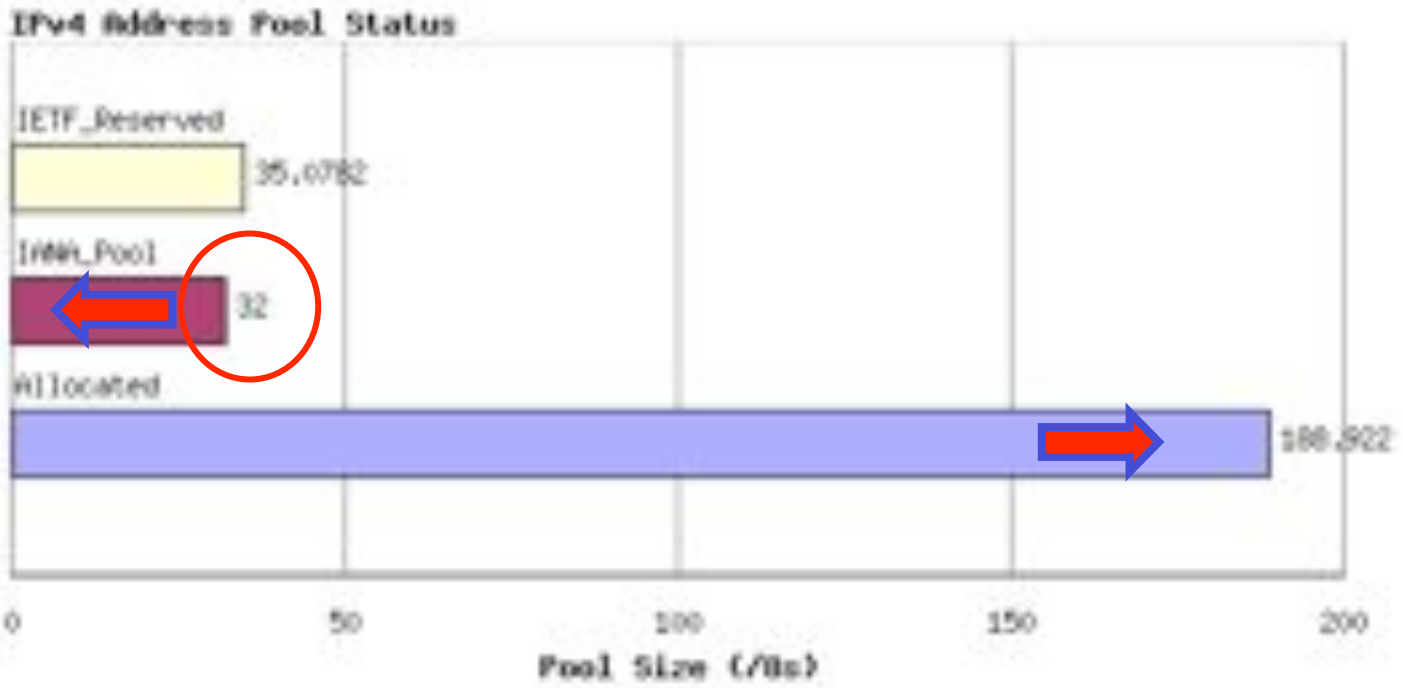
Patrik Fältström
paf@cisco.com

Do we need IPv6?

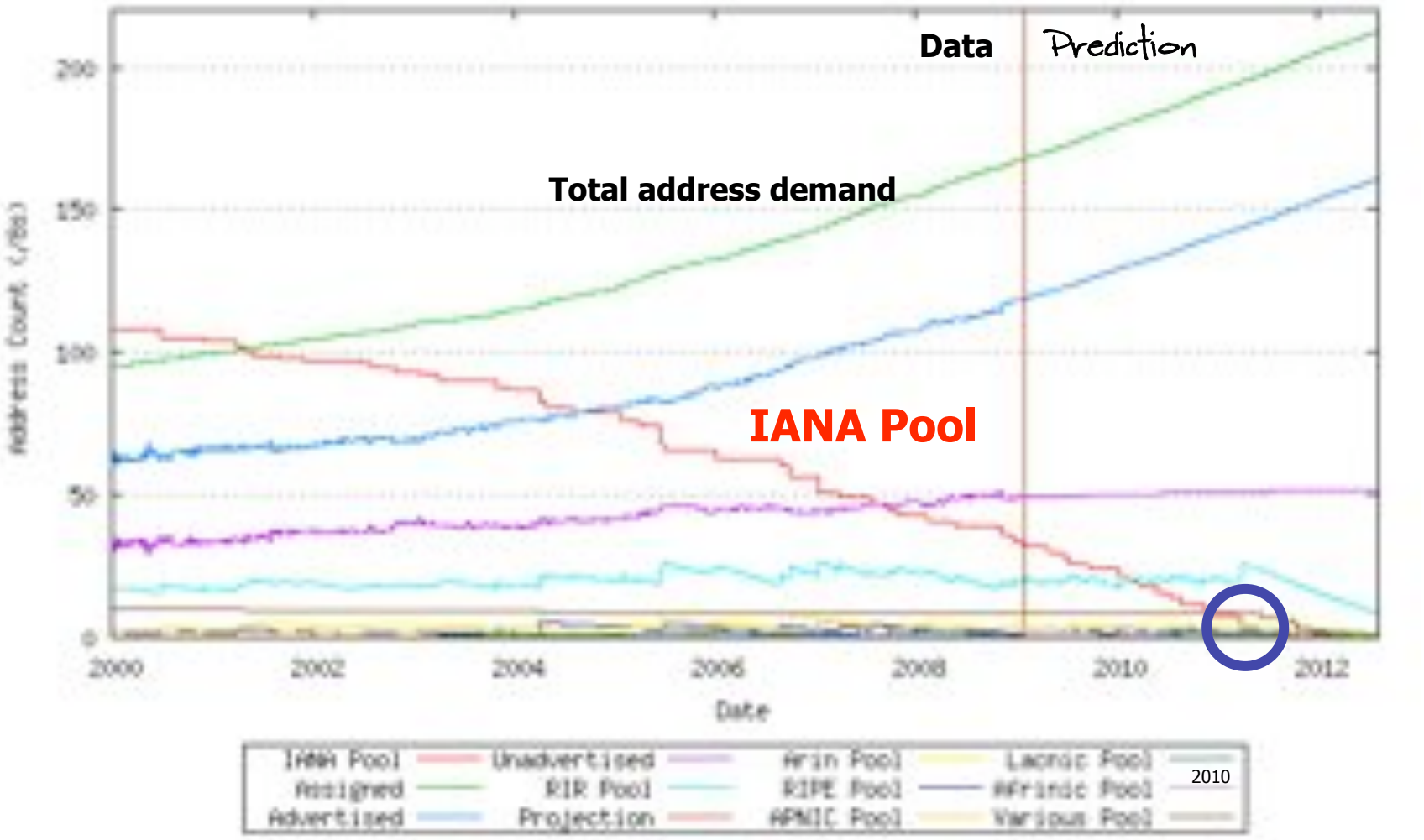
Before looking at IPv6 and Security, we have to look at alternatives to IPv6.

Do we have a plan B?

Today


IPv4 Address Pool Status
IETF_Reserved
35.0782
IANA_Pool
32
Allocated
188.922
0
50
100
150
200
Pool Size (/8s)

Ooops!


Data
Prediction
Total address demand
IANA Pool
200
150
100
50
0
2000
2002
2004
2006
2008
2010
2012
Date
IANA Pool
Unadvertised
Arin Pool
Lacnic Pool
Assigned
RIR Pool
RIPE Pool
Afrinic Pool
Advertised
Projection
APNIC Pool
Various Pool
2010

That's 2nd April 2011

That's a highly uncertain prediction - it could be out by as much as 18 months

http://ipv4.potaroo.net

Let's say some time between late 2009 and early 2011

We know there will be a point in time when an admin that want to add a device can not get an IPv4 address "the normal way".

What choices does that person have?

1. Add another NAT
2. Renumber, change topology
3. Start use IPv6

why is IPv6 better?

What is important to know?

- IPv6 is very similar to IPv4
- We do not know as much about IPv6 as IPv4
- Many arguments about IPv6 and security are overstated
- Many parties are nervous over features lacking in IPv6

This is why it is a good idea to start use IPv6 now!

Why is IPv6 better?

- It is harder to scan address space
- In core routing, you can use link local addresses for P-P or PE-CE interfaces
- Higher chance one use end to end connections

P-P: Point to point, PE-CE: Provider Edge - Customer Edge

Why is end to end architecture good?

Traceability

No shared addresses between nodes

Logging required in NATs to trace is not small

Overlapping addresses

No attack from co—addressed organisations against each other (for example ICMP unreachable packet being too big forcing PMTUd to decrease bandwidth)

NATs / Application level gateways

Many applications (maps.google.com, iTunes) opens tons of parallel TCP sessions, so how does this scale?

But what do people complain about?

- IPv6-only exposes IPv4 dependencies in applications and middleware.
  - “Thunderbird and Firefox disable IPv6 dns by default”
- Failures when translating between versions exposes the invalid assumptions that some ISPs have been making.
  - “Linux NAT-PT (naptd) has stability issues and wedges”
- Provisioning model assumptions are exposed by new ways of handling addressing.
  - “it's a real pain in the ass to get DHCPv6 working”
  - “why doesn’t the RA include the DNS service”
- Typing ‘ : ’ instead of ‘ . ’ in a literal address exposes how resistant people are to change.
  - “why do we have to type colon instead of dot like in a real address”

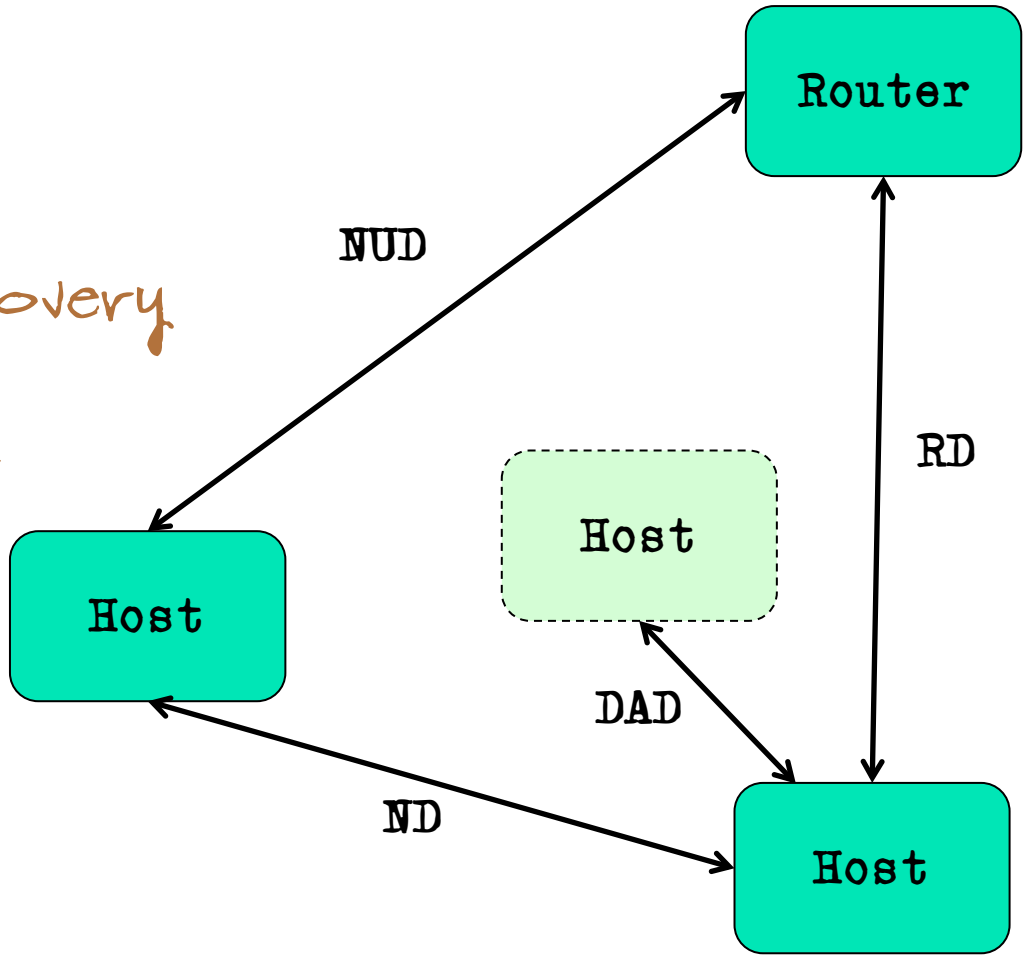
But, those are not security problems, right?

ARP spoofing?

SEND

Secure the Neighbor Discovery Protocols (NDP) with cryptographic mechanisms

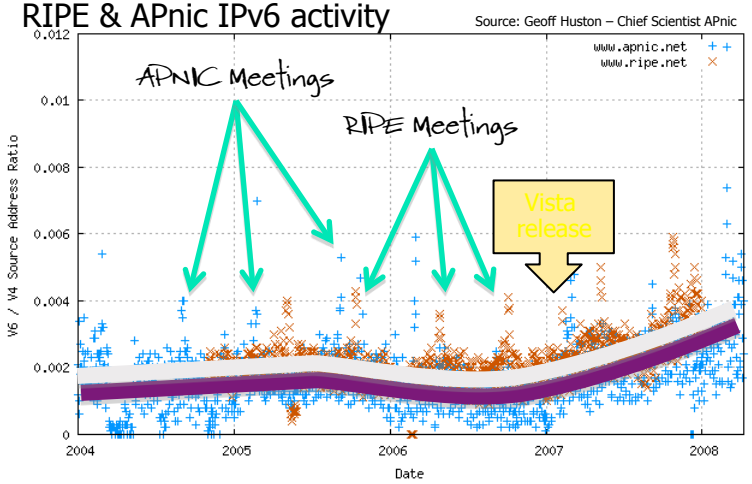
Only LAN environments



http://www.ipv6.com/articles/research/Secure-Neighbor-Discovery.htm

But people use IPv6!

RIPE & APnic IPv6 activity



ipv6.google.com & ipv6.google.com.cn

http://[2001:252:0:1::2008:6]

http://[2620:0:2d0:1::193]

http://[2a01:e0c:1:1599::1]

http://[2001:4830:2480:11::137]

http://[2001:1890:1112:1::20]

http://[2001:dc0:2001:0:4608:20::]

http://[2001:610:240:11::c100:1319]

http://[2001:4f8:fff6::21]

http://[2001:9b0:1:104:230:48ff:fe56:31ae]

http://[2001:500:4:13::81]

http://[2001:48a8:6880:95::21]

http://[2001:630:200:4240:203:baff:fe87:14ed]

http://[2a01:48:1:0:2e0:81ff:fe05:4658]

http://[2001:440:fff9:100:202:b3ff:fea4:a44e]

http://[2a01:a8:0:5::26]

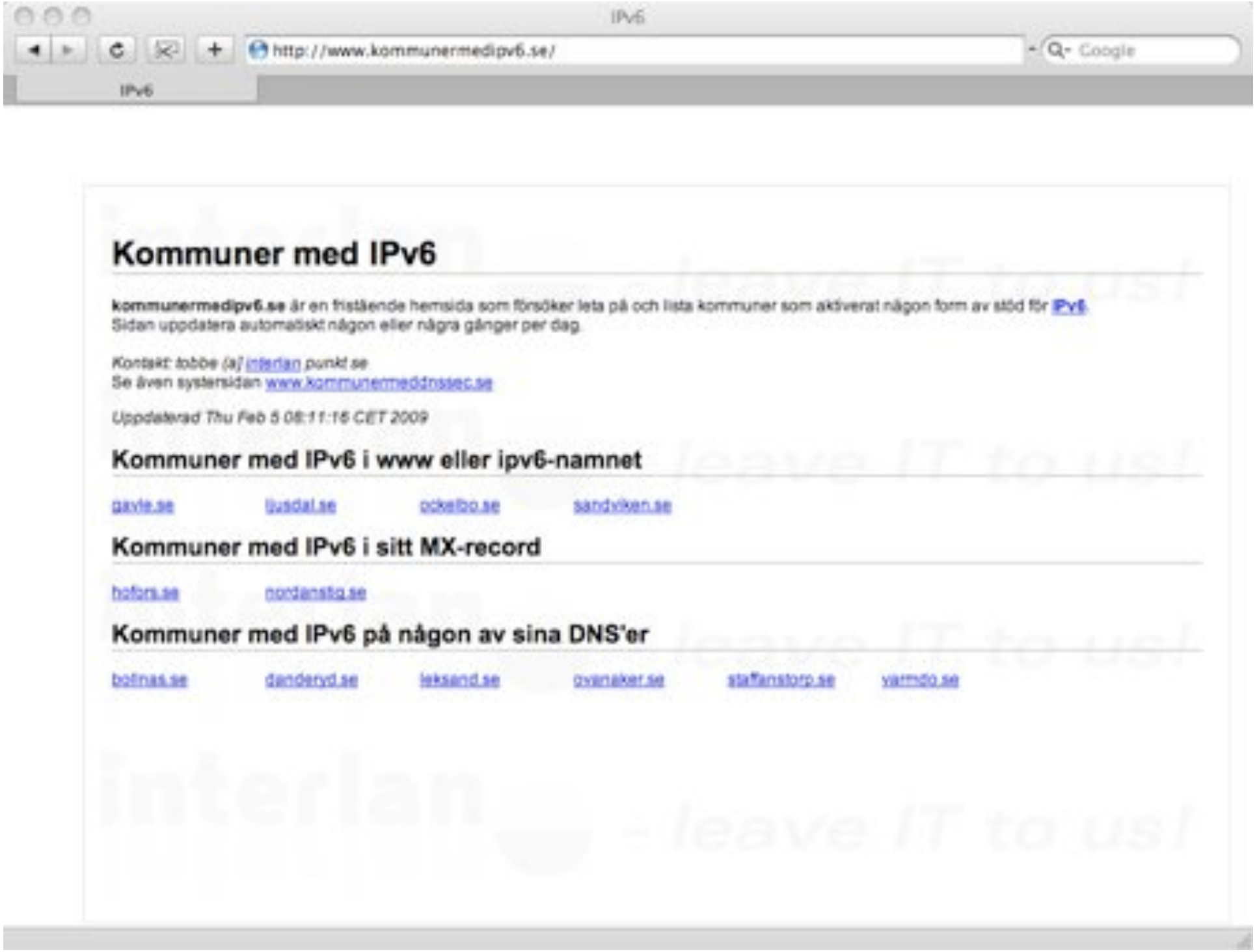
http://[2a02:250::6]

http://[2001:838:1:1:210:dcff:fe20:7c7c]

http://[2001:a18:1:20::22]

http://[2001:218:2001:3005::8a]

http://[2001:470:0:64::2]


IPv6
http://www.kommunermedipv6.se/
Google
IPv6
Kommuner med IPv6
kommunermedipv6.se är en fristående hemsida som försöker leta på och lista kommuner som aktiverat någon form av stöd för IPv6.
Sidan uppdatera automatiskt någon eller några gånger per dag.
Kontakt: tobbe (a) interlan punkt se
Se även systersidan www.kommunermeddnssec.se
Uppdaterad Thu Feb 5 08:11:16 CET 2009
Kommuner med IPv6 i www eller ipv6-namnet
gavle.se
ljusdal.se
ockelbo.se
sandviken.se
Kommuner med IPv6 i sitt MX-record
hofors.se
nordanstig.se
Kommuner med IPv6 på någon av sina DNS'er
botkyrka.se
danderyd.se
leksand.se
ovanaker.se
staffanstorp.se
varmdo.se
interlan
- leave IT to us!

If IPv6 is NOT the answer then...

Plan B: IPv4 for ever

~~Leisurely IPv6 deployment~~

~~and~~

Persist with IPv4 networks using more NATs

NAT Futures

Are NATs just more of the same?
Is this the "safe" option?

How far can NATs scale?

200M new users / year
A /16 would help 6 million users
1 billion behind a /8

How complex can we get with this network?

Are we willing to find out?

If IPv6 is NOT the answer then...

Plan X: end-to-end IP is NOT the answer either!

huh?

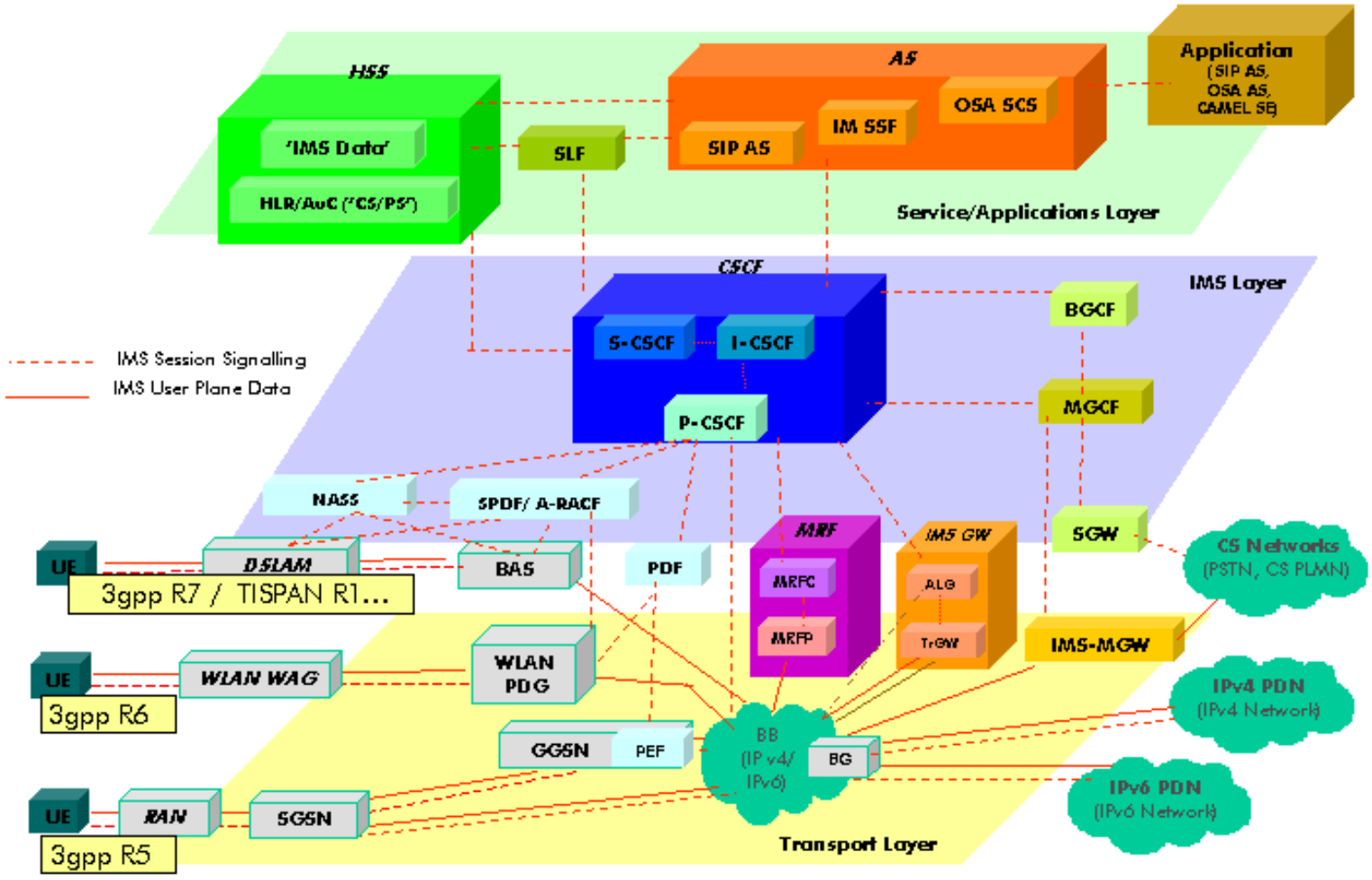
Application Level Gateways!

For example:
Use the 3G approach - IMS

IMS is an architecture of application level gateways

- front-end proxies act as agents for local clients
- applications are relayed through the proxy
- no end-to-end IP at the packet level

Yes, it's VERY ugly! More secure?



Are you feeling lucky today?

Do you understand enough about application layer gateway architectures to bet the entire future of the Internet on this theory of the evolution of network architectures?

I'm not!

But what could be useful right now is …

- An appreciation of the broader context of business imperatives and technology possibilities when confronting imminent IPv4 exhaustion
- An understanding that leaving things to the last millisecond may not be the wisest choice for anyone

An appreciation IPv6 still represents the lowest risk option of all the potential futures - and therefore the most secure

Patrik Fältström
paf@cisco.com