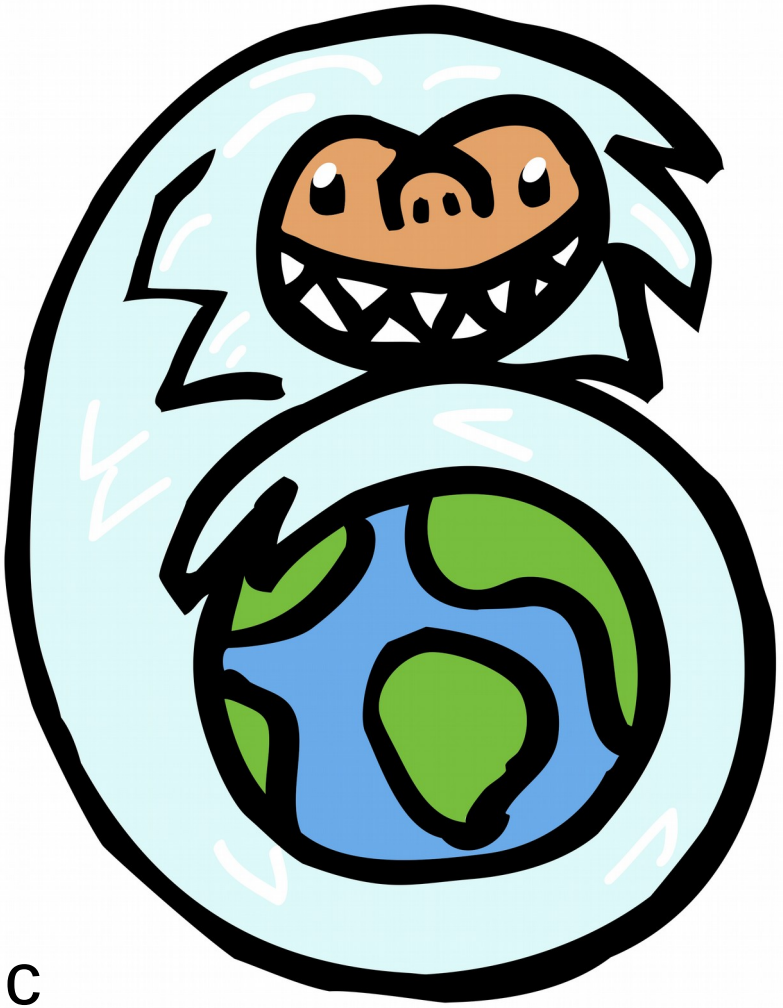
Yeti DNS

IEPG July 2015

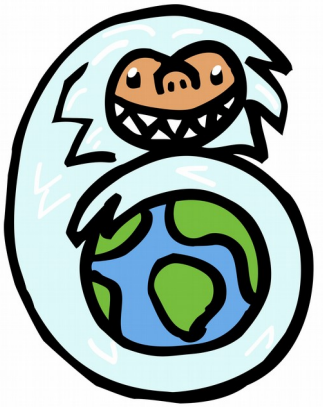


Shane Kerr / BII Lab

2015-07-19 / Prague, Czech Republic

BII 天地互连

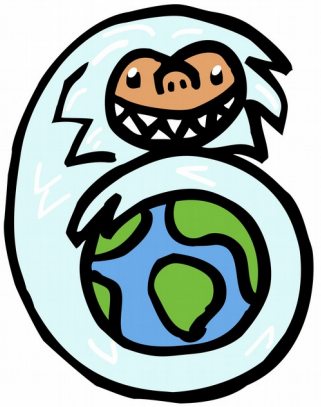
Goals



1. We want more Yeti participants!
2. We want people who can not or will not participate to know about the project.

Bii 天地互连

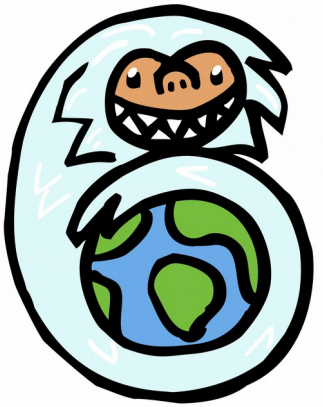
Origin Story



Once upon a time at WIDE Camp,
Davey Song and Paul Vixie were wondering if there was a way to research the DNS root server system without process or political issues.

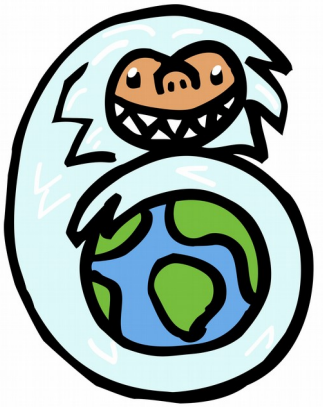
”If only there was a way to look at technical questions in a scientific way... a way to strictly research... if only...”

DNS Root Server System



- There are 13 root servers
  - 12 operators, more than 450 sites
  - *Possibly* the very best possible configuration
  - Let's test it!
- Stability needs make it hard to test new ideas
  - Lab experiments cannot match the real-world, diverse user environments

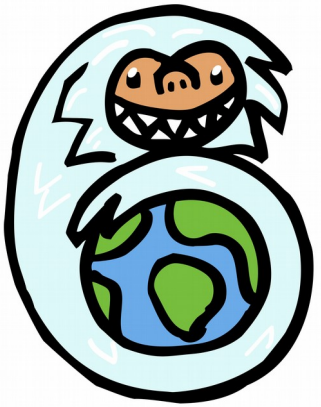
What is the Yeti DNS Project?



- Large-scale testbed
- Parallel root server system
- Yeti Participants:
  - Operators of Yeti components, or experimenters
  - DNS experts, with varied backgrounds and interests

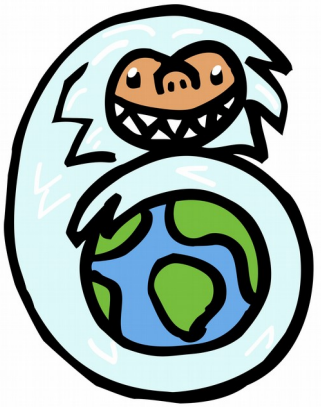
Bii 天地互连

Yeti Components (1 of 2)



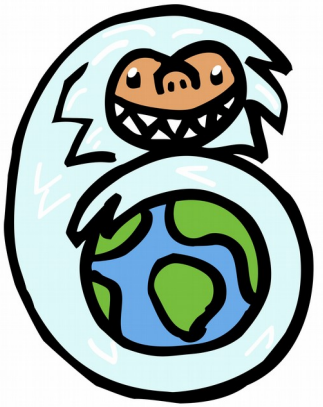
- Yeti Distribution Masters (DM)
  - Start with IANA root (via AXFR)
  - Change IANA root servers to Yeti root servers
  - Sign using Yeti KSK
- Yeti root servers
  - AXFR Yeti root from Yeti DM
  - Serve as DNS root servers
  - Capture traffic information

Yeti Components (2 of 2)



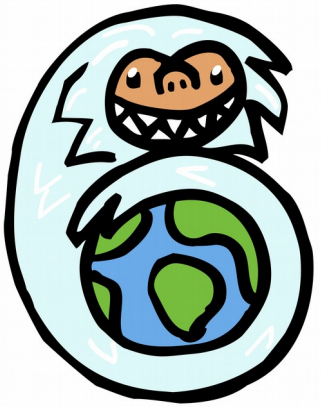
- Yeti resolvers
  - Use Yeti root servers
  - May capture traffic information
- IPv6-only FTW ;)

Things That Yeti is Not...



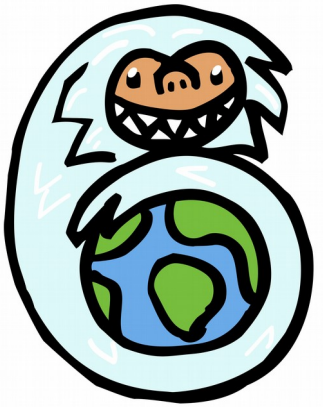
- ***NOT*** research into alternatives to the IANA root
- ***NOT*** interested in policy or political work
  - Although such work may eventually result from Yeti findings

Planned Experiments & Other Investigations



- Impacts of IPv6-only DNS
  - Bigger minimum packet size, no IP-fragmentation
- Changes in DNSSEC
  - KSK rollover, KSK/ZSK rollover frequency, algorithm, signature size
- Changes to root servers
  - Lots/few of root servers, churn in root server set

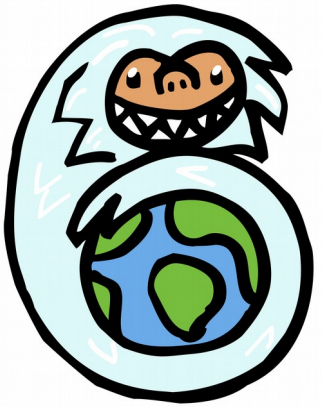
Current Status



- System functioning
- Infrastructure up
  - Web site, http://yeti-dns.org
  - Mailing lists, DSC, RT ticketing, ...
- Docs & scripts in GitHub (IPv4 only!)
  - https://github.com/BII-Lab/Yeti-Project
- Currently gathering Yeti root operators
  - 9 up, more pending

Bii 天地互连

Some Findings So Far…
Glue



- Priming queries made from resolvers

  `$ dig +norecurse -t ns . @some-root`

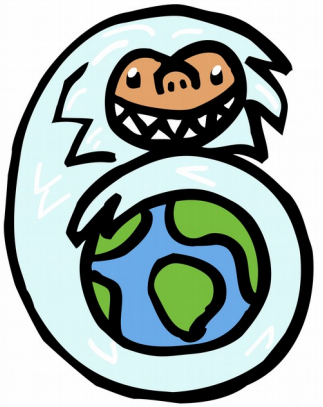
- Current root servers answer for the **`root-servers.net`** zone
- Without this setup, BIND 9 does not include glue in answers to priming queries
- NSD works as desired; patch for BIND 9 developed

Some Findings So Far… dnscap

- dnscap saves packet captures (like tcpdump)
- DNS sends *messages*, not *packets*
  - IPv4 fragmentation, TCP
- Currently able to run dnscap since it captures a super-set of desired packets
  - Not ideal, possibly switch to dnstap later

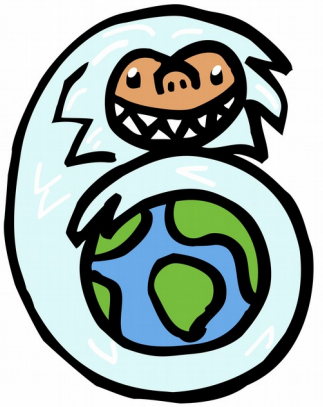
- Currently investigating dnscap packet loss

Probl^H^H^H^H^HChallenges



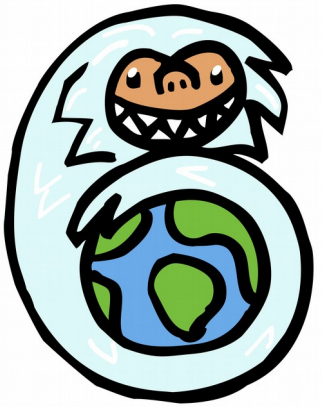
- KSK roll
  - Not really planned or organized
  - RFC 5011 issue
    - BIND 9 worked, Unbound not
    - Difference in hold-down timer?
  - Will Do It Right
- Generating different root with same serial
  - Need to only generate on serial increase

Probl^H^H^H^H^HChallenges



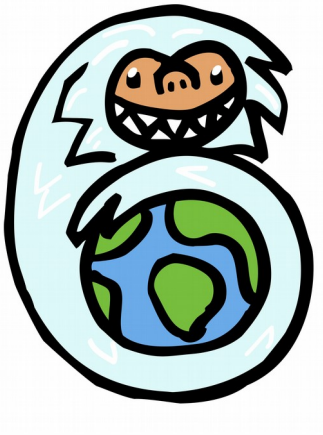
- Authoritative for ARPA
  - DM currently generates root zone with broken ARPA non-delegation (oops)
- Reliability issues with packet captures
  - Improving setup, adding redundancy
- Monitoring
  - Minimal, working to make systematic

Next Steps



- Get ”enough” Yeti root servers
- Fill gaps, fix issues in process & infrastructure
  - Document results in informational RFC?
- Get more resolvers
- Run some experiments!

Yeti Coordinators



BII Group — the parent company of BII (Beijing Internet Institute), a public interest company serving as BII's Engineering Research Center.

WIDE — Widely Integrated Distributed Environment.

TISF — a collaborative engineering and security project by Paul Vixie.