Network Working Group
Request for Comments: 2826
Category: Informational

Internet Architecture Board
May 2000

IAB Technical Comment on the Unique DNS Root

Status of this Memo

Copyright Notice

Summary

To remain a global network, the Internet requires the existence of a globally unique public name space. The DNS name space is a hierarchical name space derived from a single, globally unique root. This is a technical constraint inherent in the design of the DNS. Therefore it is not technically feasible for there to be more than one root in the public DNS. That one root must be supported by a set of coordinated root servers administered by a unique naming authority.

Put simply, deploying multiple public DNS roots would raise a very strong possibility that users of different ISPs who click on the same link on a web page could end up at different destinations, against the will of the web page designers.

This does not preclude private networks from operating their own private name spaces, but if they wish to make use of names uniquely defined for the global Internet, they have to fetch that information from the global DNS naming hierarchy, and in particular from the coordinated root servers of the global DNS naming hierarchy.

1. Detailed Explanation

There are several distinct reasons why the DNS requires a single root in order to operate properly.

1.1. Maintenance of a Common Symbol Set

Effective communications between two parties requires two essential preconditions:

- The existence of a common symbol set, and

- The existence of a common semantic interpretation of these symbols.

Failure to meet the first condition implies a failure to communicate at all, while failure to meet the second implies that the meaning of the communication is lost.

In the case of a public communications system this condition of a common symbol set with a common semantic interpretation must be further strengthened to that of a unique symbol set with a unique semantic interpretation. This condition of uniqueness allows any party to initiate a communication that can be received and understood by any other party. Such a condition rules out the ability to define a symbol within some bounded context. In such a case, once the communication moves out of the context of interpretation in which it was defined, the meaning of the symbol becomes lost.

Within public digital communications networks such as the Internet this requirement for a uniquely defined symbol set with a uniquely defined meaning exists at many levels, commencing with the binary encoding scheme, extending to packet headers and payload formats and the protocol that an application uses to interact. In each case a variation of the symbol set or a difference of interpretation of the symbols being used within the interaction causes a protocol failure, and the communication fails. The property of uniqueness allows a symbol to be used unambiguously in any context, allowing the symbol to be passed on, referred to, and reused, while still preserving the meaning of the original use.

The DNS fulfills an essential role within the Internet protocol environment, allowing network locations to be referred to using a label other than a protocol address. As with any other such symbol set, DNS names are designed to be globally unique, that is, for any one DNS name at any one time there must be a single set of DNS records uniquely describing protocol addresses, network resources and services associated with that DNS name. All of the applications deployed on the Internet which use the DNS assume this, and Internet users expect such behavior from DNS names. Names are then constant symbols, whose interpretation does not specifically require knowledge of the context of any individual party. A DNS name can be passed from one party to another without altering the semantic intent of the name.

Since the DNS is hierarchically structured into domains, the uniqueness requirement for DNS names in their entirety implies that each of the names (sub-domains) defined within a domain has a unique

meaning (i.e., set of DNS records) within that domain. This is as true for the root domain as for any other DNS domain. The requirement for uniqueness within a domain further implies that there be some mechanism to prevent name conflicts within a domain. In DNS this is accomplished by assigning a single owner or maintainer to every domain, including the root domain, who is responsible for ensuring that each sub-domain of that domain has the proper records associated with it. This is a technical requirement, not a policy choice.

1.2. Coordination of Updates

Both the design and implementations of the DNS protocol are heavily based on the assumption that there is a single owner or maintainer for every domain, and that any set of resources records associated with a domain is modified in a single-copy serializable fashion. That is, even assuming that a single domain could somehow be "shared" by uncooperating parties, there is no means within the DNS protocol by which a user or client could discover, and choose between, conflicting definitions of a DNS name made by different parties. The client will simply return the first set of resource records that it finds that matches the requested domain, and assume that these are valid. This protocol is embedded in the operating software of hundreds of millions of computer systems, and is not easily updated to support a shared domain scenario.

Moreover, even supposing that some other means of resolving conflicting definitions could be provided in the future, it would have to be based on objective rules established in advance. For example, zone A.B could declare that naming authority Y had been delegated all subdomains of A.B with an odd number of characters, and that naming authority Z had been delegated authority to define subdomains of A.B with an even number of characters. Thus, a single set of rules would have to be agreed to prevent Y and Z from making conflicting assignments, and with this train of actions a single unique space has been created in any case. Even this would not allow multiple non-cooperating authorities to assign arbitrary sub-domains within a single domain.

It seems that 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 the root.

1.3. Difficulty of Relocating the Root Zone

There is one specific technical respect in which the root zone differs from all other DNS zones: the addresses of the name servers for the root zone come primarily from out-of-band information. This out-of-band information is often poorly maintained and, unlike all other data in the DNS, the out-of-band information has no automatic timeout mechanism. It is not uncommon for this information to be years out of date at many sites.

Like any other zone, the root zone contains a set of "name server" resource records listing its servers, but a resolver with no valid addresses for the current set of root servers will never be able to obtain these records. More insidiously, a resolver that has a mixed set of partially valid and partially stale out-of-band configuration information will not be able to tell which are the "real" root servers if it gets back conflicting answers; thus, it is very difficult to revoke the status of a malicious root server, or even to route around a buggy root server.

In effect, every full-service resolver in the world "delegates" the root of the public tree to the public root server(s) of its choice.

As a direct consequence, any change to the list of IP addresses that specify the public root zone is significantly more difficult than changing any other aspect of the DNS delegation chain. Thus, stability of the system calls for extremely conservative and cautious management of the public root zone: the frequency of updates to the root zone must be kept low, and the servers for the root zone must be closely coordinated.

These problems can be ameliorated to some extent by the DNS Security Extensions [DNSSEC], but a similar out-of-band configuration problem exists for the cryptographic signature key to the root zone, so the root zone still requires tight coupling and coordinated management even in the presence of DNSSEC.

2. Conclusion

The DNS type of unique naming and name-mapping system may not be ideal for a number of purposes for which it was never designed, such a locating information when the user doesn’t precisely know the correct names. As the Internet continues to expand, we would expect directory systems to evolve which can assist the user in dealing with vague or ambiguous references. To preserve the many important features of the DNS and its multiple record types -- including the Internet’s equivalent of telephone number portability -- we would expect the result of directory lookups and identification of the

correct names for a particular purpose to be unique DNS names that are then resolved normally, rather than having directory systems "replace" the DNS.

There is no getting away from the unique root of the public DNS.

3. Security Considerations

This memo does not introduce any new security issues, but it does attempt to identify some of the problems inherent in a family of recurring technically naive proposals.

4. IANA Considerations

This memo is not intended to create any new issues for IANA.

5. References

[DNS-CONCEPTS] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[DNS-IMPLEMENTATION] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[DNSSEC] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

6. Author’s Address

Internet Architecture Board

EMail: iab@iab.org

7. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.