Knot DNS - update

Tech Day – ICANN 50

Ondrej Filip • ondrej.filip@nic.cz • 23 Jun 2014 • London

What is Knot DNS?

- https://www.knot-dns.cz/
- High-performance and scalable authoritative DNS server
- Free, open-source, written from scratch
- Under active development
- Standards compliant and fast tracking
- Non-stop operation (runtime reconfiguration)
- Usable for root, TLD and DNS hosting
- DNSSEC automatic signing
- Pluggable modules

Knot DNS history & roadmap

- Knot DNS 0.8 – 1.4.6 [stable release]
  - First public release in 2011 (0.8)
  - Active development - fast-forward
  - DNSSEC automatic signing (1.4)
- Knot DNS 1.5 [release candidate]
  - Lots of refactoring under the hood
  - Pluggable modules
- Knot DNS 1.6 [WIP]
  - Real-time DNSSEC signing
  - Own key management utilities

DNSSEC automatic signing

- Technology Preview (but rock stable – large ISP)
- Simple configuration


```
zones {
    example.com {
        file "example.com";
        dnssec-enable on;
        dnssec-keydir "/etc/knot/keys";
    }
}
$ knotc signzone
```

Pluggable modules

- Hooks in query-response processing
- Different possibilities
  - Split-horizon (GeoIP, ...)
  - Poor man’s HA
  - **Reverse and forward resource record synthesis**
  - **dnstap**

Synthetized resource records

- IPv6 address space is vast
  - It’s not possible to have all PTR records in the DNS server manually
  - Customers want to send e-mails from DSL lines
  - MTAs are checking for reverse records and rejecting e-mails
  - Customers are complaining
- Configuration (more in user manual)

```
synth_record "(forward|reverse) \
        <prefix> <ttl> <address>/<nn>";
```

- No DNSSEC signing (planned for 1.6)

Example configuration

```
example.org. {
    query_module {
        synth_record "forward gen- 400 2620:0:b61::/52";
        synth_record "forward gen- 400 192.168.1.0/25";
    }
}
1.168.192.in-addr.arpa {
    query_module { synth_record "reverse gen- example.org.
      400 192.168.1.0/25"; }
}
1.6.b.0.0.0.0.0.0.0.2.6.2.ip6.arpa {
    query_module { synth_record "reverse gen- example.org.
      400 2620:0:b61::/52"; }
}
```

Example output

```
$ kdig AAAA gen-2620-0000-0b61-0100-0000-0000-0000-
0000.example.org.

[...]

;; QUESTION SECTION:

;; gen-2620-0000-0b61-0100-0000-0000-0000-0000.example.org.
0 IN AAAA

;; ANSWER SECTION:

gen-2620-0000-0b61-0100[...] 400 IN AAAA 2620:0:b61:100::

$ kdig PTR 1.0.0...1.6.b.0.0.0.0.0.0.0.2.6.2.ip6.arpa.

[...]

;; QUESTION SECTION:

;; 1.0.0...1.6.b.0.0.0.0.0.0.0.2.6.2.ip6.arpa. 0 IN PTR

;; ANSWER SECTION:

[...] 400 IN PTR gen-2620-0000-0b61-0000-0000-0000-0000-
0001.example.org.
```

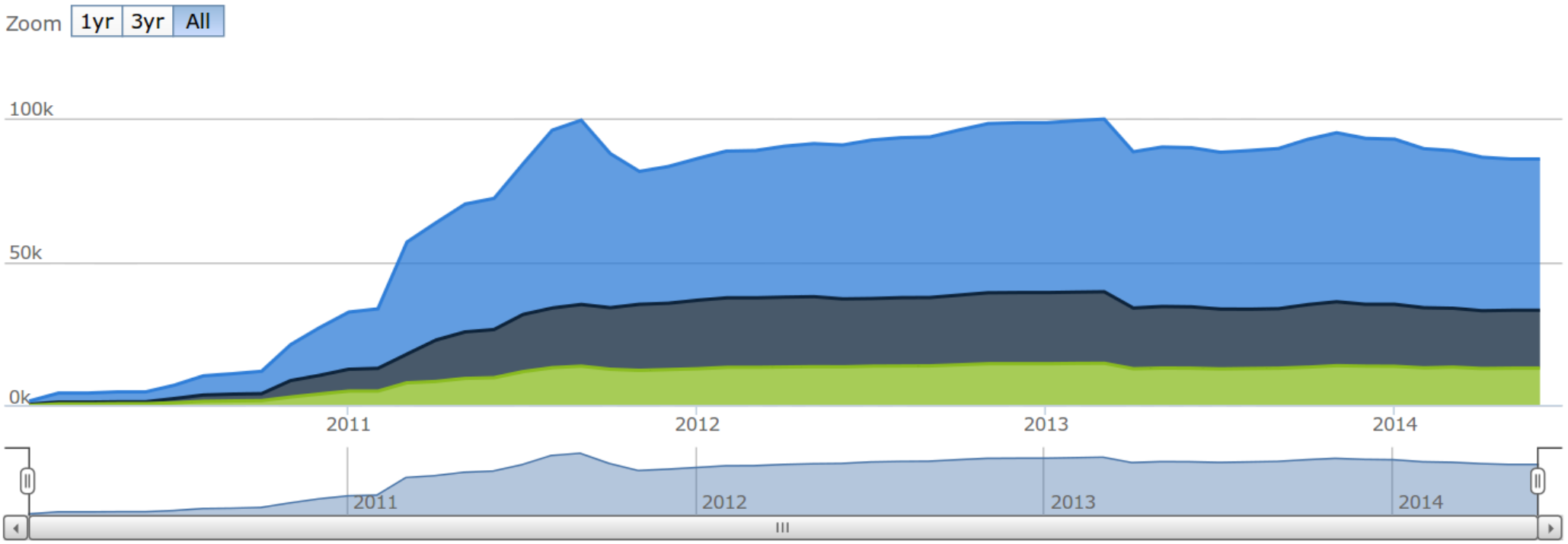
Improved DNSSEC support plan

- libdnssec separation
  - Switch from OpenSSL to GnuTLS (nope, not heartbleed related)
  - Support for hardware security modules (PKCS#11)
  - Key and Signing Policy and tools
- On-line signing
  - Minimal NSEC3 encloser responses
  - Dynamic modules

Refactoring

Total Lines :	85,950	Code Lines :	52,493	Percent Code Lines :	61.1%
Number of Languages :	6	Total Comment Lines :	20,134	Percent Comment Lines :	23.4%
		Total Blank Lines :	13,323	Percent Blank Lines :	15.5%

Code, Comments and Blank Lines



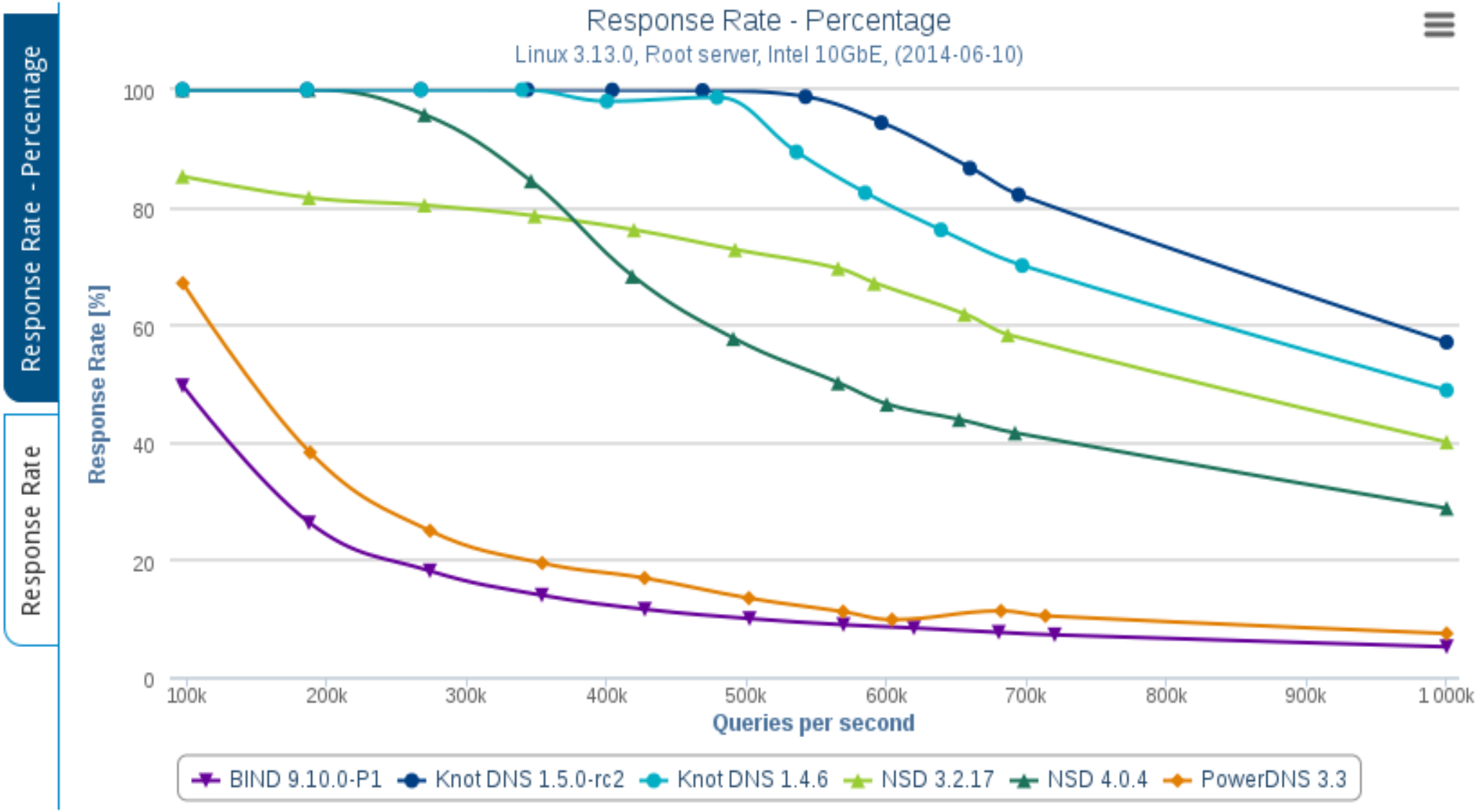
Benchmarking

- Authoritative DNS servers:
  - Bind 9.10.0-P1
  - Knot DNS 1.4.6
  - Knot DNS 1.5.0rc2
  - NSD 3.2.17
  - NSD 4.0.4
  - PowerDNS 3.3

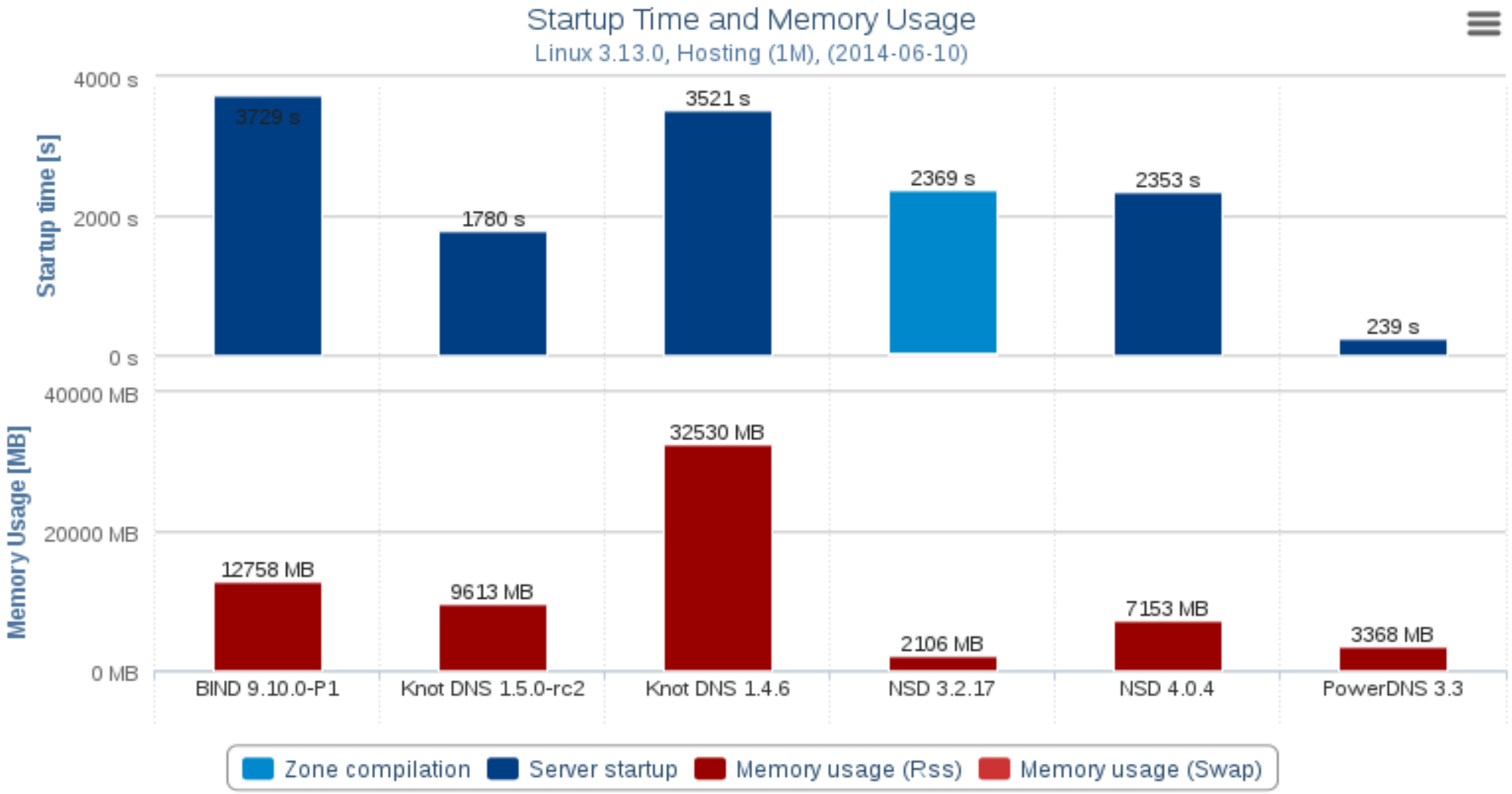
Benchmark setup

- Open source (https://gitlab.labs.nic.cz/labs/dns-benchmarking)
- DISTEL-like setup (Courtesy of NLnet Labs)
- tcpreplay & tcpdump based
- servers: player, listener and server
- Linux 3.13.0; 10GbE Intel NICs, commodity hardware
- Scenarios:
  - Root Zone
  - TLD & TLD (DNSSEC Signed)
  - DNS Hosting (100k & 1M)
  - Results: https://www.knot-dns.cz/pages/benchmark.html

Response rate – percentage (root)



Startup time & memory (1M zones)



Thank You!

Ondrej Filip • ondrej.filip@nic.cz • http://www.knot-dns.cz