RIPE NCC DNS Update

Wolfgang Nagele
DNS Services Manager

RIPE NCC

DNS Department Services

- Reverse DNS for RIPE NCC zones
- Secondary for other RIRs
- K-root
- F-reverse (in-addr.arpa & ip6.arpa)
- Secondary DNS for ccTLDs
- ENUM Tier-0 (e164.arpa)
- AS112 node at AMS-IX (RFC1918 space sink)

Anycast Cluster (AS197000)

- Two anycast instances operational
  - London (LINX) & Amsterdam (AMS-IX)
- Production for critical zones
  - in-addr.arpa (Reverse IPv4 parent zone)
  - ip6.arpa (Reverse IPv6 parent zone)
  - IPv4 and IPv6 reverse parent zones
    - Primary for RIPE NCC
    - Secondary for other RIRs
  - RIPE NCC forward zones (ripe.net, etc.)

F-reverse

- Serves in-addr.arpa and ip6.arpa
- According to RFC5855 (BCP)
- Servers operated by
  - ARIN, APNIC, AfriNIC, LACNIC, RIPE NCC, ICANN

New Provisioning System

- Production since January 2011
  - Using dynamic updates to allow near real-time updates
- Upcoming features:
  - ERX provisioning equal to other space
  - Support for RFC2317 delegation (< /24 Assignments)
  - Simplified delegation checker

DNSSEC Outages: The Ugly

- Encountered a bug during KSK rollover
- Signature over DNSKEY set missing
  - Affected e164.arpa on 15 February 2011
- Vendor could not reproduce the problem and concluded that high load on system caused it

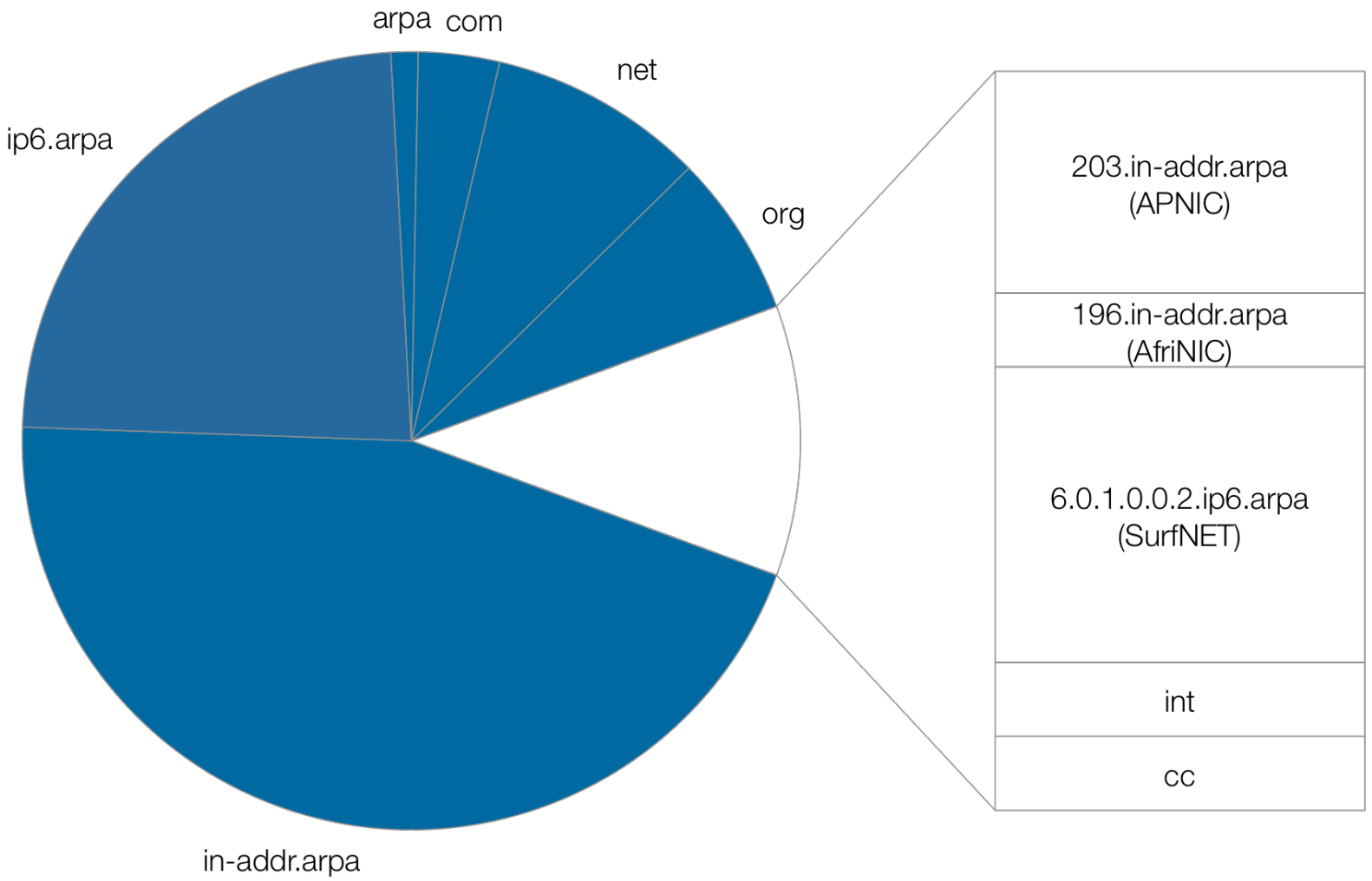
DNSSEC Outages: The Bad

- Second outage on 14 April 2011
  - Affected ripe.net and 0.a.2.ip6.arpa
- Same exact problem – no high system load

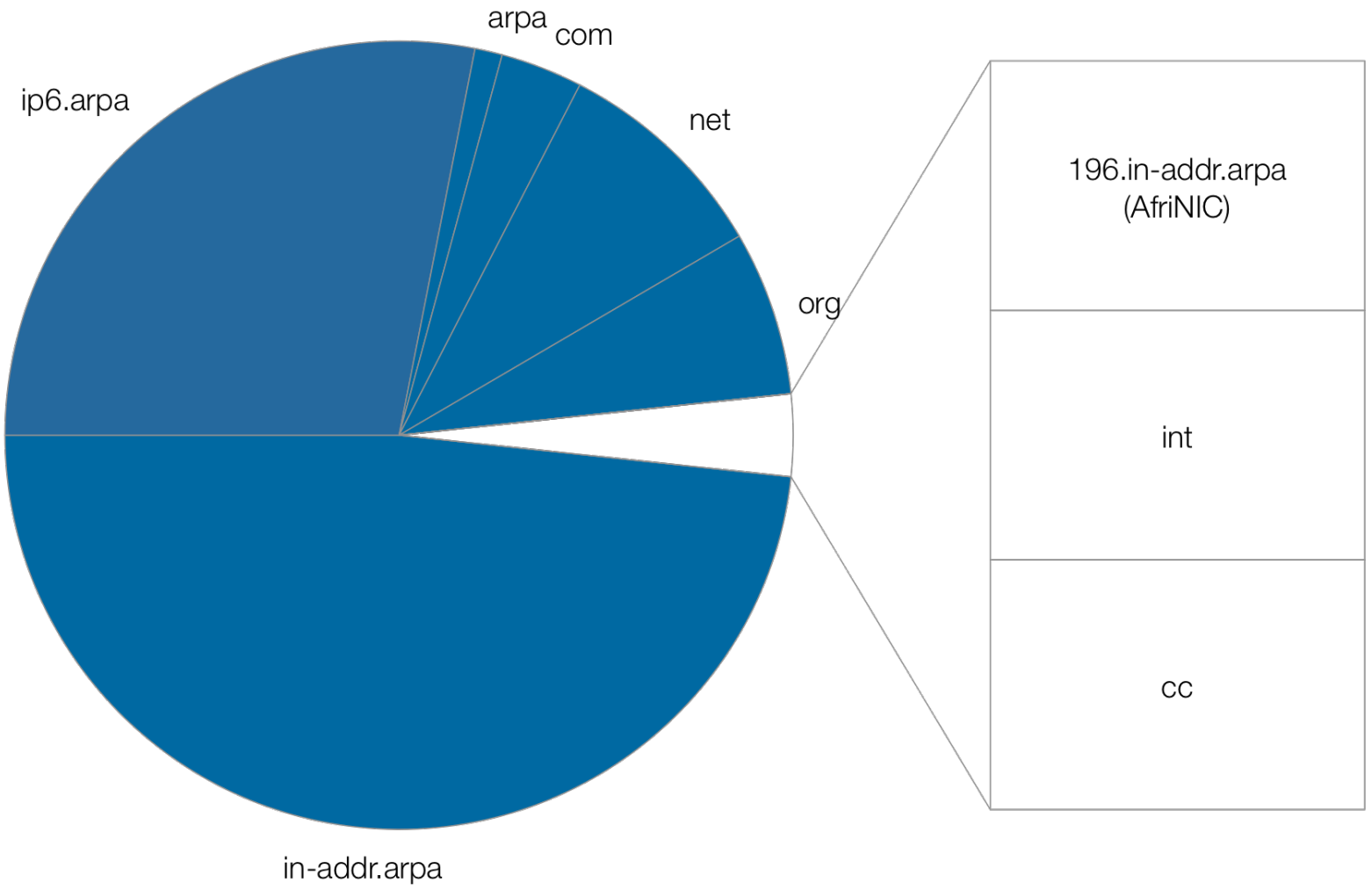
DNSSEC Outages: The Good

- Gathered enough data to reproduce the bug
  - Awaiting release with bug fix before our next rollover
- Called for broad work on a safeguard
  - Spurred interest from others (SIDN, AFNIC, DENIC, …)
  - Initial work on a DNSSEC verification proxy started
  - Coordination on the DNSSEXY mailinglist
    - http://nlnetlabs.nl/mailman/listinfo/dnssexy

DNSSEC: Signed Parents

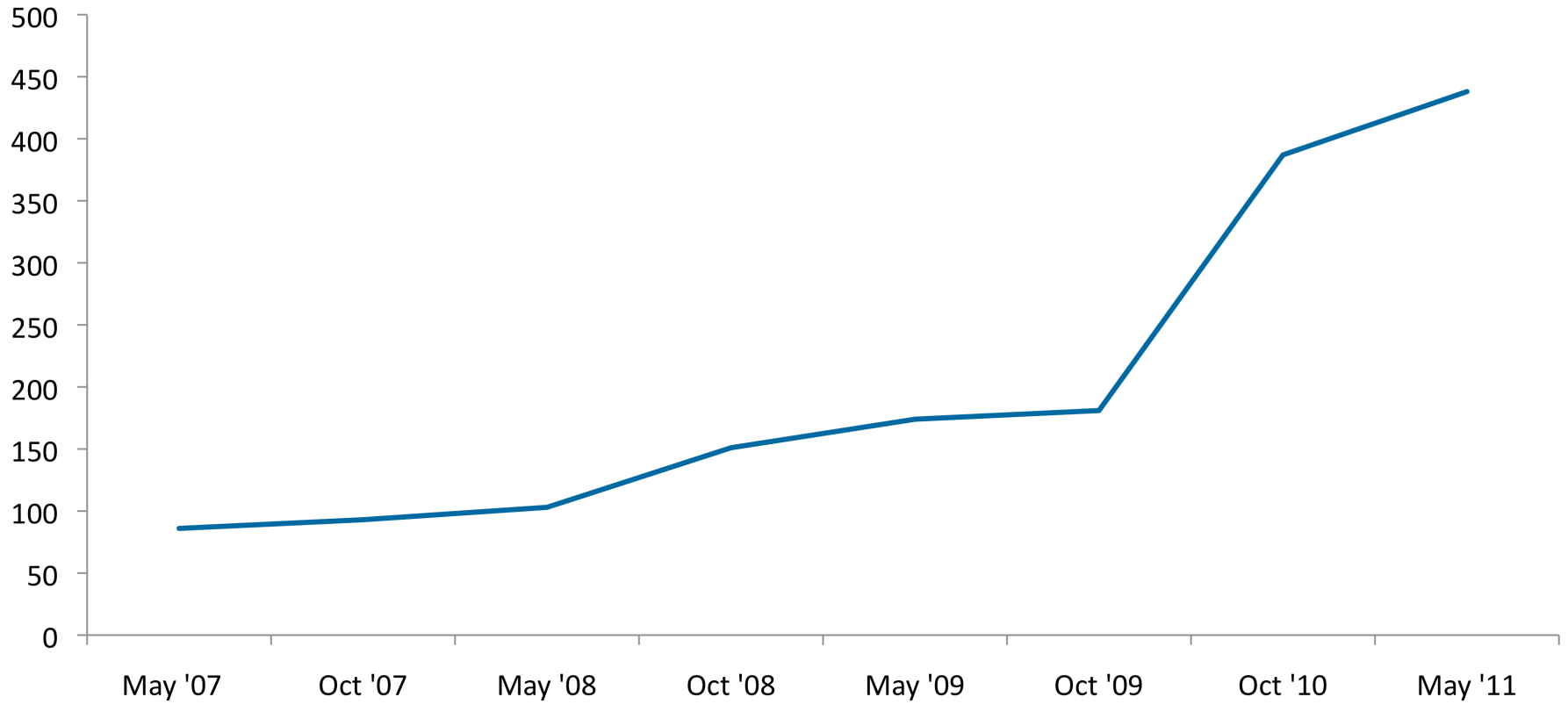


DNSSEC: Signed Parents (By Fall 2011)



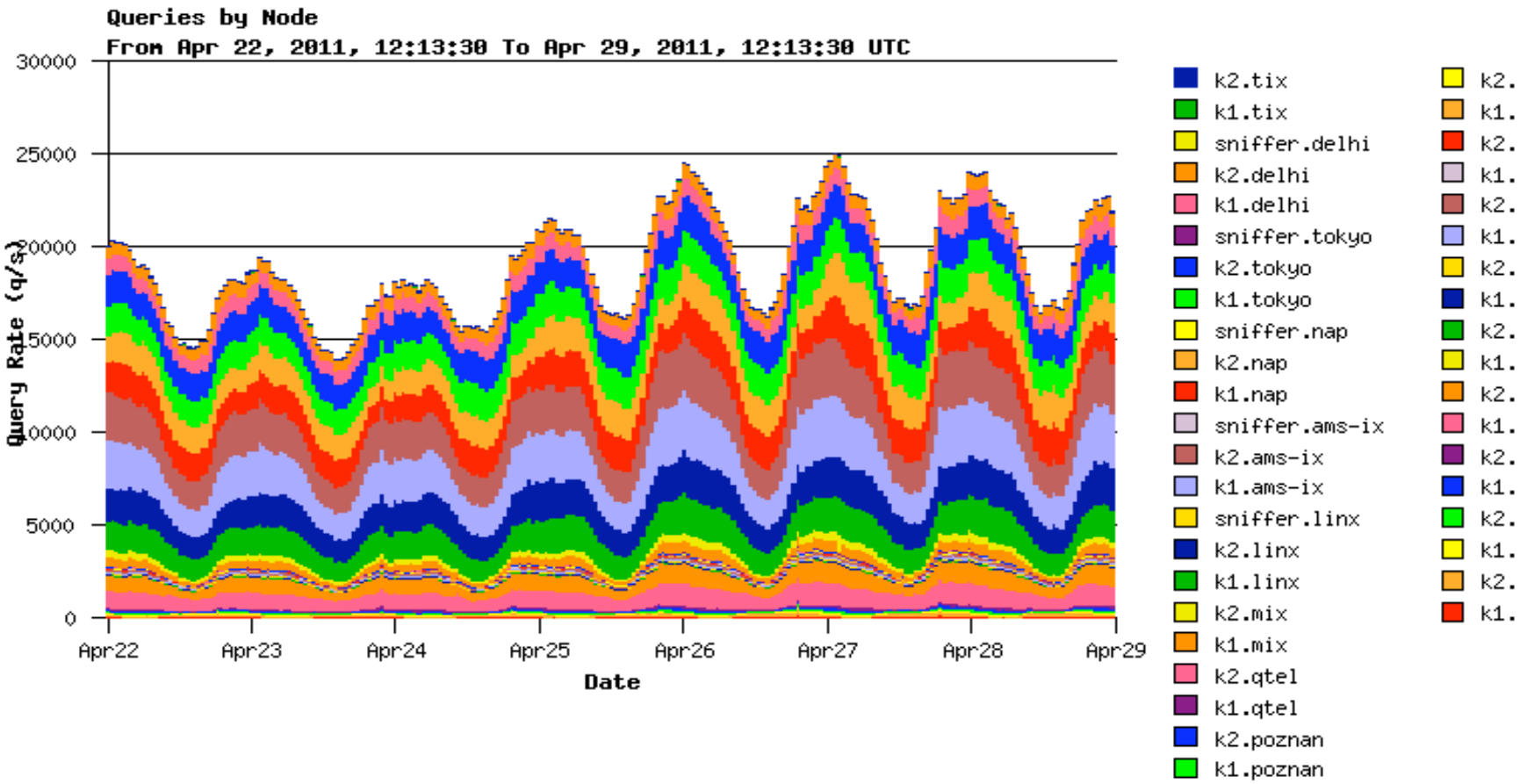
DNSSEC in Reverse DNS

- DS records over time



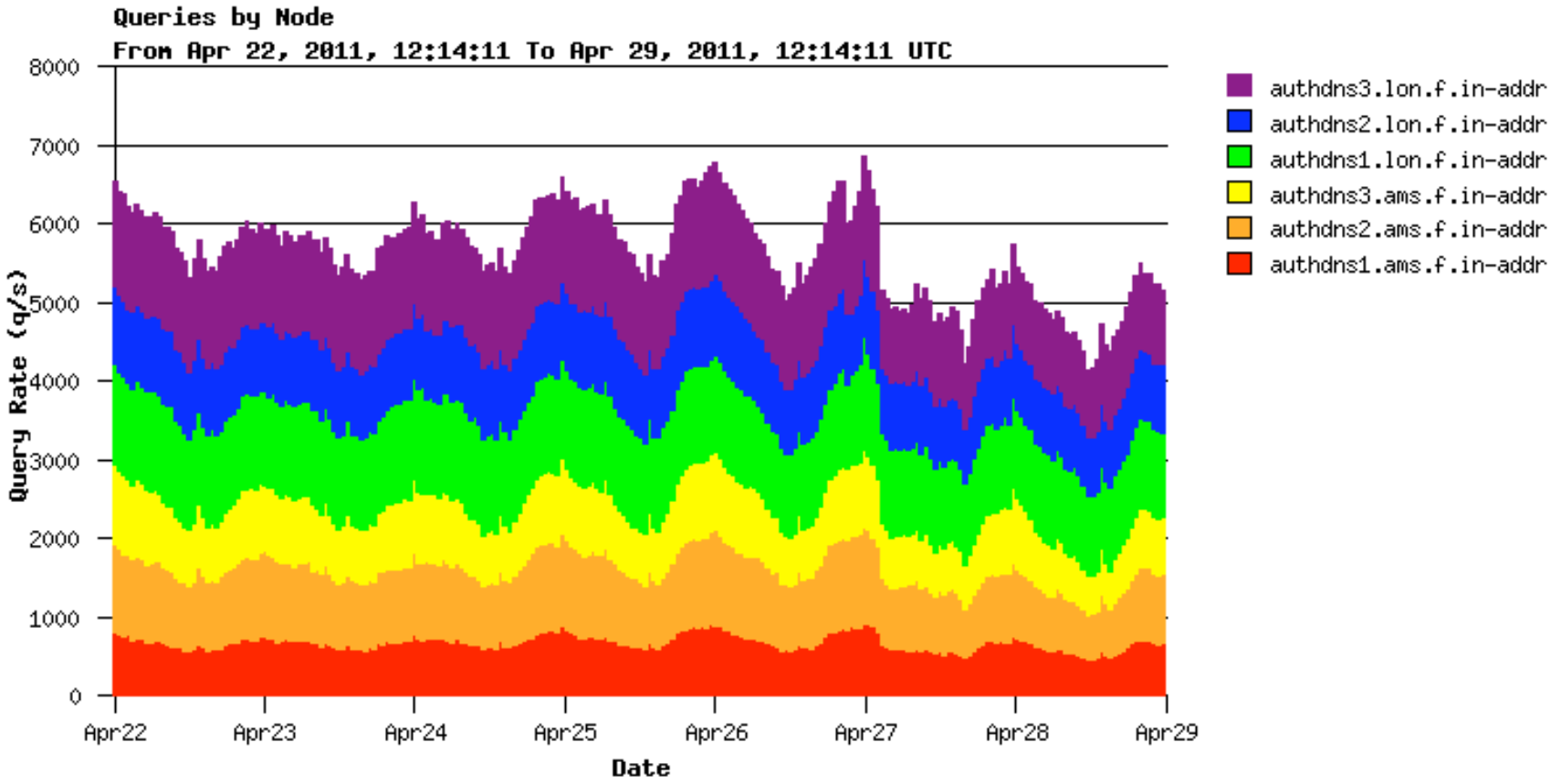
K-root

- Operations stable with 18 instances



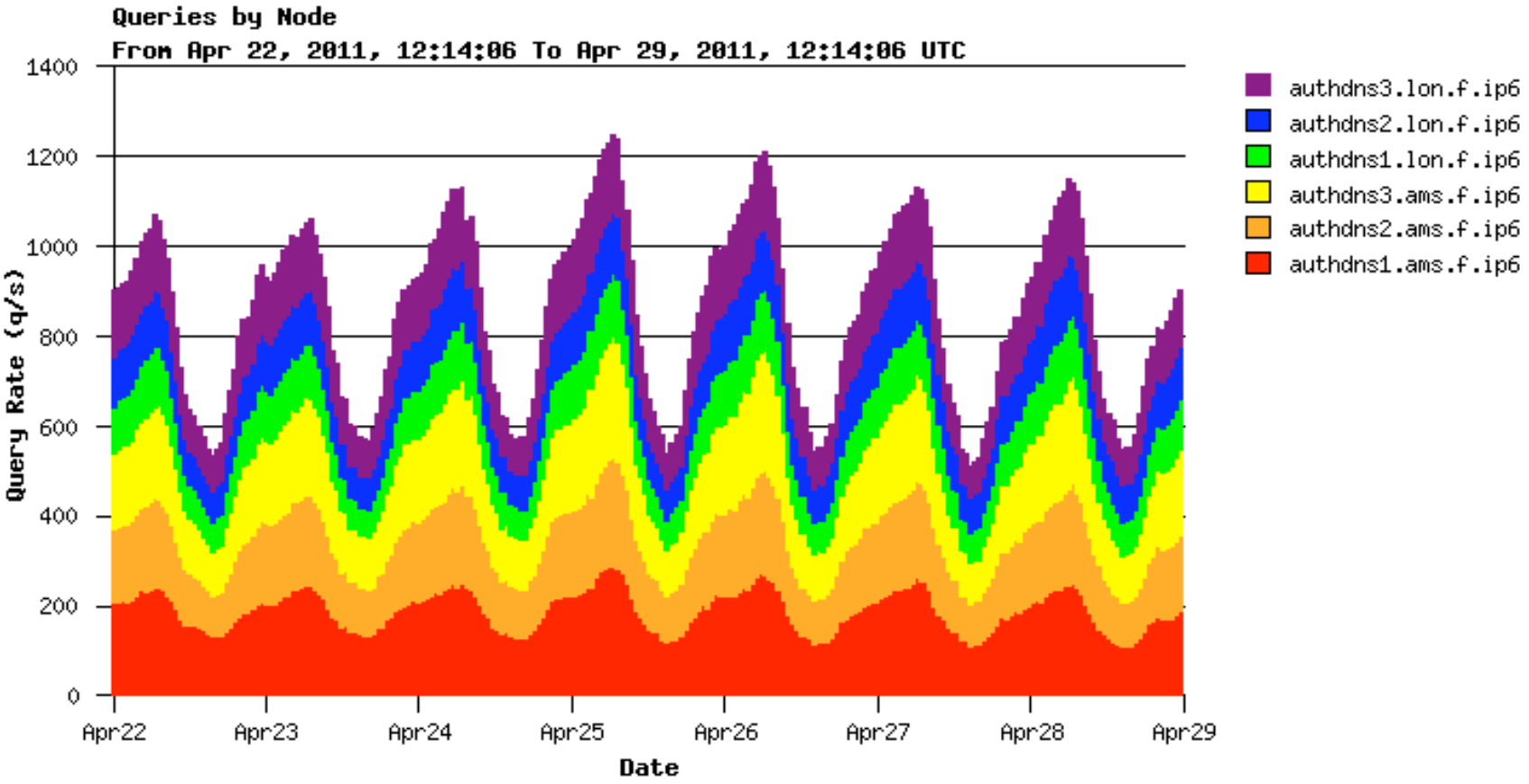
F-reverse (in-addr.arpa)

- Operations stable with 2 instances



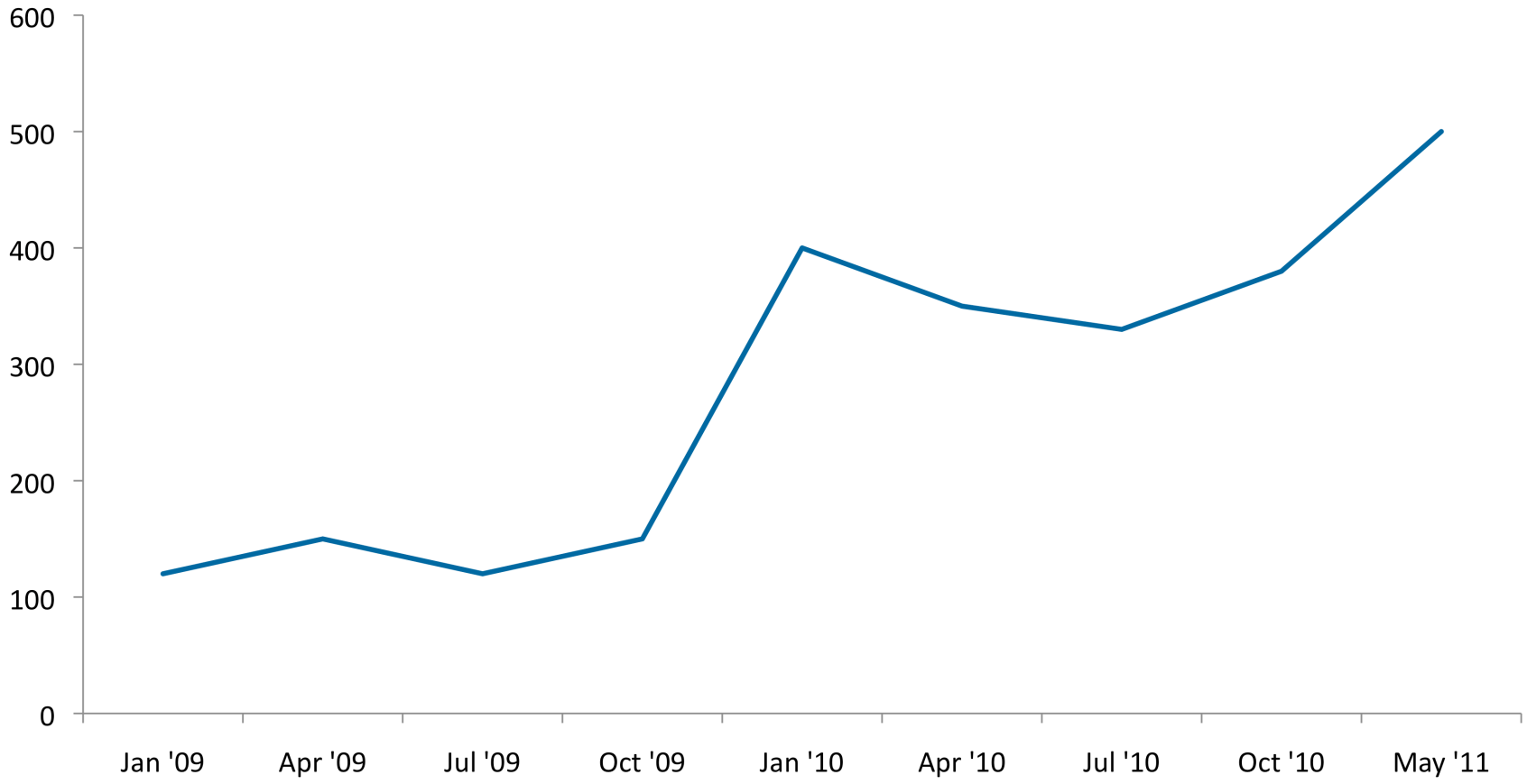
F-reverse (ip6.arpa)

- Operations stable with two instances



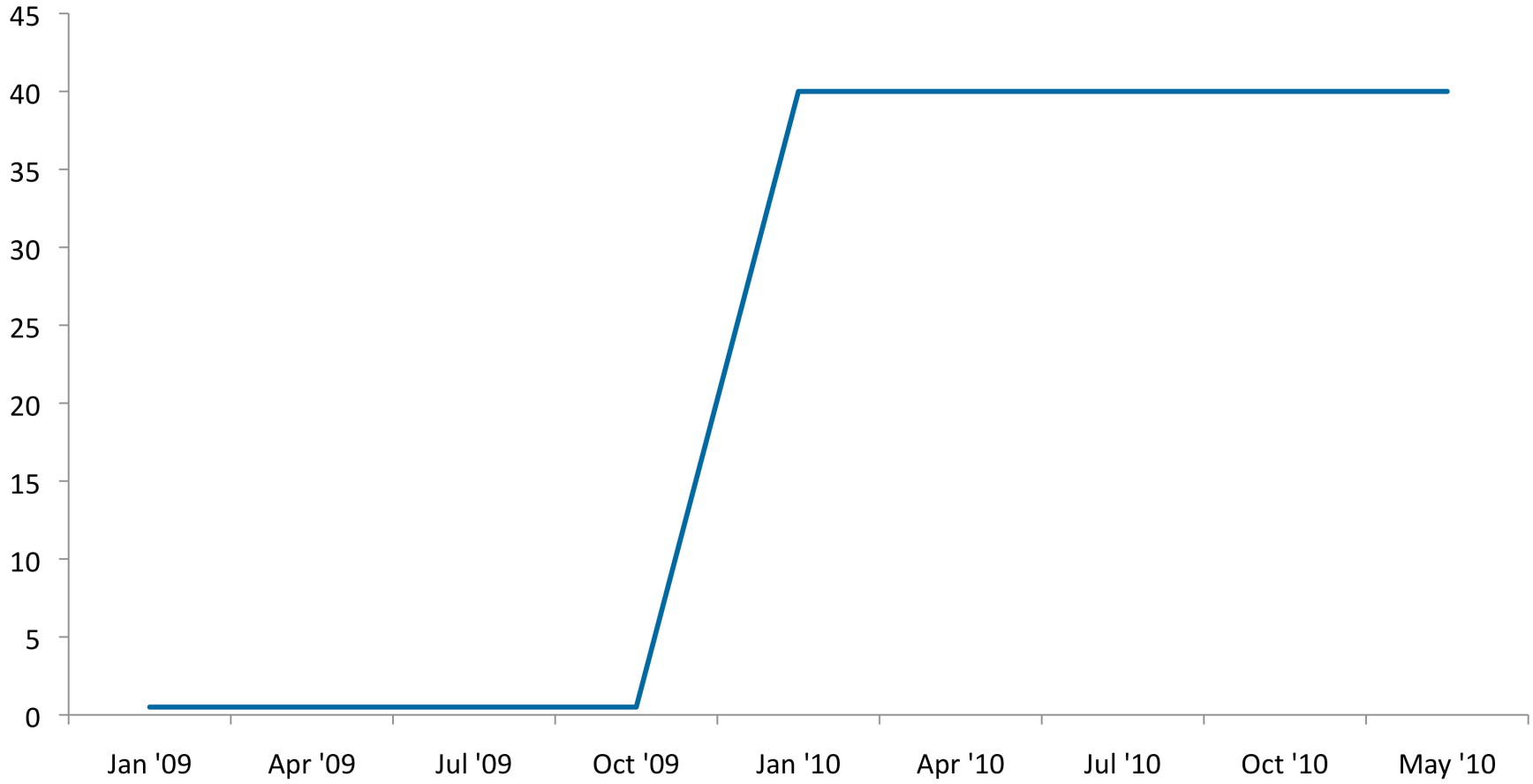
K-root IPv6

- Queries per second received over IPv6



K-root and TCP

- Queries per second received over TCP



Future Plans: Analysis

- Extend operational analysis and monitoring
  - Using scalable infrastructure based on Apache Hadoop
  - Allows near real-time inspection of traffic patterns
- Continuous data input from our DNS systems
  - AS112, K-root, F-reverse
- Code to be released on RIPE Labs

Future Plans: Anycast Cluster

- ns.ripe.net
  - Secondary for LIR reverse space
  - Hosts around ~4,500 zones

- ns-<ccTLD>.ripe.net
  - Secondary for developing country ccTLDs
  - Lots of communication with all the ccTLDs involved

Future Plans: Provisioning For < /24 Zones

- Currently done manually on request
- Will integrate into automated provisioning
  - Create a domain object in RFC2317 format
  - Example

    192.0.2.0/25 = domain: 0-128.2.0.192.in-addr.arpa

Dash Notation in Reverse DOMAIN

- Proposal sent to mailing list
- Drop current dash '-' syntax and expansion from third octet (1-100.2.10.in-addr.arpa)
- Causes problems with DNSSEC
- Allow dash in fourth octet for classless delegations (6-25.1.2.10.in-addr.arpa)
- Stored in RIPE Database with dash
- Expansion done by DNS provisioning

AP57.2: Cleanup Forward Domain Data

- Started with **domain** objects in the RIPE Database for 43 ccTLDs
- Three are still actively using the RIPE Database
  - All three working on alternative solutions
- 40 deleted – TLD object with all sub-domains
- Users cannot create new TLD objects
- Syntax will be changed when last three deleted

Questions?

wnagele@ripe.net

RIPE NCC