IANA Update for TLD operators

Sydney, Australia
June 2009

Kim Davies
Manager, Root Zone Services

Internet Corporation for
Assigned Names & Numbers

Technical Conformance

Technical Conformance

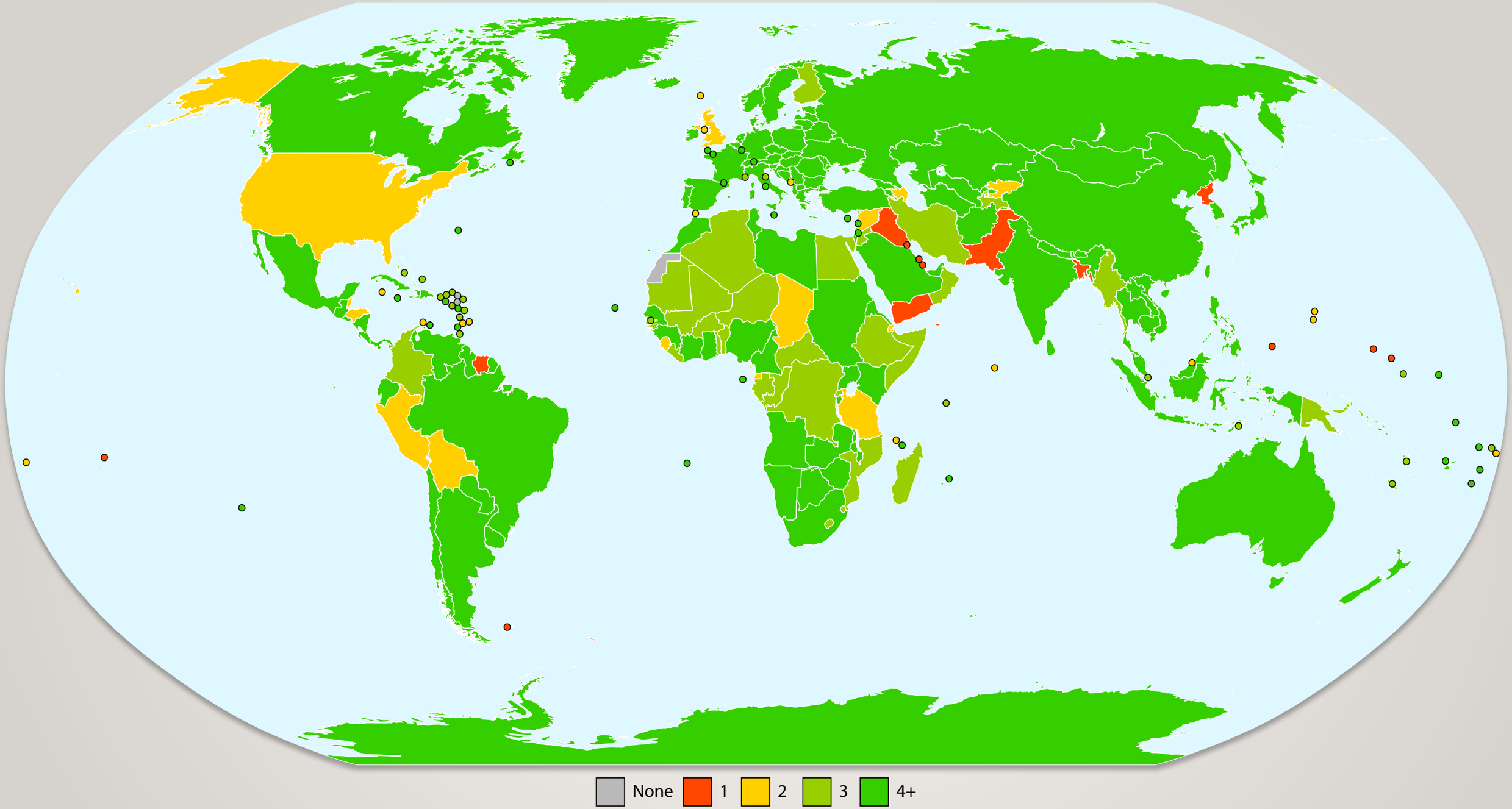
- Bring our minimum technical criteria for root zone changes up to date
- Phasing in:
  - Prohibition on open recursive name servers
  - More appropriate name server diversity requirement
  - No fragmentation of root zone referrals

1 Open recursive name servers

- Not good network citizens
  - Open to cache poisoning attacks (Kaminsky, et.al)
  - Open to amplification attacks
- Not required for authoritative service

❷ Network diversity for name servers

- Current informal rule is a minimum of two “not in the same /24 subnet”
  - Not very relevant to networks today
- Each IP address on the Internet’s network location is derived through announcements in the “global routing table” using BGP
- Each network is roughly organised into a group called an “autonomous system”
- Require name servers to be announced in at least two different autonomous systems



ccTLDs with AS diversity

As at 1 March 2009

❸ Referrals should not fragment

- A query for a domain name to the root servers should result in a referral to the TLD's authorities
- Classical limit for response size is 512 bytes
- If the root server needs to send back more than 512 bytes of in a response, it will need to use the much more complicated TCP protocol, rather than the simpler UDP protocol.
- This is not good for load and reliability

The bottom line

✔ TLDs with open recursive name servers	9.6%
✔ TLDs without diverse IPv4 connectivity	7.2%
✔ TLDs with referrals that can fragment	4.3%

Now published

Technical requirements for authoritative name servers

This document describes the baseline technical conformance criteria for authoritative name servers. These are evaluated for changes to delegations in domains that IANA maintains, such as the DNS root zone.

1 Definitions

1.1 The **designated domain** is the zone for which the change of delegation is sought, and for which IANA maintains the parent zone.

1.2 For the purposes of this document, a **name server** is a DNS server that has been proposed to answer authoritatively for the designated domain, and is being requested to be listed in the delegation. It is recorded by its fully-qualified domain name, potentially along with its IP addresses.

1.3 Name server tests are completed against each unique tuple of a hostname, an IP address, and a protocol. If a hostname has multiple IP addresses, for example, the tests will be conducted against each IP address.

2 Technical requirements

2.1 Minimum number of name servers

2.1.1 There must be at least two NS records listed in a delegation, and the hosts must not resolve to the same IP address.

2.2 Valid hostnames

Next steps

- Implemented in RZM automation software
- Online web tool to check conformance (separate implementation)
  - Library
- Quarterly audit emails

Documenting IANA processes

Documenting Procedures

- ICP-1 debacle means ICANN has been hesitant to publish its procedures
  - Times have moved on since 2002?
- Thoroughly documenting all procedures for public review
- Redelegation procedures will provide input for the ccNSO redelegation working group
- Also developing an analysis of the current processes for community review

#	RFC 1591 *(1994)*	Status	ICP 1 *(1999)*	Status
56	"...the regional registries are often enlisted to assist in the administration of the DNS, especially in solving problems with a country administration."	Invalid	(removed)	—
57	"Currently the RIPE NCC is the regional registry for Europe and the APNIC is the regional registry for the Asia-Pacific region, while INTERNIC administers the North America region, and all the as yet undelegated regions"	Invalid	(removed)	—
58	"A new top-level domain is usually created and its management to a "designated manager" all at once"	Invalid	(removed)	—
59	"Most of these same concerns are relevant when a sub-domain is delegated and in general the principles described here apply recursively to all delegations of the Internet DNS name space."	Valid	"In general, the principles described here apply recursively to all delegations of the Internet DNS name space."	Valid
60	"The major concern in selecting a designated manager for a domain is that it be able to carry out the necessary responsibility, and have the ability to do an equitable, just, honest and competent job."	Valid	"Delegation of a new top-level domain requires the completion of a number of procedures, including the identification of a TLD manager with the requisite skills and authority to operate the TLD appropriately."	Valid
61	— (*note: phrasing from Jon Postel's memo to ccTLD operators on 23 October 1997*)	—	"The desires of the government of a country with regard to delegation of a ccTLD are taken very seriously. The IANA will make them a major consideration in any TLD delegation/ transfer discussions."	Valid

Root Zone Workflow Automation

Moving forward

- With NTIA staffing change, a new deployment approach was requested involving pre-approving a test and deployment plan
- Test plan submitted in October 2008
- Authorisation to proceed on test plan received June 2009
- Parallel operations to commence shortly
  - Setting launch timeline with VeriSign and NTIA
- NTIA has agreed with ICANN to make public our submission

Signing the Root Zone

Signing the root zone?

- ICANN developed a proposal to sign the root zone which was submitted to US Government
- VeriSign followed up with a different proposal to sign the root zone
- The US Government has issued a "Notice of Inquiry" to seek views relating to signing the DNS root zone, which was open to comments until November 24.
  - http://tinyurl.com/3v8akt

ACTION: Notice of Inquiry

SUMMARY: The Department of Commerce (Department) notes the increase in interest among government, technology experts and industry representatives regarding the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. The Department remains committed to preserving the security and stability of the DNS and is exploring the implementation of DNSSEC in the DNS hierarchy, including at the authoritative root zone level. Accordingly, the Department is issuing this notice to invite comments regarding DNSSEC implementation at the root zone.

DATES: Comments are due on November 24, 2008.

ADDRESSES: Written comments may be submitted by mail to Fiona Alexander, Associate Administrator, Office of International Affairs, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., Room 4701, Washington, DC 20230. Written comments may also be sent by facsimile to (202) 482–1865 or electronically via electronic mail to DNSSEC@ntia.doc.gov. Comments will be posted on NTIA's website at http://

Outcome

- Wired: *Internet experts are siding overwhelmingly with ICANN*
- NTIA has instructed that VeriSign sign the root zone
- ICANN accepts that it is important to sign the root zone swiftly, and will proceed accordingly
- See http://tr.im/signedroot
- NTIA will present at DNSSEC workshop on Wednesday

Other IANA activities

Quality Management

- Working on quality management of IANA services using EFQM model (www.efqm.org)
- First evaluation of IANA proposed for May 2010
- Aim is to capture full range of resources required for excellent performance of IANA functions
- Compare ICANN's performance to similar organisations
- Adopt performance objectives and achieve excellence

Trust Anchor Repository

- Continues to function
- Apart from some minor tweaks in the first weeks, been running without incident
- Automated system, but many TLDs are replying manually rather than clicking “accept” links — negating benefits of automation.

New WHOIS server

- Will contain IP address objects as well as existing domain objects (TLDs, .INT, .ARPA, IANA registrar domains)
- RPSL style notation
- Will be deployed to coincide with:
  - RZM Workflow Automation for the root zone
  - RDNS management system for .ARPA

Thanks!

kim.davies@icann.org