ISC, F-Root, BIND & DHCP Updates

AFRINIC-21

Eddy Winstead
Agenda

• ISC overview
• F-Root in Africa
• ISC Open Source
  – BIND roadmap update
  – DHCP update
  – How to get involved in the projects
• ISC certification program
ISC Overview

- Founded in 1994
- Non-profit, self-funding
- 36 Employees
  - 1/3 sales, marketing, technical support
  - 1/3 software development
  - 1/3 network and business operations
- Based in Redwood City, CA with employees and network nodes all over the world
ISC Project Focus

Open Source Software
- BIND DNS Server
- ISC DHCP server, relay, client
- Kea DHCP (new)
- BIND DNS and DHCP training and certification

Network Services
- F-Root: Critical Internet Infrastructure
- Secondary Name services (DNS anycast) for non-profits
- Project hosting (FreeBSD, NTP, etc)

© 2013 www.isc.org
2013 Financials posted

ISC 2013 Revenue

- BIND Sub/Support: 45%
- Hosted @/ISP: 14%
- SIE/Security: 12%
- DHCP Sub/Support: 11%
- SNS: 3%
- Training: 3%
- Other: 2%
- Sponsored Research: 6%
- F-Root: 4%

ISC 2013 Expenses

- Personnel Costs: 77%
- Depreciation: 9%
- Facilities: 4%
- Travel: 2%
- Other: 2%
- Bandwidth: 6%

We have adequate stable funding now, based almost entirely on support subscriptions.
Agenda

• ISC overview
• F-Root in Africa
• ISC Open Source
  – BIND roadmap update
  – DHCP update
• ISC certification program
ISC has operated F-root since 1994
F-root is one of 13 root servers
There are 55 local F-root nodes worldwide
The number of nodes fluctuates, as sometimes the hardware becomes obsolete and is not refreshed, or carriers or hosts move or are acquired
F-Root in Africa Today

- Lagos, Nigeria (IPv4)
- Nairobi, Kenya (IPv4)
- Dar Es Salaam, Tanzania (IPv4 & IPv6)
- Johannesburg, South Africa (IPv4 & IPv6)
- Cairo, Egypt (IPv4)
- New sites?!
Comparative DNS Root RTT

The map below shows a comparison of response times for DNS SOA queries to all the root DNS servers.

For each probe, a marker shows the "best" root server with colours identifying the related minimum response time. Clicking on a probe reveals all the measurements to reachable root servers, ordered by response time. It is possible to filter by protocol (IPv4, IPv6, or both).

We display measurement results only from the last hour.

Address Family: All

Filter by ASN, prefix, or country:

https://atlas.ripe.net/results/maps/comparative-dns-root-rtt/
Root Access in Mauritius

© 2013 www.isc.org

https://atlas.ripe.net/results/maps/comparative-dns-root-rtt/
F-Root Nodes

- ISC manages F-Root for the public good, to provide DNS stability, access and good response time to users.
- Nodes are located where there are sponsors who request and can support them.
- Sponsor provides rackspace with good interconnection/peering, power and remote hands, and purchases the equipment. ISC will specify the equipment, install and manage the nodes.
- Nodes are available to anyone who can meet the technical requirements.
Root Node Cost

- Cost of Hardware ($?? - $??)
- Annual Management fee (up to $10K USD)

• Cost depends on node size
• Subsidies are available, through ISC or the AfriNIC root server program

http://www.afrinic.net/en/initiatives/root-server-copy
Node sizes

Traditional Redundant Node

- Router/switch
- DNS server
- Management server

New ‘F-single’ node

- Router/switch
- DNS server
F-Root Nodes

**Traditional Node**
- Redundant platform
- Two router/switches
- Three DNS servers
- Designed for high traffic Internet Exchange Points
- Example: AMS-IX, LINX

**New ‘F-single’ Node**
- Single-box solution
- Smaller footprint, lower power/AC requirements
- Lower hardware cost
- Suited for smaller IXPs where all peers connect to a shared route server

ISC will decide which platform is appropriate based on site review
Request Information
- ISC sends Sponsorship requirements

Installation
- ISC Engineer for traditional node
- ISC remote engineer + local hands for mini-node

Traditional or F-Single node?
- ISC reviews the site and determines which is appropriate

Sponsor purchases HW
- specified by ISC
- wait for equipment receipt

Sponsorship?
- Determine funding for the node
- Annual operation $10K USD
- Equipment cost

Sign MoU

6 – 24 months
Agenda

• ISC overview
• F-Root in Africa
• ISC Open Source
  – BIND roadmap update
  – DHCP update
  – How to get involved in the projects
• ISC certification program
2014 Development Initiatives

• Refocusing on BIND9
  • Released BIND 9.10.0, 9.10.1
  • DDOS mitigation, simulation test bed
  • Fuzz testing (Codenomicon CROSS)
    – Improving automated test coverage
    – Creating new DNSSEC documentation

• Writing NEW DHCP server for 2015 release kea.isc.org

• Open source contributors, OS packagers source.isc.org

• Re-hosted DLV site, upgrading bug db
BIND 9.10 – April, 2014

- RRL is now on by default
- MAP zone file format
- DNS Pre-fetch (Hammer time)
- Zones shared between views
- New stats, new style sheet
- Delv – DNSSEC troubleshooting
- Native PKCS#11
- DNS Cookies (experimental)

22,825 copies downloaded since 2/25/14

Considered experimental until at least 9.10.3
ISC F-Root Before and After RRL

![Graph showing f-ams1 traffic with RRL implementation and attackers giving up in frustration.](image-url)

- **max input**: 11.48Mb
- **avg input**: 4.43Mb
- **max output**: 11.48Mb
- **avg output**: 0b
- **IN**
  - Max(Max) = 11.48Mb
  - Avg(Max) = 4.43Mb
  - Max(Avg) = 11.48Mb
  - Cur(Avg) = 0b
- **OUT**
  - Max(Max) = 56.53Mb
  - Avg(Max) = 9.21Mb
  - Max(Avg) = 56.53Mb
  - Cur(Avg) = 0b
9.10 Performance

- DNS Pre-fetch – early refresh of cache records due to expire soon
- EDNS(0) processing change to reduce the # of round-trips on slow or lossy connections.
- MAP zone file format – image of zone db that can be loaded directly into memory. Recommended only for slaves.
Native PKCS#11 Benefits

- Fewer software components with native PKCS #11 feature
- Highest security for your keys
  - (HSMs are generally FIPS certified)
- HSM-provided key management
- HSMs are required for some domains
BIND planned features

- Streamlined zone addition
- DNSSEC Key policy manager
- Wire-speed logging with DNStap
- Parent updating (CDNS, CDNSKEY rr)
- On-the-fly IPv6 ptr records
- DNSSEC Negative Trust Anchor
- DDOS mitigations (resolver features)

In Planning & Design phase
Targeted – mid 2015
DHCP Update

ISC DHCP

• 4.3.0 December 2013 provided IPv6 parity
• 4.3.1 released July 2014
• 4.3.2 planned for January 2015
• Release 4.2 will EOL March 2015
• Extended Release 4.1 EOL indefinitely (smaller footprint)

Kea

• New DHCP server
• No client, no relay
• UNIX/BSD only
• Higher performance
• Easily extensible with ‘hooks’ to your own applications
• Release 0.91 planned for March, 2015, with Host reservation, MAC address associated with IPv6
How to get involved

• Use www.isc.org or source.isc.org to pull the latest code
• Report bugs (www.isc.org for more information)
• Follow @ISCdotORG on Twitter
• Look for the new DNSSEC guide in Q1, 2015
• Subscribe (support) ISC’s open source developers
How does one send a DNS query towards a specific DNS server with "dig"?

- **dig -s server -q query**
- On the **dig** command prompt, enter "server <servername>"
- **dig @server request**
- **dig server request**
- **edit "/etc/resolv.conf" and then use "dig query"**
- **dig request @server**
QUESTIONS?
Thank You