

RFC 2826: A Comment on its Relevance to the Policy Debate over Alternate Roots

Dr. Milton Mueller, Associate Professor, Syracuse University School of Information Studies

RFC 2826, “IAB Technical Comment on the Unique DNS Root,” is often cited in the policy debates over alternate roots as if it were the last word on the subject. The statement is useful as a description of one of the original design parameters of the DNS. But this paper shows that it provides no guidance as to how to resolve the policy issues posed by the existence of competing or multiple roots.

What RFC 2826 says

According to RFC 2826, the DNS protocol was designed with the assumption that there would be only one authoritative root zone file. The statement goes on to describe some of the difficulties that might occur if computers attempting to resolve domain names are confused about the contents of the root zone file. The fundamental conclusion of RFC 2826 is this:

...a degree of cooperation and agreed technical rules are required in order to guarantee the uniqueness of names. In the DNS, these rules are established independently for each part of the naming hierarchy, and the root domain is no exception. Thus, there must be a generally agreed single set of rules for [assigning the top-level domain names listed in] the root.

I agree with this statement. In fact, it is difficult to find anyone who does not agree with it. The differences arise over how to apply this simple concept to DNS policy.

Alternate Roots Exist

The IAB statement attempts to jump to a policy conclusion. It states “it is not technically feasible for there to be more than one root in the public DNS.” It is a rather strange claim. There *are* different root server systems in operation. These alternate root systems use the same DNS protocol and the same software implementation (BIND) as the ICANN root servers. Most, if not all, of them are capable of resolving all names under the IANA-delegated top-level domains. So it cannot be argued that they are not an implementation of the Domain Name System protocol. Nor it is technically correct to say that they are “private” rather than “public” name spaces. All of the alternate root systems are open to any ISP or end user who wishes to point resolvers or name servers in their direction.

Even if alternate roots did not exist now, nothing in the DNS protocol prevents a subset of the world’s Internet service providers or end users from redirecting their name servers

to some place other than the ICANN-administered root, if they wished to do so, at any time. The IAB statement is wrong: it is possible for there to be “more than one root in the public DNS.”

What the IAB really wants to say is that such roots may lead to compatibility problems in resolving names. But whether the value added by competing roots is worth the price is not a technical matter and is therefore beyond the purview of the IAB. Also, RFC 2826 provides no guidance as to how to respond to the compatibility problems posed by alternate roots, once they exist

RFC 2826 and DNS Policy

Because it is premised on the false idea that multiple roots cannot exist, RFC 2826 contributes very little of value to the policy debate over what to do about competing roots when and if they arise. Indeed, in many ways RFC 2826’s insistence on the singularity of the root has become an obstacle to rational discussion of the problem of multiple roots.

Both RFC 2826 and many of its advocates seem to suffer from a fundamental confusion. Are they arguing that multiple roots *do not exist*, as RFC 2826 states, or are they stating a belief that alternate roots *should not exist*? A statement that something should not exist has entirely different implications than a statement that something does not or cannot exist. If one believes that alternate roots *should not exist*, one must come up with concrete, feasible, and legal proposals to preserve the singularity of the root, and one must deal with a variety of socio-economic tradeoffs. One does not, for example, contribute much to crime control policy by repeatedly asserting “crime is bad” or “crime should not exist.” An effective crime prevention policy must identify specific measures to reduce or eliminate crime – and those measures must balance the goal of crime prevention against other social values, such as privacy, individual rights, cost constraints, and so on.

Assuming one accepts the basic premise of RFC 2826 that the root should be coordinated, and one accepts the fact that alternate roots can and do exist, one can identify several different policy options that might be advanced to achieve coordination:

- ICANN could agree to coordinate its top-level domain assignments with those of alternate roots, by adding their TLDs to its root zone
- The ICANN root could ignore alternate roots, but avoid assigning TLDs that conflicted with TLDs in alternate roots
- ICANN could pretend the alternate roots don’t exist and assign TLDs that conflicted with TLDs in alternate roots, and attempt to drive them out of existence
- The backers of ICANN could seek legislation to ban alternate roots
- There are many other options too complex to go into here; e.g., ICANN could set thresholds that determined when a TLD from another root would be entered into its own root, or fix some other algorithm determining its relationship with them.

RFC 2826 provides no guidance as to which of these options is best. Nor should it; the IAB’s expertise is in protocols, not public policy. It is not a policy making body and its

technical pronouncements, as demonstrated above, are not particularly useful in policy debates.

What Sustains Alternate Roots?

To demonstrate just how irrelevant RFC 2826 is to the real policy dilemmas posed by multiple roots, consider the following scenario. Suppose that the performance of the ICANN-administered root servers deteriorated significantly, and ICANN, for whatever reason, failed to take action to resolve the problem. Suppose that a group of ISPs, instead of suffering from continued poor performance, decided to operate their own DNS root with better performance, and in the process they added a few new TLDs to the root they administered.

If ISPs are defecting from the ICANN root, or altering it in specific ways, it is not very intelligent to hurl religious admonitions about the need for a single, authoritative root at them. It would be much wiser to ask what is motivating their defection. If the market sustains and rewards these defections, it is not only unwise but dangerous for ICANN to attempt to stop it.

Conclusion

RFC 2826's statement that "there must be a generally agreed single set of rules for the root" is a good starting point for policy discussion. However, that assertion is both uncontroversial and not dispositive of the policy options available. Advocates of a "single authoritative root" need to face the reality that portions of the Internet community can and are defecting from or supplementing the ICANN root. Asserting that a particular root server system "should be" authoritative and singular does not make it so. One can agree on the need for coordination at the root level without necessarily agreeing that ICANN is the sole or proper source of those rules. Nor does the general need for a single set of rules eliminate the legitimacy and benefit of debate over what those rules should be.