Network Working Group
Request for Comments: 3245
Category: Informational

J. Klensin, Ed.
IAB

March 2002

The History and Context of Telephone Number Mapping (ENUM) Operational Decisions: Informational Documents Contributed to ITU-T Study Group 2 (SG2)

Status of this Memo

Copyright Notice

Abstract

RFC 2916 assigned responsibility for a number of administrative and operational details of Telephone Number Mapping (ENUM) to the IAB. It also anticipated that ITU would take responsibility for determining the legitimacy and appropriateness of applicants for delegation of "country code"-level subdomains of the top-level ENUM domain. Recently, three memos have been prepared for the ITU-T Study Group 2 (SG2) to explain the background of, and reasoning for, the relevant decisions. The IAB has also supplied a set of procedural instructions to the RIPE NCC for implementation of their part of the model. The content of the three memos is provided in this document for the information of the IETF community.

Table of Contents

1. Introduction: ENUM Background Information 2
2. Why one and only one domain is used in ENUM 2
3. Why .ARPA was selected as the top level domain for ENUM 4
4. The selection of an operator for E164.ARPA 7
5. Procedures to be followed by RIPE NCC 8
6. References 8
6.1. Normative references 8
6.2. Informative and explanatory references 8
7. Security Considerations 9
8. IANA Considerations 9
9. Authors' Addresses 9
10. Full Copyright Statement 10

1. Introduction: ENUM Background Information

In January 2002, in response to questions from the ITU-T Study Group 2 (referred to just as "SG2", below), specifically its group working on "Questions 1 and 2", and members of the IETF and telecommunications communities, Scott Bradner, as Area Director responsible for the ENUM work and ISOC Vice President for Standards, initiated an effort to produce explanations of the decisions made by the IETF about ENUM administration. The effort to produce and refine those documents eventually involved him, Patrik Faltstrom (author of RFC 2916), and several members of the IAB.

The documents have now been contributed to ITU-T, and are being published as internal SG2 documents. This document provides the IETF community a copy of the information provided to SG2. Section 2 below contains the same content as COM 2-11-E, section 3 contains the same content as COM 2-12-E, and section 4 contains the same content as SG2 document COM 2-10-E. The documents being published within SG2 show their source as "THE INTERNET SOCIETY ON BEHALF OF THE IETF", which is a formality deriving from the fact that ISOC holds an ITU sector membership on behalf of the IETF.

2. Why one and only one domain is used in ENUM

2.1. Introduction

This contribution is one of a series provided by the IETF to ITU-T SG2 to provide background information about the IETF’s ENUM Working Group deliberations and decisions. This particular contribution addresses the IETF’s decision that only a single domain could be supported in ENUM.

2.2. The need for a single root in the DNS

In the Domain Name System (DNS), each domain name is globally unique. This is a fundamental fact in the DNS system and follows mathematically from the structure of that system as well as the resource identification requirements of the Internet. Which DNS server is authoritative for a specific domain is defined by delegations from the parent domain, and this is repeated recursively until the so-called root zone, which is handled by a well-known set of DNS servers. Note that words like "authoritative" and "delegation" and their variations are used here in their specific, technical, DNS sense and may not have the same meanings they normally would in an ITU context.

Given that one starts with the well-known root zone, every party querying the DNS system will end up at the same set of servers for the same domain, regardless of who is sending the query, when the query is sent and where in the network the query is initiated. In May 2000 the IAB published a document on the need for a single root in the DNS. This document explores the issues in greater detail. See RFC 2826 (http://www.ietf.org/rfc/rfc2826.txt).

2.3. Storing E.164 numbers in the DNS

An E.164 number is also globally unique, and because of that it has most of the same properties as a domain name. This was the reason why storing E.164 numbers in the DNS system is technically a simple mapping. ENUM is just that, a way to store E.164 numbers in the DNS. Multiple ENUM trees in the DNS hierarchy would have the telephony equivalent of permitting every carrier to assign a different meaning to an E.164 country code, with each one potentially mapping a given number to a different circuit or rejecting it entirely. For the Internet, if there were multiple trees, there would be no way to determine which domains might contain ENUM records. Thus, each application that uses ENUM facilities would have to be manually configured with a list of domains to be searched. This would incur the same problems of scaling and updates that led to the development of the DNS.

The goal with ENUM is that one party should be able to look up information in DNS, which another party has stored in DNS. This must be possible with only the E.164 number as input to the algorithm.

If the party storing information in DNS has two (or more) places to choose from, and chooses one of them, how is a second party looking up things to know what place was selected? An analogy would be if one knew only www.whitehouse, and not the TLD, and ask people to go to that website. Is the correct domain name www.whitehouse.gov, www.whitehouse.com or www.whitehouse.se? It should be noted that www.whitehouse.com exists and is a pornography site.

Thus, the only way of knowing where to look up E.164/ENUM numbers in DNS is to use one and only one domain, and have everyone agree on what that domain is. Note that ENUM is a system for use with E.164 numbers in their general, global, context. Nothing technical can, or should, try to prevent parties that wish to use ENUM-like mechanisms, or other systems that have the same general structure as telephone numbers, from working out private, out of band, agreements to support those applications. However, such applications are neither E.164 nor ENUM, any more than internal extension numbers in a PBX are normally considered to be part of either.

3. Why .ARPA was selected as the top level domain for ENUM

3.1. Introduction

This memo is one of a series provided by the IETF to SG2 to provide background information about the IETF's ENUM Working Group deliberations and decisions. This particular memo addresses the IETF's decision that the ENUM DNS tree would use the .ARPA top level domain.

3.2. IAB Statement on Infrastructure Domain and Subdomains

(Taken from http://www.iab.org/iab/DOCUMENTS/iab-arpa-stmt.txt, May 2000.)

Over the last several months, the IAB has been reviewing, and discussing with ICANN and other parties, the handling of various Internet Protocol-related infrastructure components that the community has concluded should be placed into the DNS.

Historically, the most visible infrastructure domain has been the IPv4 address reverse-mapping domain. This domain was placed in "in-addr.arpa" as part of the initial ARPANET transition strategy from host table naming (see RFC 881-http://www.ietf.org/rfc/ rfc0881.txt). Other than the IPv4 reverse-mapping subdomain, it became the only active subdomain of that domain as the <host-table-name>.ARPA names that were also part of the transition were gradually removed. Other infrastructure domains were, in the past, placed under the "INT" TLD and various organizational names.

It is in the interest of general Internet stability, to pay adequate attention to the placement of secondary DNS servers, and administrative cleanliness, to start rationalizing this situation by locating new infrastructure subdomains in a single domain and migrating existing ones to it as appropriate. It appears that our original infrastructure domain "ARPA", redesignated from an abbreviation for "ARPANET" to an acronym for "Address and Routing Parameters Area" is best suited for this purpose.

3.3. Infrastructure subdomains

Operationally, it is easier to ensure good stability for DNS in general if we have as few DNS zones as possible that are used for parameters for infrastructure purposes. Today, new infrastructure domains are put in ARPA and old assignments which were made in other domains are being migrated to ARPA. Currently, ARPA is used for in-addr.arpa (for reverse mapping of IPv4 addresses), ip6.arpa, (for

reverse mapping of IPv6 addresses), and e164.arpa, (the subject of this memo). In the future, URI schemes, URN namespaces and other new address families will be stored in ARPA.

Theoretically, each set of infrastructure parameters could be stored in a separate domain as a TLD. (For example, .URI, .UNI, .IPV6, new TLD, which only can be created via the ICANN process (which might take a year or more) and would unnecessarily and undesirably flatten the DNS tree. It is much easier to have one TLD with easily created new subdomains (2nd level domains), one for each parameter. Thus it was logical to store E.164 numbers in ARPA.

3.4. The ARPA domain (derived from RFC 3172, September 2001)

The "arpa" domain was originally established as part of the initial deployment of the DNS, to provide a transition mechanism from the Host Tables that were previously standard in the ARPANET. It was also used to provide a permanent home for IPv4 address to name mappings ("reverse mappings") which were previously also handled using the Host Table mechanism. The Internet Architecture Board (IAB), in cooperation with the Internet Corporation for Assigned Names and Numbers (ICANN), is currently responsible for managing the Top Level Domain (TLD) name "arpa". This arrangement is documented in Appendix A of RFC 3172. This domain name provides the root of the name hierarchy of the reverse mapping of IP addresses to domain names. More generally, this domain name undertakes a role as a limited use domain for Internet infrastructure applications, by providing a name root for the mapping of particular protocol values to names of service entities. This domain name provides a name root for the mapping of protocol values into lookup keys to retrieve operationally critical protocol infrastructure data records or objects for the Internet.

The IAB may add other infrastructure uses to the "arpa" domain in the future. Any such additions or changes will be in accordance with the procedures documented in Section 2.1 and Section 3 of this document. [referring to RFC 3172] This domain is termed an "infrastructure domain", as its role is to support the operating infrastructure of the Internet. In particular, the "arpa" domain is not to be used in the same manner (e.g., for naming hosts) as other generic Top Level Domains are commonly used.

The operational administration of this domain, in accordance with the provisions described in this document, shall be performed by the IANA under the terms of the MoU between the IAB and ICANN concerning the IANA [RFC 2860].

3.5. Assignment of the .ARPA top level domain

As documented in appendix A of RFC 3172, on April 28, 2000 the US Department of Commerce, acting under the authority of its purchase order with ICANN, directed ICANN to operate the .ARPA TLD under the guidance of the IAB, as a limited use domain for internet infrastructure applications.

3.6. Name Server Requirements for .ARPA (from RFC 3172)

As this domain is part of the operationally critical infrastructure of the Internet, the stability, integrity and efficiency of the operation of this domain is a matter of importance for all Internet users.

The "arpa" domain is positioned as a top level domain in order to avoid potential operational instabilities caused by multiple DNS lookups spanning several operational domains that would be required to locate the servers of each of the parent names of a more deeply nested infrastructure name. The maximal lookup set for ARPA is a lookup of the name servers for the "arpa" domain from a root server, and the query agent is then provided with a list of authoritative "arpa" name servers.

The efficient and correct operation of the "arpa" domain is considered to be sufficiently critical that the operational requirements for the root servers apply to the operational requirements of the "arpa" servers. All operational requirements noted in RFC 2870, as they apply to the operational requirements of the root servers, shall apply to the operation of the "arpa" servers. Any revision to RFC 2870 in relation to the operation of the root servers shall also apply to the operation of the "arpa" servers.

Many of the servers that are authoritative for the root zone (or the "." zone) also currently serve as authoritative for the "arpa" zone. As noted in RFC 2870, this arrangement is likely to change in the future.

3.7. Summary: ENUM use of .ARPA

The ARPA domain is the preferred TLD for infrastructure and parameter use. The ENUM structure should be placed in a single domain subtree (see separate contribution, COM 2-11), and is expected to evolve into important Internet infrastructure, and hence should be placed there. This decision is facilitated by the MOU between ICANN and IETF and the instructions from the US Government to ICANN, which provide for IAB supervision of that domain. Despite some confusion with the name of a US Department of Defense agency, DARPA, these uses are

consistent with all of the historical uses of the ARPA domain, which have been for infrastructure purposes (initially when the hierarchical DNS was created to replace the old flat namespace of ARPANET): the domain was never used for any internal or specific DARPA purpose. Recognizing the potential difficulties with multiple infrastructure domains, the Internet Architecture Board concluded in May 2000 that all new infrastructure information was to be stored in the ARPA domain and existing infrastructure subtrees migrated there as feasible. http://www.iab.org/iab/DOCUMENTS/iab-arpa-stmt.txt provides additional context for these decisions.

The ENUM Working Group decided to follow that recommendation.

4. The selection of an operator for E164.ARPA

4.1. Introduction

This contribution is one of a series provided by the IETF to SG2 to provide background information about the IETF's ENUM Working Group deliberations and decisions. This particular contribution addresses the IETF's selection of an operator for the E164.ARPA domain.

4.2. Name server operator requirements

RFC 2870 (http://www.ietf.org/rfc/rfc2780.txt) describes the requirements for operating DNS root servers. Important DNS-based infrastructure services require that their servers be operated with the same level of attention to reliability and security that the root servers require. In addition, for an infrastructure service such as E164.ARPA some additional requirements were felt by the IAB to be important. Organizations that operate core services such as IN-ADDR.ARPA and E164.ARPA must have a history of reliable operation of DNS servers and be highly respected and known for both their relevant technical skills and their fairness and impartiality. In addition, the IAB felt that the organization that operates such infrastructure domains must be a non-profit and public-service-oriented one to remove any incentive for exploitative behavior based on profit motives that depend on, e.g., the number of records in the database even if some reasonable registration fee is charged to recover costs. The IAB also felt that they wanted an organization with good (and extensive) experience working with governments when necessary and one with experience working with the IAB and the IETF more generally.

4.3. Evaluating possible operators

The IAB researched various options for operators and came to the conclusion that the regional IP address registries (RIRs) met all of the criteria. They all had extensive experience providing and supporting infrastructure services reliably and securely and all three of them had a long history of working with the IETF.

4.4. Selecting a particular operator

Given that all of the RIRs would have met the criteria, the selection of a particular RIR required looking at other factors. The IAB concluded that RIPE NCC would be the best operator for E164.ARPA, based largely on their somewhat greater experience in running DNS servers and on their location in a neutral legal jurisdiction.

4.5. Country administration of cc subdomains

Of course, once a subdomain associated with a country code is assigned for registration and operations to an appropriately-designated entity for the associated country or numbering plan, administration of that subdomain is entirely a National Matter, with no involvement anticipated from the IAB/IETF, the E164.ARPA registry, or from the ITU.

5. Procedures to be followed by RIPE NCC

The IAB and the RIPE NCC have agreed on procedures for the latter to follow in making ENUM registrations at the country code level. Those instructions are expected to evolve as experience is accumulated. Current versions will be posted on the IAB and/or RIPE NCC web sites.

6. References

6.1. Normative references

None. This document is intended to be self-contained and purely informational.

6.2. Informative and explanatory references.

[RFC 2860] Carpenter, B., Baker, F. and M. Roberts, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority", RFC 2860, June 2000.

[RFC 2870] Bush, R., Karrenberg, D., Kosters, M. and R. Plzak, "Root Name Server Operational Requirements", BCP 40, RFC 2870, June 2000.

[RFC 2916] Faltstrom, P., "E.164 number and DNS", RFC 2916, September 2000.

[RFC 3172] Huston, G., Ed., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ('arpa')", BCP 52, RFC 3172, September 2001.

7. Security Considerations

This document provides information only and raises no new security issues. The security issues associated with the underlying protocols are described in RFC 2916.

8. IANA Considerations

There are no IANA considerations regarding this document. Sections 3 and 4 contain a record of actions already performed by IANA and partial explanations for them.

9. Authors' Addresses

Internet Architecture Board EMail: iab@iab.org

Membership at time this document was completed:

Harald Alvestrand
Ran Atkinson
Rob Austein
Fred Baker
Steve Bellovin
Brian Carpenter
Jon Crowcroft
Leslie Daigle
Steve Deering
Sally Floyd
Geoff Huston
John Klensin
Henning Schulzrinne

Scott Bradner
EMail: sob@harvard.edu

Patrik Faltstrom
EMail: paf@cisco.com

10. Full Copyright Statement

Acknowledgement

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