ccTLD Best Practices & Consideration

Save Vocea
ICANN's regional rep. – Australasia/Pacific
Presentation @ PacNOG 4, Vanuatu
30 June 2008

Overview

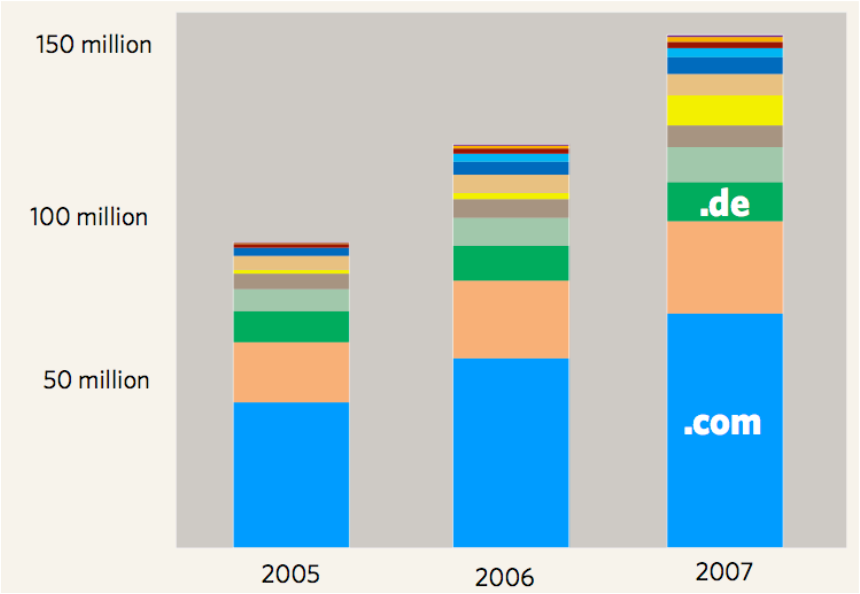
- Introduction to the DNS
- IANA root management
- How a ccTLD can be structured
- Best Current Practices
- Q & A

The Domain Name System is…

- The less technical version:
  - An eco-system for new business accounting for hundreds of millions of $$$ in revenues
  - A venue in which international politics play out
- The technical version:
  - What most Internet users use directly to reference anything on the Internet
  - A lookup mechanism for translating one protocol objects into another
    - Not just names to addresses
      - E.g., a name into a load balanced pointer to a service, an IP address into a name, a name into a X.509 cert, etc

DNS in business

- Since the commercial-ization of the DNS began around 1996, a new industry has been created (“domaining”)
  - New business opportunities and opportunities for value added services
  - Fraud, trademark infringement, “typo-squatting”, etc.



DNS in politics

- Domain names are seen as presence on the Internet
  - In some cases, that presence isn't wanted, e.g.:
    - Territorial disputes
      - E.g., delegation of .tp, discussions of the creation of .quebec
    - "Free speech" arguments
      - E.g., "walmartsucks.com", "freetibet.info", etc.
- USG role in "authorizing" root zone changes
- Creation of new top-level domains
  - E.g., .XXX
- Etc.

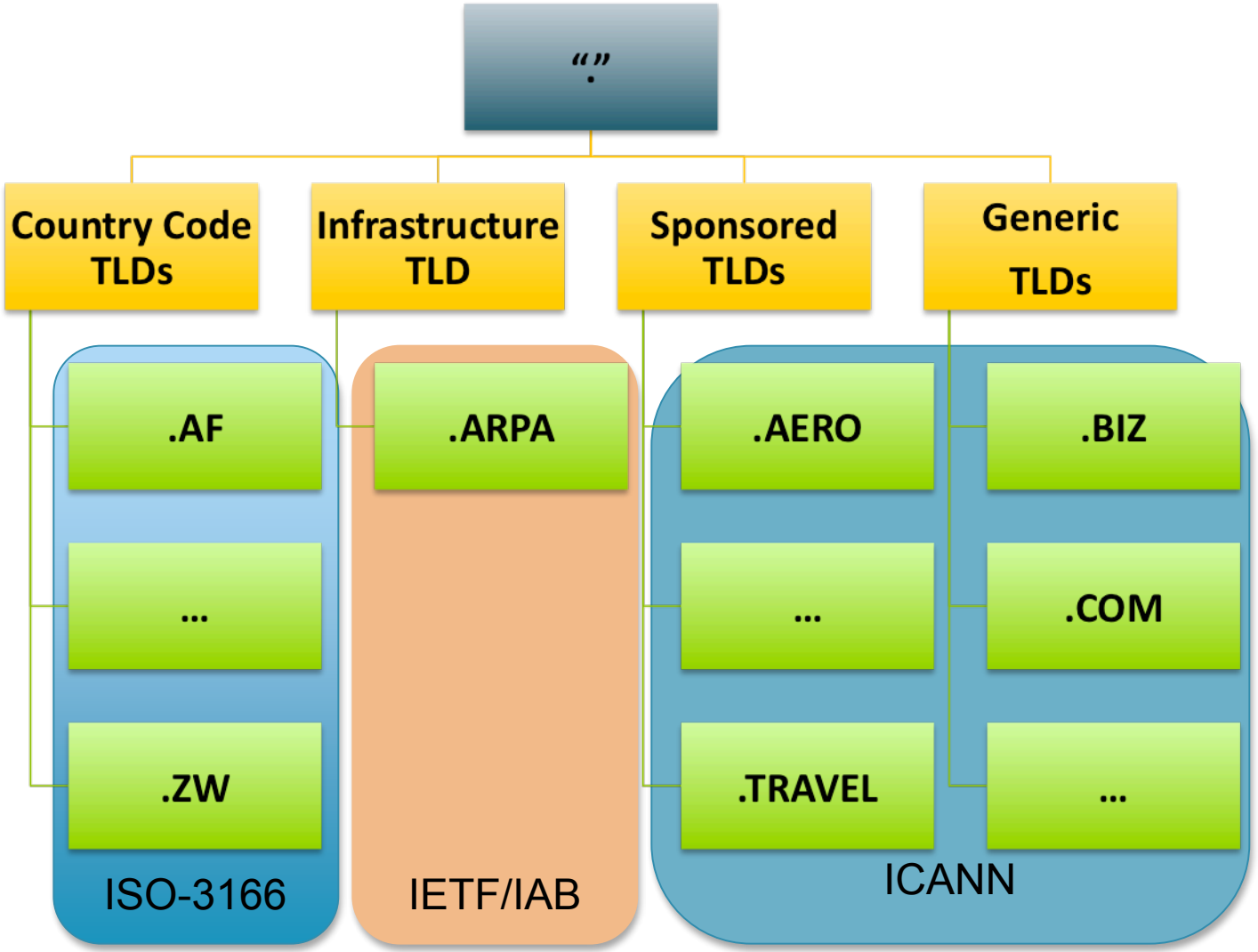
The technical side

- DNS is a globally distributed, loosely coherent, scalable, reliable key/value lookup system
  - **NOT** a directory
    - Think “directory assistance operator” instead of “telephone book”
- DNS admins publish “zones” of DNS data
- End users make use of agents (“caching resolvers”) to fetch data from those zones
  - Caching resolvers usually operated by ISPs

Random DNS trivia slide

- Invented in 1983, core remains unchanged
- Over 170,000,000 delegations (assignment of administrative authority over a zone)
  - Actual number unknowable
    - 75M+ in one zone alone (at ~$6/year each)
- Busiest servers handle 8-10K+ queries per second 24x7x365 each
  - Peaks of 100K+ qps reported
  - Average query size: ~60 bytes, response: ~200 bytes

DNS structure



Overview

- Introduction to the DNS
- IANA root management
- How a ccTLD can be structured
- Best Current Practices
- Q & A

IANA – What is it?

- The **Internet Assigned Numbers Authority**
- “Dedicated to preserving the central coordinating functions of the global Internet for the public good.”

What does that mean?

- The Internet is not 100% anarchy
- There does need to be some technical coordination, otherwise there would be no interoperability.
- IANA was designed to be that definitive central coordinating body.
  - Maintain the identifiers used on the Internet that need to be unique.

How IANA manages the root

- Maintain data for the DNS root
  - Technical data (NS records, “glue”)
  - Social data (admin and tech contacts, support organisations, WHOIS, Registration URL)
- Two types of changes
  - 1. Routine changes (easy!)
    - Confirm authenticity, check for technical problems, implement.
  - 2. Reassignments (hard!)
    - Perform evaluation, submit to ICANN board, implement as appropriate.

What IANA does not do

- Don’t set policy
  - Follow precedent where possible, encourage review of operations by community.
- Don’t unilaterally decide what the two letter codes should be
  - ISO 3166 standard provides these, ISO 3166 Maintenance Agency makes revisions
    - Additions may be applied for by appropriate parties, deletions should be replaced.
    - ICANN is one of ten members of the ISO 3166 MA
- Don’t decide who runs a ccTLD
  - local Internet community decision - IANA performs due diligence.

Overview

- Introduction to the DNS
- IANA root management
- How a ccTLD can be structured
- Best Current Practices
- Q & A

Country Code Top-Level Domains (ccTLDs)

- ISO 3166-1 standard nominates two-letter codes for countries and autonomous regions (as defined by UN)
- IANA will assign the operator of a ccTLD at the request of the local Internet community in a particular country.
  - initial request is a “delegation”, changing operators of an existing code is a “redelegation”.
- IANA doesn’t take an ongoing role in operating the domain, simply appoints the operator. Local interests should decide how the domain is run within country.

Key criteria for a ccTLD operator

- Summarizing from RFC 1591:
  1. Operator must show operational and technical skills. Must be able to operate the TLD in an effective and proper manner. Meet certain testable technical criteria.
  2. Operator must be in country. Allows the operation to be subject to local law.
  3. Operator must treat LIC fairly and equitably. The operator, for example, can't discriminate within the local Internet community on who it may provide service for.
  4. Operator must demonstrate community/government support. Operator needs to show that it has reasonable support to operate the resource.
- Ability to meet these criteria is formally assessed in the event of a delegation or redelegation request.

Get your data in order

- IANA keeps records on who runs each TLD
- If it is out of date, IANA doesn't know who is responsible any more
  - Causes problems if changes need to be made later
  - Also causes problems if someone needs to contact you for operational reasons.
- **Check your IANA records and update if necessary! Go to http://whois.iana.org**

For changes

- A simple text template available for ccTLD operators to complete and email IANA.
- Download from
  - http://www.iana.org/cctld/cctld-template.txt

(Re)Delegation procedure

- IANA performs evaluation in consultation with:
  - requestor to understand situation, seek additional documentation
  - current operators (if they exist) to determine consent
  - local Internet actors to confirm assertions on LIC support
  - governments to identify support
  - ICANN staff who have insight into local situation
- If assessed to proceed, considered by ICANN board
  - Multi-stakeholder board from many nations
  - Focus is on answering two questions:
    - Does the request reflect the in-country consensus?
    - Does the application preserve the stability of the Internet?
- Upon approval, implemented normally

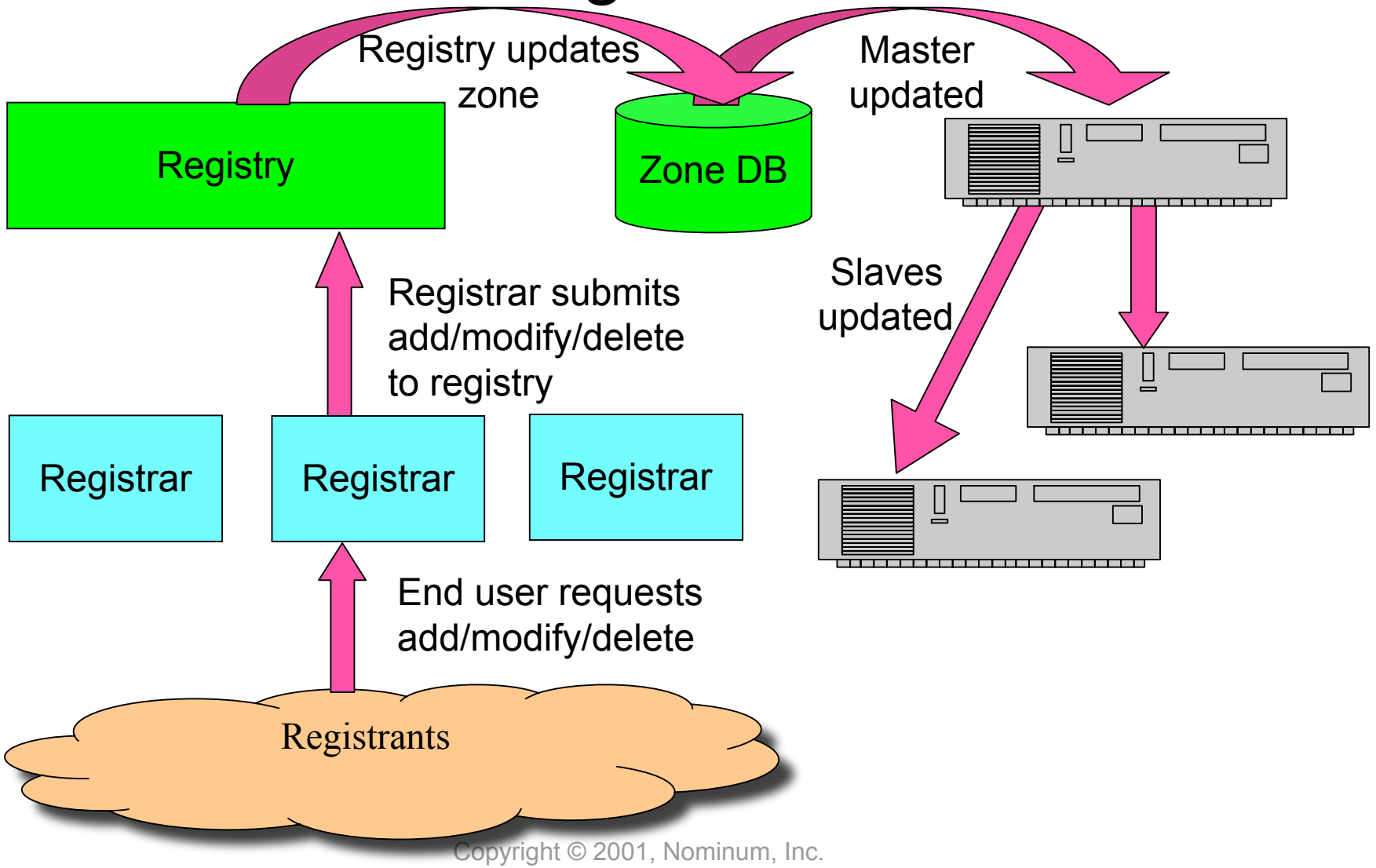
ccTLD structures

- Some options
  - Government?
  - Not for profit?
  - Outsource?
- Most common:
  - Not for profit private organization
  - Appropriate membership from the community
  - Chartered for limited scope
  - Some kind of liaison with the government
  - Often light regulatory oversight

Sales model

- Direct registration
  - No middle man - easier to control most aspects of registration
- Registry-registrar model
  - Requires an interface between registry and registrar
  - Offloads end-user interface from registry
- Both

Registries, Registrars, and Registrants



Scope

- Local or Global sales?
- Decide what best serves local community
- For global, consider legal aspects

Overview

- Introduction to the DNS
- IANA root management
- How a ccTLD can be structured
- Best Current Practices
- Q & A

Best practices

- These are some highlighted points from a few key documents on best practice
  - It is not exhaustive
- There is a wealth of information on ccTLD Operations out there
  - Check regional ccTLD organisation websites and meeting proceedings

RFC 2870 - Root Server Name operational requirements

- Document designed for Root Servers
  - Still some valuable advice for TLD operators
- Root servers and TLD servers aren't that different!
  - Or at least they shouldn't be
    - TLDs are at risk of "Denial of Service" attacks

Server considerations

- Must run servers that supports technical standards
- Must handle load 3x the measured peak
- Diverse bandwidth to support above
- Must answer authoritatively, and NOT be recursive
- Can’t block access from a valid Internet host
- Shouldn’t support AXFR (zone transfer)
- Diverse eco-system: heterogenous server software

Security considerations

- Physical security
  - Limited to a specific set of individuals
- Don’t provide other services on the servers (mail, ftp, web etc.)
- Keep on a separate network segment from public hosts
- Log attempts at intrusion
- Set your reverse DNS

Facilities considerations

- Power continuity for 48 hours
- Fire detection and retardation
- Backups

Communications

- Coordinate downtime between nameserver operators
- Coordinate backups between servers
  - keep backups off site
- Exchange logs and statistics between nameserver operators
- Nameserver operator personnel should be on call 24x7x365

RFC 2182 - Selection and operation of Secondary DNS servers

- Don’t place all on the same LAN/building/segment
- Host offline doesn’t mean DNS doesn’t matter!
- How many? 4 or 5 is probably good rule for TLDs, varies depending on circumstances !
  - Note: There is roughly a hard limit of 13, and of course there should be more than 1!

“ccTLD Best Practices” Draft

- A document in progress for a number of years
- Tries to describe some of the common practices of ccTLDs

Human Resources

- Administrative Point of Contact
  - Responsible for making clear rules for domain policy and operation.
  - Should represent the local Internet community and ensure ccTLD run for benefit of country and its citizens.
- Technical Point of Contact
  - Maintains the zone and makes sure systems run
- Programmers and Technical Staff
  - DNS experts, UNIX administrators should be in the team
- Finance and Billing
  - If you are to charge fees...
- Lawyers
  - A reality if you trade globally

Structuring the TLD

- Flat or hierarchical?
  - Flat - simpler, equal access
  - Hierarchical - more domains, less disputes
  - Difficult to change later
- Two (.co.xy) or Three (.com.xy) SLDs?
  - Matter of preference, really
- Distributed distribution?
  - Delegating sub domains to other parties
  - More complicated administration for small registries

Technical requirements for Registries

- Secondary Servers
- Networks (redundant)
- Physical and Electronic Security
- Quality of Service (24/7/365 availability!)
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol

Other considerations

- Dispute Resolution
  - Local law prevails
  - Alternate Dispute Resolution (ADR) designed to be more lightweight
  - ICANN UDRP is often used as a model
    - http://www.icann.org/udrp/udrp.htm

Organizations

- Regional organisations
  - APTLD (www.aptld.org)
  - CENTR (www.centr.org)
  - LACTLD (www.lactld.org)
  - AfTLD (www.aftld.org)
- Country Code Network Operators Group
  - www.ccnog.org
- ICANN
  - ccNSO (ccnso.icann.org)

More Information

- RFC 1591 - ccTLD governance
  - http://www.rfc-editor.org/rfc/rfc1591.txt
- RFC 2182 – Secondary selection
  - http://www.rfc-editor.org/rfc/rfc2182.txt
- RFC 2870 - Root Server BCP
  - http://www.rfc-editor.org/rfc/rfc2870.txt
- Accountability Frameworks
  - http://ccnso.icann.org/announcements/announcement-06jan06.html
- ccTLD Best Current Practice Draft
  - http://www.tinyurl.com/wdvqq
  - Currently a draft under development, comments welcome to the authors.

Summary

- IANA manages the root, and therefore the delegations that allow TLDs to do their work.
- TLDs should ensure their data (contact details, nameserves) are accurate with IANA.
- IANA's procedures to verify changes are thorough, to ensure stability of the DNS root.
- Full changes to the operator involve an investigation to ensure the changes are in

Contacts at IANA:

kim.davies@icann.org

naela.saras@icann.org

Your regional rep:

save.vocea@icann.org