ISC & BIND Update

ICANN 51, October 2014

Vicky Risk, Product Manager

Peter Losher
Sr. Sys. Eng

Jeff Osborn
President

Jim Martin
Dir. Network Ops

Evan Hunt
Sr. Software Eng

Eddy Winstead
Sr. Sales Eng

Michael McNally
Support Engineer

Agenda

1. **Current offering for TLD operators**
   - 2014 Development Initiatives
   - Missing features & Roadmap
   - Software support strategies
   - Development and support team
   - Security vulnerability process
2. Performance vs. Functionality
3. New feature decisions
4. TLD User base

2014 Development Initiatives

- Refocusing on BIND9
  - ✓Released BIND 9.10.0, 9.10.1
  - ✓DDOS support, simulation test bed
  - ✓Fuzz testing (Codenomicon CROSS)
  - – Improving automated test coverage
  - – Creating new DNSSEC documentation

- Open source contributors, OS packagers

  source.isc.org

- Re-hosted DLV site, upgrading bug db

“Missing” Features & RFCs

- DNSSEC Key policy manager
  - We have key generation, and in-line signing, this would automate rolling keys, manage overlap and housekeeping (deleting old files)
- DNS Parent updating
  - Child DNS, Child DNS KEY records
  - http://tools.ietf.org/html/draft-ietf-dnsop-delegation-trust-maintainance-14
- Negative trust anchor
  - Available today to subscribers, will be in 9.11

BIND 9.10 - April 2014

- MAP zone file format
  - speed start-up
- Native PKCS#11
  - simplify HSM integration

  - RRL on by default
  - New statistics
  - Zones sharing between views
  - DNSSEC troubleshooting “Delv”
  - DNS Pre-fetch
  - DNS Cookies (first DNS server to implement)
  - CAA records support (9.10.1)
  - Linux SECCOMP (9.10.1)

BIND 9.11 planned features

- One-touch zone addition
- DNSSEC Key policy manager
- Wire-speed logging with DNStap
- Parent updating (CDNS, CDNSKEY rr)
- DNSSEC Negative Trust Anchor
- DDOS mitigations (resolver features)

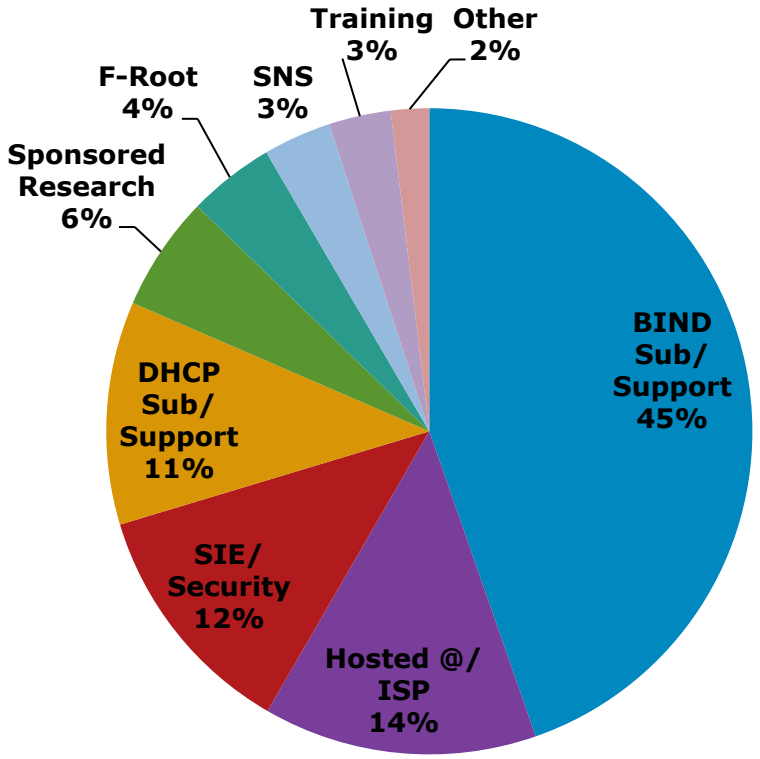
In Planning & Design phase
Targeted – mid 2015

Agenda

1. **Current offering for TLD operators**
   - Development Initiatives
   - Missing features & Roadmap
   - **Software support strategies**
   - **Development and support team**
   - **Security vulnerability process**
2. Performance vs. Functionality
3. New feature decisions
4. TLD User base

Open Source – funded by subscriptions

- In 2013 we introduced support subscriptions, replacing the BIND Forum Membership as our primary funding mechanism
- SW maintenance and incremental feature development is entirely funded by support subscriptions



ISC 2013 Revenue

Multiple Support Levels

Benefits & Levels	Gold	Silver	Bronze	Basic
Product Support Traditional software support, including troubleshooting and how-to questions. Also includes software updates and patches.	**Critical Response** 30 minutes 24 x 7 **Standard Response** 4 business hours 9am - 5pm EST Monday - Friday Phone & Email	**Critical Response** 1 hour 24 x 7 **Standard Response** 8 business hours 9am - 5pm EST Monday - Friday Phone & Email	**Critical Response** 2 hours Business hours only **Standard Response** 8 business hours 9am - 5pm EST Monday - Friday Email	Not included
Advance Security Incident Notifications Proactive notification of security issues before public announcement. In some instances, no advance notification is possible.	When first patch is available for security issue	5 business days before public disclosure	5 business days before public disclosure	3 business days before public disclosure

Basic Subscription

- $10k USD annual subscription
- Good for people who don't need technical support
- >3 days advance notice of a security vulnerability
- Software fix for the problem
- Security for your network

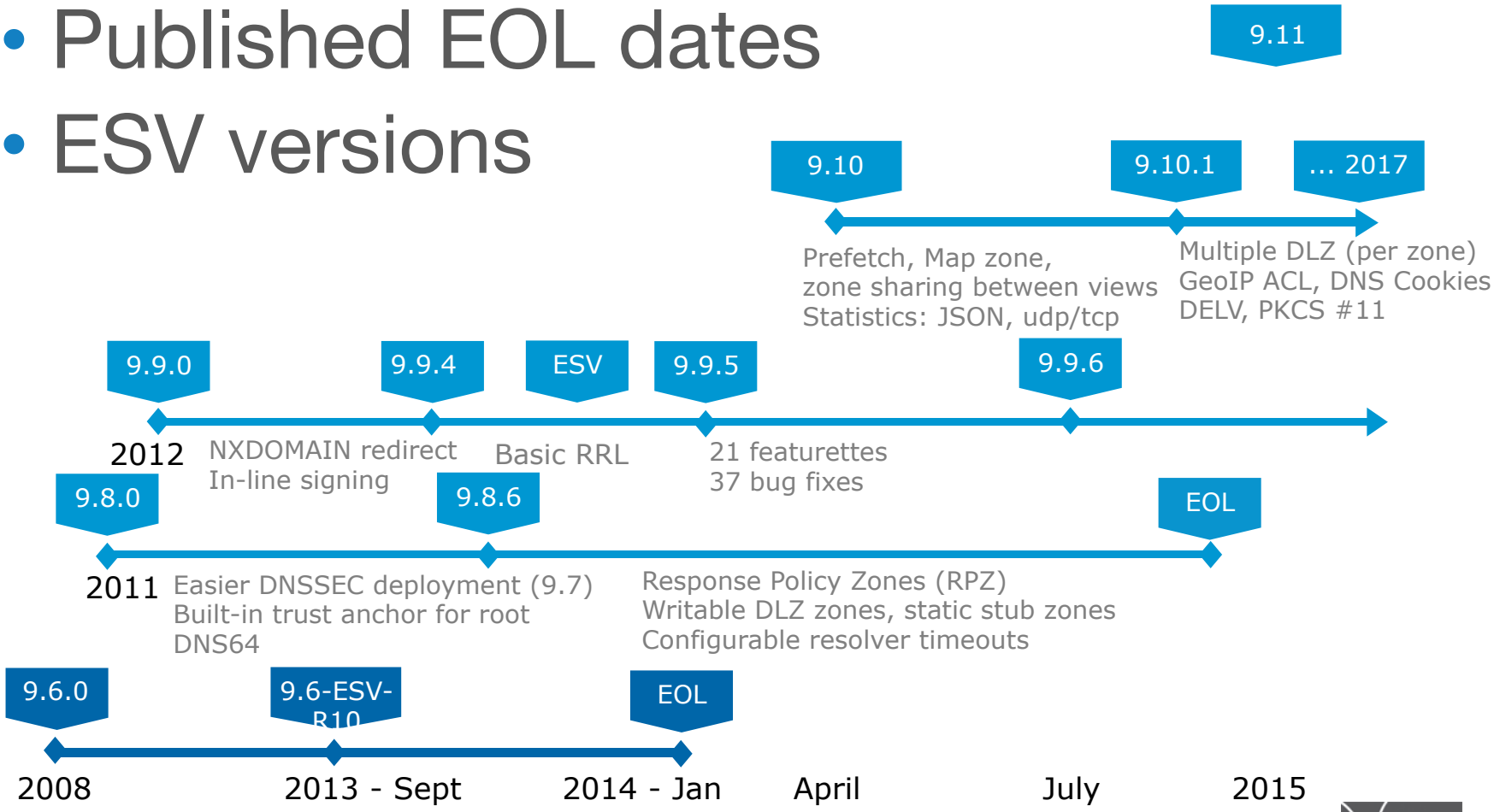
the BASELINE for everyone

Support customers

- ~~Search engine~~
- Privacy for your support issues (no need to post on open lists)
- Priority in getting bugs fixed and feature requirements addressed
- Annual configuration review
- Up to 7x24 support with 30 minute response time for critical issues

Multiple release train options

- Published EOL dates
- ESV versions



Operating Systems

Microsoft
Windows®

Staff supporting BIND

7 x 24 On-call rota includes both support & development (escalation)

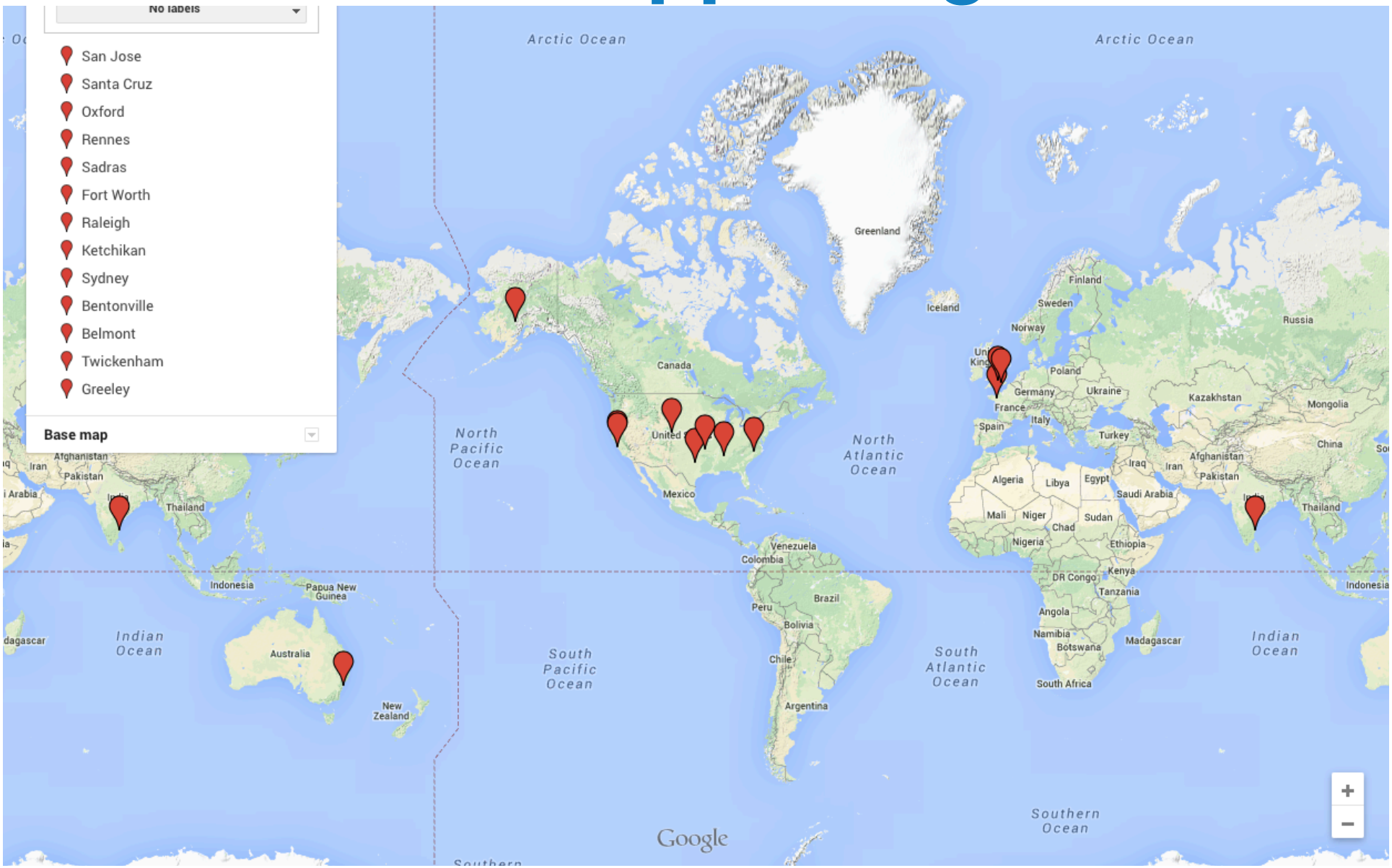
BIND9 Development

- Dedicated BIND Software Engineering (3 + 1 p/t)
- Build/test/security engineer (1)
- Engineering Director (1)

BIND9 Support

- Tech support staff (4)
- Consulting and training (2)
- Customer service (1)
- Project manager (1)

ISC Staff supporting BIND



Security Vulnerability Process

- Published security vulnerability handling policy
  - http://www.isc.org/downloads/software-support-policy/security-advisory/
- Conduct analysis and communications confidentially and securely
- Leverage Industry best-practices

www.first.org/cvss
Risk assessment

http://cve.mitre.org/
Unique identifier

ISC

Phased Disclosure Process

- Enables operators to upgrade critical systems before the vulnerability is published
- We provide advance notification to:
  - Root operators (free, 5-day)
  - Operating system packagers (free, 24 hour)
  - Subscribers
  - OEMs
- We make it very easy for others to get public notification, via www.isc.org, https://lists.isc.org/mailman/listinfo/bind-announce, and RSS feed: https://www.isc.org/?feed=security-feed

Agenda

1. Current offering for TLD operators
2. **Performance vs. Functionality**
3. New feature decisions
4. TLD User base

Performance vs. Functionality

- BIND is intended as a complete, reference implementation
- A comprehensive feature set and faithful adherence to standards is higher priority than performance leadership

Features vs. Performance

Adding features

Periodically, optimize

Features vs. Performance

- In general, adding features reduces performance
- Ideally, you periodically schedule in optimization work or new methods
  - e.g. Map-zone file format, DNS pre-fetch
- We look for unexpected changes in performance

TLD Requirements

Manageability, stability & performance

- Efficient, automate-able process for adding zones, updating a large network of slaves frequently
- DNSSEC operational support – In-line signing
- HSM support

Performance - incremental signing for large zones

- Time to transfer large, signed zones
- Fast reload/restart

Independent Benchmarking

What would make this most useful?

- Active participation from users in creating realistic test scenarios
- Ability to compare configuration options (which may be product-specific)
- Comparisons between successive versions of the same product
- Comparisons between h/w or OS platform choices per product

Agenda

1. Current offering for TLD operators
2. Performance vs. Functionality
3. **New feature decisions**
4. **TLD User base**

New Feature Considerations

- **Do no harm**
- Long-standing commitment to open standards
- Scalability, efficiency and security of the DNS & Internet
- Is requestor contributing somehow?
- Balance the needs of different types of users

BIND installed base?

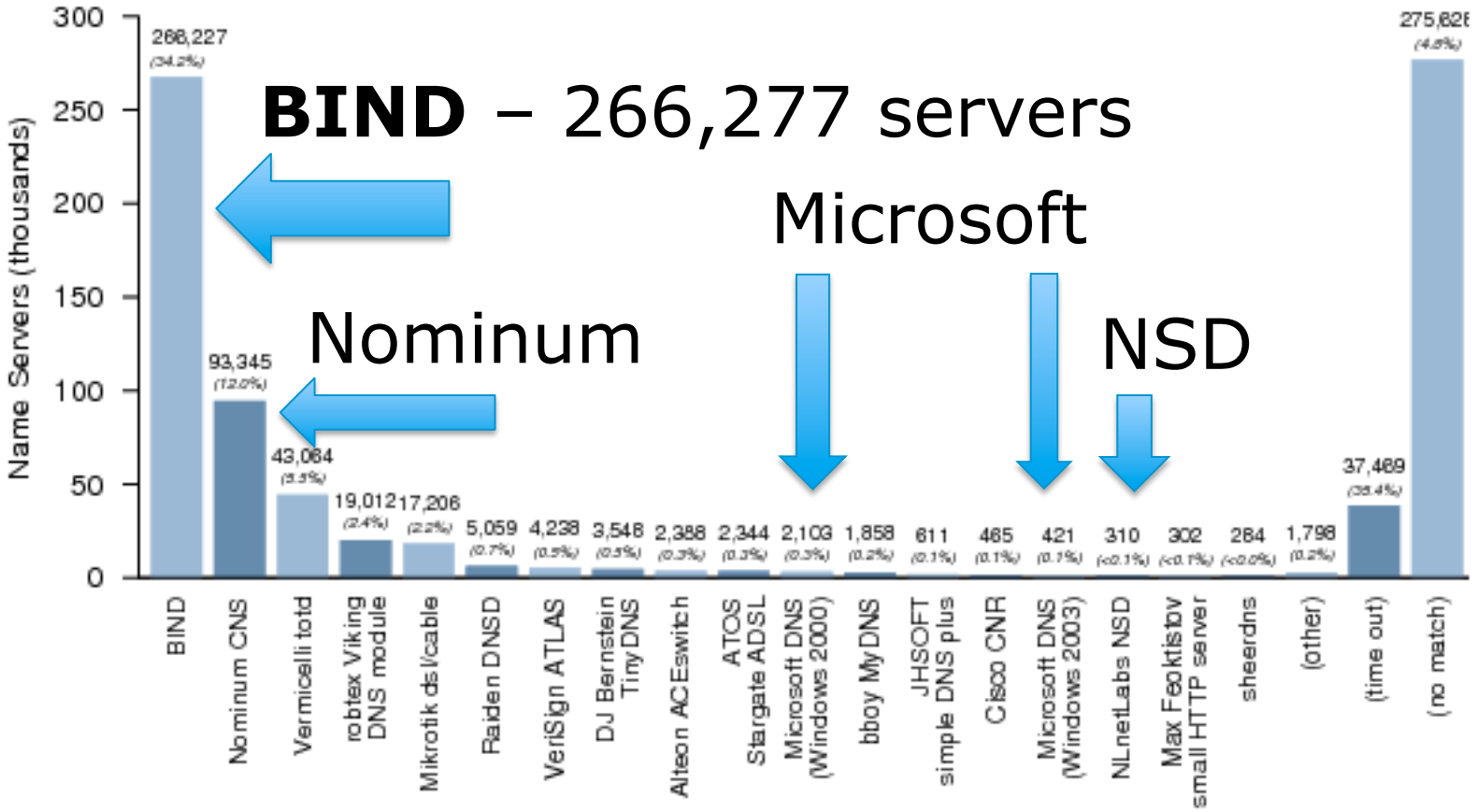


Figure 1: Distribution of name server software versions — Dataset I.
From The Measurement Factory, 2010
http://dns.measurement-factory.com/surveys/201010/

BIND in F-Root

Since 1994, ~55 nodes
First to sign mutual responsibilities agreement with ICANN

TLDs using *and supporting* BIND

* multi-vendor

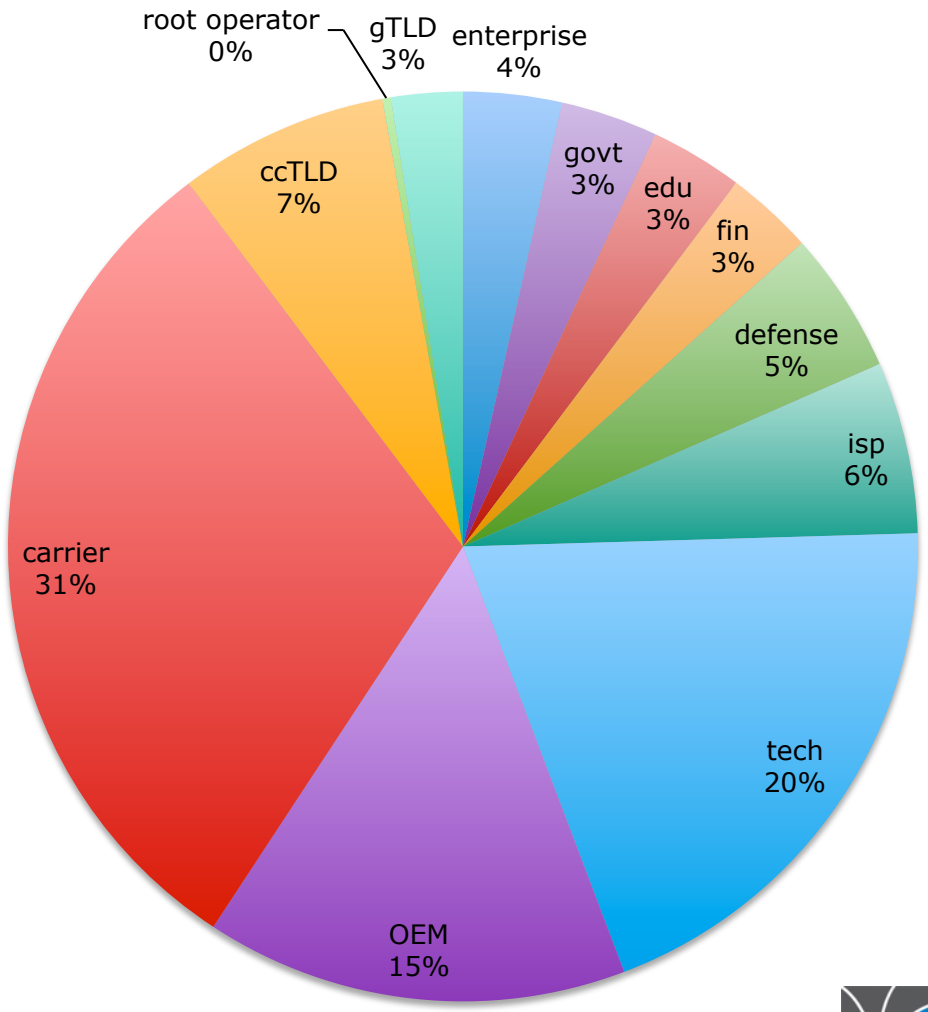
Permission received to list

User Base

A very small proportion of users actually support the open source they use

CCTLD and GTLDs supporting BIND make up 10% of our support base

Annualized BIND subscription revenue as of August 29, 2014 by industry grouping



References

- 2013 Annual Report
  - http://www.isc.org/2013-isc-annual-report-2/
- Sign up to receive Bind Announcements
  - https://lists.isc.org/mailman/listinfo/bind-announce
- Software support policy
  - http://www.isc.org/downloads/software-support-policy/
- Security vulnerabiity reporting
  - http://www.isc.org/downloads/software-support-policy/security-advisory/
- Security vulnerability disclosure
  - https://kb.isc.org/article/AA-00861/0
- ISC Open Source license
  - http://www.isc.org/downloads/software-support-policy/isc-license/