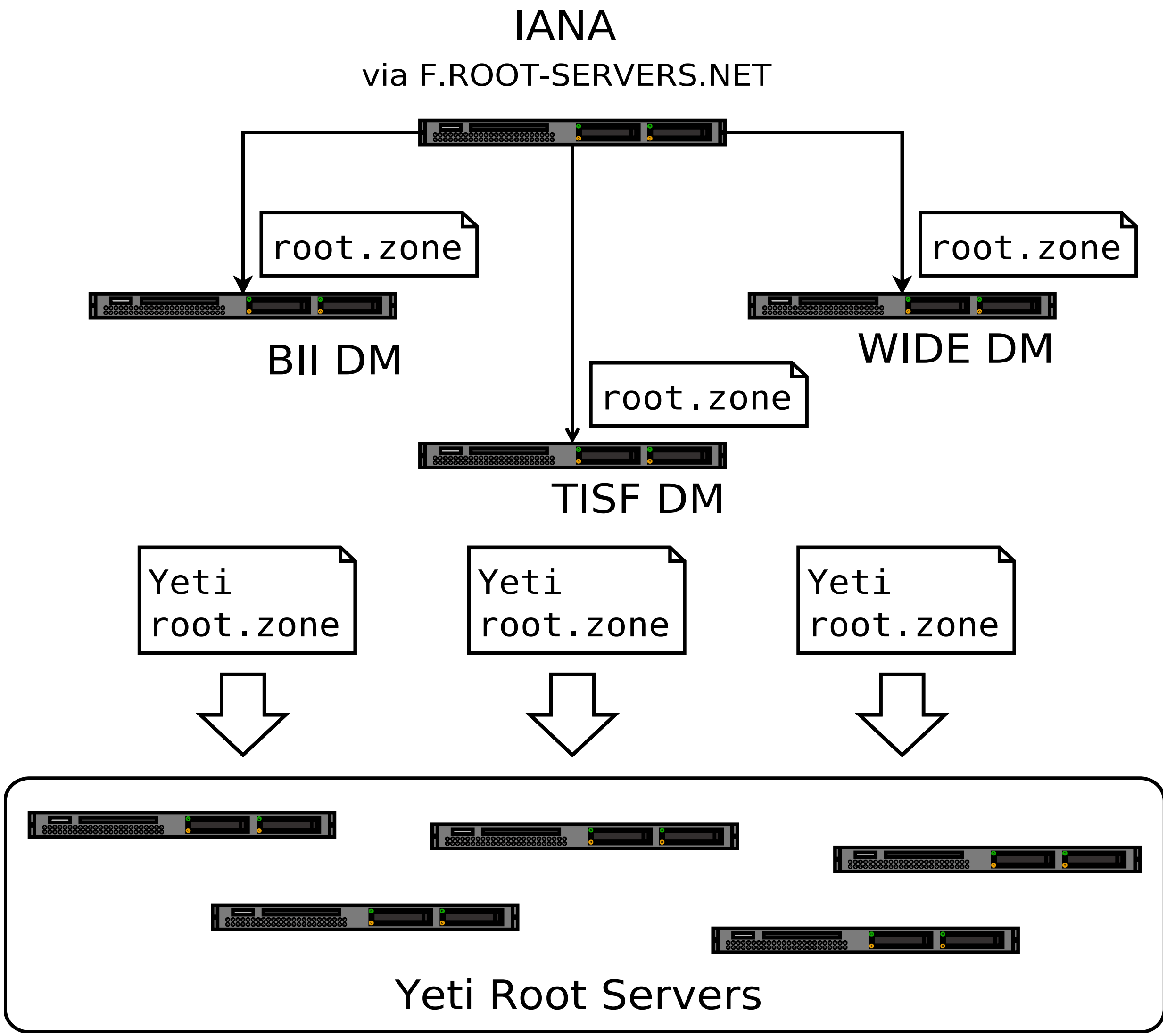
Yeti MZSK Experiment Status

Shane Kerr / BII Labs
2016-03-24 / Yeti Virtual Meeting

Bii
天地互连

Yeti Signing: “Classic”



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

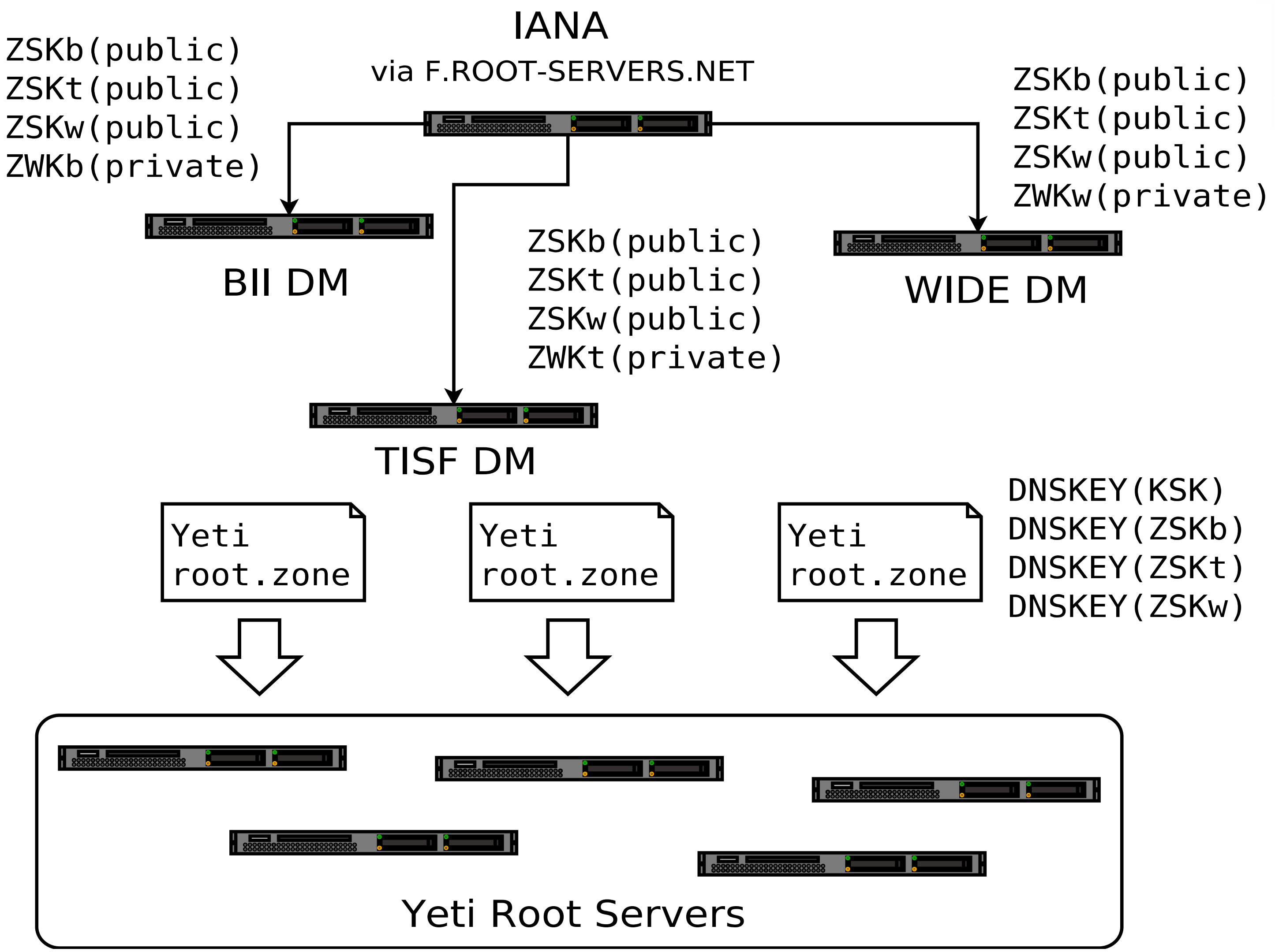
Bii 天地互连

Yeti Signing: Multi-ZSK

- Simple: A separate ZSK for each DM
- Proposed by Davey on mailing list
- Experiment detailed in GitHub

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

Yeti Signing: Multi-ZSK



IANA
via F.ROOT-SERVERS.NET

ZSKb(public)
ZSKt(public)
ZSKw(public)
ZWKb(private)

BII DM

ZSKb(public)
ZSKt(public)
ZSKw(public)
ZWKt(private)

TISF DM

ZSKb(public)
ZSKt(public)
ZSKw(public)
ZWKw(private)

WIDE DM

Yeti
root.zone

Yeti
root.zone

Yeti
root.zone

DNSKEY(KSK)
DNSKEY(ZSKb)
DNSKEY(ZSKt)
DNSKEY(ZSKw)

Yeti Root Servers

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

RIPE Atlas Measurements

- 1 “good” probe in each country w/ Yeti server

-
  ```
  dig . -6 -t dnskey \
      +dnssec +nsid +bufsize=4096
  ```
- Query every 240 seconds
  - Had to create a new set during 1st week because I forgot the “DO” bit in my creation script. :(

https://atlas.ripe.net/measurements/?search=mzsk

Validation Verification

- BII runs two resolvers (Unbound, BIND)
- Send queries to DM & Yeti root servers
  1. Start `tcpdump`
  2. `dig` for SOA, NS, DNSKEY with +dnssec
     - Log output
  3. Check errcode, AD flag, packet size
  4. Flush caches & repeat
- Also check BII corporate resolvers :)

MZSK Phases

- Proposal (done!)
- Lab test (done!)
- Yeti test phase 1 (done!)
- Yeti test phase 2 (in progress)
- Report (pending)

MZSK Phase 1

- Verify the DNS works properly
- Worst-case test of packet size
  - 1 KSK
  - 3 ZSK... all rolling
  - 7 DNSKEY records
- All generated by BII for simplicity

MZSK Phase 2

- Actually generate separate ZSK
- Modify git repository to share ZSK
- Update DM scripts to use new layout
  - All separate implementations
- Use schedule to stagger rolls
  - 3x 4-day = 12 days to roll

Observations

- Extra RRSIG at one DM (fixed)
- UDP broke on one Yeti server (fixed)
- Separate ZSK causes IXFR to fail
  - General problem with DNS... use AXFR
- Co-ordinating DM is tricky

Status

- Waiting on last ZSK
- Should we wait for another ZSK roll?
- KSK still shared
  - Ceremonies needed to finish split
- Fix IXFR to support our use case?
  - General problem with redundant signers
  - There are other issues with AXFR & IXFR...