BIND 10
DNS Project Status + DNS Resolver Status/Plans

Shane Kerr
shane@isc.org

23 January 2013

DNS Project Status

BIND 10 Introduction

- A radical look at network daemon architecture and design
- Customizable
- Scalable
- Reliable
- Re-usable

DNS Subsystems (1 of 2)

- Authoritative DNS working
  - SQLite or in-memory data source
  - Answers slightly better than BIND 9
  - Much reduced memory footprint
  - Needs work for large/many zones
- Zone transfers working
  - AXFR or IXFR, inbound or outbound
  - ACL / TSIG secured
  - Needs work for large/many zones
- DDNS working

DNS Subsystems (2 of 2)

- Statistics working
  - Working on scaling
- DDNS zone management missing
  - No signing, re-signing, inline signing
  - No HSM support
- Resolver just proof-of-concept
  - Low performance
  - No DNSSEC
  - Buggy

Release Timeline

- Currently in Beta for 1.0.0
  - Feature freeze
- Release candidate 2013-02-07
- Release to follow shortly after
- 1.0.0 based on subsystem status
  - Basically... authoritative only

DNS Resolver Status/Plans

Resolver Phases

1)Research & Design

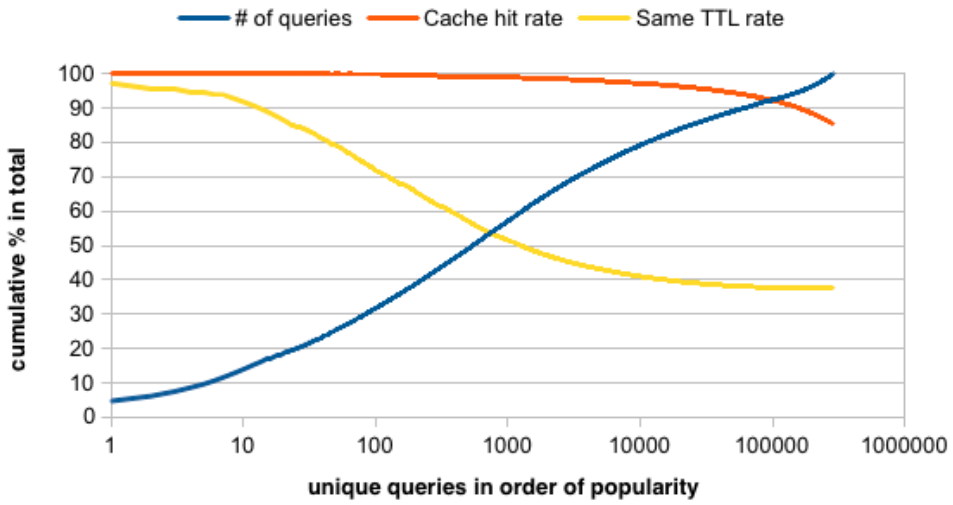
2)Basic Resolver

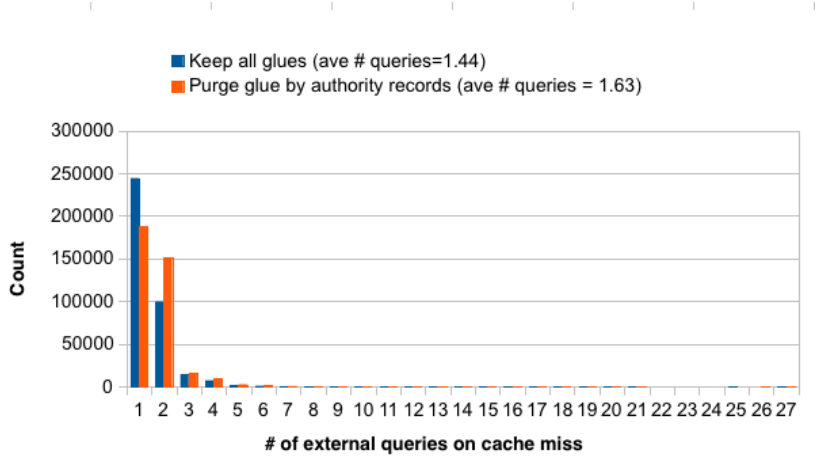
3)Validating Resolver

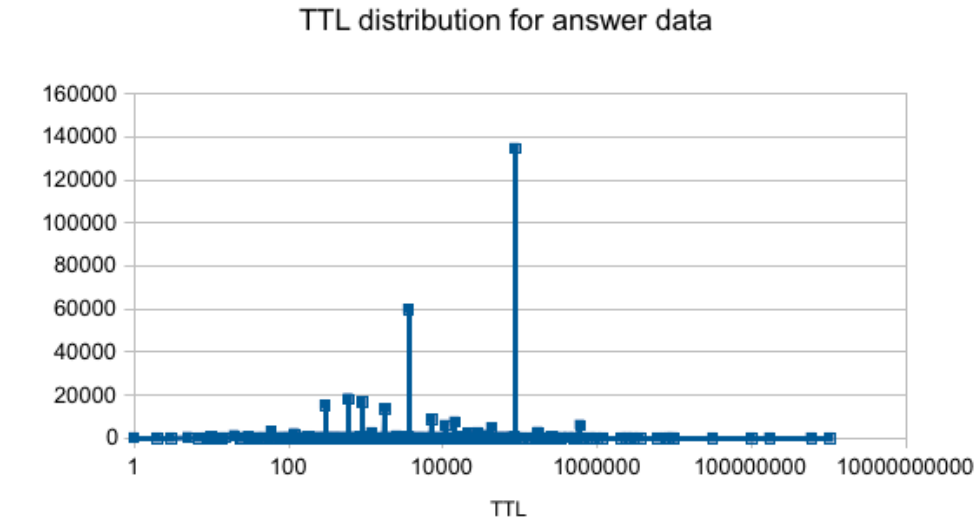
4)Hooks

x)Non-Essential Stuff

Research


# of queries
Cache hit rate
Same TTL rate
cumulative % in total
100
90
80
70
60
50
40
30
20
10
0
1
10
100
1000
10000
100000
1000000
unique queries in order of popularity


Keep all glues (ave # queries=1.44)
Purge glue by authority records (ave # queries = 1.63)
Count
300000
250000
200000
150000
100000
50000
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
# of external queries on cache miss


TTL distribution for answer data
160000
140000
120000
100000
80000
60000
40000
20000
0
1
100
10000
1000000
100000000
10000000000
TTL

Research

- Analyzed real-world data
- Built tools to measure properties
- Checked several theories
- First pass of iteration only!
  - Needs several design/analysis loops

http://bind10.isc.org/wiki/ResolverPerformanceResearch

Basic Resolver

- Recursion
- DNS cache
- Query tracing
- Server capability tracking
- Port randomization
- Root priming
- EDNS0
- Locally-served zones
- DNSKEY fetching

Validating Resolver

- Manual trust anchor configuration
- Signature verification
- Cache modifications
- CD/AD bit handling
- RRSIG RR validity checking
- NSEC handling
- NSEC3 handling
- SHA-2, GOST, ECDSA
- Negative trust anchors

Code Hooks

- Define a way to extend BIND 10
  - Like plug-ins
  - GeoIP, RPZ, RRL, and similar will probably all be via hooks in BIND 10

Non-Essential Stuff

- RFC 5011
- ICMP port unreachable collection
- Multi-tiered cache
- Cache persistence
- Cache migration