Current status of Yeti DNS Project

Davey Song @ BII Lab
2015.10.31 Yeti Workshop, Yokohama
Outline

• Background & Motivation
• Yeti Testbed & Statistics
  • Distribution master
  • Authority server
  • Resolver & traffic
  • Data collection & Monitoring
• Some technical findings and bugs report
• Conclusion
Related work & discussion on Root System

- ICANN ITI Panel & technical report
- ICANN RSSAC documents
  - RSSAC 002: Advisory on Measurements of the Root Server System
  - RSSAC003: Report on Root Zone TTLs
  - History and Technical Analysis of the Naming Scheme Used for Individual Root Servers (working on)
- [ICANN Root Zone KSK Rollover Plan](#)
- [Scaling the Root by Geoff Huston, IPJ, March 2015](#)
- IETF work on DNS Root system
  - draft-ietf-dnsop-root-loopback-05
  - draft-ietf-dnsop-resolver-priming-05
  - RFC7626: DNS Privacy Considerations, by S. Bortzmeyer
Root system is “special”? 

• The top infrastructure /entrance of DNS system/
• The priming process & hint file stuff is not fully documented as part of DNS protocol
• Produce Root zone / signed the Root zone /Distribute the root zone by various parties
• The KSK of Root zone is the Trust anchor / No parent DS
• Rely heavily on BGP routing system (Anycast) to support Root system
• Regarding Internet governance for non-technical people
  • may view the root as “the control of Internet”
What is Yeti?

• Yeti is an IPv6 only Live Root DNS Server System Testbed
  • Precisely mirrors the IANA DNS namespace
  • Experimental project with 3 years duration and clear goal
• Like IANA, has diverse servers globally
  • Server operators are volunteers from many nations
• Like IANA, has DNSSEC, with a published signing key
  • Has its own DNSSEC signing and validation keys
• System is intended for Internet-scale *science*
Why: Problem Space of Yeti(1)

Conflict between DNS Centralization Vs. Network Autonomy

- **External Dependency**
  - Local services rely on external root services
  - Require external management and support

- **Surveillance risk**
  - Information leakage cause by the DNS Root lookup
  - RFC7626: DNS Privacy Considerations, by S. Bortzmeyer
Why: Problem Space of Yeti(2)

• Can IPv6-only DNS survive?
  • Some DNS servers which support both A & AAAA (IPv4 & IPv6) records still do not respond to IPv6 queries
  • IPv6 introduces larger MTU (1280 bytes), but a different fragmentation model

• Is it ready for KSK Rollover, or not?
  • Not all resolver is compliant to RFC5011
  • Larger packets will introduce risks during ksk/zsk rollover

• And, Renumbering issue

https://github.com/BII-Lab/Yeti-Project/blob/master/doc/Yeti_PS.md
Hypothesis & Experiments expected on Yeti

- IPv6-only operation
- DNSSEC Key rollover and even algorithm rollover
- Renumbering with larger frequency
- Adding more than 13 root servers (How about 25 or more?)
- Multiple zone file signers
- Multiple zone file editors (some kind of Shared zone control)

“a good design could allow a political process of deciding how control for a particular zone should be shared to start” --- ICANN ITI technical report
Architecture Design for Yeti

**Current Model:**
- IANA
- NTIA
- DM
- Verisign

- Unique IANA name space and KSK
- Vetting the root zone changes
- Sign and distribute the root zone file

**Yeti Model:**
- IANA
- DM coordination protocol
- DM
- DM
- DM

- Unique IANA name space and KSK
- Sign and distribute the root zone file

DM: distribution master

Group A of root server

Group B of root server
Three DMs setup and coordination

Timing setting

<table>
<thead>
<tr>
<th>DM</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>BII</td>
<td>hour + 00</td>
</tr>
<tr>
<td>WIDE</td>
<td>hour + 20</td>
</tr>
<tr>
<td>TISF</td>
<td>hour + 40</td>
</tr>
</tbody>
</table>

Synchronizing

- WIDE DM REOP
- TISF DM REPO
- BII DM REPO

Time of Fetching the zone

- KSK, ZSK, server list, IANA serial number

https://github.com/BII-Lab/Yeti-Project/blob/master/doc/Yeti-DM-Setup.md
https://github.com/BII-Lab/Yeti-Project/blob/master/doc/Yeti-DM-Sync.md
Yeit Root server

- Machine, OS system, DNS software

Virtual Machine: 3
Physical Machine: 11

OS:
- NetBSD: 6
- FreeBSD: 5
- Linux: 1

Software:
- BIND: 4
- Knot: 2
- NSD: 8

Version:
- Bind9.10.3, BIND 9.10.2, BIND 9.9.7-P2, BIND9.9.8
- NSD 4.1.5, NSD 4.1.0
- Knot 2.0.1, Knot 2.1.0
Resolvers

From Oct 01, 2015, 00:00:00 To Oct 30, 2015, 03:13:07 UTC

Mean Query Rate (q/s)

- REFUSED
- NOTIMPL
- NXDOMAIN
- SERVFAIL
- FORMERR
- NOERROR
Experimental traffic
Resolvers and experimental traffic
Experiment in BUPT

- Test the feasibility of Yeti concept in campus network with over 10,000 IPv6 active users
- Accessibility of one Yeti DNS root server from BUPT
- Setup a dual stack Recursive-DNS and DHCPv6 server in WiFi network of BUPT Building-3
- Setup IPv6-Yeti-test as one WiFi SSID
- Distribute R-DNS to IPv6 users via DHCPv6 server
- Encourage student to try
- Collect access information for further analysis

System Ready for Yeti Experiment
Yeti R-DNS Traffic Analysis

Peak: 205 qps
Major Qtype: AAAA, A

AAAA query: 37%
A query: 58%
Other Qtype: 5%
Data collection and monitoring

• DSC page in Yeti website:  http://yeti-dns.org/statistics.html
• Health monitoring page:  http://yeti-dns.org/yeti_server_status.txt
• Yeti debug page:  http://yeti-dns.org/resource/yeti-bug.txt
Findings & bugs

- **Root Glue issues (Resolved!)**
  - Current root servers answer for the `root-servers.net` zone, but Yeti root server does not (independent domain). Without this setup, BIND 9 does not include glue in answers to priming queries.
  - Resolved! With a patch for BIND9

- **Related issues**
  - .arpa. zone issue
  - Unused Glue issue
Findings & bugs

- A Bug in Knot 2.0 *(Resolved!)*
  - Knot 2 compress even the root. It is useless since it is a zero-length label, only one byte. Knot 1.6 used for K-root do not do that

- DNSCAP issues
  - Current DNSCAP(both DNS-OARC and Verisign versions ) was observed losing some packet which is not ideal
Findings & bugs

• Failure on Root server zone transfer
  • Some authoritative server on some VPS failed to pull the zone from Distribution Master
  • One fact : TCP fails to respect IPV6_USE_MIN_MTU (draft-andrews-tcp-and-ipv6-use-minmtu-04)
  • Another fact : there are bugs in Virtual machine software failing to receive IPv6 fragments (One Example: FreeBSD on VMware ESXI 5.5)

• Recommendation:
  • 1) Change the IPV6_USE_MIN_MTU setting on server side to 1500 (DM in Yeti case)
  • 2) Or set TCP MSS to 1280 on client side (Root server in Yeti case)
In conclusion

- All most finish the engineering part of Yeti testbed
- Three DMs are running, more than 13 root servers are running
- Lack of traffic, resolvers, and end-to-end measurement
- Experiments agenda expected
Thank you! Any Questions?

More information on website:

http://yeti-dns.org/
https://github.com/BII-Lab/Yeti-Project
http://lists.yeti-dns.org/mailman/listinfo/discuss