Beyond BIND and NSD

Peter Janssen, EURid.eu
Vienna, RIPE 26-1
Beyond BIND and NSD

AGENDA

- Who are we?
- What have we done?
- Why are we doing it?
- Where are we going?
- When?
- Wow?
Who is EURid?

- Belgian not for profit organisation
- Under contract with the European Commission
- Offices in Brussels, Prague, Stockholm and Pisa
- Manage .eu TLD space
  - Registration services (EPP, IDN, DNSSEC, …)
  - “Run” the .eu zone
  - Support services (phone, email, chat, …) in all 23 official languages of the EU
- Currently 3.4 million domain names
The .eu zone

- Name servers
  - “Own maintained” unicast nodes
  - “Third party” anycast meshes

- Update mechanism
  - Dynamic updates
The .eu zone

- Name servers
  - “Own maintained” unicast nodes
  - “Third party” anycast meshes

- Update mechanism
  - Dynamic updates
“Challenges”

- TLD public authoritative slaves
  - Geographical spread
  - Network topological spread
  - Hardware diversification
  - OS diversification
  - Name server software diversification

- Zone Update mechanism
  - Separate process
    - “Listening” on core database
    - Sending “dynamic update” messages to name server
    - Room for improvement/de-complexification
A new DNS implementation

- Primary Design goals
  - Standards compliant
    - Only “RFCs” as design goals
    - Common sense/practice where RFCs are “open for interpretation”
  - Portable, clean, fast
  - Authoritative
  - DNSSEC support
  - AXFR/IXFR support (master and slave)

- Secondary goals
  - Recursive caching resolver?
  - “higher level storage” backend (sql, …)
  - Dynamic update API
  - Dynamic provisioning
Release 1.0 (Roadmap)

- Supported platform: Linux, *BSD, OS X, Windows
- Authoritative
- Load/parse zone files
  - *Include*, *, @, /
  - Resource record types
    - SOA, A, AAAA, NS, CNAME, PTR, DNAME, HINFO, MX, TXT
    - DNSKEY, DS, RRSIG, NSEC, NSEC3, NSEC3PARAM
- Zone transfer
  - Master & Slave
  - AXFR / IXFR
  - Notify
  - TSIG
- nsupdate
  - add, remove RR
- DNSSEC
  - RSASHA1(5,7)
  - Online re-signing
  - key roll-over
Release x.y (Roadmap)

- Release 1.1
  - DSA/SHA1, DSA-NSEC3-SHA1, RSASHA256, RSASHA512
- Release 1.2
  - Full client to “control” the name server daemon
- Release 2.0
  - Caching resolver
  - Validating
  - Stand alone libraries; perl wrapper around dnsresolv
- Release 3.0
  - Sql backend API
  - ...

Peter Janssen, EURid.eu    Vienna, RIPE 26-1
Roadmap

- Code clean up
- Bug fixing
- Documentation
Performance measurements

- The setup

Dual Xeon 2Ghz, 8GB RAM, Linux 2.6.32 (x64)

Client

Dual Xeon 2Ghz, 4GB RAM, Linux 2.6.32 (x64)

Server

www.domainname.eu A (no DNSSEC)
Random query list
50% existing domain names
.eu zone (3.3M domain names, 7.7M records)
NSEC3 signed
The setup
- Pre-created PCAP file
- Tcpreplay `-p speed `pcapfile’ : to generate queries
- Tcpdump : to capture responses
- Runs of 30 seconds

Eg. 50Kq/s
- 50Kq/s * 30s = 1,500,000 packets -> pcap file
- Tcpreplay `-p 50000
  - 29.7 seconds -> 50,505 q/s
- Tcpdump results
  - How many packets received

<table>
<thead>
<tr>
<th>q/s</th>
<th>Real q/s</th>
<th>Sent</th>
<th>Received</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>50K</td>
<td>50.50K</td>
<td>1.5M</td>
<td>1.5M</td>
<td>100</td>
</tr>
<tr>
<td>75K</td>
<td>74.47K</td>
<td>2.25M</td>
<td>2.2M</td>
<td>97.7</td>
</tr>
<tr>
<td>100K</td>
<td>101.2K</td>
<td>3M</td>
<td>2.8M</td>
<td>93.3</td>
</tr>
</tbody>
</table>
Performance measurements

Response Rate vs. Query Rate (Qps)

- Series 1
- Series 2
- Series 3
- Series 4

Queries per second (Qps)

Response Rate (Percentage)

0,00%  20,00%  40,00%  60,00%  80,00%  100,00%
Performance measurements

- The setup (2nd coming)

Client

tcpreplay

tcpdump

Server
Performance measurements

Response Rate vs. Query Rate (Qps)

- Series 1
- Series 2
- Series 3
- Series 4

Queries per second (Qps)

Response Rate (Percentage)

- 100.00%
- 90.00%
- 80.00%
- 70.00%
- 60.00%
- 50.00%
- 40.00%
- 30.00%
- 20.00%
- 10.00%
- 0.00%
Performance measurements

- The setup (3rd coming)

Client

---

Server

tcpdump

Block outgoing packets

Query

Response

tcpreplay
Performance measurements

- **Response Rate vs. Query Rate (Qps)**

  - Mirror
  - .eu
  - nsd
  - Bind
  - MirrorB
  - .euB
  - NSDB
  - BindB

  - **queries per second (Qps)**: 0K, 50K, 100K, 150K, 200K, 250K, 300K, 350K, 400K, 450K, 500K
  - **Response Rate (Percentage)**: 0%, 0.00%, 20%, 40%, 60%, 80%, 100%
Conformity testing

- RFCs
- Automated testing
  - Random Bit flipping
- Manual testing
  - Deliberate bit manipulation
- Community input/testing
  - Node on the internet with “known zone file”
Availibility

- “Some sort of open source” license
- Test node(s)
- Binary packages for “home testing/playing”
Code & stats

- Written in C
- Libraries
  - dnscore : 11K lines code + 2.6K lines header
  - dnsdb : 17K lines code + 2.7K lines header
  - dnszone : 2K lines code + 0.2K lines header
- Main program
  - 8.9K lines code + 1.1K lines header
- Dev effort
  - 2.2 man year
Does it have a name?

- All the good ones were taken....
- But yes, it has a name.....
Does it have a name?
One more thing …

yadifa.eu. IN SOA …
  NS ns.yadifa.eu.
  NS yadifa.eurid.eu.

www.yadifa.eu. A ….
yadifa.eu. MX ….

http://www.yadifa.eu

info@yadifa.eu