SOURCE: Internet Architecture Board (IAB), ISOC
TITLE: Administrative aspects of ENUM - Security
LIAISON STATEMENT
TO: ITU-T SG2

In reference to the query raised by SG2 [1] regarding studies or evaluations relative to the ability of root and .arpa servers to survive disasters and mechanisms that are used for recovery the IAB makes the following response.

With respect to the servers of the DNS root zone (the "root servers", the IETF's responsibility is as a source of technical advice and operational standards. This effort is undertaken by the DNS Operations Working Group of the IETF. The most recent outcomes from this working group on this topic is RFC 2870, "Root Name Server Operational Requirements" [2].

The IAB notes that the question being asked also refers to aspects of the operational capability of the root servers, a matter that is of interest to the Domain Name Server Operations Working Group. The charter of this group can be found at http://www.ietf.org/html.charters/dnsop-charter.html

The .arpa top level domain is operated under the arrangements described in RFC 3172 [3]. At present the .arpa domain is served by 12 root servers. This is the entire collection of root servers with the exception of a single US-based server. The operational characteristics of the .arpa domain with respect to the considerations noted in the liaison statement are therefore closely similar to those of the root server system.

Subsequent to the issue of this ITU-T liaison statement the IAB understands Jim Reid of Nominum provided a contribution to SG2 on this topic, and as this contribution is relevant to the question under study, a copy of the relevant sections of this contribution is attached here for information. We note that since this contribution all root servers with the exception of the J root server also serve the .arpa domain, and there will shortly be code diversity within the root servers, with the K server using nsd 1.0.2-rel. as of the 19th February 2003.

Leslie Daigle.
Chair, Internet Architecture Board
iab-chair@ietf.org

16 February 2003

References

[1] ITU-T SG2 Liaison Statement, Administrative aspects of ENUM - Security http://www.ietf.org/IESG/LIAISON/COM2-055.htm.

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

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

Attachment

Extract from a contribution from Jim Reid, Nominum to SG22:

1 Introduction

Concern has been expressed within Study Group 2 at the stability and robustness of the name server infrastructure for the top-level domain, .arpa. The IAB/IETF have determined that this domain will be used for infrastructure resources such as the reverse lookup of IPv4 and IPv6 addresses and E.164 telephone numbers. See RFC 3172. This document discusses the current name server setup for .arpa and the changes that can be expected to occur in the coming months.

2 Current name server infrastructure for .arpa

Until late November 2002, the .arpa zone was served by 9 of the 13 internet root servers: a-i.root-servers.net. These name servers are operated by a variety of organisations -- universities, not-for-profit institutions, commercial companies, government agencies and the US military.

This diversity provides robustness as there is no single source of funding for operating or administering these servers.

Furthermore there is no one set of operating and administration procedures which might prove to be a potential single point of failure. Eight of these servers are in the USA, 4 in California and 4 in the Washington DC area. The remaining server, i.root-servers.net, is in Stockholm. All of these servers run on a diverse set of hardware and operating system platforms, eliminating these as potential single points of failure.

Currently, all these name servers run the same DNS software, BIND, though there are plans to introduce other DNS implementations to provide a more diverse code base. This will prevent a catastrophic failure if an error or vulnerability is found in BIND. All 9 of these servers are configured and operated in accordance with RFC2780. They do not serve other zones (apart from the root and root-servers.net).

Recursion is disabled which makes the servers immune from cache poisoning attacks. Great care is taken when new copies of the root, arpa and root-servers.net zone files are loaded on to the name servers. The name servers are monitored round the clock.

They are also continually checked from a number of remote locations on the internet. This process detects trouble that might occur from routing, congestion or connectivity problems which could make the servers appear to be unreachable from large parts of the internet even though the name servers themselves are alive and responding to queries as normal.

The name servers are located in secure facilities, typically internet exchange points or co-location centres. Physical access to the buildings and systems is strictly controlled. Multiple network connections from different providers are available. The facilities have uninterruptable power supplies backed by generators to guard against failures of the public electricity supply. Adequate air conditioning and fire prevention measures are in place. To reduce the risk of network failure, the name servers have multiple logical and physical connections to the internet. Access to these high bandwidth links is provided by high-speed routers.

These also have extensive packet filtering and access control mechanisms to isolate the servers from excessive or malicious traffic. This provides some protection from distributed denial of service (DDoS) attacks which are often carried out against the root and .arpa servers. A benefit of having these root servers also serve .arpa is that the expertise and experience for dealing with these DDoS attacks can be concentrated where it is most needed.

It is hard to conceive of a DNS infrastructure which could be more robust and highly available than the current internet root and .arpa servers. The operators of these servers are technically knowledgable, take their responsibilities very seriously and have many years of experience running this critical infrastructure. Great care has been taken to avoid single points of failure. There are frequent reviews and audits of procedures and operations which are sometimes adjusted to take account of lessons learned after concerted DDoS attacks on the servers and related network equipment. This self- correcting behaviour further enhances the overall stability and security of the root server system.

By implication, the .arpa name servers benefit from this too.

One perceived weakness with the current infrastructure is the lack of geographic diversity. This may be a problem because of the potential impact of a natural disaster: California is an earthquake zone. Siting the .arpa name servers in other locations could mitigate the impact of an earthquake or flood. However it is not clear that for internet users other locations would be better in terms of packet round trip times, hop counts and so on. Most of the transcontinental links and major providers tend to concentrate their connections at these exchange points and co- location facilities on the east and west coast of the USA. Routes on the internet do not respect national borders. In one example, the author found that traffic between two UK-based ISPs was routed via PAIX in California! Although both ISPs had a presence at the London Internet Exchange, they chose not to exchange routing data with each other there. It may be that a name server in say Silicon Valley has better reachability and packet round trip times for most Asian clients than a server in say Singapore. For instance it is common to find that internet traffic between two countries in the Asia-Pacific region travels via California because that is the way the high-capacity links used by carriers and ISPs routing policies are arranged. Another benefit of having these root servers also serve .arpa is a speed up in DNS resolution and reduction in traffic. If one of these servers is queried for a domain name in e164.arpa, it can return a referral to the e164.arpa servers directly. If the servers did not do that, they would return a referral to the .arpa name servers. The name server making the lookup would then have to query one of the .arpa servers to find out the names and addresses of the e164.arpa servers. Having the root servers also serve .arpa provides a convenient short cut which saves resolution time and the number of queries needed to resolve an infrastructure domain name in .arpa.