IPv6 Deployment for Social and Economic Development in Latin America and the Caribbean

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA
www.caf.com

lacnic
www.lacnic.net

IPv6 Deployment for Social and Economic Development in Latin America and the Caribbean

Presented to:
CAF – development bank of Latin America –.

Eduardo Mauricio Agudelo
Senior Executive / Department of Analysis and Sectoral Programming

Presented by:
LACNIC (the Internet Addresses Registry for Latin America and the Caribbean)

Working Team: Carlos Martínez, Guillermo Cicileo, Alejandro Acosta, César Díaz, Ernesto Majó and Laura Kaplan.

External Researcher: Omar de León, Teleconsult (Global Telecommunication Services).

10 December 2015

This research on the transition to IPv6 was conducted by Omar de León, Director of Teleconsult Ltda, coordinated, implemented and monitored by LACNIC and in accordance with the terms established by CAF - development bank of Latin America -.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Table of Contents

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

1. EXECUTIVE SUMMARY

This research is meant to provide the most comprehensive body of knowledge regarding all aspects affecting the transition to IPv6 in the LACNIC region.

In addition to studying extensive documentation obtained from relevant institutions worldwide concerning the problems that exist with the exhaustion of IPv4 addresses and the advantages and methods of IPv6 deployment, the behavior of different players, economic issues and modeling of alternatives, best practices and success stories, among others, an in-depth analysis of the situation in the region was conducted from three complementary perspectives. Finally, guidelines and recommendations were developed for IPv6 deployment, its scope, instructions and required training.

Three main sources of information were used as a basis for this analysis of the situation in the LACNIC region, each of which provides a different perspective.

1. Primary and secondary indicators of the current transition status, generated from multiple sources.

2. Survey results showing the reasons behind the current status and trends.

3. Results of interviews conducted in ten countries providing consolidated information on the situation, trends and reasons why stakeholders adopt certain actions regarding the transition to IPv6.

In the ten countries in which face-to-face meetings were held, an additional source of information was obtained on the current status, behavior and trends of LACNIC members. Results of the other two sources, indicators and survey are presented for all the countries in the region.

IPv4 address sharing was the first step taken by ISPs in response to the exhaustion of IPv4 addresses, using the CGNAT (Carrier Grade Network Address Translation), or carrier-class network address translators. This solution has several problems if used in isolation, as there are applications which do not work well behind CGNAT (PS3, Peer to Peer, Netflix in some cases, etc.) and others which use a large number of ports (Google Earth, iTunes, etc.) and therefore work poorly and slowly in the case of intense address sharing, resulting in a 15%-40% delay increase according to sources and circumstances.

Lastly, this solution is neither completely scalable nor very efficient and therefore requires permanent investments in a supposedly temporary technique and is subject to the inevitable migration to IPv6 when IPv6-only applications and content appear, as relevant operators are currently predicting.

The simultaneous deployment of IPv6 and CGNAT at access level is an efficient solution that provides superior quality of service, taking advantage of the fact that 50% of the content is accessible over IPv6, thus reducing CGNAT use as calculated in our model. Therefore, it minimizes investment in these assets, including long-term investments, avoiding problems with applications that do not work well with CGNAT, given that these start using IPv6, reducing delays caused by CGNAT and allowing the progressive use of the Internet of Things, among other points favorable to deployment.

According to best practices, the IPv6 transition process consists of several stages which begin with an inventory of the network status, systems and ancillary services (DNS, Firewall, etc.) and connectivity and end with deployment itself. The development of the various stages varies depending on the case of each ISP, institution, company and other users, including the difficulties and the procedures to be followed in each case. These differences can be observed in the international background research, in the results of the meetings held in different countries, in the survey and in the results of the main indicators of the value chain and in the LACNIC IPv6 indicator. Two main conclusions stem from the above:

1. The difficulties and time required to solve these issues involve high levels of uncertainty in most cases.

2. As soon as the planning process and gradual transition begins, greater economic deployment benefits will be obtained as equipment and systems are replaced, while the inevitable start of the transition itself will be achieved in a non-traumatic way without uncertainties or surprises.

This transition involves multiple stakeholders which we will analyze to provide a better description of the context in which it is taking place, including infrastructure vendors, manufacturers of computers and other electronic devices, access providers or ISPs, content providers, corporations, users, government authorities, universities and academic networks. The behaviors and motivations driving each of these will be duly analyzed, as will their impact on deployment, recommended actions for some of these stakeholders such as government authorities, including the possible scope of these regulations, among others.

Policies and guidelines play an important role in public procurement and security, as well as in the development of e-government and educational content, including the actions available to universities and academic networks from the point of view of their own deployment and impact on ISPs and equipment vendors, as well as their important role in spreading knowledge on IPv6.

This transition involves drivers which are studied as additional elements affecting IPv6 deployment, e.g., the shortage of IPv4 addresses, network effects, the actions of major ISPs, the improvement of user experience and government initiatives.

An economic model comparing three alternatives for dealing with IPv4 address exhaustion was developed: transition to IPv6 using the dual-stack technique with CGNAT, continue using only CGNAT, and buying IPv4 addresses. This latter alternative can be considered in cases of very low customer growth rates. The alternative of sharing IPv4 addresses through the use of CGNAT gives rise to problems with applications and fails to provide a clear picture of which the best economic model is. Moreover, in either alternative, IPv6 migration is inevitable particularly due to the expected development of applications and sites which will only operate in IPv6, as already anticipated by some ISPs.

As the results of the economic model show, the dual-stack deployment alternative is very efficient in the use of resources as compared to the other two. In particular, the flow of investments in CGNAT clearly show that there comes a time during IPv6 deployment when it is not necessary to make any more investments in CGNAT, mainly due to the fact that reduction in the use of sessions outweighs the sessions necessary to support user growth. The table below is an example of the results of the model which calculates the Net Present Value of each alternative, for certain cases, considering the costs, expenses and incremental investments, in order to take into account the effect of time and the rate of opportunity cost of capital.

Alternatives	Net Present Value
Alternative 1, transition with dual-stack and CGNAT with CPE	$4.910.952,82
Alternative 1, transition with dual-stack and CGNAT without CPE	$2.312.338,22
Alternative 2, using CGNAT without implementing IPv6	$6.192.207,28
Alternative 3, purchasing IPv4 addresses without NAT or IPv6	$4.077.689,49

The results of the survey and of the meetings conducted as part of this research show great variability in the situation in different countries and in different ISPs, universities, academic networks and government authorities.

In general, IPv6 readiness is quite variable among the region's ISPs, as are the different timeframes in which they are planning to begin mass deployment. In this regard, about 30% of respondents are planning to start deployment on their access networks in 2016. In the meetings held in the various countries, almost all ISPs providing mass residential services are planning to start this deployment in 2016. It is not possible to act externally on the ISPs; for this reason, the recommendations given relate to indirect actions such as public procurement, among others.

Universities exhibit a similar level of disparity among the different countries. Thus, given their importance in IPv6 deployment, special attention should be given to the causes of their shortcomings where possible.

Only four countries were observed with a percentage of users potentially eligible to operate in IPv6 greater than 1%: Bolivia, Brazil, Ecuador and Peru. In the remaining countries, this indicator is well below 1%. In the case of Bolivia, Ecuador and Peru, only one ISP in each of these countries is responsible for these relatively high numbers (as compared to the rest of the region).

Cases of these operators identified as success stories will be analyzed, along with other cases outside the region. The goal is to show the process they followed so that it can serve as a reference. In general, we can say that in these cases, after a gradual start to the deployment process, IPv6 deployment is triggered by the shortage of IPv4 addresses, not prior to that. One extra-regional success story shows an operator with operations in Africa (where there is no IPv4 address shortage yet) which has begun the deployment process anticipating that IPv6-only sites and applications might be developed at any time.

On average, the value of the LACNIC/CAF ICAv6 indicator developed for the region is significantly lower than the one corresponding to the countries selected for international comparison. These values as well as the four partial indicators are shown in the table below:

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Indicator	LACNIC Region	Reference countries	Reference countries / LACNIC region
LACNIC/CAF ICAv6	21.39%	39.59%	1.85
Planning	18.08%	28.89%	1.60
Transit AS	55.30%	79.23%	1.43
Content	50.77%	49.96%	0.98
Users	1.31%	15.08%	11.51

The LACNIC/CAF ICAv6 indicator is meant for countries in the initial stages of IPv6 deployment, which is why it assigns a weight of 30% to planning and the early stages of deployment, such as having IPv6 transit available in autonomous systems. In terms of these two indicators, the countries of the region are well below the selected countries, but the efforts required to achieve progress in these countries are small as compared to overall deployment efforts. In this sense, the most effective tool is LACNIC's effort to obtain more in-depth knowledge, whether on its own or working jointly with other stakeholders such as universities, academic networks and/or governments.

As to content, the percentage of IPv6 accessible content is similar worldwide; moreover, there are no effective actions to improve this situation, except for e-government and educational content.

Finally, the User indicator (which represents the percentage of users who are potentially able to operate in IPv6) is very low in the region. Ultimately, this is the main indicator which shows the gap with more advanced countries and represents the greatest challenge to overcome.

Based on this analysis, recommendations and guidelines are presented to help achieve the timely deployment of IPv6, classified as follows:

1. Main problems in the transition process in the countries of the region; regional challenges.

2. Adjustments to regulatory frameworks and policies so that they will facilitate IPv6 deployment

a. Regulatory framework for telecommunications

b. ICT regulators

c. Regulatory framework for public procurement

3. Academic networks and universities

4. Companies

5. ISPs

The above is summarized in a road map to encourage the region's timely transition to IPv6, combined with a training plan. LACNIC's actions are essential in this road map, as they have been so far both in terms of spreading knowledge as well as in developing a benchmarking database through its website. In this sense, it is very important to disseminate extra-technological knowledge as well as the contents of this document, as this is the area where the greatest deficiencies have been observed by the majority of stakeholders in different countries.

As for the impact on productivity under current conditions, competition among ISPs leads them to adopt a series of measures, both in the residential as well as in the corporate market, which significantly mitigate, or even eliminate, the potential negative impacts on productivity during the transition to IPv6.

A prospective analysis of this transition shows that the use of CGNAT imposes further delays which limit certain applications that depend on this technology (e.g., vehicle control or telesurgeries), gives rise to uncertainties relating to application development thus restricting entrepreneurship, etc.

As the Internet of Things (IoT) gains momentum, in order to maximize its benefits it will be necessary to uniquely identify each device regardless of technology, whether fixed or mobile, or even when ISP changes occur, in which case mobility and multihoming must be possible, as well as the ability to process a significant increase in traffic, provide robust routes, ensure confidentiality, allow device auto-configuration and selective traffic prioritization. This set of conditions required for the development of the IoT will be a strong incentive for the deployment and provision of services over IPv6, given that only services based on this protocol comply with such conditions and will allow the Internet to expand to user devices, to systems and virtually to anything that will benefit from Internet connectivity.

2. PROBLEMS IN THE USE OF IPV4 IN THE FACE OF IPV4 EXHAUSTION

2.1 Use of NAT

The first reaction from providers in the face of IPv4 address exhaustion has been to try to share the same address among multiple users. Known as NAT, this technique has been used at user level in order to share a public IP address allocated by the provider among multiple devices. This is called NAT44 as it translates public IPv4 addresses into private IPv4 address blocks.

On a provider network level, sometimes the NAT444 technique is used, which involves a double stateful NAT44 layer on the network which does not require the use of IPv6 addresses. This technique is called CGNAT (Carrier Grade NAT) or LSNAT (Large Scale NAT). The transition techniques described in the Annex include NAT on the provider network, except for MAP in its two versions, which can also be considered a type of CGNAT (Carrier Grade NAT), but requires the use of IPv6 and is recommended only during the transition process.

There are still situations where maintaining operations in IPv4 is an alternative that does not require the use of NAT. This may be the case for operators with low growth rates who have enough IPv4 addresses to cover their expected growth and who can still purchase additional blocks on the secondary market (also more feasible in the case of small operators).

In general, the use of NAT has the following disadvantages:

1. It modifies the following basic Internet principles: end-to-end connectivity, simple transport network without any complex equipment, intelligence transferred to network end-points. This complicates network management, increases the risk of failure and results in difficulties in its use as will be shown later.

2. Access Control Lists (ACL) — which are used to block access through the IP address — have side effects on users who operate properly. Blocking is done at IP address level, which are shared by several independent users who will all suffer the measures applied as a result of address misuse by one of the users.

3. Some legislations requires that both the IP address and the server port be kept on record in order to identify who accessed a particular service. All TCP sessions must be recorded, otherwise it is not possible to respond to the requirements of the authorities when a crime is committed using a public IP address. This represents significant storage costs and increased complexity in operations. In certain cases, this data must be kept for up to 5 years.

4. Some applications do not work well behind a NAT, or more particularly when using CGNAT. Problems have been detected in video streaming applications, online gaming with multiple participants and peer to peer file sharing, while simpler applications such as email or web browsers have not shown any difficulties.

5. The major problem with NATs is that they are not scalable to large numbers of users, mainly because of limitations on the number of ports opened by users. In theory, one IP address allows opening a total of 64K ports.

a. A study conducted by Shin Miyakawa[1] shows that a Google Map image deteriorates from a correct situation (30 to 60 concurrent sessions) to a situation where a map is not visible with 5 concurrent sessions. To achieve this, a device was placed between the PC and the Internet which progressively reduced the number of enabled sessions while duly observing how the application's performance deteriorated.

b. This is because AJAX (Asynchronous JavaScript + XML) is used to provide proper operation quality. AJAX uses several concurrent TCP sessions to accelerate the receipt of information.

c. This same study also determined the minimum number of sessions by reducing this number until deterioration in the service was observed. Results were as follows:

i. Yahoo main page: 10 to 20.

ii. Google image search: 30 to 60.

iii. iTunes: 230 to 270.

iv. Amazon or YouTube: 90.

v. Non-operational web page: 5 to 10.

d. For security and other reasons, only the upper 32K addresses can be used, which further reduces the ability of a single IP address to concurrently open multiple applications when shared among multiple users.

1- "From IPv4 only To v4/v6 Dual Stack-IETF IAB Technical Plenary". NTT Communications Corporation

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

e. In view of this, each user should be assigned at least 1,000 to 3,000 ports, which leaves a maximum safe limit of 10 users per shared IPv4 address.

f. However, it must be kept in mind that, in turn, customers use NAT44 to connect several internal devices. Therefore, if one considers, for example, a total of three devices operating simultaneously at the customer's premises, if the same IP address was provided to 10 different customers, each user would be at the lower limit of 1,000 ports, in which case applications could start deteriorating. Given that this is a stochastic phenomenon, when dynamic and non-static sharing is used, the minimum quantity may vary depending on the time of day and other factors.

g. Obviously, for corporate customers, address sharing on CGNAT is not possible.

6. Additionally, recent studies completed in September 2015, such as those by Facebook or Verizon, indicate that IPv6 connections are 15% or more faster than IPv4 with NAT.

7. The difficulties that may occur with certain applications in networks with CGNAT have economic effects due to additional transaction costs in the case of applications using the Internet. Although the Internet is a platform that operates seamlessly with applications, lowering transaction costs encourages entrepreneurs to create new services. The uncertainty as to whether an application will operate in different environments (e.g., in user environments involving CGNAT networks) increases transaction costs. Large companies which develop online services do not have major problems with these difficulties, which generate a barrier to small companies and discourage entrepreneurship.

8. The difficulties derived from the CGNAT may also affect companies that provide services, forcing them to upgrade their services in the upper layers to solve problems generated in the lower layers. A typical case is that of Microsoft, which had to update its Xbox in 2011 to allow certain online multi-player games.

2.2 Block transfers on the secondary market

Buying IPv4 blocks increases operational costs and also has a short service life if the buyer has moderate growth. This operation can only be justified in cases of very low growth in the number of users, along with NAT, for a period of time until the migration to IPv6 is inevitable. An economic model using reallocated blocks will be analyzed later. Some operators (Orange) already understand that they must inevitably migrate as they anticipate they will have to deal with IPv6-only sites.

Ultimately, this reallocation is made by moving the scarce resource (IPv4 addresses) from users (providers) who assign them less value, to those who assign them greater value. This process is very similar to the one that occurs in countries where the telecommunications regulator authorizes a secondary spectrum market. Spectrum blocks (bands) can be sold, leased, etc., sometimes with the intervention of the regulator and others by simply recording the transaction.

An undesirable consequence of these transactions is block fragmentation, which can already be observed in IPv4 routing tables, which is why RIRs usually place a lower limit of /24 blocks.

Due to historical reasons having to do with how easy it was to obtain IP address blocks before the creation of the RIRs, certain providers, universities and government institutions were able to obtain a significant number of unutilized blocks they are now able to transfer. Likewise, certain address users currently have available IPv4 addresses and would be willing to transfer them if transfer conditions were to improve.

These transfers are causing problems for applications which depend on the user-specific context, delivering unwanted information (e.g. advertising a restaurant in New York to a user located in Los Angeles), or forcing changes and major complications. Something similar occurs locally with CGNAT.

In the case of LACNIC, transfer conditions are stated in Section 2 of the Policy Manual, IPv4 Addresses[2]. These transfers have not been activated yet. Generally speaking, transfers would operate under rules of good practice which must be met by the parties involved in the transaction.

"2.3.2.17. Mergers, Acquisitions or Sales of ISPs or End Users

LACNIC's policies do not recognize the non-authorized sale or transfer of IPv4 address space and therefore such transfers shall be considered invalid, with the exception of those subject to the provisions of section 2.3.2.18.

Should an ISP or end user change ownership due to a merger, sale, or acquisition, the new entity shall register these changes with LACNIC. If the name of the company is modified, legal documentation validating this change of name shall be submitted.

The information that may be requested includes, but is not limited to, the following:

2- Policy Manual (v2.3 – 16 July 2015). http://www.lacnic.net/web/lacnic/manual-2

A copy of the legal document validating the transfer of assets.

A detailed inventory of all assets used by the applicant for maintaining the IPv4 address space in use.

A list of the applicant's clients that use portions of the allocated space.

2.3.2.18.- Transfer of IPv4 Blocks within the LACNIC Region.

NOTE: This section will come into force when LACNIC or any of its NIRs becomes unable, for the first time, to cover an IPv4 block allocation or assignment because of lack of resources.

IPv4 block transfers shall be allowed between LIRs and/or End Users within the LACNIC region (hereinafter organizations) in accordance with the conditions set forth in this section.

2.3.2.18.1.- The minimum block size that may be transferred is a /24.

2.3.2.18.2.- In order for an organization to qualify for receiving a transfer, it must first go through the process of justifying its IPv4 resource needs before LACNIC.

That is to say, the organization must justify before LACNIC the initial/additional allocation/assignment, as applicable, according to the policies in force.

2.3.2.18.3.- Upon receiving an IPv4 address block transfer request, LACNIC shall verify that the organization transferring the block is in fact the holder of said block according to LACNIC's records. The approved applicant and the organization transferring the resources must present before LACNIC a copy of the legal document supporting the transfer.

2.3.2.18.4.- LACNIC shall maintain a publicly accessible transfer log of all IPv4 address block transfers registered before LACNIC. Said log shall specify the date on which each transaction took place, the organization from which the transfer originated, the receiving organization, and the block that was transferred.

2.3.2.18.5.- The organization in which the transfer originated shall automatically be ineligible to receive IPv4 resource allocations and/or assignments from LACNIC for a period of one year as of the transaction date registered in the transfer log.

2.3.2.18.6.- A block that has previously been transferred may not subsequently be transferred again for a period of one year as of the transaction date registered in the transfer log. The same applies to its sub-blocks, i.e. blocks consisting of a subset of the IPv4 addresses contained in the block.

2.3.2.18.7.- Once the transfer is complete, LACNIC shall modify the information on the transferred resource in order to reflect the change of holder.

2.3.2.18.8.- The receiving organization must comply with all LACNIC policies in force.

2.3.2.18.9.- Blocks and their sub-blocks from allocations or assignments from LACNIC, whether initial or additional, cannot be transferred for a period of one year as of the allocation or assignment date.

2.3.2.18.10.- Transferred legacy resources will no longer be considered as such.

2.3.2.19.- Inclusion of origin ASN in the WHOIS database when available.

When available, LACNIC shall include in its WHOIS database the origin ASN of all prefixes directly assigned by LACNIC.

Block holders may enter the origin ASN of their blocks through LACNIC's resource administration system. Providing this information shall be the members' responsibility.

When a block's origin ASN is not specified, the WHOIS response shall explicitly state this fact.

Research conducted in 2012[3] presents interesting results regarding address transfers at global level. This address transfer market became public in April 2011 when Microsoft purchased from Nortel (then under bankruptcy proceedings) addresses that had been obtained prior to the existence of ARIN (1991) and from other companies. Over time, the RIR began adopting different policies. RIPE was the first registry in approving the commercial transfer of addresses in 2008. It should be noted that Europe was also one of the pioneers in the creation of secondary spectrum markets APNIC was the first to propose the opening of this secondary market, but discussions delayed the adoption of the new policy until 2010.

The authors of this study estimate that in 2012 each IPv4 address will be worth $10.

3- "Dimensioning the Elephant: An Empirical Analysis of the IPv4 Number Market". Milton Mueller and Brenden Kuerbis, Syracuse University School of Information Studies, and Hadi Asghari, Technology University of Delft, School of Technology, Policy and Management. http://internetgovernance.org/pdf/IPv4marketTPRC20122.pdf

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Market transfers of IPv4 address blocks grew rapidly, at least until the first semester of 2012 (1S12):

	2009	2010	2011	1S12
# transactions	3	2	27	52
# blocks traded	8	3	109	84
# IP addresses	11,264	10,240	1,013,246	4,999,936

ARIN was the region most involved in transfers. The following table shows a quantitative comparison of ARIN allocation and market allocation from between 2009 up to the first semester of 2012:

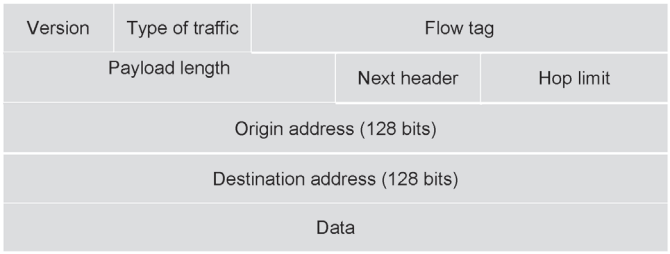
	2009	2010	2011	1S12
IP numbers allocation	41,317,376	45,266,688	22,471,424	16,077,056
IP numbers transferred via market ARIN	11,264	8,192	1,150,976	4,221,184
Percent allocated via market	0.03%	0.02%	5.12%	26.26%

This topic will be further analyzed in another section of this document (economic analysis).

3. TECHNICAL ASPECTS AND BENEFITS OF THE IPV6 PROTOCOL

3.1 Technical overview of IPv6

In terms of purely technical aspects, the main reason for the development of the IPv6 protocol was the need to increase the number of IP addresses in view of IPv4 address exhaustion. The IPv6 datagram header has the structure shown in the diagram below.



As we can see, it is simpler than the IPv4 header, uses the 128-bit addresses as opposed to the 32-bit addresses used by IPv4. As discussed in this report, this is the main feature driving IPv6 deployment.

In addition to the traditional use of the Internet where each user typically has more than one connected device (Notebook, smartphone, etc.) but needs only one IP address, massive use such as that resulting from the Internet of Things requires that each user employ multiple IP addresses at the same time. This will be discussed later.

With the IPv4 protocol, on average, as at August 2015, each person on the planet has 0.58 addresses available, which is clearly not enough to use multiple devices and the future development of the Internet of Things, even when according to the ITU Internet penetration worldwide was 43%. Consequently, the transition to IPv6 is inevitable for all stakeholders, as it will allow a total of 4.65 1028 addresses per inhabitant.

3.2 Latest results regarding IPv6

At the @Scale of Facebook conference, Paul Saab highlighted several important issues.

Regarding terminals, he noted that the new iOS9 released on September 16, 2015 will place both protocols on an equal basis, so IPv6 will be used much more on these terminals than it has been so far when preference is given to IPv4. He estimated that, while with iOS8 only about 50% of potentially IPv6 connections were actually made over IPv6, with the new OS this percentage will rise to 99%.

Considering the impact of iOS9 deployment, Verizon Wireless estimates that by September 2016 IPv6 traffic will increase from 50% to 70%. According to the company's chief IPv6 architect, the impact of Apple's decision may also encourage the use of IPv6 at Comcast, thus increasing current utilization (25%) to 50% in one year.

At the @Scale conference, operators and Facebook noted that the use of NAT delays traffic. Limited testing conducted by Facebook in early 2015 showed that the use of IPv6 increases connection speed by approximately 40%, while more extensive tests conducted recently showed that IPv6 increases connection speed by 15%. Verizon has also noticed similar improvements in connection speeds with IPv6.

In turn, Deutsche Telekom's VP of aggregation and IP transport mentioned the impact that the new protocol will have on mobile networks, primarily through home automation applications and the Internet of Things, all of which could not be supported over IPv4.

Likewise, SK Telecom's Emerging Technologies Project Manager said that delay-sensitive applications such as vehicle controls would not be feasible with IPv4.

It is understood that the requirement imposed by Apple Store, where only IPv6 compatible applications will be accepted starting in 2016, might boost the use of "IPv6 only" and progressively eliminate the need for IPv4, even to the point of totally dispensing with IPv4.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

4. KEY ACTORS IN THE TRANSITION PROCESS. PUBLIC–PRIVATE SECTOR INTERACTION

This section discusses the participation, current situation and impact of the actions of the main key actors in terms of IPv6 deployment. For reasons of clarity, in reference to Governments and their various agencies (telecommunications and ICT regulators, agencies responsible for public procurement, among others), academic networks, universities and companies, this analysis is presented in the section titled "Deployment Guidelines and Recommendations, Scope, Instructions and Training."

Various stakeholders act in a way that either accelerates or slows down IPv6 deployment. Some such as users, equipment vendors, content and application providers have a direct effect on IPv6 drivers, while others such as access providers react and make economic decisions based on the drivers discussed in the section titled "Transition drivers."

A recurring theme in these studies is the difficulty in obtaining reliable data on the costs and benefits of IPv6 deployment from the different actors, as well as the variability in their behavior, which makes it difficult to quantify results. For this reason, reference is first made to factors affecting deployment costs and benefits according to the different actors involved. An economic evaluation model is then developed for ISPs.

In 2014, the OECD published a relevant document[4] on the specific qualitative factors that influence the decision of different stakeholder groups to migrate to IPv6.

4.1 Infrastructure vendors

4.1.1 Networking equipment

This aspect is completely covered with the provision of equipment tested in the use of the IPv6 protocol for both corporate routers and network core equipment. This assertion is verified by the high values of the AS indicators with IPv6 transit (network core development indicator), duly analyzed to determine the LACNIC/CAF ICAv6 indicator.

This is not the same for smaller user equipment.

Regarding user equipment for wired networks (CPE), full compatibility with any provider's network is not often achieved, which creates problems in countries such as the USA where users can purchase their own CPE. In this way, CPE may not actually support IPv6 or be IPv6-compatible. In any case, they cannot operate in IPv6 even if the provider is IPv6-ready.

Moreover, there are studies that show that CPEs, which in theory are IPv6-ready, come with IPv6 disabled by default, thus requiring configuration to enable the new protocol. One reason for this may be that these CPEs are not 100% compatible with RFC specifications: they are marketed as IPv6, but the manufacturer prefers IPv6 not to be enabled.

For example, for Internet access using the hybrid networks of cable TV operators (HFC networks) there are standards that support IPv6, but in some cases difficulties have been reported in the LACNIC region. These seem to relate mainly to equipment quality and to the fact that they are not fully IPv6-compatible, whether because of the upgrade from DOCSIS 2.0 to the "DOCSIS 2.0 + IPv6" standard, or directly because of DOCSIS 3.0 - 3.1 equipment.

This factor discourages deployment, as the provider finds itself deploying the network but unable to use it to its full potential or incurs in expenses to allow the use of IPv6 by users experimenting issues. Consequently, it was repeatedly stated that the deployment of IPv6-compatible CPE requires extensive ¬human and material resources.

While there are a couple of institutions in the United States[5] that test equipment for IPv6 compatibility, information on CPE IPv6-incompatibility is scarce and does not allow a clear understanding of the true situation of CPEs, routers and hosts for non-corporate use.

4.1.2 General purpose computers

Modern operating systems support IPv6 but sometimes require that certain prior configurations. Browsers already support IPv6 and have done so for some time. In the case of using a dual stack IPv6 and IPv4 configuration, a problem can arise if a connection is first established over IPv6 and is then interrupted. In this case it is necessary to wait a few seconds before attempting to establish an IPv4 connection. This generates a poor user experience.

4- OECD (2014), "The Economics of Transition to Internet Protocol version 6 (IPv6)", OECD Digital Economy Papers, No. 244, OECD Publishing.
5- University of New Hampshire's Interoperability Laboratory and National Institute of Standards and Technology.

This gave rise to the algorithm known as "Happy Eyeballs," which basically focuses on human beings. Described in RFC 6555, this algorithm selects which protocol provides the best service by testing both simultaneously and giving preference to IPv6. Several browsers support this algorithm. However, its implementation has not been uniformly successful among the different browsers, and cases have been observed where a browser chooses IPv4 when it could have used IPv6.

It is important to reduce the above-mentioned problems and others through deployments that allow end users to take full advantage of networks that provide IPv6 access. Otherwise, efforts to encourage migration to IPv6 will be frustrated by an unjustified discrediting of IPv6. Likewise, if users employ IPv4 when they can already use IPv6, they will be sending the wrong signals regarding low IPv6 adoption rates at user level, which has multiple negative effects for IPv6 development. Among these, those observing the evolution of IPv6 utilization at user level will tend to adopt a reactive stance rather than promoting IPv6 development. Indicators involving users (included in the indicator section) outline this problem, as they opt for measurements which seek to determine whether users are potentially able to use IPv6, not only whether they are actually using the protocol.

4.1.3 Consumer electronic devices

Systematic information about the IPv6 compatibility of these devices is generally unavailable, although it is observed that IPv6 compatibility issues exist (e.g., the same brand has IPv6-compatible TVs and non-compatible gaming equipment). Users have difficulty in understanding this topic and there are no incentives for manufacturers to devote their efforts to the issue. An increase in the number IPv6 users and awareness of the protocol's advantages —or the advent of IPv6-only sites — may act as drivers to promote the development of IPv6 devices. One way of perceiving the advantages of IPv6 will be the appearance of IPv6-only applications on the market, primarily due to the request for end-to-end connectivity.

By way of exception, it is observed that manufacturers of new connected TVs (Smart TV) are moving towards robust platforms that would ensure good IPv6 connectivity.

The emergence of general IPv6-compatible devices, or those which require IPv6 to operate, will likewise be a driver for access providers to see the real importance of IPv6 network deployment.

4.2 Wired access providers

This section analyzes the costs and benefits of IPv6 deployment from the point of view of wired network operators. This report analyzes the significant diversity of situations in different countries in terms of network-readiness so that users can be reached over IPv6 based on the Google and APNIC methodologies. This diversity also exists among operators within the same country. An example of this is the diversity that existed within the USA in late 2013 amng Google Fiber (60.7%), AT&T (13.6%) and Time Warner Cable (3.3%). As at November 19, 2015, this also occurs in the LACNIC region, where there are operators with high levels of IPv6 deployment such as Telefonica of Peru (22.3%), CNT of Ecuador (14.8%), COMTECO of Bolivia (19.40%), and CVT of Brazil (14.76%), among others.

It is understood that this variability is primarily motivated by how different access providers perceive the cost-benefit relationship of IPv6 deployment, in addition to the impact of IPv4 exhaustion. On the one hand, deployment costs vary depending on user demand, network architecture, human resource training and perception of IPv6, and network equipment technology, among others; on the other hand, benefits may vary depending on each provider. ISPs which began an early migration were not subjected to high costs because they began upgrading their networks to IPv6 while at the same time upgrading due to obsolescence.

As mentioned in the "Transition drivers" section, various deployment drivers affect the economic analysis in such a way that can lead to different conclusions about the extent of deployment and its timeliness.

The final decision on deployment depends on economic aspects which, in turn, depend on the chosen migration path (for which no recommended best practices are specified in detail). In principle, three non-exclusive alternatives are observed in the region which can be combined to optimize the transition: CGNAT, the purchase of IPv4 blocks or IPv6 deployment. These options increase the variability of each provider's decision. Likewise, a strong trend is observed in the region toward dual-stack with or without CGNAT, but mainly with CGNAT due to the shortage of IPv4 addresses. The economic benefits of this IPv6 transition alternative can also be observed in the economic model.

As for the CGNAT, the cost estimates prepared by Lee Howard are discussed below in the section titled "Estimated costs for the different alternatives." For example, Lee Howard estimates an investment of $90,000 for each 10,000 users, plus Operation and

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Maintenance costs of $10,000 per year. Decision-makers must also add the negative effects of NAT utilization described in the section titled "Use of NAT." These negative effects might impact the economic equation through a reduction in the customer base, thus creating a negative benefit that must be considered, to the extent that other providers in the same geographical area have begun IPv6 deployment.

In the consultant's analysis of the estimated values provided by the operators surveyed in the region, costs are mainly calculated mainly per million simultaneous sessions. These costs are presented in the analysis of the model for the economic evaluation of alternatives.

The purchase of IP address blocks is a viable alternative growth rates are low in terms of the number of users. In 2012 its cost was estimated at $10 per address, a figure somewhat equivalent to that of CGNAT as determined through a very preliminary assessment.

IPv6 deployment also requires IPv4 addresses (unless it is greenfield using a technique which allows accessing IPv4 sites) as well as transition equipment; thus, positive results derive primarily from future flows rather than from the initial assessment. In other words, investments must be made in this case, but, being that it is the definitive technology, it will generate future benefits that justify its deployment.

This is mainly a decision based on opportunity: the best time to begin deployment is the time when it will result in the greatest benefit.

Evidence suggests that IPv6 network deployment costs are not very high. However, as already mentioned, economic benefits are not immediately seen as are other effects such as an improved user experience. Therefore, investments require detailed decisions and must consider future flows, the multiple positive impacts deployment will bring about as well as the negative impacts it will prevent. Other factors should also be considered, such as the learning curve, future cost declines and other factors relating to the deployment timeframe.

To include the future effects of current decisions, the model developed in this research uses the Net Present Value and considers various conditions and future changes.

An important point to mention here is that when old routers that support IPv6 are used, significant declines in performance are sometimes observed. This might occur because IPv4 traffic is routed using tables which are loaded into firmware, something which cannot be done with IPv6 routing. Performance may decline, for example, from 5,000 pkts/sec. to 500 pkts/sec.

4.3 Wireless access providers

This type of provider refers primarily to mobile service providers.

In this case, annual user base growth rates for mobile broadband are quite high; this first difference as regards wired operators shows that alternatives using only CGNAT or address transfers to continue operation on IPv4 are not viable. In addition, most operators are already using CGNAT.

Moreover, mobile operators introduce greater changes to their networks due to growth in terms of traffic and coverage, and even in terms of technologies (e.g. LTE and VoLTE) and services. This results in a point of view that is different from that of wired providers, in the sense that changes and the addition of equipment for reasons of growth or obsolescence are seen as natural occurrences. In cases where equipment is being incorporated for other reasons, IPv6 deployment means marginal investment costs for IPv6 adoption are very low but not zero, as these additions are made in an IPv4 network environment where IPv6 routes may not be the best, transit providers may not support IPv6 traffic increases, etc. In other words, it is not entirely greenfield.

LTE deployments are virtually all dual-stack. Some operators such as SK Telecom[6] have chosen IPv6 only for their mobile networks using an IPv4 transition technology, with dual-stack available in their backbone and transition techniques in the fixed network to access sites that are still IPv4 only.

An issue that must be considered is the availability of IPv6 terminals: while a high percentage of the terminals available on the market are advertised as IPv6-compatible, they may have compatibility issues with the operator's network. This is why operators do their best to ensure compatibility and make sure they can take advantage of their IPv6 networks, including the obligation on manufacturers to produce compatible equipment so that they can be connected to their networks. In addition, contrary to what happens in the case of CPEs in wired networks, mobile terminals are regularly replaced at shorter intervals due to technological progress, which eliminates the problem of obsolete equipment which are not IPv6-compatible. In November 2015, the main providers using Android 4.4 and Windows Phone 8.1 began supporting NAT64 CLAT

6- "Applying IPv6 to LTE Networks". May 6, 2015. SK Telekom.

according to RFC 6877. In June, it was announced at Apple WWDC 2015 that iOS9 would support DNS64/NAT64 "IPv6 only" network services.

Another aspect which favors IPv6 deployment in mobile operators is that they can develop an IPv6-only network using the 464XLAT technique as described in Annex II of this research, thus allowing applications that run on IPv4 only to be employed by users, who in turn maintain their native IPv6 quality. Such applications are still relevant in mobile networks.

The use of NAT64/DNS64 is not appropriate, as certain applications are coded to use IPv4 addresses instead of the domain name, or the mobile device does not query the DNS64 server. This is why Apple is simultaneously announcing that all applications uploaded to the Apple Store must support IPv6.

4.4 Content providers

Of the 500 major content providers accessed by each country in the LACNIC region, about 50% (weighted average per country considering [unique users] * [pages viewed]) are accessible over IPv6. However, if one looks at IPv6 readiness without considering the number of visitors (i.e., a very popular website has the same weight as one which isn't popular at all), no significant growth is observed. In August 2015, there were approximately 7 times less IPv6-accessible websites than non-IPv6-accessible websites.

In this case, deployment costs (equipment, training, etc.) have a greater impact on smaller sites because of fixed costs. Moreover, due to massive incoming traffic from different networks worldwide, deployment is complex and can lead to specific problems that must be solved even when the operation has been running for some time. Large providers have their own qualified employees to work on these problems, but smaller providers cannot find such employees on the market because of the current lack of experience in this field. Further problems may arise from networks or users themselves which may make response appear poor when in fact the problem lies elsewhere.

Such difficulties can deter IPv6 deployment.

4.5 Enterprise networks

These networks are already prepared and accustomed to the use of NAT. In principle, for these networks an evolution towards IPv6 involves investing in equipment which may not otherwise be necessary at this time; in addition, the change of protocol can result in compatibility issues affecting their entire network and applications, to adapt the new protocol to the existing infrastructure. Especially in the case of applications, significant problems and costs may be involved.

Security concerns may also increase when making these protocol changes at network level.

It is noted that the development of the Internet of Things and Cloud applications will make it necessary for companies to deploy IPv6, as it will no longer be possible to increase the number of private addresses to accompany the strong demand these will create, or even for the company to support the creation of subnets, etc. All this represents operational complications which can stimulate the migration to IPv6, thus avoiding IPv4 network fragmentation.

4.6 Non-corporate end users

End user behavior promoting IPv6 deployment is closely linked to what has already been analyzed in terms of user infrastructure. Users are only interested in obtaining quality services regardless of technology — this is where infrastructure comes into play (CPEs, computers, software, browsers, devices, etc.), meaning that taking care of these aspects is vital when providing IPv6 services to users.

A major problem is that of networks which rely solely on CGNAT, as certain applications do not work well with this technology, meaning that users may require IPv6 to use them, thus motivating the provider to offer IPv6 access. In some cases, ISPs provide a global address for customers who complain repeatedly. In other cases, when sharing increases, speed begins to decrease because each user does not have the number of simultaneous sessions required for proper response quality. Lately Facebook and Verizon are claiming that the use of CGNAT increases delay by about 15% or more (Facebook has recorded increases of up to 40%). These issues are starting to become visible to users and will probably increase in time. This might lead users to begin noticing — or hearing of — differences in quality, something which would encourage ISPs to initiate and promote the transition process in case of IPv4 address shortage.

Finally, the Internet of Things will bring special requirements which definitely cannot be solved by using CGNAT. The efficient and effective use of the Internet of Things depends on the use of IPv6.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

4.7 Conclusions for each stakeholder group

The main considerations or requirements regarding how the different stakeholders view IPv6 deployment are summarized below, including certain key aspects that might encourage this deployment.

1. Infrastructure vendors

a. No difficulties have been encountered in relation to corporate equipment and providers' network core.

b. Improve CPE compatibility for fixed networks.

c. Ensure the implementation of "Happy Eyeballs" in browsers so that whenever possible priority will be given to the establishment of a successful IPv6 connection.

d. In general, attempt that networks which allow IPv6 access can effectively achieve quality IPv6 access.

e. Improve the compatibility of consumer electronic devices, something which is not generally observed. Users do not yet fully perceive the advantages of IPv6, at least until its use becomes more widespread; therefore, manufacturers feel no pressure to make their devices IPv6-compatible. Results are already being published which show that the use of CGNAT increases delay between 15% and 40%.

f. The emergence of IPv6 devices, or those which only operate with IPv6 (e.g. through end-to-end connections), will also drive access providers to begin IPv6 deployment.

g. This does not seem to be the case for TVs, where a strong trend towards IPv6 compatibility can already be observed.

2. Wired access service providers

a. Their situation varies considerably. The decision as to which way direction to follow and with what intensity depends on the economic result arising from the cost-to-benefit ratio, which in turn is affected by the drivers discussed in the section titled "Transition drivers."

b. Analyses on which investment decisions will be based need to be detailed and must consider future flows, the multiple positive impacts deployment will bring about as well as the negative impacts it will prevent. Other factors should also be considered, such as the learning curve, future cost declines and other factors relating to the deployment timeframe.

c. The Drivers section shows some of the actions which might be implemented to encourage deployment.

d. In any case, a predominance of the dual-stack technique with CGNAT can be observed.

3. Mobile access service providers. These operators have the best conditions for IPv6 deployment: high rates of broadband user growth, terminals upgraded frequently by users themselves, reduction of marginal costs by expanding and upgrading network technologies, and availability of mobile terminal devices supporting 464XLAT or dual-stack, among others. In this case a predominance of the dual-stack technique with CGNAT can also be observed.

4. Content providers. IPv6 deployment has stagnated for these operators as far as the number of websites accessible over IPv6. Major service providers in terms of weighted average per country (considering [unique users] * [pages viewed]) have made progress thanks to their ability to bear deployment costs, which is not the case for small and medium providers. All things considered, compared to other issues, the impact on the region is not very important at the moment as approximately 50% of websites (weighted average per country) are accessible over IPv6, just as in the rest of the world.

5. Enterprise networks. In principle, the migration to IPv6 does not benefit business results and has no noticeable benefits due to the habitual use of NAT. It is understood that incentives will not arise until the Internet of Things, perhaps combined with Cloud applications, intervenes requiring an enormous amount of addresses which would not be supported by private IPv4 addresses, or by a single network.

6. Non-corporate end users. These users affect deployment in two different ways: on the one hand, they may question their access provider for having deployed IPv6 when user infrastructure was not ready; on the other, if an ISP does not deploy IPv6, users will not be able to access certain applications or service quality may deteriorate due to lower speed and other issues, something which is currently gaining visibility.

4.8 Final conclusions from the analysis

The sector is currently in a transition stage in which there are incentives to improve services over IPv6; likewise, it is facing difficulties, uncertainties and an involuntary lack of coordination among actors.

1. IPv6 deployment is the final and unavoidable situation for Internet networks worldwide.

2. Due to its decentralized nature, it is not possible to coordinate responses and requirements, as these generally lie with different stakeholder groups.

3. Each stakeholder, part of different groups, prepares its own economic estimates, which include multiple inputs (equipment cost reductions, improved learning curve, etc.) with particular impact on the future.

4. The transition drivers discussed in the next section affect the economic analyses conducted by access service providers.

5. Uncertainty creates risks that are incorporated into analyses prior to the deployment decision.

6. The interaction among the different stakeholder groups should also be included as inputs for the analyses. For example, incentives for the deployment of mobile IPv6 networks could have a direct (shared infrastructure) or indirect (user perception of better mobile broadband service) influence on accelerating the deployment of wired IPv6 networks.

7. User infrastructure plays an important role in discouraging (or stimulating) deployment on the part of access providers.

8. No drivers have been identified for content providers nor for enterprise networks. Deployment in these environments will follow at a much slower pace, one that will be determined by the development and growth of the Internet of Things, the migration to Cloud-based services and by user requirements.

9. Training is an essential factor in all these aspects.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

5. ECONOMIC ASPECTS OF THE TRANSITION

An important feature of the IPv6 Internet, one that affects its adoption, is that it is not compatible with IPv4. Thus, IPv6 deployment necessarily involves solving the transition, i.e., providing compatibility or interoperability while IPv6-based infrastructure is developed.

> From an economic point of view, those responsible for IPv6 deployment will do so when they are able to verify that deployment will produce positive economic results, and that these results will be greater if deployment occurs at that particular time as opposed to another. All this with the understanding that the final migration to IPv6 is inevitable. The quantified risks deriving from the uncertainty surrounding this decision-making process and their results should be considered in the analysis and can favor a "sit and wait" strategy or the start of deployment. The model for the economic evaluation of alternatives developed in this research aims at simplifying such decision-making.

It is important to highlight that this economic analysis is highly affected by the timeframe in which deployment is expected, or by the rate of deployment. If the timeframe is long, several factors favor the decision to deploy IPv6, as can later be observed through the economic model:

1. First, equipment costs tend to decline with the increase in the scale of production, which will increase over time considering the volumes pending deployment. In addition, there is a trend towards a decrease in the cost of electronic equipment in general.

2. Current equipment is nearing the end of its service life and is therefore is replaced with IPv6 equipment without having to implement any advanced replacements.

3. The service provider advances in the learning curve reducing costs by streamlining processes and reducing design, installation, operation and maintenance, and other errors. Learning will be applied to a larger volume of equipment and customers, and will thus achieve greater impact.

4. In view of the above, beginning the transition process early is also important. The first stage of this process consists of surveying the current situation for IPv6 deployment.

The process of analyzing economic results includes considerations which are important to the decision-making process. These considerations are presented as transition drivers, which may act either directly or indirectly on the economic considerations mentioned above.

It is reasonable to start by identifying deployment drivers and evaluating their power or the efforts they require. These drivers are numerous and affect the various actors in different ways, also depending on whether they experience high or low address utilization growth rates.

5.1 Transition drivers

Some of the most well-known drivers and their impact on IPv6 deployment are described below.

5.1.1 Shortage of IPv4 addresses

The main driver for the transition from IPv4 to IPv6 is the growing shortage of IPv4 addresses required due to the increase in services, number of users, and the use of addresses in applications with massive addressing needs such as the Internet of Things, among others. Although there are techniques that reduce the urgent need for IPv4 addresses, most of these techniques are based mainly on sharing addresses among multiple users. In addition to having a limited service life, this line of evolution decreases Internet quality from multiple points of view, as we have already explained.

These issues related to pure address sharing have led to IPv6 deployment, although mainly subject to the fact that, while IPv6 implementation costs are not very high, quantifiable economic benefits are somewhat uncertain and will occur in the future, leading some sectors to adopt an attitude of "sit and wait" despite knowing that full IPv6 networks are the future.

5.1.2 Network effects

Network effects are manifested through the value contributed by each new user to other users of the network; together, they encourage the development of networks as their number of subscribers increases.

A typical and current example is that which occurs in mobile networks where, under certain economic circumstances, the largest networks tend to become even larger, thus creating the so called "club effect." Mobile users perceive the value provided by other users connected to a network and this leads them to do the same. This approach of observing drivers for the development of IPv6 networks is not successful as an incentive for IPv6 adoption, as it is not clearly manifested on IPv6 networks. The main reason for this is that it is a decentralized network in which each of the main stages of the value chain (network core, access network, content servers and applications) does not have strong effects on the others, and virtually no network effects occur within each stage.

A multilateral and mainly bilateral market between users and content providers is generated through the Internet. This market is clearly developed when CDNs (Content Delivery Networks) are close to end users, and providers are able to charge both groups of users by adopting appropriate policies in multilateral markets. Multilateral markets involve at least two groups of actors which interact with each other through intermediaries, known as "platforms" (or, in this case, providers), in such a way that the benefit obtained by one of the groups by joining the platform depends on the size of the other groups which are part of the platform. Therefore, indirect network effects appear due to the emergence of CDNs required by users.

The disparity in the values of the main IPv6 deployment indicators (previously analyzed when developing a joint LACNIC/CAF ICAv6 indicator) seems to be showing that there may be significant progress in IPv6 deployment in content servers and applications or at network core level, but not in access networks. Indeed, in the LACNIC region, while in all but four countries we observed user indicator values (access network) lower than 1%, we observed content (content servers and applications) and transit indicators (core network) with average values of the order of 50%.

Thus, it can be concluded that network effects (both direct and indirect) are low or inexistent.

5.1.3 Steps taken by major players in the IPv6 field

Another mechanism for advancing technology occurs when major industry players adopt a certain technology. This phenomenon occurred in the telecommunications industry at the start of 4G deployment. Until 2008, there were two sets of standards that could potentially be used for developing mobile broadband networks: on the one hand, those managed by 3GPP (GSM, EDGE, UMTS, HSPA, LTE) and 3GGP2 (CDMA2000 1x RTT, CDMA2000 1xEV-DO, CDMA2000 1xEV-DV, UMB); on the other, WiMax (which had fewer possibilities). All of the these were being considered by the ITU. On this date, Verizon Wireless made a rather unexpected announcement: they would be abandoning 3GPP2's UMB in 2009 and deploying LTE on their newly acquired 700 Mhz spectrum bands. This made LTE the dominant technology against 3GPP2's UMB and highly accelerated the deployment of LTE services even when there would be no LTE-enabled terminals until 2010. Today, LTE is the de facto standard for 4G technologies and the basis of the evolution towards 5G.

As for IPv6 deployment, major players in the content market have already deployed IPv6, among them Google, Akamai, Facebook and others. However, it was not enough to encourage the deployment of access networks due to the still limited perception of users and the non-promotional use by the few ISPs deploying IPv6.

It is believed that, if major providers in each country begin deploying IPv6 on their access networks, the inherent advantages of this technology mean that this will encourage other providers to deploy the v6 protocol. This effect occurs within each country, which is why it is important for each country's leading operators to begin deploying IPv6 — in addition to improving the quality of Internet access services, this will also improve the economic equation in case of high growth rates, thus encouraging widespread IPv6 adoption. Governments might encourage these actions by applying fiscal incentives consisting of predefined amounts or valid for certain periods of time: for example, tax exemptions on the import of IPv6-compatible equipment during a number of years, or tax deductions in case of investing in IPv6 equipment.

As part of a policy of deploying IPv6 at national level, government users can also promote IPv6 adoption by mandating IPv6 compatibility when purchasing equipment and systems, and even requiring that access providers allow native IPv6 connectivity. In this sense, governments play an important role in IPv6 dissemination.

In addition to the actions of government institutions, training activities also continue to be important.

5.1.4 Improved user experience

While still a technically viable option, maintaining a network using the IPv4 protocol implies a gradual increase of the difficulties faced by users, including the inability to simultaneously open all desired applications due to a lack of ports with the same address, increased delays, higher failure rates, a lack of public addresses

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

for the enterprise network to allow applications and promote the development of the Internet of Things, etc.

5.1.5 Government actions

In the case of actors dealing with (at times) conflicting incentives as regards to when to deploy IPv6, government actions play an important role in their decisions.
Initially, the following government actions were identified.

1. IPv6 deployment within government, public education, research and other government institutions, attempting to achieve greater uniformity. Due to their size, these institutions could strongly promote IPv6 deployment among service providers.

2. Tax exemptions or other types of time-limited fiscal incentives for all investments involving the migration to IPv6.

3. Coordinating with access providers and equipment vendors actions for the approval of IPv6-compatible equipment at user level.

5.1.6 Summary of IPv6 deployment drivers

1. ↑↑ Growing shortage of IPv4 addresses and problems with initial address sharing techniques.

2. ↓ The benefits of migrating to IPv6 are certain, but uncertain in time. There is no clear equation for determining the urgency of IPv6 deployment.

3. ↑↓ Low or inexistent direct and indirect network effects.

4. ↑↑ IPv6 deployment in the access networks of each country's leading providers. Promotion through tax exemptions limited in time or amount.

5. ↑↑ IPv6 deployment in government user networks through guidelines and policies in public procurements.

6. ↑↑ Improved user experience when using native IPv6.

7. ↑↑ End-user device certification.

5.2 General comments on economic aspects

This paper analyzes various aspects of the transition to IPv6, technologies, points of view of the different players, drivers, player interaction, state of evolution at the different stages of the value chain, advantages and disadvantages, factors involved in decision-making processes, key development indicators, and the joint LACNIC/CAF ICAv6 indicator.

This section will take a closer look at the economic aspects involved.

As in the early stages of any new technology, it is currently difficult to obtain precise and detailed information from several reliable sources regarding the costs and benefits involved. A detailed study involves understanding not only the initial fixed and variable investments required depending on the number of users (including operation and maintenance costs), but also the costs in terms of training, hiring special services, progress made along the learning curve, and positive and negative impacts on demand, among others. In the early stages, these costs are often important, as they depend mainly on the type of organization, its stage of development, the availability of trained and specialized personnel within the institution and within the market, vendor support, etc. In addition, many of these costs may vary depending on the actions undertaken by other players in the value chain.

This situation, including the procedures which should be followed to assess various economic aspects, is also noted in recent documents such as the report approved in October 2014 by the OECD Committee on Digital Economy Policy[7]. In turn, this document makes several references to the cost estimates prepared by Lee Howard, Director of Network Technologies at Time Warner Cable USA, who also expressly stated the difficulties encountered in estimating the costs involved in the deployment of CGNAT and IPv6.

As described later, in this document the consultant advances this economic evaluation of alternatives by developing a model that considers the main costs and evaluation procedures, including a prospective analysis of the transition and the effects of time through the rate of opportunity cost of capital. It does not seek to determine profitability due to the limited degree to which income may vary. When deciding the right time for IPv6 deployment, what matters is determining which alternative involves the lowest cost based on its net present value — this is how this model operates. As to the costs employed, these have been parameterized so that each user of the model can adjust them to fit their unique situation. Likewise, the values initially included in the model were gathered from multiple sources and interviews.

7 OECD (2014), "The Economics of Transition to Internet Protocol version 6 (IPv6)", OECD Digital Economy Papers, No. 244, OECD Publishing.

For example, in the section titled "Overview of benefits and costs for different players within the platform," the OECD document notes the following:

"A common theme in this section is the difficulty of obtaining hard data on benefits and costs of deployment for each player. Rather than providing such estimates, here the document seeks to describe some institutional factors that influence the costs and benefits to deployment - and so, through the probit model, inform the understanding of adoption decisions - for different players in the platform."

Regarding access providers (ISPs), the document states the following:

"The payoffs to adopting IPv6 compared to various alternatives have probably been investigated more extensively for network operators than for any other group in the platform (e.g., Howard 2013a, 2013c; Chandler 2012, 2013). Still, hard data are very difficult to obtain. As is common in any enterprise IT deployment, the returns to adopting new technologies are very uncertain. This is particularly the case for IPv6, where the payoffs for adoption depend in a very complicated way on the decisions of other players in the ecosystem … Moreover, as noted above, there is a wide range of approaches to deploy IPv6, and the costs and benefits of different deployment strategies will depend in a very significant way on legacy infrastructure investments. Thus, estimating ex ante deployment costs in any particular setting will be hard."

5.3 Prior work aimed at evaluating different alternatives

This section presents the results of the information survey conducted by Lee Howard[8] which, even while Howard himself warned about the lack of accuracy of the data he was provided, makes a simple evaluation of different post-IPv4 runout alternatives, including the costs for content providers.

In any case, it is an important precedent which implies a first attempt to quantify the costs of various alternatives in view of the shortage of IPv4 addresses, and focus attention on the main factors which must be considered during the decision-making process.

Although the results are not precise, this work provides an initial idea of how specific costs impact total costs. Of course, any costing conducted for decision-making purposes must consider many other factors which have already been discussed, as well as the effect of time and the opportunity cost of capital.

Some major costs obtained during our meetings with the ISPs (e.g., CGNAT, CPE) are validated in the description of the model developed by the consultant, thus advancing with a model that takes into account the present value of future actions.

5.3.1 CGNAT deployment

The use of CGNAT appears to be necessary in many situations involving the transition to IPv6, or when an operator decides to maintain its network operating on IPv4. One alternative is to purchase IPv4 addresses, which is appropriate in certain situations, even in conjunction with deployment CGNAT.

The analysis[9] presented in this section is simple yet consistent with the difficulties in obtaining accurate information. Understanding the cost of CGNAT deployment and the purchase of IPv4 addresses can serve as a reference when evaluating which decision to make. The idea behind this analysis is to provide a first approach to the economic study of migration through CGNAT.

The analysis is based on an initial module of 10,000 users which were studied to determine the costs involved.

First, the undesirable effects of introducing CGNAT are analyzed in terms of failures and complaints relating to applications. Four main groups are considered which at the time of conducting the study had problems on CGNAT testbeds. Likewise, PS3 presents problems with CGNAT and issues are even being reported when using PS4 with multi-player games in cases where public IPv4 access is not available. With regard to P2P, as a basic rule, "downloaders (leeches)" are also simultaneously "uploaders (seeders)," at least in an acceptable proportion; if the user's computer is behind NAT, it is not visible from the Internet and will have problems with P2P. With Netflix, problems tend to appear when multiple customers using the same IPv4 download videos. When analyzing this situation, the number of calls to customer support is estimated as well as the number of users who disconnected due to these problems. The number of potential customers per 10,000 customers were taken from equipment sales and service statistics. The negative effects of CGNAT on our region's countries are significantly lower than the effects analyzed in this case, both in terms of support incidents and in terms of ARPU. Consequently, the model developed by the consultant introduces baseline values that are appropriate for the region and result in lower costs for the CGNAT alternative.

8- https://www.youtube.com/watch?v=_iHIQ55cR-w at LACNIC 21. May 2014
9- Lee Howard. Internet Access Pricing in a Post-IPv4 Runout World. Time Warner Cable

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

The following is a summary of the percentage of application failures due to CGNAT, calls made to the call center, and number of disconnections.

Use	Number of potential users w/o sales	Affected (%)	Affected	Calls to the Call Center (%)	Number of calls to the Call Center	% who cancel the service	Number of lost users
PS3	1100	50%	550	25%	137	25%	137,5
P2P	1500	80%	1200	25%	300	25%	300
Netflix	1200	5%	60	25%	15	25%	15
Misc.	800	100%	800	25%	200	25%	200
	4.600		2.610		652		652,5

As for the cost of CGNAT per 10,000 customers, the cost for customer support calls and provider's loss of customers are estimated as follows:

CGNAT hardware	$70,000
Logging systems	$10,000
Software development	$10,000
Total CAPEX for CGNAT	$90,000
Annual OPEX: Space, power, cooling, staff, etc.	$10,000
One-time OPEX for 652 calls at $20/call	$13,040
Loss of revenue considering an annual ARPU of $400 and 652 lost customers	$260,800

The following table summarizes the main items that make up the costs, disregarding the effects of time and cost of capital.

Year 1	Year 2	Year 3	Year 4	Year 5	
$18.000	$18.000	$18.000	$18.000	$18.000	CAPEX (depreciation)
$10.000	$10.000	$10.000	$10.000	$10.000	OPEX
$13.040	0	0	0	0	Customer support
$261.000	$261.000	$261.000	$261.000	$261.000	Loss of income
$302.040	$289.000	$289.000	$289.000	$289.000	Annual totals
				TOTAL	$1.458.040

Thus, the cost of implementing CGNAT per customer, per year, for 10,000 customers is $29.

5.3.2 Estimated cost of dual-stack

In order to analyze the cost of deploying IPv6 and setting up a dual-stack network and related ongoing operational costs, Lee Howard consulted a large number of experts, among them IETF document authors, business executives, etc. He calculated estimates for three groups: content providers, Internet service providers (ISPs), and consumer electronics.

These costs represent a worst-case scenario for dual-stack deployment (they ware estimated as such) and can be reduced as follows: 1. deployment costs can be reduced by starting sooner so as to spread these costs over time, and 2. operational cost can be lowered by eliminating IPv4 as soon as possible, thus limiting the time dual-stack is supported.

Cost of deploying dual-stack

In the case of data center, hosting and content providers, Howard did not obtain precise information but rather % of revenue or similar values. He then estimated the average annual revenue per user ($40) and obtained the deployment costs shown in the table below ($1 + $6). Costs per user are separated into application development and monitoring and security systems.

As for ISPs, CPEs represent the highest cost because they include not only the equipment itself but also a visit to the customer's premises. After checking with various ISPs, he obtained values ranging from $30 to $90 and therefore assumed a cost of $50 per CPE replaced. Moreover, because a large part of CPEs are new, he assumed that only 50% would have to be replaced. In this case, reference is made to non-HFC fixed access providers.

It should be noted that this situation does not occur in the LACNIC region, where the percentage of CPEs which will need to be replaced will be significantly higher, typically close to 100%. Moreover, the situation of fixed access providers is different from that of mobile access providers and those using hybrid fiber-coaxial networks (HFC). The alternatives for mobile networks have already been described, as well as the specific case of how to implement the transition in an environment where customers purchase their own terminals. The situation is more complex for HFC deployments, as the cable modem must be replaced along with the central controller system (CMTS) and the relevant management systems. As for CPE costs, lower values were determined during interviews, which were then averaged and included as baseline values in the model developed in this report.

In addition to this one-time cost, NOC support staff training costs must be added at a rate of $150 (2-3 hours) per person needed to support 1,000 customers. That is equivalent to $0.15 per customer.

Finally, they estimate that deploying IPv6 for end-user or consumer devices considering, for example, 1.000.0000 IPv6-enabled mobile phones, would cost $0.30 per device.

Initial deployment costs are as follows:

Data Center, Hosting, & Content Providers	Security and monitoring systems	$1 per user
	Application development	$6 per user
ISP	Training at the NOC	$0.15 per user
	CPE	$25 per user
Consumer Electronics	Labor (development)	$0.30 per device

Recurring operational costs of dual-stack

After analyzing content, hosting and datacenter service providers, he reaches the following conclusions:

The cost of developing applications for deployment is $6 (according to the information available, this cost is calculated as 10-30% of the company's R&D cost). He accepts the same percentages and values for the recurring development cost, which thus represents $6 per user per year (PUPY). This value is much lower in the specific case of hosting providers, as this type of operators do not have to develop any applications except those needed to ensure the proper operation of the hosting service. As for operational costs, he assumes that IPv6 only increases by about 1% to 5% the part of

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

operation and maintenance costs potentially affected by IPv6, which he in turn estimates as 20% of total OPEX (a logical estimate if one considers only marginal costs); thus, he estimates a cost of $0.08 PUPY.

For access providers he estimates the following annual costs:

1. Network engineering costs, including router testing and testing of other equipment to be deployed. He estimates an additional 10% of effort will be needed for IPv6-specific testing before deployment. An increase of 5% in OPEX due to Network Engineering is also estimated. The total would be $6.40 PUPY.

2. Operational costs are very low and consider the support provided through phone calls and other means. He estimates these costs as $0.25 - $1.27 PUPY.

Total cost of deploying dual-stack

The costs described above can be summarized as follows:

	Deployment costs	Recurring operational costs
Data Center, Hosting, & Content Providers	$7 per user	$6.08 *PUPY*
ISPs	$25.15 per user	$7.50 *PUPY*
Consumer Electronics	$0.30 per device	$0 per device

5.3.3 Cost of purchasing IPv4 addresses

Another temporary alternative is to purchase IPv4 addresses to continue supporting customer growth. The costs involved are discussed in this section.

The following table summarizes the costs for each IPv4 address, classified by tier. The most accurate data is for Tiers 0 and 1. Tiers depend on how the addresses were used before their sale.

Tiers	Address features	Cost per address	Availability as at May 2014
Tier 0	Remaining RIR space	$0.03 – $4	74,000,000 (LACNIC, ARIN and AFRINIC)
Tier 1	Unused Large blocks with very little use or blocks not used at all	$9 – $12	480,000,000
Tier 2	Underutilized Implies internal reassignment and regrouping addresses	$10 – $16	520,000,000
Tier 3	Replaceable	> $100	All addresses

This is the situation according to the anticipated demand.

	2015	2016	2017
Estimated demand.	310 M	330 M	350 M
Supply. Unused.	100 M	0	0
Supply. Underutilized.	520 M	290 M	0
Cost	$9 - $16	$16 - $20	?

5.4 Cost summary[10]

1. CGNAT: $29 per user per year.

2. Dual-Stack:

a. ISP: $12.50 per user per year ($25 in 5 years and $7.50 per year for operations).

b. Content Providers: $7.48 per user per year ($7 in 5 years and $6.08 for operations).

3. Purchasing IPv4 addresses: At least $9-20 per new user per year, at least until 2017. The cost per address might then continue to rise.

10- Adjustments have been made to include all costs.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

6. MODEL FOR THE ECONOMIC COMPARISON OF VARIOUS TRANSITION ALTERNATIVES

A model for comparing economic alternatives is presented in this section which is designed mainly, but not exclusively, to allow fixed ISPs to measure incremental costs of three basic solutions to deal with the shortage of IPv4 addresses. Its goal is to offer a means to quantify the costs involved in each alternative, taking into account all incremental factors and the effect of time and rate of opportunity cost of capital.

It does not include the analysis of revenues, costs, expenses and investments that are not incremental to IPv6 deployment or solutions for supporting the shortage of IPv4 addresses.

This model can be used for a mobile ISP or a fixed HFC network, adjusting the main costs according to the specific network and technique used.

The model is highly parameterized and can be easily adapted to different situations. For example, it is possible to change the number of customers, growth rates, CPE deployment strategy, future price changes, as well as other variables.

The basic mechanism for comparing different alternatives consists of calculating the net present value (NPV) of cost flows, expenditures, lost income and investments with a parameterized rate of opportunity cost of capital. This allows a simple comparison of the future economic impact of the decision to adopt each alternative.

6.1 Alternatives

The following three alternatives have been adopted. All three are considered essential for making a decision from an economic point of view and their implementation should be considered from the moment when the ISP's IPv4 addresses are exhausted.

An ISP can choose to postpone these actions whle it has the IPv4 addresses needed to continue to grow. In any case, best practices indicate that it is desirable not only to prepare in advance for such exhaustion, but it is also appropriate to begin the transition in the core, in the distribution network and in other areas where the difference in the cost of replacing equipment or software by IPv4-only or dual-stack equipment is not relevant. A more detailed analysis of ISP actions and best practices is presented in other sections of this document.

Likewise, many operators are starting to worry about the fact that IPv6-only sites will start appearing shortly.

1. Alternative 1: Deploying an IPv6 transition technique, while seeking compatibility with applications and servers that only support IPv4. Dual-stack with CGNAT is used, the technique most commonly used in the region, although the model can be used for other techniques as well. Thus, the network operates over IPv6 for all content and applications that support this protocol, while IPv4 is used as necessary. This alternative does not require an increase in the number of IPv4 addresses and address sharing is the same as in the alternative of using CGNAT44 only. However, it does not have the same negative effects as the technique based solely on CGNAT44, given that fewer user applications will employ shared addresses. As we have seen in this document, all applications which can run on IPv6 and those not operating behind CGNAT will use native IPv6. In turn, the number of ports per user and address sharing will decrease, meaning that the effect on applications will not be not be reduced due to the limitations on the number of ports which can be opened simultaneously.

2. Alternative 2: Deploying or continuing to deploy the CGNAT44 technique and share IPv4 addresses at the service provider level. In this case, IPv6 is not deployed on the network. Both the provider's network as well as customers continue using IPv4-only equipment. This alternative involves costs and losses derived from operational problems behind CGNAT, as well as the limitation on the number of ports allowed per IPv4 address.

3. Alternative 3: Purchasing IPv4 addresses to support the growth of the number of customers without resorting to address sharing. This "sit and wait" approach may be a valid alternative in cases where there is little growth. As already mentioned, this alternative shares the drawback noted for the previous alternative: IPv6-only services might begin to be deployed on the Internet, in which case both alternatives could generate unsolvable problems in the future.

6.2 Description of the model

Aimed at helping decision-making processes, this economic model is simple and direct in its conceptual structure. Difficulties in determining the quality of the results provided by the model depend, as always, on the robustness of the initial data and on the technical and

commercial analysis of the drivers and other factors affecting the model. The model presented in this report already contains the basic elements of a comprehensive and detailed analysis.

The most relevant general aspects of each alternative are described below.

6.2.1 General aspects

The following parameters and general assumptions are considered:

1. The evaluation period covers a 5-year span, which is considered sufficient due to the evolution in IPv6 deployment which can generate huge changes in a few years. For example, it is quite possible that IPv6-only sites could begin appearing in that period.

2. The model provides two options for replacing CPEs:

a. For the migration to dual-stack CPEs (Alternative 1), the model considers the investment needed to replace obsolete IPv4-only CPEs with dual-stack CPEs, plus the investment needed to provide dual-stack CPEs to new customers. For the case of replacing IPv4-only CPEs, the model allows freely establishing the number of years during which this replacement will be completed (starting from the first year). It accepts full years or fractions thereof.

b. For the case of replacing IPv4-only CPEs with other IPv4-only CPEs (Alternative 2, use of CGNAT only), service life can be extended from the initial 5 years.

3. For CPE costs, the model allows entering IPv4 and dual-sack CPE values in year 1; it also allows establishing the estimated annual drop in CPE prices as well as the reduction of the price difference between both types of CPEs up to a maximum of 20% (five years until prices are equal).

4. The main output is the net present value (NPV) of the flow of investments, costs, expenditures, and incremental losses for each alternative.

5. Prior investments with residual capacity to meet customer growth may already exist for Alternatives 2 and 3. The model considers these under "Idem but already served with IPv4 addresses, and CGNAT with the design number of sessions."

6. Not included in the model are investments in the core and distribution network, as these are virtually identical for IPv4-only and dual-stack, and the model only determines the incremental costs needed to decide which alternative to follow. In other words, including these investments in the model does not change the relative ranking of the different alternatives in terms of their calculated NPV.

7. Previous investments in dual-stack CPEs are not considered as in that case the decision to migrate to IPv6 would have already been made, thus rendering the use of the model irrelevant.

8. Spreadsheets II and III (basic data and cost information) allow changing, aggregating or disaggregating different items and then taking them into consideration in the final calculation.

9. The term "customers" refers to users (CPEs) directly connected to the provider's network.

10. The term "users" refers to those connected to the service provider behind CPEs.

11. If the total number of customers served with CGNAT is taken into account, only Alternatives 1 and 2 are considered as it is understood that an evaluation is being made as to whether to continue using only CGNAT or to start deploying IPv6 while maintaining the use of CGNAT. In both cases, if CGNAT capacity already exists, this capacity is deducted from NAT growth requirements.

12. It is assumed that, when using IPv6 together with CGNAT, the reduction (in percentage) in the use of CGNAT sessions is equal to the complement of the CONT indicator (% of accessible sites in IPv6). As at 18 November, the average CONT indicator for the LACNIC region was 50.77%; thus, the model considers that the use of IPv6 reduces the minimum number of required sessions to 49.23% of those needed when using CGNAT only. The value of this parameter can be changed in the model.

13. When introducing IPv6, this reduction of the number of CGNAT sessions applies only to customers with IPv6. Therefore, the number of sessions that must be available each year is equal to the number of sessions (reduced considering IPv6 traffic) for dual-stack customers, plus the number of sessions of those customers who are still using IPv4 only with CGNAT, i.e., the total number of customers minus those who already have dual-stack CPEs. For determining the model's "Minimum design number of incremental sessions for CGNAT," the number of sessions installed to serve customers using CGNAT at time 0 are subtracted from the total number of sessions per year.

14. It should be noted that, under certain circumstances, the parameters input for a specific year might result in the need for fewer sessions than for the previous

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

year, thus making further investments in CGNAT unnecessary. In this case, the incremental investment in CGNAT reflected in the "Asset and Expenditure Flows" spreadsheet will be 0.

15. According to the analysis included in the "Use of NAT" section regarding the effect of a reduction of the number of sessions on service quality, the control panel assumes a minimum number of 1,000 sessions per user. At the same time, it is assumed that 30% are active during peak hours and that there is an average of 3 users per CPE. These values are parameterized in the model.

16. Regarding the cost of CGNAT, the costs entered into the model were obtained from at least four independent sources with which interviews were held. CGNAT costs are entered in the model in proportion to the number of sessions required. Purchases are actually modular, so, in order to obtain more precise values, when entering costs it is necessary to use the proper modularity.

A reference capacity of 10,000,000 sessions is used simply to standardize the cost per session. The total cost for 10,000,000 sessions was obtained considering different configurations for various capacities analyzed during interviews.

17. As for the replacement of CPEs with dual-stack equipment, it is estimated a stable flow of CPEs is replaced each year due to obsolescence. This flow is equal to the total number of CPEs in year 1 divided by their service life, or by the period of time set by the ISP for their complete replacement (in years and fractions thereof). At the same time, a number of dual-stack CPEs is added which is equal to the number of new customers per year.

18. Planning, network design, installation and other costs incurred are included under equipment costs.

19. For cases of disconnection and claims resulting from application issues caused by CGNAT44, the causes for claims and disconnections are considered to be unrelated. This means that no customers are simultaneously dissatisfied with more than one application. Also excluded are the effects resulting when an ISP provides a public address not subject to CGNAT to customers who are dissatisfied due to the effects of address sharing. Users of the model can always modify the parameters relating to CGNAT effects on applications by taking these actions into account in Table "I.3 Applications and the impact of address sharing in the alternative consisting of CGNAT with no transition to IPv6."

20. The percentage of the number of calls involving claims applies only to new customers each year.

21. The percentage of customer loss due to disconnections resulting from quality of service issues applies to the "Aggregate total net potential connections for new CGNAT-only customers," as it is assumed that for those who were disconnected the loss of ARPU is spread over time.

22. Churn is not included, as the sole purpose of the model is to quantify the effects of IPv4 address exhaustion and those of potential alternatives.

23. In cases where IPv6 is deployed, the negative effects of CGNAT on applications is not considered, as this would lead to additional costs for two reasons:

a. If customers have problems because they are still using a private IPv4 address, the ISP can install a dual-stack CPE, in which case the applications experiencing negative effects will stop using CGNAT.

Here it is assumed that the ISP has a dual-stack distribution network in the customer's area, such that installing such a CPE is possible.

b. When customers have dual-stack, CGNAT is used for applications that have no issues with this technique, in which case its effect on the service is negligible.

24. Considering its centralized nature, operating expenses for the CGNAT44 network are assumed constant until year 5. This assumption should be revised in the case of very large networks/.

25. Customers' ARPU is assumed constant over time.

26. In Alternative 3, it is not necessary for the provider to purchase addresses at time 0 because these are already available, but will only need to do so in the following years. It is also assumed that addresses are not purchased for stocking purposes but only to meet the provider's demand.

27. Price growth rates are adopted for cases of IPv4 addresses for years 3 to 5. The actual variation may be higher or lower than estimated due to an increase in address shortage or due to new addresses on the market derived from the transition to IPv6.

28. Income from the sale of IPv4 addresses is not considered in the model as IPv6 use increases in the case of Alternative 1.

6.2.2 Alternative 1

This section considers the case of a provider that decides to begin deploying the transition based on the use of dual-stack. Given that this is a decision-making model based on alternatives, no deployment is considered implemented at this time. In case of deployment, the model would not be of interest because the decision was already made. Therefore, the model takes into consideration all current customers and planned growth rates.

6.2.3 Alternative 2

Both options in the model are considered in this alternative: the provider has already deployed CGNAT and will continue to do so, with or without CGNAT residual capacity, and that the decision is being made to start the deployment due to the absence of IPv4 addresses in stock.

6.2.4 Alternative 3

In this case, it is considered that the provider purchases IPv4 addresses as needed according to its growth. The alternative where there are addresses in stock is not considered.

6.2.5 Conclusions

The model shows the final table in the Control Panel, which also includes a table of the main physical parameters, both of which are shown in the image below.

Control Panel

I.1 NLV of the Costs of Each Alternative

	Net Present Value
Alternative 1, transition with dual-stack and CGNAT with CPE	$4.910.952,82
Alternative 1, transition with dual-stack and CGNAT without CPE	$2.312.338,22
Alternative 2, using CGNAT without implementing IPv6	$6.192.207,28
Alternative 3, purchasing IPv4 addresses without NAT or IPv6	$4.077.689,49

I.2 Main Parameters

Rate of opportunity cost of capital.	12%
Service life of dual-stack CPEs or timeframe for replacement of IPv4-only CPEs with dual-stack CPEs	5,0
Service life of IPv4-only CPEs. Alternative 2.	5,0
Total number of current residential customers	100.000
Idem but already served with IPv4 addresses (CGNAT or individual IPv4 addresses)	50.000
Annual customer base growth rate	15%
CGNAT operational capacity – simultaneous sessions – calculation module	10.000.000
Maximum average number of sessions per user without dual-stack	1.000
Minimum design number of sessions with CGNAT per user without dual-stack, by quality	1.000
% of IPv4 sessions per user with dual-stack (CONT indicator)	4,92%
Minimum design number of sessions with CGNAT per use with dual-stack, by quality	492
% of users connected simultaneously	30%
Average number of users per client	3
Annual drop in IPv4-only CPE prices	10%
Reduction of the price difference between dual-stack vs. IPv4-only CPEs = 0 in 5 years	20%
Annual ARPU per customer assumed to be constant	$240,00

The model allows modifying parameters, investments, costs and expenditures. While results for the different alternatives can change depending on the data input into the model, it can be seen that, in general, deploying IPv6 with CGNAT, even if the ISP is responsible for the investment in CPEs, is a good option from an economic point of view.

In addition, this is the only alternative in which investments will survive when the use of IPv4 tends to disappear; therefore, all things considered, this is the best alternative in the opinion of the consultant.

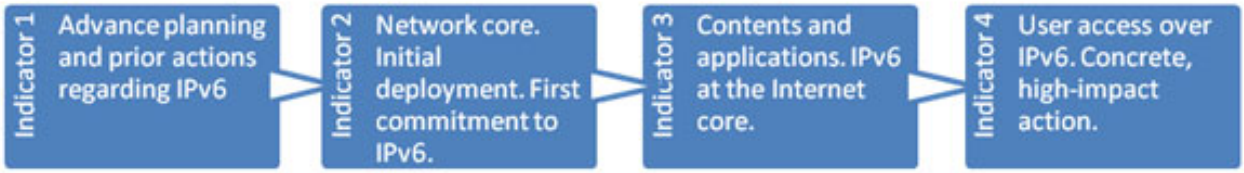
Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

7. CURRENT STATUS OF IPV6 DEPLOYMENT IN THE LACNIC REGION. QUANTITATIVE INDICATORS

7.1 Key Progress Indicators (KPI) of IPv6 deployment

After having analyzed the behavior of IPv6 deployment in the different stages of the value chain, as well as information published by major stakeholders, it is observed that, due to the decentralized nature of the Internet, it is not possible to obtain a single indicator that is highly correlated with the deployment. Therefore, to quantify IPv6 deployment, the position adopted in this case is through indicators that quantify the deployment at various stages of the value chain.

In addition to using these individual indicators to focus on each stage, a Key Progress Indicator towards IPv6 is developed which allows a quick comparison to be made between countries.



In this sense, although various sources have published indicators, Cisco presented a full set of indicators in these four stages, including an extensive explanation of the procedures used for their calculation. These indicators have been carefully analyzed and, in the opinion of the consultant, are currently considered to be the most approximate and fully justified to represent deployment progress at each stage of the value chain. Therefore, they are accepted as secondary sources of development indicators for these main stages in the countries of the region.

For the LACNIC region, a Key Progress Indicator towards a fully IPv6-enabled network is developed which reflects a better analysis of the current situation where most of the countries are in the planning stage. For this LACNIC indicator (LACNIC/CAF ICAv6), partial indicators are used to ponder planning and early actions in the IPv6 deployment process.

As to prior actions, transit Autonomous Systems with an IPv6 prefix are assigned weight, and is taken as an indication that the holding organization is currently in the process of deploying IPv6. It is also believed that it should be given special consideration in the countries within the LACNIC service region.

Furthermore, partial indicators of each stage of the value chain are presented to show the different progress which has been made.

7.1.1 Key IPv6 progress indicator (LACNIC/CAF ICAv6) and indicators for each stage of the value chain

The formula chosen to calculate the Key Progress Indicator towards a fully IPv6-enabled network is shown below.

$$\frac{LACNIC}{CAF} ICAv6\,\% = 0{,}3 * (0{,}1 * PACTO + 0{,}9 * ASTRAN) + 0{,}7 * \sqrt{CONT * USERS}$$

The composite indicators used in this formula are listed below. These indicators will also be used when comparing countries according to the stages of the value chain.

• PACTO: A Spanish acronym that represents the number of allocated IPv6 prefixes with observed traffic as a percentage of the total number of allocated IPv6 prefixes. It is an indicator that the country not only has requested and been allocated IPv6 prefixes, but that some of these already have noticeable traffic. It is given little weight, as it depends on the efficiency with which prefix requests have been handled: a lot of space may have been requested but little space may be in used where less space might have been requested. Although in both cases the use is the same in terms of deployment, in the first case the indicator is lower.

• ASTRAN: Spanish acronym for AS with observed traffic. For the purpose of taking into consideration the AS that provide IPv4 transit with the IPv6 prefix,

besides the AS that provide IPv6 traffic, given that the first show a path towards the future implementation of IPv6 transit, the following average is used as transit indicator:

$$ASTRAN = 0{,}5 * (\%\ IPv6\ Transit\ AS + \%\ IPv4\ transit\ AS\ with\ IPv6\ Prefix)$$

Given that IPv6 Transit AS % = weighted % of AS numbers which are IPv6 transit with regard to AS numbers which are IPv4 transit, and % IPv4 Transit AS % with IPv6 prefix = weighted % of IPv4 transit AS with IPv6 prefix, with regard to AS numbers which are IPv4 transit.

• CONT: The content indicator is the sum of the weighted % of websites accessible over IPv6 plus the weighted % of IPv6-proof domains ("IPv6 embryos" according to LACNIC). It is a mechanism for assigning value to these so-called "IPv6 embryos" which are beginning to prepare for providing IPv6 services, something very useful for the LACNIC region.

• USERS: This indicator is the average % of IPv6-ready users, determined considering the values calculated by Google and those calculated by APNIC. These are two sources that use similar methods but on different universes.

As for the weights:

1. 0.3 and 0.7 are used to give more weight to CONT and USERS indicators, which ultimately show IPv6 utilization results. CONTS*USERS is used because this value is strongly correlated to a country's potential IPv6 traffic. The root mean square value is used to maintain the indicator's proportions.

2. For the first term, 0.10 and 0.90 are used to give certain weight to the use of allocated IPv6 prefixes. The low weight is due to the fact that the percentage of allocated prefixes showing traffic is not a strong indicator of deployment, although it has some value for consideration.

3. In the case of ASTRAN, by using the average, the same weight is given to Autonomous Systems that already have IPv6 transit as to those in the process of providing this transit, given that the latter are already Transit AS's and have IPv6 prefixes.

4. In the case of CONT, both % are added in order to place websites providing IPv6 services on an equal basis as those which are already in the testing stage ("IPv6 embryos").

5. Finally, the average of both sources Google and APNIC) is employed for the Users indicator in order to take into account both universes in which each methodology operates and eliminate possible biases.

7.1.2 Partial indicators of the stages of the IPv6 deployment value chain

During each stage of the value chain, the main indicators to be considered as regards IPv6 deployment are those which arise from technical and operational considerations, can be modified, and are best suited to the development stage to which they refer. It is noted herein that all identified sources of information have indicators that serve these stages in one way or another. Among these is the set of indicators published by Cisco, which, while considered by many as a secondary source, is the best set of indicators for observing the different perspectives for each stage of the value chain.

These indicators are summarized below and their calculation methods can be found in "Annex III. Detailed analysis of quantitative information relevant for the transition to an IPv6 network."

Although all indicators are described, for comparison between countries, the composite indicators used in determining the Key IPv6 Progress Indicator are adopted.

7.1.2.1 Planning. Allocation and routing.

1. Percentage of allocated IPv6 prefixes that are routed, with respect to the total number of allocated IPv6 prefixes. These percentages are published as values and with different colors on Cisco's world map[11].

2. Percentage of allocated IPv6 prefixes with regard to allocated IPv4 prefixes. This value is obtained from the RIR and is published for each country.

3. Percentage of allocated IPv6 prefixes in which traffic has been observed, with regard to the total number of allocated IPv6 prefixes. This value is also published for each country.

7.1.2.2 Network core. Core. Transit AS.

1. Weighted % of Autonomous Systems which are IPv6 transit with regard to the number of Autonomous Systems which are IPv4 transit. (IPv6 transit AS). An IPv6 transit AS provides transit over both IPv4 and IPv6 networks.

11- http://6lab.cisco.com/stats/index.php?option=prefixes

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

2. Weighted % of IPv4 transit Autonomous Systems which have been assigned at least one IPv6 prefix, with regard to the number of Autonomous which are IPv4 transit. (Transit AS which has an IPv6 prefix). A transit AS which has an IPv6 prefix is one which provides transit over the IPv4 network and has at least one IPv6 prefix, but is not necessarily an IPv6 transit AS.

7.1.2.3 Content. Websites

1. Weighted % of sites accessible over IPv6 (considering the number of pages viewed - unique users). It also shows the number of enabled websites over a total of 500 per country.

2. For testing: domain name used for testing in IPv6. Weighted % of domains for testing over the 500 sites analyzed.

3. Failure: AAAA records exist but the website is not operational in IPv6. % of domains which experienced IPv6 access failures over the 500 sites.

4. Others: Websites not IPv6-enabled. % over the 500 sites.

7.1.2.4 Users

1. Google. % of users searching in selected servers with potential IPv6 access, over the total number of searches.

2. APNIC. Idem.

7.1.3 Final values of the selected indicators as at 18 November 2015.

LACNIC countries	LACNIC (18/11/2015)					CISCO (18/11/2015)	
	LACNIC/CAF ICAv6	Planning (PACTO)	Transit AS (ASTRAN)	Content (CONT)	Users (USERS)	Joint % of IPv6 implementation	Country's relative indicator (IR) as compared to the rest of the world. Values from 1 to 10.
Argentina	19,09%	5,58%	66,75%	46,95%	0,04%	16,56%	1,9
Aruba	N/D	50,00%	50,00%	N/D	0,00%	5,00%	0,5
Belize	21,41%	10,00%	34,74%	N/D	0,04%	7,86%	0,8
Bolivia	N/D	10,00%	43,00%	49,74%	3,70%	12,92%	2,5
Bonaire	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Brazil	29,52%	11,91%	55,72%	60,39%	6,74%	26,98%	4,7
Chile	20,43%	15,74%	70,83%	47,38%	0,03%	17,91%	2
Colombia	26,24%	16,54%	93,04%	52,53%	0,02%	24,00%	2,6
Costa Rica	17,81%	11,59%	62,87%	49,12%	0,01%	15,31	1,7
Cuba	29,67%	16,67%	100,00%	52,03%	0,19%	28,24%	3,4
Curacao	N/D	5,88%	0,00%	N/D	0,16%	0,00%	0
Ecuador	41,57%	72,55%	96,96%	47,79%	7,46%	37,79%	5,8
El Salvador	2,76%	5,56%	7,78%	49,52%	0,01%	1,30%	0,2
Guatemala	23,22%	9,09%	78,91%	52,67%	0,11%	20,92%	2,4
Guyana	29,61%	50,00%	100,00%	50,07%	0,05%	26,47%	3
French Guiana	N/D	0,00%	N/D	N/D	0,02%	0,00%	0
Haiti	N/D	0,00%	0,00%	N/D	0,01%	0,00%	0
Honduras	10,89%	7,89%	33,61%	53,68%	0,10%	5,37%	0,7%
Falkland Islands	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Mexico	15,57%	25,25%	51,07%	53,39%	0,04%	12,57%	1,5
Nicaragua	21,70%	6,25%	79,66%	50,76%	0,00%	18,78%	2
Panama	10,64%	3,77%	37,72%	49,64%	0,01%	8,55%	0,9
Paraguay	17,59%	3,45%	63,47%	49,17%	0,01%	13,71%	1,4
Peru	37,05%	28,21%	57,55%	52,67%	16,54%	26,55%	5,6
Dominican Republic	7,09%	10,34%	22,17%	51,76%	0,03%	5,54%	0,6
Saba	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Saint Eustace	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Saint Martin	N/D	N/D	N/D	N/D	N/D	N/D	N/D
South Georgia and The	N/D	N/D	N/D	N/D	N/D	N/D	N/D
Suriname	N/D	66,67%	0,00%	N/D	0,01%	0,00%	0
Trinidad and Tobago	21,81%	16,67%	71,57%	50,41%	0,16%	16,57%	2
Uruguay	23,22%	12,00%	81,82%	48,19%	0,03%	20,77%	2,3
Venezuela	22,33%	16,67%	78,65%	48,26	0,02%	19,40%	2,1
Reference countries							
Germany	46,86%	22,92%	86,34%	43,36%	24,51%	42,45%	7,3
Australia	27,14%	18,84%	69,93%	49,00%	2,47%	23,45%	3,4
Belgium	56,50%	34,47%	82,44%	50,63%	44,45%	53,47%	10
France	34,57%	19,27%	77,49%	51,47%	6,78%	31,55%	5,1
Greece	41,76%	22,22%	71,85%	51,82%	18,55%	39,12%	7
Hong Kong	24,56%	16,46%	71,98%	53,64%	0,82%	19,41%	2,4
India	24,67%	27,63%	73,41%	54,20%	0,61%	21,74%	2,8
Japan	37,39%	30,97%	87,47%	26,18%	12,86%	32,49%	4,9
Luxembourg	43,49%	28,13%	79,64%	54,20%	16,84%	39,39%	6,9
Malaysia	36,42%	22,07%	73,38%	54,53%	9,51%	32,69%	5,5
Norway	40,47%	26,07%	89,55%	54,48%	9,01%	37,22%	5,9
Portugal	47,59%	21,88%	88,63%	53,56%	20,17%	45,66%	8
Singapore	40,18%	92,28%	86,65%	52,53%	7,63%	34,74%	5,4
Switzerland	49,17%	17,76%	83,92%	51,56%	26,72%	47,06%	8,5
USA	43,16%	32,45%	65,74%	48,28%	25,24%	39,55%	7,3

7.2 Conclusions and partial indicators, as well as LACNIC/CAF ICAv6 as at 18 November 2015

The following conclusions were reached based on the indicators that were developed[12].

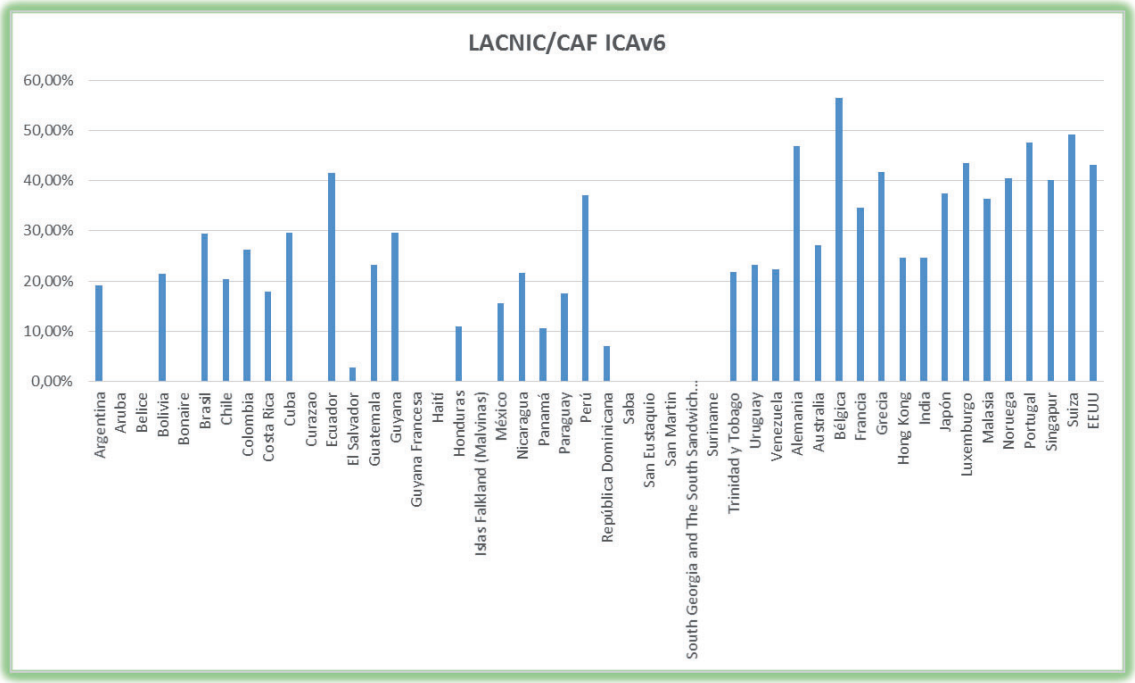
7.2.1 Key IPv6 Progress Indicator, LACNIC/CAF ICAv6

Results of this global indicator for LACNIC countries and for reference countries are seen in the following chart. In general, the countries of the region are at a less developed stage. In any case, progress is slow at global level: the indicator for Belgium, the world leader, is 56.5%.

In this sense, countries exceeding a reference value of 20% for this indicator are duly noted: Bolivia (21.41% with an interesting User indicator value), Brazil (29.52% with an interesting User indicator value), Chile (20.43%), Colombia (26.24%), Cuba (29.67%), Ecuador (41,57% with an interesting User indicator value), Guatemala (23.22%), Guyana (29.61%), Nicaragua (21.70%), Peru (37,05% with an interesting User indicator value), Trinidad and Tobago (21.81%), Uruguay (23.22%) and Venezuela (22.33%).

The LACNIC/CAF ICAv6 indicator has the virtue of presenting a global view of IPv6 deployment based on the four main viewpoints: use of IPv6 prefixes, Core, Content and Users. Thus, a value greater than 20% can be achieved through planning and initial deployment (which can be observed in the region) or through a combination of planning and initial deployment, together with IPv6 in accesses. Values higher than 30% are only achieved in cases where IPv6 deployment is also available for residential access customers. As of November 18, only Bolivia, Brazil, Ecuador and Peru had interesting values in terms of the number of users operating over IPv6.

Later it will be seen how the countries of the region rank differently in each stage of the value chain.



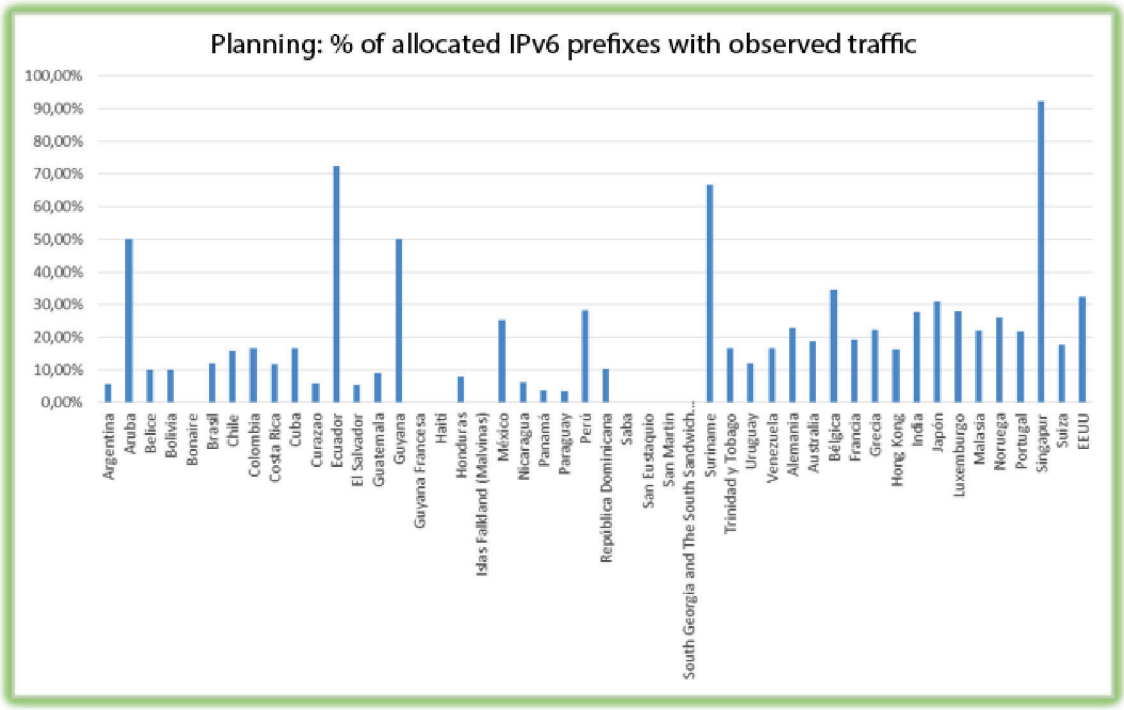
7.2.2 Planning stage

Indicator values for this stage reflect two issues: firstly, the planning stages prior to IPv6 deployment and secondly, the efficiency in the real use of allocated prefixes. The LACNIC/CAF ICAv6 formula gives little weight to this partial indicator precisely for this same reason.

This indicator is expected to increase along with the User indicator to the extent in which the IPv6 access network is developed.

12- In the charts, values which are not available (N/A) in the tables are represented as 0.

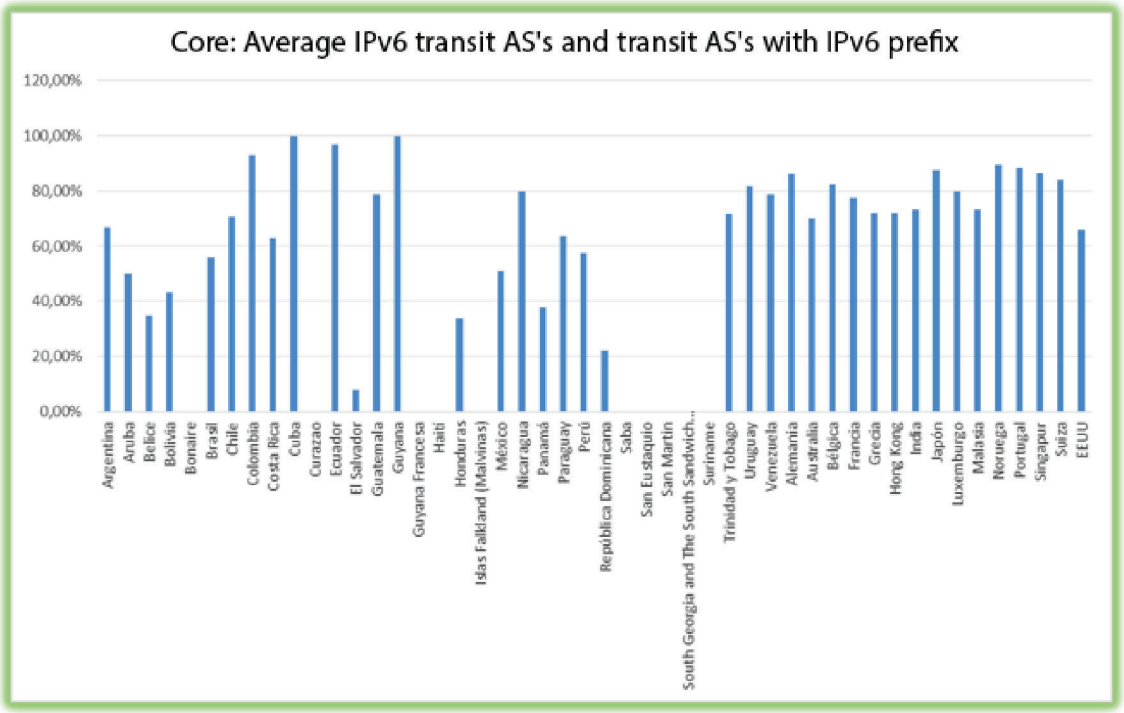
Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222



7.2.3 Core stage

In this stage represented by indicators of AS % providing IPv6 transit, or in a stage prior to providing transit and having IPv6 prefixes, the countries of the region have made less progress than reference countries, but values are generally close. Therefore, no major development difficulties are observed in this stage of the value chain.

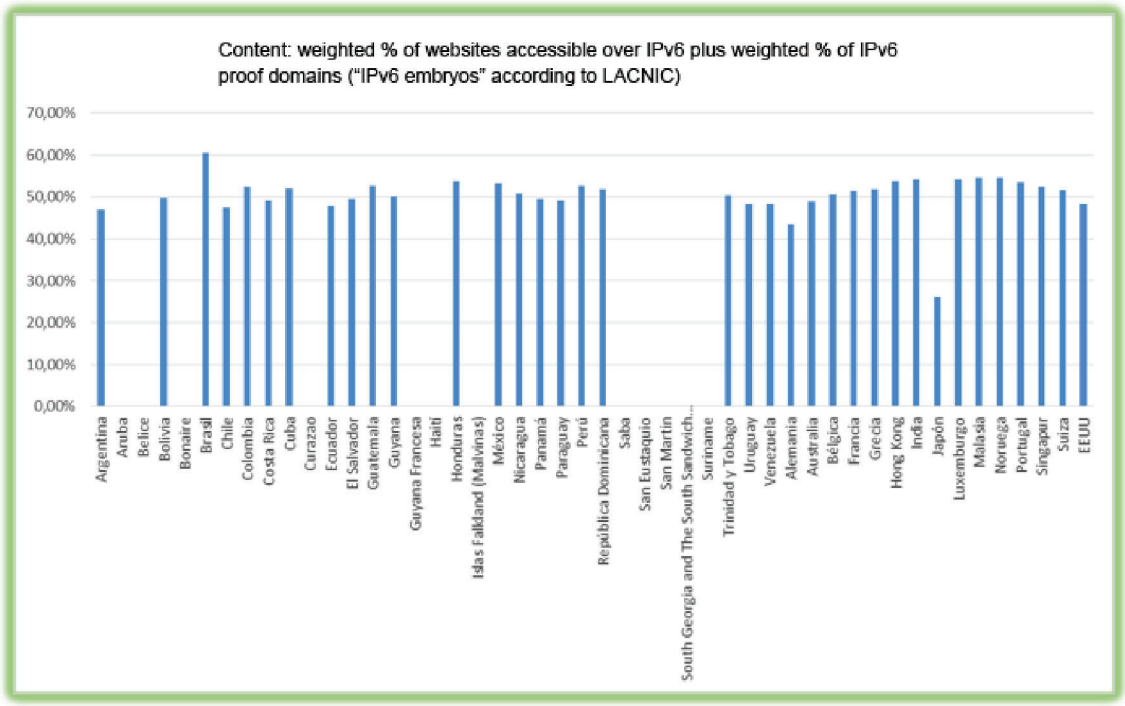
It is also important to note that, in small countries with very few Autonomous Systems, the decision of any of them to provide IPv6 transit causes the % to increase rapidly. Nonetheless, it is a relevant indicator.



7.2.4 Content stage

In this stage, all countries show similar values. This is due to the fact that the list of TOP 500 sites in different countries share many sites. In just one of these websites starts offering services over IPv6, the % will increase in every country where it is used. Examples: Facebook, Google, Youtube, Yahoo, or Amazon. "Local" websites generally have much less weight than these major websites.

Values noted as 0 include those countries where no data was available in the sources which were analyzed.

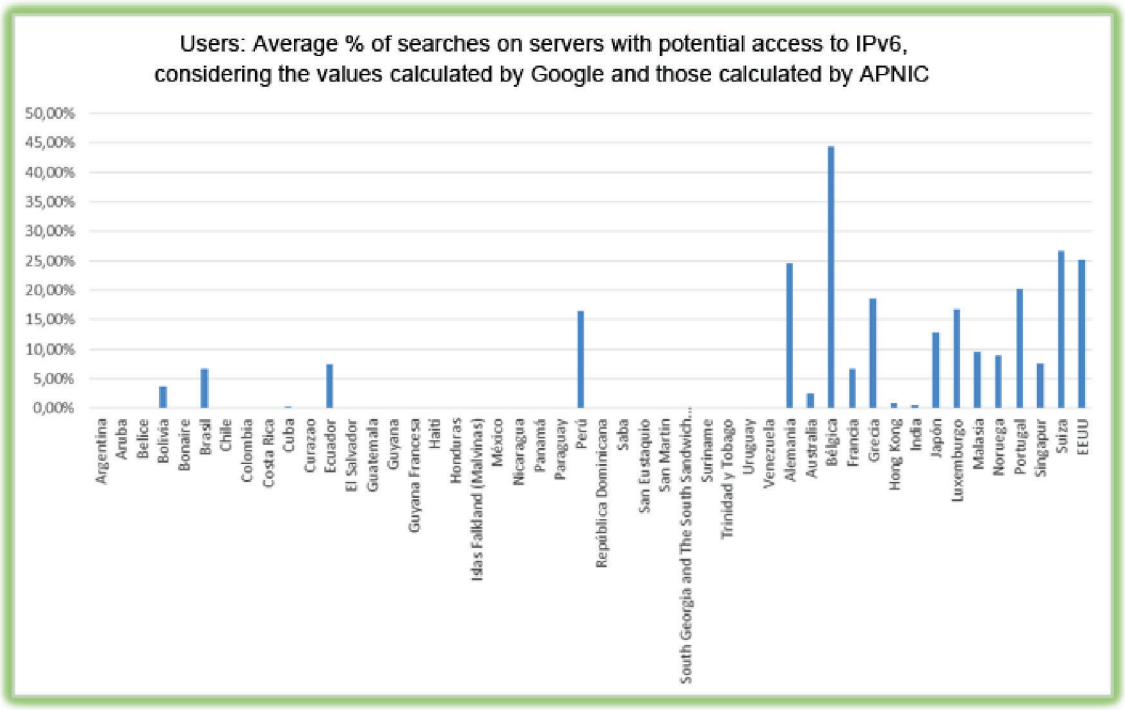


7.2.5 User stage

In general, from the user's point of view, IPv6 adoption levels vary greatly worldwide, although figures are typically higher or much higher than in the LACNIC region. In this region there are four countries where this indicator is greater than 1% according to Google /APNIC / Akamai: Bolivia (2.72% / 4.68% / 2.9%), Brazil (5.9% / 7.58% / 4.9%), Ecuador (7.12% / 7.8% / 6.9%) and Peru (15.5% / 17.58% / 18.0%). Reasonably consistent indicators are observed for the three sources, considering the different universes used in each case.

This indicator is an IPv6 final transition indicator, where users are able to access the Internet via IPv6. Along with the content indicator are the indicators whose result is the % of potential access to IPv6 sites, and a high number of sites correlated to IPv6 traffic.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222



7.2.6 Main conclusion

Measures that tend to increase the User indicator (e.g., upgrading the IPv6 access network, whether at ISP or by the large government or university institution level) will have a direct impact not only on this partial indicator, but also on the LACNIC/CAF ICAv6 indicator due to the 70% weight that justifiably affects the geometric mean of Content and Users.

In turn, an increase in this indicator has a direct impact on users' perception of the Internet.

Consequently, IPv6 deployment in the access network should be the main objective for achieving global IPv6 deployment results.

8. CURRENT STATUS OF IPV6 DEPLOYMENT IN THE LACNIC REGION. SURVEY CONDUCTED.

8.1 Technical fact file

The main objective of the survey was to complement the information obtained through an analysis of quantitative indicators and meetings conducted during field work.

Thus, these three main sources of information are available concerning the situation in the LACNIC region:

1. Primary and secondary indicators of the current transition status, generated from multiple sources.

2. Survey results showing the reasons behind the current status and trends.

3. Results of interviews conducted in the 10 countries included in the sample selected for the research, which provide consolidated information on the current situation, trends and motivations behind stakeholders' actions as regards the transition to IPv6.

A model survey was designed and conducted in the first weeks of the project for the purpose of obtaining information about the different countries on aspects relating to their current situation, reasons for deploying or not deploying IPv6, difficulties encountered or anticipated, among other aspects of interest for the research.

The survey was sent to all LACNIC members, so if the response rate had been 100%, it would have been equivalent to a census. In order to obtain a larger number of replies and more detailed information, it was decided that the survey would be anonymous, thus sacrificing the possibility of linking replies to any specific organization.

The information that was gathered was classified by member groups as follows:

1. ISPs deploying IPv6: % of native customers, technique they use, reasons, difficulties encountered, and opinion on the results of their action.

2. ISPs not deploying IPv6: reasons for not deploying, deployment time frame, and expected difficulties.

3. Non-ISPs deploying IPv6: reasons for deploying IPv6, difficulties encountered, and whether results benefited the organization.

4. Non-ISPs not deploying IPv6: reasons for not deploying IPv6, deployment time frame, and expected difficulties.

Responses were satisfactory and are summarized in the table below:

	Large	Medium	Small	Total
Spanish	29	113	250	392
English	5	17	35	57
Portuguese	7	218	458	683
Total	41	348	743	1132
Universe	148	1374	3178	
Response rate	28%	25%	23%	

The basic parameters of the survey were as follows:

1. Universe: End Users / Small and Medium members / Large members. The universe totaled 4,000 members.

2. Quantitative methodology: Online survey sent via e-mail using the database provided by LACNIC

3. Unit of analysis: Heads of the departments responsible for maintaining relations with LACNIC.

4. Maximum duration of the questionnaire: 5 minutes.

5. Field work: July-August 2015.

8.2 Results

Results relevant to this report are presented below.

Results segmented by country, along with the total for the region[13], are shown in various charts. Results per country may include few replies for each segment, mainly due to the small number of organizations which exist in many countries and the fact that, as already seen, only about 25% of these replied. For this reason, it is advisable to use these results together with the indicators in order to have a more detailed view of what is happening in each country. In the ten countries in which face-to-face meetings were held, an additional source of information on the current status, behavior and rtends among LACNIC members was obtained.

13- The source for the charts is MERCOPLUS Latin America, which was the company that performed the field work and processing of the survey.

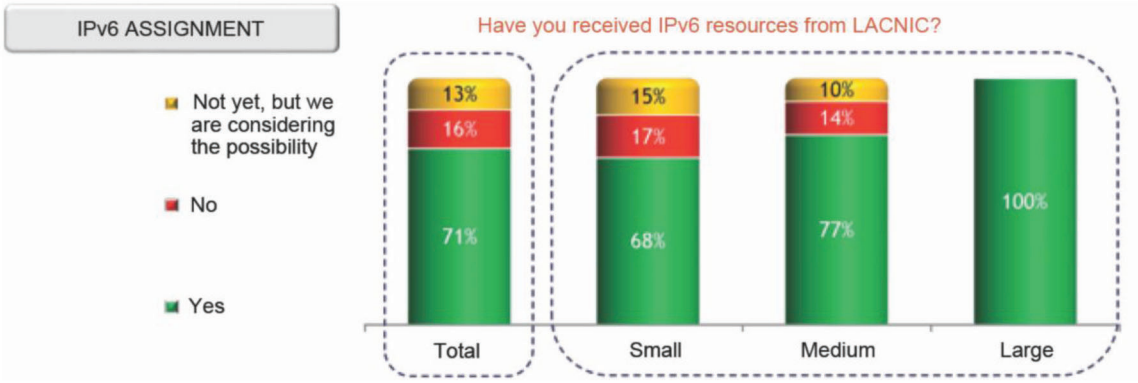
Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

For greater clarity in the interpretation of results, charts include results for all countries and consolidated results for the region. The total membership base ("Base") who answered the survey is shown on the bottom part of each bar of the chart, including how each question applied to a certain percentage of those who answered the survey ("Applicable"). By way of example, out of all those who replied, some are ISPs while others are not, etc. When the question refers to ISPs, "Applicable" specifies what percentage of respondents are ISPs.

8.2.1 IPv6 address assignment in the region

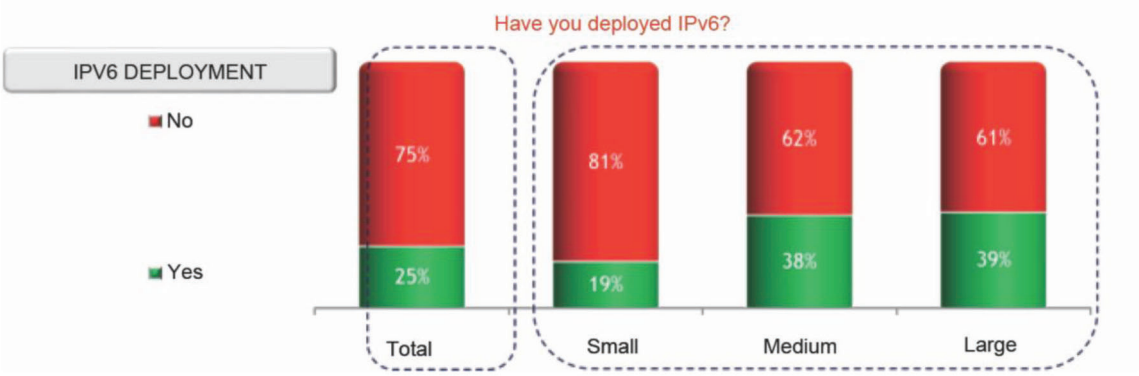
As seen in this report, some members have not yet received an IPv6 assignment, a topic which should be considered as a starting point for the transition.

In most countries, there are still non-major members with IPv6 block assignments. In terms of university institutions, the number of countries in this situation is around 30%. It is interesting to note that, based on the survey, out of those who do not have allocated IPv6 addresses, approximately half of them are already considering the request but have not done so.



8.2.2 IPv6 deployment in the region and in individual countries

It is observed that deployment levels in the region are quite low (less than 25% of small organizations), a fact that was verified during the meetings in the countries visited as part of this work. The following charts show the situation first by region and then country by country. Regarding the country-by-country situation, those who have started some kind of deployment still represent a low percentage of total members.

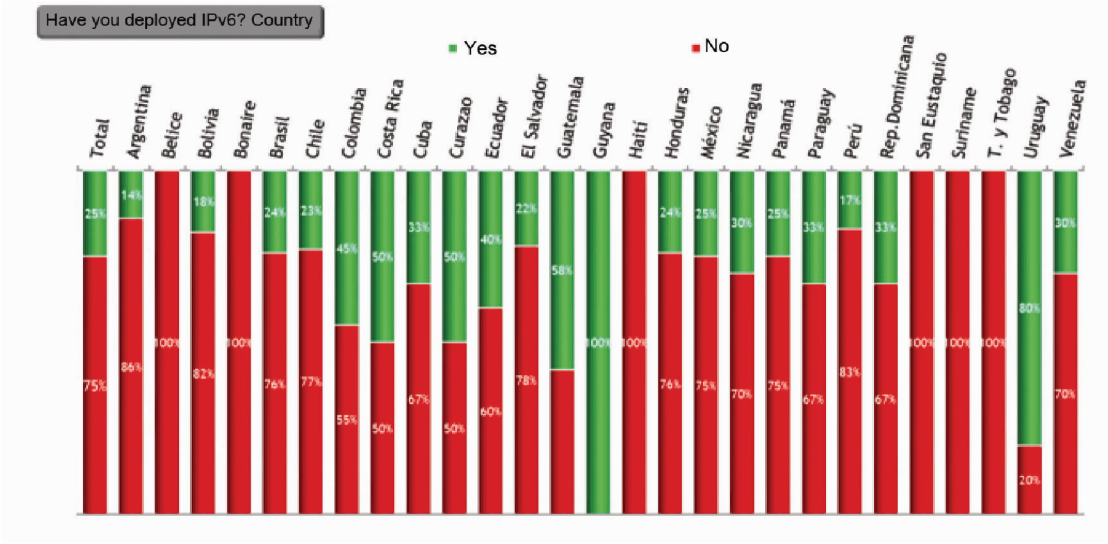


13- The source for the charts is MERCOPLUS Latin America, which was the company that performed the field work and processing of the survey.

8.2.3 ISPs deploying IPv6 to end clients

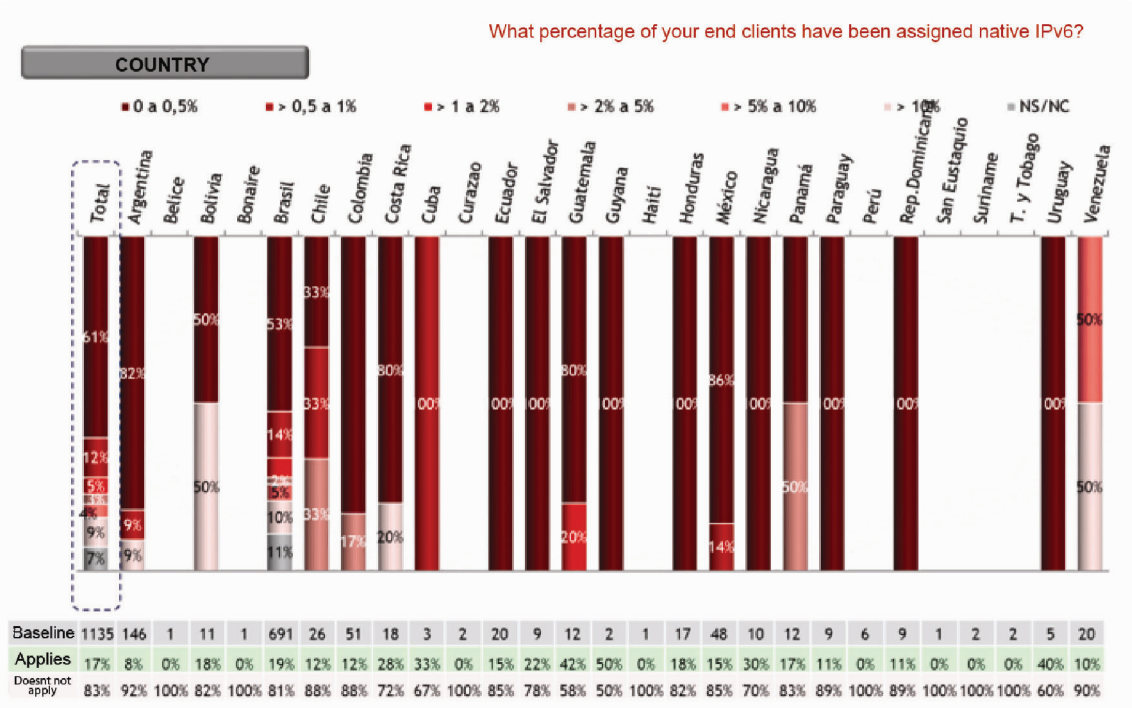
The following results show the percentage of ISPs which specified the percentage of customers to which IPv6 addresses had been assigned. It should be noted that "ISPs" includes operators of all sizes, even those that only provide corporate services, usually on a small scale.

In turn, those who have not deployed IPv6 to any customer are in the range of 0 to 0.5%, as well as those who have or have had customers on a trial basis, which includes most of them according to face-to-face meetings.



This chart is sensitive to who replied or not. In Ecuador, for example, at the time of the survey, CNT had deployed IPv6 to more than 10% of its customers, yet Ecuador appears with a very low percentage, possibly because CNT did not respond to this question[14].

With the observation that relevant operators may not have responded to the survey, results show great variability between countries in terms of the percentage of customers with native IPv6, and a regional percentage of 32% with more than 0.5% of customers. This percentage was calculated based on 190 replies.



14- It should be remembered that the survey was anonymous for the reasons mentioned

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

8.2.4 ISPs not deploying native IPv6. Reasons why IPv6 deployment has not been considered.

In this case, respondents had the option of specifying more than one reason. The most commonly mentioned reasons include; 1. Current infrastructure presents problems for transitioning to IPv6, and 2. Deployment and operational difficulties are expected. Both of these reasons will attenuate over time considering that ISPs may not have suitable networks at the moment, but practically all interviewed operators are making progress in upgrading their networks and systems. In turn, due to the actions that LACNIC is implementing and will continue to implement, any misgivings regarding future difficulties will be reduced or eliminated.

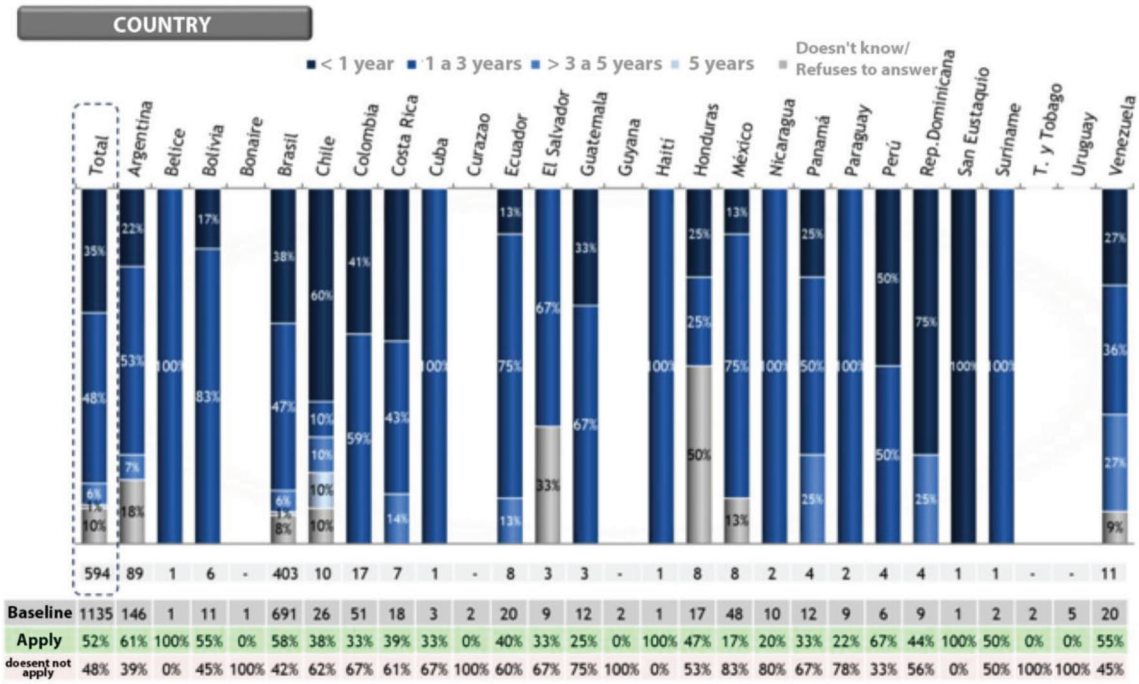
The use of CGNAT to the point where it is enough for their current customer base and projected growth was the reason least mentioned by the ISPs.

Why haven't you considered deploying IPv6?

PAÍS	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haiti	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rép.. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Current infrastructure presents problems for transitioning to IPv6	49%	46%	100%	50%	-	49%	50%	35%	86%	100%	-	50%	-	33%	-	100%	63%	75%	50%	25%	50%	25%	75%	-	-	-	-	45%
Deployment and operational difficulties are expected	45%	40%	100%	50%	-	49%	-	35%	43%	100%	-	13%	33%	67%	-	-	13%	25%	-	50%	-	50%	25%	100%	-	-	-	36%
We still have enough IPv4 addresses or can buy IPv4 addresses	22%	24%	-	67%	-	20%	40%	29%	-	-	-	25%	-	-	-	-	25%	25%	-	50%	50%	25%	50%	-	-	-	-	27%
Customer requirements do not justify the investment	18%	18%	-	-	-	18%	20%	6%	29%	-	-	13%	33%	-	-	-	63%	13%	-	50%	-	50%	50%	-	100%	-	-	9%
We have not yet considered deploying IPv6	9%	13%	-	17%	-	7%	10%	12%	-	-	-	25%	33%	-	-	-	25%	25%	50%	-	-	-	25%	-	100%	-	-	-
We are using CGNAT and this is enough for our current customer base and projected growth	5%	4%	-	17%	-	4%	20%	18%	-	-	-	13%	-	-	-	-	13%	-	-	-	100%	-	-	-	-	-	-	18%
Other reasons	22%	19%	-	17%	-	22%	20%	41%	14%	-	-	50%	-	33%	-	-	-	25%	50%	-	-	25%	-	-	-	-	-	45%
Baseline	594	89	1	6	-	403	10	17	7	1	-	8	3	3	-	1	8	8	2	4	2	4	4	1	1	-	-	11
Base	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
Aplica	52%	61%	100%	55%	0%	58%	38%	33%	39%	33%	0%	40%	33%	25%	0%	100%	47%	17%	20%	33%	22%	67%	44%	100%	50%	0%	0%	55%
No Aplica	48%	39%	0%	45%	100%	42%	62%	67%	61%	67%	100%	60%	67%	75%	100%	0%	53%	83%	80%	67%	78%	33%	56%	0%	50%	100%	100%	45%

8.2.5 ISPs not deploying native IPv6. Time frame in which they expect to begin deploying IPv6.

This information is relevant in order to know the trends of future IPv6 deployment. About one-third of the respondents consider beginning deployment in 2016, although the situation is different depending on the country.



	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haiti	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
	594	89	1	6	-	403	10	17	7	1	-	8	3	3	-	1	8	8	2	4	2	4	4	1	1	-	-	11
Baseline	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
Apply	52%	61%	100%	55%	0%	58%	38%	33%	39%	33%	0%	40%	33%	25%	0%	100%	47%	17%	20%	33%	22%	67%	44%	100%	50%	0%	0%	55%
doesent not apply	48%	39%	0%	45%	100%	42%	62%	67%	61%	67%	100%	60%	67%	75%	100%	0%	53%	83%	80%	67%	78%	33%	56%	0%	50%	100%	100%	45%

8.2.6 ISPs which have already started deploying IPv6. Techniques employed.

The survey confirms a conclusion reached after the interviews: virtually all the ISPs are considering using dual-stack as the transition technique. Cases of pure dual-stack were observed during the interviews, most of which were using or considering the use of dual-stack with CGNAT .

The survey shows that the majority of respondents opted for dual-stack.

Which technologies were used in the transition?

COUNTRY	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haiti	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Dual-Stack	88%	91%	-	100%	-	87%	100%	100%	100%	100%	-	100%	100%	80%	100%	-	100%	57%	67%	100%	100%	-	100%	-	-	-	50%	100%
NAT64	12%	-	-	-	-	12%	-	-	20%	-	-	-	-	80%	-	-	-	29%	-	-	-	-	-	-	-	-	-	-
6PVE	3%	9%	-	-	-	1%	-	-	20%	-	-	-	-	20%	-	-	-	-	-	-	-	-	-	-	-	-	50%	-
464XLAT	2%	-	-	-	-	1%	-	-	-	-	-	-	-	20%	-	-	-	14%	-	-	-	-	-	-	-	-	-	-
DS-Lite	1%	-	-	-	-	-	-	17%	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Other technologies	7%	-	-	-	-	6%	-	-	20%	-	-	-	-	-	-	-	-	43%	33%	-	-	-	-	-	-	-	-	-
Base	193	11	-	2	-	133	3	6	5	1	-	3	2	5	1	-	3	7	3	2	1	-	1	-	-	-	2	2

	Apply	Baseline	doesent not apply
Total	1135	17%	83%
Argentina	146	8%	92%
Belice	1	0%	100%
Bolivia	11	18%	82%
Bonaire	1	0%	100%
Brasil	691	19%	81%
Chile	26	12%	88%
Colombia	51	12%	88%
Costa Rica	18	28%	72%
Cuba	3	33%	67%
Curazao	2	0%	100%
Ecuador	20	15%	85%
El Salvador	9	22%	78%
Guatemala	12	42%	58%
Guyana	2	50%	50%
Haiti	1	0%	100%
Honduras	17	18%	82%
México	48	15%	85%
Nicaragua	10	30%	70%
Panamá	12	17%	83%
Paraguay	9	11%	89%
Perú	6	0%	100%
Rep. Dominicana	9	11%	89%
San Eustaquio	1	0%	100%
Suriname	2	0%	100%
T. y Tobago	2	0%	100%
Uruguay	5	40%	60%
Venezuela	20	10%	90%

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

8.2.7 ISPs which have already started deploying IPv6. Reasons for starting IPv6 deployment.

The most common reasons for IPv6 deployment include the following:

1. Declining availability and rising cost of IPv4 addresses

2. Corporate image

3. Migrating to IPv6 without further IPv4 growth is the most cost-effective solution

4. Significant customer base growth

5. Business opportunity

All these reasons are in the range of 32% to 45% of the responses of the ISPs that answered the survey.

Given that ISPs purchases of IPv4 addresses in the region have not been noticed, it is understood that the answers regarding the first reason are mainly due to decreasing availability.

As for the Business opportunity, it was observed during meetings that in many cases deployment began as a result of corporate clients requirements, particularly universities.

What are your reasons for deploying IPv6?

PAÍS	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haiti	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep., Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Declining availability and rising cost of IPv4 addresses	45%	55%	-	50%	-	47%	33%	50%	20%	-	-	-	100%	40%	100%	-	-	29%	-	100%	-	-	100%	-	-	-	-	50%
Corporate image	45%	36%	-	100%	-	43%	100%	50%	80%	-	-	67%	-	-	100%	-	67%	43%	-	100%	100%	-	-	-	-	-	100%	-
Migrating to IPv6 without further IPv4 growth is the most cost-effective solution	37%	18%	-	-	-	46%	-	-	20%	-	-	33%	50%	20%	-	-	-	29%	-	50%	-	-	-	-	-	-	-	50%
Significant customer base growth	32%	27%	-	50%	-	32%	-	33%	40%	-	-	33%	-	80%	-	-	-	29%	67%	-	-	-	-	-	-	-	-	50%
Business opportunity	32%	18%	-	-	-	30%	67%	83%	40%	-	-	33%	-	40%	-	-	-	43%	33%	50%	100%	-	100%	-	-	-	50%	-
Customer requests	24%	45%	-	50%	-	17%	67%	50%	40%	-	-	33%	-	20%	-	-	100%	43%	33%	50%	-	-	-	-	-	-	-	100%
Negative experience with NAT444, 6to4 and other non-native IPv6 technologies	5%	9%	-	-	-	5%	33%	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Other	6%	-	-	-	-	5%	-	17%	20%	100%	-	-	-	-	-	-	-	-	-	50%	-	-	-	-	-	-	50%	-
Baseline	193	11	-	2	-	133	3	6	5	1	-	3	2	5	1	-	3	7	3	2	1	-	1	-	-	-	2	2

Baseline	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
Apply	17%	8%	0%	18%	0%	19%	12%	12%	28%	33%	0%	15%	22%	42%	50%	0%	18%	15%	30%	17%	11%	0%	11%	0%	0%	0%	40%	10%
Not Apply	83%	92%	100%	82%	100%	81%	88%	88%	72%	67%	100%	85%	78%	58%	50%	100%	82%	85%	70%	83%	89%	100%	89%	100%	100%	100%	60%	90%

8.2.8 ISPs which have already started deploying IPv6. Main difficulties encountered.

The main difficulties encountered in IPv6 deployment, which generally exceed 50% of the responses, are as follows:

1. Network equipment not fully compatible with IPv6

2. End-user devices not fully compatible with IPv6

3. Staff learning curve
4. Applications that don't support IPv6 addressing

5. Lack of vendor support

Main difficulties encountered in IPv6 deployment

COUNTRY	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haití	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep.. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Network equipment not fully compatible with IPv6	66%	46%	-	50%	-	74%	67%	67%	60%	100%	-	33%	50%	20%	100%	-	-	43%	33%	50%	-	-	100%	-	-	-	100%	100%
Terminal devices not fully compatible with IPv6	65%	36%	-	50%	-	71%	67%	67%	80%	-	-	67%	50%	60%	-	-	-	43%	100%	50%	100%	-	-	-	-	-	100%	50%
Staff learning curve	63%	73%	-	-	-	64%	33%	67%	60%	-	-	100%	100%	40%	-	-	100%	0%	67%	100%	100%	-	100%	-	-	-	100%	100%
Applications that don't support IPv6 addressing	52%	36%	-	50%	-	59%	67%	-	60%	-	-	67%	50%	40%	-	-	-	57%	33%	50%	-	-	-	-	-	-	-	50%
Lack of vendor support	44%	55%	-	50%	-	48%	33%	17%	20%	100%	-	33%	50%	20%	100%	-	33%	14%	-	100%	-	-	100%	-	-	-	50%	-
Costs higher than anticipated	22%	9%	-	-	-	26%	67%	33%	-	-	-	33%	50%	-	-	-	-	-	-	50%	-	-	-	-	-	-	-	-
Difficulties with the BSS/OSS systems	20%	27%	-	-	-	23%	-	17%	20%	-	-	-	50%	-	-	-	-	14%	-	50%	-	-	-	-	-	-	-	-
Other	14%	-	-	-	-	12%	-	33%	20%	-	-	-	-	40%	100%	-	-	29%	33%	-	-	-	100%	-	-	-	-	50%
Baseline	193	11	-	2	-	133	3	6	5	1	-	3	2	5	1	-	3	7	3	2	1	-	1	-	-	-	2	2

Baseline	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
Apply	17%	8%	0%	18%	0%	19%	12%	12%	28%	33%	0%	15%	22%	42%	50%	0%	18%	15%	30%	17%	11%	0%	11%	0%	0%	0%	40%	10%
Not apply	83%	92%	100%	82%	100%	81%	88%	88%	72%	67%	100%	85%	78%	58%	50%	100%	82%	85%	70%	83%	89%	100%	89%	100%	100%	100%	60%	90%

8.2.9 ISPs which have already started deploying IPv6. Results of IPv6 operation.

Fifty-eight percent of survey respondents replied that deployment had improved their business results.

8.2.10 Non-ISPs which have not started deploying IPv6. Reasons.

In the case of non-ISPs, while the situation is different in different countries, roughly a third of regional respondents specified the following reasons:

1. They fear deployment and operational difficulties

2. They have not yet considered deploying IPv6

3. Current infrastructure creates problems for transitioning to IPv6

These organizations do not have overall rapid growth in the number of users, therefore, the difficulties mentioned above are reason enough to postpone deployment and wait.

Why haven't you considered deploying IPv6?

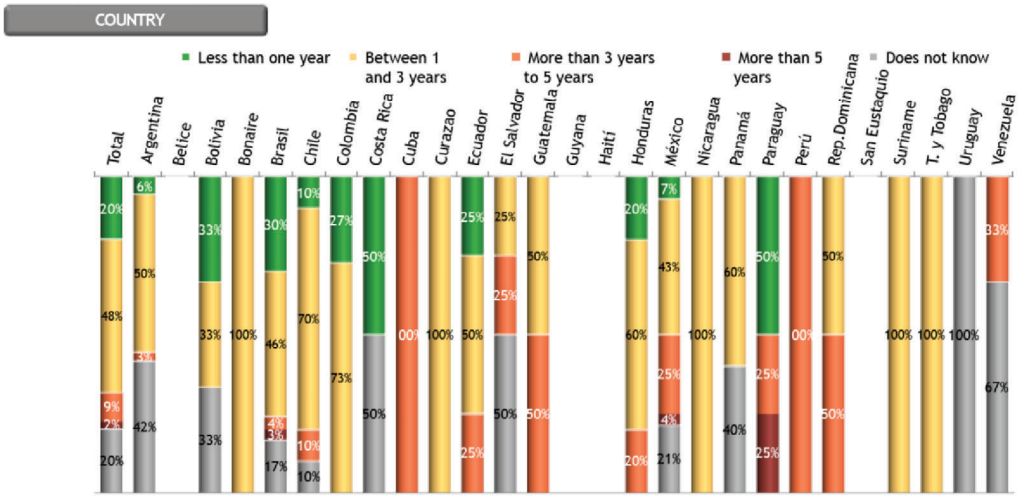
COUNTRY	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haití	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep.. Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Deployment and operational difficulties are expected	35%	31%	-	33%	-	39%	10%	27%	100%	-	-	75%	50%	100%	-	-	60%	21%	40%	60%	-	-	-	-	-	-	-	67%
We have not yet considered deploying IPv6	34%	36%	-	-	-	31%	40%	27%	-	-	-	25%	50%	-	-	-	40%	50%	20%	60%	50%	-	50%	-	100%	-	100%	33%
Current infrastructure presents problems for transitioning to IPv6	29%	19%	-	33%	100%	35%	10%	27%	-	100%	-	50%	25%	50%	-	-	20%	21%	40%	20%	25%	-	-	-	-	50%	-	-
The organization's needs don't justify the investment	17%	14%	-	-	-	18%	30%	27%	-	-	-	25%	25%	-	-	-	-	25%	-	-	25%	-	-	-	-	-	-	-
The ISP doesn't support IPv6	16%	17%	-	100%	-	11%	40%	9%	-	100%	-	-	-	50%	-	-	20%	4%	20%	40%	25%	100%	50%	-	-	-	-	67%
Other	20%	28%	-	-	-	16%	30%	55%	50%	-	100%	-	50%	-	-	-	40%	11%	20%	-	25%	-	-	-	-	50%	-	-
Baseline	252	36	-	3	1	120	10	11	2	1	1	4	4	2	-	-	5	28	5	5	4	1	2	-	1	2	1	3

Baseline	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
Apply	22%	25%	0%	27%	100%	17%	38%	22%	11%	33%	50%	20%	44%	17%	0%	0%	29%	58%	50%	42%	44%	17%	22%	0%	50%	100%	20%	15%
Not Apply	78%	75%	100%	73%	0%	83%	62%	78%	89%	67%	50%	80%	56%	83%	100%	100%	71%	42%	50%	58%	56%	83%	78%	100%	50%	0%	80%	85%

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

8.2.11 Non-ISPs which have not started deploying IPv6. Time frame in which they expect to begin deployment.

Approximately 20% of non-ISPs expect to begin IPv6 deployment in 2016. The vast majority replied they expect to begin deployment in 1 to 3 years.



	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haití	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep.Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
Baseline	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
Apply	22%	25%	0%	27%	100%	17%	38%	22%	11%	33%	50%	20%	44%	17%	0%	0%	29%	58%	50%	42%	44%	17%	22%	0%	50%	100%	20%	15%
Not apply	78%	75%	100%	73%	0%	83%	62%	78%	89%	67%	50%	80%	56%	83%	100%	100%	71%	42%	50%	58%	56%	83%	78%	100%	50%	0%	80%	85%

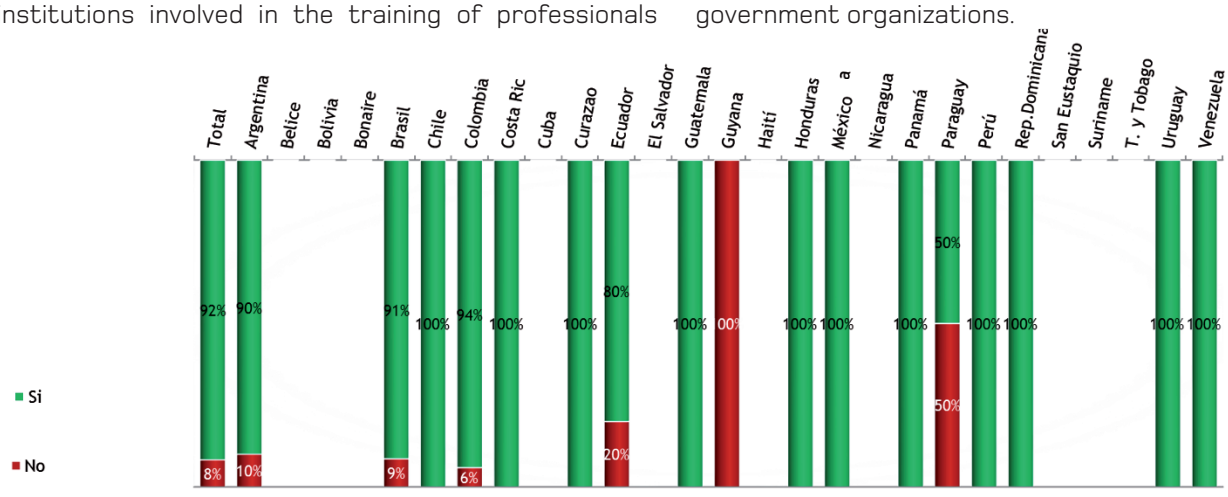
8.2.12 Non-ISP already deploying IPv6. Reasons for IPv6 deployment.

The reason most frequently mentioned by these LACNIC members when asked why they had begun deploying IPv6 was to promote its development. The region's research and education organizations are the main promoters of the new protocol: 93% of respondents in this category mentioned this as their main motivation.

This reason has been expressed by almost all those academic organizations interviewed, meaning that as institutions involved in the training of professionals for the country, they cannot teach IPv6 if they are not deploying it.

8.2.13 Non-ISP already deploying IPv6. Results for the organization.

Almost all the organizations which completed the survey replied they had benefited from IPv6 deployment (92% at regional level). One possible reason for this is that these organizations generally have technical support mainly through university networks, or through specialized departments in the case of large government organizations.



	Total	Argentina	Belice	Bolivia	Bonaire	Brasil	Chile	Colombia	Costa Rica	Cuba	Curazao	Ecuador	El Salvador	Guatemala	Guyana	Haití	Honduras	México	Nicaragua	Panamá	Paraguay	Perú	Rep.Dominicana	San Eustaquio	Suriname	T. y Tobago	Uruguay	Venezuela
	96	10	-	-	-	35	3	17	4	-	1	5	-	2	1	-	1	5	-	1	2	1	2	-	-	-	2	4
Base	1135	146	1	11	1	691	26	51	18	3	2	20	9	12	2	1	17	48	10	12	9	6	9	1	2	2	5	20
APLICA	8%	7%	0%	0%	0%	5%	12%	33%	22%	0%	50%	25%	0%	17%	50%	0%	6%	10%	0%	8%	22%	17%	22%	0%	0%	0%	40%	20%
NO APLICA	92%	93%	100%	100%	100%	95%	88%	67%	78%	100%	50%	75%	100%	83%	50%	100%	94%	90%	100%	92%	78%	83%	78%	100%	100%	100%	60%	80%

8.2.14 Conclusions

1. In most countries, some non-major members have still not received IPv6 block allocations. If one considers university institutions, the number of countries in this situation is around 30%. Approximately half of these are already considering requesting an IPv6 block, but have not done so yet.

2. It is observed that IPv6 deployment level is still quite low (less than 25% of organizations), a fact which was verified during the meetings in the countries visited as part of this work.

3. With the observation that relevant operators may not have responded to the survey, results show great variability between countries in terms of the percentage of customers with native IPv6, and a regional percentage of 32% with more than 0.5% of customers.

4. Among the ISPs that have not deployed IPv6, the main reasons given are: 1. Current infrastructure presents problems for transitioning to IPv6, and 2. Deployment and operational difficulties are expected. The use of CGNAT to the point where it is enough for their current customer base and projected growth was the reason least mentioned by the ISPs.

5. Both of these reasons will attenuate over time considering that ISPs may not have suitable networks at the moment, but practically all interviewed operators are making progress in upgrading their networks and systems. In turn, due to the actions that LACNIC is implementing and will continue to implement, any misgivings regarding future difficulties will be reduced or eliminated.

6. About one-third of respondents are considering starting deployment in 2016, although the situation is different depending on the country.

7. Virtually all surveyed ISPs which had started IPv6 deployment have opted for dual-stack with CGNAT.

8. The most common reasons for IPv6 deployment include the following: Declining availability and rising cost of IPv4 addresses; Corporate image; Migrating to IPv6 without further IPv4 growth is the best economic solution; Significant customer base growth; and Business opportunity.

9. The main difficulties encountered in IPv6 deployment, which generally exceed 50% of the responses, are as follows: Network equipment not fully compatible with IPv6, Terminal devices not fully compatible with IPv6, Learning curve of staff, Applications that do not support IPv6 addressing and Lack of support from vendors.

10. A significant percentage of survey respondents (58% at regional level) replied that deployment had benefited their business results.

11. As for non-ISPs which have not started deploying IPv6, the main reason mentioned for their lack of deployment include the fact that deployment and operational difficulties are expected, existing infrastructure, and the fact that deployment has not yet been considered.

12. Approximately 20% if non-ISPs expect to begin IPv6 deployment in 2016. The vast majority replied that they expect to begin deployment in 1 to 3 years. This extended timeframe would be mainly due to reasons they consider for not starting deployment at this time.

13. The reason most frequently mentioned by non-ISPs who have started to deploy IPv6 was to promote its development. The region's research and education organizations are the main promoters of the new protocol: 93% of respondents in this category mentioned this as their main motivation.

14. Almost all non-ISP organizations which completed the survey replied that they had benefited from IPv6 deployment (92% at regional level).

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

9. CURRENT STATUS OF IPV6 DEPLOYMENT IN THE LACNIC REGION. FIELD WORK.

This section contains a summary of the diagnosis obtained through the meetings conducted as part of the field work. The opinions and information made available to the community in this document are the result of the interviews that were conducted and the selfless and valuable collaboration of multiple stakeholders with whom we worked in the different countries. Their publication does not necessarily mean that LACNIC validates these views and information. Detailed information can be found in Annex I, Field Work.

1. Growth of massive IPv6 deployment in the four countries where more than 1% of users are IPv6-ready is accounted for by very few operators. In Bolivia, Ecuador and Peru the result is due to one operator in each country and in Brazil it is due to more than one operator.

2. Members were interviewed who have still not been allocated IPv6 addresses. Some of them are unaware of the procedures or the need to move forward through this first step. The above was observed mainly in universities or government institutions using their providers' blocks.

3. Regardless of whether there are countries with stocks of IPv4 addresses that do not require IPv6 transition, it is believed that the Internet of Things will eventually produce a significant increase in demand for addresses which will drive mass IPv6 deployment.

4. Government authorities

a. Most government authorities responsible for public procurement and/or ICT have not approved guidelines in relation to IPv6-compatible public procurement in terms of hardware, software and access. Neither have they approved any others related to security systems to accompany these guidelines.

b. Given the importance of these government actions, the issuance of these instructions is considered good practice.

c. Additionally, e-government is seen as an incentive for IPv6 deployment from the point of view of the Contents indicator.

d. One regulator has stated its policy for creating a sense of urgency, developing training and awareness-building actions, working jointly with all stakeholders, and promoting IPv6 deployment within government institutions. This initiative is worth highlighting.

5. University networks

a. In countries in which university networks are involved, including hardware and software compatibility in purchases and access with IPv6, the need is generated in the ISPs to begin deployment in at least the core and the access of the institutions.

b. There is sufficient evidence in the region regarding this role of university networks. Additionally, when universities deploy IPv6 internally, the % of Users is boosted at country level.

6. ISPs providing residential access services

a. Uneven progress has been observed in the region, mainly due to the different times at which the transition to IPv6 was initiated.

b. The transition process involves multiple actions that depend on network characteristics, systems and other aspects of each operator.

c. The main actions are intended to act upon the following areas: core, distribution networks, access networks, business support systems (BSS) and operations support systems (OSS), business intelligence, after sales service, legally required records, and training.

d. Overall, the same weight is given to emerging difficulties of the networks themselves up to access points as that given to difficulties in upgrading the other internal areas.

e. It is common to observe that unexpected difficulties arise which delay progress towards IPv6, mainly due to the variability in the characteristics of each area of every company as compared with others. For example, CPE problems of one company are not similar to those of others, and a solution in one case is not applicable to the others. These problems are more common in everything related to internal areas (e.g., "provisioning").

f. At least one case has been noted where an ISP has deployed a high percentage of dual-stack CPEs but was unable to make the progress needed in other areas to provide large-scale IPv6 service.

g. Some dissemination of knowledge to address these difficulties has begun at different levels which will ease the transition as time passes.

h. ISPs which began planning for the transition early, starting with a situational analysis of different areas including hardware, software, processes and procedures have benefited from a progressive transition process requiring only marginal additional investment as their assets naturally reached obsolescence and had to be replaced. Replacing obsolete equipment with other IPv6-compatible equipment has not meant additional investment, particularly in the case of their core networks.

i. In conclusion, something that stands out is the importance of an early start to the transition through a program which aligns the investments and actions needed to the IPv4 shortage predictions in the best way possible.

j. Almost all operators are providing or considering providing services using dual-stack, usually in combination with CGNAT.

k. Fixed network operators will make slower progress, as they will replace CPEs with dual-stack CPEs as replacement becomes necessary due to obsolescence, taking into account the high impact of this investment on the total investment required for the transition.

l. Mobile network operators will evolve at a faster pace, as terminals are paid for by users who often change them over short periods of time. Likewise, their own expansion makes it necessary for them to purchase more IPv6-ready equipment.

m. In general, there is a shortage of IPv4 addresses that has led to the use of CGNAT and promoted IPv6 deployment. However, very few operators in the region have made significant deployments on a massive scale. Most operators mentioned 2016 as the year in which they will begin large-scale deployment, while many others mentioned later dates due to their stock of IPv4 addresses.

n. Where problems are encountered with certain applications behind CGNAT, ISPs with sufficient addresses provide the service using a public IP, while maintaining CGNAT for the remaining customers.

o. Given the need to use CGNAT until the final transition to IPv6, the legal requirements for logging user's physical address (IP address + port) may become a major economic burden for the ISPs.

7. ISP offering corporate services

a. It is much easier for these ISPs to provide IPv6 services than it is for large-scale residential service operators.

b. They generally have no shortage of IPv4 addresses and their customers do not request IPv6 services. Moreover, it has been mentioned that in some cases customers do not want to switch to IPv6.

8. Wholesale ISPs. In general, most wholesale ISPs are prepared to provide services over IPv6 (including peering); these services, however, are not always provided as their customers have no need for them.

9. IXPs. Generally speaking, IXPs are IPv6-ready but have not received any requests for IPv6 interconnection, and will possibly not receive any until 2016, when deployments are set to begin at user level.

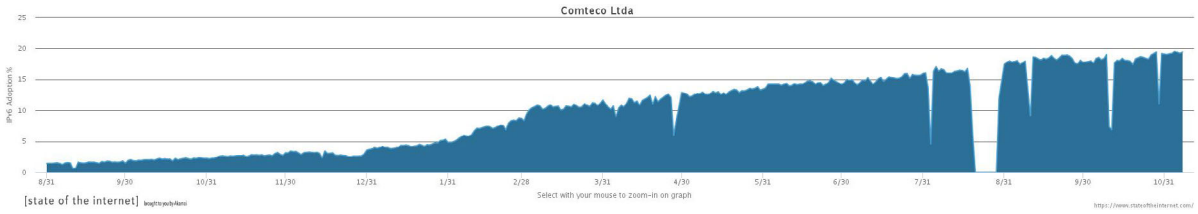
Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

10. ANALYSIS OF SUCCESS STORIES IN THE LACNIC REGION

10.1 Major large-scale deployments in the region

Only four countries in the region have achieved User indicator values higher than 1%. In three of these countries, IPv6 deployment was driven by one operator. These are the following:

1. Bolivia. COMTECO promoted mass deployment to end users. As of November 19, an IPv6 user percentage of 19.4% was observed according to the Akamai methodology. Progressive growth can be observed in the same over the past year and a half.



2. Brazil. In this case, several ISPs are driving a strong and speedy increase in the percentage of IPv6 users, which, according to Google and APNIC, on average, increased 2.5 times between 13 July 13 and 17 November, thus reaching 7.58%. The following chart shows how it grew from practically 0% in early 2015 to its current value according to Akamai.

Brazilian operators

a. Operators promoting this growth include Oi, GVT and Vivo. These values were recorded on 12 November.

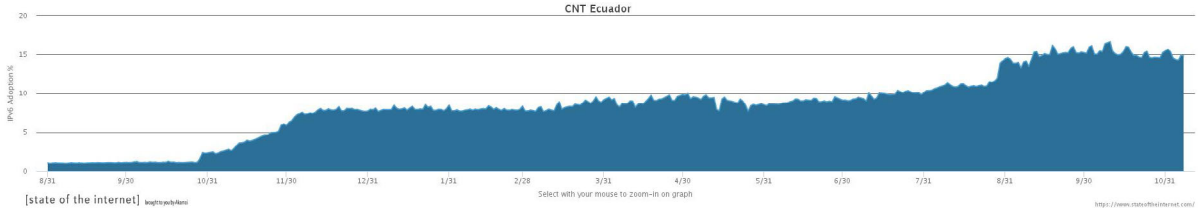
b. Oi - Telemar with 1.3% according to Akamai starting in late May 2015.

c. Oi - Brasil Telecom with 0.9% according Akamai, starting on the same date.

d. GVT, which went from 3.5% to 14.76% in 6 months according to World IPv6 Launch[15].

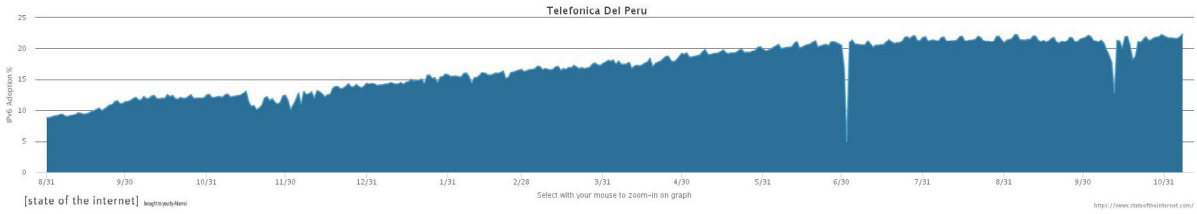
e. Vivo, which went from 1.9% to 3.04% in 30 days according to World IPv6 Launch.

3. Ecuador. In this case, CNT promoted IPv6 deployment, which went from 1% to 14.8% in one year, according to Akamai.



15- http://www.worldipv6launch.org/measurements/

4. Peru. Telefonica of Peru is the operator responsible for the high IPv6 deployment rates thanks to a gradual process which, according to Akamai, allowed the company to reach 22.3% on 17 November.



Success stories presented in detail in this section pertain to countries which are part of the sample that we visited and interviewed.

The Brazilian case emerged recently as an example of rapid deployment.

In the investigation of the success stories in the sample countries, two types were considered: an example of an operator that has made significant preparation over a period of several years and is ready for mass deployment, and those who have already started deployment successfully. The difference between the two cases is mainly a matter of timeliness, given that up to now, IPv6 deployment is motivated primarily due to the shortage of IPv4 addresses and there may be operators who have already taken all the steps for transition but do not yet require mass deployment to end users.

That is, they have early foreseen the need to start the transition, they have gradually made the same while minimizing investments to the extent the replacement of equipment was necessary, adapting their systems to the new protocol, but have not taken the final step of granting end-user access due to economic - financial reasons. This last part requires the greatest investment; therefore, deployment timing is postponed until it is really necessary.

The success stories analyzed during this research are as follows.

10.2 Major operator. Successful preparation for the transition.

While it may not strictly be classified as a success story due to the actual results in terms of the LACNIC/CAF ICAv6 indicator, a large multinational ISP which provides residential, wholesale, mobile and corporate services has a well-defined plan and is well-advanced in terms of IPv6 deployment. It is interesting to note the work which has been carried out and the direction in which they've taken their project.

At international level, approximately five years ago the ISP adopted the strategy of migrating all operations to IPv6. At the time, dual-stack and DS-Lite techniques were being established and the ISP adopted the first of these options. The main reasons for this were, first, to address the shortage of IPv4 addresses and high broadband growth rates; second, corporate strategy. This plan began with a detailed inventory of all network equipment: their ability to be upgraded to IPv6, whether they were IPv6-ready, etc. Overall, aggregators had the greatest replacement needs.

In one of the countries visited for this report, this operation began about two years ago with proofs of concept, pilot projects, equipment and system upgrades, etc. in all their business units, particularly their fixed and mobile retailers. Due to the difficulties inherent to mobile networks, pilot tests conducted on fixed networks were the first to be completed. This operator's transport network has been operating on IPv6 for years using 6VPE. Provisioning and other systems are also IPv6-ready, as are the operator's aggregators and xDSL CPEs.

Corporate customers have no pressing current or future need for IPv6 services, so this service has no commercial value. In any case, they are provided with IPv6 over MPLS using 6VPE with CPEs and routers in dual-stack mode. This observation is important because it is valid regardless of the country and the provider.

As for wholesale customers, this operator has been providing services over IIPv6 (including peering) for some time. The main reason for this is that, as soon as they have or plan to provide end users with IPv6, wholesale customers require IPv6 peering or transit services.

With regard to fixed and mobile retail customers, IPv6 has no commercial value; therefore, in this case the deployment will be carried out according to the needs or development strategy assumed by the operator.

15- http://www.worldipv6launch.org/measurements/

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

All operations have adopted dual-stack with native IPv6 access and dynamic CGNAT44 to continue supporting the services that still require IPv4. It's an interesting strategy that minimizes future disposable investments, thus lowering IPv4 address demand for all services which may be provided over IPv6. CGNAT deployments are initially centralized, but the evolution of high-speed services such as video streaming drives the network to a decentralized model and brings NAT closer to the edges where aggregation occurs.

The consultant notes that this strategy leads to higher network O&M costs due to the need to maintain dual-stack, while the operator noted that economic studies favored this solution.

High speed deployments are based mainly on FTTC and VDSL.

The strategy does not involve the complete replacement of client terminals with dual-stack, as this has not been required by customers who don't care about technology as long as they receive a quality service. Terminals will be replaced gradually as they reach obsolescence or when necessary to provide the service. The consultant notes that the cost of the terminals is an important percentage of the investment in IPv6 deployment in the access, as seen in the cost analysis of the model. Moreover, the acceleration of customer mobile replacement rates means that IPv6 deployment with significant impact on the mobile ISP can be expected.

10.3 Success story: Cooperativa de Telecomunicaciones Cochabamba Ltda. (COMTECO)

Cooperativa de Telecomunicaciones de Cochabamba is the operator which has so far driven IPv6 deployment in Bolivia and accounts for Bolivia's relatively high indicator in terms of potential IPv6 users. It provides cable television services, mobile telephony services through NUEVATEL - VIVA, long distance, broadband, satellite Internet, satellite television and other services.

In late 2010, COMTECO made the decision to deploy IPv6 on its network; in 2012, it requested an IPv6 prefix from LACNIC; in 2013, it activated a BGP link using IPv6 with its transit provider and published the prefix 2803:9400::/32. Early tests showed that while edge routers, the DNS, certain modems and other equipment operated on IPv6, this was not the case with AAA.

In parallel, in early 2013 a call for tender was made in order to change the platform's core and this call for tender included IPv6 compatibility. The first tests were conducted in March 2014; customer deployment began on 22 August 2014 using dual-stack.
The operator believes they will not need CGNAT until 2017. Thus, this is the only successful case study we observed where an early IPv6 planning and deployment decision was made without yet needing to use CGNAT. In other words, it has taken advantage of the replacement of equipment or the installation of new equipment to anticipate future needs, the foregoing, knowing that this operator would only begin having a shortage of IPv4 addresses in 2017.

By December 2014, 4,000 users were accessing the Internet via IPv6 during peak hours, totaling 300 Mbps of IPv6 traffic.
In October 2015 these values increased to more than 17,000 users and a total traffic of 2 Gbps.
By then, 40% of their customers were IPv6-ready.
COMTECO believes that users have not noticed whether they are using IPv4 or IPv6, but greater latency has occasionally been noted for IPv6 websites.

Currently, as its IPv6 user base grows, COMTECO continues to implement these IPv6 transition tasks: configuring server farm components, DNS, firewalls, anti-spam software and authentication portals.

These actions stem from an early awareness of the need to migrate to IPv6 as well as from the need to replace equipment, which was already purchased considering IPv6 compatibility, particularly CPEs.

They found no problems or need for changes in their BSS, partly because it uses a flat rate model.

10.4 Success story: Corporación Nacional de Telecomunicaciones E.P. (CNT)

CNT adopted the early strategic decision to deploy IPv6 driven by two agreements by the Ministry of Telecommunications and Information Society in 2011 and 2012[16] for the development of IPv6 networks in Ecuador, and the anticipated shortage of IPv4 addresses.

CNT also began to experience the significant growth of its fixed Internet access customer base, which placed greater pressure on its stock of IPv4 addresses. As of 30 June 2015, CNT had 814,143 accounts for dedicated Internet access[17] and 57.47% of the market. This growth occurred several times in a few years, which, added to the shortage of IPv4 addresses, contributed to reaching a faster decision for IPv6 deployment on the fixed network.

16- 0133-2011 y 007-2012
17- http://www.arcotel.gob.ec/servicio-acceso-internet/

Deployment in the fixed network involves the use of the dual-stack technique and CGNAT, in line with the decision of practically all operators in the region. At the moment the effort is concentrated on the fixed network, leaving for later the decision regarding the mobile network currently operating in CGNAT. One of the potential problems that require attention in this mobile network concerns terminals.

As for corporate customers, we were told that they do not want to move to IPv6.

Deployment in the fixed network had an early start in 2011-2012. Highlights of this deployment include the early use of wireless dual-stack CPEs (which started in 2012). Thanks to high replacement rates, for reasons unrelated to the CPEs themselves, today there are more dual-stack CPEs than potential IPv6-enabled users. This means there has been great progress in access terminals, which will also lead to a significant increase in the number of users as soon as minor deployments are completed in the access network, such as some BRAS. Furthermore, the entire core is dual-stack and causes no issues in terms of systems and other backoffice equipment.

In short, this network is fully prepared for IPv6 with significant progress in the deployment of dual-stack CPEs; therefore, significant progress is expected in the near future with regard to the number of IPv6 accounts. The consultant notes that most of the operators find that CPE deployment costs are one of the obstacles for the rapid increase in the number of fixed IPv6 users. That is why, in general, they decide to move to IPv6 in the equipment replacement stages. In this case, an early replacement for CPE IPv6 compatible equipment occurred.

Customers have not found any perceptible differences. Deployment was performed carefully through two consecutive pilot plans. Problems were solved as they arose and today IPv6 deployment poses no problem at all.

Pilot tests were conducted with services with dual-stack in operation. In cases where some problems with the CPEs occurred, one of the alternatives was disconnected and a problem was detected which was solved through a software upgrade.

At this time, CNT is working on improving network management systems in order to increase operational efficiency.

In conclusion, early actions such as taking advantage of the natural replacement cycle to deploy new IPv6-compatible equipment results in a smooth transition without major problems and prepares the network for its evolution accompanying IPv6 content and applications progress, thus gradually reducing the use of IPv4.

10.5 Success story: Telefonica del Peru S.A.

This operator has the region's highest deployment indicators.

Considering the high growth rates and in an attempt to deal with the future exhaustion of IPv4 addresses led mainly by mobile and fixed ADSL services (Speedy) which are experiencing significant natural growth particularly in terms of HFC, starting in 2008 the operator developed a strategy for intensive IPv6 deployment along with a series of awareness-building initiatives which include sessions for companies and institutions considered important for the development and transmission of knowledge, etc. Thus, early awareness of IPv4 exhaustion was the main reason behind the IPv6 transition project. This strategy allowed freeing IPv4 addresses used in ADSL services, which were then used for a smoother transition in other areas.

As part of this plan, testing began in 2010.

Due to this deployment, the operation in Peru became the leading IPv6 deployment in the various Telefonica operations in the region. The main stages are described below according to the presentation made by the company during the LACNIC 24 LACNOG event held in the city of Bogota in 2015.

In 2009, there were alarms regarding IPv4 address exhaustion, thus the need to start using IPv6 by 2012 was duly noted. By that time, other operators such as NTT, Orange and COMCAST had already begun deployment.

At that time Telefonica had about 1.2 million IPv4 addresses and 1.1 million regular customers. At the same time, mobile customers were already using mobile services through CGNAT. Thus, they found it necessary to switch to using dual-stack with CGNAT.

Their strategy can be summarized as follows:

1. Use dual-stack with CGNAT for all future network growth

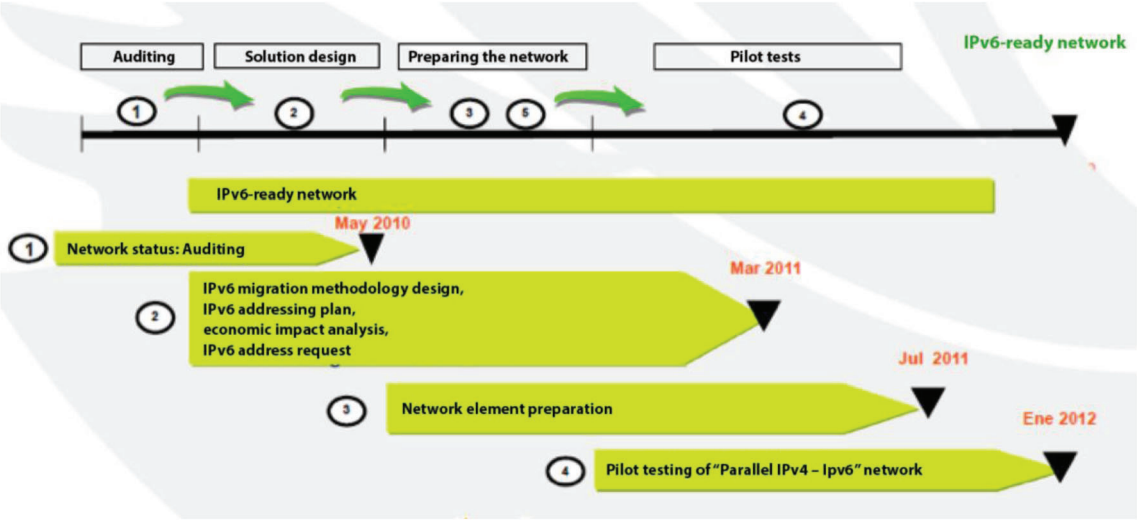
17- http://www.arcotel.gob.ec/servicio-acceso-internet/

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

2. Maintain high-value customers with public IPv4 addresses

3. Offer IPv6 services to any content provider requesting such services

A transition plan was developed which is shown in the image below.



Three main actions were identified:

1. Making sure CPEs will progressively support dual-stack

2. Providing dual-stack capability at the network's edge (BRAS and GGSN) and in the DNS

3. Making sure that OSS systems support dual-stack

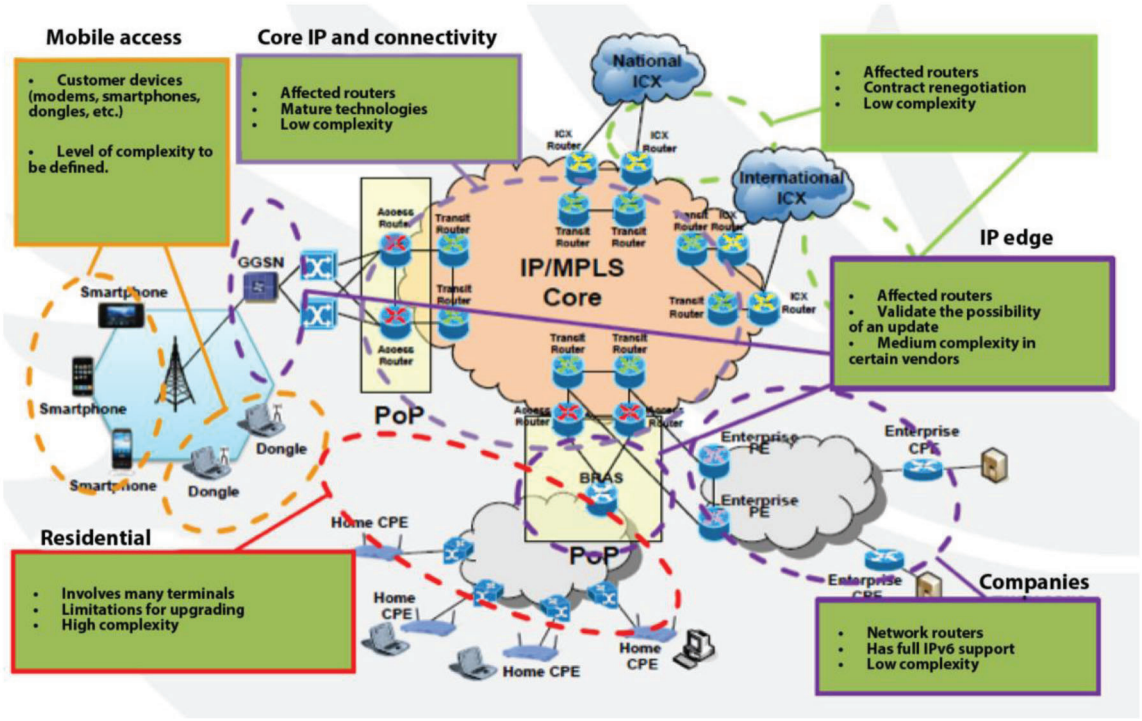
The following image shows the different parts of the network, their difficulties and the procedures that must be followed. It is an interesting example of the full fixed and mobile network structure of a horizontally-integrated operator and of the main points and issues on which operators must work. Every part of this network has been individually analyzed based on an inventory conducted at the beginning of Telefonica's transition process.

At present, Telefonica del Peru has 1.6 million fixed access customers, a figure that far exceeds the number of IPv4 addresses. The situation is as follows:

1. Twenty-seven percent of IPv4 addresses are being used through CGNAT, while the remaining 83% are used as public IPv4 addresses.

2. As for the use of public addresses, 20% of these are IPv6 while 80% are IPv4.

It is noted that IPv6 addresses play an important role along with the 27% of IPv4 addresses used with NAT.



The early adoption of measures to mitigate the reduction in the stock of IPv4 addresses has allowed Telefonica to begin deploying IPv6 addresses, thus reducing the pressure on the use of IPv4 addresses, many of which can still be used as public addresses. This allows for a progressive adoption process, free from the pressures exerted by quality issues deriving from high levels of IPv4 address sharing. Moreover, this early adoption has made it possible to deploy a dual-stack network through progressive network upgrades, without requiring any investments exclusively for the transition.

The general plan is as follows:

1. IPv6 deployment began in the ADSL network in 2012 using dual-stack, WiFi-enabled CPEs.

2. IPv6 deployment for corporate customers for which the network is ready should begin by 2016, as well as for those using the HFC network.

3. It is estimated that in 2017 deployment will reach mobile services, also using dual-stack with CGNAT.

All service activations are made employing dual-stack CPEs and, as seen above, CGNAT is deployed progressively on those nodes where a gradual reduction in the use of public IPv4 addresses is required.

As for large clients, only universities have requested IPv6; no demand has been observed from corporate customers, not even from those with international connections in Peru.

Due to the early adoption of a transition strategy, internal systems were upgraded progressively as necessary without having to deal with any problems. BSS systems are transparent to the addressing system employed so it was only necessary to update the provisioning systems.

With regard to the HFC system, they are currently working on provisioning and on CM validation. CMTS's have already been validated. Public addresses are being used at the moment, but plans have also been made to use dual-stack with CGNAT in this service.

11. SUCCESS STORIES OUTSIDE THE LACNIC REGION

This section contains a brief description of several successful cases worldwide. As reference, we have used a document prepared by a group of experts from the European Union and China which was published in March 2015[18].

11.1 France Telecom – Orange

This is a multinational company with operations in 32 countries and approximately 250 million customers. They operate mainly in the mobile market, providing broadband Internet access and corporate services.

In 2008, they launched a program to prepare an inventory of all equipment and systems with the potential to be affected by IPv6 implementation, evaluating their technical and economic impact. They organized this program in three phases for all their mobile, residential and business fixed services.

1. Introduction, in 2008-2009;

2. Migration of services, between 2009 and 2013; and

3. Production, a phase which began in 2013 due to the needs arising from the shortage of addresses observed for each of the operations.

They adopted the dual-stack technique, as this allows the most efficient and direct transition from both a technical as well as from an economic point of view. Highlights of their architecture include:

1.. Dual-stack-enabled routers are employed as CPEs.

2. Both CPE (fixed) as well as UE (mobile) are dynamically assigned by default a /56 IPv6 prefix (residential or corporate), at least in the RIPE region. Corporate customers have the option of requesting a /48. Prefixes are assigned to CPE via DHCPv6.

3. UE support CLAT and are assigned a /56. Mobile customers are provided with an IPv6-only connection based on a single PDP[19] IPv6 context.

In any case, depending on the development of their networks and business conditions, Orange's operations may choose to go through a dual-stack transition phase using two different PDP contexts, or a single dual-stack IPv4v6 context.

4. In the core network, IPv6 traffic is transported natively on a 6PE network through MPLS. Thus, the routers become dual-stack without changing anything in the MPLS IPv4 network.

Orange has been providing IPv6 peering since 2002 and IPv6 VPN services since 2009. Orange Poland was the first operation to start offering mass fixed and mobile IPv6 services in November and March 2013, respectively. In December 2014, 25% of Orange Poland's traffic was IPv6 traffic.

Other operations such as Spain and France will begin mass deployment in 2016 or 2017. Internal tests were conducted in France in 2013 and field testing with more than 100,000 FTTH customers will begin in 2015.

In Africa, Orange is working intensively in preparation for the transition, although it does not anticipate shortage of IPv4 addresses until 2019. This movement is primarily motivated by the expectation that IPv6-only content may begin to appear, in which case IPv4-only customers will not have access to the same.

In turn, the development of the Internet of Things is anticipated which will surely change the current situation of the Internet. The following challenges are observed:

1. The need to uniquely identify each object, regardless of the technology they employ and whether they are fixed or mobile.

2. The ability to support a significant traffic increase at access and core level, which would have a strong impact on their design, considering the volume and traffic pattern generated among these objects.

3. The characteristics of the services provided, which will affect traffic management policies, traffic prioritization (e.g. medical services), route reliability and robustness, etc.

In order to support the challenges arising from the transition, Orange considers it very important for vendors to align with operators' plans. They also believe that education and training in IPv6 must be permanently available in order to achieve success thanks to the knowledge of all stakeholders.

18- Project funded by the European Union to strengthen cooperation between the European Union and China in the deployment of IPv6 and Future Internet Research and Experimentation (FIRE) activities.
19- The context in these cases refers to the virtual circuit of data, or tunnel, from the user terminal to the external packet network to the mobile service. Also known as PDP/PDN context in GPRS/UMTS networks. PDP stands for Packet Data Protocol; PDN stands for Packet Data Network. In LTE networks, these virtual circuits are called EPS carriers and serve a similar function. EPS is the Evolved Packet System, also by its acronym in English.

They also repeated something that was also observed during meetings with LACNIC in different countries of the region in the sense that the problems that need to be solved are varied, not primarily technical, and of varying degrees of difficulty depending on each case: training for the NOC, marketing staff, managers and others; service platforms; systems in general; etc.

11.2 Deutsche Telekom

In December 2012, Hrvatski Telekom, an operation of Deutsche Telekom (DT) providing residential and corporate fixed and mobile services in Croatia, launched TeraStream, a native IPv6 network based on a combination of cutting-edge network and Cloud technologies which DT is considering deploying in its operations.

Furthermore, DT provides IPv6 mobile services in 16 countries and fixed services in 11 countries, in all cases due to the exhaustion of IPv4 addresses. Since 2012, all new fixed services are dual-stack enabled.

Regarding mobile networks, DT considers the following:

1. There are two main impacts of IPv6 on its networks: the platforms that carry traffic and the platforms that process IP addresses in the application layer.

2. Dual-stack support is as follows:

a. Two primary PDP carriers in IPv4 and IPv6 from the Rel-99 of the 3GPP.

b. New data network (PDN) IPv4v6 from the Rel-8 of the LTE and Rel-9 of 2G/3G networks.

3. The development of IPv6 support is required in the terminal, the core, the transport network and the OSS/BSS systems.

4. The new network architectures such as TeraStream show that IPv6 provides substantial improvement in customer experience and significant cost savings for the operator.

11.3 Telefonica

Two main issues are analyzed in from the point of view of Telefonica's transition to IPv6. It has already been mentioned how their regional operations have begun aligning with these corporate guidelines starting from 2009-2010.

11.3.1 IPv6 transition methodology

The most common methodology adopted in each of Telefonica's operations is quite similar to that adopted in Spain.

1. Early testing in network and R+D labs. Most networks have been involved in IPv6 testing for about 15 years, mainly through collaborative projects with universities or as part of national and regional initiatives. The most famous of these projects was Euro6IX, which was funded by the European Union and took place between 2002 and 2006.

2. Auditing network impacts. Many networks have already gone through this stage where affected parties are identified and actions and related costs are anticipated. The areas under study are the peering nodes, the core, the access nodes, CPE and UE, BSS/OSS and marketing areas (definition of the service / product).

3. Transitioning the core network and access nodes. This area of work requires the intense and essential involvement of human resources of the network engineering and planning department for each operation. Transition work in the core and in the transit and or peering nodes is the simplest and in turn essential prior to developing IPv6 elsewhere on the network. Core traffic is usually carried on the MPLS network after enabling 6PE on edge routers. As for the transition of the access network, a strategy must first be selected after which nodes not supporting IPv6 must be migrated at carrier level. The strategy depends on several factors such as the current status of the network, the stock of IPv4 addresses, the level of maturity and availability of the equipment required by each technique, etc. Since IPv6 deployment begins when there is a shortage of IPv4 addresses, pure dual-stack with global IPv4 will generally be combined with other IPv4 address sharing techniques.

4. Commercial IPv6 deployment. This complex phase involves defining services, network engineering and operation and management areas. In Spain this stage has not started yet, due to the priority given to other deployments such as LTE and fiber networks.

11.3.2 IPv6 transition strategy

As already mentioned, because of the diversity of architecture, equipment, services and deployment agendas, Telefonica believes that there is no single solution for all its operations. In general, the following can be used as a guide:

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

1. Residential fixed broadband networks. Wherever possible, the dual-stack technique will be the main strategy. If there is a shortage of IPv4 addresses, these networks must resort to CGNAT. PCP (Port Control Protocol) techniques are necessary due to double NAT at carrier and customer level, so that the terminal can control how IPv4 and IPv6 packets are translated and sent through the router operating as NAT. In Spain, customers are provided with a dynamic IPv4 address, a dynamic IPv6 /60 prefix and a dynamic /64 prefix for WAN router connectivity.

2. Mobile broadband. At this time, a private IPv4 address is supplied to users within the main PDP context. As for IPv6, a dynamic /64 block is provided within the same PDP context (3GPP Rel-8 LTE and Rel-9 2G/3G). In other words, the dual-stack technique is used in a single context or EPS carrier.

11.4 Conclusions

In this brief review of success stories outside the region, we conclude the following:

1. Orange began working early on preparing for IPv6 deployment through a three-stage program that ended in 2013.

2. Deployment is being carried out in operations as the necessary conditions arise, having started in Poland in 2013.

3. In Africa no shortage of IPv4 addresses is expected until 2019; nevertheless, Orange is working on preparing for deployment anticipating that IPv6-only accessible websites might start being developed at any time.

4. It is considered very important that vendors be aligned with the operators' plans in order to support the challenges arising from the transition.

5. Likewise, the provision of ongoing education and training in IPv6 is considered important to achieve success by raising the awareness of all stakeholders.

6. The duration of the transition project can take from several months to several years depending on the particularities of networks, country size, etc.

7. DT understands that the deployment of IPv6 affects not only the network but all systems such as OSS/BSS.

8. The use of native IPv6 substantially improves customer experience and results in significant cost savings for the operator.

9. In line with those of other operators and with the logic behind IPv6 deployment, Telefonica is implementing the main stages of IPv6 deployment: laboratory testing, auditing the impact of IPv6 on the entire network and all systems, transitioning the core network and access nodes, and, finally, large-scale deployment at residential level.

10. Telefonica has selected dual-stack for fixed networks and dual-stack in the same context for mobile networks.

12. STRATEGIC IMPORTANCE OF IPV6 DEPLOYMENT

The strategic importance of this deployment is seen on two levels: at national level (Internet service provided to users) and at provider level.

As to providers, the most active players in this deployment process, every aspect involved has been qualitatively and quantitatively analyzed in earlier sections, outlining their strategic importance for ISPs and how providers are facing the transition efficiently.
This section will analyze strategic importance at country level.

12.1 Most significant current impact of IPv6 adoption on public and private sector productivity

In this section, the impact of the transition to IPv6 with current market conditions is analyzed. The following section outlines certain trends that may lead to more drastic changes in the deployment.

Impact on productivity may arise from two main aspects that have already been discussed: the quality of service that affects the operations carried out over the Internet (inquiries, exchange of documents, etc.), and whether or not certain contents and applications can be used. This impact is similar in the case of leisure activities.

While an ISP provides Internet access services with IPv4 addresses and no address sharing (e.g., when its stock of IPv4 addresses is enough to support the growth of its customer base), users will not encounter any problems nor will they notice any improvement if the ISP provides IPv6 addresses, e.g., through dual-stack.

In the case of markets where there are enough IPv4 addresses (e.g., Chile, where there the IPv4 address stock is enough for at least two years) or in the case of ISPs with little growth of their customer base (e.g., ISPs offering only corporate services), there is no strong pressure to share these resources; consequently, the solution to continue using public IPv4 addresses is appropriate as long as the transition process is planned and started.
This situation can be maintained as long as content and applications accessible over IPv6 only do not begin to appear. While there are no studies indicating when this might occur, several operators (i.e. Orange operations in Africa) have already started the migration process even though they still have enough IPv4 addresses to cover their current needs.
In competitive Internet access markets, there is feedback which puts pressure on ISPs to provide the service with the quality required by users and to transition to IPv6 as soon they see or anticipate the negative effects of continuing to share IPv4 addresses. Sometimes, as noted during the interviews, ISPs deploy IPv6 and continue using CGNAT, but provide public IPv4 addresses when customers demand greater quality. All this is part of a balance that optimizes ISPs' investments, thus maintaining quality of service. This greatly reduces the impact which the transition to IPv6, its start and deployment have on productivity.

In addition, ISPs provide public IPv4 addresses to corporate customers, universities and government institutions because, in the context of these companies' private internal networks, IPv4 addresses do not usually yield high sharing ratios and also because it is what their customers demand. Therefore, this situation does not occur in cases where IPv4 address sharing might affect productivity.

In conclusion, competition among ISPs has led them to adopt a series of measures both in the residential as well as in the corporate market which have significantly mitigated - or even eliminated - potential negative impacts on productivity during the transition to IPv6 and under current conditions.

12.2 Prospective analysis of the impact of IPv6 adoption on public and private sector productivity

The impact discussed in the previous section refers to behavior at a macro level, and shows feedback leading to a general convergence of supply and demand under current conditions. That is, ISPs seek the most efficient way to meet the demand in volume and quality of service. This section provides a qualitative analysis along a prospective analysis of other possible effects that the IPv6 transition may have on productivity, depending on how it adapts to new requirements. A quantitative analysis would require more precise knowledge regarding the future evolution of the transition, the policies adopted by ISPs, how ISPs will adapt to new requirements, how users and application developers will adapt, and emerging technology requirements that rely on the Internet, among others.
Even if ISPs adopt mitigation measures at macro level, the difficulties which certain applications may encounter on networks using CGNAT have economic effects due to uncertainties regarding additional transaction costs for applications using the Internet. When a degree of uncertainty is introduced as to whether an application will be able to operate in different environments (e.g., user environments involving CGNAT networks), transaction costs increase and entrepreneurship is therefore discouraged. These problems are not a major concern for large companies, yet they create a barrier for smaller companies.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Furthermore, it is observed that the use of CGNAT increases delay by about 15% to 40% depending on which source of information or measurement protocol is considered. There are currently many applications being developed or implemented, such as remote control applications, vehicle monitoring, telesurgery and other similar applications related to the Internet of Things (IoT), for which reducing the delay and keeping it below certain safety thresholds is essential. The use of CGNAT should be avoided in these applications.
Corporate use of the Internet of Things also requires the possibility of building several separate subnets for different features such as security, production-cycle controls, management and others. These subnets are facilitated by the use of IPv6 addresses.
At the same time, other types of objections to IPv4 are starting to appear, such as the one mentioned by SK Telecom's Emerging Technologies Project Manager at @ Scale 2015 in the sense that delay-sensitive applications such as vehicular control applications would not be feasible with IPv4. This type of emerging issues having to do with the Internet of Things should be monitored, as they do not seem to fit with the high level provisions outlined in the previous section.

These are just a few of the objections which will be encountered as new applications are developed, particularly applications relating to the Internet of Things. This might accelerate IPv6 deployment.
It is believed that as the IoT advances it will have a significant impact on the Internet, as the connection of billions of smart and independently addressable devices is expected. The possibilities of the IoT would be severely limited without the use of public addresses. When the IoT gains momentum, in order to make the most of the possibilities it offers, it will be necessary to uniquely identify each device regardless of technology, regardless of whether devices are fixed or mobile or even if they change ISPs, in which case mobility and multihoming must be possible and the ability to process a significant increase in traffic will be required, as well as the ability to provide robust routes, ensure confidentiality, allow device auto-configuration and selective traffic prioritization.
This set of conditions required for the IoT will be a strong incentive for the deployment and provision of IPv6 services, given that services based on this protocol meet these conditions and allow expanding the Internet to user devices, systems, and virtually any equipment or item that might benefit from Internet connectivity.

12.3 Benefits of IPv6 deployment in terms of technical and economic efficiency

Many technical improvements have a direct impact on economic efficiency (e.g. in the reduced use of CGNAT) or indirect (e.g. due to better operation of applications, the use of subnets connected directly to the Internet in corporations, and others). The following are some of the main aspects that allow improving technical and economic efficiency through the use of IPv6.

1. With this system, the number of users under a network with public addresses can be increased despite IPv4 address exhaustion, thus maintaining the principles of end-to-end connectivity and the simplicity of network access and transport, transferring intelligence to user ends. Ultimately, it enables the simple, direct and efficient connection between any two users of the Internet.
2. Due to the number of available addresses, it is possible to have subnets for each end user and for different purposes (administrative network, security camera network, etc.) providing direct end-to-end connections without using proxy servers.
3. Communication via mobile networks currently implies that moving traffic is always commanded centrally by the operator, which gives rise to certain difficulties. Work is being carried out to allow distributed mobility management in IPv6, as noted in RFC 7429 (January 2015), thus improving the quality and simplifying management, mainly in view of the massive expansion of mobile devices. In this sense, mobility involves moving from one network to another while maintaining the same IP address, while multihoming makes it possible to be connected to more than one ISP at the same time.
4. Only services offering IPv6 allow taking full advantage of the benefits of the IoT.
5. Routing is easier to implement. It is possible to add user prefixes operating on the same network into a single prefix for publication, eliminating also error control in each network hop. This is possible due to error controls in other layers above and below the network in which the IP protocol operates, thus obtaining higher quality of transmission in existing networks. The ability to add routes in IPv6 is far superior to that of IPv4, given that the latter protocol allows variable lengths for hosts and networks, while IPv6 has reserved 64 bits for identifying each part of the address: the network and the interface (host). This makes it possible to add an increasing number when uploading on the network: /56, /48, etc.
6. An increase in delay occurs when using CGNAT, which worsens performance for applications where delay is critical.
7. The IPv6 network allows "stateless" host autoconfiguration in the allocation of addresses. The router sends the prefix and the host can configure the address using its MAC address, or do so randomly so as to not reveal its MAC. New methods for configuring addresses have appeared recently which do not to use the MAC address. For example, RFC7217 specifies privacy addresses that will be used in Linux by default.

13. DEPLOYMENT GUIDELINES AND RECOMMENDATIONS, SCOPE, INSTRUCTIONS AND TRAINING

These recommendations and guidelines are based on one of the main conclusions of this research:

> None of the stakeholders can be externally forced to initiate or accelerate the transition to IPv6. Every decision is based on each stakeholder's development strategy and economic assessment, both of which rely on a prospective analysis of future requirements and constraints and the impact thereof.

Consequently, these recommendations and guidelines are aimed primarily at disseminating in-depth knowledge among stakeholders regarding all current and future implications of the decision to to deploy IPv6 or not, so that these can be taken into account in the process of deciding which strategy to follow. All information contained in this document, including the model for the economic comparison of transition alternatives, can be used to support these guidelines and recommendations.

13.1 Main problems encountered during the transition in the countries of the region. Regional challenges.

On average, the region shows a LACNIC/CAF ICAv6 indicator that is significantly lower than the one corresponding to the countries selected for international comparison. As for partial indicators, the one pertaining to Users is a partial indicator of IPv6 deployment according to which the region is far behind more advanced countries. These indicators are shown in the table below.

Indicator	LACNIC Region	Reference countries	Reference countries / LACNIC region
LACNIC/CAF ICAv6	21.39%	39.59%	1.85
Planning	18.08%	28.89%	1.60
Transit AS	55.30%	79.23%	1.43
Content	50.77%	49.96%	0.98
Users	1.31%	15.08%	11.51

The LACNIC/CAF ICAv6 indicator is meant for countries in the initial stages of IPv6 deployment, which is why it assigns a weight of 30% to planning and the early stages of deployment, such as having IPv6 transit available in autonomous systems. In terms of these two indicators, the countries of the region are well below the selected countries, but the efforts required to achieve progress in these countries are small as compared to overall deployment efforts. Progress in these two indicators is directly related to a large extent to the depth of knowledge which stakeholders have concerning all matters with reference to migration to IPv6, apart from the strictly technical issues. In this sense, the most effective tools are LACNIC's actions aimed at obtaining further knowledge, whether on its own or working jointly with other stakeholders such as universities, academic networks and/or governments.

As for content, the percentage of IPv6-accessible content is similar worldwide and there are no effective actions for improving this situation. By way of exception, it should be noted that the expansion of e-government and educational content, all in IPv6, may increase this percentage, although not in a very relevant way. All things considered, this expansion to IPv6 is inevitable in future development.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Finally, the User indicator (which represents the percentage of users who are potentially able to operate in IPv6) is very low in the region. It is ultimately the main indicator where the gap with more advanced countries can be seen and represents one of the main challenges to overcome.

In regard to this indicator, the survey shows that approximately 30% of respondents are planning to start deployment in their access network in 2016. In the meetings held in the various countries, practically all ISPs providing residential services (mostly medium and large providers) noted they are planning to start this deployment in 2016.

In order to align the situation in the region with that in more advanced countries, the following recommendations should be taken into account.

13.2 Adjustments to regulatory frameworks and policies so that they will facilitate IPv6 deployment

The main regulatory frameworks that can facilitate IPv6 deployment are analyzed. This deployment is necessary to avoid some of the problems at country level discussed in other sections:

1. Some ISPs that fail to start the transition in a timely fashion may have problems with the exclusive use of CGNAT, given that there are applications that do not work behind CGNAT and this solution limits the number of ports supplied to each user. Under these circumstances, quality of service suffers.

2. IPv6 deployment improves communication quality, for example in terms of delay, as is currently being manifested by companies such as Facebook and Verizon, among others.

3. As mentioned by Orange, many operators believe the transition should begin even though they have sufficient stock of IPv4 addresses, given that in the near future websites only accessible via Pv6 may begin to appear.

4. At country level, the early implementation of actions aimed at transitioning to IPv6 (e.g., replacing obsolete equipment with IPv6-compatible equipment) can reduce future investments required at national level when problems arise which force IPv6 deployment.

All these problems and actions have to do with the quality of service (delays, operation and quality in use of applications, etc.) of Internet access within the country and with the reduction of the social cost of investments. Likewise, quality of service also has to do with the recurring social cost of a reduction in quality or limitations on applications. Because of this, the applicability of regulatory measures to promote this deployment should be analyzed.

13.2.1 Regulatory framework for telecommunications

The basic principles of telecommunications regulations include technological neutrality, which is separate from and has a larger scope than net neutrality.

Published on 12 May, 2004, the Declaration of Principles of the World Summit on the Information Society organized by the International Telecommunication Union (ITU), states that "The rule of law, accompanied by a supportive, transparent, pro-competitive, technologically neutral and predictable policy and regulatory framework reflecting national realities, is essential for building a people-centered Information Society. Governments should intervene, as appropriate, to correct market failures, to maintain fair competition, to attract investment, to enhance the development of the ICT infrastructure and applications, to maximize economic and social benefits, and to serve national priorities." (Section B6, Enabling environment, Principle No. 39)

This principle is recorded in the above regulation, comparing the text before and after the Summit. By way of example:

General Telecommunications Act 8642 (June 30, 2008) of Costa Rica states in its recitals as follows: "The General Telecommunications Act is a modern act and one of the first acts regulating convergence in the Americas. (...) The regulation on convergence involves guaranteeing interconnection between different types of networks, the establishment of a strong and independent regulator, and the introduction of the principle of technological neutrality as a basic principle. (...)"

Article 10 of the El Salvador's Telecommunications Act (updated on 25 November 2010) establishes a provision applicable to mobile services: "The National Frequency Allocations Table should respect the relevant rules and recommendations issued by the ITU, without preventing the alternative use of the spectrum by different technologies."

The principle of technological neutrality appeared in European regulations in 1999, during the review of the regulatory framework. It was adopted as one of the five basic principles governing the regulatory framework for electronic communications in the European Union. The preamble of framework Directive 21/2002/EC6 and, more recently, the articles of Directive 2009/140/EC, incorporate this as a basic principle for regulating electronic communications within a converging environment.

Thus, establishing regulations requiring the use of a specific technology such as IPv6 would not be consistent with the above and would violate a basic principle, except as noted below.

The consultant believes that the compatibility of this universal principle with imposing requirements for the issuance of new operating licenses (which, depending on the issuing country and scope, might be referred to as licenses, permits, concessions, authorizations or similar) should be analyzed on a case-by-case basis.

First, requiring IPv6 deployment is not the same case as imposing one of several available technologies; instead, it only means requiring an early start in the use of a technology which every operator must inevitably implement in the near future. Moreover, this obligation always results in a reduction of future costs and problems which might affect quality of service and is therefore part of the usual powers of regulatory agencies. Ultimately, it is not a pure violation of the principle as there is no doubt that it is the only viable alternative.

With this issue clarified, the next step is to analyze when this obligation might be established.

Clearly not when operating licenses have already been granted. At the time the operator submitted a request for the license there was no obligation to use IPv6. Therefore - and this issue is beyond the scope of the regulator - the operator structured its business plan based on the principle of technological neutrality and has the right to maintain the conditions existing prior to the granting of the operating license.

The situation is different in the case of new licenses, as several reasons concur to support the establishment of the ex-ante obligation to deploy IPv6:

1. The regulator would include this requirement as part of its requirements for granting the license, which may include obligations relating to universalization, broadband deployment in certain rural, remote or underserved areas, etc.

2. In that case, the applicant might not be interested or, typically, might include such obligation in their business plan.

3. Clearly this requirement does not impose a distortionary limitation on the market; instead, it establishes regulations for taking early action on something that is inevitable and beneficial for citizens in general.

In view of the above, the consultant believes it would be possible to amend the regulations affecting the sector without violating this principle if an obligation to deploy IPv6 were to be included at the license granting stage.

In this regard, during our visits to the different countries of the region we observed that a new entrant operator with high growth rates and major investments had no plans to deploy IPv6 ¬until the meeting. These are the situations that should be avoided through training and the ex-ante actions mentioned above.

13.2.2 ICT regulators

Regulators exist in most countries and are responsible for the development of ICTs in general, including the dissemination and promotion of the knowledge people need in order to enter the Digital Economy. Given the fact that a timely transition to IPv6 — or at least that all stakeholders have the knowledge needed to make effective, efficient, and sound decisions — is so important for any country, it is recommended that ICT regulators become involved in the dissemination of knowledge on IPv6. LACNIC plays a very important role in the region and can provide the necessary support for these actions. This transfer of knowledge might be in line with the main topics included in this document.

13.2.3 Regulatory framework for public procurements

The consultant believes that the only regulatory framework on which it is possible to act is the one governing public procurements. In many cases, large public institutions include IPv6 support in their purchases. However, many small and medium agencies do not, or do so incompletely (e.g., replacing part of the network with IPv6-compatible equipment, yet maintaining IPv4-only wireless equipment).

Therefore, it is very desirable to have general and uniform guidelines to ensure an efficient, orderly and full transition to IPv6 for both large as well as small and medium agencies. These regulations have several important advantages:

1. The main rules are developed by a team highly specialized in the transition, ensuring the consistency of progress of institutional networks towards IPv6.

2. Requirements for public hardware, software and connectivity procurements are standardized. These represent very large volumes for different market players such as ISPs, software and hardware suppliers, and terminal equipment vendors, among others.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

3. Thus, even small purchases are guaranteed to be in line with the general policy expressed through the guidelines.

4. This standardization creates efficiencies across one of the main customers of IP equipment. This increase in efficiency not only affects public institutions but also ISPs and other stakeholders.

These regulations should be complemented with one for ensuring network security and the privacy of personal information, all of which may present points of vulnerability in the transition process.

The general stages of the transition to IPv6 have many similarities with those developed by some ISPs for evolving their own networks. The following list is presented merely as an example.

1. Defining the major technical guidelines to be followed (e.g., transition technique, addressing plans, inventory management for IPv4 and IPv6 addresses).

2. Preparing an inventory of all hardware, software, internal services and connectivity, which will provide a solid diagnosis before beginning the transition. This inventory should include every network component and service (web server, email server, etc.), their current status, the feasibility of their being upgraded, or replacement requirements.

3. Preparing an inventory of the equipment and systems that provide security and privacy to the institution's network.

4. Developing a detailed transition plan which considers the inventory as well as current and future requirements, budget, stages of the transition, etc. This plan should include the security and privacy plan to be implemented simultaneously with network transition and its connectivity.

5. Defining the specifications required to ensure the transition to IPv6, including even the simplest equipment such as hotspots.

6. Establishing protocols for equipment testing and approval.

7. Specifying training courses covering technical and operational issues, as well as general knowledge of the institution.

8. Defining procedures for installing new equipment or upgrades, as well as mechanisms for approving their operation.

9. Validating the IPv6 compatibility of all hardware, software, applications, systems and connectivity prior to commissioning.

10. Validating security and confidentiality policies.

11. Conducting operational tests for all network equipment, software, applications, systems, and connectivity.

12. Conducting operational tests regarding security and confidentiality.

13.3 Academic networks and universities

Academic networks and universities play a crucial role in IPv6 development.

According to the evidence collected during our research, they are important from four main points of view:

1. Education. Universities are the leading institutions for transmitting knowledge on Internet technology. As regards IPv6, it is believed they should extend the scope of knowledge beyond the protocol itself and matters strictly related to IPv6. Considering the role students or graduates will play in decision-making and other processes, it is important that they also obtain knowledge on aspects related to the impact of deploying IPv6 or not, for which the general ideas expressed in this document might be considered.

2. Training. Given their accumulated knowledge, academic networks and universities are also LACNIC's natural allies in training stakeholders: ISP engineering, operation and maintenance staff, content providers, government institutions, websites and others. It is important for this training to also reach non-technological universities which, due to their nature, may not have sufficiently trained technical staff to receive and implement the transition to IPv6.

3. Key deployment drivers. There is enough evidence showing how first academic networks and then isolated universities have played a prominent role in the initial deployment, and even in collaborative work with providers, in the initial moments of deployment in several countries of the region. This effect occurs in cases where IPv6 compatibility is established when purchasing equipment and connectivity, thus driving some vendors who are still not involved in IPv6 deployment to prepare their networks and services in order to be able to compete in procurements.

4. Internal training. There have been cases of academic networks with IPv6 connectivity enabled at the border

but where deployment stalls and does not follow through towards the internal network. Hence the importance of knowledge transfer to all institutions and mainly to those which are non-specialized in these technologies.

This means that the academic networks and universities are agents of major innovation and thus play an important role in the timely deployment of IPv6. Faced with this situation in which disparity in progress or stagnation is evident in the region, LACNIC actions focusing on this state of affairs, seen in the training on extra-technology details as part of those developed in this research, can make the progress more efficient and generate positive results at country level. Practical issues are essential for a timely deployment for many reasons: from an economic perspective, better quality of service, taking advantages of the features IPv6 offers, and the restrictions of IPv4-only utilization.

13.4 Companies

Their internal networks are prepared for the use of NAT and their staff is familiar with this technology. The evolution towards IPv6 involves investments which are typically not required for other reasons; in addition, the new protocol can bring compatibility issues that may potentially affect their entire network and applications.

Notwithstanding the above, it is observed that the future development of the Internet, particularly the Internet of Things or the appearance IPv6-only websites, may cause problems for the efficient operation of companies that do not migrate to IPv6.

The gradual transition to IPv6 is considered essential so that companies can also progressively take advantage of the advances that this new Internet will bring.

For all of the above, it is recommended that both LACNIC and universities, whether jointly or separately, make progress in training companies through the institutions which bring them together (e.g., chambers of commerce) so that they will b aware of the consequences of not taking early action in the transition to IPv6.

13.5 ISP

Each ISP must take action regarding the transition to IPv6 according to their economic, financial, commercial, strategic and technological evaluations. Notwithstanding the above, it would be desirable for ISPs to consider certain issues arising from the results of this research.

1. Initiate IPv6 transition actions as early as possible. There is sufficient evidence at regional and global level to suggest that the transition process presents difficulties, many of them unexpected, an that these are encountered not only on the network but also on internal and peripheral systems and services, as described in the analysis of the regional situation presented in Annex I - Field Work and international and regional success stories.

2. The sooner the process begins, urgencies due to IPv4 address exhaustion will be avoided; in addition, many of the actions involved in the transition can be implemented during the natural process of replacing or upgrading outdated equipment and systems, or as required due to other reasons unrelated to IPv6. In these cases, additional investment for IPv6 may be marginal or even zero. This even applies to CPEs.

3. The process should begin with basic training on IPv6 in all relevant areas of the company, with strong emphasis on engineering and operations if these do not exist.

4. This should be followed by a stage in which a complete inventory of equipment, systems, software and connectivity is conducted for determining the readiness of each item for the transition. In the case of the most important equipment, an evaluation of costs and timing for their replacement or upgrade is also required.

5. Develop a transition strategy which includes the techniques to be employed, as well as anticipated stages, according to the requirements set by IPv4 address demand and existing stock.

6. This strategy generally follows a gradual, initial and simultaneous mode of action in the core and access nodes, as well as in the work systems (OSS, BSS, address inventories, business intelligence, etc.) and central services (DNS Firewall, etc.). Finally, the deployment at access points is reached.

7. Develop the main structure of procurement documents with specific conditions that fulfill the transition objectives, as well as approval protocols and equipment testing.

8. Develop a progressive training plan suitable to the deployment.

9. Make the economic-financial evaluations of alternatives based on an analysis that includes the impact of the strategy adopted over the next 5 years. The model developed for this study can be used as the basis for this analysis, as it is ideal for adjusting operational expectations to financial expectations. This model is highly modular and fully customizable.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

13.6 Road map to encourage a timely transition to IPv6 in the region. Training plan.

In this road map, LACNIC's role is essential for establishing the conditions for a timely transition to IPv6. LACNIC's work is ongoing with regard to raising awareness among its members and governments and promoting IPv6 deployment, and is widely recognized at regional level, which in this particular case has been reflected in the results of the survey and in the meetings conducted in each country.

This work concludes that it would be appropriate for LACNIC should focus its activity on certain issues that would encourage the timely start of the transition to IPv6. As used above, the term timely refers to the fact that the transition cannot be mandated and therefore actions should seek to provide evidence and knowledge so that the transition can be completed efficiently and in due time. Priority issues for 2016 include:

1. Developing a set of activities to provide all actors involved in the transition knowledge regarding the implications of IPv4 address exhaustion. These implications should include the many aspects described in this document: problems stemming from the use of CGNAT, the importance of deploying IPv6 in access networks, quality of service and efficient use of resources, current status and behavior of the various actors, an economic evaluation of available alternatives according to each ISP, best practices at regional and global level, the importance of an early start to the process of preparing for the transition, appropriate and necessary government actions to facilitate the transition, and the importance of universities and university networks, among other aspects.

2. Conducting activities aimed at developing public policies and guidelines that will harmonize and ensure deployment at national level:

a. Making sure that public procurements for hardware, software, systems and connectivity require IPv6 compatibility.

b. Purchases and procedures that ensure high security standards during the transition to IPv6.

c. Developing e-government and educational content which is accessible via IPv6.

d. Universal networks such as community WiFi (squares, schools, etc.) and similar using dual-stack.

3. Preparing model policies and guidelines based on best practices which can be used as input for the activities described above and as a reference for different countries.

4. Updating LACNIC's website structure as regards the Observatory on the transition to IPv6.

a. Considering the implementation of some type of "distinguished IPv6" badge and publishing on LACNIC's website the countries and stakeholders which meet certain conditions in the IPv6 transition process.

b. Keeping up-to-date LACNIC/CAF ICAv6 as well as partial indicator values on LACNIC's website so that they can serve as as a benchmark for different countries and operators.

c. Making the model for the economic evaluation of alternatives available on its website.

d. Including a blog on different aspects of the IPv6 transition that will also highlight success stories.

e. Expanding the repository of relevant documents, possibly including, among others, all the references used in preparing this document.

5. Achieving the goal that 100% of its members will have been assigned an IPv6 address by the end of 2016. Survey results illustrate the fact that in most countries some smaller ISPs have not been assigned any IPv6 address blocks. As for universities, approximately 30% of countries are in the same situation.

Considering the dynamics of the situation as far as IPv6 deployment, it is recommended that a plan for 2017 be developed in mid-2016 containing any new requirements which may arise as a result of the activities conducted in 2016.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

ANNEX I. FIELD WORK

The opinions and information made available to the community in this document are the result of the interviews that were conducted and the selfless and valuable collaboration of multiple stakeholders with whom we worked in the different countries. Their publication does not necessarily mean that LACNIC validates these views and information.

1. ARGENTINA

The institutions we interviewed included RIU (the Association of University Interconnection Networks), CABASE and NIC Argentina, as well as some horizontally or vertically integrated operators, large and small ISPs, fixed HFC and non-HFC, mobile ISPs, transit ISPs, wholesaler, corporate and retail providers. These included: Cablevisión, Gigared, iPlan, Level (3), Telecentro, Telecom Personal, and Telefonica Movistar.

Highlights of our findings are listed below.

1.1 RIU – Association of University Interconnection Networks

RIU has been an important vector for IPv6 deployment in Argentina since their major purchases began requesting the provision of IPv6 services. In its 2007 tender, RIU made IPv6 support a mandatory feature for the international link of the university network's core. One reason is that since 2003 universities have been working on IPv6 and it was essential to be able to connect to the outside world using this protocol.

Operators weren't ready at the time, so they formed a joint task force with the contractor to implement IPv6. Thus, IPv6 connectivity was ready in 2008 and was fully operational on the operator's backbone in 2009.

This role of the RIU was important both because it promoted early deployment of IPv6 at operator level and because it kicked off the collaborative work that led to IPv6 implementation. In any case, RIU had already implemented IPv6 on its CLARA Network interconnection.

From then on, other customers began using the IPv6 backbone network which had been deployed.

In 2011, RIU issued a new call for tender, the winner of which was a different operator which also deployed IPv6 in its backbone to provide the service to RIU.

As for IPv6 deployment, it's all dual-stack and they have IPv6 peering agreements with CABASE, Google and others.

They have also found that various academic institutions may have firewalls that don't support IPv6 and most WiFi networks don't support this protocol. Thus, observed IPv6 traffic is considerably lower than potential IPv6 traffic.

The use of free software made it easier to use IPv6, as free software was IPv6-ready before proprietary software.

In short, the role of the RIU has been to promote IPv6 in Argentina through pioneering its deployment, making knowledge available and requiring IPv6 connectivity in its purchases.

1.2 Major ISPs providing services to end customers

1.2.1 Case 1

While it may not strictly be classified as a success story due to the actual results in terms of the LACNIC/CAF ICAv6 indicator, a large multinational ISP which provides residential, wholesale, mobile and corporate services has a well-defined plan and is well-advanced in terms of IPv6 deployment. It is interesting to note the work which has been carried out and the direction in which they've taken their project.

At international level, approximately five years ago the ISP adopted the strategy of migrating all operations to IPv6. At the time, dual-stack and DS-Lite techniques were being established and the ISP adopted the first of these options. The main reasons for this were, first, to address the shortage of IPv4 addresses and high broadband growth rates; second, corporate strategy. This plan began with a detailed inventory of all network equipment and their ability to be upgraded to IPv6, whether they were IPv6-ready, etc. Overall, aggregators had the greatest replacement needs.

About two years ago, the ISP began its preparations in Argentina with proofs of concept, pilot projects, equipment and system upgrades, etc. in all business units, particularly its fixed and mobile retailers. Due to the difficulties inherent to mobile networks, pilot tests conducted on fixed networks were the first to be completed. This operator's transport network has been operating on IPv6 for years using 6VPE. Provisioning and other systems are also IPv6-ready, as are the operator's aggregators and xDSL CPEs.

Corporate customers have no pressing current or future need for IPv6 services, so this service has no commercial value. In any case, they are provided with IPv6 over MPLS using 6VPE with CPEs and routers in dual-stack mode. This is valid regardless of the country and provider.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

As for wholesale customers, this operator has been providing IPv6services, including peering. The main reason for this is that, as soon as they have or plan to provide end users with IPv6, wholesale customers require IPv6 peering or transit services.

Likewise, IPv6 itself has no commercial value for retail, fixed and mobile customers, so in this case IPv6 deployment will occur according to the needs and development strategy adopted by the operator.

All operations have adopted dual-stack with native IPv6 access and dynamic CGNAT44 to continue supporting the services that still require IPv4. It's an interesting strategy that minimizes future disposable investments, thus lowering IPv4 address demand for all services which may be provided over IPv6. CGNAT deployments are initially centralized, but the evolution of high-speed services such as video streaming drives the network to a decentralized model and brings NAT closer to the edges where aggregation occurs.

High speed deployments are based mainly on FTTC and VDSL.

The strategy does not involve the complete replacement of client terminals with dual-stack, as this has not been required by customers who don't care about technology as long as they receive a quality service. Terminals will be replaced gradually as they reach obsolescence or when necessary to provide the service. In access networks, the cost of the terminals represents an important portion of the investment in IPv6 deployment, as we already showed in our study of the costs in the model. Moreover, the acceleration of customer mobile replacement rates means that IPv6 deployment with significant impact on the mobile ISP can be expected.

1.2.2 Case 2

Another large ISP which has also opted for dual-stack with CGNAT as its development strategy reported similar motivations for deploying IPv6 in its access network. Because fixed end client growth rates are not high, IPv4 without CGNAT is maintained. Therefore, deployment efforts focus on mobile services with high growth rates and apply CGNAT.

As for the mobile network, a series of measures have also been implemented, among them the optimization of the use of IPv4 addresses, freeing resources in order to be able to continue to grow without unnecessary address scarcity issues. In any case, IPv6 will be deployed in the operator's access network with the addition of DS terminals that have already been approved, while at the same time maintaining CGNAT, which has been operational for about three years.

They mentioned that the main problems they need to solve concern maintaining the stock of addresses, post-sale support, and provisioning. Due to the simplicity of the process in the mass market with an address transparently assigned to each terminal, it should be noted that until now the assigned address was of no concern to the systems or the staff.

They have found that smaller clients - whether wholesale or corporate - do not require IPv6.

As for the training required for this deployment, they understand it is very important at all levels but mainly for staff involved in operations.

A notable aspect that was also brought up was the development of new aspects of business intelligence such as traffic systems, registering and monitoring customers who migrate to IPv6, attention to legal affairs, mitigating attacks, etc. This is an important set of issues that must be solved in parallel with those relating to the network and systems.

1.2.3 Case 3

This is the case of a multi-service provider using HFC networks.

This operator believes they would have no problem with CGNAT if the allocation was dynamic and also used dual-stack. They understand there may be problems with CPEs and share the opinion of other operators who believe that not all new equipment is fully IPv6-compatible. This is a matter on which they are working and for which they do not receive the necessary support from equipment vendors, something they consider to be a recurring issue.

The consultant notes that motivation for IPv6 deployment will be mainly due to operator rather than customer requirements.

1.3 Other ISPs not providing mass services

Generally speaking, they've already deployed IPv6 in their core and in certain cases in their corporate access networks as well. In this case too the consultant notes that the way forward is to deploy dual-stack directly to end customers and 6VPE for IPv6 in the backbone as it runs on MPLS. In certain cases, they receive requests from abroad for corporate IPv6 termination.

An accepted view is that the basic problems do not involve the network but rather the systems.

They note that corporations and government institutions often request the provision of IPv4 blocks along with the service, something which in certain cases might be motivated by an awareness of IPv4 exhaustion (when the request exceeds a reasonable amount of addresses).

1.4 NIC.ar

There has been a move towards IPv6 deployment within NIC.ar. In addition, NIC.ar is significantly promoting IPv6 deployment at government institution level through the Department of Cybersecurity under the President's Office.

1.5 Conclusions

1. Argentina is expected to experience a rapid growth of the Users indicator (currently 0.02%) and this will boost the joint indicator, thus reflecting native IPv6 access, mainly through mobile networks.

2. RIU has been a major player in this deployment thanks to its purchases requiring IPv6, the early accumulation and sharing of knowledge, and pioneering the move to IPv6.

3. In general, we observed that at one time or another all the institutions we interviewed had detected issues with full IPv6 compatibility, particularly in CPEs.

4. Another recurring problem in mass services concerns systems and mainly "provisioning," inventory, allocation, CRM, customer care, business intelligence, records and logs, etc. In addition, different interviewees observed they were at different stages of deployment and expressed varying levels of concern.

5. Overall, the consultant notes that the effects of the shortage of IPv4 addresses are starting to be felt and will increase when Phase 3 is triggered.

6. The need for training, mainly on practical issues relating to access networks through workshops with simulators (CMTS, CM, xDSL DSLAM, etc.) was manifested by those ISPs that do not have significant support through multinational operations.

7. At government level, NIC.ar is driving the start of IPv6 deployment in state institutions.

8. As for large ISP:

a. They started preparing for the deployment several years ago and the deployment itself at core level about two or three years ago.

b. For their access networks they have chosen dual-stack with CGNAT, though none of them is providing mass services.

c. The core is fully prepared for IPv6, as are the distribution and access systems and equipment, including the approval of CPE and mobile terminals (UE).

d. At wholesale level they are already providing IPv6 services and have even signed IPv6 peering agreements with other operators.

e. Considering the rapid terminal replacement rate among customers who will naturally migrate to new equipment with Dual, it is expected that the growth of IPv6 access will be much more intense in the mobile network.

f. Initially, growth among fixed customers will be determined by how CPEs are replaced. For the moment, the strategy is to maintain public services in IPv4 with public addresses. In the future it is always possible to use CGNAT and provide public addresses to those who request them because of the applications they typically use.

g. Applications which are affected by CGNAT, such as P2P, PS3 or Netflix, are not essential to the mobile network so CGNAT's negative effects on such applications would be irrelevant. The use of dongles for these applications is not unusual.

2. BOLIVIA

In Bolivia, a meeting was held at the headquarters and with the participation of the Transport and Telecommunications Authority (ATT) in which several ISPs and ISP union officials participated. This meeting was attended by the ATT, AXS, CATELBO, COMTECO, COTAS, COTEL, ENTEL, FECOTEL, NUEVATEL VIVA, and TELECEL TIGO. A meeting was later held with the Deputy Telecommunications Minister and the ATT.

2.1 Success story: Cooperativa de Telecomunicaciones Cochabamba Ltda. (COMTECO)

Cooperativa de Telecomunicaciones of Cochabamba is the operator that has so far driven IPv6 deployment in Bolivia, accounting for the relatively high indicator in this country with regard to users potentially eligible for IPv6. It provides cable television services, mobile telephony through its subsidiary NUEVATEL - VIVA, long distance, broadband, satellite Internet, satellite television and others.

In late 2010, COMTECO made the decision to deploy IPv6 on its network; in 2012, it requested an IPv6 prefix

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

from LACNIC; in 2013, it activated a BGP link using IPv6 with its transit provider and published the prefix 2803:9400::/32. Early tests showed that while edge routers, the DNS, certain modems and other equipment operated on IPv6, this was not the case with AAA.

In parallel, in early 2013 a call for tender was made in order to change the platform's core and this call for tender included IPv6 compatibility. The first tests were conducted in March 2014; customer deployment began on 22 August 2014 using dual-stack.

It is their understanding that they will not need CGNAT until 2017, so this is the only successful case study we observed where an early IPv6 planning and deployment decision was made without yet needing to use CGNAT. This operator has taken equipment replacement and the installation of new network hardware as an opportunity to anticipate future needs, considering that it will only be affected by IPv4 address scarcity beginning in 2017.

By December 2014, 4,000 users were accessing the Internet via IPv6 during peak hours, totaling 300 Mbps of IPv6 traffic.

In October 2015 these values increased to more than 17,000 users and a total traffic of 2 Gbps. By then, 40% of their customers were IPv6-ready.

COMTECO believes that users have not noticed whether they are using IPv4 or IPv6, but greater latency has occasionally been noted in IPv6 websites. The consultant notes that by not using CGNAT the operator is not taking into account the greater delay observed when using this IP sharing equipment.

Currently, as its IPv6 user base grows, COMTECO continues to implement these IPv6 transition tasks: configuring server farm components, DNS, firewalls, anti-spam software and authentication portals.

These actions stem from an early awareness of the need to migrate to IPv6 as well as from the need to replace equipment, which has been purchased considering IPv6 compatibility, particularly CPEs.

The operator found no problems or need for changes in their BSS, partly because it uses a flat rate model.

2.2 Major cooperative providing multiple services

This cooperative provides multiple fixed wired and wireless telephony services, Internet access over copper plant, access over GPON, and convergent services over its hybrid fiber and cable network (HFC), telephony services, satellite Internet and data, television over HFC network and satellite, among others.

They are currently working on a pilot project all the way up to the CPE. Its core is fully IPv6 enabled and they estimate that they will start deployment to their customers in early 2016.

This operator would start providing services simultaneously with three types of access (CM, ADSL and GPON) when its integrated provisioning system for these technologies is ready. Because they did not receive any adequate response from its providers, they decided to design this system themselves.

Although they will have IPv4 addresses at least until 2017, COMTECO also made an early start both in terms of equipment and training. This is why they are not planning to roll out CGNAT until 2017.

2.3 Third Cooperative of the La Paz, Cochabamba and Santa Cruz Axis

This third cooperative is starting to plan its IPv6 deployment and thinking of transitioning its core in 2016. Its CPEs are not yet IPv6-compatible.

2.4 Major nationwide operator including mobile services

Approximately 40% of this operator's CPEs are deployed with dual-stack. Likewise, they are currently in the planning stage for their core network, after which they will continue with their distribution network (BRAS, etc.).

The IPv6 development team working on its mobile operations is different; during the meeting we were told that they are in the process of unifying this team with the one working on fixed access.

This provisioning system has also been developed in house.

This operator has enough IPv4 addresses and is therefore not yet using CGNAT.

Considering the fact that these are recent investments, its FTTH network might reach 80% of its customers over IPv6 in late October 2015 (an estimated total of 95,000).

2.5 Mobile operator also providing fixed services

This operator understands it is running out of IPv4 addresses and expects to begin using CGNAT in 2016, along with the deployment of IPv6 in their fixed operations. Their IPv6 deployment is quite advanced: they have already published IPv6 prefixes (they have a /32 they received from LACNIC) after satisfactory internal testing of the entire infrastructure for GPON and HFC during 2015.

As for fixed network CPEs, most are dual-stack because they are on recently deployed networks. They have 13,000 over 20,000 CM and approximately 1,500 with GPON.

For their mobile operations they are planning a two-stage approach:

1. DS

2. IPv6 only with NAT64/DNS64 or probably 464XLAT

Because they need to renew their entire mobile core network, they are planning to start their deployment in 2017-2018, beginning with dual-stack.

2.6 Mobile operator with the participation of a cooperative

This operator is assessing its entire network and anticipates that its purchases will include an upgrade to IPv6 in 2016-2017.

They are now using CGNAT and are planning to use dual-stack.

2.7 Multi-service operator including wholesale services

This operator has conducted tests on its core network and except for a few minor changes is fully prepared for IPv6. They will begin their first tests on Internet access in 2016 using dual-stack.

They have already completed tests with carriers and dedicated services.

They are planning to deploy CGNAT and estimate that they will run out of IPv4 addresses in 2017.

2.8 Meeting with the Deputy Telecommunications Minister and the ATT

So far, there is no IPv6 policy for public institutions.

The Internet Exchange Point installed at the ATT and to which all major Bolivian carriers are connected is fully prepared to exchange IPv6 traffic.

2.9 Conclusions

1. In general, no IPv4 scarcity issues were observed, so most of the operators we interviewed stated they wouldn't need to use CGNAT until about 2017.

2. COMTECO is the only success story where IPv6 deployment was not motivated by the impending shortage of IPv4 addresses. This operator has taken equipment replacement and the installation of new network hardware as an opportunity to anticipate future needs, considering that it will only be affected by IPv4 address scarcity beginning in 2017. 40% of their customers are IPv6-ready.

3. Another one of the three major cooperatives providing multiple convergent services has made good progress for starting to deploy IPv6 in its three forms of access (CM, ADSL and GPON) by early 2016. Their early work activity in this area even included developing their own integrated provisioning system on all three platforms. In this case there is also no shortage of IPv4 addresses, so they are considering using CGNAT beginning in 2017.

4. A high proportion of a major national operator's CPEs are IPv6-ready (40% in ADSL and 80% in FTTH), but they are working on their core and distribution networks. Intensive deployment is expected once network activities are completed.

5. A mobile operator which provides fixed services has made great progress in terms of IPv6 deployment, as a very high percentage of its CPEs are IPv6-ready.

6. Overall, the three mobile operators anticipate they will begin IPv6 deployment no earlier than 2017.

7. So far, there is no IPv6 policy for public institutions.

8. The Internet Exchange Point installed at the ATT and to which all major Bolivian carriers are connected is fully prepared to exchange IPv6 traffic.

3. COLOMBIA

Activities in Colombia included interviews with the following stakeholders: Information Technology Department of MINTIC and RENATA, as well as ISPs BT, Claro, ETB, IFX, Mercanet, Telefonica, UNE, and Verizon,

3.1 Multi-service operator

This operator provides Internet access services with ADSL, GPON, HFC and mobile technologies. It is owned by a national company and has merged with an international operator with mobile operations in several countries in the region. In the past they provided services with WiMax technology, but these services were discontinued in early 2015.

In their opinion, ADSL CPEs have presented the most problems. In addition, software updates are required for the network's most modern CPEs. In any case, their strategy is to limit ADSL growth and transition to GPON. Other CPEs will need to be replaced. In general

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

they noted the following:

1. They understand CPEs have the most potential for problems during the transition.

2. BRAS have had no issues.

3. The core has been updated to IPv6.

4. They have IPv6 connections to NAP Colombia.

5. DNS is available over IPv6.

6. The corporate site offers IPv6 access.

7. Certain upgrades are still needed in their management systems, and these increase the cost of the transition.

8. They did not report any issues with GPON corporate services with routers, although generally speaking customers don't make intensive use of IPv6 or have any significant IPv6 requirements.

Moreover, as already mentioned when describing other operators in different countries, the consultant notes that software upgrades for internal equipment are often expensive.

In their mobile network they are using CGNAT, so they are able to maintain a stock of IPv4 addresses needed for all their services. They may eventually deploy dual-stack or 464XLAT, but no decision has been made so far. Fixed Internet access services are provided with LTE where there is no wired network available.

They estimate massive IPv6 deployment will begin in late 2016.

3.2 Large multinational operator

This operator began deploying mobile services with CGNAT (but not fixed services) in 2014. This allows them to free addresses from the mobile network (about 1 million addresses) and use them in their fixed network, where they are not using CGNAT due to issues with content and applications.

They have three POPs and use a CGNAT in each region.

As for IPv6 deployment, it is their understanding that 95% of their infrastructure supports IPv6 (excluding CPEs). There is a single, dual-stack ready Internet core for both fixed and mobile access networks

They provide corporate IPv6 services.

For their fixed mass service they are modifying their BSS, where they are finding greater difficulties and hope to have these systems IPv6-ready by mid-2016. In parallel, they are also working on CPEs.

In general, in this case deployment in the mass market is expected to occur in 2016.

3.3 Corporate multinational operator

This operator has its own POPs in Brazil, Colombia and Mexico and co-locates POPs with operators in other countries.

They provide services to multinational clients exclusively over IPv4; none of their customers has asked for IPv6.

The consultant observes that this situation is up to the operators, as in other cases corporate customers with headquarters in Asia or similar request IPv6 termination as part of their corporate strategy.

3.4 RENATA

RENATA is a major player in promoting IPv6 deployment from the point of view of the institutions within its area of influence. Likewise, in 2011 RENATA participated in IPv6 purchasing policies according to MINTIC's Res. 002/11.

Its strategic importance lies in that it supports the Science, Technology and Innovation System's national network, which includes 1,024 institutions throughout Colombia with a total of 4.5 million users: approximately 400 universities with 1.5 million users, museums, libraries and hospitals, among others.

RENATA has opted for a dark fiber backbone, which allows them to configure services independently, even if they are operated by the private sector.

Signed in early October 2015, their 10-year contract with a major Colombian operator includes 19,400 km of fiber, delivered to 22 national nodes and the last miles of 220 centers.

The membership-based services offered by the operator include strategic issues such as IPv6 access to the commercial and academic Internet; collaboration in the deployment of video conferencing, Cloud services, LAN, streaming, and others; training on IPv6 as well as on security and management topics.

They have a dual-stack network with public addresses.

In the consultant's opinion, RENATA's actions represent

a major milestone in IPv6 deployment and the addition of native IPv6 users.

In any case, the consultant feels it is necessary to simultaneously ensure internal deployment within the various institutions, most notably in key places such as firewalls and WiFi networks. There have been cases of university networks where IPv6 reaches a university's edge router, but then IPv6 traffic is stopped by a firewall or WiFi networks are only able to handle IPv4.

3.5 Major regional operator

This operator provides fixed Internet access services in the mass and corporate markets. Their main business is currently based on DSL, but they are evolving towards GPON.

Their core network uses dual-stack and they provide dual-stack IPv6 services to their corporate customers (universities, etc.).

Their strategy is to use the CGNAT in their DSL network, thus freeing addresses for their GPON network which only uses public addresses. In many cases DSL customers migrate to GPON, so there is no reduction of the use of IPv4 addresses. While no formal decision has been made, this operator expects to begin introducing IPv6 in 2 to 2.5 years, initially using NAT64.

In terms of network readiness, its core network, DNS servers and web portals are already dual-stack. The operator is working on its systems, particularly on its provisioning system. CPEs will be replaced by IPv6-compatible equipment as they become obsolete.

The operator noted that, according to their equipment providers, the use of CGNAT use can cause problems in applications for 5% to 10% of their customers, and that in those cases it's necessary to switch these customers to a public IPv4 address.

A major concern which was also brought up in other countries is the need to keep the information regarding users utilizing specific IPv4 address for five years, which to them means an operational cost of USD 1 million per year. In order to comply with applicable legislation, they are in talks so that user information is requested based on their address and port.

3.6 MINTIC

Internally, the Ministry is 92% IPv6-compatible; this year, IPv6 will be available in their access networks and Cloud services using their own prefixes.

The Ministry has issued two guideline documents on IPv6 which might be interpreted as best practices for the region:

1. "Guía de Transición de IPV4 a IPV6 para Colombia" (Guide for the Transition from IPv4 to IPv6 in Colombia)[20]. The goal is dual-stack implementation.

2. "Guía para el Aseguramiento del Protocolo IPV6" (Guide for Securing the IPv6 Protocol)[21].
The Guide for the Transition from IPv4 to IPv6 establishes the following:

"Likewise, in order to meet the technological innovation goals the country requires, the country's institutions must begin the process of transitioning from IPv4 to the new IPv6 protocol following the instructions set forth in Circular 002 by the Ministry of Information and Communication Technologies dated 6 July 2011, which seeks to promote IPv6 adoption in Colombia[22]."

It also establishes the different stages and tasks needed for state institutions to transition to IPv6:

"In order to begin the process of adopting this new protocol, we recommend conducting an inventory of information assets, reviewing existing IT and communications infrastructure, validating all hardware and software components, reviewing all services which are provided, reviewing information systems, standards and policies to determine the impact of the adoption of the new version of the IP protocol with the aim of facilitating the work of planning and implementing the transition from IPv4 to IPv6 and guaranteeing that operations will continue to function normally within state entities.

Likewise, in order to address the country's pressing need for technological innovation, through this instrument MINTIC would like to set forth the guidelines needed to diagnose, raise awareness, develop, and implement the IPv6 protocol in state entities, with the aim of adopting the new technology in parallel with the current IPv4 protocol, in accordance with Circular 002 dated July 2011, guaranteeing that hardware, software, and service infrastructure will continue to operate normally in the country's various institutions.

Finally, the same document will support the accompanying guide plan, which will facilitate the actions needed for the adoption of the new protocol in the country's institutions, beginning with an initial phase of IT infrastructure diagnosis (hardware and software) to a final phase which includes implementing and monitoring the new protocol in the various institutions."

20- http://www.mintic.gov.co/gestionti/615/articles-5482_transicion_IPV4.pdf
21- http://www.mintic.gov.co/gestionti/615/articles-5482_Protocolo_IPV6.pdf
22- Circular 002, 6 July 2011: Transition plan for the adoption of IPv6 in coexistence with IPv4

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

It is a very comprehensive document that includes the details of each transition phase and their deliverables to ensure that the goals are met, as well as the requirements for each phase, technical aspects, training and other elements.

The Guide for Securing the IPv6 Protocol is also a very comprehensive document which covers all aspects relating to local and Cloud-based systems, risk analysis and mitigation, RPKI and others. It states the following:

"This document presents the guidelines and policies which must be considered in order to secure the IPv6 protocol in the Information and Communications Technology infrastructure of State Entities, considering their application throughout the cycle of development phases followed by the new protocol, in a safe and controlled environment that will allow consolidating the process of IPv6 adoption with high levels of security and a highly positive impact on all of the country's organizations."

Its overall goal is stated as follows:

"To present a framework of IPv6 security guidelines that will serve as a reference when addressing the diagnostic plan, the implementation and monitoring plan for the transition from IPv4 to IPv6 in each State Entity; to adopt the IPv6 protocol based on confidentiality, integrity, availability and privacy of information; to create secure mechanisms for accessing IP addresses and the efficient use of the information and communication infrastructure available to the various State agencies."

Together with the previous document, this is a very good framework for a secure transition in all State institutions.

This action obviously includes all aspects of e-government and free WiFi access throughout the country.

3.7 Multinational, multi-service operator

This operator provides of fixed and mobile telephony services, subscription-based television services and Internet access, as well as corporate data center and Cloud services.

Fixed Internet access is provided through multiple HFC networks in different regions of Colombia, using an average of two CMs per customer. Some networks are not yet fully bidirectional.

It has a dual-stack core network and provides corporate dual-stack IPv6 services (currently only to universities) in at least 80% of the country. They've recently received requests for IPv6 services from international corporations.

For residential fixed services, they are upgrading their access network, purchasing IPv6-compatible CM DOCSIS 3.0 CM modems which already account for about a third of their networks. Likewise, they are in the process of upgrading their CMTS and backoffice: they haven't yet upgraded provisioning but other systems such as DNS, website, etc., are already on IPv6. Their strategy would be to use dual-stack with CGNAT. Due to the delays involved in system upgrades, they expect to begin deploying IPv6 in the second half of 2016.

For mobile services they are currently using CGNAT.

3.8 Corporate operator

This small corporate services operator has long been preparing for IPv6. IPv6 requirements come mainly from its multinational customers.

3.9 Large corporate multinational operator

It might migrate to IPv6 through a plan the corporation has at Latin American level. Some customers have already requested IPv6, but no agreements have been signed. In some parts of the network they could provide IPv6 services and already have IPv6 interconnections.

3.10 Small corporate operator

Part of its core already operates on IPv6, yet they have not received any customer requests for IPv6 services.

3.11 Conclusions

1. Two of the main drivers of IPv6 deployment are in advanced stages of planning.

a. MINTIC has developed two essential documents: the Guide for the Transition from IPv4 to IPv6 in Colombia and the Guide for Securing the IPv6 Protocol.

b. RENATA is deploying an extensive network which supports IPv6 and covers 1,200 State institutions: universities, museums, hospitals and others.

2. In general, networks typically show progress in IPv6 deployment in their core and systems. Some aspects still need to be developed, most notably the provisioning systems.

3. Great progress has been made in terms of corporate IPv6 access with dual-stack; no major issues were reported in this area. Customer requirements originate almost exclusively from multinational corporate customers, particularly from those in Asia.

4. There is still no deployment in residential access, mainly due to difficulties with CPEs. In some cases, operators will be able to perform software upgrades; in others, they will need to replace CPEs. A significant proportion of one major provider's CPEs are already IP6-compatible, In no case did we observe IPv6 deployment in access networks.

5. There is broad consensus that mass deployment to customers will begin in 2016, mostly during the the second semester.

6. There is also agreement regarding the high cost of equipment and system upgrades, which are hindering progress.

7. The use of CGNAT in mobile services is widespread, and this may evolve to dual-stack or 464 XLAT. This use of CGNAT allows freeing addresses for fixed access.

8. In fixed networks, no general tendency to use CGNAT has been observed, but there appears to be a tendency towards using dual-stack with CGNAT.

9. One of the operators is using CGNAT on its ADSL network CGNAT, thus freeing addresses for the GPON network which does not use NAT. Although the final decision has not been made, this operator believes they will start deploying IPv6 in about two years using NAT64.

10. A significant part of an HFC network operator's CMs are IPv6-ready, but the same progress has not been made in their CMTS.

11. In general, several operators should begin deploying IPv6 in 2016.

4. CHILE

Three meetings were scheduled with multiple stakeholders. Two meetings were held at the Department of Telecommunications (Subtel), one at the National University Network (REUNA). During the first meeting at SUBTEL we interviewed the head of the department and professionals who were part of his cabinet. The second meeting brought together multiple ISPs, including: Telefonica - Movistar, Claro, ENTEL, GTD, VTR, Torres Unidas and WOM.

4.1 Subsecretaría de Telecomunicaciones (Department of Telecommunications)

The department itself has been received an IPv6 allocation and their internal network is IPv6-enabled.

As to establishing requirements for software, hardware, and connectivity procurements for all State agencies to include IPv6 support, the authority responsible for issuing and enforcing these requirements is currently being defined. The initial reference is to the Office for State Modernization.

Special interest was expressed on this matter and it is believed that relevant provisions will be ready within a reasonable timeframe.

4.2 Meeting with several ISPs held at SUBTEL

This meeting allowed us to gather information from the country's leading ISPs, who also had the chance to share their opinions with their colleagues. The main results are summarized below:

IPv6 interconnection is almost non-existent at national level: until about a year ago, no national connectivity provider was offering IPv6.

In general, it appears that fixed access is not growing significantly as it already exhibited major growth rates in previous years. Thus, IPv4 address exhaustion does not have a significant effect on operators. Overall, they estimate their IPv4 addresses will be enough for the fixed network for about two years.

The largest ISPs (one of them with mostly corporate services) have already deployed IPv6 in their core networks and upgraded their systems. They all noted that they had begun deploying IPv6 4-6 years ago and have been solving issues as they have appeared. All agree that deployment in the core network has presented problems and that their resolution has taken some time, although these problems have not been as complex as those encountered in the access network. They mentioned that Help Desks had to be upgraded in order to respond to inquiries involving customers using IPv6.

One of the major operators noted that, for the time being, high churn rates (meaning that CPEs are lost along with the customers) make it difficult to replace CPEs with others which support IPv6 in order to reduce the CPE-related costs. Their goal is to reduce costs by not installing more expensive CPE. In addition, in this case the introduction of new CPEs requires long approval times to ensure they are compatible with about three dozen cards they have deployed in their access network.

As customers don't perceive any differentiating factor, there will only be intensive IPv6 deployment in access networks after IPv4 address exhaustion.

Two major operators noted they have already started

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

to use CGNAT in their mobile operations. They observed that, although in Chile mobile terminals are often used as hotspots, no issues have been reported as regards content and applications.

4.3 REUNA

REUNA is a network comprising universities, research centers of excellence and international astronomy groups. It provides a communications platform that interconnects scientific, education and national culture institutions and provides them with external connectivity.

REUNA is made up of more than 30 institutions. So far, REUNA covers twelve regions from Arica to Osorno and is hoping to extend its reach to all regions. It is also interconnected to its international peers in Latin America (RedCLARA), North America (Internet2 and Canarie), Europe (GÉANT), Asia (APAN) and Oceania (AARNET). Through this international connection, REUNA is able to expand its opportunities for collaboration with its partners to more than 1,400 institutions in Latin America and more than 40,000 worldwide.

It is an institution of the greatest importance in supporting IPv6 deployment Chile.

Five years ago, they began requiring IPv6 from their connectivity provider. Institutions which do not obtain Internet connectivity from REUNA are also asking their providers for IPv6. As for the network, all routers are dual-stack since 2000, have IPv6 interconnection with Google and international access via IPv6, but they don't yet have national IPv6 access as there is still no Pv6 connectivity with all ISPs. It is estimated that national IPv6 connectivity may be available in less than a year.

In any case, the level of deployment of IPv6-ready equipment within the various interconnected institutions is unclear at this time, regardless of their requirements in terms of connectivity.

In certain institutions which, due to their specialization, lacked the necessary technical human resources, REUNA detected that routers had been replaced with routers managed in the Cloud and using NAT, something which has already been corrected. Meanwhile, the use of broadband had decreased by half, most likely due to session sharing. Such situations shows how important it is for network management to be carried out by the technical teams of centralized university networks, particularly when it evolves towards IPv4-IPv6.

It understands that CORFO (the Corporation for Promoting Production), which has been an important institution for decades and promotes projects for productive development, could encourage IPv6 deployment with its Smart City and the Internet of Things projects (e.g., pilot project for parking in Conception).

4.4 Conclusions

1. In Chile, fixed Internet connections exhibit low growth rates, as a result of which there will be no IPv4 address shortage for at least two years. Mentioned by several ISPs, one possible explanation for this situation is that high growth rates have occurred at times during which there were no IPv4 address availability problems at LACNIC. At present there are no high growth rates, and this means that the IPv4 shortage which exists at regional level is not felt.

2. Overall, there is low IPv6 interconnection at national level, probably due to the same cause mentioned above, as operators work mainly on IPv4.

3. The low rate of users potentially able to access IPv6 should not be seen as an indicator of delay, but rather as an indicator of past years' high Internet connection growth rates, which have currently slowed down.

4. Likewise, SUBTEL also estimates that address requirements will increase in Chile accompanying the development of the Internet of Things. In this sense, there are several initial projects such as one for the parking lots in Concepción run by CORFO.

5. At least two mobile networks have begun using CGNAT.

6. For the moment, fixed networks are not affected by IPv4 scarcity, although most already began preparing their systems for deployment 4-6 years ago.

7. REUNA has adopted provisions for the transition to IPv6, but in most cases has no impact within the interconnected institutions or on Internet connectivity. There is yet no national IPv6 connectivity because not all ISPs are interconnected over this protocol.

5. ECUADOR

In Ecuador, meetings were held with the Ecuadorian Consortium for the Development of Advanced Internet (CEDIA); with AEPROVI, an IXP who then arranged a meeting with multiple stakeholders such as Telecable, Netlife, Cablenet, ARCOTEL (the telecommunications regulator), business entities, CNT and PuntoNet.

5.1 Success story. Corporación Nacional de Telecomunicaciones E.P. (CNT)

CNT adopted the early strategic decision to deploy

IPv6 driven by two agreements of the Ministry of Telecommunications and Information Society in 2011 and 2012[23] for the development of IPv6 networks in Ecuador, and the anticipated shortage in the stock of IPv4 addresses.

CNT also began to experience the significant growth of its fixed Internet access customer base, which placed greater pressure on its stock of IPv4 addresses. As at June 30 2015, CNT had 814,143 accounts for dedicated Internet access[24] and held 57.47% of the market. This growth occurred several times in a few years, which, added to the shortage of IPv4 addresses, contributed to reaching a faster decision for IPv6 deployment on the fixed network.

Deployment in the fixed network involves the use of the dual-stack technique and CGNAT, in line with the decision of practically all operators in the region. At the moment the effort is concentrated on the fixed network, leaving for later the decision regarding the mobile network currently operating in CGNAT. One of the potential problems that requires attention in this mobile network is regarding terminals.

As for corporate customers, we were told that they do not want to move to IPv6.

Deployment in the fixed network had an early start in 2011-2012. The early use of wireless dual-stack CPEs since 2012 is noticeable in this deployment, which due to the high rate of device replacement has resulted in that today there are more dual-stack CPEs than users. This means there has been great progress in access terminals, which will also lead to a significant increase in the number of users as soon as minor deployments are completed in the access network, such as some BRAS. Furthermore, the entire core is dual-stack and causes no issues in terms of systems and other backoffice equipment.

In short, this network is fully prepared for IPv6 with significant progress in the deployment of dual-stack CPEs; therefore, significant progress is expected in the near future with regard to the number of IPv6 accounts. The consultant notes that most of the operators find that CPE deployment costs are one of the obstacles for the rapid increase in the number of fixed IPv6 users. That is why, in general, they decide to move to IPv6 when they replace their equipment. In this case, an early replacement for IPv6 compatible equipment occurred.

Customers have not found any perceptible differences. Deployment was performed carefully through two consecutive pilot plans, solving any problems that arose; today, IPv6 deployment poses no problem at all.

Pilot tests were conducted with services with dual-stack in operation. In cases where some problems with the CPEs were occurred, one of the alternatives was disconnected and a problem was detected which was solved through a software upgrade.

At this time, CNT is working on the improvement of the network management systems for the purpose of obtaining better operational efficiency.

In conclusion, early actions such as taking advantage of the natural replacement cycle to deploy new IPv6-compatible equipment results in a smooth transition without major problems and prepares the network for its evolution as IPv6 content and applications progress, thus gradually reducing the use of IPv4.

5.2 CEDIA (Ecuadorian Consortium for the Development of Advanced Internet)

CEDIA is Ecuador's national research and education network. Its activities include serving as a consultant for MINTEL for the development of public procurement guidelines. As reference, they used RIPE 554[25]. Requirements for IPv6 in ICT Equipment. In any case, the Ministry already issued two agreements (in 2011 and 2012) concerning IPv6 deployment, which have prompted operators and CEDIA to begin working in this direction.

CEDIA has developed an important network to provide academic and commercial Internet access services through two VLANs using public addresses. They understood that, from an academic standpoint, universities could not keep using IPv4. They have an Autonomous System which is 100% IPv6-compatible.

They provide access to 35 universities interconnected through a 1 Gbps ring (expandable to approximately 10 Gbps), with access to universities at 1 Gbps and Red Clara in Guayaquil. TELCONET is responsible for the entire infrastructure and its management. This network was the result of a purchase which required native IPv6 service.

CEDIA estimates that 70% of universities are ready to work on IPv6, though for the time being very few of them actually do. It is expected that when all universities complete their IPv6 deployment plans, mainly in at firewall level, a very significant amount of IPv6 users will be added.

23- 0133-2011 and 007-2012
24- http://www.arcotel.gob.ec/servicio-acceso-internet/
25- https://ripe68.ripe.net/presentations/340-RIPE-554bis.pdf

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

They have a dual-stack Google cache.

5.3 Medium-size residential and corporate operator

They began working on the transition after the ministerial agreements of 2011 and 2012 in order to prepare for future public procurements.

They have a national national MPLS network. They provide IPv6 services to university customers over MPLS and to corporate customers when requested. For their corporate customers they use dual-stack.

For their residential customers they've decided to use DS-Lite, which they have implemented on a pilot network with active customers and have already authorized two different CPE models by different manufacturers. Nevertheless, the final decision to launch has not been made as they are awaiting certain investments in NAT.

They have enabled IPv6 for two of the three access providers and perform IPv6 peering at national level.

For the moment, they have delayed their work on the residential transition and continue working on various aspects relating to the network as well as on their systems and Operation and Maintenance procedures.

5.4 AEPROVI

AEPROVI is Ecuador's IXP and has POPs in Guayaquil and Quito. AEPROVI organized a meeting which was attended by large and small ISPs, as well as by ARCOTEL and other AEPROVI member institutions.

This Ecuadorian IXP is fully equipped for IPv6 using dual-stack. At this time, anyone participating in AEPROVI can establish an IPv6 connection over the same physical connection as IPv4. It provides hosting to the major CDNs such as Google and Akamai, which also provide services over IPv6.

During this meeting a relatively small ISP stated they had only deployed IPv6 at residential level in Quito six months ago (April 2015), using the dual-stack technique. Smaller businesses do not want to deploy IPv6 because of the internal changes which would be needed and don't feel the need for such changes.

An ISP with HFC network is studying which technique they will employ, which will most likely be dual-stack.

5.5 Conclusions

1. CNT E.P. leads IPv6 deployment: all its fixed infrastructure operates in dual-stack mode and a large part of their CPE is dual-stack.

2. As for mobile broadband, deployment has not started and they are using CGNAT.

3. Two ministerial agreements were established in 2011 and 2012 encouraging IPv6 deployment. These agreements served as an initial driver of IPv6 adoption.

4. CEDIA (Ecuador's national research and education network) has procured a ring, access network and interconnection points on IPv6. With few exceptions, IPv6 deployment is somewhat delayed at university level. When they deploy IPv6, they will already have national and international IPv6 access, including the Clara network, based on two commercial and academic VPNs.

5. A medium-size residential ISP has conducted tests on DS-Lite but has not yet decided which technique it will ultimately use.

6. A policy for deployment at public company level is being studied.

6. PANAMA.

Meetings were held with UTN (the National Technological University), AIG (the National Agency for Government Innovation), ASEP (the National Public Services Authority) and ISPs Cable Onda, Cable & Wireless, Claro, Digicel, and Unión Fenosa.

6.1 UTN (National Technological University)

In 2005, they obtained IPv6 prefixes and began implementing IPv6 connectivity through a tunnel. Since then they have been working intensely on internal deployment, including Access Points. The main problem they have encountered is the firewall, a fairly common issue in IPv6 deployment, even for ISPs. At the same time, the Panama IPv6 Working Group was created, a group which includes all stakeholders and resumed its activities two years ago.

The University's actions will undoubtedly serve as a pillar in promoting IPv6 development, as will those of the other stakeholders that are part of the Working Group.

6.2 AIG (National Agency for Government Innovation)

The Agency is involved in the positive development of Internet indicators in Panama, as part of the country's overall position. They are part of the Working Group

on this subject along with ASEP, NIC Panama, the Technological University and others.

One of their actions - one they consider very important - is that they will establish standards so that the more than 100 state institutions will demand IPv6-compatibility in their purchases. They are also developing a circular which will be distributed among all providers advising them of the requirement to include IPv6 in all public procurements.

In addition, they operate Internet for All - a network with public access points used by about 180,000 people - where they will begin deploying IPv6. Finally, they plan to have their own IPv6-based server to provide hosting services to state institutions such as the tourism authority.

6.3 ASEP (National Public Services Authority)

They understand that not only the speed of services should be specified but also whether or not they support IPv6. This appears to be an interesting consideration.

Renewal of RNMS, the national multi-service network operated by AIG should begin in a few months. ASEP believes that, if AIG were to add an IPv6 compatibility requirement to their procurement processes, an important incentive for deployment would be created.

They are part of the Working Group, where there is consensus as to the actions that need to be undertaken, particularly in terms of public procurements and creating awareness.

6.4 Multi-service operator

This operator provides mobile and fixed telephony services, broadband access and subscription-based television services.

Six years ago, they made the strategic decision that all purchased equipment should also support IPv6 (dual-stack with CGNAT). Thus, their core and edge networks began to gradually prepare for IPv6 and are now totally IPv6-ready.

Currently much progress has been made, as they have modified, adapted or replaced their systems. Likewise, training activities are underway and the DNS is being upgraded to IPv6. Wholesale access providers with which they contracted already use IPv6 and they are now planning to move forward with upstream IPv6 interconnections.

As for deployment of IPv6 access, just as other ISPs interviewed in other countries, they will proceed as it becomes necessary to replace obsolete equipment or when clients migrate to fiber access.

In what we consider to be an interesting perspective, they believe that deploying IPv6 in their mobile network will result in savings due to the fact that they will not need to operate "keep alive" packets as when exclusively using NAT. The use of the Radio Access Network (RAN) and firewalls is reduced (approximately 5%) due to the reduction of unwanted traffic.

Generally speaking, the costs involved in the use of NAT are quite high due to the legal requirement to maintain user address and port data records for 24 months, and this represents a significant portion of network costs. They noted that in the US AT&T and Verizon had turned to Congress and succeeded in reducing the period during which these records must be kept to just three months.

6.5 New entrant operator

This operator is part of a company with multiple operations. No corporate plan has been made public, but this is not out of the ordinary. It is expected that this operator will begin the process of deploying IPv6 in the coming months.

6.6 New entrant operator

As to the use of IP addresses, this new entrant provides mobile services. As part of a multinational corporation, their decisions are in line with the provisions adopted for all operations. These decisions might be imminent and it is estimated that deployment will begin in 2016, something already included in the operator's plans for this year. For some time they have been freeing IPv4 addresses through the use of NAT with the aim of progressively moving forward with IPv6 deployment, having reached utilization rates of 40% to 60%.

They will use DS with CGNAT, as observed in other countries throughout the region.

They understand that Panama has a unique customer profile (use of mid- and high-range mobile telephones, intensive use of mobile devices as hotspots to share connectivity via WiFi) and therefore applications used in vehicles or at home are similar to those used by regular fixed access customers (Torrent, Netflix, etc.). Indeed, it is common for a mobile terminal to serve as a dongle, resulting in traffic patters which are unusual for purely mobile users. Confirmed through high consumption rates and download speed requirements, this makes the behavior of mobile customers similar to that of fixed

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

broadband customers using P2P, Netflix, PS and other such applications.

The latter observation shows that, in Panama, the use of CGNAT might result in problems similar to those of fixed terminals, i.e., applications that do not work well with NAT.

6.7 Multi-service operator with HFC network

This operator has made good progress in all aspects of IPv6 deployment using dual-stack with CGNAT. They are finishing the upgrade of their provisioning system, which would be the final limitation before being able to start commercial deployment. The necessary equipment has been replaced, including the CMTS.

A few years ago they restructured the number of public addresses allocated to their customers, which left them with a volume of addresses that allows them to implement the transition phase without any issues.

It is estimated that mass deployment will begin in 2016; meanwhile, IPv6 will be provided at corporate level.

6.8 Wholesale operator

This wholesale operator operates mainly in the dark fiber infrastructure and Layer 2 transport market. For the moment it does not provide Layer 3 services. At corporate level, this operator provides services in Central America up to Guatemala and Colombia.

It has no plans to move to IPv6 and believe that this decision will be made for the entire service region.

It is nevertheless getting ready to offer IPv6 interconnection.

6.9 Conclusions

1. Government institutions such as ASEP, AIG and UNT are aligned in promoting the use of IPv6 through the Working Group, and are also taking appropriate steps in this direction. They are aware of the fact that they are a major driver in promoting awareness of the importance of IPv6 deployment in Panama.

2. Upgrading RNMS, the national multi-service network, can be an opportunity to promote the deployment of IPv6.

3. The entire network of a major multi-service operator is already IPv6-ready, while their various systems are in the final phase of entering commercial operation.

4. An HFC operator is ready to begin deployment shortly.

5. An new entrant believes that the company has plans to begin deployment in 2016 using dual-stack and CGNAT. According th their estimates, in Panama, the use of CGNAT might result in problems similar to those of fixed terminals, i.e., applications that do not work well with NAT.

6. The legal requirement of maintaining records is an important consideration in the case of CGNAT, given that the length of time required by law results in major unavoidable costs and that CGNAT or similar techniques are essential during the transition.

7. ISPs who have already made their decision have adopted dual-stack with CGNAT.

8. In principle, 2016 would be the year of mass IPv6 deployment in Panama. Deployment would occur earlier for those corporate customers who request the new protocol.

7. PERU

Meetings were held ONGEI (Peru's National Office for e-Government), INICTEL (Peru's National Institute for Research and Training in Telecommunications), NAP Peru, the University of San Marcos, and ISPs Bitel, ENTEL, Telefonica del Peru, and Level (3)

7.1 Success story: Telefonica del Peru S.A.

This operators has the region's highest deployment indicators.

Considering the high growth rates and in an attempt to deal with the future exhaustion of IPv4 addresses led mainly by mobile and fixed ADSL services (Speedy) which are experiencing significant natural growth particularly in terms of HFC, starting in 2008 the operator developed a strategy for intensive IPv6 deployment along with a series of awareness-building initiatives which include sessions for companies and institutions considered important for the development and transmission of knowledge, etc. Thus, early awareness of IPv4 exhaustion was the main reason behind the IPv6 transition project. This strategy allowed freeing IPv4 addresses used in ADSL services, which were then used for a smoother transition in other areas.

This deployment made the Peruvian operation the leader of the Telefonica's various operations in the region in terms of IPv6 deployment. The main stages are described below according to the presentation made by the company during the LACNIC 24 LACNOG meeting held in Bogota in 2015.

In 2009, there were alarms regarding IPv4 address exhaustion, thus the need to start using IPv6 by 2012 was duly noted. By that time, other operators such as NTT, Orange and COMCAST had already begun deployment.

At that time Telefonica had about 1.2 million IPv4 addresses and 1.1 million regular customers. At the same time, mobile customers were already using mobile services through CGNAT. Thus, they found it necessary to switch to the use of dual-stack with CGNAT.

As part of this plan, testing began in 2010.

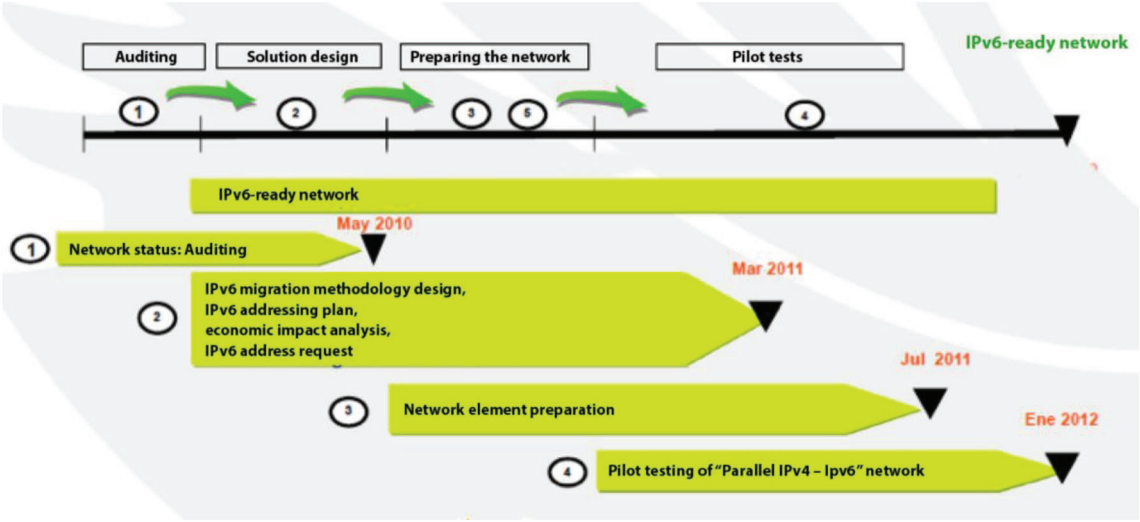
Their strategy can be summarized as follows:

1. Use dual-stack with CGNAT for all future network growth.

2. Maintain high-value customers with public IPv4 addresses.

3. Offer IPv6 services to any content provider requesting such services.

A transition plan was developed which is shown in the image below.



Three main actions were identified:

1. Making sure that CPEs will progressively support dual-stack.

2. Providing dual-stack capabilities at the network's edge (BRAS and GGSN) and in the DNS.

3. Making sure that OSS systems support dual-stack.

The following image shows the different parts of the network, their difficulties and the procedures that must be followed. It is an interesting example of the full fixed and mobile network structure of a horizontally-integrated operator and of the main points and issues on which operators must work. Every part of this network has been individually analyzed based on an inventory conducted at the beginning of the Telefonica transitio process.

At present, Telefonica of Peru has 1.6 million fixed access customers, a figure that far exceeds the number of IPv4 addresses. The situation is as follows:

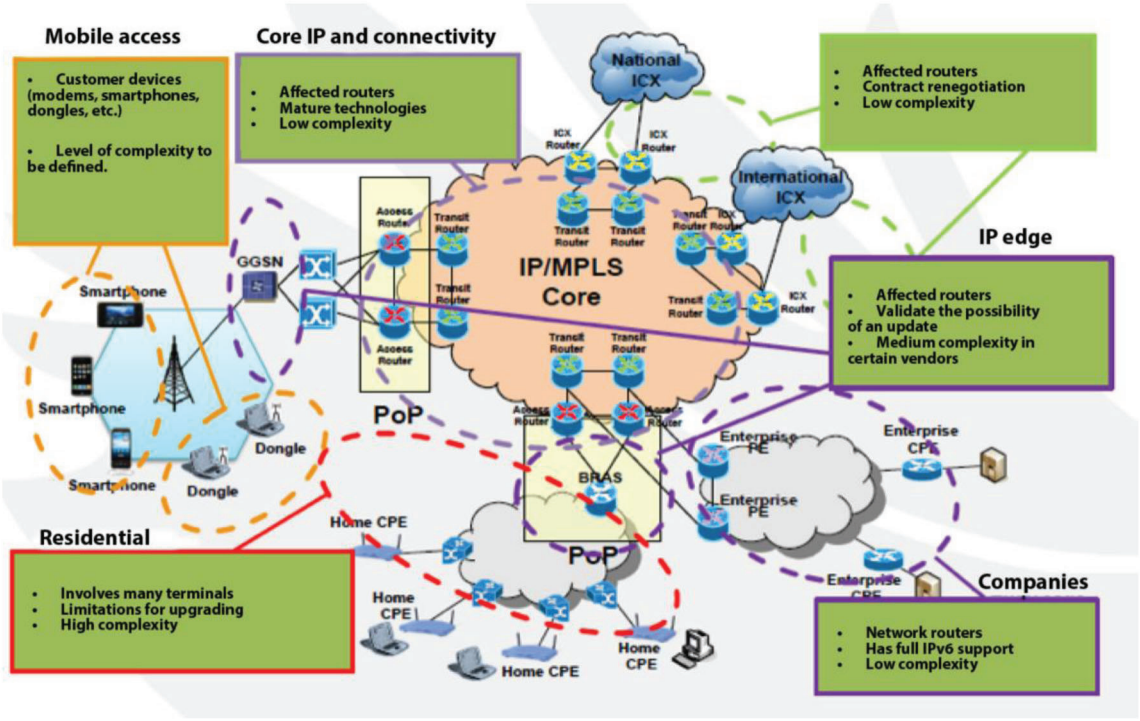
1. 27% of IPv4 addresses are being used through CGNAT, while the remaining 83% are used as public IPv4 addresses.

2. As for the use of public addresses, 20% of these are IPv6 while 80% are IPv4.

It is noted that IPv6 addresses play an important role along with the 27% of IPv4 addresses used with NAT.

The early adoption of measures to mitigate the reduction in the stock of IPv4 addresses has allowed Telefonica to begin deploying IPv6 addresses, thus reducing the pressure on the use of IPv4 addresses, many of which can still be used as public addresses.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222



This allows for a progressive adoption process, free from the pressures exerted by quality issues deriving from high levels of IPv4 address sharing. Moreover, this early adoption has made it possible to deploy the dual-stack network through progressive network upgrades, without requiring investing exclusively for the transition.

The general plan is as follows:

1. IPv6 deployment began in the ADSL network in 2012 using dual-stack, WiFi-enabled CPEs.

2. IPv6 deployment for corporate customers for which the network is ready should begin by 2016, as well as for those using the HFC network.

3. It is estimated that in 2017 deployment will reach mobile services, also using dual-stack with CGNAT.

All service activations are made using dual-stack CPEs and, as seen above, the deployment of CGNAT is progressive, affecting those nodes which require a gradual reduction in the use of public IPv4 addresses.

As for large clients, only universities have requested IPv6; no demand has been observed from corporate customers, not even from those with international connections in Peru.

Due to the early adoption of a transition strategy, internal systems were upgraded progressively as necessary without having to deal with any problems. BSS systems are transparent to the addressing system employed so it was only necessary to update the provisioning systems.

With regard to the HFC system, they are currently working on provisioning and on CM validation. CMTS's have already been validated. Public addresses are being used at the moment, but plans have also been made to use dual-stack with CGNAT in this service.

7.2 NAP Peru

NAP Peru has enabled IPv6; however, of a total of twelve members, only four major operators and one institution are interconnected over IPv6: Level (3), Claro, Telefonica del Peru, Optical IP and RCP (the Peruvian Scientific Network).

7.3 Major corporate-only and wholesale operator

This international operator pointed that only major ISPs are requesting IPv4-IPv6 services, although their network and systems are completely IPv6-ready.

7.4 ONGEI (National Office for e-Government and Information Technologies)

At government level, activities calling for the use of IPv6 began in 2008; hosted at BCP, the interoperation platform among public agencies, opened in 2011.

At this time, ONGEI has drafted a Supreme Decree mandating that all Public Administration agencies must "gradually implement the use of IPv6 in their computer resources, as appropriate and according to each agency's IPv6 migration and implementation plan."

For this, "All hardware or software procurements by public administration agencies making use of the Internet must include native IPv6 and support IPv4." Any exception must be authorized by OBGEI.

The decree also requires preparing a migration plan which must receive prior input from ONGEI.

Most importantly, it states that "ONGEI shall be responsible for preparing an IPv6 Implementation Manual and establish implementation timeframes and goals for the various entities."

Deadlines are established and technical support and training plans are defined for which ONGEI will be responsible.

Once approved, the consultant believes this action will strongly encourage deployment among operators who have not yet deployed IPv6, while at the same time increasing the number of users operating over IPv6.

7.5 New entrant mobile operator

A subsidiary of another Latin American mobile operator, this operator still has enough IPv4 addresses and is considering starting to deploy IPv6 in 2016.

Because a high percentage of its terminals are IPv6-compatible, their current focus is on planning and preliminary actions at network and Business Support System (BSS) level. They have deployed MPLS on their network core and have decided to use 6PE.

7.6 Operator providing corporate services

This operator is currently deploying fiber optic for its corporate clients and is fully operating with dual-stack.

7.7 INICTEL (Peru's National Institute for Research and Training in Telecommunications)

This institute has procured access services from a provider that offers IPv6. Dual-stack is used in all their all classrooms their wireless network is also ready.

The final phase will be the migration of their administrative network.

7.8 New entrant mobile services operator

This operator is in a deployment stage which also includes the installation of 17,000 km of optical fiber across the country, covering half of the districts (950), providing 3G mobile services in more than 17,000 villages, and also considering the possibility of offering mass fixed Internet services in the future. This operator officially started providing services one a year ago and currently has around 1 million mobile customers using 3G and approximately 5,000 using FTTH (schools and corporate customers).

Their entire network is IPv6-ready and their core will operate with 6PE, although they have not yet started providing the service with this protocol, something they expect to do in about two months.

They will use dual-stack with CGNAT.

7.9 Conclusions

1. Telefonica del Peru S.A. has made an early start in preparing for and deploying IPv6, and currently leads the region in terms of IPv6-ready users.

2. A new entrant mobile operator which is deploying an extensive fiber optic network and considering offering mass fixed services in the future (it currently offers services to 5,000 corporate customers and schools) has a fully IPv6-ready network and is considering starting deploying IPv6 to its customers in about two months.

3. Another new entrant mobile operator believes it will begin mass deployment in 2016. A high percentage of its terminals are IPv6-compatible; their current focus is on planning and preliminary actions at network and Business Support System (BSS) level. They have deployed MPLS on their network core and have decided to use 6PE.

4. NAP Peru is IPv6-ready but only 5 of its 12 members are exchanging IPv6 traffic.

5. ONGEI has prepared a draft decree to harmonize all purchases by Public Administration agencies so that they will include IPv6 support.

8. DOMINICAN REPUBLIC

Meetings were held with INDOTEL and OPTIC, as well as with NAP Caribbean, Claro CODETEL, and Wind.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

8.1 Leading operator

The largest operator provides fixed, mobile and subscription-based television services (DTH and cable). Its IPv6 deployment levels vary according to the services provided. Overall, they are currently not experiencing a shortage of IPv4 addresses but have still started working on the migration to IPv6. Decisions concerning the transition technique involve various types of technical difficulties — very similar to other cases — such as a shortage of staff exclusively devoted to studying the issue for their particular network and conflicting signals received regarding the best transition technique which do not show important practical details (e.g., a few providers have recommended waiting and not adopting DS). As in other cases, they understand it would be useful to have access to detailed information or success stories that will allow them to decide on the most appropriate solution.

They are using 6VPE in their backbone and international border links; they also have IPv6 connectivity with content providers. They have purchased CGNAT equipment and are testing 6rd in ADSL accesses; however, while some DSLAMs support this technology, CPEs do not and must be replaced. These tests are consistent with an ISP with no IPv4 exhaustion issues who wishes to begin the transition to IPv6, as they are not aimed at solving IPv4 scarcity issues.

The next step is to work with GPON.

For their mobile network they have deployed LTE with equipment which supports IPv6, but the final decision regarding the transition will be made in 2016. For the moment they are using CGNAT.

In conclusion, this operator is preparing to deploy IPv6 in its networks and internal systems, but a final definition has not been made.

8.2 Smaller operator

A smaller operator was also interviewed which provides dedicated and end-user services using WiMax and more recently deployed LTE and fiber optic. This operator provides subscription-based television services over LMDS, Internet access with TD-LTE (band 41: 2496 - 2690 MHz), voice over IP, as well as corporate and wholesale services. In 2012, they began conducting studies aimed at defining their transition to IPv6. This was both due to a strategic decision an to the fact that they no longer have enough IPv4 addresses to support significant growth. In general, although they have received support from their providers, they have had problems with the techniques they have tested. They have made major progress in IPv6 deployment in their backbone, backhaul, systems, etc.

They are providing dual-stack services to major customers such as universities and government agencies.

Aspects on which they are still working include enabling IPv6 on their DNS, something they expect to complete by October (at the time of the interview they were outsourcing the service).

At this moment they are partially deactivating the WiMax network — which can only support IPv4 — and migrating their customers, spectrum and addresses to the TD-LTE network. Many problems relating to the shortage of IPv4 addresses may appear in this transition process.
They have encountered problems with corporate customers' CPEs and providers are working on these so that they will dual-stack. They have not found any problems with residential customers as their CPEs were purchased less than a year ago for the deployment of LTE and can operate on dual-stack after a simple software version upgrade.

As for their systems, an important issue with CGNAT is responding to legal requirements requesting information about the user holding a given public IPv4 address but without providing further information. They are currently negotiating a solution where, in addition to the IPv4 address, requests would include the port number and perhaps the protocol, or where it would be acceptable to provide only the list of users utilizing that address at the time specified in the request.

As for technical tests, NAT64 testing showed problems with Skype and voice over WhatsApp. When they attempted to conduct tests with MAP, they were told by their CPE providers that they were first focusing their efforts on completing the adaptations needed for dual-stack.

For these reasons, in the end they will likely opt for dual-stack with CGNAT for residential customers, as they are already prepared for this technology; in addition, this is the alternative selected for corporate customers in general, the result of previous agreements and requiring the replacement of CPEs. They noted that, when consulted, with the exception of one in Central America, all other similar Latin American operators replied that they had experienced the same problems and were therefore also planning to adopt dual-stack. The Central American operator is considering working with Skype to fix the problem.

Another problem they found is that end-user equipment (computers) sometimes run operating systems which do not support IPv6, such as XP or earlier versions of OS X, and would therefore continue using IPv4 despite CPE migration.

In conclusion, they are already migrating corporate and wholesale customers to IPv6 with 6VPE and providing new CPEs, they will maintain WiMax customers on IPv4 due to network equipment incompatibilities, and they will migrate LTE customers to IPv6, probably using dual-stack, a technique for which they are prepared.

8.3 OPTIC

OPTIC — the Presidential Office for Information and Communications Technology — is charged with planning, overseeing, and executing the actions needed to implement e-government in the Dominican Republic, disseminating and using Information and Communications Technology (ICT).

OPTIC has no power to mandate State institutions to use and deploy IPv6. Nevertheless, they have taken the initiative to establish a set of best practices for government procurements, including the adoption of IPv6. In addition, if applicable, OPTIC grants a certificate of compliance with these best practices. While no data is available, it is believed that many institutions are adopting IPv6 when making new purchases.

According to a survey conducted by INDOTEL, these actions began in 2014.

8.4 INDOTEL

INDOTEL has decided to urge IPv6 deployment in the Dominican Republic through Resolution No. 021/15 dated July 2015.

Based on a diagnostic report on the level of IPv6 readiness of Dominican government institutions, this resolution establishes the following: "URGE telecommunications service providers to implement and offer IPv6 in all its various technologies for both fixed and mobile networks, high-end corporate and residential user technologies, in order to meet the demands of their customers and new users."

In addition, through this resolution INDOTEL assumes responsibility for implementing actions that will promote the use of IPv6.

It states the need for a meeting of the interested parties to acknowledge the report they produced and to "INSTRUCT the Executive Director that, in coordination with the Technical Team working on IPv6 and INDOTEL's Communications Department, he must develop and disseminate information and promotional materials on the importance of IPv6 deployment for the security and stability of the country's network infrastructure."

To comply with the resolution, INDOTEL has prepared a work plan ending in December 2015.

The diagnostic report on the level of IPv6 readiness of Dominican government institutions was based primarily on the results of a survey conducted among 66 institutions, 53 of which replied to 24 questions during a period from May to June 2015.

Relevant data presented in this diagnostic report include:

1. While they all replied that they are aware of the issue and linked it to IPv4 exhaustion, 87% of institutions do not have staff trained in IPv6.

2. As for the presence of IPv6 in their institution, 87% replied they have none, 9% replied they were only using IPv6 for testing purposes, and only 2% replied they were only using IPv6 to connect to the Internet or in internal networks.

3. 87% have no plans for transitioning to IPv6 technology.

4. As for requesting IPv6 address blocks, 75% has no plans to request an IPv6 block, while only 13% do.

5. 57% of institutions have not considered including IPv6 in its network design. 43% have considered including IPv6 but have not started to do so.

6. 70% have recently purchased software that supports IPv6.

The next steps INDOTEL is adopting are the direct result of the conclusions and recommendations contained in section 6 of the report, originally focusing on State institutions. These include:

1. Based on the data included in the diagnostic report and the reality described in the introduction, they believe they are facing "a major event, such that IPv6 deployment is now more pressing than ever and has become inevitable and urgent."

2. "Plans must be promoted for building awareness, providing technical training, and offering consulting services for the adoption of the Internet Protocol in State institutions in order to drive the country forward, the State serving as the catalyst for this deployment."

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

3. "Hold a meeting with State institutions and the country's various sectors, or create meeting places that will allow presenting the results of this report. All this in order to motivate and transmit the implications of not deploying the Protocol, thus promoting widespread use of Internet and achieving IPv6 adoption in the Dominican Republic in the shortest time possible."

4. "The State should lead IPv6 adoption in government networks."

5. "Propose that when State institutions procure or purchase new technological products which use the IP protocol, IPv6-compatibility should be a major requirement so that such investments do not need to be reconsidered in the near future."

6. "Prepare promotion and dissemination plans."

7. "Urge telecommunications service providers to start offering IPv6 to satisfy the demand of its customers and new users."

8. "Conduct training workshops and provide general consulting services aimed at IPv6 adoption and reducing resistance to change."

9. "After the training workshops, specify a deadline for government agencies to include a "Transition Plan for the Adoption of IPv6 in Coexistence with IPv4" in their administrations, a plan that will allow a safe transition and ensure the effectiveness of the tasks to be performed during IPv6 deployment."

To summarize, INDOTEL is adopting a work plan that includes the following main areas: creating a sense of urgency, developing training and awareness building actions, working jointly with all stakeholders, and promoting IPv6 deployment within government institutions in agreement with OPTIC. These areas are in line with best practices for government actions aimed at IPv6 deployment.

8.5 NAP Caribbean

This NAP provides multiple services in the Dominican Republic: international connectivity (through national wholesaler providers), IXP, hosting, collocation, virtual machines and other typical NAP services.

The IXP platform supports IPv6 but no providers have expressed interest in interconnecting over this protocol. The NAP itself requires just a few upgrades to be able to provide services over IPv6.

The lack of available IPv4 addresses poses the need to deploy IPv6, and the most viable option would be by deploying dual-stack. So far, they have not considered the use of NAT64.

They believe that the government initiative to promote IPv6 is an important mechanism that will kickstart IPv6 deployment in the country.

8.6 Conclusions

1. INDOTEL is adopting an important work plan that includes the following main areas: creating a sense of urgency, developing training and awareness-building actions, working jointly with all stakeholders, and promoting IPv6 deployment within government institutions in agreement with OPTIC. These areas are in line with best practices for government actions aimed at IPv6 deployment.

2. OPTIC has no power to mandate IPv6 deployment in State institutions. Nevertheless, they have taken the initiative to establish a set of best practices for government procurements, including the adoption of IPv6. In addition, if applicable, OPTIC grants a certificate of compliance with these best practices.

3. Thanks to preventative measures implemented taken long ago, the largest operator has no pressing need for IPv4 addresses. They are using 6VPE in their backbone and international border links; they have IPv6 connectivity with content providers. For the moment, they are using CGNAT. It is expected that the corporate decision to begin IPv6 deployment will be made in 2016.

4. A smaller WiMax operator is migrating to TD-LTE. This operator began conducting studies aimed at defining their transition to IPv6 in 2012, both due to a strategic decision an to the fact that they no longer have enough IPv4 addresses. They are providing dual-stack services with 6VPE to major customers such as universities and government agencies. The operator will likely opt for dual-stack with CGNAT for residential customers as they are already prepared for this technology; in addition, this is the alternative selected for corporate customers in general, the result of previous agreements and requiring the replacement of CPEs.

9. TRINIDAD AND TOBAGO

Meetings were held with several ISPs providing Internet access: TSTT (Blink and Bmobile, fixed and mobile services), Columbus Communications (Flow, fixed HFC services), Digicel (mobile and fixed fiber services, Open Telecom (wireless residential and corporate access), LISA Communications (corporate), and TTIX (an IXP). Meetings were also held with the regulator (TATT)

and the Ministry of Public Administration, the agency responsible for ICTs. As to academia, meetings were held with the University of the West Indies (UWI), Trinidad and Tobago Research & Education Network (TTRENT), and the University of Trinidad and Tobago (UTT).
The two major operators already host Google caches in their networks but it is not known whether they are IPv6-enabled.

9.1 Main operator

The main operator is not providing or planning to provide IPv6 services to residential customers in the near future because, as they explained, at the moment they have enough IPv4 addresses. For now, they are simply planning to perform IPv6 related updates to their core network. The consultant believes that this strategy is consistent with an economic vision.

9.2 Wireless residential and corporate access provider

This wireless access provider does not currently offer services over IPv6.

9.3 Mobile and FTTH operator

The mobile and FTTH operator has recently started deploying IPv6 in its access network for 1,000 fixed network customers and was hoping to have an important degree of development by 2015, along with FTTB. It should be noted that its new network has been IPv6-ready since it was installed. Its entire core is operating in IPv6 and it is currently working on their mobile deployment, which is expected to begin in early 2016. For FTTH, the operator is using dual-stack with CGNAT. For mobile services, it has not decided which technique it will use but will possibly use dual-stack for initial tests. The operator noted it had encountered problems with terminals, something also reported by other operators. For the moment they are nor providing corporate IPv6 services over IPv6.

9.4 HFC operator

The operator which uses an HFC network has a dual-stack core and has implemented CGNAT in certain areas. It is ready to provide corporate services over its cable network, but still not ready to do so for residential customers. Its cable modems are DOCSIS 2.0 and 3.0, so the consultant believes that part of these should be IPv6-ready. It provides IPv6 transit services.

It is planning to deploy IPv6 for residential customers in 2016. This operator has the advantage of having a centralized provisioning system for several islands (Trinidad, Curacao, Granada, etc.), so Trinidad's system will be ready when the islands' are.

9.5 Operator only providing corporate services

In this case, the operator has enough IPv4 addresses and is therefore not planning to deploy IPv6.

9.6 TTIX

This meeting was quite a highlight thanks to the overview of Trinidad and Tobago's market and the trends observed regarding IPv6. The comments received reinforce the opinions received in our meetings with the ISPs.

It was noted that there is bilateral peering at the IXP, which is discussing entering IPv6 peering agreements. Increased IPv6 traffic is also expected. Despite having autonomous systems, neither of the two universities (UTT and UWI) is connected to the IXP because of the cost of the necessary links. Traffic is exchanged through their ISPs. They believe universities will begin working on IPv6 as soon as the ISPs beging offering the service. For instance, UTT obtains Internet access from two providers, ensuring that at least one of them will be able to provide IPv6 service. There is no mass international traffic exchange at the IXP.

Google, Akamai and Netflix have installed servers in the country.

9.7 TATT

It is believed that when the new policy regarding public sector investments is defined there will be an opportunity to include guidelines for deploying IPv6 in State institutions as investments are made.

9.8 Ministry of Public Administration (formerly, Ministry of Science and Technology)

GobNETT connects all government sites and may have approximately 15,000 users. While tenders consider IPv6 deployment, at the moment there is no special emphasis on the IPv6 protocol. GobNETT is currently using NAT.

Today, no guidelines exist for government procurements. iGovTT is reviewing a set of guidelines, but none have been approved.

9.9 University of West Indies

They have been working on IPv6 since 2009. They have done laboratory work with IPv6 in relation to their academic activity.

As for IPv6-readiness, all their wireless points of access are IPv4. The consultant notes that this is a recurring problem in university environments, and represents a limitation on the actual use of IPv6 even when the service reaches the institution.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

This university is using dual-stack and all their equipment except the firewall is IPv6-ready. They are waiting for the ISP to offer IPv6 services before updating their firewall. An aspect worth noting is that so far they have had no additional costs, as their equipment purchases have requested IPV6 compatibility.

At the moment they are waiting for ISPs to provide IPv6 services. Meanwhile, they are using a connection through Miami which supports IPv6 - most of their contents use this route.

Assuming an upgrade of their hotspots, their transition to IPv6 would reach 17,000 students and 3,000 teachers.

9.10 Trinidad and Tobago Research and Education Network (TTRENT)

TTRENT provides connectivity to certain universities, which are responsible for their own networks. They are connected to UWI, UTT, COSTTAAT and USC, and have external connections through GEANT and RedCLARA.

They are working on a project called EDUROAM for students to have wireless access wherever they go.

It is estimated that the total average number of users in all institutions employing TTRENT is 50,000 to 60,000. It is believed that the new government might integrate TRENTT and the tertiary education portfolio within the Ministry of Education (primary and secondary). This would mean that any measures adopted aimed at deploying IPv6 in education would have a much greater impact on national indicators.

9.11 University of Trinidad and Tobago

This University has included the study of IPv6 in its curriculum, but only technical aspects are covered, not the consequences of IPv6 adoption (or lack of adoption) on the Internet and on society in general. The importance of this deployment is not perceived, an issue that must be considered. We are unaware of the existence of student projects in this sense. Education in this area is important, as students will later work at various ISPs, government institutions, etc.

9.12 Conclusions

1. The situation is different for different ISPs. The major ISP has a large stock of IPv4 addresses and does not feel the need to deploy IPv6.

2. -The mobile and FTTH/FTTB operator has made much progress: approximately 1,000 of their customers are connected to their fixed network via IPv6 and they anticipate even greater deployment towards the end of the year. They use dual-stack with CGNAT.

3. The HFC operator already has a dual-stack core and has implemented CGNAT in certain areas.

4. As for mobile services, this operator is in the initial stages of deployment with a dual-stack core and expecting to begin providing IPv6 services in early 2016. It already has DOCSIS 2.0 and 3.0 CPE, so they expect to begin deploying IPv6 in mid-2016.

5. The IXP has not yet entered into any IPv6 peering agreement.

6. A policy for IPv6 deployment has not been defined at government level, although progress has been made in this sense.

7. At university level, UWI has made progress except in their hotspots and firewall, two important aspects.

8. Due to the impact that university graduates have on society, it is important for courses to be available that not only deal with the technical aspects of IPv6,

10. VENEZUELA

Meetings were held in Venezuela with CONATEL and CNTI, as well as with ISPs CANTV Movilnet, Digitel and Telefonica.

10.1 CNTI

The National Center for Information Technology (CNTI) is a State institution under the Ministry of the People's Power for Higher Education, Science and Technology (MPPEUCT), dedicated to the promotion of open information technologies in Venezuela's Public Administration. The Center strengthens e-government, supports public institutions in the training of its staff, and encourages and promotes policies for updating technology within the Venezuelan State.

It provides connectivity to fifty universities and serves more than three hundred. CANTV provides their IPv4 and IPv6 connectivity to the router at the university and is responsible for operating and maintaining their networks. They work with the CLARA network and Internet 2 in the USA.

Between 2004 and 2007 there was a lot of work on IPv6 and guidelines were developed jointly with the Ministry of the People's Power for Science and Technology. CONATEL has developed courses and worked with the community.

10.2 CONATEL

CONATEL is currently considering developing a draft public policy aimed at deploying IPv6 in government institutions. The country's current economic situation makes it difficult to implement this type of policy.

In Venezuela there is no requirement to provide information on users who use a specific IP address.

10.3 Major multi-service operator (fixed and mobile ISP)

This operator is in the early planning stages of IPv6 deployment, focusing mainly on their backbone as they want to take advantage of the fact that a network upgrade is needed. Although they have sufficient IPv4 addresses, given the importance of this deployment, they are alerady working on their backbone and will continue in other areas.

10.4 Mobile telephony and corporate services operator.

Case 1

For mobile services, one of the alternative they are considering is dual-stack with CGNAT; the other might be XLAT where the HLR records whether the terminal supports XLAT and, if so, offers this technique. However, a final decision has not been made due to the difficulties posed by the latter option due to the fact that it is not automatic.

Mobile operations are the first to be considered for the transition to IPv6, although they believe this will take some time. For now, they are using CGNAT, a technology with which they have encountered problems when translations are stopped as, in order to restart them, administrative packets must be sent in both directions using the signaling channels, which creates traffic that affects operation. They are expanding their CGNAT.

The core, DNS, billing systems and other infrastructure are expected to be IPv6-ready in late 2015. No problems are anticipated.

As far as terminals, they are beginning to conduct tests and anticipate they will find problems con the equipment they purchase.

They have received very few requests for IPv6 at the corporate level and are considering working on this issue after completing their work on the mobile network.

10.5 Mobile telephony and corporate services operator

Case 2

This operator is part of a multinational company which has been planning and advancing towards IPv6 deployment since 2008.

They have been using NAT for two years and they will employ dual-stack with CGNAT. The use of NAT is considered beneficial, as it avoids incoming flows, device push does not work, and other aspects which have improved customer use of broadband packets due to their lower consumption. The NATs they employ prioritize applications which need more sessions.

At the moment, the only problem they need to solve in order to be able to launch the service is upgrading their appraisal system, which does not support IPv6. This requires a significant investment which they are unable to make at this time due to issues external to the company. In the past four years they purchased IPv6-compatible equipment whenever they performed network or system upgrades.

As a result of their socioeconomic profile, their customers use IPv6-ready smartphones.

As for corporate clients, they have no problem provide these services over IPv6.

10.6 Conclusions

1. CONATEL is aware of the importance of publishing guidelines for the public sector.

2. The main operator is in the early stages of planning IPv6 deployment in its backbone.

3. Other major operators have made much progress and have only encountered minor problems they had to solve in order to begin mass mobile deployment.

4. There are not problems for corporate deployment.

5. The country's economic difficulties are hindering IPv6 deployment.

6. Smaller operators will use the dual-stack technique with CGNAT.

11. AKAMAI

Akamai is an important content distribution network with presence in over 110 countries with 200,000 servers on 1,400 networks. In late 2015, Akamai deployed servers that provide IPv6 services in 95 countries.

During this transition period, one of the main challenges they found was that, even when they are using IPv6 servers, many datacenters providing hosting services to Akamai do not provide IPv6 connectivity that can

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

be accessed by users who are already prepared. This observation reinforces the situation found in other countries in the sense that network cores are not fully IPv6-ready. In this case, users can still access contents provided by Akamai over IPv6, but they must do so from more distant servers, or, because of the protocols in the users' computer, even if they are IPv6-ready, they end up downloading these contents locally over IPv4 as the most efficient choice. This situation is currently observed in Asia and Latin America.

Their main customers typically offer services using dual-stack, so that IPv6 access is possible, either via their own servers or via Akamai's. The case may exist where, for example, a news channel provides access to content subject to frequent changes (such as text) through own sites, and delivers content which changes less frequently (photos and videos) via Akamai's servers. Likewise, if a customer maintains IPv4-only servers, users can reach their contents over either IPv4 or over IPv6, depending on whether a specific content is hosted on their own servers or on those of Akamai, which are IPv6-compatible.

Another aspect worth noting is the need to implement - gradually but as quickly as possible - IPv6 peering and interconnection networks at least similar to those currently operating with IPv4. This will allow IPv6 and IPv4 content to to compete on an even playing field. It is noted that, because the level of IPv6 connectivity varies at national or regional level, access to IPv4 content might be prioritized.

This peering-related issue adds to those which have already been accepted as favoring IPv4 access over IPv6 content (e.g., happy eyeball, CPE configuration, etc.).

12. GOOGLE

For obvious reasons of confidentiality, the information provided was not very detailed, yet it revealed some relevant issues.

The transfer of address blocks as a result of sales on the secondary market creates geolocalization problems, which are partly corrected with additional user location information (e.g., WiFi hotspots).

As already mentioned, CGNAT also complicates their operation due to the number of sessions, as a single public address might be being used in very different geographic locations, which also causes geolocalization problems.

Casa de Internet
de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

ANNEX II. BEST PRACTICES FOR TRANSITIONING TO AN IPV6 NETWORK

1. GENERAL ASPECTS

The transition from an IPv4 network to an IPv6 network can be achieved in three basic ways:

1. Dual Stack, where both protocols coexist and operate simultaneously across the network and user devices. This technique may use public IPv4 addresses (if there are enough of these available) or it may be combined with CGNAT.

2. Tunneling. Two IPv6 networks can communicate using tunnels to span an IPv4 network. These technologies have now practically been abandoned due to their cost, their disruption of basic Internet principles such as end-to-end connectivity, problems with the lists of blocked addresses, the need to keep records of addresses and ports, etc.

3. Translation. This is a set of techniques that allow IPv6 devices to communicate with IPv4 devices, without tunneling over IPv4 networks. Translators translate IPv6 packets into IPv4 packets and vice versa, applying both address and port translation. NAT444 is not considered in this section, as the use of this technique is not recommended because it tends to maintain a dependency on IPv4 addresses without requiring the use of IPv6. This means that it is not specifically a transition technique.

2. BRIEF DESCRIPTION OF THE DIFFERENT IPV6 TRANSITION TECHNIQUES

This brief description of IPv6 transition techniques is based on a book published by the ISOC Argentina Chapter, which may be consulted for further information[26].

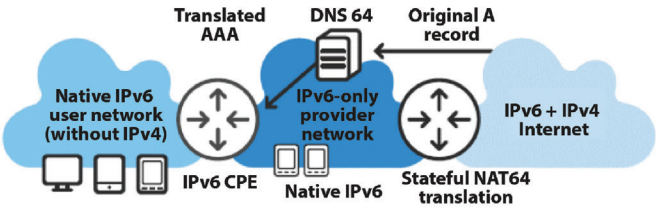
New transition techniques will be analyzed, disregarding techniques based on tunneling which have practically been abandoned.

1. NAT64/DNS64
2. 464XLAT
3. DS-Lite
4. MAP-T
5. MAP-E
6. Dual-Stack
7. 6PE/6VPE

2.1 NAT64/DNS64

NAT64[27] is a stateful technique for translating IPv6 packets and ports to IPv4. It allows sharing IPv4 addresses. DNS64 is an auxiliary NAT64 technique that allows mapping names.

Both techniques allow native IPv6 users - even those who can only receive IPv6 addresses from their ISP - to see all Internet services and websites as if they were IPv6 and to access the IPv4 world without any problems at all. Of course, they allow direct access to the IPv6 world. In turn, an Internet user employing this technique to access the IPv4 Internet appears to be employing a shared IPv4 address to connect to IPv4 Internet services and websites. This technique is used as follows:



The basic principle behind its operation is that IPv4 addresses are mapped to a /96 IPv6 prefix on the provider's network. While any of the provider's blocks may be used, there is a block specifically reserved for this purpose (64:ff9b::/96)[28]. IPv4 address 203.0.113.1 is translated into 64:ff9b::203.0.113.1.

The network function that complements NAT64 is DNS64. When a user must access an Internet resource, it queries the DNS in the usual way; however, in this particular case, the queried DNS is a DNS64. This DNS64 acts as a normal recursive DNS server but if the queried name does not have an AAAA record (i.e., if it does not return an IPv6 address), it sends a synthetic response to the user as if the queried name indeed had an AAAA record and returns an IPv6 address for the resource built by applying the rule described above for IPv4 - IPv6 mapping. Once this synthesized address is received, a network request is made with that destination address. This request is routed through the NAT64 device, which performs the stateful translation to and from IPv4. The source address of the packet which continues on the IPv4 network is an IPv4 address which is part of the provider's pool. The response follows the reverse path.

26- "IPv6 para Operadores de Red" 1st Edition. 2014, Ebook, ISBN 978-987-45725-0-9. ISOC – Ar, Asociación Civil de Ingenieros Argentinos en Internet. This is also the source of the images used in this report.
27- Described together with DNS64 in RFCs 5146 and 6147.
28- Described in RFC 6052.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

This technique can be classified as CGNAT, although it has the advantage of performing a single translation and incorporating a provider's IPv6 transport network, while being able to serve native IPv6 users without using IPv4 addresses. There is also the need to keep track of source ports in order to identify users who have accessed resources with shared IPv4 addresses, and this increases network core costs and complexity and breaks end-to-end connectivity.

One problem is that it does not work well for applications that need IPv4 addresses to function properly. An example of this is the requirement Apple recently imposed for applications to access the Apple Store through its iOS9, where it requires that applications must be able to operate in an IPv6-only environment. Furthermore, this technique has the advantage that, because all users are native IPv6 users with no IPv4 assignments, when the network makes the full transition to IPv6, this transition will be transparent to these users. In other transition techniques, because users have IPv4 and IPv6 addresses, there is always the possibility they will continue to use IPv4 even when this is not necessary.

An important aspect of this technique is that it is very suitable for mobile services, as it makes all users connect via IPv6 only while allowing them to access IPv4 services.

However, the problem of applications which run on IPv4 only remains. This refers to the fact that certain applications have hardcoded IPv4 sockets but encounter interfaces which only offer IPv6, or use literal IPv4 addresses without using DNS, as in the case of Skype and Spotify. In these cases, the applications will not work behind a DNS64/NAT64.

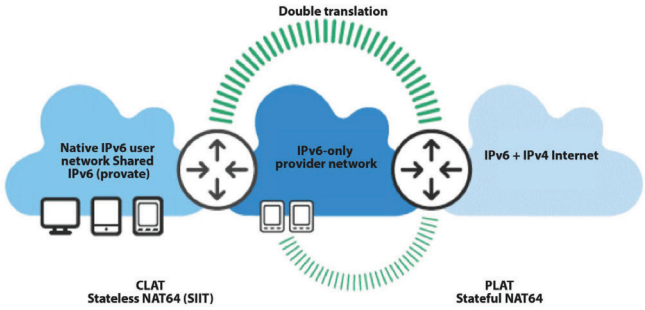
This is the reason why the 464XLAT technique was developed.

2.2 464XLAT

This technique[29] complements NAT64. It is a combination of a stateful IPv6-IPv4 translation similar to the NAT64 technique described above, well known and deployed in the provider's network core, and, according to RFC 6146, a stateless translation known as SIIT (Stateless IP/ICMP Translation Algorithm)[30]. This is a simple and scalable technique that allows users to have IPv4 on an IPv6 network.

It was developed to allow operating applications which are still IPv4-only and do not support IPv6. The second stateless translation allows providing a private IPv4 address so that the user can operate with those applications.

This second translation allows assigning users both types of addresses, and can be introduced in the network or in the user's device without disturbing the rest of the existing network which is already using NAT64.



Because they are native IPv6, users can operate transparently in this protocol. If the desired resource or application does not operate on IPv6, the user then moves on to a double translation. The CLAT learns the prefix used by the PLAT and something similar to an IPv4 tunnel is established on the IPv6 network. This is why this technique does not use DNS64.

It is used mainly by mobile operators when applications do not allow the use of NAT64/DNS64. It is also a form of CGNAT. According to an ARIN[31] report updated in June 2015, some mobile devices already include CLAT (464XLAT). The report specifies that Android 4.4 and Windows Phone 8.1 support NAT64 CLAT according to RFC 6877. In June, it was announced at Apple WWDC 2015 that iOS9 would support DNS64/NAT64 "IPv6 only" network services. It was also announced that apps published on the Apple Store must support DNS64/NAT64 begginng in the early months of 2016.

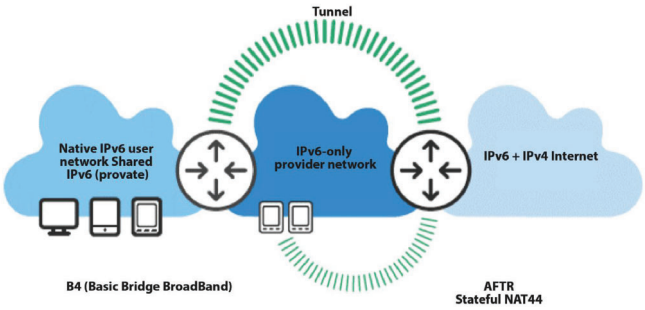
While this technique is well suited for mobile services, during the interviews and in the survey it was mentioned that the region has a preference for dual-stack.

2.3 DS-Lite

The Dual Stack Lite[32] technique solves the problems of applications which only operate on IPv4 in a manner similar to the 464XLAT technique, except that, instead of a double translation, it uses a tunnel that encapsulates IPv4 over IPv6. In this case too, users can communicate natively over IPv6 while also receiving a private IPv4 address.

29- XLAT is short for Translator. Described in RFC 6877.
30- Described in RFC 6145.
31- https://getipv6.info/display/IPv6/3GPP+Mobile+Networks
32- Described in RFC 6233.

It is also a form of CGNAT, as it requires a Stateful NAT44 at the provider's network core. The device that provides the NAT44 is called AFTR (Address Family Transition Router). On the user's side, the CPE is called B4 (Basic Bridge BroadBand) and operates as a bridge for IPv4 on the tunnel termination.



By combining the function of the NAT44 with the bridge on the CPE, NAT44 directly connects the users' port as if it were a user-controlled NAT.

This technique shares the disadvantages of using NAT: it is necessary to keep a record of ports and addresses and this increases costs, there is no end-to-end connectivity, etc.

The use of this technique is recommended for general Internet access providers.

2.4 MAP

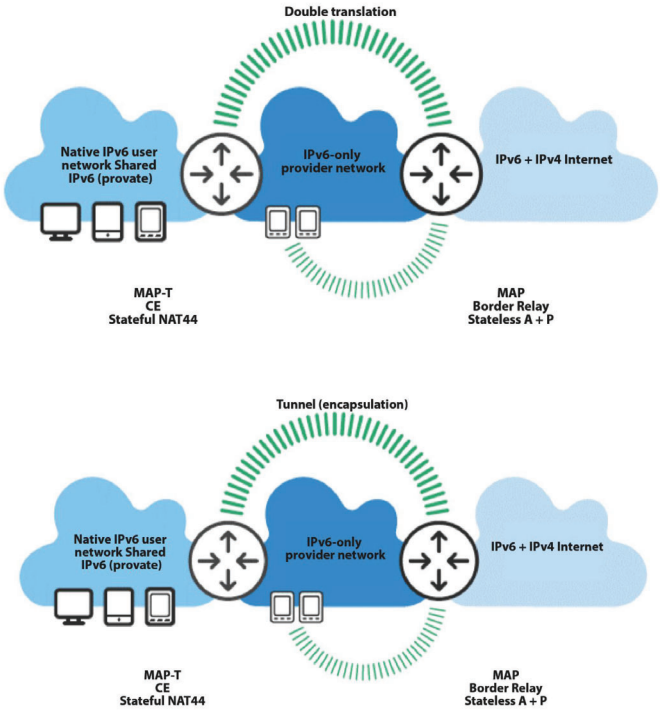
From the user's point of view, this technique is very similar to DS-Lite and 464XLAT. Two versions exist and their corresponding RFCs were published in July 2015: la MAP-T and MAP-E (Mapping of Address and Port using Translation and Encapsulation).

In these cases, the user is also connected natively via IPv6 and using private IPv4 addresses.

MAP-T performs a translation between IPv4 and IPv6 in a manner similar to the 464XLAT technique. MAP-E uses an IPv4 over IPv6 tunnel in a manner similar to DS-Lite.

In both cases, the router responsible for sharing IPv4 addresses is known as a MAP Border Relay. On the user's side, the CPE is known as a MAP CE. Both implement stateful NAT44.

The main difference with the other techniques is that it is not CGNAT, as it does not use NAT in the access provider's core network. The shared use of IPv4



addresses is implemented through the technique known as A+P (Address plus Port)[34]. A+P allows stateless IPv4 address sharing: although one valid IPv4 address is assigned to multiple independent users, each user is also assigned a certain range of ports. Each CPE is then responsible for establishing a stateful NAT44 where end users are assigned private addresses, without them being aware of the ports limitations.

On the provider's side, the A+P translation is performed using an algorithm and therefore this solution is less resource-intensive, cheaper and more scalable than the NAT44.

It is the technique with fewer operational issues for both the supplier and the users, so it is recommended for access providers.

2.5 Dual-Stack

This technique requires that the devices connected to the network and the network itself run both IPv4 and IPv6 protocol stacks in parallel. Thus, all network nodes must have implemented both protocols and be able to access both types of networks. If both endpoints of the communication support IPv6, they will communicate using this protocol; however, if either endpoint only supports IPv4, communication will be established over IPv4. Generally speaking, in each case the protocol will be chosen according to the network administrator's policy.

34- Described in RFC 6346.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

As the results of the interviews conducted as part of this research show, this technique is the most popular choice in countries of the LAC region.

2.6 6PE/6VPE

These techniques[35] operate on an MPLS network without altering it - a great advantage to those who use it; in turn, this network is implemented overIPv4. There is still no MPLS over IPv6. Because of the reasons above, these transition technologies are recommended for operators who have MPLS in their core network. They are mature technologies supported by major equipment vendors and widely used throughout the region.

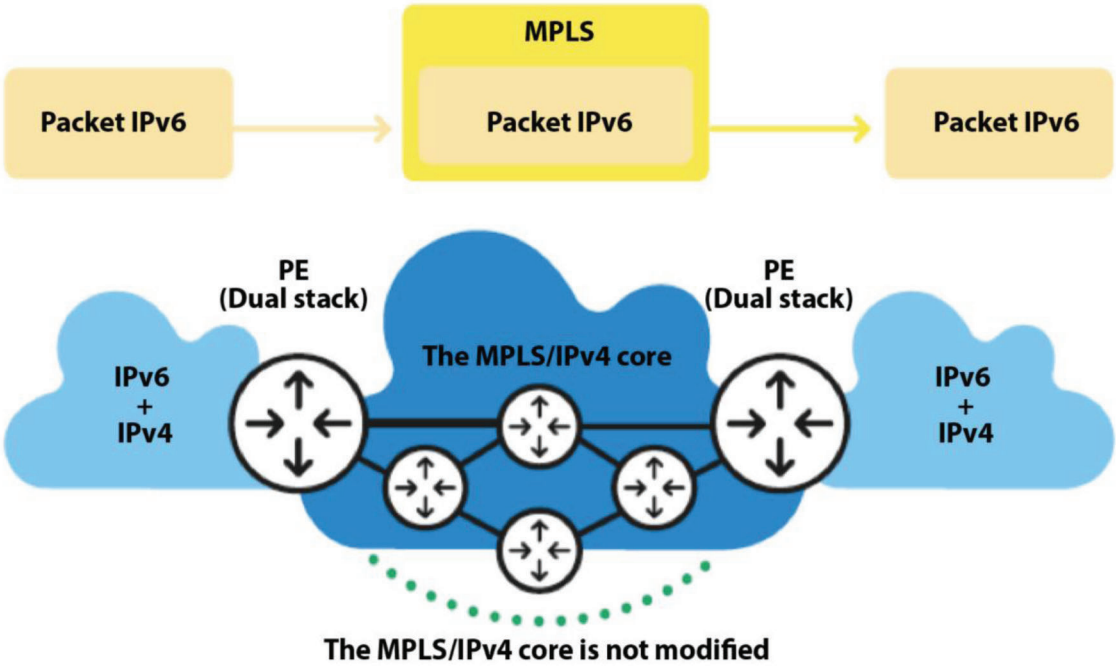
This technology is supported on the following network structure:

Apart from setting up the new configuration, all that is necessary is to upgrade provider edge (PE) software.

When MPLS is used, paths are established which are identified by their origin and destination. Datagrams are sent over these end-to-end paths without having to be switched hop by hop. This way, a routed network is converted into something similar to a circuit-switched network, thus gaining transport efficiency and other benefits. In fact, the paths on which the MPLS is based are known as "label-switched paths" (LSP). Both techniques use MP-BGP[36] (multiprotocol BGP) over IPv4 to exchange IPv6 routes. Only border routers must necessarily be dual-stack.

With 6PE, a single routing table is maintained which is why this technology is suitable for the Internet in general. In 6VPE, it is possible to maintain multiple tables, so this technique is suitable when virtual private networks (VPN) are used.

This technique is in widespread use in transport networks of ISPs across the LACNIC region.



35- Described in RFCs 4798 and 4659.
36- IETF RFC 4760

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

ANNEX III. DETAILED ANALYSIS OF QUANTITATIVE INFORMATION RELEVANT FOR THE TRANSITION TO AN IPV6 NETWORK

The goal of this research is to find up-to-date primary and secondary information on IPv6 deployment throughout the value chain published worldwide that will allow choosing and calculating IPv6 development indicators for different countries of the LACNIC service region and other countries selected for reference purposes. This research includes different data published by LACNIC, the different RIRs, equipment and service providers such as Akamai, Cisco and Google, and international organizations.

As for historical records, in general, these records do not provide any information that would help draw conclusions regarding projected IPv6 deployment. Most historical graphs contain discrete values or abrupt changes which, while exhibiting a tendency to grow in the short periods on record, generally correspond to very low indicator values and therefore variations or growth rates are not very representative.

When the analyzed indicators include other regions or the world as a whole, growth curves are more regular (e.g., IPv6 traffic compared to IPv4 traffic on Google servers, data Google has been recording since 2008). This aggregate information, however, provides no per country breakdown, which is the goal of this work.

For this reason, while important references are established to further study historical variations, the authors have chosen to research the situation in the LACNIC region and in countries selected worldwide, based on a careful selection of indicators from the wealth of information available. These are representative of various aspects of current IPv6 deployment, and can be considered clear indicators of progress in different areas of IPv6 deployment, all of which will be analyzed.

1. HISTORICAL DATA PUBLISHED BY LACNIC

LACNIC[37] presents an interesting breakdown of IPv6 deployment indicators, including, for example, a breakdown by country and by major LACNIC member. This Internet observatory is currently being expanded. The authors recommend that anyone interested in further understanding the historical evolution of any specific indicator should analyze this information. This information includes:

1. IPv6 statistics by ASN members corresponding to LACNIC's "Major" category

2. IPv6 penetration statistics by country (updated daily)

3. IPv6 allocations by country (LACNIC)

4. IPv6 penetration in the academic sector

5. IPv6 statistics by country according to Akamai (LACNIC)

6. IPv6 prefixed published via BGP

7. Websites currently IPv6 enabled

8. Website embryos

2. HISTORICAL DATA PUBLISHED BY RIPE

On its main statistics page, RIPE[38] also publishes data on various IPv6 related metrics, including data from countries outside their region.

This data is not vital for this analysis, but it is complementary in that it provides details on IPv6 deployment worldwide.

As in LACNIC, statistics are updated regularly and extended over time. These include the number of LIRs in the region, LIRs with and without IPv6, number of IPv4 transfers (which were growing strongly in late 2014), IPv6 allocations and assignments in the RIPE region and worldwide, as well as other statistics.

3. DATA PUBLISHED BY GOOGLE

Google has been collecting statistics about IPv6 adoption in the Internet on an ongoing basis since 2008[39]. Given its share of global traffic, the information provided by Google is relevant. Interesting data are observed for 8 June 2011 (World IPv6 Day) and 6 June 6 2012 (World IPv6 Launch Day). Between those two points in time, native IPv6 traffic doubled from 0.3% to 0.61%, while tunneled traffic (6to4 and Teredo) fell from 0.04% to 0.01%.

As at 17 November 2015, global native IPv6 traffic averaged 7.40% and exhibited a growing trend, with daily variations in the order of +/- 1 pp. By contrast, tunneled traffic stagnated between 0 to 0.01%. This tendency of tunneled traffic to disappear with the growth of native IPv6 began in mid-March 2010, and was further strengthened after World IPv6 Day.

Google employs a special mechanism[40] to determine clients' ability to use IPv6: it uses its service delivery

37- http://stats.labs.lacnic.net/
38- https://labs.ripe.net/statistics/?az=true
39- http://www.google.com/intl/es/ipv6/statistics.html
40- http://static.googleusercontent.com/media/research.google.com/es//pubs/archive/36240.pdf

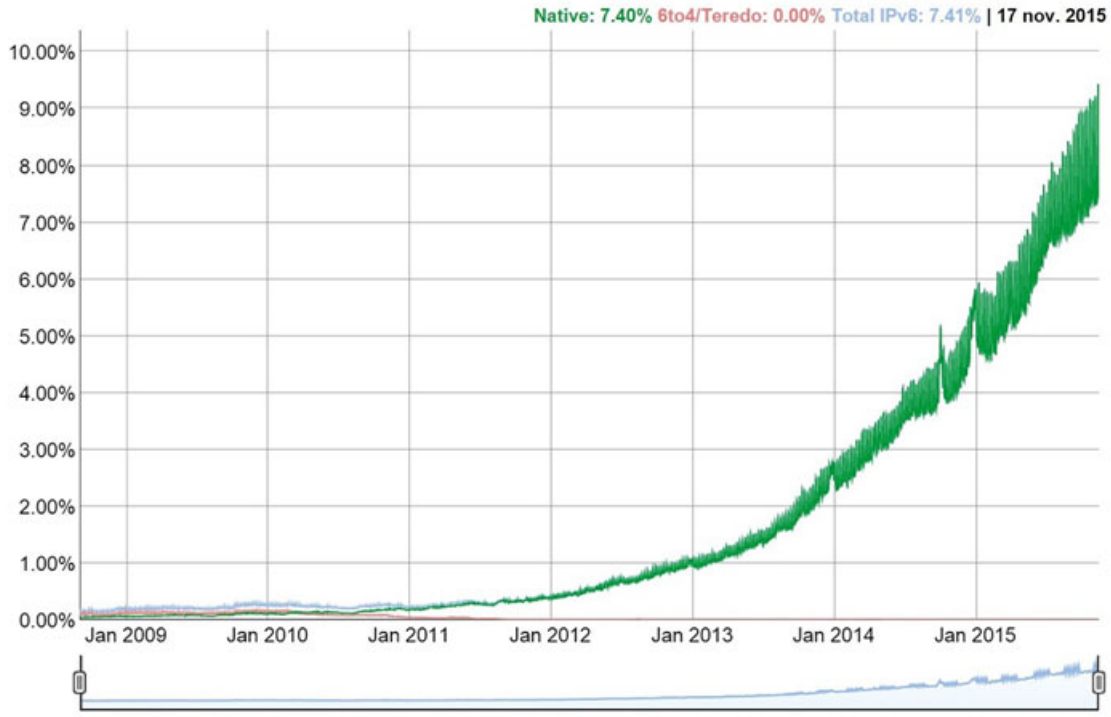
Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

points configured with dual-stack IPv4 and IPv6 protocols, and counts the number of customers that access the same service over IPv6. The measurement methodology is based on asking Web clients to send HTTP requests to either an IPv4-only host or a dual-stack host and comparing the results This is done by modifying the answers to just a small, randomly-selected fraction of Google search requests.

Initially, Google offers the graph below which shows the percentage of global users that access Google over IPv6.

Google also provides current data on the percentage of IPv6 adoption in practically all countries, which is used in joint indicator developed within the framework of this research. This indicator is used to assess the end user's ability to access IPv6 natively, along with the data published by APNIC. Akamai, a similar source, will be analyzed below.

Google also allows the public in general to verify whether their devices are IPv6-ready[41].



4. DATA PUBLISHED BY AKAMAI

On its main IPv6 page[42], Akamai presents general statistics on the number of "hits" per second received by Akamai servers over IPv6 since 28 March 2012, classified by region.

Akamai also publishes information on IPv6 adoption rates by country and by region[43]. In addition, it offers historical information on IPv6 adoption at country/operator level since 31 August 2014. These percentages are calculated by dividing the number of content requests sent to Akamai over IPv6 by the total number of requests received by Akamai (IPv4 and IPv6) on their dual-stack servers.

This indicator is similar to Google's, although apparently it does not include the values returned by the testing software.

5. DATA PUBLISHED BY CISCO

This section describes the primary and secondary data published by Cisco regarding IPv6 adoption, different IPv6 adoption metrics, and the rationale behind them according to their own documents[44]. The IPv6 website shows the indicators' historical evolution.

The varied data published, prepared or authorized by Cisco can be used to assess IPv6 deployment in countries within the LACNIC service region and compare them to that of others.

41- ipv6test.google.com
42- http://www.akamai.com/ipv6
43- http://www.stateoftheinternet.com/trends-visualizations-ipv6-adoption-ipv4-exhaustion-global-heat-map-network-country-growth-data.html#networks
44- Olivier Bournez. "Internet IPv6 Adoption: Methodology, Measurement and Tools." Cisco France. 2012. http://6lab.cisco.com/stats/data/Internet%20IPv6%20Adoption.pdf
http://6lab.cisco.com/stats/

In addition, it creates a pair of joint indicators which include - in weighted form - three approaches to IPv6 adoption for each country or region. Cisco has published several documents, one of which is used as a reference on the chosen methodology.

This section provides a detailed explanation of how Cisco prepares selected indicators, including joint indicators, so that the basic measurement and calculation principles can be better understood.

Cisco generates its statistics based on indicators targeting four main groups of actions and results, which are applied to the Internet's value chain during IPv6 adoption. This vision matches the direction defined for evaluating the situation in different countries and seeks to identify the current status and progress in different parts of the networks which can be measured through sometimes complex procedures.

1. Planning. A prefix assignment is the first step on the road towards IPv6 adoption. The growth rate of IPv6 assignments is an indicator of future deployment. In addition, the percentage of these prefixes in the BGP routing table is a metric of current deployment, as prefixes are gradually routed over the Internet. While these indicators do not have a strong correlation with IPv6 deployment, they do serve as indicators of existing trends in IPv6 adoption.

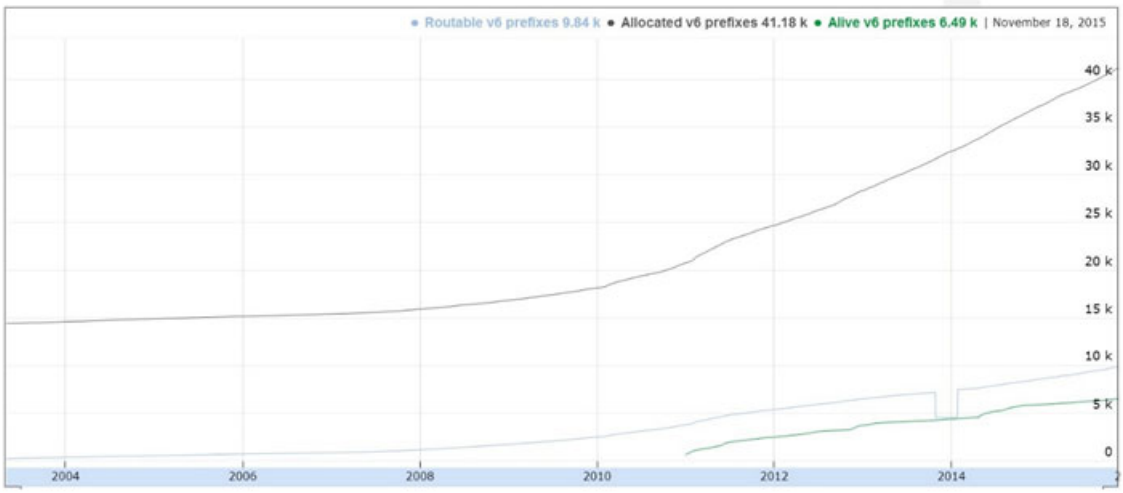
2. Core network. Because the first place in which IPv6 must be deployed is the core network (Internet transit providers), it makes sense to determine IPv6 penetration in the core network, which can be measured through the global Internet routing table.

3. Content. Once the core network is IPv6-enabled, content providers and applications can begin enabling their deployments to provide services over IPv6. These providers' readiness allows obtaining another indicator of IPv6 adoption and its potential use by IPv6-enabled users.

4. Users. Finally, it is important to determine the degree of progress achieved in user IPv6 access.

5.1 Planning. Allocation and routing.

Cisco presents a graph such as the one below to connect three metrics regarding IPv6 prefix assignments worldwide. This graph shows the number of IPv6 prefixes that are allocated, routable and "alive."



The number of allocated prefixes can be found the whois databases of the different RIRs.

Routable allocated prefixes are obtained analyzing the routeviews project's global BGP table, which is an aggregation of BGP tables from Tier one ISPs and big IXPs. The indicator is calculated with a cross check between the prefixes table and all the destinations in the BGP table.

To calculate the "alive" prefixes, Cisco uses Geoff Huston's dataset[46] with a JavaScript program that triggers on Internet ads. It is not known which one nor on which websites does the script apply (for confidentiality reasons) but it is indeed known that it's partially on Google search but not only. The program analyzes prefixes showing activity.

46- Chief Scientist at APNIC.
47- https://tools.ietf.org/html/draft-vyncke-ipv6-traffic-in-p2p-networks-01

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Cisco also uses the data collected by Eric Vyncke, which measures IPv6 traffic in the BitTorrent peer-to-peer network. Eric Vyncke uses this network because it transports a good part of Internet traffic, and because its structure and functions allow quickly discovering a large number of nodes worldwide. P2P users prefer IPv6 because it does not share the problems encountered when using NAT with IPv4, and the long periods during which the links are established allow better discovery activity prefixes. A detailed description of the procedure can be found in an IETF Internet Draft published in 2012[47].

When Cisco observes traffic from a prefix according to one of these two sources, they understand that the prefix is "alive."

Based on these three types of information, Cisco calculates the following indicators:

1. Percentage of routable allocated IPv6 prefixes, with respect to the total number of allocated IPv6 prefixes. These percentages are published and shown in different colors on Cisco's world map[48].

2. Percentage of allocated IPv6 prefixes with regard to allocated IPv4 prefixes. This value, which is obtained from the RIR, is published for each country.

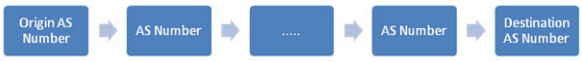
3. Percentage of allocated IPv6 prefixes in which traffic has been observed, with regard to the total number of allocated IPv6 prefixes. This value is also published for each country.

5.2 Core network. Core. Autonomous Systems offering IPv4 transit.

IPv6 adoption in the core network is observed by analyzing the behavior of transit AS's. In this section, Cisco tries to determine which AS's provides transit, whether they are IPv6 and their weight within the network, in order to determine the weighted presence of IPv6 AS traffic.

To analyze the Internet core both at global or local level, the routing tables provided by the routeviews[49] project are used, the same as those used to track routable IPv6 prefixes. This data provides routing information for multiple routers, those with the best connectivity, and those which are assumed to receive the global BGP table or a global routing table so those tables do not contain default routes for sending a packet to several destination AS's. This guarantees the unique identification of source AS to destination AS.

What can be acquired from routeviews are two big BGP tables: one in IPv4 and one in IPv6. Even though some routers are dual-stack, bot tables are completely different. What the routeviews BGP table gives are thousands of lines of the following pattern:



Cisco considers that all AS's that appear in an AS path of the BGP table are transit AS's, so, for the purposes of the study, source and destination AS's are removed from the tables. The weight of a transit AS is calculated by computing the number of times an AS appears in all AS paths in the table. AS's that appear multiple times but only one behind the other are also deleted, as sometimes this is is for traffic engineering purposes.

The indicators of IPv6 adoption at core network level are as follows:

1. Weighted % of AS's which are IPv6 transit with regard to the number of AS's which are IPv4 transit. (IPv6 transit AS). An IPv6 transit AS provides transit over both IPv4 and IPv6 networks.

2. Weighted % of IPv4 transit AS's which have been assigned at least one IPv6 prefix, with regard to the number of Autonomous which are IPv4 transit. (Transit AS which has an IPv6 prefix). A transit AS which has an IPv6 prefix is one that is transit over the IPv4 network and has at least one IPv6 prefix, but is not necessarily an IPv6 transit AS.

AS's are weighted on each network (IPv4 or IPv6) applying a factor described and explained in the reference document[50]. This is not relevant at this time, as it is simply a factor which is adequate for obtaining a better approximation, and is closely and exclusively related to the number of times an AS appears on the global routing tables.

5.3 Content. Websites.

Cisco tests and measures two indicators for this category:

1. The number of websites that are announced as IPv6 on a DNS server (those that have an AAAA record).

2. The number of websites among the first category that are effectively accessible in IPv6

Website operators launch a proof-of-concept IPv6 accessible website before going into full production.

48- http://6lab.cisco.com/stats/index.php?option=prefixes
49- http://www.routeviews.org/
50- Olivier Bournez. "Internet IPv6 Adoption: Methodology, Measurement and Tools." Cisco France. 2012. http://6lab.cisco.com/stats/data/Internet%20IPv6%20Adoption.pdf

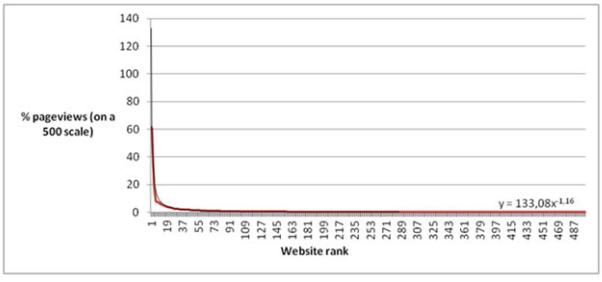
LACNIC calls them "IPv6 embryos." Those websites' domain names are clones of the main domain names and are often identified by a prefix such as ww6.domain, IPv6.domain, or similar. These particular domain name prefixes are also looked up, as they allow observing the trend towards IPv6.

Moreover, considering that a small number of websites concentrate the largest number of users and exchange the largest volumes of information, testing is limited to Alexa's top 500 websites[51] in approximately 130 countries. The rest of the websites are not really representative. Each website was assigned a weight (percentile) according to the number of pageviews - unique users, also according to Alexa.

Thus, a weight is obtained for each top 500 website. These weights are calculated based on the average monthly number of unique visitors and daily pageviews are ranked from the highest to the lowest, and a graph is obtained like the one below which reflects the preponderance of some of the major websites. The same weights were used for the top 100 most visited websites in each country. Alexa publishes information on the top 500 websites in each country, ranked by number of visitors and pageviews. This is an adequate approach considering that Alexa provides a ranking in order of importance (visitors - pageviews) for each country.

For each website - obtained from a survey of the 500 most visited websites in each country - AAAA requests are made to DNS servers for the exact domain name, and also for possible test sites such as ww6.domain or ipv6.domain. Indicators are calculated computing the positive responses received for these queries.

By adding the weights for each IPv6-enabled website, it is possible to estimate the weighted average percentage of websites accessible over IPv6, according to website traffic profiles for each country. It should be noted that not all visited websites are hosted in the same country as their visitors; for example, in smaller countries very few of these are on Alexa's list.



Note: The weight obtained for website X represents the probability that a random user in a random country will access a random page that is part of website X.

51- www.alexa.com
52- http://labs.apnic.net/dists/v6dcc.html
53- http://www.circleid.com/posts/20120625_measuring_ipv6_country_by_country/

These indicators are:

1. Weighted % of sites accessible over IPv6 (considers the number of pages viewed - unique users). It also shows the number of enabled websites over a total of 500 per country.

2. Testing: domain name tested in IPv6. Weighted % of domains for testing corresponding to the 500 sites analyzed.

3. Faillure: AAAA records exist but the website is not operational in IPv6. % of the 500 domains which experienced IPv6 access failures.

4. Others: Websites not IPv6-enabled. % of the 500 websites.

These indicators allow determining the approximate total IPv6 website traffic if all users were IPv6-enabled.

5.4 Users

Monitoring users is not easy and requires a lot of data coming from different sources. Google and APNIC labs do the same method with pixels loading in IPv4 or IPv6. The two sources used by Cisco are different; Google is more reliable for smaller countries, not for those such as China where Google is not the first website in Alexa's ranking.

The indicators published by Cisco are those of Google and APNIC: the ratio between the number of searches in selected servers with potential IPv6 access, and the total number of searches.

Google applies the methodology to their websites and publishes the data collected, as is described above in section "3. Data published by Google." The indicator shows the number of users who can access using IPv6 as compared to the total number of users.

As for the data provided by APNIC, this data is collected country by country and day by day. The ratio between IPv6 users and total users is published the APNIC Labs page[52], along with many other datasets such as absolute number of users, population, GDP, GDP per /32, etc. APNIC's procedure[53] answers the following question: "What proportion of the Internet's users are capable of using IPv6 when offered a choice of protocols?" In other words, how far are the users in different countries from being able to access websites over IPv6? To answer this question, similar to the approach adopted by Google, the test they used was silent, non-disruptive and very lightweight in terms of traffic and processing. The mechanism for injecting this testing software is to use the online advertising distribution networks.

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

These two datasets, country by country, are highly correlated

5.5 Composite metrics published by Cisco

Cisco presents two composite metrics by country, both of which are very useful for international comparisons but are not very suited to the conditions of the LACNIC region. The reasons for this were analyzed earlier in the section where the "LACNIC/CAF ICAv6" indicator was described.

% IPv6 deployment by Cisco

This indicator is calculated based on three of the four metric categories described above, selecting the following indicators in each category:

1. Transit AS: According to Cisco's original reference documents, this value was represented by the weighted % of IPv4 transit AS having an IPv6 prefix (including AS's which are IPv6 transit), relative to the number of AS's that are IPv4 transit. From the IPv6 deployment percentages published on Cisco's world map, it follows that as at July 2015 a composite indicator was being used which is calculated as follows:

$$\%\ Transit\ AS\ = \%\ IPv6\ Transit\ AS\ + 0.2 * (\%\ \textbf{Transit with an IPv6 prefix} - \%\ IPv6\ Transit\ AS)$$

2. Content: Weighted % of IPv6-enabled websites.

3. Users: % of searches on servers selected with a preference for IPv6.

The formula for calculating the joint indicator is as follows:

$$\%\ Total\ IPv6\ Deployment = \frac{\%\ Transit\ AS\ + 3 * \sqrt{\%\ Content * \%\ Users}}{4}$$

This indicator takes into account the following:

1. A country's IPv6 readiness factor is the transit AS and is assigned a weight of 25%.

2. The remaining 75% is assigned the geometric mean of content and users. Considering that the product between Users and the Content available to these users provides a simple estimate of the actual IPv6 traffic in the country, it is reasonable to use the geometric mean rather than the arithmetic mean.

Average and comparative country index by Cisco.

Two additional joint indicators are defined:

1. A country's Average Relative Indicator (Indicador Promedio Relativo or IPR) as regards the rest of the world. This indicator uses the same weights and metrics as the % IPv6 deployment, but each term is normalized to maximum global-level values (Max Mund).

2. A country's Relative Indicator (Indicador Relativo or IR) as regards the rest of the world. The country's IPR, divided by the highest IR at global level, and normalized to a 0-10 scale. The smaller this value is for a country, they lower its IPv6 deployment status, with values between 0 and 10 for the most prepared country.

$$IPR = 0.25 * \frac{\%\ Transit\ AS}{Max\ Mund\ (\%\ Transist\ AS)} + 0.75 * \frac{\sqrt{\%\ Content * \%\ Users}}{Max\ Mund\ (\sqrt{\%\ Content * \%\ Users})}$$

$$IR = 10 * \frac{IPR}{Max\ Mund\ (IPR)}$$

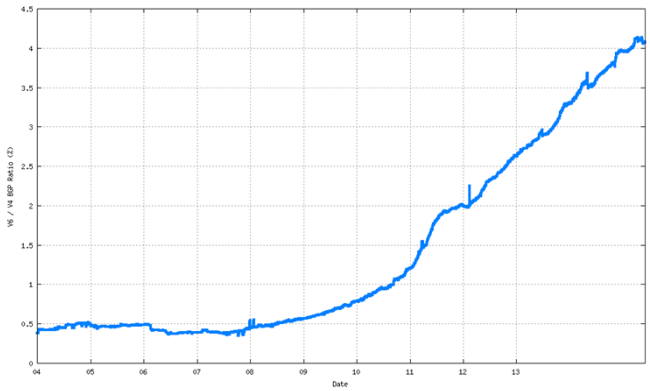
6. INDICATORS PROPOSED BY THE OECD

This classification takes into account the OECD's approach for measuring the transition to IPv6 included in document prepared in 2013[54] and published in 2014. The indicators they propose are in line with those used in this work.

This document also provides the sources of information used for each perspective, which in several cases match those considered in different sources.

6.1 Indicators using the routing systems

This system analyzes the number of routes published on both IPv4 and IPv6 in the global routing system. One way to visualize this indicator is through the ratio of IPv6 advertised prefixes : IPv4 advertised prefixes. The figure below shows how this ratio is growing[55]:



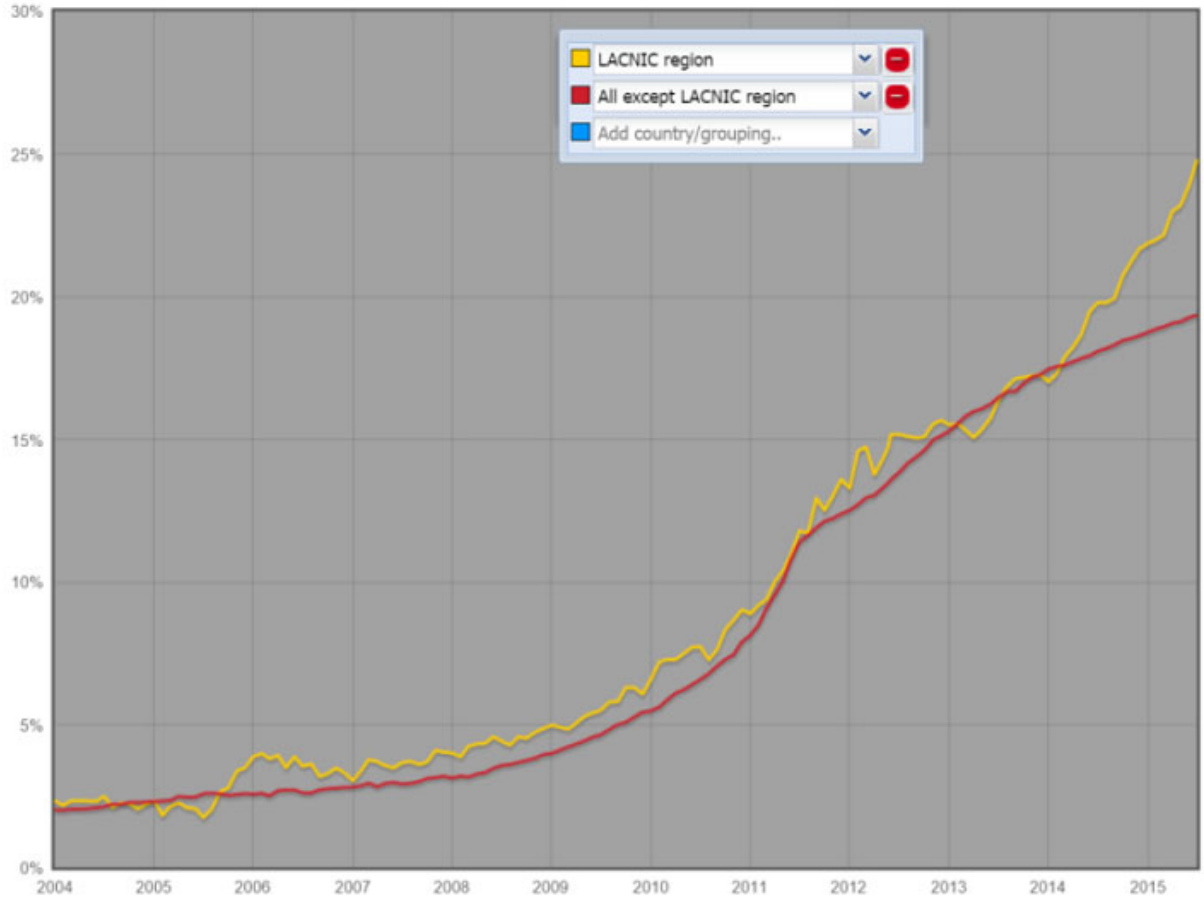
54- OECD (2014), "The Internet in Transition: The State of the Transition to IPv6 in Today's Internet and Measures to Support the Continued Use of IPv4", OECD Digital Economy. Papers, No. 234, OECD Publishing. http://dx.doi.org/10.1787/5jz5sq5d7cq2-en

55- Source: http://bgp.potaroo.net/stats/nro/v6 . Update on the statistics presented in the NRO report to the OECD Working Party on Communication and Infrastructure Services Policy, June 2009. http://www.nro.net/news/cisp-ipv6.pdf

A more accurate indicator of IPv6 deployment is to count the number of routing entities that are routing each type of address. Thus, each autonomous routing entity is counted only once (the entries in the routing system are not counted), which is a better indication of deployment. An important difference from the previous routing table entry counting system is that, in the case of IPv4, in addition to the fragmentation caused by block transfers, there is an amount of inherited legacy of fragmentation of network announcements that is not replicated in IPv6. In addition, IPv6 facilitates route aggregation. Thus, the ratio of IPv4 vs. IPv6 entries does not match the reality of registered addresses due to the different prefix sizes.

The following table shows the ratio of IPv6 AS's[56]: IPv4 AS's . In this case, RIPE uses a methodology similar to the one used by Cisco and also shows the historical evolution. It is also possible to obtain the historical evolution since 2004 for a large number of countries which can be selected and compared against each other, including countries in the LACNIC region.

The following graph shows the evolution of the countries in the LACNIC region, which since 2014 has been higher than the average for the countries in the other regions.



This indicator shows a clearer and more positive view of IPv6 deployment. This is a proxy of actual deployment, as it does not allow estimating the actual number of services provided over IPv6 or IPv6 packets sent over the network; however, it is considered important in terms of the readiness of each country's networks to provide IPv6 transit. Cisco has two Transit indicators, which are computed as described above.

6.2 Indicator using the domain name system

For a client to initiate a connection to a server using IPv6, it must necessarily use a function of the Internet's domain name system (DNS).

The number of domain names configured with IPv6 addresses can provide additional insight into the level of IPv6 deployment, but this indicator alone does not provide any relevant data on actual IPv6 deployment.

56- http://v6asns.ripe.net/v/6?s=_ALL

Casa de Internet de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

One approach for estimating this indicator is to take a list of the more popular web sites and see which of them have an IPv6 address. The most common source of such popular domain names is Alexa[57]. Once the most popular websites have been identified, this set of domain names is queried to determine which are using an IPv6 address.

This information can be observed on the World UPv6 Launch[58] website. This website shows the percentage of Alexa Top 1,000 websites currently reachable over IPv6 (aggregate, by network and by ASN). As at 1st June 2015, 15.9% of these websites were using IPv6 addresses.

Lars Eggert[59] has also been monitoring this indicator since 2007 (based on 500 websites) and has published the following graphs (June 2015, global and by country). The results are not entirely consistent with those of World IPv6 Launch, but it should be noted that they are different websites. Growth peaks can be observed in July 2011 and 2012, in the months following IPv6 and IPv6 Launch Day.

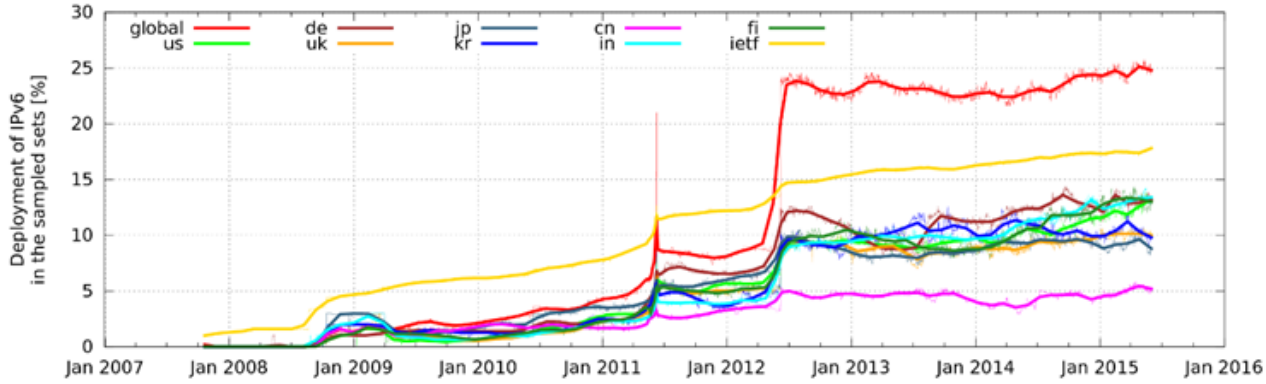
6.3 Indicator using Internet traffic statistics

Another form of measuring IPv6 deployment is to look directly at traffic volumes in IPv4 and IPv6. Such data is usually considered to be proprietary data and is not released to the public. This problem is solved by turning to IXPs that publish these results, such as those mentioned in LACNIC's statistics. One such IXP is the Amsterdam Internet Exchange (AMSIX). As at June 2015, DE-CIX was not publishing this information due to a problem with its platform.

Therefore, it is practically impossible to determine this very important indicator due to a lack of available data.

6.4 End client capabilities

The indicators discussed so far refer to parts of the Internet system and do not necessarily guarantee that the client's full and final experience is correct in IPv6.



Another indicator which also uses the DNS is the proportion of clients who are capable of resolving domain names using the DNS protocol over an IPv6 transport. This is not a direct client capability indicator, but a general indicator that reflects the degree to which the common infrastructure of the Internet, particularly the DNS name resolution infrastructure, is capable of operating in a dual-stack mode and is equally capable of operating over IPv6 as it is over IPv4. In September 2012, it was found that 18% of a sample of more than 2,000,000 clients used DNS resolvers that were capable of supporting queries over IPv6.

Presented by the OECD, this indicator is also calculated by Cisco under the Content category (using Alexa's Top 500 websites, in general and by country), and trying to determine IPv4 and IPv6 resolution in the domain name system.

This requires that each part of the Internet system be functional in supporting IPv6.

One simple way to measure the number of IPv6-capable clients is to use a dual-stack service point and count the number of clients who successfully establish contact with the service point using IPv6. Google and Akamai have been using their infrastructure to provide such data as discussed in the previous section, not only looking at IPv6 access but also at potential access.

6.5 Conclusions regarding the OECD

In their 2014 document, the OECD proposes different ways to analyze IPv6 deployment using methods similar to those developed in this work and those used by Cisco and other international references.

56- www.alexa.com
57- http://www.worldipv6launch.org/measurements/
58- L. Eggert: www.eggert.org/meter/ipv6

Casa de Internet
de Latinoamérica y el Caribe
Rambla República de México 6125
11400 - Montevideo, Uruguay
Teléfono: (+598) 2604 2222

Internet growth is leading to the imminent exhaustion of IPv4 addresses. IPv6 deployment represents the most sustainable alternative for allowing the Internet to continue to grow in a safe and stable manner.

This work reviews different aspects that affect the transition to IPv6 within the region. It contains a diagnosis of the status of IPv6 deployment in Latin America and the Caribbean, which summarizes different indicators by country and generates evidence to facilitate the decision-making process for large and small ISPs, content providers, academic networks, universities and governments throughout the region.

LACNIC - the Latin American and Caribbean Internet Address Registry - is the organization responsible for assigning and managing IP addresses and related resources for the region of Latin America and the Caribbean. It is one of the five Regional Registries that exist worldwide. For more information, go to www.lacnic.net.

CAF - the development bank of Latin America - has the mission of promoting sustainable development and regional integration by financing projects in the public and private sectors, as well as providing technical cooperation and other specialized services. Founded in 1970 and currently made up by 19 member countries (17 Latin American and Caribbean countries, Spain, and Portugal) and 14 private banks, CAF is a leading source of multilateral funding and an important generator of knowledge for the region. For more information, go to www.caf.com.