Use of DNS Root Servers in Latin America

Measurements and a Historical Analysis of the Behavior of DNS Root Servers

Hugo Salgado

October 2019

lacnic

INTRODUCTION

DNS root servers are critical services for the basic operation of the Internet. They allow addressing and locating websites, email mailboxes, mobile applications, etc. For their proper operation and response speed, root servers must be located as close as possible to end users.

Since 2003, both the organizations that manage root servers as well as different regional Latin American organizations, such as the Latin American and Caribbean Internet Addresses Registry (LACNIC) and its +RAICES Project, have been undertaking efforts to install copies of these servers in regions that are far from the classic location of these services. To date, such efforts have resulted in the installation of more than a thousand such copies worldwide.

This study is the first of its kind conducted in our region to measure the results of these years of efforts. The historical data available since 2013 has made it possible to assess the improvement in the locations where copies have been installed, as well as to detect locations and regions where the projects should focus in the future.

CONTENT OF THE REPORT

ROOT SERVERS AND THEIR IMPORTANCE

The DNS service allows website addresses, email messages and multiple other Internet services to be correctly translated into "IP" addresses so that they can be reached by the servers routing traffic. It is a critical and essential service.

This service originally dates back to 1985 and has accompanied the exponential growth of networks and Internet services. The DNS owes its success to its essentially distributed and decentralized nature: distributed because there are multiple, redundant ways to obtain the service, which increases its effective speed, performance, robustness and resilience; and decentralized, as it allows different organizations to be responsible for different labels in the DNS so that they can each have the independence and prerogative to manage their own space as they see fit.

To achieve this, it was decided that the DNS would be a series of hierarchical labels with the root domain at the bottom, which would branch out to higher levels just as the branches of an actual tree. Because the hierarchy is delegated from the root upwards, this is generally represented as an inverted tree, with the root at the top supporting descending branches with the delegation of the administration for each label.

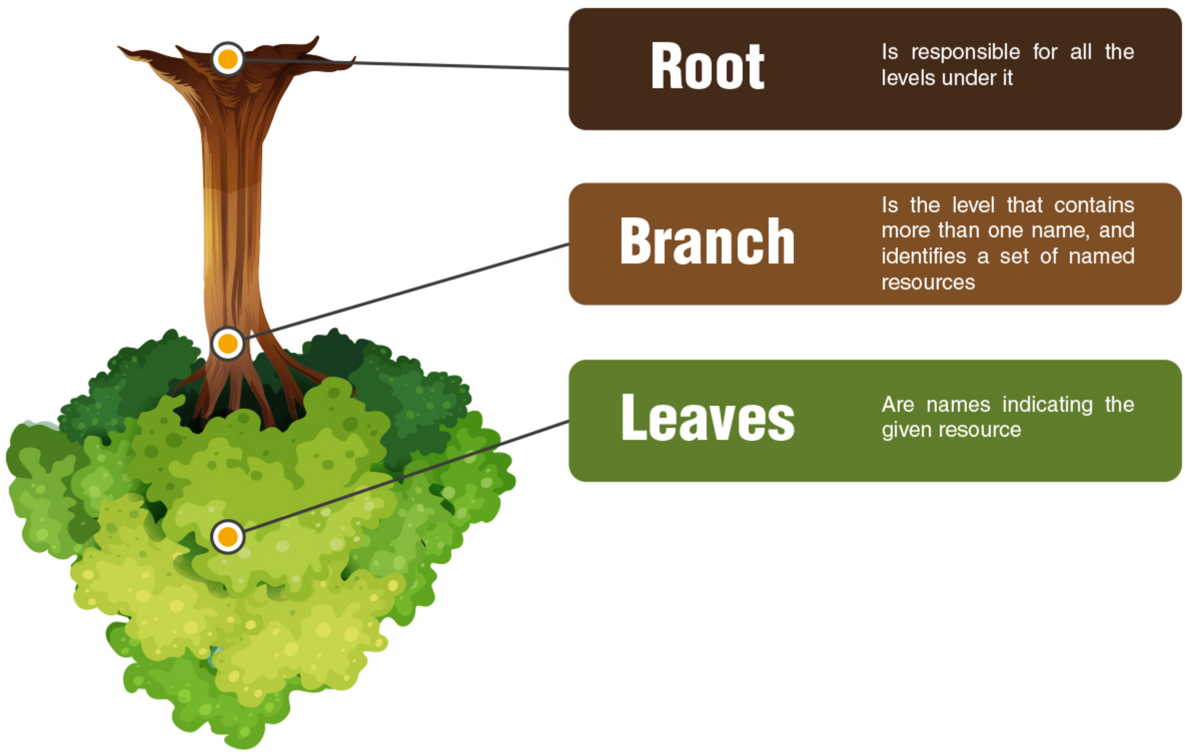

Figure 1: Representation of the hierarchical inverted tree structure of the DNS
By Jane Kruch. Own work. [cc by-sa 3.0 https://commons.wikimedia.org/w/index.php?curid=31749683]

This structure is what has allowed a robust and effective DNS from the time when there were just a few hundreds of servers connected to the Internet, to the 4.5 billion estimated users in 2019.

However, this structure has a critical and sensitive element: its root. This is why, from the very beginning, it was decided that the root of the DNS would be distributed among twelve different organizations[1]. Each of these organizations would manage one root server, which in turn would be named with a different letter of the alphabet. The number twelve was not selected at random, but instead represents the maximum number allowed by the size of the messages at the time. These twelve organizations maintained their servers for almost twenty years until the explosive growth of the Internet led to the decision that adjustments and additional copies would be necessary. As a result, the features of Internet routing enabled a technology known as Anycast, which allows each of these twelve letters to be subdivided into a cloud of nodes at different physical locations, so it is possible to continue to scale up the service. Thus, for example, the “F” DNS server, originally a server located in California (USA), now includes 241 copies in more than 90 different countries, each of them capable of serving their own region.

These particular efforts by each organization were also supported by regional organizations such as LACNIC and its +RAICES Project created in 2004, which promotes the deployment of root server copies in the region of Latin America and the Caribbean (LAC) by providing communication, coordination and contact among organizations willing to host a copy and root server administrators, and even by offering financial support to purchase the equipment and manage its installation. As a result, +RAICES has already installed 26 copies in our region, it launches an annual call for proposals for organizations willing to host a copy, and a committee selects which proposals will be worthy of support.

[1] More information: <https://root-servers.org/>.

RESEARCH METHODOLOGY

This goal of this study is to provide specific figures on the improvements that the installation of root server copies has represented for our region, by conducting a historical analysis of performance measurements.

In addition, these figures also allow identifying which regions still maintain lower standards, which in turn will allow better focusing the various efforts and results.

The data we will use is the information maintained by the European organization Réseaux IP Européen (RIPE) as well as by its RIPE Atlas project, a global network of measurement probes installed worldwide by volunteers and which are constantly measuring and analyzing information they gather from important elements of Internet infrastructure such as root servers. A little over a thousand RIPE Atlas probes have been installed in the countries of our region, a figure that is still low compared to the coverage achieved in other regions such as Europe and North America, but which still provides a relevant overview.

It is also important to call on additional volunteers to host RIPE Atlas probes in the countries of Latin America and the Caribbean. The probes are autonomous devices designed to be installed by regular users in residential connections and to operate autonomously without the users' supervision. Having a larger number of probes in our region will contribute to this and other studies that will benefit us all[2].

From a more technical point of view, the specific measurements analyzed in this study are the normal DNS queries over UDP for IPv4, using class CHAOS, type TXT and QNAME version.bind from each of the probes to each of the root servers {a-m}.root-servers.net. Representative samples were taken of these measurements. Each measurement was performed every 12 hours.

[2] More information: <https://atlas.ripe.net>.

RESULTS

REGIONAL RESPONSE TIMES FOR EACH ROOT SERVER

A first analysis averaged the response times — the historical round-trip times (RTT) — of all the probes in the region when querying each root server.

Despite being quite a rough measurement and one with many peculiarities due to the diversity of the region, it provides a first overview of the evolution of each root server and allows immediately identifying the letters with the best and worst performances.

In the following charts, each point and color represent an average measurement for each probe over time. The x-axis represents time, while the y-axis represents response times in milliseconds up to 300 ms, a number that represents a typical waiting time limit.

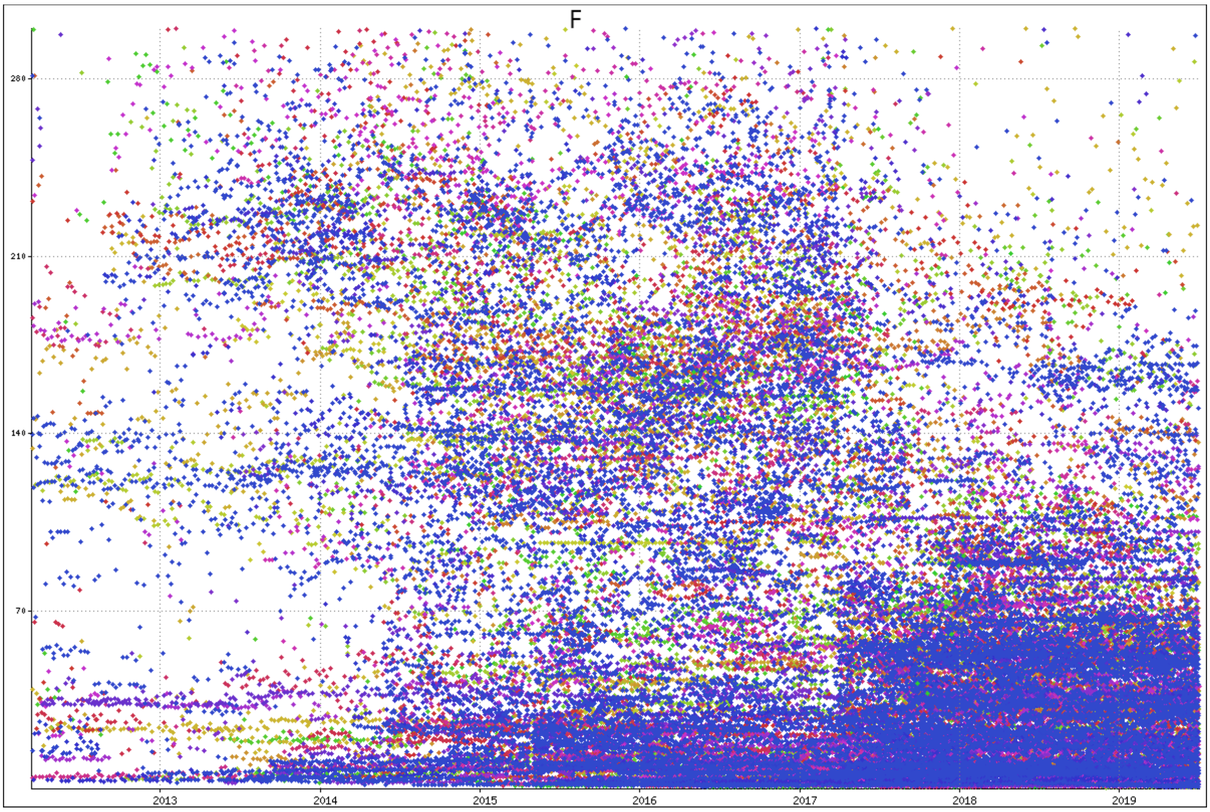

Figure 2: Historical response times from LAC to the F-root server.

This scatter diagram shows the measurements for the F-root server and immediately allows us to see that during the early years (towards the left of the chart) very few probes were available. Then, beginning in 2014, the figure shows more probes, yet their response times are scattered, which means there was a high variability. Finally, as the data approaches 2019, the points begin to concentrate in the lower part of the chart, which indicates a good result, as it represents lower response times and less variability, which in turn is indicative of the stability of the responses. In general, the lower and more concentrated the points on the scatter diagram, the better the scenario. It is also possible to identify important moments, such as a vertical line in the first trimester of 2017 resulting from a sudden improvement. This likely represents the installation of a copy of the F-root server in our region, a fact that will be verified against official data obtained from Internet Systems Consortium, the corporation that operates the F-root server.

Below is a similar chart for the L-root server operated by the Internet Corporation for Assigned Names and Numbers (ICANN), an organization that is also noted for its constant efforts to deploy root server instances worldwide.

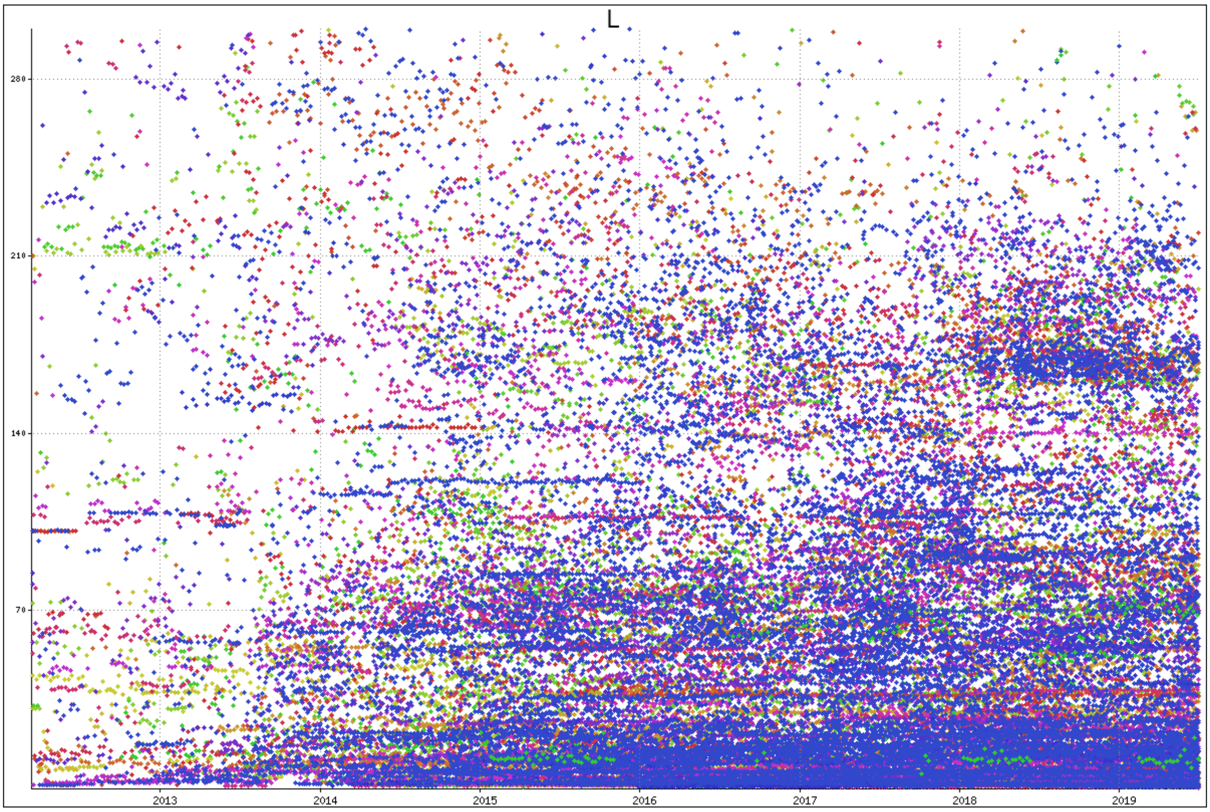

Figure 3: Historical response times from LAC to the L-root server.

This chart also shows a constant and more stable evolution over time, with response times achieving an average of less than 50 ms in 2017. However, a cluster is detected close to 150 ms in a specific region that warrants further analysis.

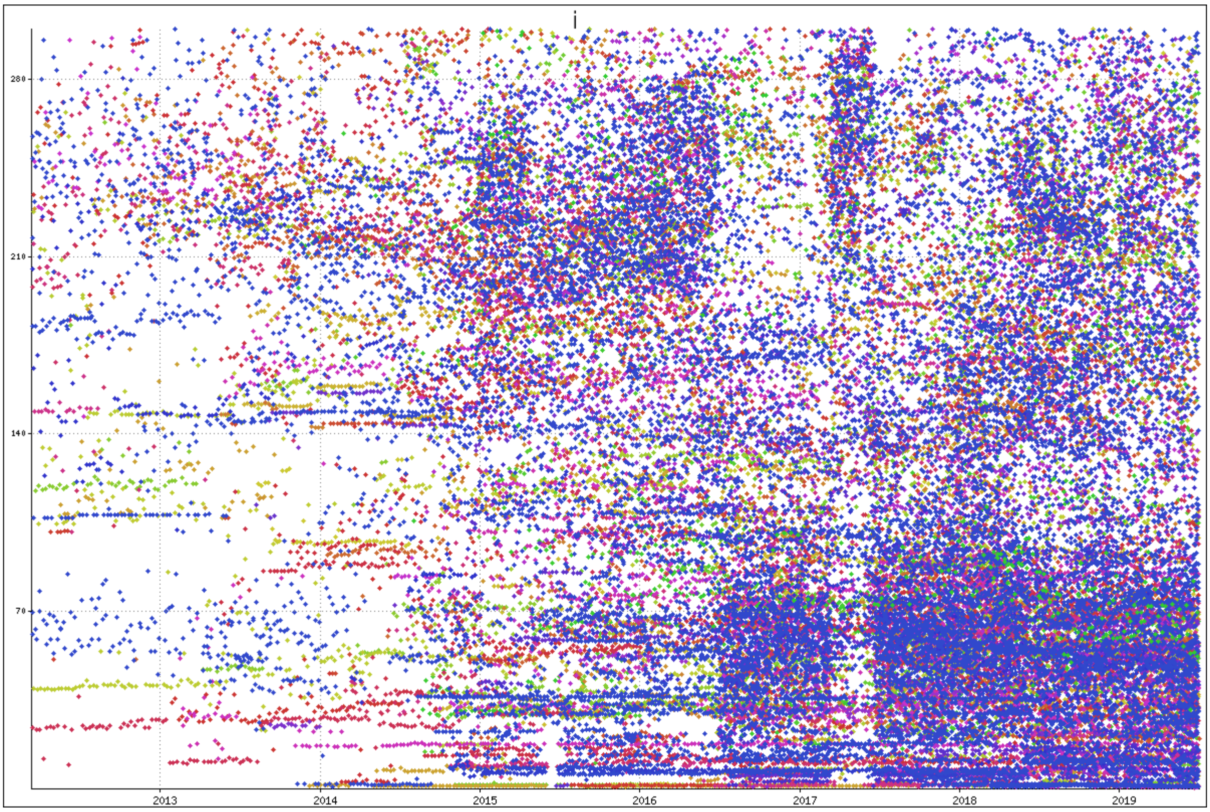

Figure 4: Historical response times from LAC to the I-root server.

In the case of the I-root server, the scatter diagram shows an important moment in mid-2016 when there was a notable improvement which later reverted in the third quarter of 2017. It is important to note that these situations may represent issues involving node failures or inefficient routing that might have increased response times for a few moments, but that were adequately solved by mid-2017.

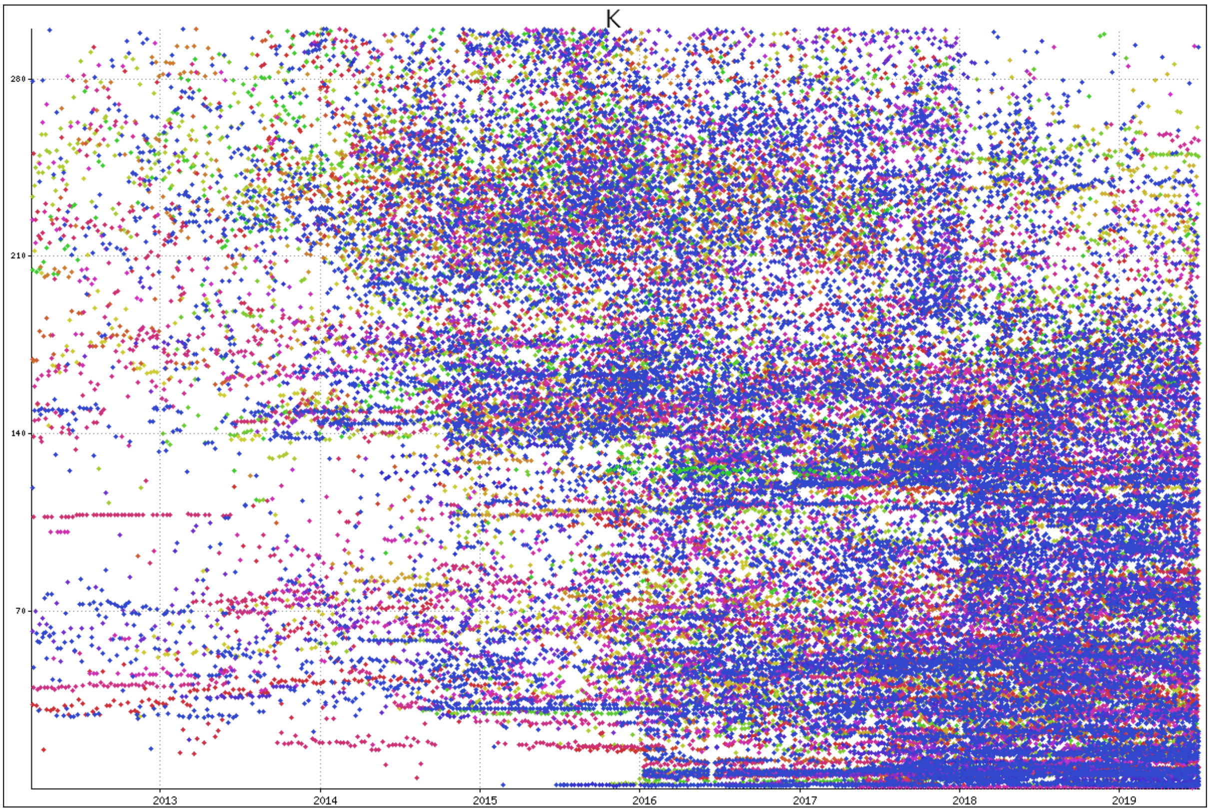

Figure 5: Historical response times from LAC to the K-root server.

The K-root server operated by the RIPE NCC is another example of a good deployment and improvements in the region, as shown in the figure above with a progressive concentration of the points towards the lower right section of the chart.

Finally, Figure 6 presents the case of the M-root server operated by the WIDE Project (Japan), which is the one furthest from the region as can be appreciated by the distance above the y-axis in the chart.

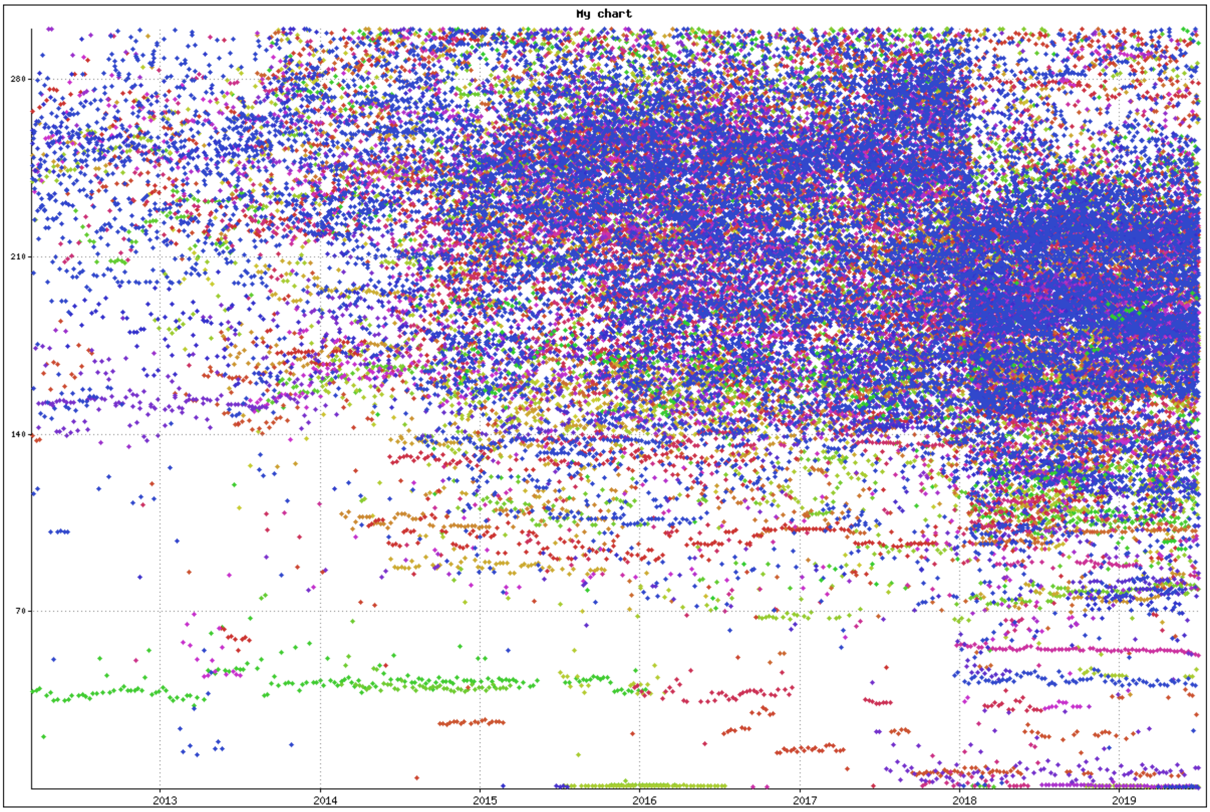

Figure 6: Historical response times from LAC to the M-root server.

However, it should be noted that it is not necessary for all the root servers (A to M) to be in close proximity. End users are served by the best root server they find, so, while it is always important and more robust to have as many root servers identified with different letters as possible, there is also no problem if some of these root servers are located far away. Each organization operating a root server can have different global deployment strategies targeting different service regions and different technologies. Instead of this being a problem, it is one of the strengths of the distributed DNS system, as it allows for diversity and avoids single points of failure.

The charts for the remaining root servers can be found in the full analysis for which a link is provided in Annex A.

NATIONAL RESPONSE TIMES FOR EACH ROOT SERVER

A second analysis also considered response time measurements (RTT), but in this case the data was disaggregated by country. Just as in the preceding charts, each point and color represent an average measurement for each probe over time. The x-axis represents time, while the y-axis represents response times in milliseconds up to 300 ms.

This level of detail allows better identifying when and where each copy was deployed. However, in this case, the difference in the coverage achieved by RIPE Atlas probes in each country is much more evident: in certain countries such as Argentina, Brazil, Chile, Mexico and Uruguay penetration rates are higher and therefore allow a better analysis, while in others probe density is very low so it is very difficult to identify or extrapolate results.

For the full results for each country, see the information provided in Annex A.

The following figure shows the response times of the probes installed in Brazil when querying the E-root server.

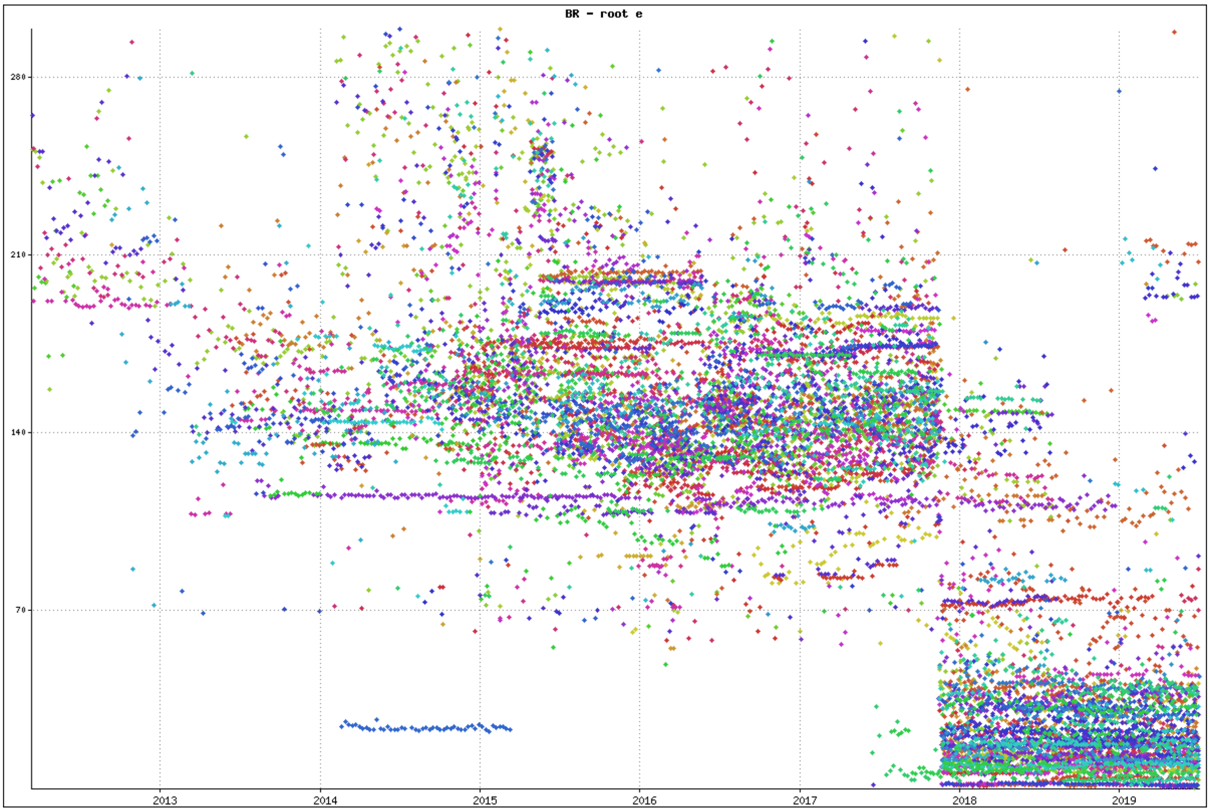

Figure 7: Historical response times from LAC to the E-root server.

This figure clearly shows that response times experienced a notable improvement in late 2017, decreasing from an average of 150 ms to less than 50 ms, which is most likely the result of the installation of an E-root server copy in the country.

Another interesting case worth noting is access to the B-root server from Chile.

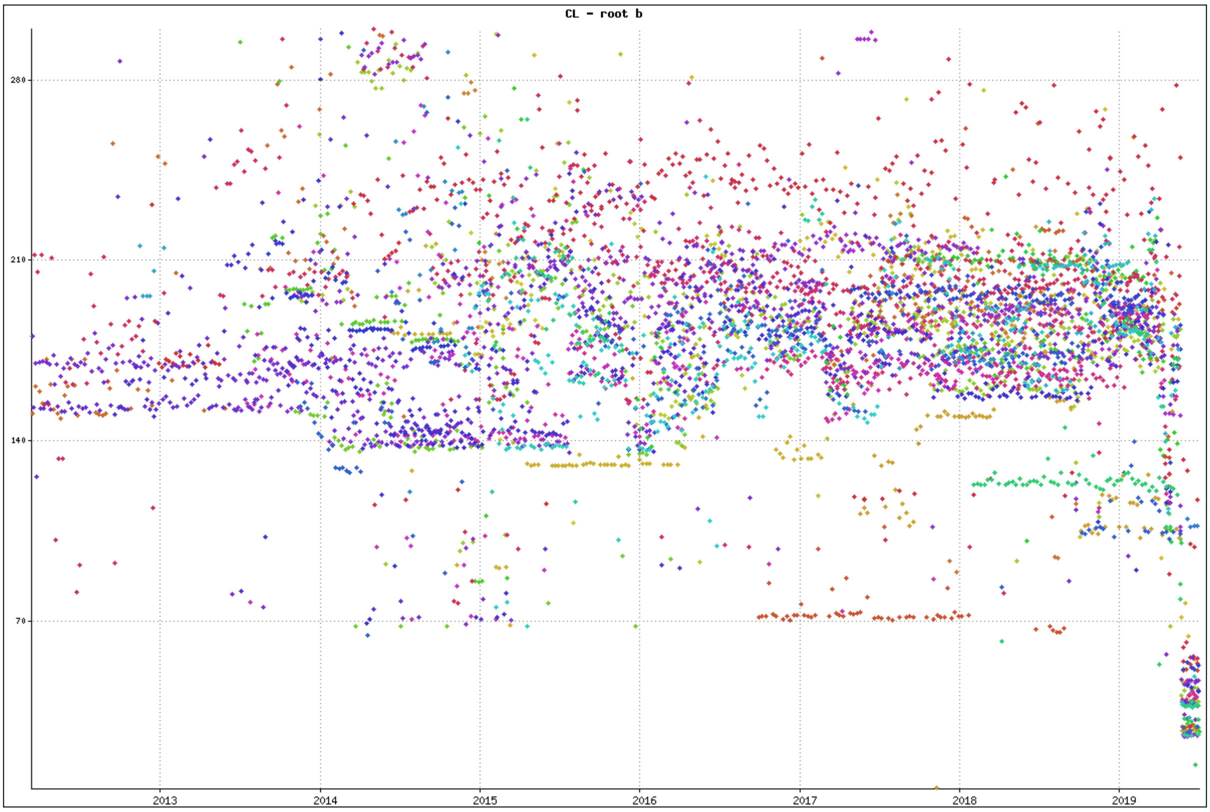

Figure 8: Historical response times from Chile to the B-root server.

This figure clearly shows an improvement in mid-2019, corroborated by the fact that the Information Sciences Institute of the University of Southern California — operator of the B-root server — first installed a node outside the United States on this date, precisely in a city in northern Chile.

Finally, Figure 9 clearly shows how a country benefits from the installation of a node in its territory. In mid-2015, LACNIC launched its +RAICES Project with the installation of a copy of the F-root server in Montevideo.

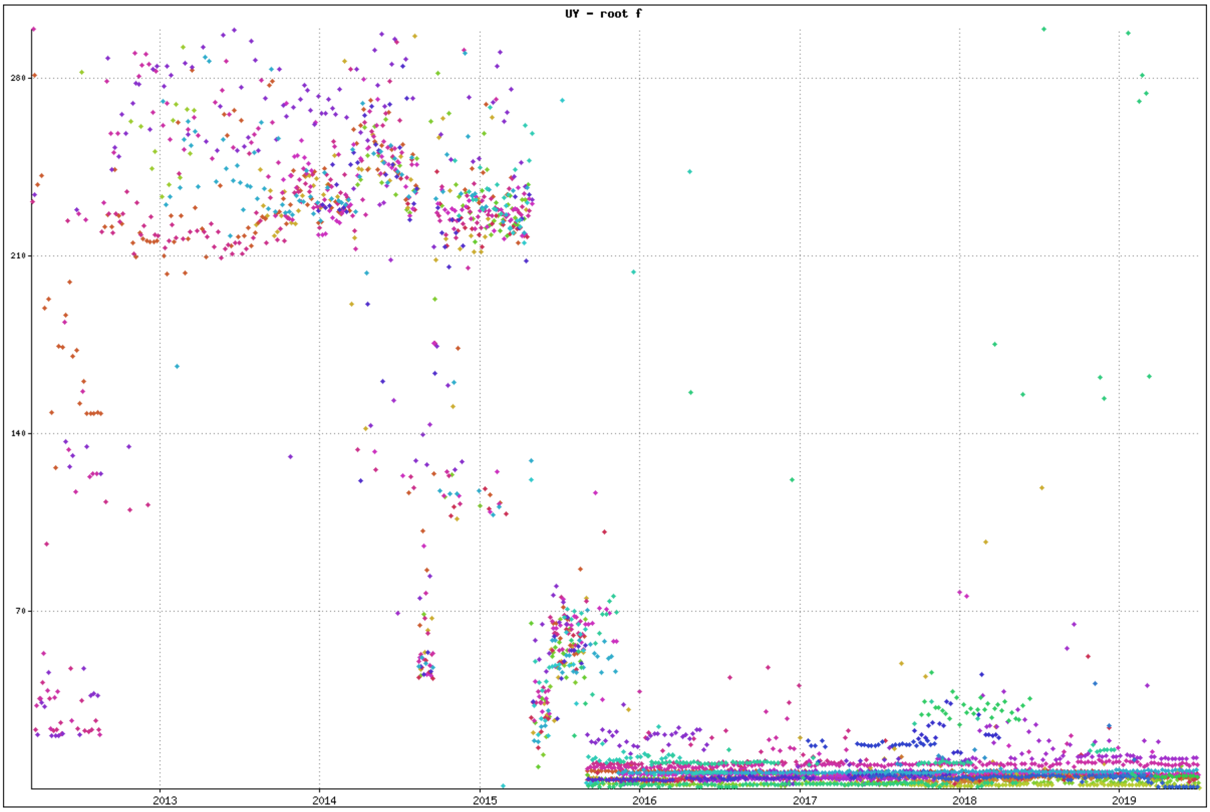

Figure 9: Historical response times from Uruguay to the F-root server.

AVERAGE RESPONSE TIMES BY COUNTRY

Another interesting measurement is the average response time from all the probes in a country to each root server. This measurement allows us to summarize the points plotted for the previous cases and provides us with numbers that allow us to estimate the improvements that have occurred during this time. In addition, by plotting each root server in a different color, we can clearly distinguish the root servers with the best performance.

The following line chart represents average response times from Chile to each root server. Each curve represents a different root server (different letter). The x-axis represents time, while the y-axis represents response times in milliseconds.

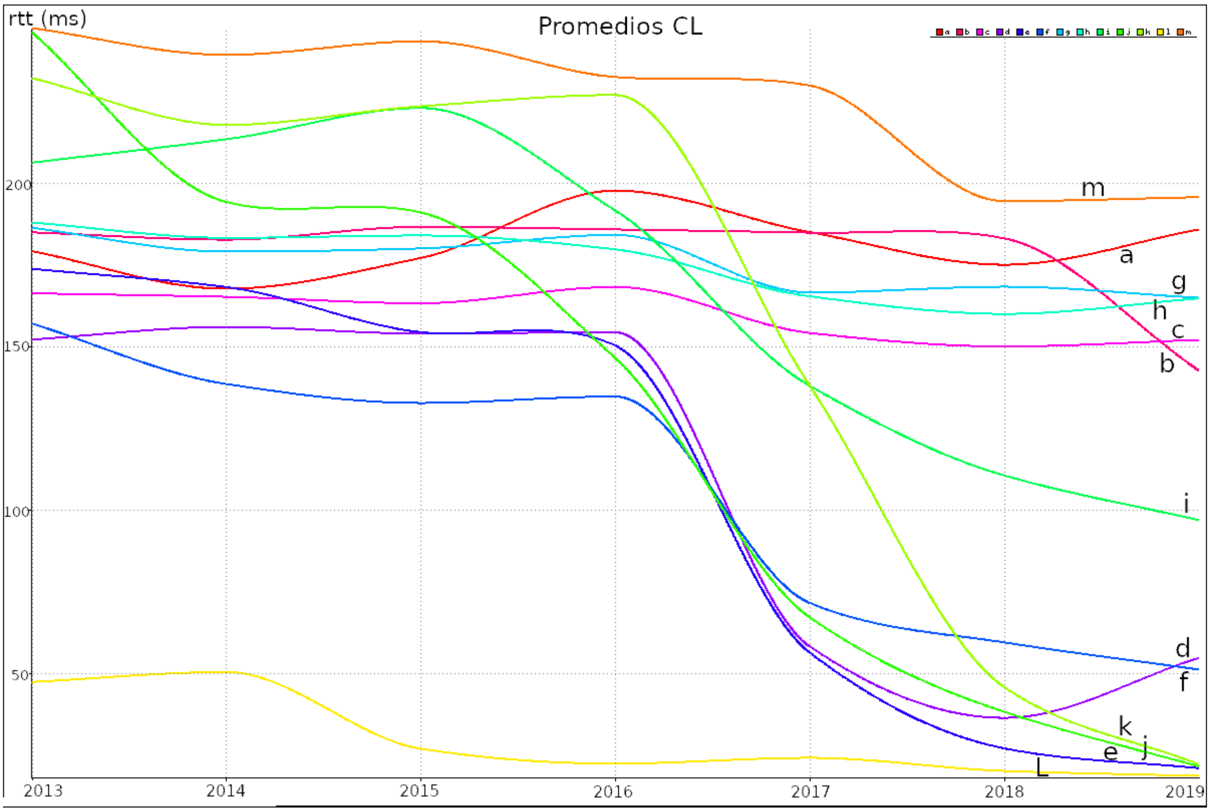

Figure 10: Historical response times from Chile to the different root servers.

The curves tend to fall towards the right of the chart, which it is a good sign and indicates that response times have decreased over time. Currently, the L-, E-, J- and K-root servers are clearly the ones with the best response times when queried from Chile, with the F- and D-root servers taking second place but still close to 50 ms, which is also quite good. The remaining servers are lagging, with the M-root server having a response time close to 200 ms, a figure indicative of a poor performance. Likewise, we can also calculate overall average response times: 182 ms for 2013 and 99 ms for 2019, a 45% reduction in response times.

The following figure shows the case of Argentina.

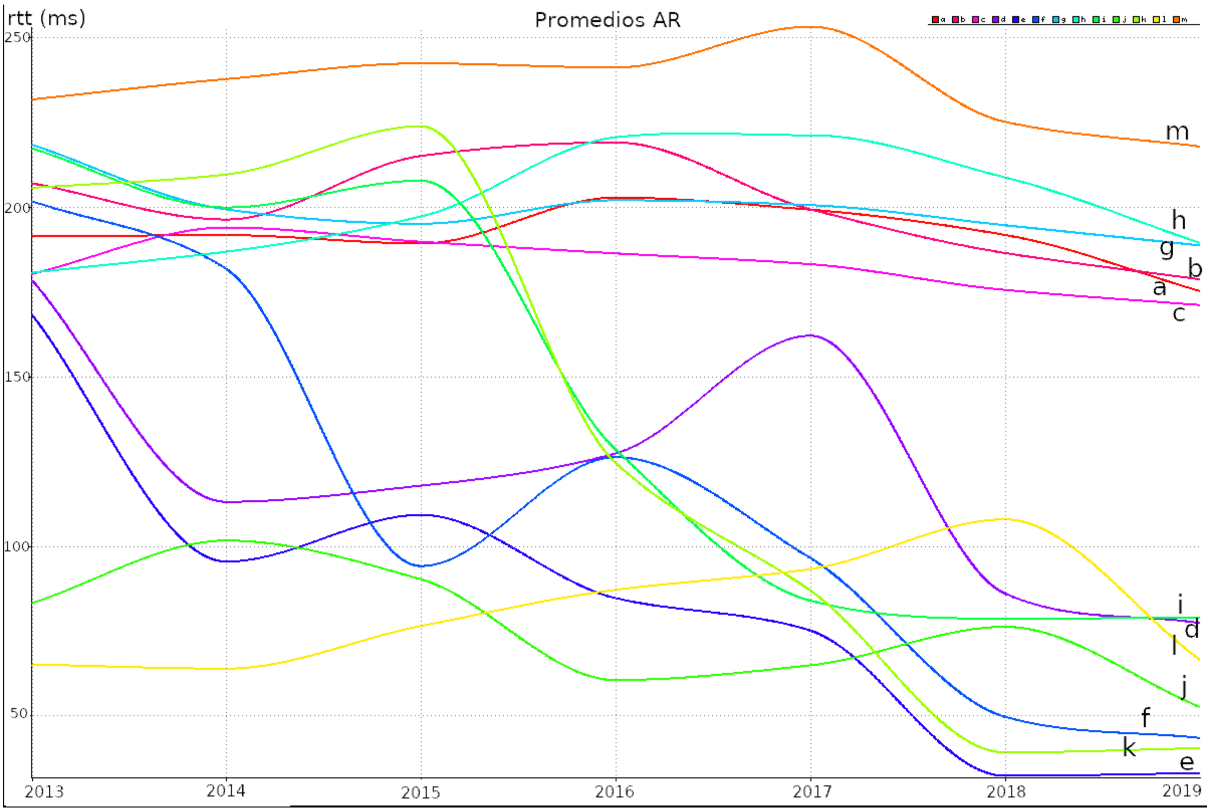

Figure 11. Historical response times from Argentina to the different root servers.

Generally speaking, the root servers with the best performance are similar and the M-root server also has the worst coverage. Issues can also be detected for root servers D and M in early 2017, which are likely the result of international routing policies that affected response times from these locations and which were quickly solved. In the case of Argentina, the average response time fell from 179 ms in 2013 to 116 ms in 2019, representing a reduction of 35%.

The rest of the countries can be found in the information included in Annex A to this report.

CONCLUSIONS

The results show a clear and continuous evolution towards improved route server reachability since 2013. Moments of change mark the installation of root server copies, which strengthen these initiatives and encourage the region to continue deploying new instances.

In general, we can say that 58% of the countries in the region have at least one root server that is reachable with an RTT lower than 50 ms, an acceptable response time for a DNS query. An analysis of response times under 85 ms shows that 84% of the countries are already covered, a figure that represents all the areas with relevant measurements in this study.

Likewise, these figures are expected to continue to improve. The installation of new root server copies — by both the +RAICES initiatives as well as by the root server operators themselves — and technologies such as Decreasing Access Time to Root Servers by Running One on Loopback (RFC 7706[3]) which allow having internal mirrors of the DNS root zone will improve the user experience in Internet browsing.

This study was presented during the LACNOG 2019 conference held in Panama in the month of October. It was very well-received by the Internet service providers present at the meeting, who observed that the figures at both regional and national level as well as the possibility of identifying locations with poor quality of service will allow them to better handle the installation of root server copies and to justify the investments within each organization.

We expect to continue this report with an analysis of the coverage radius of each node within the region, including the installation data provided by each root server administrator and, in the future, expanding the scope of the study by moving down the DNS tree, beginning at root server level and working our way down to the ccTLDs of the region.

[3] See <https://tools.ietf.org/html/rfc7706>.

ABOUT THIS STUDY

This research study was conducted by Hugo Salgado at the request of and with the supervision of LACNIC between the months of June and September of 2019. Hugo Salgado is an expert on topics relating to the DNS and domain names and works at NIC Chile, the .cl ccTLD registry.

The comments and suggestions by Guillermo Cicileo, Head of LACNIC's Internet Security and Stability Program, were also very important.

For more information on RIPE Atlas — the project that allowed obtaining the data for this report — or if you would like to host a measurement probe, please contact <https://atlas.ripe.net/>.

If your organization would like to host a root server copy, please contact LACNIC's +RAICES Project at <https://www.lacnic.net/993/1/lacnic/proyecto-+raices>.

ANNEXES

Annex A. Availability of Complete Data Sets

The charts for each country mentioned in this document are available at the website created by LACNIC's +RAICES Project for this study:
<https://www.lacnic.net/993/1/lacnic/proyecto-+raices>.

Annex B. Detailed Information on the RIPE Atlas Measurements

The recurring measurements used for this study correspond to measurement IDs 10209, 10210, 10211, 10212, 10213, 10204, 10214, 10215, 10205, 10216, 10201, 10208 and 10206 (IPv4 DNS UPD version.bind).

Historically, a total of 1024 probes were used (not all of them active at this moment), available in the following countries: mx, gt, bz, hn, sv, ni, cr, pa, cu, ky, jm, ht, do, pr, vi, bq, gp, dm, mq, lc, vc, bb, tt, cw, co, ve, gy, sr, gf, br, ec, pe, bo, cl, ar, uy and py.