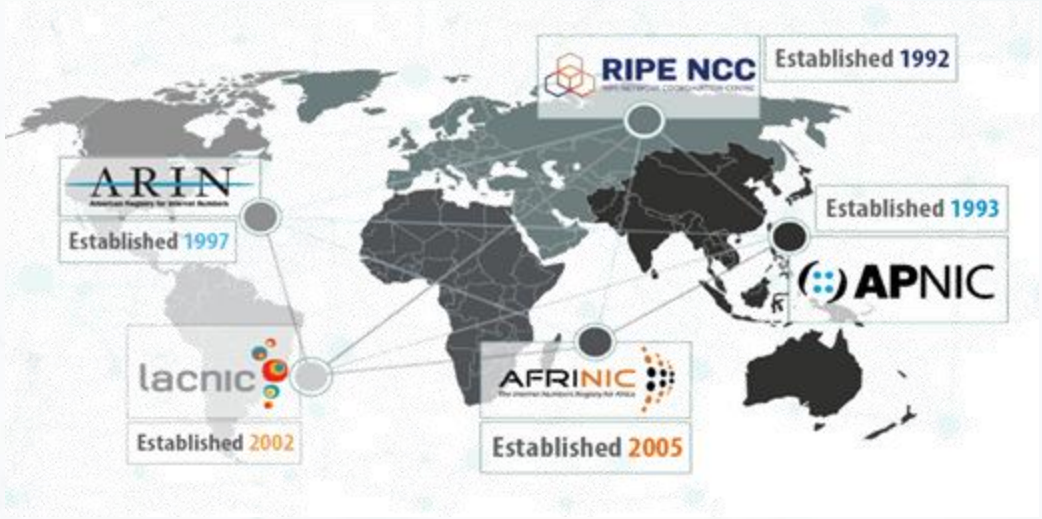
DNS Services at ARIN

David Jeffers

Who am I?

- Senior Site Reliability Engineer
- Started January 2015
- DNS and database operations
- Occasional NANOG attendee
- DNS-OARC lurker

What is ARIN?



Regional Internet Registry (RIR) that administers Internet number resources for North America

- IP Addresses (IPv4 and IPv6)
- Autonomous System Numbers (ASNs)

Provides services supporting the Internet community

- Routing security (RPKI/IRR)
- Directory services (RDAP/Whois)
- Community outreach/participation
- DNS (Reverse DNS, DNSSEC, and more)

DNS Services

Reverse DNS

- $zone.in-addr.arpa
- $zone.ip6.arpa

Corporate DNS

- arin.net
- Reverse DNS
  - 136.136.192.in-addr.arpa
  - 4.0.0.0.0.0.5.0.1.0.0.2.ip6.arpa
- Internal and external views

Secondary DNS

- Other RIRs
  - as3333.net
  - 0.c.2.ip6.arpa
  - lacnic.net
  - 1.in-addr.arpa
- nro.net
- aso.icann.org
- a.in-addr-servers.arpa
  - in-addr-servers.arpa
  - ip6-servers.arpa

Reverse DNS

"Zonegen"

DNSSEC Signing

Hidden distribution master

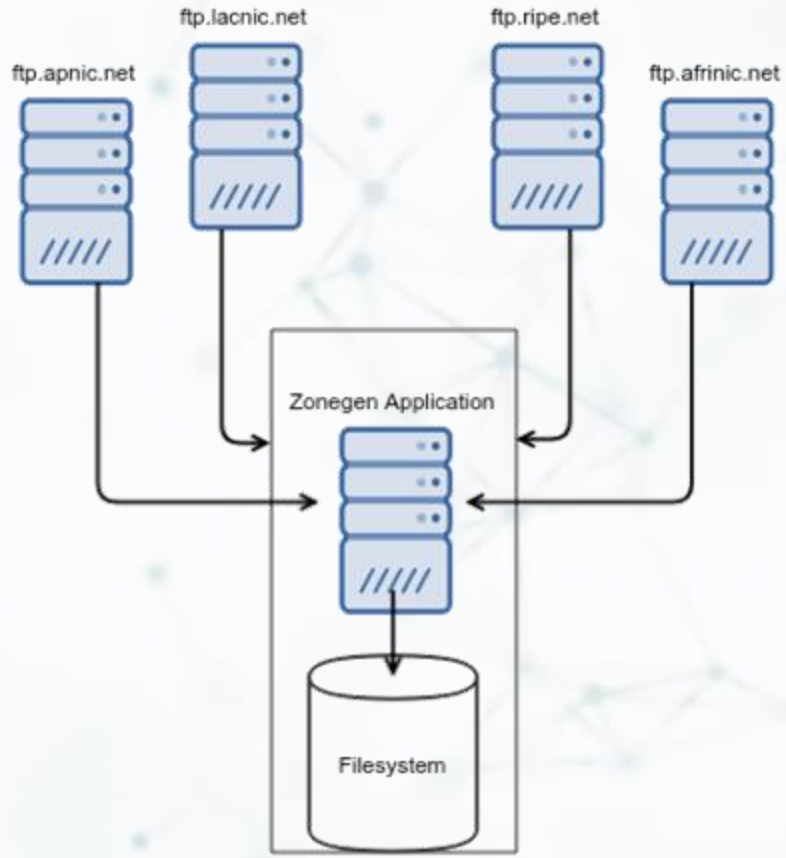
Public Facing Services (PFS) sites, anycast nameservers (r.arin.net) & FTP (ftp.arin.net)

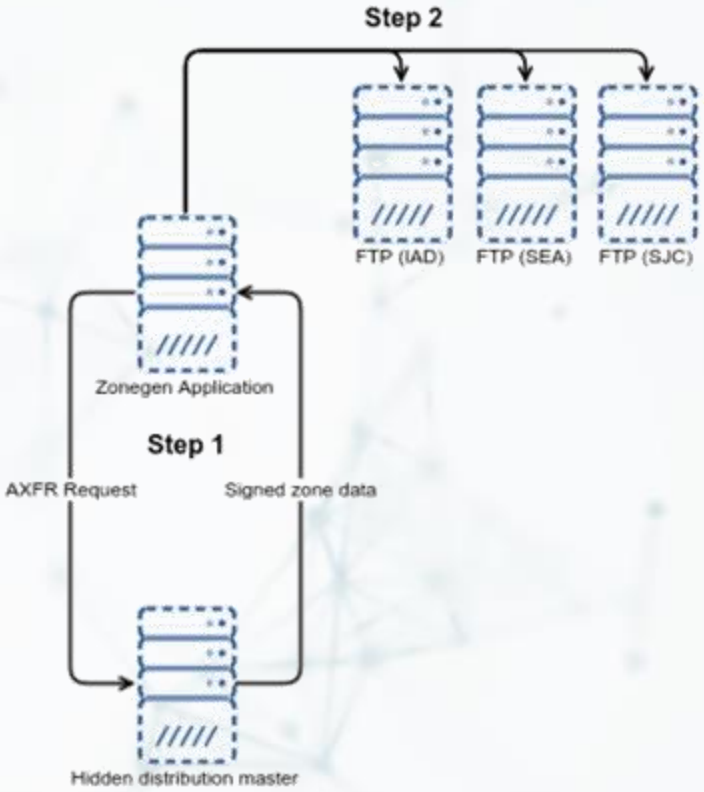
Secondary DNS providers

Reverse DNS - Zonegen

Gathers customer DNS data (nameservers, DS records) from the provisioning database

Gathers zonelets via public FTP from the other RIRs





https://ftp.ripe.net/ripe/reverse/zones/inter-rir-zonelet-exchange-1.0.txt

Reverse DNS

DNSSEC Signing

- Bump-in-the-wire signing
- Hardware appliance made by Secure64 DNS Signer
- Zone-signing key pairs are rolled monthly
- Key-signing key pairs are rolled annually

Corporate DNS

- Provisioned via version control (Git)
- Externally available zones follow similar path
  - DNSSEC-signed
  - Hidden distribution master
  - PFS sites and secondary DNS providers

Secondary DNS

- Standard primary/secondary syncing mechanisms
  - Notifies
  - Incremental zone transfers/authoritative zone transfers

DNSSEC – Past, Present, and Future

DNSSEC – Distant Past

Trust anchors were initially published on arin.net

arpa, in-addr.arpa, and ip6.arpa were subsequently signed

27 April 2011: ARIN placed DS records into in-addr.arpa and ip6.arpa [1]

Key signing keys were rolled [1]

[1] https://www.arin.net/vault/announcements/20110428/

DNSSEC - Past

- Initially ran BIND
- Moved to Secure64 to ease operational concerns
- Keys imported to Secure64
  - Keys were the same as what was listed on the trust anchor
  - Secure64 wrote custom code to import our keys

DNSSEC - Past

Worked with IANA to create Delegation automation for in-addr.arpa zones (NS and DS resource records) – a RESTful endpoint.

- We wrote a Bash script leveraging the RESTful endpoint (described in RFC 7745) [1]
- KSK rolls generated a lot of toil since it was very manual

[1] https://datatracker.ietf.org/doc/html/rfc7745

DNSSEC - Past

- DS and NS record updates with our registrar (GKG) were manual
- DS and NS record updates with our own registry done through ARIN Online interface

DNSSEC - Past

- Secure64 DNS Signer maintenance lagged
  - Manual operations for adding users, retrieving DS records, etc.
  - Custom code meant updates caused delay in new OS rollouts
- Initially set to Algorithm 5 - RSA/SHA-1
- Two published digests

DNSSEC - Present

- DS and NS records updates are done via Ansible playbooks
  - Key rolls went from weeks to hours; safety timeframe calculated by the time to live
  - ARIN Online RegRWS API used for corporate reverse updates
  - GKG API for corporate forward updates
  - IANA RESTful updates for reverse DNS
- DNS Signer interactions are mostly done through Ansible playbooks
  - User management, reports, configuration updates
  - Key signing key algorithm rolls
- Algorithm 8 - RSA/SHA-256 [1]
- Only one published digest [1]

[1] https://datatracker.ietf.org/doc/html/rfc8624

DNSSEC - Future

- Human-less key signing key rolls
- Hardware updates, network hardware security modules
- Algorithm 13 and beyond
  - Particularly for in-addr.arpa and ip6.arpa

DNS Application Management – Past, Present, and Future

DNS App Management- Past

BIND 9

- Configuration updates made by hand, backported to version control
- Custom rolled RPMs
- Some heterogeneity through multiple operating systems

"Zonegen"

- RPM installations
- Ceremonious weekend configuration changes and upgrades

DNS servers were Unicast

DNS App Management – Present

BIND 9

- Entirely handled in configuration management
- Containerized

"Zonegen"

- Containerized
- Configuration changes and upgrades happen during the workday
- Customer record updates pushed to PFS every 4 hours

Even geographic distribution

Stage and QA environments

DNS servers are Anycast

DNS App Management – Future

- Container orchestration (Kubernetes)
- Better analytics
- More frequent changes for zones we manage
  - Currently four hours
  - Reduce it to a smaller increment (yet to be determined)

ANY QUESTIONS ?

Thank You