Yeti: First Experiments

Yeti Workshop

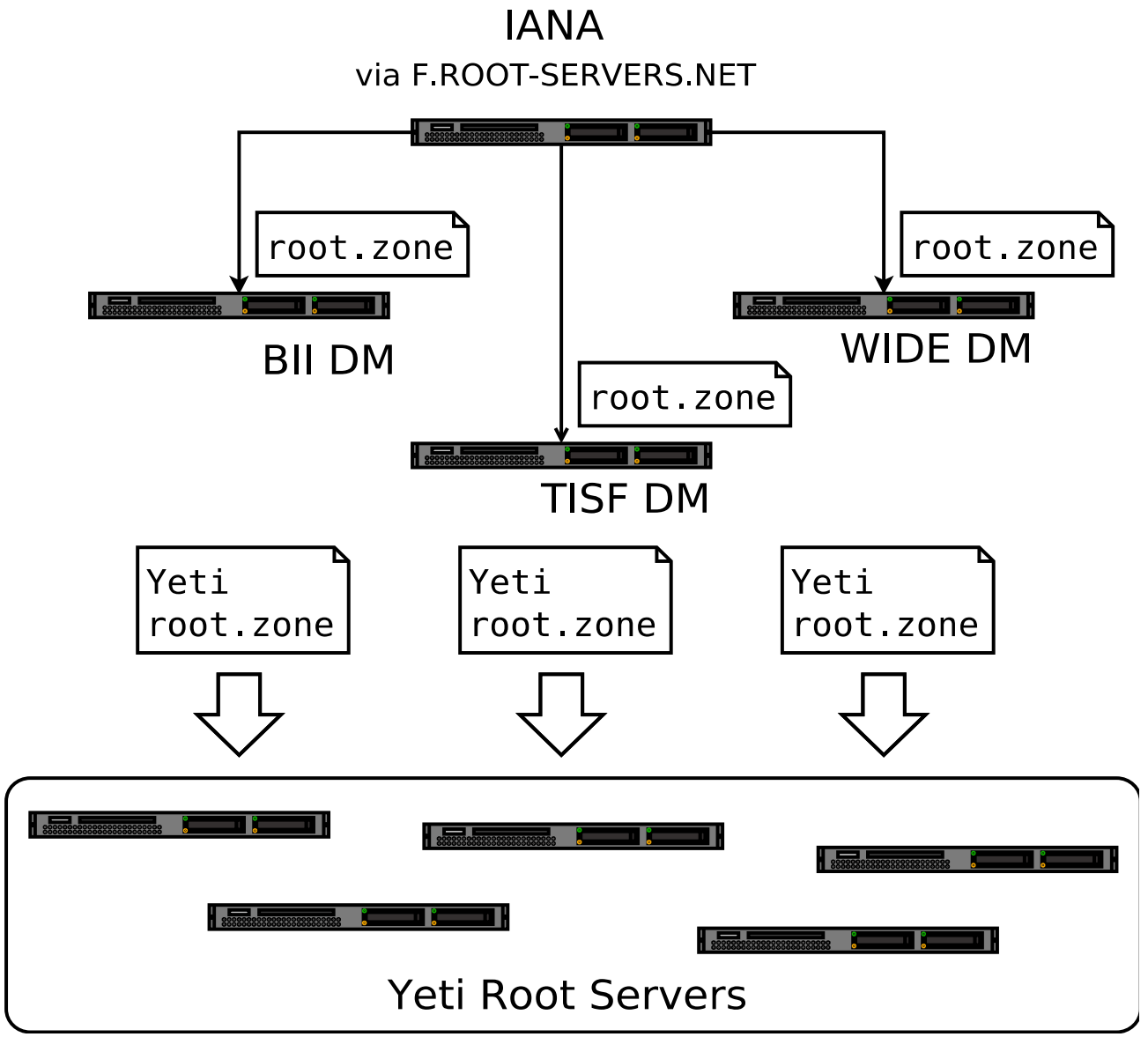
Shane Kerr / BII Lab
2015-10-31 / Yokohama, Japan

BII 天地互连

Yeti Experiment Protocol

1. Proposal
2. Lab Test
3. Yeti Test
4. Report of Findings

https://github.com/BII-Lab/.../doc/Experiment-Protocol.md



https://github.com/BII-Lab/Yeti-Project/.../doc/Yeti-DM-Setup.md

Bii 天地互连

Yeti DM Synchronization

Git synchronized directory:

```
yeti-root-servers.yaml
iana-start-serial.txt
yeti-root-ksk.key
yeti-root-ksk.private
yeti-root-zsk.key
yeti-root-zsk.private
```

YAML has server name, IP, NOTIFY and XFR addresses.

https://github.com/BII-Lab/Yeti-Project/.../doc/Yeti-DM-Sync.md

Yeti Zone Generation

1. The SOA is updated:
   - The MNAME and RNAME are set to Yeti values
2. The IANA DNSSEC information is removed:
   - The DNSKEY records
   - The RRSIG and NSEC records
3. The IANA root server records are removed:
   - The NS records for [A-M].ROOT-SERVERS.NET
4. The Yeti DNSSEC information is added:
   - The DNSKEY records
5. The Yeti root server records are added:
   - The NS records
   - The AAAA glue records
6. The Yeti root zone is (re-)signed

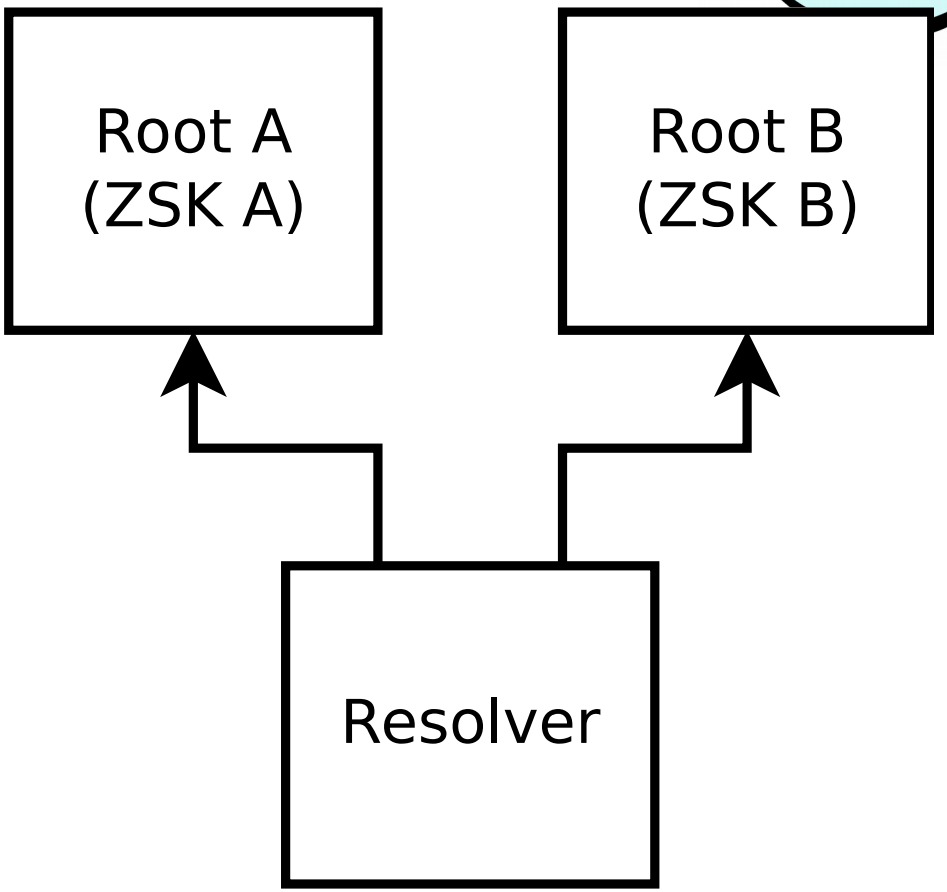
https://github.com/BII-Lab/Yeti-Project/.../doc/Yeti-DM-Setup.md

Multi-ZSK: Motivation

- Currently one KSK, one ZSK
- KSK and ZSK shared by all 3 DM
- Increases required shared secrets
  - No split like IANA/Verisign roles
- Separate ZSK increases DM independence

Multi-ZSK: Lab Test

- Single KSK
- Root A & B have separate ZSK
- Resolver uses hints file with only Root A & B
- BIND 9 and Unbound resolvers



Multi-ZSK: Experiment

- Turn off Root B
- Let Resolver perform priming queries
- Query signed TLD
  - This should validate
- Turn off Root A, turn on Root B
- Query another signed TLD
  - This should validate

Multi-ZSK: Test Cases

1. Two ZSK, not shared
2. Two ZSK, shared by both servers
3. Root A rolls to new ZSK using pre-publish
4. Root A rolls to new ZSK using double signature rollover

Multi-ZSK: Results

1. Two ZSK, not shared
   - SERVFAIL
2. Two ZSK, shared by both servers
   - NOERROR
3. Root A rolls to new ZSK using pre-publish
   - NOERROR
4. Root A rolls to new ZSK using double signature rollover
   - NOERROR

Multi-ZSK: Example Response

```
; <<>> DiG 9.10.2-P3 <<>> @240c:f:1:122::99 . dnskey +dnssec +multi
   ...
;; ANSWER SECTION:
.                       86395 IN DNSKEY 256 3 5 (
                              AwEAActs8YXonx5o6KavhZGh9nWkhcKMDacREsMkNxLP
                              W6jSkntGYWDMOwdMXLStiukjWhkcvyxbnI8o0qa050xC
                              GzVHnFzcJc5+mHtfa0+ZMfZxmeeun2mMl7iz3RySnAZI
                              bzfdupJAQ2wKmiw2pvqb3fmusovUfpMDmkbYBArWZyhv
                              ) ; ZSK; alg = RSASHA1; key id = 50688
.                       86395 IN DNSKEY 256 3 8 (
                              AwEAAcAqV/Sd04tnuDt/BK1sbk6adEiK04Wcc/D+/zG2
  ...
;; MSG SIZE  rcvd: 1030
```

Multi-ZSK: Next Steps

- Impact analysis (review of packet sizes)
- Yeti experiment!

KSK Roll: ICANN Plan

- ICANN has a design team
- Returned feedback
- Initial plan – novel characteristics
  - Strict adherence to timing in DPS
  - Fear of large packets
- Was high priority for Yeti
  - Now uncertain; waiting for design team output

KSK Roll: Double-DS

- Currently no KSK roll for Yeti
- First attempt failed
  - RFC 5011 holddown timer not respected
  - BIND 9 worked fine, in violation of RFC!
- Next attempt: run as experiment
- Related proposal: Un-DPS for Yeti?

Related: Hint Management

- New IANA root addresses?
  - One possible alternative to KSK roll
- Research on old-J root
  - Still receiving queries after 10 years
- Automate hints.txt updates?
  - Simple script
  - Include with software & distributions?

Related: Fragmentation

- Failed fragmentation very expensive
  - Timeout and retries for EDNS size probing
- Mukund Sivaraman's idea
  - DNS application-level fragmentation
  - Proof-of-concept proxy implementation
  - draft-muks-dns-message-fragments-00
  - Proxy already deployed alongside BII Yeti root
- DNS over DTLS has separate proposal

BII 天地互连