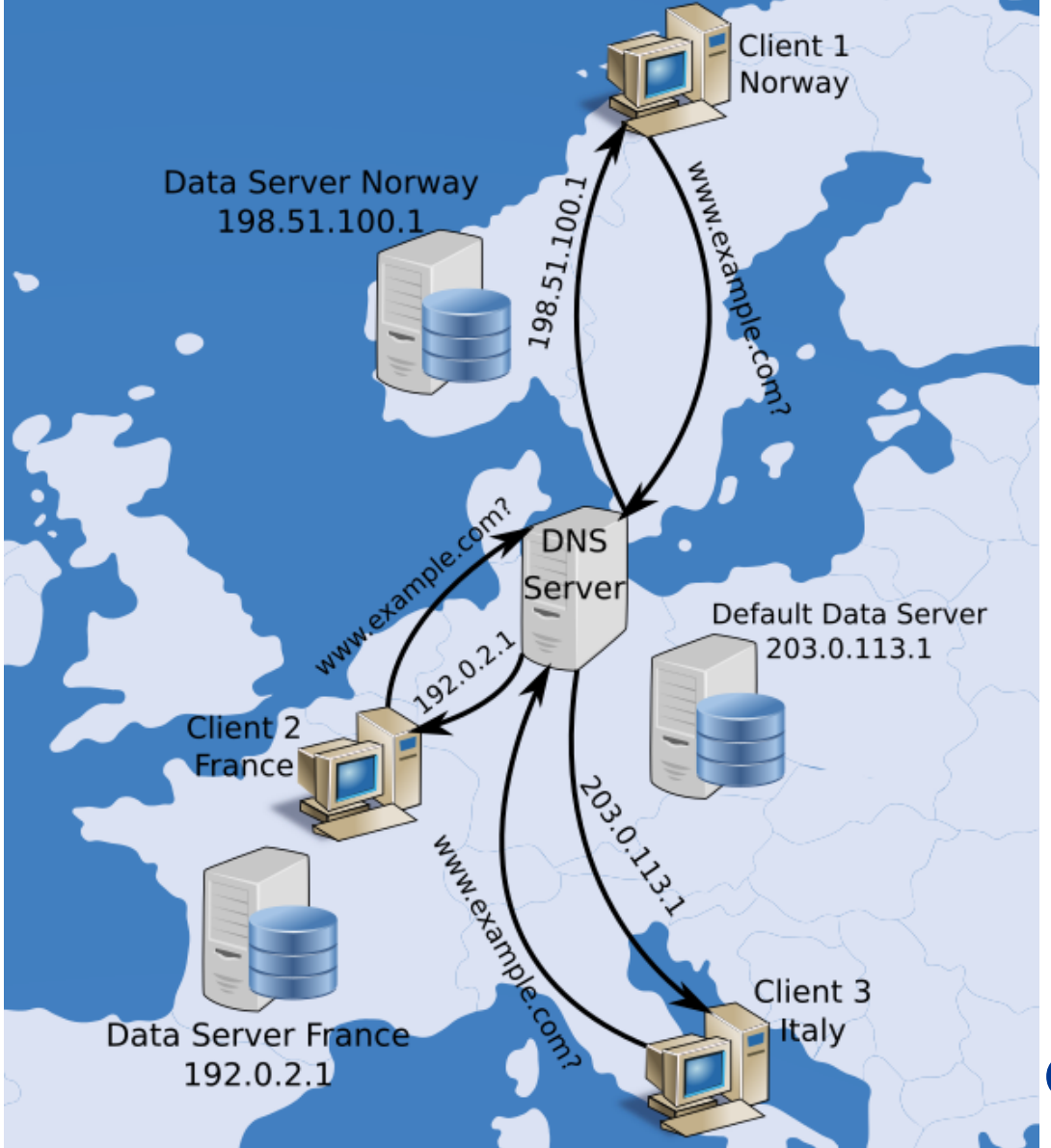
GeoIP + DNSSEC in Knot DNS 2.7

Petr Špaček • petr.spacek@nic.cz • 2018-10-18

GeoIP?

- GeoDNS
  - Tailored DNS responses
    - DNS lies
      - Stupid DNS tricks (credit to Paul Vixie)
- Different responses for different clients
  - Related to EDNS Client Subnet (ECS, RFC 7871)
    - Lowers cache hit rate on DNS resolvers
  - "Cheap"/"application layer" anycast

GeoIP



GeoIP – challenges

- Configuration
  - No standard format for authoritatives
  - Geolocation DB quality
- Performance
  - DNSSEC – on-line signing?
- Complexity
  - Don't do it :-)

GeoIP in Knot DNS 2.7

- Multiple options
- Selection criteria
  - Source IP address / ECS address
  - Subnet / Geo information (MaxMind DB format)
- DNSSEC
  - on-line signing
  - pre-signed zone (pre-computed signatures)
- New feature, feedback is welcome!

Configuration prerequisites

- Zone file with default values (fallback)

```
www.example.com.   3600   A    203.0.113.50
www.example.com.   3600   TXT  "default server"
```

- For EDNS Client Subnet

```
server:
    edns-client-subnet: on
```

- For Geo-based selection
  - IP database in MaxMind DB v2.0 format

Per-subnet: configuration

- server:
  edns-client-subnet: on
- mod-geoip:
  - id: net
    mode: subnet
    ttl: 60
    config-file: "/path/to/net.conf"
- zone:
  - domain: example.com.
    file: "/path/to/example.com.zone"
    module: mod-geoip/net

Per-subnet: data

- File /path/to/net.conf
- ```
  www.example.com:
      - net: 192.0.2.0/24
        A: 192.0.2.50
      - net: 198.51.100.0/24
        A: 198.51.100.50
  ```
- Fallback – zone data

```
www.example.com.  3600  A  203.0.113.50
```
```

Per-subnet: testing

```
$ kdig @127.0.0.1 A www.example.com
   +subnet=192.0.2.66

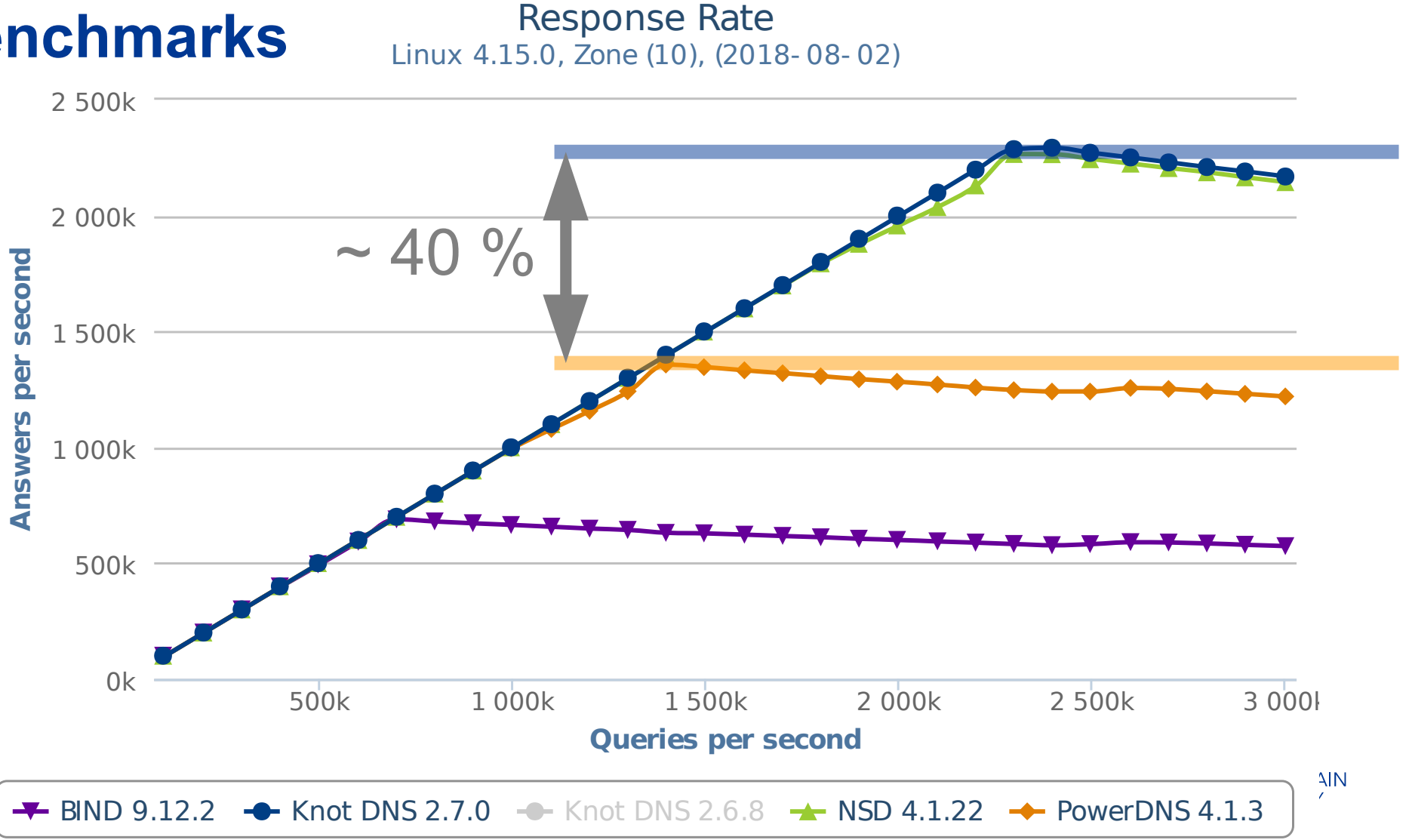

;; EDNS PSEUDOSECTION:
;; CLIENT-SUBNET: 192.0.2.66/32/24
;; ANSWER SECTION:
www.example.com.  60  A  192.0.2.50
```

Per-subnet: performance

Configuration	Queries/second	
unsigned zone	2.5 M	
+ subnet	1.8 M	(72 %)
pre-signed	2.0 M	(80 %)
+ subnet	1.7 M	(68 %)
on-line signing	32 k	(1.3 %)

NSEC, ECDSAP256SHA256

Benchmarks


Response Rate
Linux 4.15.0, Zone (10), (2018- 08- 02)
2 500k
2 000k
1 500k
1 000k
500k
0k
Answers per second
~ 40 %
500k
1 000k
1 500k
2 000k
2 500k
3 000k
Queries per second
BIND 9.12.2
Knot DNS 2.7.0
Knot DNS 2.6.8
NSD 4.1.22
PowerDNS 4.1.3

Moving to Geo: MaxMind DB

```
192.0.2.0/24 {
  "city": {
      "names": {
          "en": "Prague"
        }
  }
  "country": {
      "iso_code": "CZ"
      "names": {
          "en": "Czechia"
      }
  }
}
```

Geo: configuration

- ```
  server:
      edns-client-subnet: on
  ```

- ```
  mod-geoip:
    - id: geo
        mode: geodb
        geodb-file: "/to/GeoLite2City.mmdb"
        geodb-key: [country/iso_code,
                    city/names/en]
        config-file: "/path/to/geo.conf"
  ```

- ```
  zone:
    - domain: example.com.
      file: "/path/to/example.com.zone"
      module: mod-geoip/geo
  ```


  ```

Geo: data

- File /path/to/geo.conf
- ```
  www.example.com:
      - geo: "CZ;Prague"
        A: 192.0.2.0
        TXT: "Prague"
      - geo: "CZ;*"
        A: 192.0.2.2
        TXT: "Czechia"
  ```
- Fallback – zone data

```
www.example.com.  3600  A  203.0.113.50
```
```

Geo: testing

```
$ kdig @127.0.0.1 A www.example.com
   +subnet=192.0.2.66

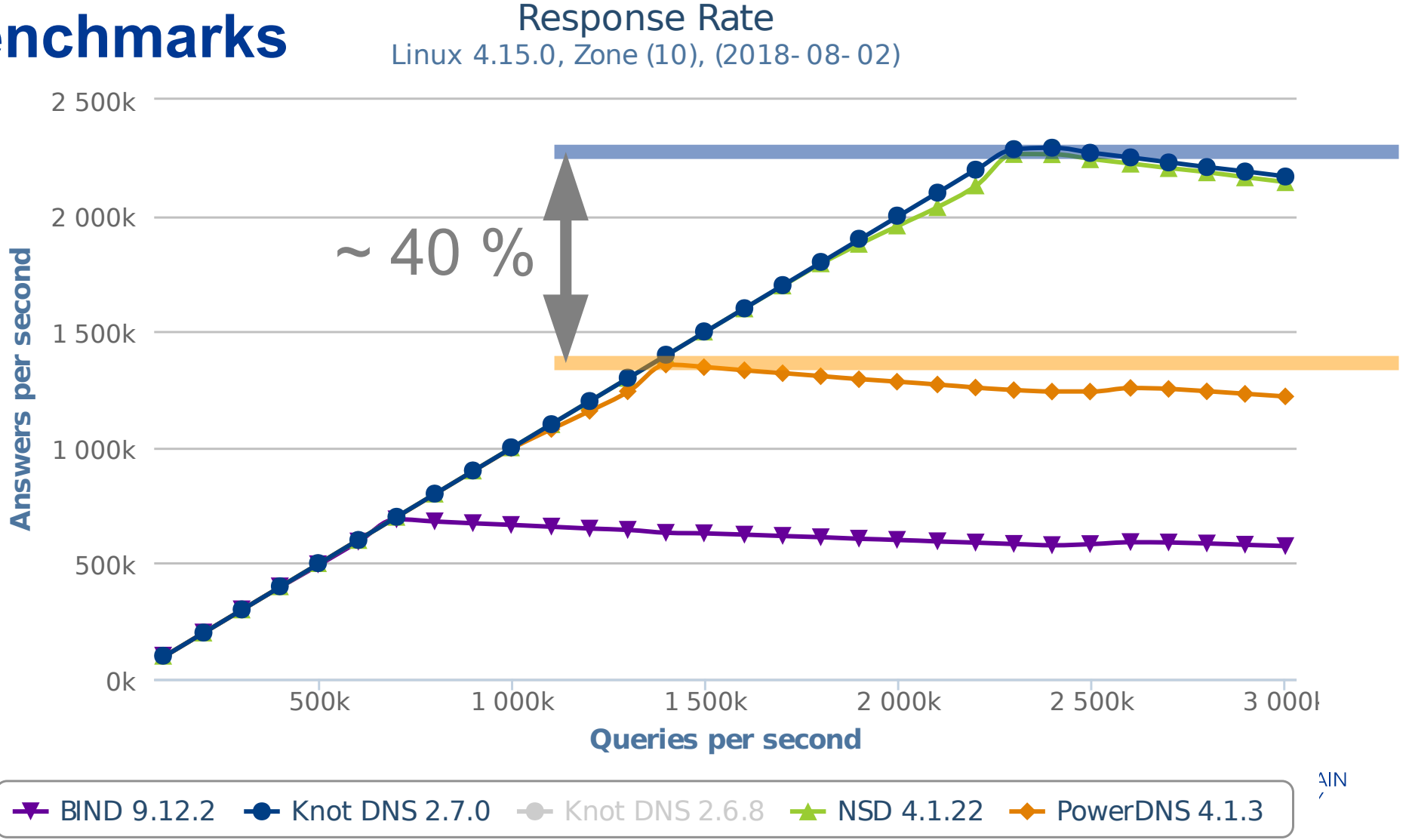
;; EDNS PSEUDOSECTION:
;; CLIENT-SUBNET: 192.0.2.66/32/24
;; ANSWER SECTION:
www.example.com.  60  A  192.0.2.50
```

Geo: performance

Configuration	Queries/second	
unsigned zone	2.5 M	
+ geo	1.6 M	(64 %)
pre-signed	2.0 M	(80 %)
+ geo	1.5 M	(60 %)
on-line signing	32 k	(1.3 %)

NSEC, ECDSAP256SHA256

Benchmarks


Response Rate
Linux 4.15.0, Zone (10), (2018- 08- 02)
2 500k
2 000k
1 500k
1 000k
500k
0k
Answers per second
~ 40 %
500k
1 000k
1 500k
2 000k
2 500k
3 000k
Queries per second
BIND 9.12.2
Knot DNS 2.7.0
Knot DNS 2.6.8
NSD 4.1.22
PowerDNS 4.1.3

GeoIP + DNSSEC

- on-line signing
  - slooooow, limited use-cases
- pre-signed zone
  - fast
  - mandatory default value in zone (NSEC)
  - manual key rollovers
    - (not a perfect integration yet)

GeoIP + DNSSEC

```
policy:
    - id: manual
      manual: on

zone:
    - domain: example.com.
      file: "/path/to/example.com.zone"
      dnssec-signing: on          1.
      dnssec-policy: manual       2.
      module: mod-geoip/net
```

```
$ knotc zone-reload example.com
```

Summary

- Tailored responses based on
  - subnet
  - MaxMind DB
  - EDNS client subnet
- available from Knot DNS 2.7
  - use 2.7.3!
  - use pre-signed variant for performance
- increase diversity of your DNS clusters