SSAC Activities

ICANN Public Forum

Steve Crocker
Chair, SSAC

November 1, 2007

Los Angeles,CA

Agenda

- New SSAC Members
- Whois/Spam Report
- Domain Name Front Running
- IPv6 Support in Firewalls
- IPv6 Adoption
- DNSSEC

Recent SSAC Publications

SAC021: Survey of IPv6 Support Among Commercial Firewalls

SAC022: Domain Name Front Running

SAC023: Is the WHOIS Service a Source for email Addresses for Spammers?

Security and Stability Advisory Committee

- Volunteers
  - With some important staff support
- Experts
  - Security
  - Domain name registry, registrar
  - Address community
  - Highly technical
- **No authority; others choose whether to use our advice**

SSAC Operation

- Examination of topics
  - Mixture of requests and self-assigned
  - Results are Reports, Advisories, Comments
- Themes (rough and not preplanned)
  - Protecting registrants
  - Stability of DNS & addressing system
  - Protection of DNS information
  - Denial of service attacks

SSAC Members

- Alain Aina
- Jaap Akkerhuis
- Jeff Bedser
- KC Claffy
- Steve Crocker, chair
- Patrik Fältström
- Johan Ihrén
- Rodney Joffe
- Mark Kosters
- Danny McPherson
- Ram Mohan
- Russ Mundy
- Frederico Neves
- Ray Plzak, vice chair
- Rajashekhar Ramaraj
- Shinta Sato
- Mark Seiden
- Mike St. Johns
- Doron Shikmoni
- Bruce Tonkin
- Paul A Vixie
- Rick Wesson
- Suzanne Woolf

Others

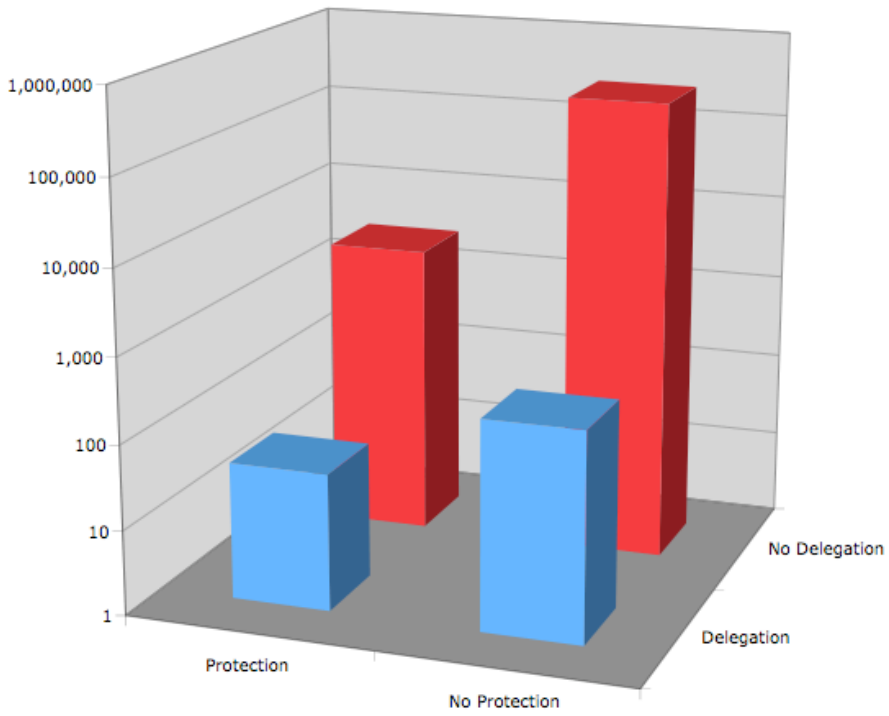
- David Conrad - VP Research and IANA Strategy
- Steve Conte - ICANN Chief Security Officer
- Dave Piscitello - ICANN Fellow
- Jim Galvin - Exec
- Daniel Karrenberg - Invited Guest
- Lyman Chapin - Invited Guest
- Stefano Trumpy - GAC Liaison
- Olaf Kolkman - IAB Point of Contact
- Robert Guerra - ALAC Liaison

Does Whois lead to Spam?

Motivation

- U.S. Federal Trade Commission report suggested whois listing did not lead to spam
- Seemed counterintuitive to our experience

Comparison of Results



For an email address that is *not* published anywhere other than the WHOIS

1. Unprotected registrant email addresses received significant amounts of spam.
2. Registrant email addresses protected by protected-WHOIS may achieve two orders of magnitude better defense against spam.
3. Registrant email addresses protected by achieve three orders of magnitude better defense against spam.
4. Registrant email addresses protected by Protected-WHOIS *and* Delegated-WHOIS may achieve close to four orders of magnitude better defense against spam.

Domain Name “Front Running”

Bad Experiences

- Check on availability of a domain name
- “Yes, it’s available”
- Try to register it
- “Sorry, that name is not available”

- Is somebody watching me?

Real or imagined?

- Is someone watching the process?
- Tasting churns a huge number of names, so coincidence is a strong possibility
- Not very much hard data is available

Next steps

- Accumulate anecdotes
- Consider ways to study more carefully
- Sentiment in favor of pushing forward
- Do contracts prohibit front running??

IPv6 Matters

The Stick

- IANA IPv4 free address pool ends ~2011
  - RIR allocations take a bit longer
- Parade of horribles…
  - Hoarding, stealing, gray market, political wars…
- Lots of time will be spent on managing the process

The Carrot

- IPv6 addresses are plentiful
  - Enough for 667,804 per square nanometer

  - (Can't really allocate uniformly, of course)

The Reality

- IPv4 networks will continue to exist and operate for a very long time. No phase out envisioned.
- Thus, we will need co-existence and interoperation of IPv4 and IPv6 services
- Lots of chicken-and-egg problems
- Some (many?) things won't work

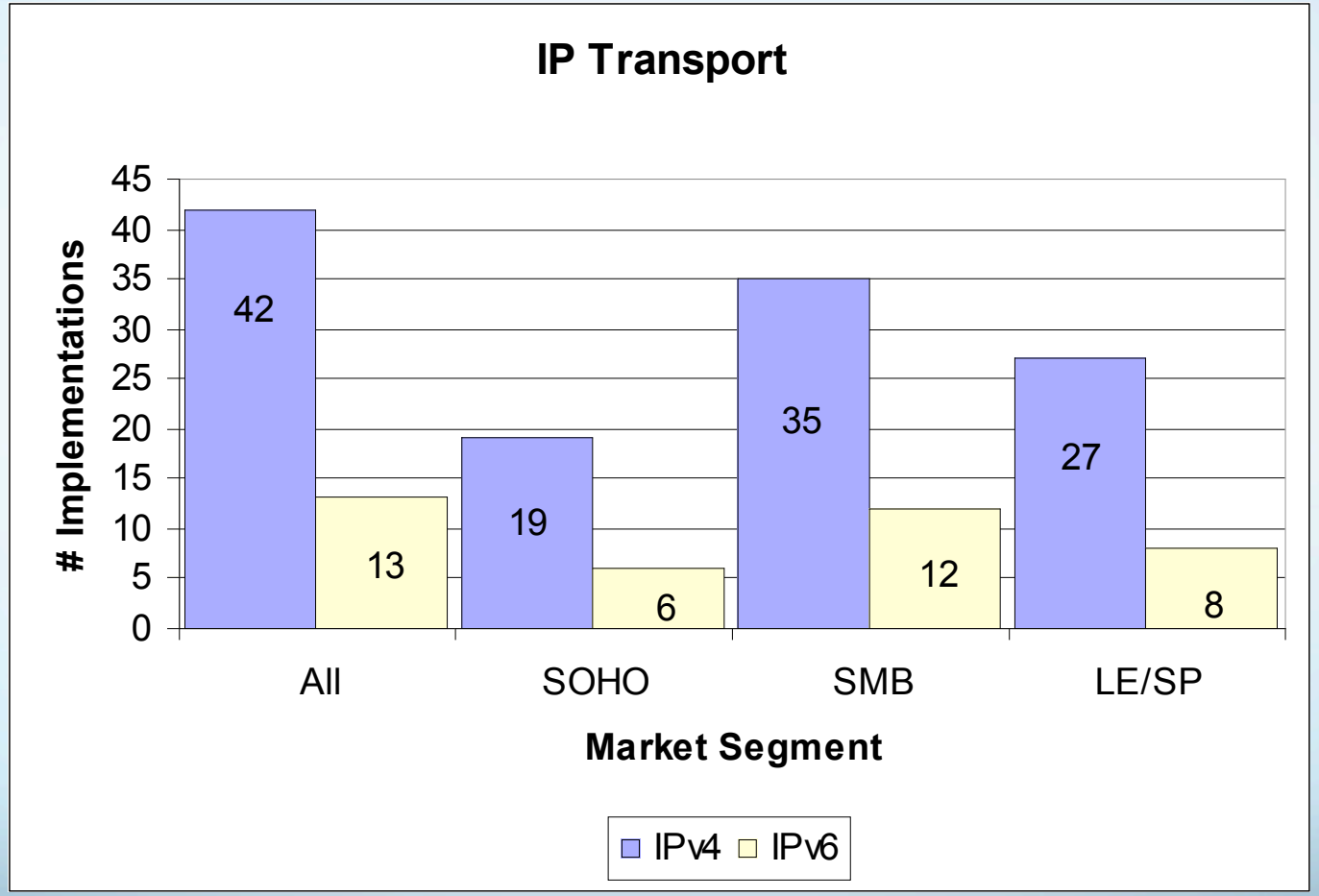
Primary categories

- ISPs -- large (backbone), small
- Large enterprises -- old, new, growing
- Small enterprises
- Content providers
- Router vendors
- Firewall and middleware vendors
- Governments
- Others?

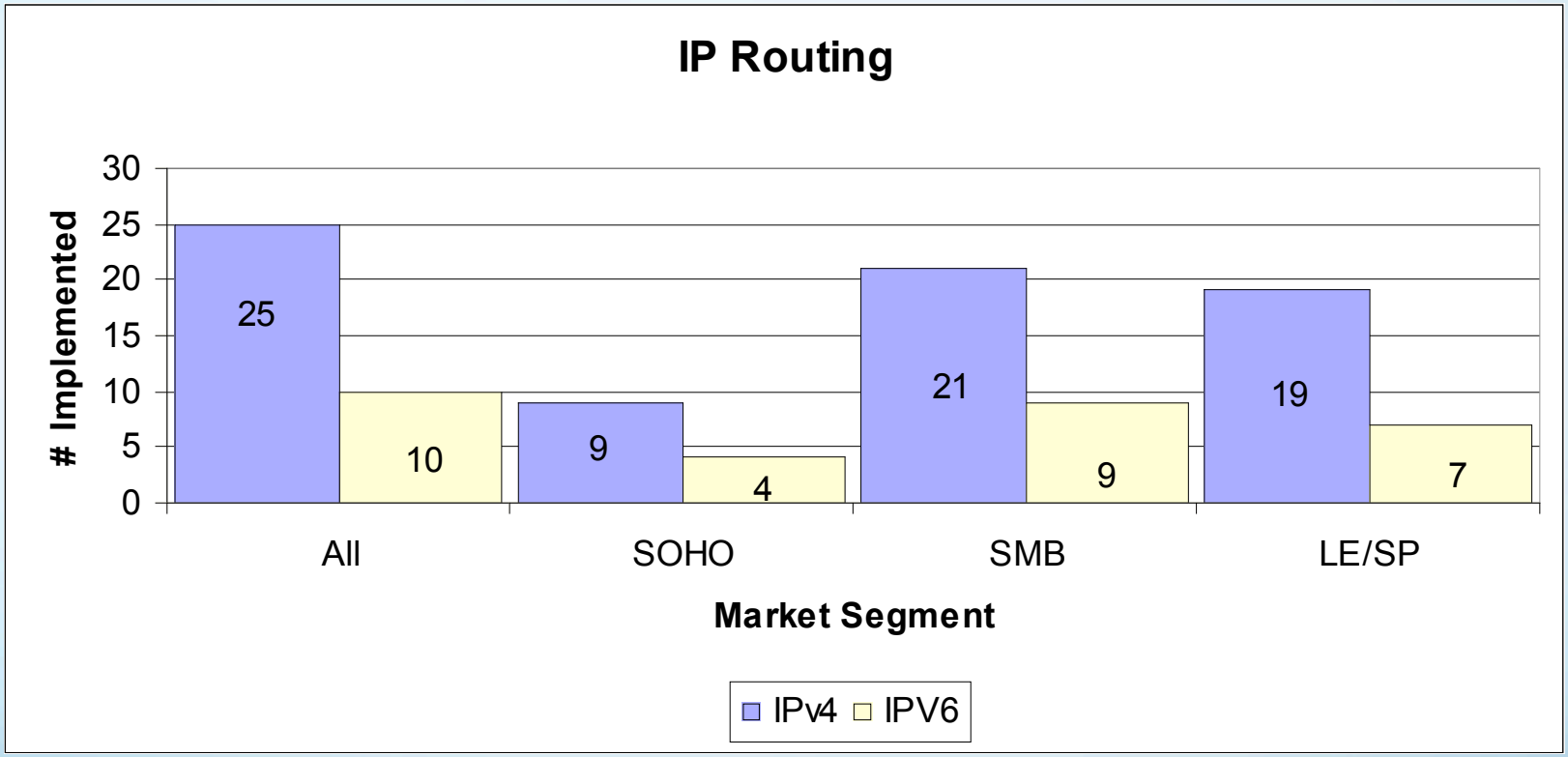
Firewall Survey

- Comparison of IPv6 vs IPv4 capabilities
- Surveyed 42 firewall products
- Looked at several features

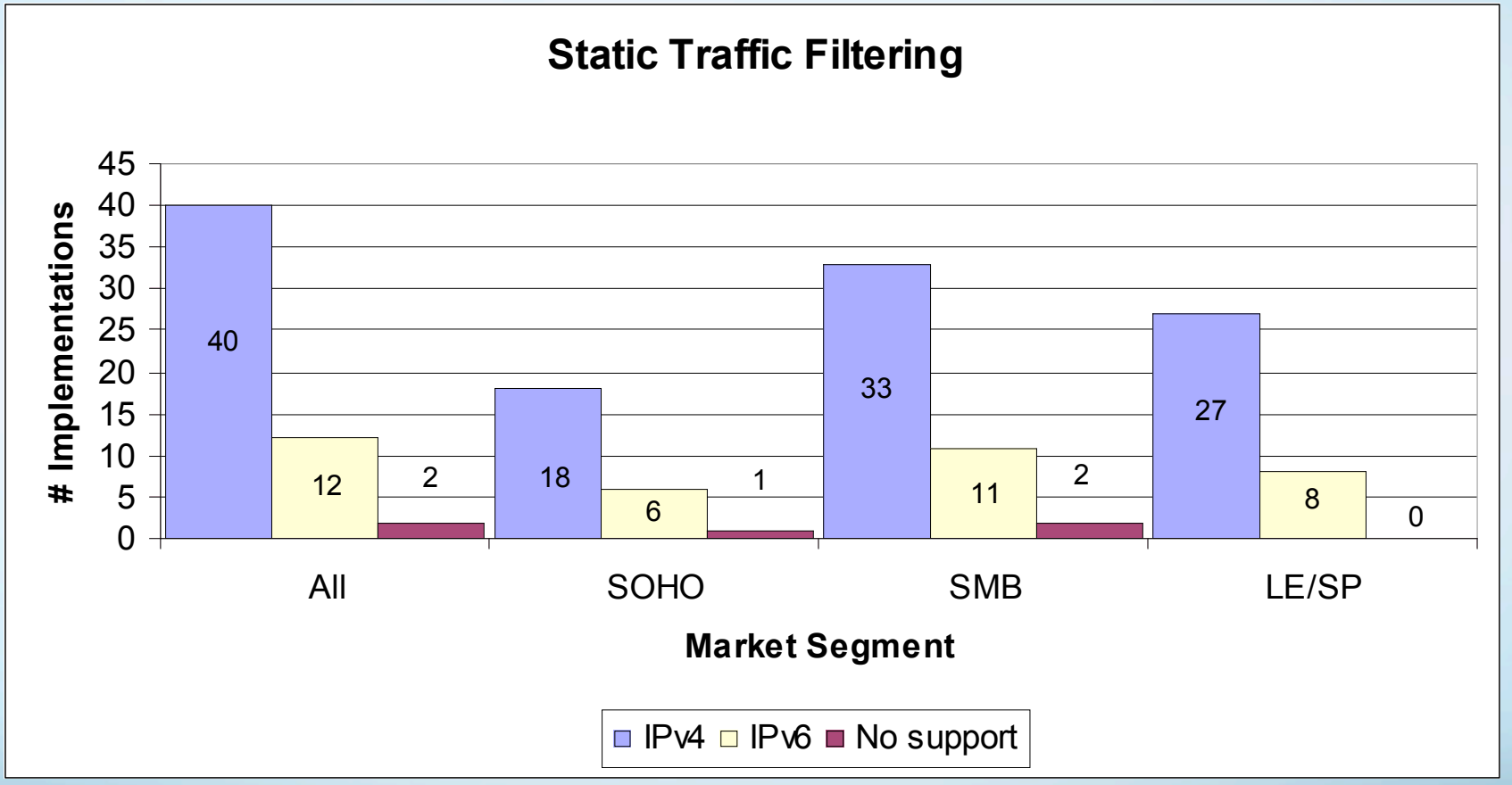
Firewall IP Transport



Firewall IP Routing



Firewall Static Filtering



Eight Questions (1-4)

1. Who will feel the pinch?
   - Existing players? New players?
2. How will pure IPv6 nets interact with IPv4 nets?
   - What role for dual stack? NAT-PT? Toredo?
3. When will there be global IPv6 connectivity?
   - What are the steps to get there?
   - Where are we as of now?
4. Impediments/incentives for ISPs?
   - Are IPv6-capable routers, network management systems, etc. available and competitive in price and performance?

Eight Questions (5-8)

5. Impediments/incentives for enterprises?
6. Imped/incentives for content providers?
   - When will content be equal over IPv6 and IPv4?
7. Are there any strong players?
   - What role have various governments played?
   - Which companies are playing a major role?
8. Who should promote IPv6 use?
   - What roles are there to play?
   - Who is playing them?
   - What new roles and players are missing?

The path forward is not yet clear

- It's not yet clear how IPv6 adoption will proceed
- It's not yet clear how IPv6 and IPv4 will interoperate
- It's not yet clear how market forces and planning/leadership should interact

- Important area. More attention needed.

DNS Security Protocol (DNSSEC)

Internet Infrastructure Security Threats

Type of Attack	Impact	Fixes
Denial of Service Attacks	!!!	??
DNS Hijacking	!!	+++
Address & Route Hijacking	!	-

Deployment Status

- Signed: Sweden (.SE), Bulgaria (.BG), Puerto Rico (.PR), Brazil (.BR)
  - RIPE's portion of in-addr.arpa too
- Under Development: Japan (.JP), Korea (.KR), Mexico (.MX), Taiwan (.TW), United Kingdon (.UK)
- .MIL, .GOV, .EDU, .ORG all moving forward
- .ARPA almost ready; .INT too

Japan, Korea, Taiwan, IANA

- Shinta Sato, JPRS, .JP (Japan)
- HanSang Lee, NIDA, .KR (South Korea)
- Nai-Wen Hsu, TWNIC, .TW (Taiwan)
- Richard Lamb, IANA