DRAFT WGIG ISSUE PAPER ON THE ADMINISTRATION OF THE ROOT SERVER SYSTEM

This paper is a 'draft working paper' reflecting the preliminary findings of the drafting team. It has been subject to review by all WGIG members, but it does not necessarily present a consensus position nor does it contain agreed language accepted by every member. The purpose of this draft is to provide a basis for the ongoing work of the group. It is therefore not to be seen as a chapter of the final WGIG report, but rather as raw material that will be used when drafting the report. This draft working paper has been published on the WGIG website for public comment, so it will evolve, taking into account input from governments and stakeholders.

Overview

The ability to determine the address of a the unique device on the Internet associated with a given domain name (resolution of domain names), "…is critically dependent on the proper, safe, and secure operation of the root domain name servers."[1] Thus, the oversight, administration and security of these servers, or of some alternative process, is of interest to those concerned with Internet Governance.

This paper includes two aspects of the root server system: 1) editing of the root zone files, and 2) operation of the servers. These functions, though related, are actually separate from each other. They are treated together in this paper, but may be separated in the future.

Background

More than 30 years ago, the U.S. Government began funding research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of Defense's Advanced Research Projects Agency (DARPA). ARPANET was later linked to other networks established by other agencies, universities and research facilities. During the 1970s, DARPA further funded the development of a "network of networks" that became known as the Internet.[2]

Until the early 1980s, the Internet was managed by DARPA and used primarily for research purposes. Beginning in 1987, IBM, MCI and Merit developed NSFNET, a national, high-speed network based on Internet protocols. In 1991-92, NSF assumed responsibility for coordinating and funding the management of the non-military portion of the combined Internet infrastructure. NSF solicited competitive proposals to manage key aspects of the infrastructure services.[3]

In 1992, the U.S. Congress gave NSF statutory authority to allow commercial activity on the NSFNET. This facilitated connections between NSFNET and newly forming commercial network service providers, paving the way for today's Internet.[4]

[1] RFC 2870, Root Name Server Operational Requirements, p 2, The Internet Society, June 2000.

[2] *Statement of Policy*, National Telecommunications and Information Administration, United States Department of Commerce, June 5, 1998, p. 2.

[3] Ibid, p. 3.

[4] Ibid.

Root Server Administration

According to *Webopedia*, the root server system is, "A system of 13 file servers that are distributed around the globe and contain authoritative databases that form a master list of all top-level domain names (TLDs). … Different organizations maintain the servers on the root server system."[5]

The remainder of this paper will refine this definition and explain some of the complexities of the root server system. The definition is included here as an initial introduction only.

The function of the root servers, the highest-level databases of the domain-name system (DNS), is to direct queries to the nameservers for the top-level domain names. Root servers do not route traffic and they do not even resolve traffic, but they may be accessed in certain queries that require pointing to servers that do. While, because of the distributed nature of the DNS, caching and other redundant design considerations, "…only a tiny fraction of all queries will have to be processed by the root servers…,"[6] they hold the addresses of servers on which ultimate resolution of any domain name rests.

The root servers are operated by a diverse group of organizations as shown in Table 1. The root server operators are focused on reliability and stability of the service, accessibility to all Internet users, technical cooperation and professionalism. They do not establish policy or modify data in any way.[7] The root server operators also participate in ICANN and many other technical and technical-policy meetings, thereby receiving continuous feedback from the stakeholder community.

Although the root server operator system is described as "voluntary," the organizations responsible for the root servers are professional organizations with a high level of technical proficiency and infrastructure. The diversity of software, infrastructure and operational practices of the operators adds significant robustness to the root server operations.

Currently, root server operators are not bound by any contractual agreement with ICANN or with any other governance entity; their abidance by service level requirements, root zone updates and other policy decisions is still voluntary. However, there are no documented cases in which a root zone operator has not abided by such requests.

[5] www.webopedia.com.

[6] The Internet Domain Name System Explained for Non-Experts, Daniel Karrenberg, ISOC Member Briefing #16, The Internet Society, March 2004.

[7] Presentation, The Root Server System, by Joao Damas, Internet Software Consortium on behalf of the Internet Society at WSIS, December 9, 2003.

Table 1 – Root Servers[8]

Server	Operator	Locations
A	VeriSign Global Registry Services	Dulles VA
B	Information Sciences Institute	Marina Del Rey CA
C	Cogent Communications	Herndon VA, Los Angeles, New York, Chicago
D	University of Maryland	College Park MD
E	NASA Ames Research Center	Mountain View CA
F	Internet Systems Consortium, Inc	Ottawa, Palo Alto CA, San Jose CA, New York, San Francisco Madrid, Hong Kong, Los Angeles, Rome, Auckland, Sao Paulo, Beijing, Seoul, Moscow, Taipei, Dubai, Paris, Singapore, Brisbane, Toronto, Monterrey, Lisbon, Johannesburg, Tel Aviv, Jakarta, Munich, Osaka, Prague
G	U.S. DOD Network Information Center	Vienna VA
H	U.S. Army Research Lab	Aberdeen, MD
I	Autonomica/NORDUnet	Stockholm, Helsinki, Milan, London, Geneva, Amsterdam, Oslo, Bangkok, Hong Kong, Brussels, Frankfurt, Ankara, Bucharest, Chicago, Washington, Tokyo, Kuala Lumpur
J	VeriSign Global Registry Services	Dulles VA (2 locations), Mountain View CA, Seattle, Amsterdam, Atlanta, Los Angeles, Miami, Stockholm, London, Tokyo, Seoul, Singapore, Sterling VA (2 locations standby)
K	Reseaux IP Europeens – Network Coordination Centre	London, Amsterdam, Frankfurt, Athens, Doha, Milan, Reykjavik, Helsinki, Geneva, Poznan
L	ICANN	Los Angeles
M	WIDE Project	Tokyo, Seoul, Paris

December 2004

The number of root servers cannot presently be increased to more than thirteen due to technical limitations in the design of the related protocols. However, as indicated in Table 1 above, the original thirteen root servers now appear in multiple locations through a technique known as "Anycast" that allows for "cloning" one server in multiple locations, all of which respond to the same IP address and all of which contain identical data.[9] The "cloned" servers are also known as "mirror servers". This scheme has solved a number of security issues and permits a better global distribution of root name service.[10] As of December 2004, the chart shows root servers in 84 locations, over half of which are located outside of the United States, and the number of locations will continue to grow.

Other benefits of using Anycast for root name services is that it permits a reduction in router and link resources, as standard IP routing protocols will deliver packets over the shortest path to the closest available host. This benefit keeps traffic in a local or regional context and thereby reduces

[8] Root Servers Technical Operations Association, www.root-servers.org, December 15, 2004.

[9] *DNS Root Server Mirror Service*, Internet Software Consortium, Information Document 23, Study Group 2, International Telecommunications Union, July 2003, Page 8.

[10] Ibid, Page 9.

the use of expensive international links, of particular benefit for developing countries and isolated nations.[11]

The Internet Assigned Names Authority (IANA) website at http://www.iana.org/root-management.htm describes the process for making changes to the root zone file. IANA functions are performed by ICANN through a contract with the U.S. Department of Commerce.. Requests for additions, deletions or modifications to the root zone file are submitted to IANA who determines the appropriateness of the request. ICANN (IANA) then submits the request to the U.S. Department of Commerce for its review of the process. Once the Department of Commerce ascertains that the proper process has been followed, the changes are submitted to VeriSign Global Registry Services for implementation. The changes are first applied to a 14th server or "Distribution Master Server", and then automatically propagated throughout the root server system.[12] The purpose of the Distribution Master is to maintain as secure a version of the root zone file as possible.

As the root server set to be used as reference by an ISP and its users is defined in the configuration of their name servers, each ISP and name server operator is free to rely on a different set of root servers. That could then provide the visibility of additional top level domains, or even delegate the existing top level domains to different managers. In fact, though not widely used, alternative root server systems already exist.[13] In addition, commercial services that emulate the same effect by browser plug-ins or other technical means also exist.[14]

On the other hand, some believe that alternative root systems that have been proposed over the years and generally rejected because of the instabilities and threats to the unique resolution of names in all types of Internet applications that they create. Relying on browser plug-ins and related technical means is not in the design of the DNS and is done at user risk.

While there has been a view that the adoption of competing root systems would reduce problems caused by the potential mismanagement of the current one, the users of different root systems could be pointed at different websites and services after entering the same domain name or URL. Thus, an open issue in the past has been whether the existence of alternative root server systems should be encouraged, accepted, subject to regulation, or allowed at all. At present, this discussion has been muted in favor of a single root.

[11] Ibid.

[12] *DNS Root Server Mirror Service*, Page 6.

[13] See for example the Open Root Server Confederation, www.open-rsc.org.

[14] See for example New.net, www.new.net.

ATTRIBUTION TO CATEGORIES

The administration of the root server system is applicable to the following categories: Equitable Distribution of Resources and the Stable and Secure Functioning of the Internet.

ACTORS

The administration of the root server system has been carefully evolving from one entirely centered within the U.S. to one of a more international character. The transition is occurring in a manner so as to not disrupt the stable, reliable operation of the Internet. The Actors described are as of the beginning of 2005.

United States Department of Commerce

The role of the U.S. Government in the development and management of the Internet has been previously described in the Background Section of this paper. On July 1, 1997, as part of the Clinton Administration's *Framework for Global Electronic Commerce,* the President directed the Secretary of Commerce to privatize the domain name system (DNS) in a manner that increases competition and facilitates international participation in its management.[15] The President's Directive was partly the result of a debate that had been going on for some time regarding the need for changes in the management of Internet resources. The Directive was also, in part, the desire of the U.S. Government, "…to facilitate its withdrawal from DNS management."[16]

On June 5, 1998, the Department of Commerce (DOC) published its Statement of Policy, *Management of Internet Names and Addresses,* 63 Federal Register, 31741 (1998) (Statement of Policy). In the *Statement of Policy*, the DOC stated its intent to enter into an agreement with a not-for-profit entity to establish a process for transition U.S. Government management of the DNS to such an entity based on the principles of stability, competition, bottom-up coordination and representation.[17]

On November 25, 1998, the DOC entered into a Memorandum of Understanding (MOU) with the Internet Corporation for Assigned Names and Numbers to carry out the transition noted above. That MOU, as amended, represents a record of the progress of the intended transition. The current Memorandum expires on September 30, 2006, at which time the transition is expected to be complete.

ICANN and IANA

As stated above, ICANN is a not-for profit organization to which the DOC is transitioning management of the DNS according to the terms of an MOU. ICANN collaborates with the DOC on operational procedures for the root name server system, including formalization of

[15] *Statement of Policy*, National Telecommunications and Information Administration, United States Department of Commerce, June 5, 1998, p. 1.
[16] Ibid, p. 6.
[17] Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, Paragraph II.A.

relationships under which root name servers throughout the world are operated. ICANN also collaborates with the DOC to promote best practices used by the root zone operators.[18]

Further, ICANN has committed to continue to consult with the managers of the root name servers and other appropriate experts with respect to operational and security matters relating to the secure and stable operations of the domain name and numbering system in order to develop and implement recommendations for improvements in those matters, including ICANN's operation of the authoritative root, under appropriate terms and conditions.[19]

Previously, the above ICANN functions with regard to the root server system rested with the Internet Assigned Names Authority (IANA). The IANA functions are now performed by ICANN.[20] The U. S. Department of Commerce has entered into a separate Agreement with ICANN for the performance of the IANA functions. [21]

<u>Root Server System Advisory Committee and Root Server Operators</u>

ICANN's By-laws establish a Root Server System Advisory Committee (RSSAC)[22] to advise the Board about the operation of the root name servers of the domain name system. The RSSAC considers and provides advice on the operational requirements of root name servers, including host hardware capacities, operating systems and name server software versions, network connectivity and physical environment. In addition, the RSSAC examines and advises on the security aspects of the root name server system. Finally, the RSSAC reviews the number, location, and distribution of root name servers considering the total system performance, robustness, and reliability. The RSSAC complements the coordination mechanisms described earlier of the root server operators.

<u>Internet Engineering Task Force</u>

The Internet Engineering Task Force (IETF) provides engineering standards with regard to the root server system to ICANN and the RSSAC. [23] The current standard in this regard is RFC 2870 – Root Name Server Operational Requirements. This RFC covers a wide range of topics dealing with the servers themselves, security considerations and communications among the various parties. For the most part, however, root server operators maintain standards in excess of RFC 2870.

FORUMS

<u>Internet Corporation for Assigned Names and Numbers (ICANN)</u>

[18] Amendment 6, Memorandum of Understanding between DOC and ICANN, September 16, 2003, Paragraph II.C.5.

[19] Ibid, Paragraph II.C.6.

[20] http://www.icann.org/general/.

[21] Contract between ICANN and the United States Government for the Performance of IANA Functions, 17 March 2003, Section C.2.1.1.2.

[22] By-laws of the Internet Corporation for Assigned Names and Numbers, Section XI.2.3, April 19, 2004

[23] RFC 2870, page 2.

As stated previously, ICANN collaborates with the DOC for the administration of the root server system. Together they develop policy and make decisions that affect the operation and security of the root servers. The description in these paragraphs combines general background information about ICANN and its formation with more specific information applicable to its role as a forum where governance aspects of the root server system are collaboratively and openly discussed.

The process leading to the decision to transition many Internet management functions, including administration of the root server system, to ICANN was open, transparent and consultative. On July 2, 1997, the DOC issued a Request for Comments (RFC) on DNS administration. The RFC solicited public input on issues relating to the overall framework of the DNS administration, the creation of new top-level domains, policies for domain name registrars, and trademark issues. The solicitation was open to any commenter, including foreign individuals, entities, and governments. More than 430 comments were received comprising over 1500 pages, some from foreign sources.[24]

On January 30, 1998, the National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce, issued for comment, *A Proposal to Improve the Technical Management of Internet Names and Addresses.* The proposed rulemaking, or "Green Paper", was published in the Federal Register on February 20, 1998, providing additional opportunity for public comment. Again, comments were welcome from any source, including foreign individuals, entities or governments. More than 650 comments were received.[25]

ICANN's By-laws lay out core values of the organization that are important to understanding the transparency and democracy of the organization.[26] Those that are particularly applicable to the administration of the root server system are:

> - Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet.
>
> - Seeking and supporting broad, informed participation reflecting the functional, geographic, and cultural diversity of the Internet at all levels of policy development and decision-making.
>
> - Employing open and transparent policy development mechanisms that (i) promote well-informed decisions based on expert advice, and (ii) ensure that those entities most affected can assist in the policy development process.
>
> - Making decisions by applying documented policies neutrally and objectively, with integrity and fairness.
>
> - Acting with a speed that is responsive to the needs of the Internet while, as part of the decision-making process, obtaining informed input from those entities most affected.

[24] *Statement of Policy*, Page 1.
[25] Ibid.
[26] ICANN By-laws, Section I.2.

- Remaining accountable to the Internet community through mechanisms that enhance ICANN's effectiveness.

- While remaining rooted in the private sector, recognizing that governments and public authorities are responsible for public policy and duly taking into account governments' or public authorities' recommendations.

Further, Articles III and IV contain specific requirements with regard to Transparency and Accountability. The Board of Directors is composed of 15 voting members and 6 non-voting liaisons. The voting members are required to be geographically diverse.[27] No government official may be a member of the Board of Directors of ICANN.[28]

Root Server System Advisory Committee to ICANN

The RSSAC advises the Board of ICANN about the operation of the root server system. Membership in the RSSAC consists of (i) each operator of an authoritative root name server, and (ii) such other persons as are appointed by the ICANN Board.[29] There are no limitations regarding the number of members of the RSSAC nor of their qualifications. In addition, the RSSAC picks one member annually to represent it on the Board of Directors and one member to represent it on the Nominating Committee.[30]

The RSSAC generally meets in conjunction with IETF meetings.

Internet Engineering Task Force

"The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet."[31] It is the principal body engaged in the development of new Internet standard specifications. Meetings are open to any interested individual, including representatives of government and the civil society.

The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year.

Its mission includes:[32]

- Identifying, and proposing solutions to, pressing operational and technical problems in the Internet;

- Specifying the development or usage of protocols and the near-term

[27] ICANN By-laws, Article VI.2.
[28] Ibid, Article VI.4.
[29] Ibid, Article XI.2.3.
[30] Ibid.
[31] www.ietf.org.
[32] Ibid.

architecture to solve such technical problems for the Internet;

- Making recommendations to the Internet Engineering Steering Group (IESG) regarding the standardization of protocols and protocol usage in the Internet;

- Facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community; and

- Providing a forum for the exchange of information within the Internet community between vendors, users, researchers, agency contractors, and network managers.

Detailed information about the operation of the IETF and its standards development process can be found in RFC 3160, The Tao of the IETF – A Novice's Guide to the Internet Engineering Task Force, August 2001.

GOVERNANCE MECHANISMS

The preceding sections, taken together, describe the current governance mechanism of the Root Server System.

SWOT[33] ANALYSIS

Strengths

- Diversity of root server operators creates robustness through diversity of operating systems, software versions, institutional arrangements, training, etc.
- Strong communications and proven commitment within the community of root server operators provide prompt, secure and flexible responses to challenges.
- Oversight authority of root server system is clearly established by MOU with the U.S. Department of Commerce.
- Multilateral, expert advisory system is available through RSSAC and IETF[34].
- The root server operators work under technical and not political criteria.[35] This means that their primary objective is to insure the proper functioning of the Internet.
- Proven record of stability and security.

[33] Strengths, Weaknesses, Opportunities and Strengths analysis – The classification and analysis of factors that will impact organizational effectiveness.

[34] One commenter disagreed that the RSSAC and IETF were multilateral in its broadest sense. According to the online version of the Oxford Dictionary, the most common definition of "multilateral" is ,"Involving three or more governments, organizations, etc., esp. as parties to an agreement, summit, etc." Thus, since there appear to be no prohibitions to government representatives participating in the RSSAC and the IETF, both organizations would fall under this definition.

[35] One commenter felt that since the U.S. Department of Commerce controlled changes to the root zone file that were propagated to all other root servers that, in fact, the root server system was operated under political criteria. The Root Server Operators do, in fact, operate under technical criteria, so the Strength, as written, is factual. However, the Commenter also has a valid point when referring to the root server system as a whole.

- Accountability of the root server operators is built from the bottom up, and works instantly and globally through the continuous contact with their various users and constituents, among which are governments, private enterprises, academic institutions and other civil-society actors, and other key operators and actors including IETF, the RIRs/NRO, ccTLD managers, etc. Among other formal elements of this accountability are the lively public discussions in which the operators engage with their constituents, and public minutes of the RSSAC meetings.

Weaknesses

- RSSAC website does not provide robust and current information about membership and activities of RSSAC.
- Lack of formal, written relationship between ICANN and Root Server Operators.
- Final U.S. Department of Commerce approval of changes to the root zone file currently is needed until the transition to ICANN is completed in 2006.
- RSSAC is advisory.
- Limited agreements between ICANN and ccTLDs, thus ICANN is not bound to take direction with regard to particular country issues from the respective country authorities.

Opportunities

- Continue to showcase an example of a public/private partnership.
- There is an opportunity to strengthen the root server operations by including new, informed actors in the dialog with them as a result of the interest raised around the world in the WSIS process.

Threats

- The Root Server Operators are a technically strong, trust-based community. Any change in the way root servers are operated, and in the institutional arrangements around them, has to be performed after careful, detailed consultations. Otherwise changes that long ago have been recognized as potentially disruptive may be implemented with negative results.
- As the root server operators are not bound by contractual agreements, they might refuse to perform changes or actions requested by ICANN or by any other governance mechanism, for reasons that suit their private interests or strategy.
- A lack of general consensus, for whatever reason, on the proper governance of the root server system might lead some stakeholders to start deploying and using alternative root systems. The use of an alternative root system would possibly result in non-uniqueness of domain name resolution and a consequent breakdown in many Internet services.
- Since ICANN is a U.S. Corporation, it could be prevented from entering into agreements with countries or root server operators in countries on the U.S. Embargo list.
- Errors in changes to the primary root server could be propagated to all others.

ADEQUACY MEASURED AGAINST CRITERIA

Table 2 below summarizes the criteria outlined in the Declaration of Principles with regard to each of the organizations involved in the administration of the root server system. Table 3 then attempts to indicate the adequacy of each of those same elements. For simplicity, the root server operators (RSO) and the RSSAC are grouped together.

Table 2 - Criteria

Org	Multilat	Transp	Demo	Coord	Govt	Civil	Busin	Other
DOC	N	N	N	N	Y	N	N	NA
ICANN	N	Y	Y	Y	[36]	Y	Y	NA
RSO/RSSAC	Y	Y	Y	N	Y	Y	Y	NA
IETF	Y	Y	Y	Y	Y	Y	Y	NA

Figure 3 - Adequacy

Org	Multilat	Transp	Demo	Coord	Govt	Civil	Busin	Other
DOC	N	N	N	N	Y	N	N	NA
ICANN	N	Y	Y	Y	[37]	N[38]	Y	NA
RSO/RSSAC	Y	Y	Y	N	Y	Y	Y	NA
IETF	Y	Y	Y	Y	Y	Y	Y	NA

With the exception of the views of some governmental actors and possibly civil society actors involvement in ICANN, the above figures seem to indicate that the organizations involved with the current administration of the root server system are adequate with respect to the Principles outlined in the Declaration of Principles. While the organizations, independently, may be individually adequate, some do not feel that that the system as a whole is adequate. Rather, they feel that the unilateral involvement of the U.S. Department of Commerce as the final approving authority of changes to the root zone file is inappropriate. As an alternative, they feel that some intergovernmental organization under the framework of the United Nations should have final authority.

[36] Governments participate through the Government Advisory Committee (GAC) of ICANN.

[37] Some believe that the current advisory status of the Government Advisory Committee (GAC) to ICANN does not provide sufficient governmental involvement in and oversight of the roles and responsibilities of ICANN. On the other hand, other governments feel that increased involvement by government is not necessary or productive. There have been no documented instances where the ICANN Board has ignored the advice of the GAC.

[38] Civil Society groups at ICANN believe that the current advisory status of the At Large Advisory Committee (ALAC) and the imbalance between commercial and non-commercial constituency groups in supporting organizations such as the Generic Names Supporting Organization (GNSO) do not provide sufficient accountability of the interests on non-commercial and individual users of the Internet. Others, on the other hand, feel that the Civil Society representatives have the same opportunity to participate in ICANN as do the commercial interests.