Technological transition from IPv4 to IPv6 at SNR: A success case

Transición tecnológica de IPv4 a IPv6 en SNR: un caso de éxito

Transição tecnológica do IPv4 para o IPv6 em SNR: uma história de sucesso

Andersson Salinas González[1]
Andrés Escobar Díaz[2]
Harold Vacca González[3]

Received: December 06th, 2020
Accepted: February 15th, 2021
Available: May 5th, 2021

How to cite this article:
Salinas González, A. Escobar Díaz, H. Vacca González, "Technological Transition From IPv4 To IPv6 At Snr: A Success Case," *Revista Ingeniería Solidaria,* vol. 17, no. 2, 2021. doi: https://doi.org/10.16925/2357-6014.2021.02.12

Research article. https://doi.org/10.16925/2357-6014.2021.02.12

[1] Electronic Technologist, Francisco José de Caldas District Univeristy; Control Engineering, Francisco José de Caldas District Univeristy, Colombia.

Email asalinasg@correo.udistrital.edu.co

ORCID: https://orcid.org/0000-0003-0445-3587

[2] Control Engineering, Francisco José de Caldas District University, Colombia. M. Sc, Universidad de los Andes, Colombia. Research group director ORCA. Plant teacher: Francisco José de Caldas District University, Colombia.

Email: aescobard@udistrital.edu.co

ORCID: https://orcid.org/0000-0003-0527-8776

[3] Graduate in mathematics and Master's degree in applied software, Universidad Distrital Francisco José de Caldas, Colombia. MSc. En Matemáticas Aplicadas Universidad EAFIT, Colombia. Director grupo de investigación SciBas. Docente de planta: Universidad Distrital Francisco José de Caldas, Colombia

Email: hvacca@udistrital.edu.co

ORCID: https://orcid.org/0000-0001-7017-007

Abstract

Introduction: This article is the product of the research "Technological transition IPv4 - IPv6 protocol" developed at the Francisco José de Caldas District University in 2020.

Problem: There is no detailed plan for the transition to IPv6 for the SNR that solves the support and connectivity problems of new devices to compete more efficiently in the telecommunications market for access to officials and the population.

Objective: To generate a transition process plan that includes a detailed description of the phases and includes the key activities for said transition.

Methodology: This article describes the research and implementation project that led to determine activities, phases and products corresponding to the technological transition from IPv4 to IPv6 in the SNR.

Results: The scope is visualized, as well as the documentary assurance through actions and recommendations of the change.

Conclusion: It is evident that, after complying with a proposed evaluation methodology, the experience can be characterized as a success case, since it facilitated the pertinent decision making within the process of adopting the new protocol.

Originality: Through this research, the three transition phases suggested by the Ministry of Information Technologies and Communications (MinTIC) are contemplated.

Limitations: The technological transition from the IPv4 to IPv6 protocol is limited by the fact that the process is not immediate but transitory, so it must be supported by transition mechanisms that allow the coexistence of both protocols.

Keywords: IPv4, IPv6, Transition mechanisms, security policies, success case

Resumen

Introducción: El artículo es producto de la investigación "Transición tecnológica IPv4 - Protocolo IPv6" desarrollada en la Universidad Distrital Francisco José de Caldas en 2020.

Problema: No existe un plan detallado de transición a IPv6 para el SNR que resuelva los problemas de soporte y conectividad de los nuevos dispositivos para competir de manera más eficiente en el mercado de las telecomunicaciones para el acceso a los funcionarios y la población.

Objetivo: Generar un plan de proceso de transición que incluya una descripción detallada de las fases e incluya las actividades clave para dicha transición.

Metodología: Este artículo, por lo tanto, describe el proyecto de investigación e implementación que llevó a determinar las actividades, fases y productos correspondientes a la transición tecnológica de IPv4 a IPv6 en la SNR.

Resultados: Se visualiza el alcance, así como el aseguramiento documental a través de acciones y recomendaciones del cambio.

Conclusión: Es evidente que, luego de cumplir con una metodología de evaluación propuesta, la experiencia puede caracterizarse como un caso de éxito, ya que facilitó la toma de decisiones pertinentes dentro del proceso de adopción del nuevo protocolo.

Originalidad: A través de esta investigación se contemplan las tres fases de transición sugeridas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Limitaciones: La transición tecnológica del protocolo IPv4 a IPv6 se limita a que el proceso no es inmediato sino transitorio, por lo que debe ser apoyado por mecanismos de transición que permitan la coexistencia de ambos protocolos.

Palabras clave: IPv4, IPv6, mecanismos de transición, políticas de seguridad, caso de éxito.

Resumo

Introdução: O artigo é produto da pesquisa "Transição Tecnológica IPv4 - Protocolo IPv6" desenvolvida na Universidade do Distrito Francisco José de Caldas em 2020.

Problema: Não existe um plano detalhado de transição para IPv6 para o SNR que resolva os problemas de suporte e conectividade dos novos dispositivos para competir com mais eficiência no mercado de telecomunicações pelo acesso aos funcionários e à população.

Objetivo: Gere um plano de processo de transição que inclua uma descrição detalhada das fases e inclua as principais atividades para essa transição.

Metodologia: Este artigo, portanto, descreve o projeto de pesquisa e implementação que levou a determinar as atividades, fases e produtos correspondentes à transição tecnológica do IPv4 para o IPv6 na SNR.

Resultados: O escopo é visualizado, bem como a garantia documental por meio de ações e recomendações da mudança.

Conclusão: Fica evidente que, após o cumprimento de uma metodologia de avaliação proposta, a experiência pode ser caracterizada como um caso de sucesso, pois facilitou a tomada de decisão pertinente dentro do processo de adoção do novo protocolo.

Originalidade: Através desta pesquisa são contempladas as três fases de transição sugeridas pelo Ministério das Tecnologias da Informação e Comunicações (MinTIC).

Limitações: A transição tecnológica do protocolo IPv4 para o IPv6 se limita ao fato de que o processo não é imediato, mas transitório, devendo ser apoiado por mecanismos de transição que permitam a coexistência dos dois protocolos.

Palavras-chave: IPv4, IPv6, mecanismos de transição, políticas de segurança, história de sucesso.

1. INTRODUCTION

Transition refers to a period of evolution or progressive change that occurs when new technologies are adopted in a sequential and complementary fashion [1]. In this sense, since the 1980s, the exponential growth of telecommunications networks has generated a greater need for services and benefits on the Internet; with the expansion of computational and communications technologies, the demand for intensive informational processes that require technological innovation has grown proportionally [2], especially in technological devices: laptops, cell phones, access points, tablets, servers, storage equipment, among others [3], [4]. Therefore, connectivity has increased in numerous world networks. However, although IPv4 (Internet Protocol Version 4) addresses were created for this purpose, at this time they entered a final exhaustion phase [5]. As a consequence, in 1992 the Internet Engineering Task Force (IETF) -from the research and development of working groups- defined RFC 2460 (Internet Protocol Version 6 (IPv6) Specifications [6], which gave rise to the new connectivity protocol called IPv6 or IPNG (Internet Protocol Next Generation).

On the other hand, Internet governance has been understood as the development and application of principles and norms, rules, decision-making procedures and programs that shape the evolution and use of the Internet [7]. In that perspective, there is no single person, company, organization or government that exclusively manages the Internet; rather, it is a globally distributed network that is made up of many voluntarily interconnected autonomous networks [8], [9]. And such governance was conceptualized with the idea of three layers or levels: Physical infrastructure level (through which the information travels), Logical level (which controls the infrastructure) and Content level (which contains the information signaled through the network).

Thus, the internet organizations, among the three levels mentioned, do not have a hierarchy, but they have specific functions that make them work in harmony. The most recognized organizations in internet governance are: IETF [10]–[13]; Internet Research Task Force (IRTF) [14]; Internet Society (ISOC) [10], [15], [16] Internet Corporation for Assigned Names and Numbers. (ICANN) [17], [18]; Internet Assigned Numbers Authority (IANA)**,** and for Latin America, the Registry of Internet Addresses of Latin America and the Caribbean (LACNIC).

On the other hand, the Ministry of Information Technologies and Communications of Colombia (MinTIC) is the entity whose charge is to "*To design, adopt and promote policies, plans, programs and projects in the Information and Communication Technologies sector*" in the Republic of Colombia,[19]. MinTIC presented the IPv4-IPv6 transition guide that establishes the guidelines to be taken into account for the implementation of the transition process from the IPv4 to IPv6 protocol [20].

Among other elements to observe, it is required that all technological devices used to connect to the internet have an IPv6 address, which will provide broadband connectivity, offering services and achieving global internet access to the entire population in order to stimulate and offer opportunities for global development [21].

However, the transition process has implied that a phased development is taken into account, in a controlled and reliable environment, so as to ensure a successful adoption of the IPv6 protocol, in terms of the technological infrastructure. Under these particularities, the Superintendency of Notaries and Registry (SNR) of Colombia, assumed the process.

The article, then, describes the research and development carried out so that the SNR, successfully, could make the aforementioned transition. The document is structured as follows: The first part describes the methodology adopted for planning the transition process, explaining the diagnostic plan, the addressing design for the new protocol, and the transition mechanism established for the transition. Subsequently, the implementation and testing model are exhibited, where the detailed

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

implementation plan, the monitoring variables in storage systems and the activation of security policies are defined. Finally, there are the conclusions of the work carried out that characterizes the SNR case as one of success under a proposed evaluation model.

2. BACKGROUND.

Since 1981, IPv4 has been the protocol in charge of addressing and accessing the internet to almost 4.3 billion devices, but that number of devices has multiplied thanks to new technologies, so it has been necessary to migrate to a broader protocol that guarantees the connection for new users, so IPv6 is a convenient solution to the absence of IP [22], [23].

In the United States, approximately 40% of companies have adopted IPv6. In Europe, the leading countries in IPv6 adoption are Belgium (61%), Germany (47%), Greece (38%) and France (27%). By 2022, 18.3 billion fixed and mobile devices connected to the network will be IPv6 compliant, and 60% of these compliant devices will be connected to IPv6 red [24], [25].

In Latin America, several countries have been introducing the IPv6 protocol through different ISPs (Internet Service Providers) that have made them pioneers in the transition to the future of communications and the Internet. For example, IFX NETWORKS is a company that offers comprehensive customized telecommunications solutions, and thus provides the best alternatives to companies and their needs for Latin America and the Caribbean. BT Latin America and GESATEL offer credible, serious and efficient communication in each of their products, backed by cutting-edge technology and a renewed technical effort. They developed a strategy of constant growth, supported by values of productive creativity in Argentina [26], [27]. NipCable do Brasil Telecom Ltda., for Brazil, offers the security and guarantee of performing services regulated by the National Telecommunications Agency (Anatel), since it has the subsidy granted by the agency to operate throughout the country, reaching homes in Brazil with new technologies on the Internet such as the adoption of IPv6 [28]. In Chile GTD has IPv6 enabled with its Global Crossing Upstream provider [29], Telecom Italia and sprint delivering transit to their IPv4 / IPv6 networks. "*We also implement IPv6 in our resolvers or DNS Cache, allowing us to deliver the name resolution service in both protocols, achieving connectivity from our servers to the ROOT SERVER in IPv6 / IPv4*." [30]. In Costa Rica, COOPEALFARORUIZ R.L. are also working with double stack to provide IPv4 / IPv6 services [31]. Likewise, in Ecuador, the University of Loja has implemented the main Internet services (Web, email, DNS, DHCP, among others),

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

with access to the commercial Internet in IPv6, and end users are in the process of implementation [32]. In Honduras, Cablecolor S.A has a native IPv6 network with dual-stack support in addition to NAT64 and DNS64 [33]. In Mexico, MCM Telecom S.A de C.V is one of the companies committed to promoting IPv6 at the national level, making customers aware of the depletion of IPv4 worldwide and the need to migrate [34]. And in the same way, other countries such as Nicaragua, the Dominican Republic, Paraguay and Venezuela are implementing the IPv6 protocol and thus improve the quality of service to Internet users and communications.

In Colombia, the IDU (Institute of Urban Development) has implemented IPv6 through hardware and software planning, complying with a stable IT infrastructure [35].

The MinTIC awarded a process that allowed for the successful adoption of the IPv6 protocol in IT and network infrastructures, making the applications and services operate under IPv6 [36]. In general terms, in Colombia and the world, the percentage of transition to IPv6 has been increasing in public and private entities due to the high access of the population to the Internet and the exhaustion of IPv4 protocol addresses.

The Francisco José de Caldas District University currently has IPv6 operation on the services of the Advanced Technology Research Network at the main headquarters. Among the services with IPv6 support are: math servers with free software, DNS, Web portal, management platforms, monitoring platforms, connectivity to academic networks, among others. Future projects are focused on extending the implementation over 16 locations and services are aimed at supporting the academic, scientific and research community [37], [38]. In mid-2014, LACNIC announced the start of the IPv4 protocol exhaustion phases in the region, for which the assignments were restricted in size and periodicity, that is, the addresses that covered the addressing needs were gradually running out [39].

For this reason, in the year 2017, MinTIC established the guidelines to adopt IPv6, through resolution 2710 that specifies in the first article on the object: *to formulate measures for the adoption of the IPv6 protocol in Colombia…* On the other hand, in the paragraph of article No. 4 it is suggested using the reference documents called "*Guía de transición de IPv4 a IPv6*" and "*Guía para el aseguramiento del protocolo IPv6*" which were published in their first version in the last quarter of 2015 [40].

In this period, few documented experiences appear in the literature. In [41], for example, a transition plan from the IPv4 to IPv6 protocol in data networks was designed for the mayor of Fusagasugá -Colombia, proposing the preparation and validation of an inventory of information assets to later be analyzed and develop a diagnosis plan that helped generate a work plan for the adoption of the new protocol.

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

Thus, failures were detected - at the network level - that could delay the transition process. In addition, it resulted in a diagnosis of the state of compatibility of the entity with IPv6; and detailed that a large number of the devices are compatible with the version 6 protocol, which did not prevent, however, the delay in the transition process.

For the year 2018, in [42] a technological strategy was designed for the adoption of the Internet Protocol Version 6 in the mayor"s office of Acacías -Meta, Colombia-, analyzing the technological structure of the entity to determine the levels of compatibility of equipment and networks with IPv6 and, likewise, generate a detailed plan of the transition process. With this exercise, the strengths and failures of the communications network were detected, which later resulted in the strategies that allowed for continuity of the service. An asset inventory was the first step in determining that 97% of the equipment was compatible with the transition process. To achieve this score, it was necessary to update the software, firmware and operating systems.

There are several examples worldwide that show the development of the transition process, as can be seen in [43]–[47], where it is evident that the technological change is linked to a diagnosis plan, followed by the implementation and a review of the security policies and later, the functionality tests.

Due to the above, the SNR has currently established methods to deploy the transition process in its facilities, taking into account the specificities and experiences such as those indicated; also taking into account the suggestions set forth in resolution 2710 of the MinTIC.

3. METHODOLOGY.

For the proposed transition planning, three phases were determined. For Phase I, the formulation of a diagnostic plan made up of four significant elements is evaluated: the hardware and software inventory, the state of technological compatibility with IPv6, the network topology, and the recommendations for the process.

Unlike the works presented as antecedents, where only Phase I was developed, this work proposed to reach the end of the process, that is, to include Phases II and III, which determine the implementation, testing and functionality analysis for a communications network segment of the SNR.

Finally, a methodology is established to evaluate the success case through compliance, emanating from a weighting scale, based on the transition model to IPv6 [48], and validated by the ORCA research group.

4. TRANSITION PLANNING FOR SNR

The planning phase of the transition process shows the development of the information asset inventory and is consolidated with the IT infrastructure diagnostic plan, including three elements that shape and support a solid structure.

The planning phase of the transition process demonstrates the development of information asset inventory and is consolidated with the IT infrastructure diagnostic plan, including three elements that shape and support a strong structure.

4.1. Diagnostic plan.

The diagnostic plan consists of four significant elements that help planning and avoid mitigating as many errors and risks as are latent in the process

4.1.1. Hardware and Software Inventory.

To carry out hardware and software inventory, a detailed information collection process had to be carried out through templates suggested by MinTIC through the IPv4 to IPv6 transition guide, shown in Figure 1. Then, the information concerning Computer Equipment, Communication Equipment, Applications and Servers was established, clearly identifying which equipment and applications support IPv6, and which require updating and / or do not support the new protocol.

Device	Brand	Model	Operating System	Ethernet ports	Role	IP version

Device	Memory	Processor	Discs	Operating System	Version	Installed software	Role	IP version

App	Feature	Type	Programming Language	Responsible	Component	Contract	IPv6 support

Server Type	Operating System	OS version	IP address	Functionality

Figure 1. Inventory model template, from top to bottom: Communication Equipment, Computer Equipment, Entity Applications and Entity Equipment and Servers.
Source. Taken from [49]

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

4.1.2. Infrastructure validation and IPv6 protocol compatibility.

Once the inventory was carried out, it was diagnosed that the degree of compatibility of the technological infrastructure with the IPv6 protocol is 69%, because not all equipment or applicators are supported in this protocol, as shown in Figure 2.

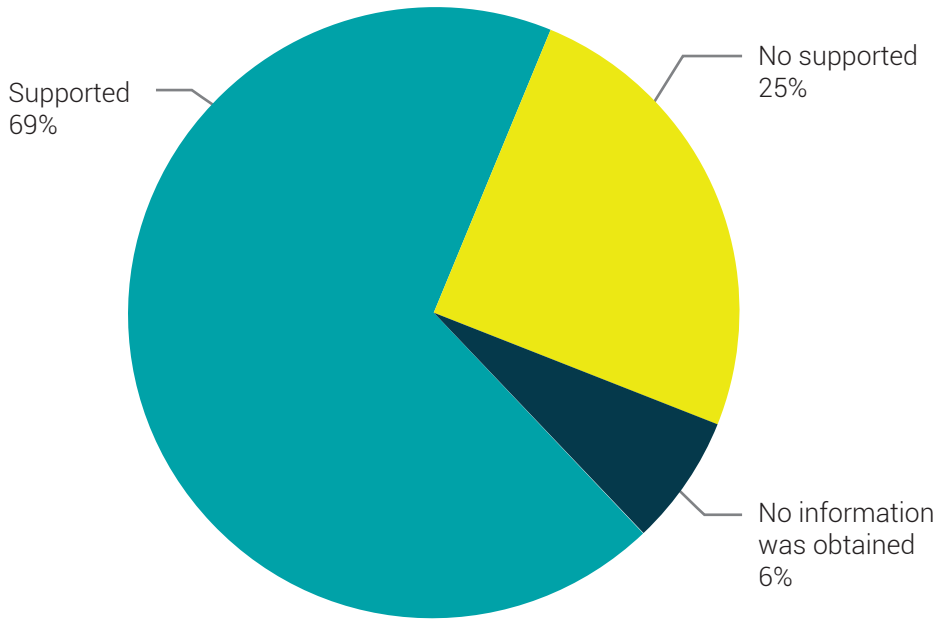

Figure 2. Degree of IPv4 and IPv6 support on the SNR.
Source: own work.

4.1.3. Network topology.

As for the network topology and its operation, a star-like network is maintained, where the MPLS service is the reception center for all requests and, in turn, authenticates the other locations in the rest of the country so that they can access the internet through the main network in Bogota, as shown in Figure 3.

By identifying the network topology and the degree of compatibility of the computers that make up the IPv6 network, a new topology was proposed that would allow for the coexistence of both protocols.

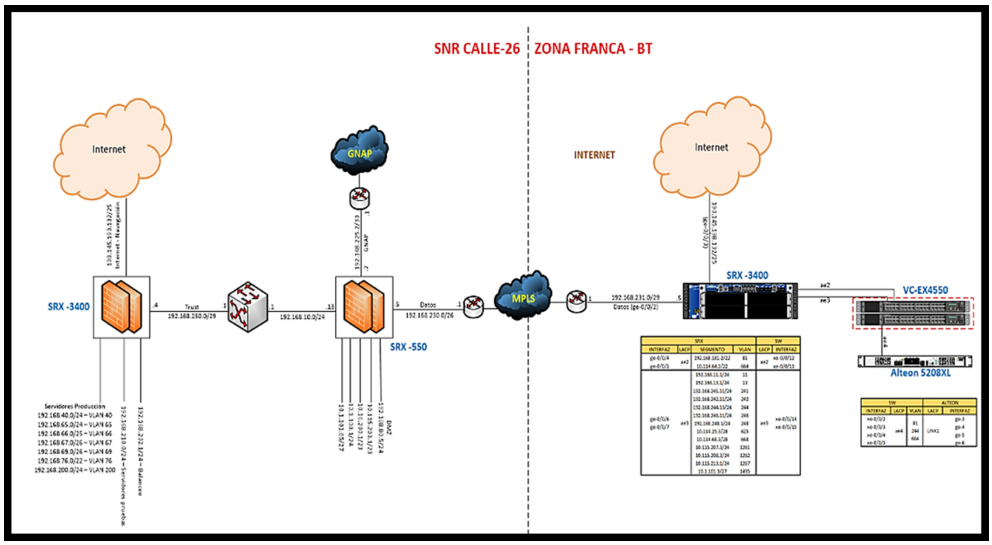

Figure 3. IPv4 topology of the network in SNR.
Source: own work.

4.1.4. Recommendations.

Once the diagnostic process was completed, it was evident that it was imperative to carry out each of the following recommendations made by the personnel who carried out said activity:

- Perform a scan for each unsupported system
- Evaluate the implications and determine the actions to follow.
- Estimate the resources and times in which IPv6 compatibility would be achieved.
- Define and execute the necessary actions on a controlled test environment.
- Gradually transition over to a double-stack environment.
- Manage an IPv6 prefix with LACNIC.

4.2. Address design

For the design of the network in IPv6 of the SNR, a Flexible Method was implemented to manage the allocation of bits of an address block, which is specified in RFC 3531, so that they are distributed, reserving a larger space between them. This way you can keep the bits on the partition boundaries as free as possible, and they can be used for any address design; however, its main use is for IPv6 [50].

Therefore, for the SNR a well-known prefix was used for documentation; **2001:db8::/32,** as indicated by RFC 3849 [51]. Subnetting changes were made using the fourth group of hextets or nibbles, so the subnetting for the SNR yielded the results, Figure 4, where a tree of addresses is displayed; address containers are in yellow, the reservations in gray and the subnets in red.

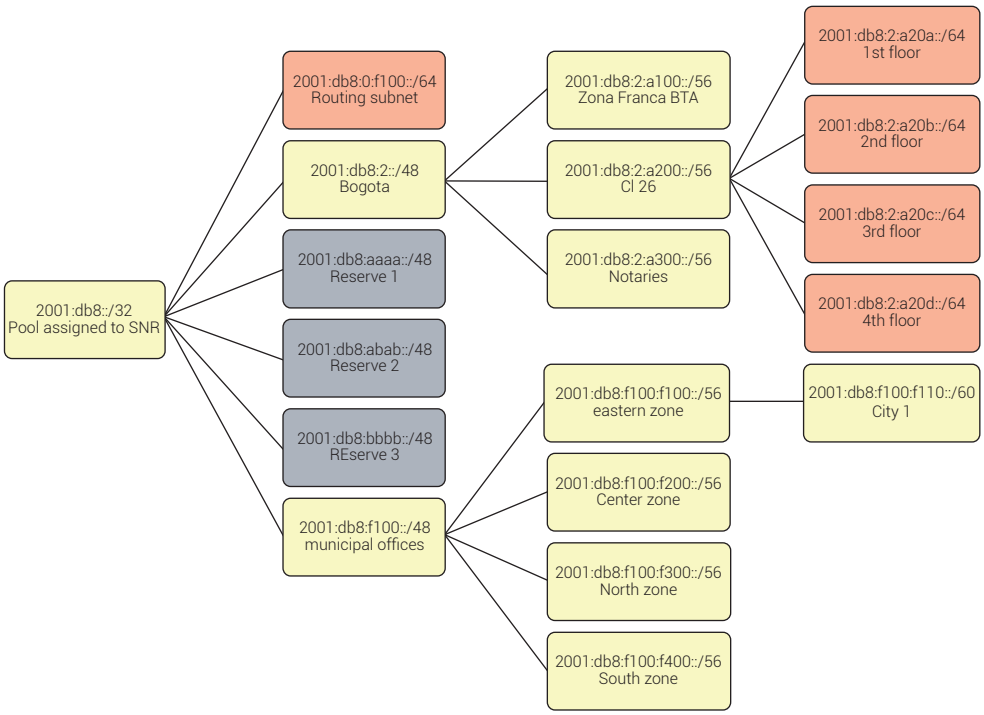

Figure 4. IPv6 Subnetting Tree for SNR.
Source: own work.

4.3. Double Stack Transition Mechanism

The SNR chose to implement the double-stack transition mechanism, as suggested by MinTIC in the IPv4 to IPv6 Transition Guide, since it has a great advantage; unlike other mechanisms, it allows for a stepped transition and does not introduce overheads. It also supports both protocols on the same device, that is, native IPv4 and IPv6 work at the same time [52]–[54]. Therefore, this method allowed both network technologies to coexist on the same link, and in turn, the implementation of the local IPv6 network without altering the operation of IPv4.

On the other hand, the dual stack implementation process consisted of configuring and enabling IPv4 and IPv6 on the same node, including terminals, devices and layer 3 devices.

Once enabled, an automatic configuration was established to detect IPv6 connectivity on the network, which in this case was provided by an ISP [55].

Another advantage of this system is that the user can choose the protocol version and the DNS (Domain Name System) announces a double-stack service (A and AAAA). In this way, hosts and routers are equipped with stacks for both protocols and have the ability to send and receive both types of packets, IPv4 and IPv6. Thus, in communication with an IPv6 node, a double stack node (or IPv6 / IPv4 node) will behave as a single IPv6 node, while in communication with an IPv4 node it will behave as a single IPv4 node. In Figure 5 we can see how the double stack works.

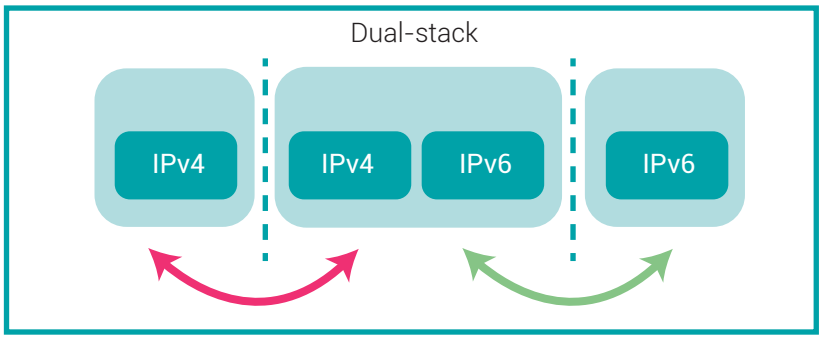

Figure 5. Double Stack Functionality.
Source: Taken From [56].

It is necessary to consider some aspects, including an analysis of the needs to make changes in the network infrastructure, such as the structuring of the DNS service and the configuration of the routing protocols and firewalls [57].

5. IMPLEMENTATION AND FUNCTIONALITY TESTING IN SNR

For the activation of the IPv4 and IPv6 protocol under the Double Stack mechanism in the SNR hardware and software, IPv6 addressing first had to be enabled in all physical and virtual devices, before carrying out the pertinent pilot test configurations and applying the transition model. Immediately, the functionality validation of the IPv6 protocol was carried out in the different services and finally, the security policies were activated.

The implementation process is described in detail below, since it includes a series of activities that allow the IPv6 protocol to be activated in dual stack for all SNR hardware and software.

5.1. Detailed implementation plan.

To begin the implementation process, IPv6 addressing was enabled through device segmentation, starting with routing equipment, servers, workstations, including PCs and laptops, and specialized videoconferencing equipment. It is important to mention that not all entities have these instantaneous transmission and reception devices, whereas the SNR uses room and desk devices.

It is recommended that, to perform the segmentation of PCs and laptops with different operating systems, they are configured automatically, preferably with a DHCPv6 server (Dynamic Host Configuration Protocol for IPv6), while videoconferencing varies depending on the model and brand.

It should be noted that firewalls are a critical point in the available network infrastructure, so it must be verified that IPv6 support exists and that it allows to configure filtering rules in a similar way as with IPv4 [58].

For the configuration of services, administration and support applications were used, in the particular case of the SNR, BINDv9 (Berkeley Internet Name Domain) was selected for the DNS server with IPv6 support, where it was analyzed if the name server had IPv6 addresses configured and if it was reachable within the internal network by both IPv4 and IPv6; which authorizes the DNS to respond natively in IPv6.

Another of the fundamental services in networks is the web server, being one of the most used in open source systems such as Apache [59], that is prepared to handle IPv6 without problems, with which the SNR holds a licensing agreement.

After enabling IPv6 addressing on the devices and the different SNR services, a pilot test was started, where the behavior of each device on the communications network was analyzed, adding load, services and end users.

In order to facilitate and standardize the transition process, tests were carried out in the network segments, made up of a few computers and users, where the homogeneity of the frame was used to allow for the consolidation and replication of increasingly extensive network segments with services, critical filtration and avoidance of damage in normal operation.

Next, Figure 6 shows a block diagram that condenses the activities of the implementation model suggested by MinTIC.

Finally, the information was collected in relation to the new network structure and its topology, which presented variations with respect to the network topology of the first phase, considering the guidelines of the new double-stack protocol. It is worth mentioning that the information must be documented to know if the IPv4 and IPv6 services are working independently but coexisting.

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

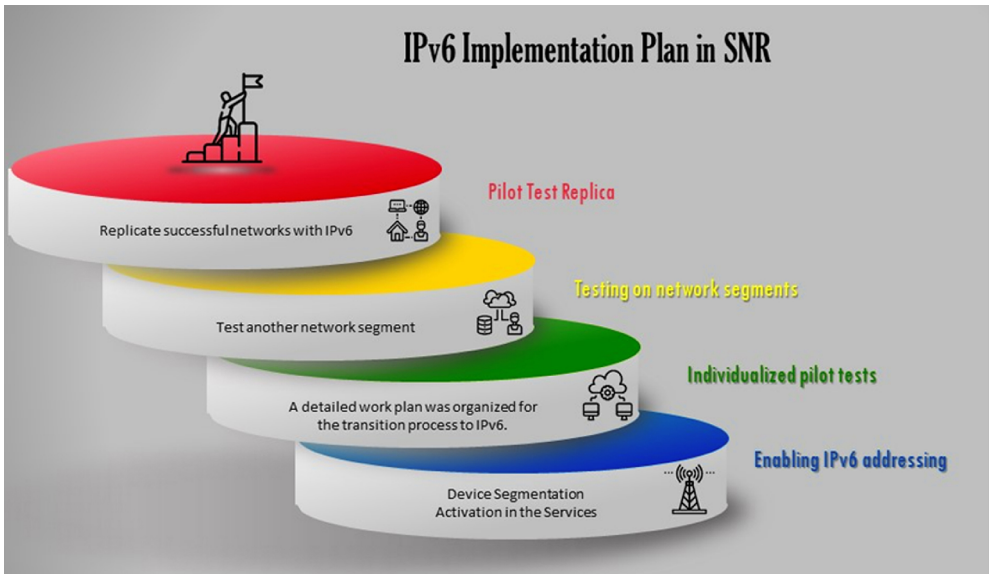

Figure 6. Activities for the implementation of IPv6 in SNR.
Source: own work.

5.2. Activation of security policies.

From a security perspective, for the IPv6 network configuration of the SNR, access through layer three was enabled, which consequently made the existing perimeter security rules for IPv4 no longer valid. However, security was not only an exclusive issue of the firewall configuration, but also included controlled processes and procedures that will validate the adoption of IPv6, which generated a highly positive impact.

In the previous sense, the information security risks that impact the services of the entities, which can cause problems, must be detected and analyzed in detail in order to find possible vulnerabilities. Even for IPv6, it is necessary to do this work because the protocol is supported by other protocols such as IPsec (Internet Protocol Security), HTTP (Hipertext Transfer Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol) or SIP (Session Initiation Protocol) [60], [61].

For the aforementioned, it is important to develop certain security guidelines, as they are done with the IPv4 protocol, because despite the fact that the entities begin to generate traffic, the attacks of the hackers do not take long to arrive. Therefore, it is crucial to generate certain standards under the premise of the basic pillars of information security such as Confidentiality, Integrity and Availability [62].

- Confidentiality is the property that prevents the disclosure of information to unauthorized persons or systems. Broadly speaking, it ensures access to information for only those people who have the proper authorization.
- Integrity is the property that seeks to keep data free from unauthorized modifications. In a rough way, integrity consists of keeping the information exactly as it was generated, without being manipulated or altered by unauthorized persons or processes.
- Availability is the characteristic, quality or condition of the information to be available to those who must access it, whether they are people, processes or applications. In general, availability is access to information and systems by authorized persons at the time they require it.

Then penetration tests were carried out on IPv6 networks, where the following points were attacked:

- Obtaining information: IP addressing, network domains, active directory accounts, personal names, IT infrastructure, scope of reconnaissance activities, obtaining information from intranet and websites, corporate information, newsgroups, social networks, personal web, metadata, among others.
- Recognition of the corporate network: DNS management, Whois, reverse searches, obtaining sloppy public information through available search tools.
- Passive collection: Make legitimate use of obtaining information through the means available on the Internet.
- Mapping the network through: Discovery of neighbors, MAC addresses, network topology, port scanning (TCP, UDP, ICMP), IP address discovery, determination of routes that packets follow supported by tools such as example trace-route, among others.
- Establishment of active services: Search for open ports and in a "listening" state.

Depending on what has been stated, the result of the penetration tests will be kept confidential, as will the scope of the tests, since it is the SNR"s own information.

To conclude, a list of RFCs that apply to IPv6 security is shared [57]:

- RFC 5619: Software Security Considerations, August 2009.

- RFC 5269: FMIP Security Distributing a Symmetric Fast Mobile IPv6 (FMIPv6).
- RFC 4942: IPv6 Transition/Coexistence Security Considerations.
- RFC 4218: Threats Relating to IPv6 Multihoming Solutions.
- RFC 4891: Using IPsec to Secure IPv6 Tunnels.
- RFC 4890: Recommendations for Filtering ICMPv6 Messages in Firewalls.
- RFC 4864: Local Network Protection for IPv6.
- RFC 4843: An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID).
- RFC 5213: Proxy Mobile IPv6.
- RFC 4835: Cryptographic Algorithm Implementation Requeriments for Encapsulating Security Payload (ESP) and Authentication Header (AH).
- RFC 4487: Mobile IPv6 and Firewalls: Problem Statement.
- RFC 4449: Securing Mobile IPv6 Route Optimization Using a Static Shared Key.
- RFC 4303: IP Encapsulating Security Payload (ESP).
- RFC 3756: IPv6 Neighbor Discovery (ND) Trust Models Threats.
- RFC 4301: Security Associations (SA). Security Architecture for the Internet Protocol. Support for IPsec-V2. (Making RFC 2401 obsolete).
- RFC 2401: Security Architecture for the Internet Protocol (Updated for RFC 3168), Support for IPsec-V2.
- RFC 4302: IP Authentication Header (Making RFC 2402 obsolete).
- RFC 4303: IP Encapsulation Security Payload.
- RFC 5282: Using Authenticated Encryption Algorithms with the encrypted payload of the internet key Exchange Version 2 (IKEv2) Protocol.
- RFC 5996: Internet Key Exchange (IKEv2) Protocol.
- RFC 4877: Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture.
- RFC 4581: Cryptographically Generated Addresses (CGA) extension field format (Updating RFC 3972).
- RFC 4982: Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGA). (Updating RFC 3972 errors).
- RFC 3414: User – Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3).
- RFC 4807: IPsec Security Policy Database Configuration – MIB.
- RFC 2406: IP Encapsulating Security Payload (ESP).
- RFC 4718: IKEv2 Clarifications and implementation Guidelines.

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

5.3. Functionality tests in storage systems, Applications and Communication Networks.

Based on the above results, functionality tests were carried out on SNR"s storage systems, applications and communication networks. For this, the following variables were taken into account for monitoring network services in IPv6, which allowed generating traffic to the Internet and vice versa.

- Traffic measurement on network interfaces and devices.
- Services status.
- Application status.
- Host activity.
- Communication channels to the Internet.

To comply with the requirements set forth in resolution 2710 of the MinTIC, below, the accessibility tests in IPv6 are set out on the website **http://servicios.supernotariado.gov.co.** Figure 7 shows the ping response for the web page from an external internet server.

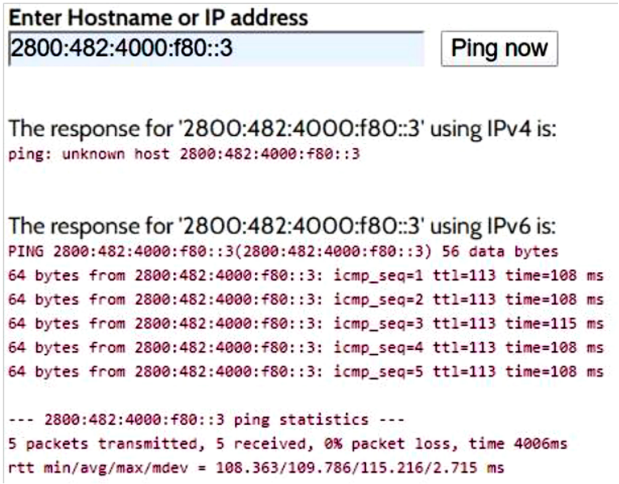

Figure 7. Ping from an external server to the SNR website.
Source: own work.

In order to verify the connectivity and speed of IPv6 and IPv4 for the status of services and applications, the reader can go to the IPv6-test.com page, which provides a free service to users where it provides an immediate diagnosis and informs which IP protocol is working at the time of the query; Figure 8 shows the connectivity scan of the SNR page.

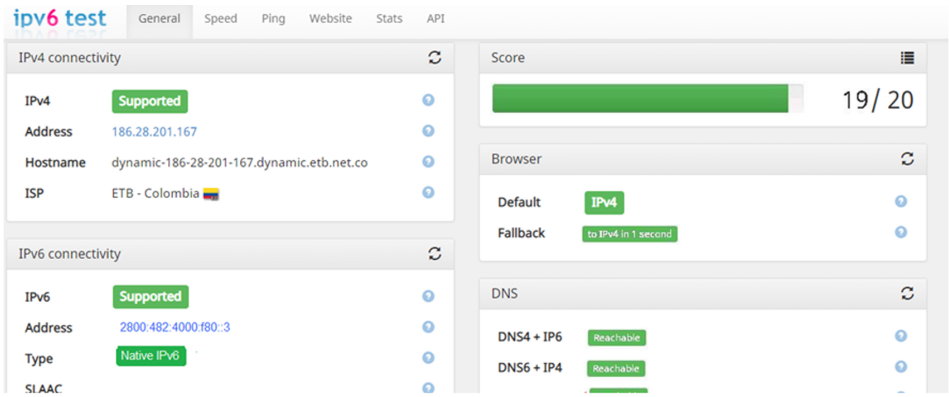

Figure 8. IPv6 connectivity scan of the SNR website.
Source: own work.

The results of the traffic measurement tests on the interfaces and activities of the hosts will be kept confidential, since it is proprietary information of SNR.

6. RESULTS

By 2018, the Superintendence of Notaries and Registration implemented an innovative technological system in each of the country"s notaries, beginning to work on electronic documentation and biometric registration systems to attend to the services provided to citizens. Therefore, the existing IP addresses in the version 4 protocol were insufficient compared to this increase in equipment that required these addresses. That said, the need to implement version six, that has the number of addresses that satisfies this need, was established. Just the previous year, in 2017, MinTIC promoted the digital government policy that involved the adoption of the IPv6 protocol in all government institutions, that helped continue advancing and innovating the technological instrument of the entity, in this way, enabling all people to have a more globalized access. The main advantage of IPv6 is its scalability, since the number of addresses prevents its exhaustion. This allows a more hierarchical and structured organization of the network. Similarly, the quality-of-service protocols in IPv6 are the same, today, as in IPv4.

The most obvious problems when implementing IPv6 were that the information of all technological assets was outdated and in other cases incomplete, Therefore, it was necessary to immediately execute an action plan that would create an inventory of assets in order to know the state of the SNR in terms of compatibility with the new protocol. In general terms, after having implemented the transition process, the superintendence has a web platform that can be reached by the IPv6 protocol. The

country"s notaries are feeding the cloud with vital information for its operation through said protocol [63].

In conclusion, the objective sought was achieved, delivering the results expected by the SNR in terms of connectivity and network security.

To ascertain whether the case was successful, it was necessary to implement the transition model towards IPv6 where the point of view of human resources and technical resources is taken into account, since it conceptualizes the entire cycle of diagnosis, planning, implementation, monitoring and launching of the new protocol and the performance functions that need to be taken into account for a successful transition process [48]. It was also necessary to resort to characterization of transition models that helped to give a better visualization of the desired characterization [64], [65].

Next, Tables 1 to 6 show the estimate of the success of the transition process which was submitted to validation by the ORCA research group of the Francisco José de Caldas District University, in the city of Bogotá, where the transition process was characterized according to a qualifying scale where the weighting was given as follows:

Technological transition from IPv4 to IPv6; low, non-compliance with the transition process, no opportunity for improvement.

(1-3) Appropriate technological transition, with opportunity for improvement.

(3-4.4) Medium technological transition, with opportunity for improvement and implementation.

(4.5-5) Total technological transition, implementation and eventual success story.

Table 1. Transition model, Project Management.

Phase	Description	Yes	No	Score
Diagnostic	Policy review and work plan	X		5
	Review of Procedures, Requirements and Needs Manuals	X		5
Planning	Determination of Scope and Time	X		5
	Schedule	X		5
	Obtaining budgets and resources	X		5
	Construction of project plan and specific plans	X		5
Implementation	Development of detailed project work plan	X		5
	Development of specific plans	X		5
Follow up	Risk controls	X		5
	Progress and management reports	X		5
	Control of scope, time, cost and quality	X		5
	Performance measurements, change controls		X	5

(continúa)

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

(viene)

Phase	Description	Yes	No	Score
Launching	Project closure and acceptance act.	X		5
	Closing of contacts		X	0
	Delivery of documentation and general recommendations	X		5
			Average	4.666666667

Source: own elaboration

Table 2. Transition model, Human talent.

Phase	Description	Yes	No	Score
Diagnostic	Human resource assessment team	X		5
Planning	Specifying roles, profiles and competencies	X		5
Implementation	Development of the team	X		5
Monitoring	Management and performance reports.	X		5
Launching	Closing of contracts		X	0
			Average	4.00

Source: own work

Table 3. Modelo de transición, Infraestructura.

Phase	Description	Yes	No	Score
Diagnostic	Inventory of information assets and services Logical interrelationship diagrams.	X		5
	Detail engineering, current request.	X		5
	Configurations bank.	X		5
Planning	Requirements evaluation.	X		5
	Detailed engineering, logic diagrams and components new solution	X		5
	Equipment specification, integration plan.	X		5
	Protocolo de pruebas.	X		5
	Success and acceptance factors	X		5
Implementation	Atmosphere of coexistence and testing.	X		5
	Physical connections.	X		5
	Quality management	X		5
	version control	X		5
	Validation of success and acceptance factors.	X		5
Follow up	exchange controls, risk management, quality management	X		5
	Validation of success and acceptance factors.	X		5

(continúa)

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

(viene)

Phase	Description	Yes	No	Score
Launching	Put into production.	X		5
	Delivery of documentation and user manuals.	X		5
	Delivery of configurations.	X		5
			Average	5

Source: own work

Table 4. Transition model, Applications.

Phase	Description	Yes	No	Score
Diagnostic	Application inventory.	X		5
	Application status evaluation (Owner, source code, copyright)	X		5
	Communications map for each application.	X		5
Planning	Source code assessment, interfaces used.	X		5
	Capacity assessment, data structures and programming languages for IPv6 support, IPv4 coexistence.	X		5
	Integration plan, testing protocol.	X		5
	Success and acceptance factors.	X		5
Implementation	Environments of coexistence and testing.	X		5
	Modification of libraries, APIs, source code, etc.	X		5
	Execution of test protocol.	X		5
Follow up	Change controls, risk management, quality management.	X		5
	Validation of success and acceptance factors.	X		5
Launching	Put into production.	X		5
	Delivery of documentation and user manuals.	X		5
			Average	5

Source: own work

Table 5. Transition model, Security.

Phase	Description	Yes	No	Score
Diagnostic	Reviewing security policies.	X		5
	Asset inventory review.	X		5
Planning	Security plan for the coexistence of the two protocols.	X		5
	Acceptance testing protocol.	X		5
Implementation	Server and service assurance.	X		5
	Running security tests.	X		5
Follow up	Running security tests.	X		5
	Security risk management.	X		5

(continúa)

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

(viene)

Phase	Description	Yes	No	Score
Launching	Adjustments to security policies.	X		5
	Delivery of documentation	X		5
			Average	5

Source: own work

Table 6. Weighting case of success.

Item	Score
Project Management	4.6667
Human Resouces	4.00
Infrastructure	5
Applications	5
Security	5
Total	**4.7333**

Source: own work

For the previous success case, a score of 4.73 was obtained, which indicates, according to the weighting given by ORCA, a total technological transition, implementation and eventual success case.

7. DISCUSSION AND CONCLUSIONS

Before the technological transition of the IPv6 protocol in the SNR, it was evidenced that the compatibility of the entity"s technological infrastructure was below 70%, causing the process to be estimated in detail, so that the connection with the new technology would not suffer trauma in terms of time and costs.

The design of the diagnostic plan for the IPv4 to IPv6 protocol allowed validating the technological infrastructure of the SNR and, in this way, it was possible to measure the degree of progress in the adoption of the new protocol.

Likewise, the development of this implementation allowed the SNR to know all the new configurations of the new protocol, and thus promoted technological progress, updating and advancing its technological infrastructure, having a significant result in the solution to its needs.

The DHCPv6 protocol allowed dynamic automation for addressing the new infrastructure of the SNR communications network.

e-ISSN 2357-6014 / Vol.17, n°. 2 / may - august 2021 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

The functionality tests for the double-stack services provided by the SNR were verified through web pages, according to the recommendations of the MinTIC issued in resolution 2710 of 2017.

This success case, close to 94% according to weighting, aims to guide companies and entities that need to adopt the transition process from IPv4 to IPv6 in order to speed up and order all the activities that must be taken into account when starting said appropriation and technological adaptation.

The contribution of this research, to continue with the understanding of the problem raised, is the detailed description of the minimum activities that must be carried out for the implementation of the technological transition from the IPv4 to IPv6 protocol.

Recognition.

To the ORCA and SciBas research groups for their methodological and implementation advice.

8. REFERENCES.

[1] I. Emanuel Maldonado Beltrán, D. Andrés Páez Sánchez, and I. S. José Patiño, "Despliegue de IPv6 para el desarrollo socioeconomico en America Latina y el Caribe," *Lacnic*, 2015. [Online]. Available: https://www.lacnic.net/innovaportal/file/3035/1/caf-lacnic-despliegue-ipv6-para-desarrollo-socio-economico-en-lac.pdf. p. 1

[2] C. H. Caicedo and A. Smida, "Intensidad informacional para la longitudinalidad asistencial en sistemas de salud," *Visión electrónica*, vol. 10, no. 1, pp. 83–95, Jun. 2016, doi: https://doi.org/10.14483/22484728.11612

[3] Sewan, "Cómo ha sido la evolución de las Telecomunicaciones," 2018. [Online]. Available: https://www.sewan.es/evolucion-de-las-telecomunicaciones

[4] A. S. Tanenbaum, "Redes de computadoras," [Online]. Available: https://books.google.es/books?id=WWD-4oF9hjEC&pg=PA459&lpg=PA459&dq=protocolo+de+puertas+de+enlace+-frontera&source=bl&ots=Xyl9UcreD5&sig=y-SZW6yXZvGl9y1DmOch2trVfdI&hl=es&sa=X#-v=onepage&q=protocolo de puertas de enlace frontera&f=false. [Accessed: 07-Jun-2020]. p. 1

[5] LACNIC, "Fases de Agotamiento de IPv4," *LACNIC.NET,* 2020. [Online]. Available: https://www.lacnic.net/web/lacnic/agotamiento-ipv4.

[6] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," *Internet Requests for Comments*, pp. 1–39, Dec. 1998, doi: https://doi.org/10.17487/RFC2460

[7] I. Society, "The Internet Ecosystem," *October*, 2010. [Online]. Available: http://www.isoc.org/pubpolpillar/docs/internetmodel.pdf.

[8] T. E. Board, "There May Soon Be Three Internets. America"s Won"t Necessarily Be the Best," *The New York Times*, New York, p. 1, 15-Oct-2018.

[9] G. Cicileo *et al.*, "IPv6 para Todos: Guía de uso y aplicación para diversos entornos," in *Books. Google.Com*, 2009, pp. 74–83.

[10] I. Society, "Sobre Internet Society," [Online]. Available: https://www.internetsociety.org/es/about-internet-society/

[11] S. Harris, "The Tao of IETF - A Novice"s Guide to the Internet Engineering Task Force", Aug. 2001, doi: https://doi.org/10.17487/RFC3160

[12] T. Berners-Lee, R. Fielding, and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", May 1996, doi: https://doi.org/10.17487/RFC1945

[13] IETF, "About IETF", *Website*, 2018. [Online]. Available: https://www.ietf.org/about/.

[14] A. Weinrib and J. Postel, "IRTF Research Group Guidelines and Procedures", *IRTF*, p. 1, Oct. 1996, doi: https://doi.org/10.17487/rfc2014

[15] "Internet Ecosystem", 2014. [Online]. Available: http://www.icann.org/sites/default/files/assets/governance-2500x1664-21mar13-en.png.

[16] I. Society, "Misión de ISOC". [Online]. Available: https://www.internetsociety.org/es/mission/. [Accessed: 02-Apr-2020]. p. 1

[17] ICANN, "Welcome to ICANN!" [Online]. Available: https://www.icann.org/resources/pages/welcome-2012-02-25-en. [Accessed: 03-Apr-2020]. p. 1

[18] ICANN, "Guía de inicio para Asesoramiento sobre políticas en el comité asesor AT-LARGE", *ICANN*, 2013. [Online]. Available: https://www.icann.org/en/system/files/files/alac-policy-advice-07nov13-es.pdf. [Accessed: 03-Apr-2020]. p. 1

[19] C. La, A. Nacional, D. E. E. Y. Se, and D. Otras, "Ley 1341 de 2009"Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la

Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones", *Ley No.1341 30 julio*, 2009. [Online]. Available: https://www.mintic.gov.co/portal/604/articles-3707_documento.pdf. p. 1

[20] Ministerio de Tecnologías de la Informacion, "Ministerio de Tecnologías de la Información y las Comunicaciones", 2013. [Online]. Available: https://www.mintic.gov.co/portal/inicio/Micrositios/IPV6/Documentacion/5903:Documentos-IPv6.

[21] I. Society, "Informe de la política pública: Adopción de IPv6". [Online]. Available: https://www.internetsociety.org/es/policybriefs/ipv6.

[22] Euro6IX and D. G. Mills, "Legal Aspects of the New Internet Protocol", in *Euro6ix*, 2011, p. 90.

[23] "Análisis comparativo de los Protocolos IPV6 e IPV4," *Ing. Solidar.*, vol. 5, no. 9, pp. 42–53, 2010. [Online]. Available: https://revistas.ucc.edu.co/index.php/in/article/view/465

[24] I. Elizalde, "¿Quién está listo para la implementación de IPv6?," *EditorTIC.es*, 2019. [Online]. Available: https://directortic.es/noticias/quien-esta-listo-la-implementacion-ipv6-20190401 21249.htm.

[25] M. A. Naagas, N. A. Macabale Jr, and T. D. Palaoag, "IPv6 campus transition: A Central Luzon State University case study," *Bull. Electr. Eng. Informatics*, vol. 9, no. 3, Jun. 2020, doi: https://doi.org/10.11591/eei.v9i3.2173

[26] BT, "BT for global business", 2020. [Online]. Available: https://www.globalservices.bt.com/en/solutions/products/diamond-ip.

[27] Gesatel, "Gesatel - La Empresa", *Gesatel*, 2017. [Online]. Available: http://www.gesatel.com/la-empresa/.

[28] N. CABLE, "NipBR CABLE", http://www.nipcable.com.br/, 2020. [Online]. Available: http://www.nipcable.com.br/.

[29] "Gtd - Internet Dedicado". [Online]. Available: https://www.gtd.cl/negocios/internet/internet-dedicado.

[30] "Gtd - Información Corporativa". [Online]. Available: https://www.gtd.cl/nuestra-empresa/informacion-corporativa.

[31] "COOPEALFARORUIZ R.L. - Cooperativa de Electrificación para la zona de Zarcero". [Online]. Available: http://www.coopealfaroruiz.com/.

[32] U. N. de Loja, "Servicios Tecnológicos", *Universidad de Loja*, 2019. [Online]. Available: https://unl.edu.ec/servicios-tecnologicos.

[33] "Cablecolor". [Online]. Available: https://cablecolor.hn/corporativo/index.php.

[34] M. Telecom, "Internet Dedicado", *MCM Telecom*, 2018. [Online]. Available: https://mcmtelecom.com/servicios/internet/.

[35] IDU, "Inicio", *IDU web*, 2016. [Online]. Available: https://openerp.idu.gov.co/.

[36] M. de T. de la I. y las Comunicaciones, "MinTIC es ejemplo en la implementación del protocolo IPv6," *MinTIC*, 2017. [Online]. Available: https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/7195:MinTIC-es-ejemplo-en-la-implementacion-del-protocolo-IPv6.

[37] C. A. Castillo Medina and F. Forero Rodríguez, "Caracterización de IPv6," *Rev. Tecnura*, vol. 17, no. 36, p. 111, 2013, doi: https://doi.org/10.14483/udistrital.jour.tecnura.2013.2.a09

[38] LACNIC, "¿Quiénes implementan?," *LACNIC.NET*, 2019. [Online]. Available: https://www.lacnic.net/3042/1/lacnic/quienes-implementan.

[39] Lacnic, "Fases de Agotamiento de IPv4," *LACNIC.NET*, 2020. [Online]. Available: https://www.lacnic.net/agotamiento.

[40] M. de las T. de la información y Comunicaciones, "Resolución 2710 de 2017," *MinTIC*, 2017. [Online]. Available: https://www.mintic.gov.co/portal/604/articles-61000_documento.pdf.

[41] D. C. Fonseca Catro, "PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED Ipv4 A Ipv6 BASADO EN LAS MIN TIC COLOMBIA", Universidad de Cundinamarca, 2018. [Online]. Available: http://hdl.handle.net/20.500.12558/1375.

[42] C. Salazar and E. Romero, "Planeación Para Adoptar El Protocolo De Internet Versión 6 (Ipv6) En La Alcaldía De Acacías (Meta)", Universidad Piloto de Colombia, 2018. [Online]. Available: http://repository.unipiloto.edu.co/handle/20.500.12277/4689.

[43] W. Wang, "Next generation Internet and IPv6 transition," *China Commun.*, vol. 12, no. 3, pp. 151–152, 2015, doi: https://doi.org/10.1109/cc.2015.7084372

[44] Y. Cui, Q. Sun, K. Xu, W. Wang, and T. Lemon, "Configuring IPv4 over IPv6 Networks: Transitioning with DHCP", *IEEE Internet Comput.*, vol. 18, no. 3, pp. 84–88, 2014, doi: https://doi.org/10.1109/MIC.2014.49

[45] N. Leavitt, "IPv6: Any closer to adoption?," *Computer (Long. Beach. Calif).*, vol. 44, no. 9, pp. 14–16, 2011, doi: https://doi.org/10.1109/MC.2011.284

[46] M. Nikkhah and R. Guerin, "Migrating the Internet to IPv6: An Exploration of the When and Why," *IEEE/ACM Trans. Netw.*, vol. 24, no. 4, pp. 2291–2304, 2016, doi: https://doi.org/10.1109/TNET.2015.2453338

[47] M. Babik et al., "IPv6 Security", *J. Phys. Conf. Ser.*, vol. 898, no. 10, 2017, doi: https://doi.org/10.1088/1742-6596/898/10/102008

[48] J. A. Velásquez, "Modelo de transición hacia IPv6," *Cintel*, 2012. p. 12

[49] Ministerio de Tecnologías de la Información y las Comunicaciones, "Cartilla Guía de Transición de IPv4 a IPv6," *MinTIC*, 2017. [Online]. Available: https://www.mintic.gov.co/portal/604/articles-102239_recurso_1.pdf.

[50] M. Blanchet, "A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block", no. 3531. pp. 1–7, 2003, doi: https://doi.org/10.17487/RFC3531

[51] G. Huston, A. Lord, and P. Smith, "IPv6 Address Prefix Reserved for Documentation", 2004, doi: https://doi.org/10.17487/rfc3849

[52] LACNIC, "Dual stack o pila doble", *LACNIC.NET*, 2019. [Online]. Available: https://www.lacnic.net/3091/1/lacnic/dual-stack-o-pila-doble.

[53] J. C. Taffernaberry, "Mecanismos de Transición hacia redes IPv6", 2011. [Online]. Available: http://sedici.unlp.edu.ar/bitstream/handle/10915/4193/Documento_completo.pdf?sequence=1&isAllowed=y. [Accessed: 30-Jul-2020]. p. 1

[54] R. Gilligan and E. Nordmark, "RFC 4213: Transition mechanisms for IPv6 hosts and routers", pp. 1–22, 2005, doi: https://doi.org/10.17487/RFC4213

[55] A. Hamarsheh and Y. AbdAlaziz, "Transition to IPv6 Protocol, Where We Are?," in 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–6, , doi: https://doi.org/10.1109/ICCISci.2019.8716482

[56] N. Red, "Curso IPv6 Forum Certified Engineer (Silver) CNE6-1", 2018. p. 1

[57] M. de T. de la información y las Comunicaciones, "Guía para el Aseguramiento del protocolo IPv6", 2015. [Online]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf. p. 1

[58] IBM, "Cortafuegos de filtro de paquetes IP", *IBM*, 2015. [Online]. Available: https://www.ibm.com/support/knowledgecenter/es/POWER8/p8ha5/packetfilterfirewall.htm.

[59] E. Borges, "Tipos de Servidores Web - Características, Ventajas y Desventajas", *InfranetWorking*, 2016. [Online]. Available: https://blog.infranetworking.com/tipos-de-servidores-web/.

[60] LACNIC, "Despliega IPv6", 2019. [Online]. Available: https://www.lacnic.net/2938/1/lacnic/wp-content/uploads/2015/02/ipv6_operadores_red-tablets.pdf.

[61] E. Davies, S. Krishnan, and P. Savola, "IPv6 Transition/Co-existence Security Considerations", Sep. 2007, doi: https://doi.org/10.17487/rfc4942

[62] C. García Martín, "Análisis de seguridad en redes IPv6", 26-Jul-2012. [Online]. Available: https://e-archivo.uc3m.es/handle/10016/16707.

[63] J. S. Sansa-Otim and A. Mile, "IPv4 to IPv6 Transition Strategies for Enterprise Networks in Developing Countries", 2013, pp. 94–104, doi: https://doi.org/10.1007/978-3-642-41178-6_10

[64] S. Cristina and R. Erazo, "Modelo para la evaluación de la efectividad de la tecnología informática en el entorno empresarial A model for assessing information technology effectiveness in the business environment," *Rev. Ing. e Investig.*, vol. 28 No. 2, no. 2, pp. 158–166, 2008.

[65] N. Phu, M. Nguyen, N. Q. Anh, T. Rantapuska, J. Utriainen, and M. Matilainen, "Transition From IPv4 To IPv6 : A Method for Large Enterprise Networks", INNOV 2012 First Int. Conf. Commun. Comput. Networks Techno*l.*, no. c, pp. 5–14, 2012.