Multilingualization within a multi-stakeholder model for Internet governance

Most of us cringe at the challenge of ubiquitous language interoperability, afraid that the technical debt amassed by tens of thousands of businesses and trillions of lines of code written over two decades has come due. Some may even wish to sweep the problem under the rug, and wonder if it would be easier if the rest of the world would just become fluent in English, so that the massive productivity gains that we have experienced may be amplified through global participation in the conversation that is the Internet.

I wonder, though, if we would have been so fortunate if we had to access the Internet in Chinese and convene our discussions at http://例子.测试 (case in point).

It is human nature to prefer to communicate in our native tongue, as it is to be masters of our own destiny. To this end, although great strides have been made in terms of internationalization, there are still issues that must be addressed in both the proliferation of infrastructure that powers the Internet and applications through which users access the Internet.

As we begin to roll out the globalization of IANA functions, perhaps via the implementation of a distributed root zone file where each country is responsible for updates to its own ccTLDs and gTLDs, an opportunity is emerging to embed governmental responsibility to support IDNA within their own aspirations.

For example, the development of language specific resources may be mandated from governments aspiring to sponsor a "regional master root server" in a system where an international technology coalition has the authority to elect regional master root servers that are globally aware of sibling regional master root servers, such that a server may broadcast a notification of the availability of a new root zone file, signed by a trusted third party, and containing updates for its respective TLDs. Every sibling may then initiate transfer of the new root zone via a protocol similar to SHA-2 TSIG enabled AXFR, validate the trusted third party signature and verify that only records for which the notifying server is authoritative have been altered before the new root zone may become active, anycast internally, and publicly available via DNS.

The signed root zone file may be obtained from an external technical authority through a process that ensures valid format of the data within an update request, before an updated root zone may ensue. For example, a semi-automated and iterative cycle may be used between the technical authority and a regional master root server to satisfy the questions "will this update result in a valid root zone file?" and "if not, why?", until the format of the update is corrected by the server operator and affirmed by the technical authority via a response that contains the updated and signed root zone file. The technical authority may then facilitate a policing function by polling regional master root servers to ensure that they are updated in a timely manner.

A dispute and resolution process may exist within the international technology coalition, to provide opportunities for mediation and, after due process, finally circumvent a response by the technical authority through majority consensus of root server operators. The dispute resolution process may also be leveraged, at the request of the technical authority, and with greater consensus, to revoke a regional master root server in order to supplement technical measures to maintain the integrity of the network.

An existing trusted third party authority should provide DNSSEC integrity to the network such that the technical authority may transmit signed root zone files to be validated by regional master root servers for distribution. A separate trusted international authority, distinct from the coalition, may be responsible for the distribution and maintenance of shared secrets for TSIG enabled AXFR (or even implement TSIG-CGA) among the regional master root servers. Movement to replace either trusted authority should be evidenced by willful malfeasance, failure to comply with the outcome of dispute processes, and require overwhelming support, such the combined near unanimous consensus of root server operators, international technology coalition vote, two-thirds majority of the UN General Assembly and trigger a periodic election to choose an entity to host the respective trusted authority.

Although open source measurement tools to collect RSSAC defined metrics may be developed in concert with ISOC, root server operators, and other stakeholders for stakeholder visibility into the entire root server system's performance, the regional master root server sponsors should bear the burden of supporting the creation and maintenance of label generation rulesets, language and variant tables, operational software, and technical training material through collaboration with both ICANN and working groups representing the relevant linguistic communities.

Further challenges to the multilingualization of the Internet exist in the handling of IDNs by web-based services. To facilitate the transition to full support of IDNs, W3C standards may enable web servers to respond with Accept-Language headers, much like clients, to signal what languages they support for input during a subsequent request. Used in conjunction with HTML5 input types such as "url" and "email", this may enable browsers to transparently convert to and from ACE-encoded representations for a language used by a client but unsupported by a server. In conjunction with tag recognition this may also enable web application developers to expect content to be transparently displayed in the user's preferred language, as opposed to PunyCode.

(Reference: RFCs 5890, 5936, 1996, 4035, 2845 and 4635)

Tamer Rizk
Cambridge, MA
March 19, 2014