Shifting Sands

PLNOG | March 2014

Andrzej Wolski
Training Department

- Began operating in 1992
- Not-for-profit membership organisation
- 10,000 members (Local Internet Registries)
- Neutral, Impartial, Open, Transparent
  - No commercial interest or influences and operates as a bottom-up and self-governing organisation
- **Provides administrative support to RIPE**

Regional Internet Registries

IANA

- Lacnic — Latin America
- ARIN — North America
- RIPE NCC — Eurasia, Middle East
- AFRINIC — Africa
- APNIC — Asia Pacific

RIPE NCC Training Services

- **Courses**
  - Local Internet Registry
  - RIPE Database
  - IPv6 for LIRs
  - Routing Security
- **New courses (Q2 2014)**
  - Deploying IPv6
  - DNSSEC
- **Webinars**
  - RIPE Database
  - IPv6
  - RPKI

- **Statistics 2013:**
  - 31 countries
  - 115 courses
  - 2347 attendees

ripe.net/training

Why the Internet is changing?

- People
- Devices
- Innovation

Internet is becoming a critical part of our life

Unprecedented changes

Artificial limitations

- Names
- Addresses

- Names resolution
- Routing

Security considerations

gTLDs

Names

RIPE NCC

TLDs

- **gTLDs**
  - .com .org .net
  - .info .biz .name
- **ccTLDs**
  - .pl .cz .nl
  - .io .ly .tv
  - امارات. .pф 台湾
- **Infrastrucure**
  - .arpa

New gTLDs

.whatever

.you

.would

.like

Closed gTLDs

- **Single registrant model**
  - Brand TLDs
  - Limited second level registration
- **Problems**
  - Abuse
  - Homonyms

- **On Hold**

Dotless gTLDs

- **Representation**
  - http://example/
  - email@example
- **Problems**
  - search lists
    - collisions with existing host names
  - certificate authorities
- **Requires apex of a TLD zone in the DNS**

- **Should be outlawed!**
  - some ccTLD operators do it anyway

Delegated gTLDs

.CHRISTMAS .GURU .PUB .HOUSE .BERLIN .みんな .بازار .SHOES .FISH .дети .TOKYO .FLORIST .MANGO .삼성 .KIWI .公司 .MENU .DATING .EMAIL .COFFEE .网络 .SEXY .AGENCY . RED .TIPS .SUPPORT

RIPE NCC

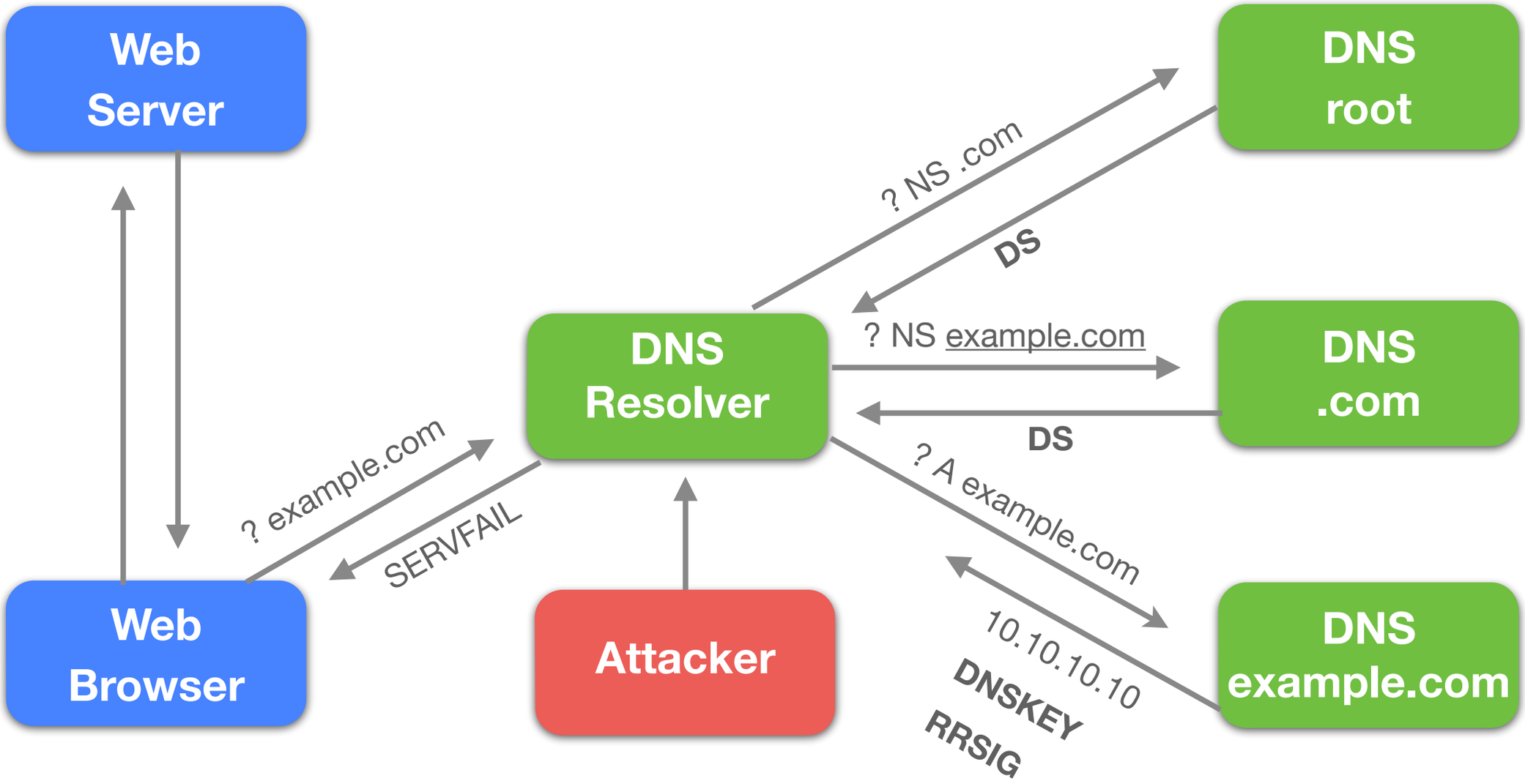
DNS Security Extensions

Names resolution

RIPE NCC

- **Overlay on top of DNS**
  - Verifies data integrity
  - Verifies data authenticity
- **Does not prevent**
  - Data snooping
    - No encryption, public data anyway
    - Attacks against the name server
- **It’s backwards compatible**

DNSSEC Chain of Trust



RIPE NCC

Every response is signed

dig -t AAA +dnssec ripe.net +short

```
2001:67c:2e8:22::c100:68b
AAAA 5 2 300 20140328144451 20140226134451 29287 ripe.net.
rMlImjMrulbY8ypLH/PN+bX2uHaYhTr3pD7aljDLWGWKRKUfk+QfvuRZ
UxZYqWRpD8o58MXPeNiRc6L9pEG6f3hoyuhxDtC9whHitCNBkNdAlytl
OJd8V9e5bmUkwtjvf/+NFtSQaxfqmgY8natE6odi5Kozu1ThvBZVoj7A 4ts=
```

dig -t NS +dnssec ripe.net +short

```
sec1.apnic.net.
sns-pb.isc.org.
ns3.nic.fr.
tinnie.arin.net.
sec3.apnic.net.
pri.authdns.ripe.net.
NS 5 2 3600 20140328144451 20140226134451 29287 ripe.net.
GtlGGBVlf71MKDmiKYzt7OKfOa6z5Y6VQwFZUug1o3MdahlOuF8+ADzJ
DA9vPRMQ8b8jhT2EHXcKKorpMB97gJjavi2Rs/D9w5TuKpBkXJ1sMJJr
Rd0H/QWJlxaKA/DMc1LuXRqjtNEnCjsZstd7NVQMA1Sq+JPVSarjTHbX
HZc=
```

SSL Certificate Pinning (DANE)

dig +dnssec +noall +answer +multi _443._tcp.www.example.com. TLSA

```
_443._tcp.www.example.com. 3342 IN     TLSA 3 0 1 (

C92D44FE99DD32B0C9335561DFAB89575DCC4C232443
                                                634E665660821A36D186 )
```

- Early adopter stage
- New DNS TLSA records
- Support in BIND 9.9.1 and up
- Support in various other software
- IETF Proposed Standard
  - RFC 6698

SSH Keys

dig +dnssec +multi host.example.com SSHFP

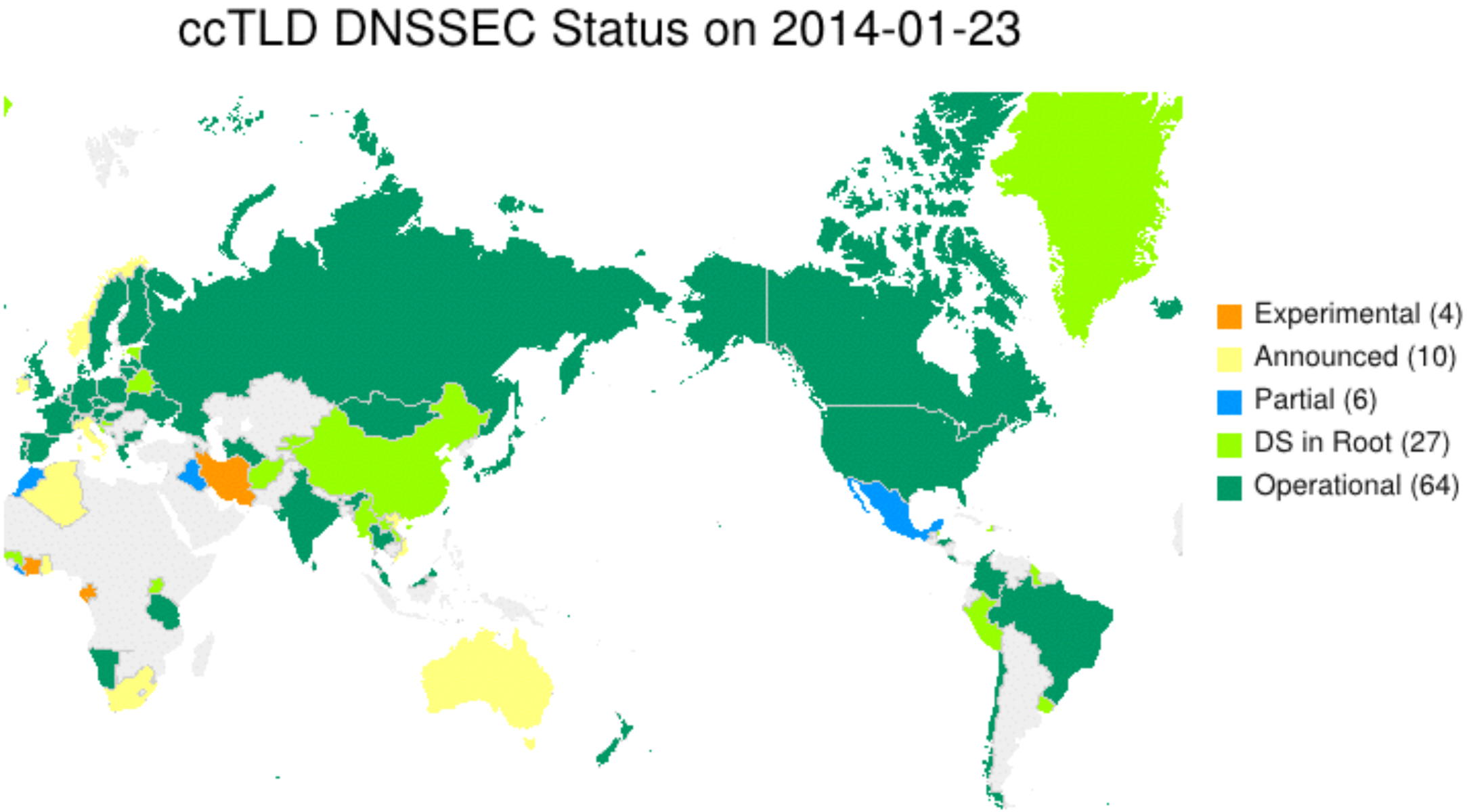
```
host.example.com.               88 IN SSHFP 1 1 (

7E7A55CEA3B8E15528665A6781CA7C35190CF0EB )
host.example.com.               88 IN SSHFP 2 1 (

CC17F14DA60CF38E809FE58B10D0F22680D59D08 )
```

- **New DNS SSHFP records**
- **Support in OpenSSH**
  - VerifyHostKeyDNS
- **IETF Standard**
  - RFC 4255

DNSSEC Deplyment Status



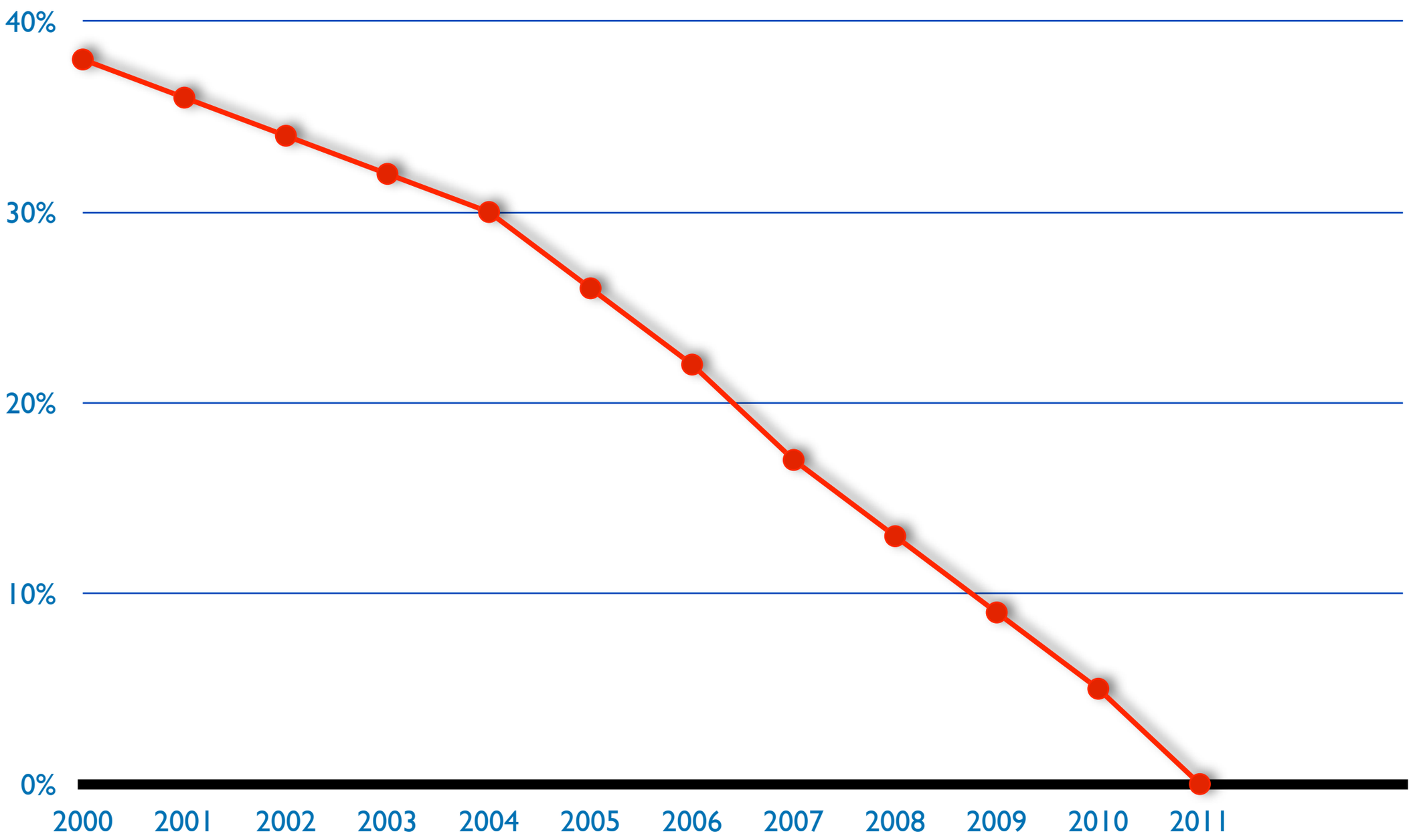
source: internetsociety.org/deploy360/dnssec/maps/

IPv6

Addresess

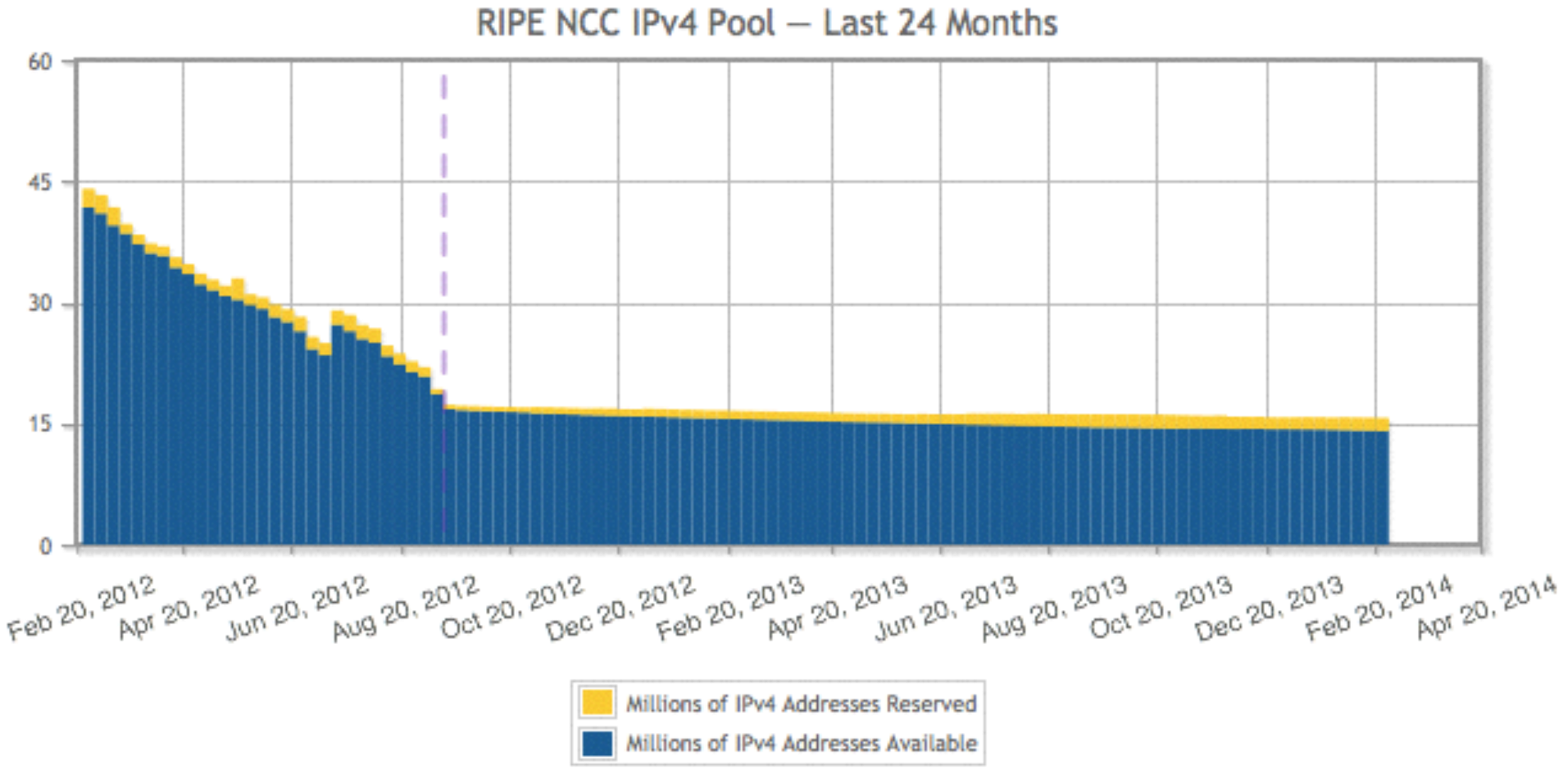
RIPE NCC

IANA IPv4 Pool



RIPE NCC IPv4 Pool

On 14 September 2012, the RIPE NCC began to allocate IPv4 address space from the last /8 of IPv4 address space it holds.



RIPE NCC

Getting an IPv6 Allocation

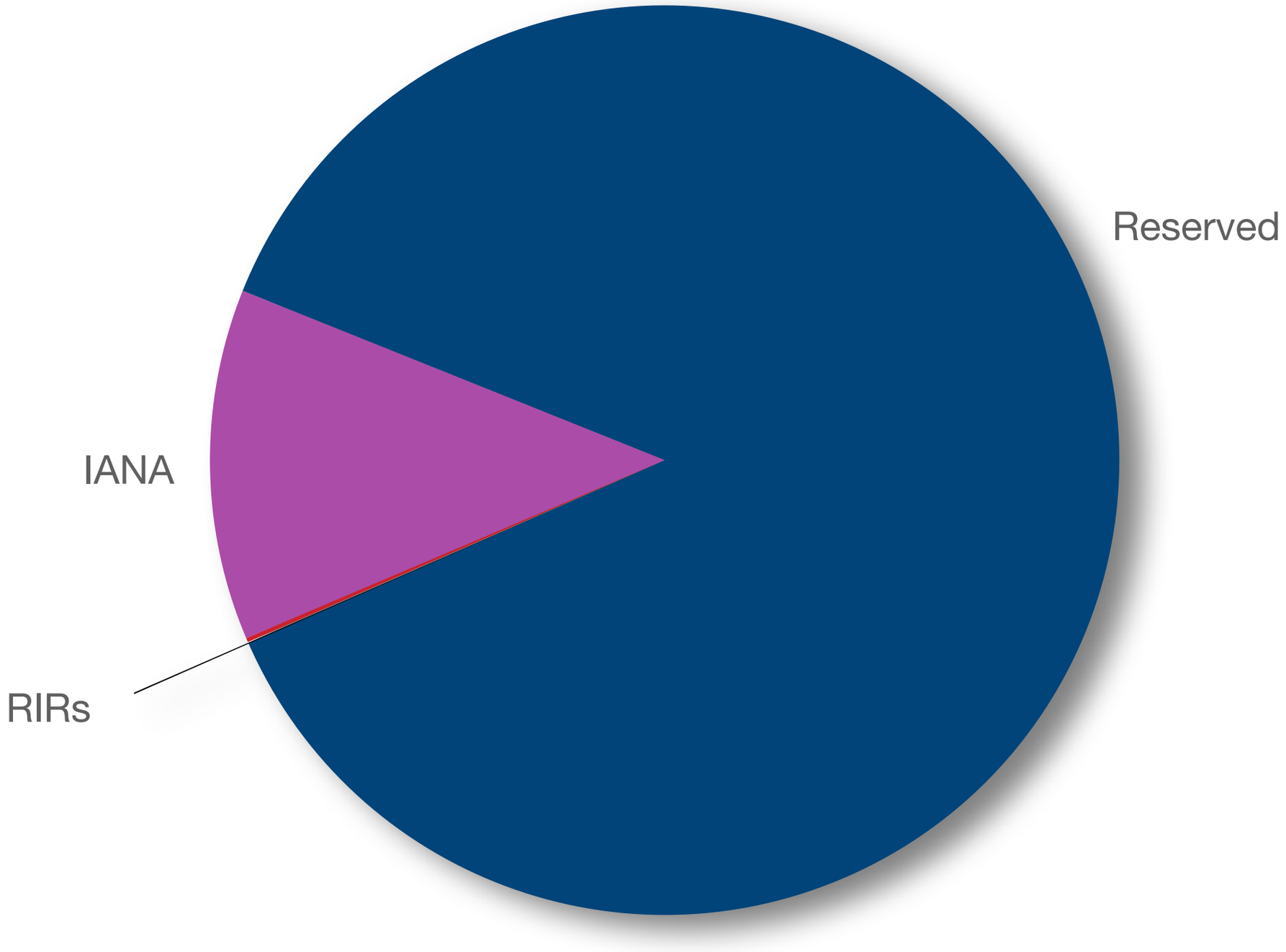
- **To qualify, an organisation must:**
  - Be an LIR
  - Have a plan for making assignments within two years

- **Minimum allocation size /32**
  - Up to a /29 without additional justification
  - More if justified by customer numbers

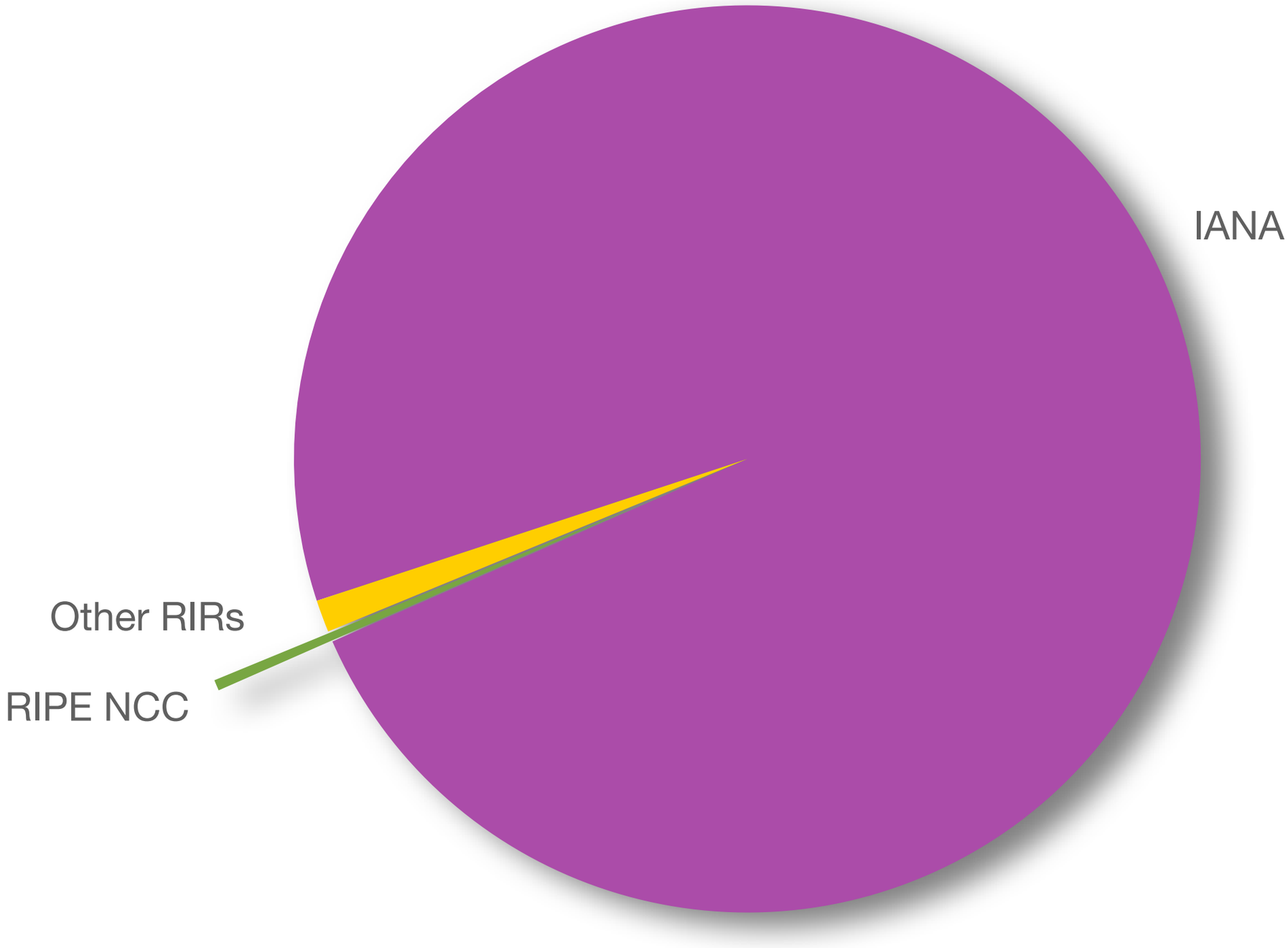
Getting IPv6 PI Assignment

- **To qualify, an organisation must**
  - Meet the contractual requirements for provider independent resources
  - LIRs must demonstrate special routing requirements
- **Minimum assignment size /48**
- **PI space can not be used for sub-assignments**
  - Not even for 1 IP address

IPv6 Global Pool



IPv6 Pool in Distribution



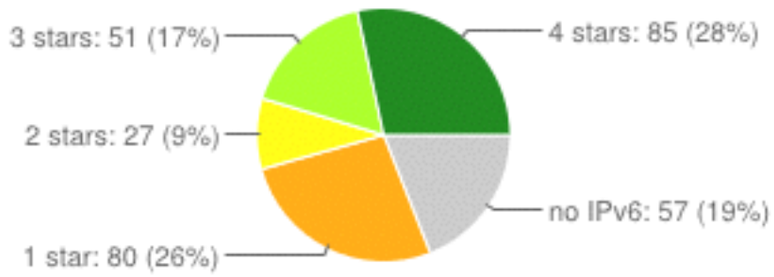
RIPE NCC

IPv6 RIPENess

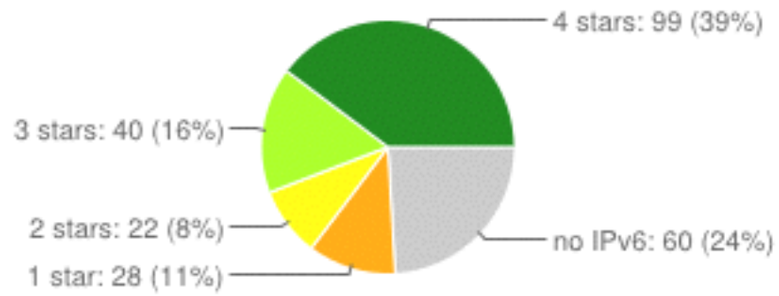
- **Rating system**
  - One star if the LIR has an IPv6 allocation
- **Additional stars if**
  - IPv6 Prefix is announced on router
  - A **route6** object is in the RIPE Database
  - Reverse DNS is set up
- A list of all 4 star LIRs: http://ripeness.ripe.net/
  - Experimental 5th star: http://ipv6ripeness.ripe.net/5star/PL.html

IPv6 RIPEness

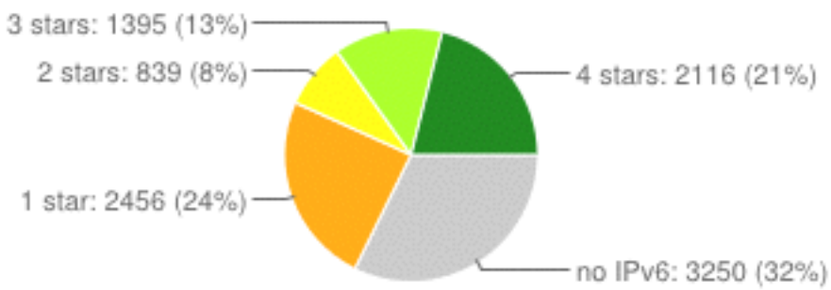
Poland (300 LIRs)



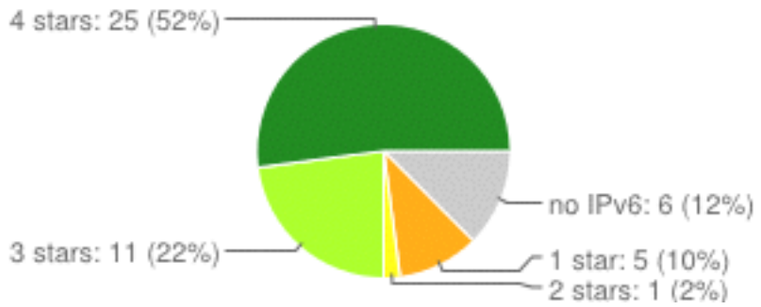
Czech Republic (249 LIRs)



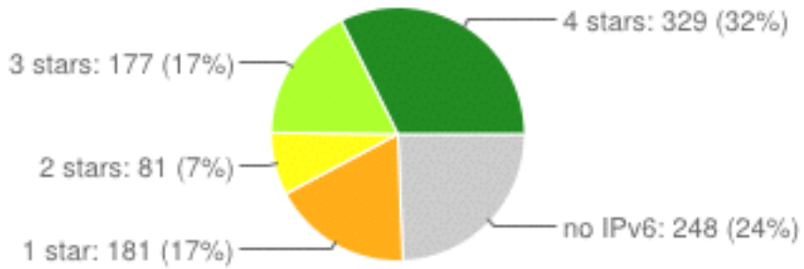
All (10056 LIRs)



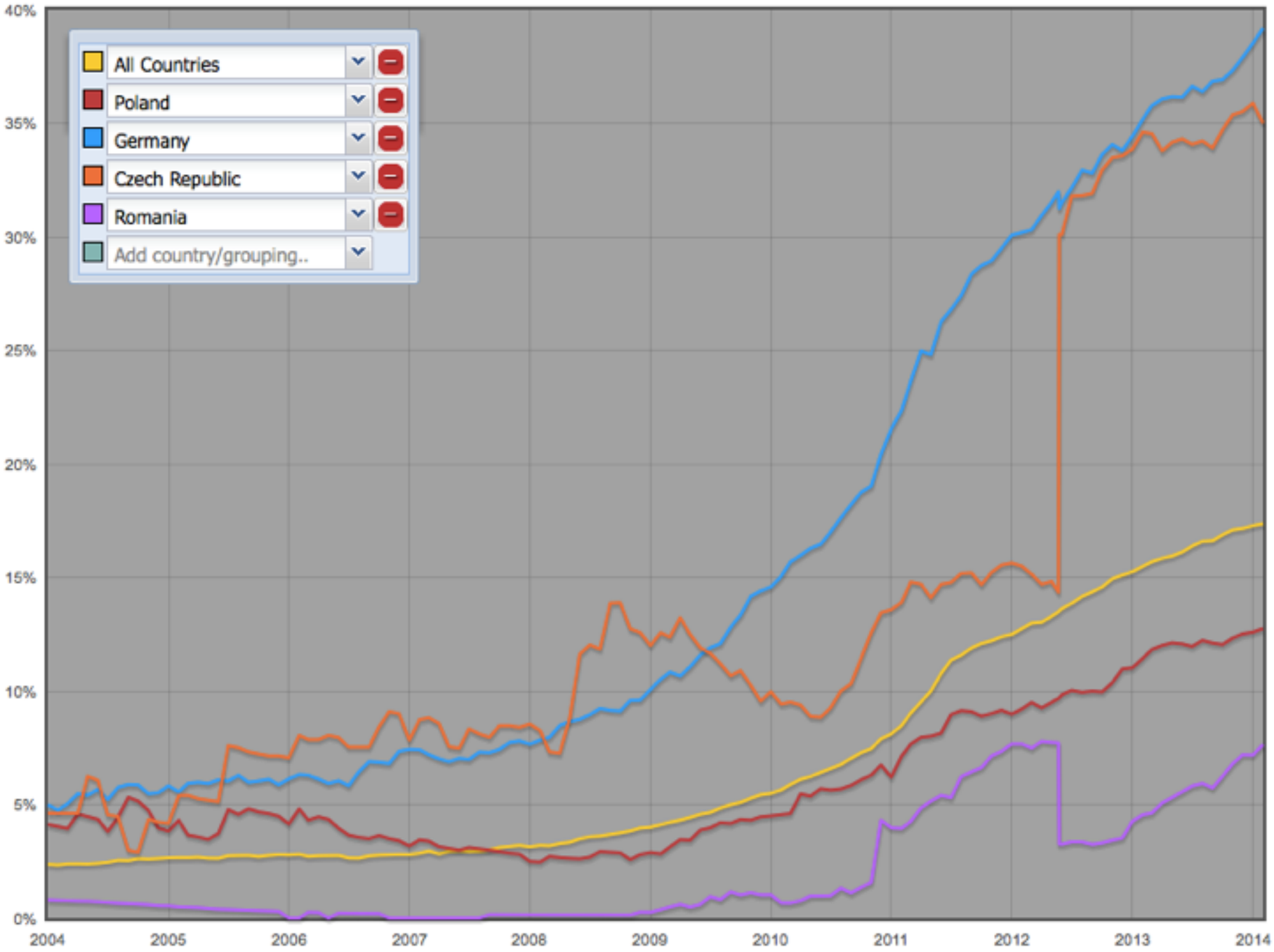
Romania (48 LIRs)



Germany (1016 LIRs)



IPv6 Enabled Networks



RIPE NCC

RPKI

Routing

RIPE NCC

Why RPKI?

- To be able to answer the question
  - Is that ASN authorised to originate that address range?

- Tight integration with routers
  - Routers have awareness of RPKI validity states
  - Can make routing decision
  - Stepping stone for AS-Path Validation
  - Prevent Attacks on BGP

RPKI BGP Origin Validation

- **LIRs can use their certificate to create a ROA for each of their resources (address ranges)**
- **ROA states**
  - address range
  - which AS this is announced from (freely chosen)
  - maximum length (freely chosen)

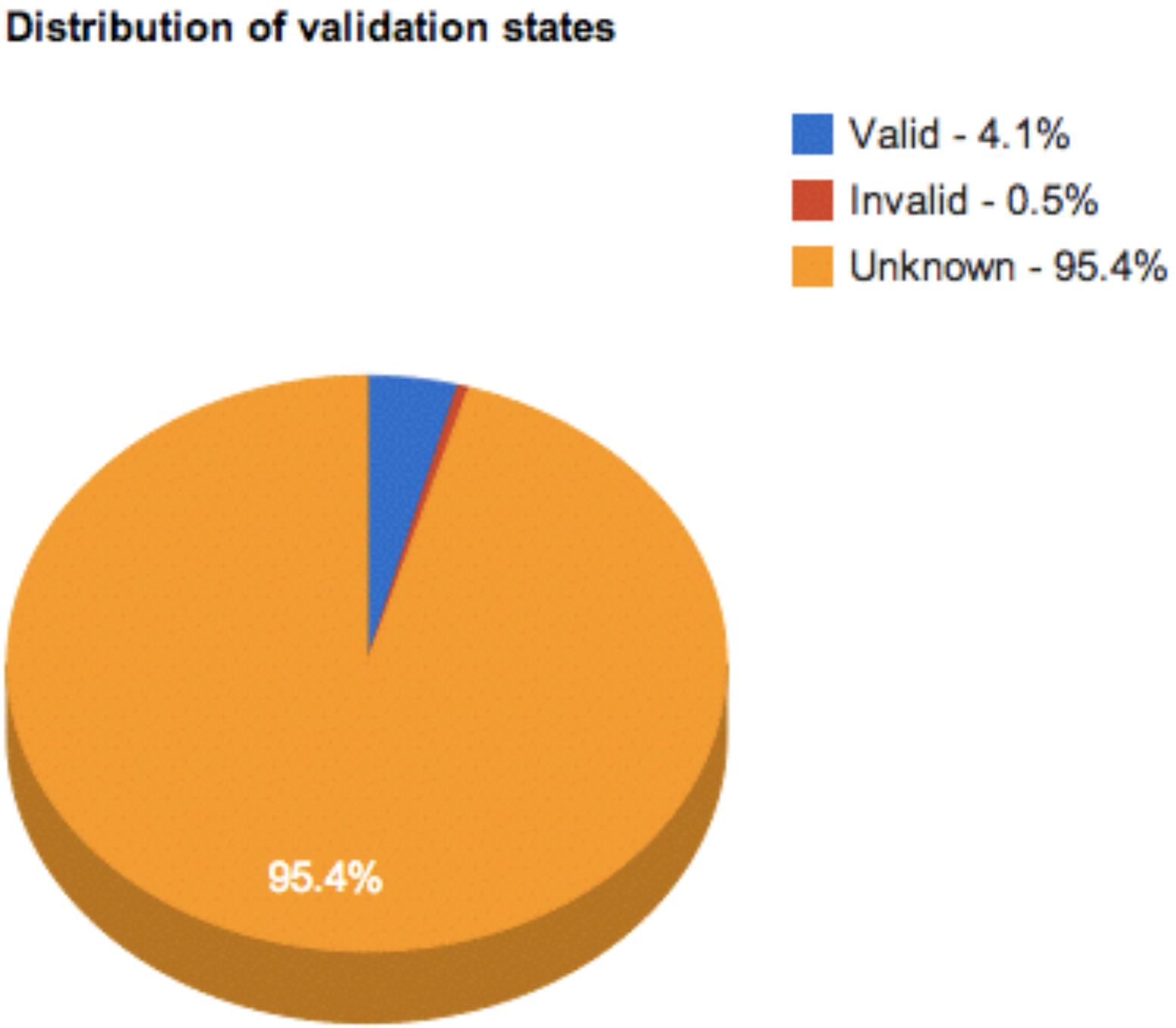
- **You can have multiple ROAs for an IP range**
  - ROAs can overlap

Can I Make Routing Decisions?

- **A ROA affects the RPKI validity of a BGP route**
  - **VALID**
    - ROA found, authorised announcement
  - **INVALID**
    - ROA found, unauthorised announcement
  - **UNKNOWN**
    - No ROA found (resource not yet signed)

Every operator is free to base any routing decision on these three validity states

Adoption



source: rpki.surfnet.nl

RPKI Support in Routers

- **RPKI and RPKI-RTR Protocol are an IETF standard**
- **All router vendors can implement it**
- **Cisco** Support:
  - XR 4.2.1 (CRS-x, ASR9000, c12K) / XR 5.1.1 (NCS6000, XRv)
  - XE 3.5 (C7200, c7600, ASR1K, CSR1Kv, ASR90x, ME3600…)
  - IOS15.2(1)S
- **Juniper** has support since version 12.2
- **Quagga** has support through BGP-SRX
- **BIRD** has support for ROA but does not do RPKI-RTR

localcert.ripe.net
ripe.net/certification

Questions?

RIPE Meeting

12 – 16 May 2014

ripe68.ripe.net

Dziękuje ;-)

Koniec