INTRODUCTION

The Domain Name System (DNS) is a critical Internet infrastructure layer which allows the operation of other layers above it, including end-user applications, such as websites, emails, instant messaging, etc. The DNS is beneath each of these technologies, supporting and allowing real-time, dynamic changes in order to adapt to traffic, avoid attacks, balance load, etc.

Being such a critical system, it is important to be concerned about its proper operation at a country level, because it is one of the foundations for community Internet presence. Every day people become increasingly dependent on Internet, and we must be up to this by providing improved DNS robustness, and redundancy, protecting against failures and unexpected events for which there are proven techniques to safeguard DNS operation.

That is why certain defined metrics to objectively measure correct compliance with safety standards and DNS robustness have been defined. These measures, although not required or requested by any domain name registry, are indeed important to deliver quality service. Having a complete view of the DNS status based on these metrics provides an overview of the current DNS situation, and allows us to compare it over time by means of recurring measures. In addition to estimating improvements throughout time, it is possible to take long, and medium-term corrective actions that should be reflected in enhancements to measurements.

The Latin American DNS Observatory is an attempt to obtain continuous and objective measures of known DNS parameters at the regional domain name level in order to get information and reports to enhance the management of this significant resource.
DATA

For a comprehensive measurement, the list of all domain names in the region is necessary. In this first preliminary report, a public, alternative source—the “Alexa 1M website list” which provides a ranking of the million most popular websites on the Internet—was selected, and it was filtered in order to obtain only Latin American domain names. The Observatory was supplied with this list of domain names, and the actions covered in this report were taken.

This Alexa list serves as a prototype, however, the results are not comparable to a full regional analysis. Alexa domains share certain unique characteristics that cannot be extrapolated to other domains. Since they are highly popular sites, they are expected to have better infrastructure than the more ordinary domains, so they actually represent an “upper threshold” in terms of measures.

In short, it is important to state that these results will not be very similar to the final report, but they constitute a sample which, as proof-of-concept, allows to analyze the types of metrics and their behavior.

Another relevant point is that results are grouped taking into account the entire region. No division or comparison per country is done, since the goal is to determine regional trends, and not to delve into the each ccTLD reality.
HOW THE OBSERVATORY WORKS

Based on this LAC domain name list, a data collector located in Santiago de Chile is supplied, which regularly (once a week) runs all the name servers of each of these domains performing DNS queries that help tracking these metrics. It also uses other sources of information (e.g. ASN autonomous numbers) to complete another sort of analysis.

With this data, a Big Data repository is created, and it is quarterly summarized, plotted and analyzed in order to draft the report.
Results

1. Total of domains

According to statistics provided by LACTLD [1], the organization gathering Latin American and Caribbean domain name registries together, there are over 8 million domain names in the region. In the Alexa list, over 30 thousand web site names can be found in the region, amounting to 0.38% of the total.

For this analysis, 31,872 domain names in the LACTLD region [2] were analyzed.

2. Amount of NS per domain

In order to deliver redundancy for the proper and prompt resolution of a domain name, the DNS allows “name servers” (NS) – that is, end servers responsible for the name–IP number translation – to be defined. The standard indicates that there should be at least two NS per domain [3]. Some registries, due to contractual policies, demand these two servers to be defined, but others leave it at the domain name owner’s discretion. In any case, at this stage of Internet development, two NS are considered to be not enough, and the minimum should be three [4]. The right amount will depend on the use given to the name, each NS capacity, and their location.
As shown in the graph, there is a correct good practice implementation, as the average is higher than three NS per domain. However, there is a large amount (38%) which only has 2, and although this complies with the recommendation, it is too risky.

It is worth noting that such a good result may be influenced by the data coming from Alexa domains, thus representing the most visited sites, and therefore the ones better prepared in terms of infrastructure. A more complete and diverse regional sampling is expected to reduce this average.

3. Amount of ASN per domain

The NS number per domain represents a first approach to the DNS status in terms of robustness and redundancy. However a second and deeper look allows to distinguish how distributed these NS are at a routing level. There are certain domains with 3 NS, which would indicate they are pretty resilient, but these 3 NS are in the same data center, or one next to another, or even sharing the same physical device! Thus, believing those 3 NS will turn the domain safe is just a wishful thinking. Said domain remains being vulnerable to localized power cuts, linking, etc. For this reason, the “ASN” metrics allows to be more rigorous and to count the number of autonomous systems resolving the domain. Autonomous systems represent different organizations, so having NS in more than 1 ASN indicates that the name servers are actually in different places, with different routings, and therefore, they do provide diversity.
Here we see that, unfortunately, the previous good result of 3.4 NS per domain is somewhat misleading from the resilience point of view. Almost 80% of domains have their NS in 1 single autonomous number ASN meaning they are in the same organization and physical location. This turns the domain very vulnerable to shut downs due to problems at the organizational level. That 16% having their NS in 2 autonomous numbers is much more robust, because failure probability in two organizations is much lower.

4. Server distribution per country

Following further analysis of the domain NS location, the physical location at a country level is analyzed.

The result is quite similar to that of the ASN number with almost 80% having all NS in the same country, and 20% in two countries. Once again, having different NS, if possible, in more than one country is advisable, considering that Internet interruptions have already occurred at national levels, and that they can be resolved by this mechanism.
To complete this analysis on NS per domain, here we see a comparative graph of the 3 metrics mentioned above:
5. IPv6 use

The domain name system, being a critical infrastructure for Internet, should be one of the pioneers to be deployed in the new IPv6 protocol, in order to provide support to all applications depending on it. For each domain name, we have analyzed whether their NS have addresses in this new protocol (AAAA record, and IPv6 connectivity):

Unfortunately, the adoption of this new technology is quite low. More than 50% of domain names in the region have no NS reachable by IPv6, which means that these domain names will not work with networks totally connected via IPv6. 12% of domain names have, at least, one, and 26% have two name servers on IPv6.
From a more global overview, 92% of the total NS in the region uses IPv4, and 8% uses IPv6.
6. DNSSEC use

Security extensions to the DNS, known as DNSSEC, allow adding data authenticity, and integrity properties to this technology. Therefore, it is possible to guarantee that the information obtained has not been modified on its way, and that it comes from a real and authoritative source. Thanks to DNSSEC, mitigation of different attacks, and improvement of overall confidence in Internet are possible.

Only 5% of the analyzed domain names have DNSSEC activated.
Conclusions

In terms of basic metrics, the results obtained for the number of name servers per domain are good, and the results in the terms of distribution per autonomous system and country diversification are not that good. This leads to further progress in improving the robustness of our domain names system in the region, by this sort of research. Furthermore, comparison throughout time will pave the way for reviewing whether incentive and education policies are delivering the expected results.

However, progress in new technologies, such as IPv6 and DNSSEC, is just beginning. It is not an exclusive issue from our region. Similar results are found worldwide. It is important to join campaigns from other regions, and to continue deploying these important technologies.
APPENDIXES

A. Glossary

DNS: Domain Name System Architecture allowing the association of host names, such as www.example.com and an IP address such as 2001:1398::1 or 200.7.7.3.

NS: DNS system name server. This document refers to one of the authoritative servers controlled by the domain name holder.

Domain: Subdivision in the labels of a host name representing a single administrative unit.

IP: number representing a service location in Internet. There are two types: version 6 (IPv6) and the old version 4 (IPv4).

ASN: Autonomous System Number – it is an identifier representing an organization within Internet in charge of the routing of information among different servers.

DNSSEC: DNS security extensions that allow to deliver authenticity and integrity in the answers.

B. Bibliography

[2]: The members of LACTLD at the time of the study are the following ccTLDs: ai, ar, aw, bo, br, bz, cl, co, cr, cu, cw, do, ec, gt, gy, hn, ht, mx, ni, pa, pe, pr, py, sv, uy, and ve.
[3]: RFC1912, “Common DNS Operational and Configuration Errors”
[4]: RFC2181, “Selection and Operation of Secondary DNS Servers”
C. Acknowledgments

This study was created as a project of the Strategic Plan for the ICANN LAC region. The original design group was composed by Alejandro Acosta (LACNIC), Juan Manuel Rojas (LACRALO), Antonio Alberti and Victor Hugo Fernandes (INATEL), and Hugo Salgado (NIC Chile) as a leader. This group defined the metrics to be analyzed and the collection mechanism.

We appreciate the support provided by ICANN by donating a server where the active collector has been installed for measurement, and storing data.

Regarding the support obtained for data analysis, we recognize the help of NIC Chile Labs, especially its director Javier Bustos, and engineer Maite González.

Finally, we would like to thank the support, and trust of the ICANN team, especially Rodrigo Saucedo, and Rodrigo de la Parra, together with LACTLD executive director, Carolina Aguerre.

The data collection tool used is DNSdelve, which is part of the DNSwitness suite, created by AFNIC, and made available to the community.

D. Author and contact

Hugo Salgado Hernández
Project Engineering
NIC Chile - University of Chile
Miraflores 222, Floor 14, Santiago, CL
hsalgado@nic.cl

Version 1, August 22nd, 2016