Some Opportunities for Sharing

DNS feature evolution and outreach

Abstract

- DNS service operations is increasingly a simple activity, with many tools available. There are also any number of vendors who will be happy to provide the basic service. Most of these services and tools are only capable of providing core or foundation level services. The DNS is evolving to add new functions and capabilities such as IDN, ENUM, and DNS security (DNSSEC). To provide a proper grounding in these issues, ICANN, ISOC, and others are providing DNS technical training. This section will touch on some of these programs.

DISCLAIMER

- DNS training resources cover a wide range of capabilities. Not all offerings are equal.
- Firm grounding in DNS basics is crucial for understanding the impact of new capabilities and vendors abilities to provide them

Attribution

- Ed Lewis
- Johan Ihren
- Olaf Kolkman
- Joe Abley
- John Hu
- David Conrad
- George Sadowsky

- The wwTLD and ccTLD members
- ICANN
- ISOC & the technology workshops
- Shinkuro

History

- Old Interop material - Paul Mockapetris - 1990s
- ISOC developing nations workshops - 1990s
- Apricot & RIPE
  - Changes in the DNS
- ICANN & the TLD constituents
- ISOC re-energized

Changing nature of resource holders

- No longer a technical/engineering community with a strong grounding in the operations
- The desire to track the human element associated with the resources.
- Perceive the DNS as a “harvest-able” resource for unintended / unexpected activities
- Often outsource operations of the publication process to focus on protecting the human/resource database(s).
- Need to be educated on what the DNS is used for and what is possible/expected as new features become available.

Drivers

- Basic DNS operational “best practices” were not well understood. Solved by:
  - Outsourcing DNS operations to third parties
  - Increasing the knowledge base in-house
- DNS capabilities vary based on base-line code.
  - BIND variants have distinct operational behaviours
  - The range of DNS software variants includes more than 140 distinguishable types.

Interoperability

- No rigorous test suite
- Based on core specification, as modified by reference implementation

- server to server
  - axfer
  - query
- resolver
  - UNIX system library

- Specification crosses “layers” and specifies a “Master File Format”
  - Does not translate well into DB based offerings

Early Work

- Dr. Mockapetris DNS tutorials held during the Interop events and later during the combined Networld/Interop conferences reached a larger technical/engineering base. This could be considered part of the initial DNS outreach/training - seeding the first strict operational groups that did not develop DNS code on their own.

ISOC developing nations WS

- training by those taught by Dr. Mockapetris to those in what were called “developing nations” - parts of Asia, Africa, South America, and eastern Europe.
- Talked to basic operational setup, building the application from source, configuration file formats, and options to modify application behaviour.
- initial effort to make material available in multiple languages
- Oriented to BIND 4 and BIND 8 versions
- Due to external events, ISOC ceased regular training events around 1997

Apricot & RIRs

- David Conrad, Pindar Wong, and Bill Manning received permission from ISOC training chair to take the DNS materials, organize them and use this as the basis of a comprehensive, hands-on core DNS workshop to be used in the Apricot conference.
- In roughly the same period, the Ripe community saw the benefit of providing core DNS training to its community.

- These workshops were very successful, with the Apricot workshops participants being asked to help train in future events.

Old things are done away

- The DNS protocol was modified to incorporate several new features:
  - IDN label encodings - although the DNS is 8bit clean, issues with the Master File Format were drivers to create an encoding that used 7bit ASCII to represent encodings aligned on 8bit boundaries. Perhaps this is more properly referred to localization
  - ENUM - with the rise of a converged telephony network that uses IP datagrams for moving voice (VoIP), the design and implementation of a number lookup method which emulates the signaling system was deemed critical … ENUM provides this capability within the construct of the DNS
  - DNS Security - perhaps the most significant changes to the DNS protocol - particularly in the ways in which the operational management of the Master File Format is accomplished.

A few - random considerations

- how will old software react to new record types
- will existing operational practice be adequate for new demands
- user expectations
  - accuracy
  - availability
  - integrity
  - timeliness
- are the old DNS trust/training models adaptable

ICANN and the TLDS

- RSSAC members were asked at the ICANN mtg in Romania to share with the TLD operators their best practices and perform outreach
- The goal seemed to be to provide “uplift” to the TLD constituents - to raise the minimum operational to be in line with the root servers as the DNS operational community prepared to adopt these new features.
- A series of training sessions was outlined, in conjunction with the ICANN meetings - with the objective to reach every TLD operator and provide a venue to explore these new features.

The ICANN trainings

- Nearly every ICANN meeting since Shanghai
- Built on the Apricot DNS training sessions, augmented with specific DNSSEC materials.
- average attendance :: 18 with 3 repeat visitors
  - do the maths…
  - three ICANN meetings per year - about 40 unique TLDs per year - just short of 10 YEARS to reach all TLDs.

- Need more exposure. Can the RIR training teams be persuaded to take on part of this task?

The RIR efforts

- RIPE members requested DNS training - esp.. DNSSEC training
- ARIN has no significant training - due to lack of member demand.
- APNIC had a developing training program - John Hu was willing to take on some DNS and DNSSEC training efforts within the APNIC service region.
- LACNIC has done some work on basic DNS training - more may be forthcoming.

- Over the past 36 months - have reached 80+ TLDS or 27%
  - this is too slow to disseminate the required knowledge
  - including RIRs into the training pool does not look sufficient
  - Are there other methods?

ISOC re-energized

- ISOC was able to redefine itself so it is able to support its core mission as well as re-engage in its legacy role of providing educational outreach.
- ISOC partnered with NSRC and some others in 2003 to collect and maintain an on-going archive of training materials, instructors, and support infrastructure to enable local communities to build a targeted program for their local needs.

- http://ws.nsrc.isoc.org/

- Target is not quite the same as the outreach program undertaken between the some members of the DNSO groups and some members of RSSAC

Other activities

- School of the Internet
  - MODA developing materials - expertise in ENUM
- Crystal Palace Press
  - Blue Ribbon Panel - target is - “The DNS at 50”
- MINC - IDN testbed/training - not much traction in the operational community - “it just works”
- Local/Regional training
  - APNIC
  - JPRS
  - etc.

Edge cases

- Clearer documentation on how data gets “into” the DNS
  - EPP
  - registry/registrar interactions
  - tangential binding to humans … e.g. IRIS/CRISP/WHOIS
- Clearer documentation on how data gets “out of” the DNS
  - Is the existing resolver sufficient?
  - is it properly documented?
  - what else can/should an application be able to learn from the DNS?

- These are areas where training/understanding is sporadic at best.

Has the DNS matured?

- It is likely the DNS will continue to evolve and grow, overcoming some of the initial constraints:
  - Fixed Master File Format
  - Always on/connected networks
  - IPv4 transport restrictions

- and adopt new features
  - (this list is intentially blank)

Ongoing education is needed

- New operators
  - instill core principles
  - expand the human “trust” network
- New features
  - what is required to exploit these new capabilities
  - are there interoperability considerations
- Upgrading legacy systems
  - help weed out older or non-compliant systems

That said, what is a typical session?

- Our target is the TLD or large ISP DNS operator
- Choice of hands on with lab work or lecture only
- one to five day sessions are possible
- working with a local organizer to ensure attendees and equipment/venue logistics are managed

- Some of the materials are available in non-English languages - need to do better.

course outline

- DNS fundamentals
- Where DNS fits
  - registry
  - application
- Configuration
- Error detection and correction
- Tuning
- Advanced features

feedback from students

- lots of interest in understanding basic DNS operations
- grateful for exposure to DNSSEC operational complexities
- exposure to some of the simpler DNSSEC concepts takes time . e.g. TSIG / SIG(0)

- This is going to be hard to integrate into existing operations…

Increasing complexity

- increased trust at what cost?
- MUCH better tools are needed
- continuous training

- slows adoption of new features/capabilities without trained staff

- How to encourage training???

NSRC tools

- content repository
- trainer listings
- course scheduling

- Still needs to have more language specific content available
- is there enough incentive for locally organized training?

Affinity-based training

- APTLD sessions
- CENTR sessions
- RIR specific DNS training
  - RIPE has an aggressive schedule
- ISPs tend to either outsource or get external training
  - AXFR
  - EP.NET
  - Mice & Men
  - InfoBlox
  - et.al.
- Affinity training may be the right approach

Questions?