DNS Registries

Shanghai, China, October 2002

Bill Manning <bmanning@karoshi.com>
Joe Abley <jabley@isc.org>
Topic Summary

- Introduction to DNS Registries
- Meta Issues: Scalability, Security
- Data Storage
- Interaction with Others
- Performance Measurement
- Policy
- Implementation Example
1. Introduction to DNS Registries
DNS and Nameservers

• DNS
• Nameservers
  – things which respond to DNS queries
• The DNS Root
  – the nameservers and the zone at the top of the tree
  – Provide entry into the distributed namespace database via structured referral
Registry Apex

- The name of root of the delegated sub-tree operated by the registry
- The closest point to the root of the DNS over which the registry has control
- Could be a gTLD, or a ccTLD
- Could be something else
Domains, Zones and Delegation

• **Domain Name**
  – A hierarchically-structured textual name with which various resource records can be associated

• **Zone**
  – “A complete database for a particular pruned subtree of the domain space” (RFC 1035)

• **Delegation**
  – The means by which requests for information about domain names are delegated to foreign authoritative nameservers
Domains, Zones and Delegation

• Domain Name
  – a name in your registry

• Zone
  – the small slice of the DNS concerned with connecting the rest of the DNS with your customers’ nameservers

• Delegation
  – Arranging things so that queries for customer names are referred to customer nameservers
  – what the customer is paying you for
Whois

- A means of extracting information from the registry
- Information may not be published in the DNS
- RFC 954
- Various query and output styles, little successful standardisation to date
Registry Model

- **Single-Point Registry Systems**
  - To obtain a delegation for a domain, talk directly to the registry operator
  - AQ, NZ (now), INT

- **“Shared Registry Systems” (SRS)**
  - Some degree of competitive access
  - Registry service reduced to minimum to encourage service differentiation
  - UK, US, NZ (soon)
Shared or Not?

• Shared Registry Systems can provide some welcome cost-savings for the Registry
  – dealing with a large customer base can be expensive and difficult
  – established registrars may provide some immediate revenue (and access to a global market) which can help with cost recovery of Registry Systems

• Single-Point Registries
  – control is retained at a central point
  – more obviously-suited to some registries due to local policies
Thick or Thin?

• A thin registry stores a minimal set of data, and distributes responsibility for other data to registrars
  – e.g. contact information
  – Verisign COM/NET/ORG registry

• A thick registry stores all data centrally, so registrars don’t have to
  – e.g. Afilias INFO registry
Registry, Registrar, Registrant

- Terms defined by ICANN to describe various parts of a Shared Registry System, as first proposed and subsequently deployed for COM, NET, ORG
- Yes, those words are very similar
- Yes, it does seem as if the choice of language was designed to confuse you
- Yes, lots of people use the wrong word, even people who almost certainly know what the words mean
Registry

• An entity which maintains a set of data, used to publish one or more zones

• The Registry’s customers are Registrars
  – few customers, low support overhead, high efficiency

• The Registry acts according to some delegated authority
  – from ICANN
  – from a government
  – from some community of interest
  – from the operator of the parent zone
Registrar

• An intermediary between registrants and registries
• Provides customer care, retail services
• May share the cost of customer care with other revenue-generating activities (web hosting, internet access)
• Customers of Registrars are Registrants
• Suppliers of Registrars are Registries
Registrant

- Someone who wants a domain name
- Suppliers of Registrants are Registrars
- Registrants can move domains between Registrars, if they want
2. Meta Issues

Scalability, Security
Registry Characteristics

• How much data?
  – how many domains?
• How often does the data change?
  – what turnaround times do you offer for changes?
  – what is the modify-transaction rate?
• How might these numbers grow?
• What bad things could happen to the data?
Nameserver Load Growth

- Bigger, faster nameservers
  - nameserver clusters
- More nameservers
  - anycast nameservers (see www.as112.net)
- Better-located nameservers
  - some resolvers (e.g. BIND) make some attempts to find “local” nameservers
Registry Growth

- Database scaling issues
  - cookbooks of how to run big databases are everywhere
  - even the biggest registry databases are small by today’s standards

- Registry Transaction Rate Growth
  - bigger, faster SRS servers
  - SRS clusters, distribution of SRS functions
Data Security

• Physical and System Security of Registry
• Authentication of Registrars
• Audit Trail
• Data Escrow
• Disaster Recovery
  – backups, dumps and restores
  – split-site architectures
3. Data Storage
To Publish a Zone File

• We need:
  – Delegations
    • NS records for domains that we want to publish in the zone
  – Glue
    • A records for nameservers named within a delegated zone, which are members of the NS set for that zone
To Maintain Registry Records

• We need:
  – a means of authenticating people who are allowed to make changes
  – a history of changes that have been made
  – a means of implementing registry policy (reserved or prohibited names, approval processes, etc)
To Meet Legal and Business Requirements

• We might well need:
  – a means of identifying who “owns” a particular domain name
  – a clear and authoritative audit trail for all changes in the registry
To Play Nicely With Others

– We need:
  
  • a method for other people on the internet can get in touch with the registrant
  
  • some way of publishing information about delegations to help registrants and others troubleshoot name resolution problems
To Generate Invoices

- We need:
  - to decide what events are billable
  - a way of collecting billable events in the registry, and directing those billable events in appropriate directions
  - a way of removing records from the registry if people don’t pay us
Example Registry Schema

- **Domains and Hosts**
  - maps of domains to hosts
- **Contacts**
  - maps of domains and hosts to contacts
  - technical, administrative, billing, …
- **Authentication**
  - maps of domains (or maybe contacts) to authentication criteria
- **Events**
  - changes, anniversary transitions, payments, notifications
DNS Registries

Tea Break
Continued at 11:00
4. Interaction with Others
Interaction with the World

- DNS
  - The reason for running a registry in the first place
- Whois
  - Metadata not published in the DNS, but associated with delegations, and available to all
Interaction with Registrars

• Deployed gTLD SRS protocols
  – Extensible Provisioning Protocol (EPP)
  – Verisign’s Registry-Registrar Protocol (RFC 2832)

• Deployed ccTLD SRS protocols
  – Lots

• Standardising on something might be nice
  – EPP seems like a reasonable choice
RRP

- RFC 2832, draft-hollenbeck-rfc2832bis-03
- Used between Verisign Registry and accredited Registrars
  - thin registry
  - somewhat single-purpose and non-extensible
- Interactive, session-oriented stream protocol carried out over SSL
EPP

• IETF standards-track protocol
• Active working group (provreg)
• Based on exchange of XML documents
• Deliverable over a variety of interactive and non-interactive transport protocols
  – TCP, BEEP
  – SMTP
• Highly extensible
If you don’t have Registrars

- You need to do the hard work of dealing with customers yourself
- You retain more control over the registry
5. Performance Measurement
Why Measure?

- Although running a registry is not as hard as some people seem to think, running any large database has potential for scaling issues.
- Registries tend to grow.
- Nice to identify the growth and deal with the scaling issues before they become scaling problems.
Nameserver Performance

• Things to Measure
  – time taken for each nameserver to process a resolver request and send a reply
  – inbound and outbound traffic at nameservers
Registry Performance

• Things to measure
  – SRS transaction request rates
  – SRS transaction completion times
  – time taken for requested changes to appear in the DNS
  – inbound and outbound traffic
6. Policy Issues
Reserved Names

• The terms under which the registry is operated may place restrictions on what names can be registered
  – offensive names
  – names which might cause confusion

• Registry implementations should probably facilitate this kind of thing, even if no such policy currently exists
  – this kind of policy has been known to appear suddenly
Grace Periods

- Registrant mistypes a name, and wants to remove the mistyped name and replace it with the name she meant to specify
- Payment for an invoice is delayed for a couple of days, and a domain name becomes deleted
- Some Registries operate grace periods to accommodate these kinds of issues
  - sometimes it’s easier and cheaper to be flexible than to punish people for making mistakes
Domain Renewal

- Some Registries automatically renew names, unless they have been explicitly deleted by their Registrar
- Multi-year renewals
Manual Authorisation

• Lost password
• Administrator e-mail address change
• Company acquisition
Registrar Accreditation

• Technical Readiness
  – certification testing

• Financial, other criteria
  – seek to avoid spontaneous registrar combustion
  – ensure that registrar’s customer fulfilment includes appropriate legal aspects
7. Implementation Example

ISC OpenReg
OpenReg

• Several slides briefly describing the ISC’s free OpenReg software will appear here